Hybrid Mesh Network Security

22 April 2026

SASE

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2024 - 2026 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Patent Notice

SASE is protected by the following patents in the United States and elsewhere. This page is intended to serve as notice under 35 U.S.C. § 287(a):
US10,440,762, US11,271,899, US11,502,993, US11,558,184, US11,777,718, US11,888,815, US12,010,132

Revision History

Date	Description
20 April 2026	Added release notes for Linux agent 10.0.6.996
20 April 2026	Added release notes for Mac agent 12.7.4.9577
20 April 2026	Added release notes for Windows agent 12.7.4.14246
20 April 2026	Added release notes for Windows agent 12.4.2.14245

Date	Description
16 April 2026	Added release notes for Mac agent 12.7.3.9355
16 April 2026	Added release notes for Windows agent 12.7.3.13958
07 April 2026	Added SASE platform release notes for March 2026.
23 March 2026	Added release notes for Windows agent 12.7.0.13190
17 March 2026	Added release notes for Mac agent 12.7.0.8565
05 March 2026	Added release notes for Mac agent 12.6.0.8419
02 March 2026	Added release notes for Windows agent 12.6.0.12786
02 February 2026	Added SASE platform release notes for February 2026.
24 February 2026	Added *"Managing SASE MSSP Tenants in Check Point Portal" on page 1183*
24 February 2026	Added *"Updatable Objects" on page 923*
19 February 2026	Added release notes for Linux agent 10.0.5.962
13 February 2026	Added release notes for Mac agent 12.5.1.8141
12 February 2026	Added *"Pre-Login Tunnel Connection for Windows" on page 146*
11 February 2026	Added release notes for Windows agent 12.4.1.12192
9 February 2026	Added release notes for Windows agent 12.5.0.11894 (Beta)
2 February 2026	Added SASE platform release notes for January 2026.
22 January 2026	Added *"Palo Alto Redundant Tunnel" on page 446*

Date	Description
20 January 2026	Added release notes for Mac agent 12.3.0.7524
5 January 2026	Added SASE platform release notes for December 2025.
30 December 2025	Added *"Enhanced Network" on page 173*
30 December 2025	Updated regions for *"Regions and Point-of-Presence" on page 157*
30 December 2025	Updated regions: ■ *"Microsoft Entra ID (formerly Azure AD) (App Registration)" on page 1067* ■ *"Microsoft Entra ID (formerly Azure AD) (Enterprise Application)" on page 1050* ■ *"Microsoft Entra ID (formerly Azure AD) (SAML 2.0)" on page 1036*
26 December 2025	Added release notes for Windows agent 12.4.0.10709.
12 December 2025	Added *"Configuring Check Point Maestro VSX Redundant IPsec Tunnel" on page 356*
12 December 2025	Added *Configuring Check Point Maestro Redundant IPsec Tunnel*
10 December 2025	Added release notes for Windows agent 12.3.0.10330.
8 December 2025	Added *"Threat Prevention Exceptions" on page 830*.
2 December 2025	Added SASE platform release notes for November 2025.
20 November 2025	Added release notes for Linux agent 10.0.4.947.
19 November 2025	Added release notes for Mac agent 12.2.0.6683.
18 November 2025	Added release notes for Windows agent 12.2.0.9608.

Date	Description
10 November 2025	Added SASE platform release notes for October 2025.
05 November 2025	■ Added: • **Automatically sign out non-active user after** settings under **General Configuration**. See *"User Configuration Profiles" on page 92*. • **Certificate Issuer & CA** device posture check requirement. See *"Posture Check" on page 109*. ■ Replaced **Certificate** device posture check requirement with **Certificate subject**. See *"Posture Check" on page 109*.
04 November 2025	Added Release notes for Android Agent 8.2.0.3395.
29 October 2025	Added release notes for Mac agent 12.1.0.6369.
24 October 2025	Added *"Data Loss Prevention" on page 836*.
22 October 2025	Added release notes for Windows agent 12.1.0.9079.
07 October 2025	Added SASE platform release notes for September 2025.
29 September 2025	Added release notes for: ■ Windows agent 12.0.0.8750 ■ Mac agent 12.0.0.6063
11 September 2025	Added *"Operational Events" on page 887*.
09 September 2025	Added release notes for Mac agent 12.0.0.6019.
02 September 2025	Added *"Device Isolation" on page 102*.
29 August 2025	Added SASE platform release notes for August 2025.

Date	Description
22 August 2025	Replaced **Diffie-Hellman Group** with **Key Exchange Method**.
14 August 2025	Added iOS agent 8.4.1.5570 release notes.
12 August 2025	Added SASE platform release notes for July 2025.
07 August 2025	■ Added: • Release notes for Mac Agent 11.7.0.5477 • Release notes for Android Agent 8.1.3.3382 • *"Enterprise Browser" on page 874* ■ Updated *"Downloads" on page 118*.
04 August 2025	Added release notes for Mac Agent 11.7.0.5310
31 July 2025	Added *"Tenant Restrictions" on page 817*.
29 July 2025	Added: ■ *"Using Model Context Protocol (MCP) Server with SASE" on page 1140* ■ *"Multiuser and User Switching on Shared Devices (Windows only)" on page 149*
07 July 2025	Renamed **Unified Log View** to **Security Events**. See *"Security Events" on page 881*.
01 July 2025	Added SASE platform release notes for June 2025.
30 June 2025	Added: ■ Release notes for Linux agent 10.0.3.933. ■ *"Remote Sign-In of Linux Devices to Private Access" on page 144*.
11 June 2025	Added release notes for Mac Agent 11.6.1.4855.
30 May 2025	Added SASE platform release notes for May 2025.
28 May 2025	Added release notes for Mac agent 11.6.0.4498.
22 May 2025	Updated Data Residency in *"Introduction to Check Point SASE" on page 42*.
21 May 2025	Added release notes for Windows agent 11.6.0.2555.

Date	Description
15 May 2025	Added *"Threat Prevention Policy " on page 823*.
13 May 2025	Added SASE iOS agent 8.4.0.4488 release notes.
08 May 2025	■ Added Application Policy in *"Access Policy" on page 778*. ■ Added SASE platform release notes for April 2025.
23 April 2025	Added release notes for Linux agent 10.0.2.915.
11 April 2025	Added *"Security Events" on page 881*.
07 April 2025	Replaced Web Filter Rule with Access Policy. See *"Access Policy" on page 778*
03 April 2025	Added SASE platform release notes for March 2025.
01 April 2025	Added release notes for Mac agent 11.5.0.4178.
28 March 2025	Added: Internet Access Speed in *"Internet Access" on page 775*. Transparent Internet Access Installation in *"Deploying the SASE Agent" on page 121*.
27 March 2025	Added release notes for Windows agent 11.5.0.2501.
03 March 2025	Added: ■ *"Cisco Firepower" on page 279* ■ URL Aliasing for Zero-Trust Applications on SASE in *"Certificate Manager" on page 1133* ■ SASE platform release notes for February 2025.
24 February 2025	Updated *"Managing a Network" on page 223*.
19 February 2025	Added *"SaaS API" on page 872*.
30 January 2025	Added SASE platform release notes for January 2025.
24 January 2025	Added *"MDM Deployment of the SASE MacOS Agent with Internet Security" on page 131*.

Date	Description
22 January 2025	■ Added *"Member Roles and Permissions" on page 75*. ■ Added release notes for: • Windows agent 11.2.1.2378 • Mac agent 11.2.1.3411
06 January 2025	Updated *"Regions and Point-of-Presence" on page 157*.
31 December 2024	■ Added *Resolving MDM Deployment Issues on MacOS*. Added SASE platform release notes for December 2024.
23 December 2024	Added *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 300*.
05 December 2024	Added SASE Linux agent 10.0.0.879 release notes.
29 November 2024	Added SASE Android / Chromebook agent 8.1.2.3355 release notes.
27 November 2024	Added SASE platform release notes for November 2024.
12 November 2024	Added SASE Windows agent 11.1.0.2248 release notes.
03 November 2024	Added information about DenyUnauthenticatedBind.
30 October 2024	■ Added SASE platform release notes for October 2024. ■ Updated the commands for Silent Installation of macOS agent to address the macOS agent installation file name. See *"Deploying the Agent Using an MDM Application" on page 122*.
21 October 2024	Added: ■ *"SASE Agent - Optimized Performance with Minimal Resource Impact" on page 144* ■ SASE Windows agent 11.0.11.2205 release notes. ■ SASE MacOS agent 11.0.10.2696 release notes.
01 October 2024	Added SASE Windows agent 11.0.10.2177 release notes.

Date	Description
30 September 2024	■ Added support for a new client type - **Native**. See *"Adding an RDP Zero Trust Application" on page 749*. ■ Added SASE platform release notes for September 2024.
25 September 2024	Added SASE Agent release notes: ■ Android / Chromebook agent 8.1.0.3337 ■ iOS agent 8.3.0.2600
16 September 2024	Added *"Data Residency" on page 46*.
30 August 2024	Added SASE platform release notes for August 2024.
28 August 2024	Added: ■ SASE Agent release notes: • Windows - *"11.0.1.2083" on page 1225* • macOS - *"11.0.1.2339" on page 1236* ■ *"Configuring Check Point Redundant IPsec Tunnel" on page 326*
09 August 2024	Added a new section for .msi installation flags for version 11.0 and above, to address the change in Windows agent installation file name. See *"Deploying the Agent Using an MDM Application" on page 122*.
07 August 2024	Added SASE MacOS agent 11.0.0.2227 release notes. See *Release Notes > SASE Agent > "MacOS" on page 1229*.
01 August 2024	Added SASE Platform release notes for July 2024. See *Release Notes > SASE Administrator Portal > 2024 > "July" on page 1214*.
31 July 2024	First release of the document in Check Point format.

Table of Contents

Introduction to Check Point SASE ... *42*
Private Access ... *42*
Internet Access ... *43*
SASE Agent ... *43*
Supported Devices and Operating Systems ... *44*
How it Works ... *45*
Use Cases ... *45*
Benefits ... *46*
Data Residency ... *46*
API Support ... *47*
Getting Started ... *48*
Check Point SASE Workspace in the Infinity Portal ... *49*
Creating an Account in the Check Point Portal ... *49*
Accessing the SASE Administrator Portal ... *49*
Licensing the Product ... *53*
Specific Service Roles ... *54*
Check Point SASE (Perimeter 81) Workspace ... *55*
Creating an Account in SASE (Perimeter 81) ... *55*
Activating SASE (Perimeter 81) Subscription ... *56*
SASE Pilot Checklist ... *57*
Defining the Pilot ... *57*
Preparing the Environment ... *57*
Configuring Policies ... *57*
Notifying Users ... *58*
Running the Pilot ... *58*
Evaluating and Deciding Rollout ... *59*
Preparing for Full Rollout ... *59*

Help Options 59
SASE User Rollout 60
Configuring Access Policies and Firewall Rules 60
Preparing Devices 60
Rolling Out in Phases 60
Communicating with Users 61
Monitoring the Deployment 61
Help Options 61
Migrating the SASE (Perimeter 81) Workspace to Check Point Portal 62
Using Check Point User Center for Billing and Subscription 62
Dashboard 64
Active Sessions 64
Member Licenses 65
Gateway Licenses 65
Applications 66
Active Agent Users 66
Users Bandwidth 67
OS Distribution 67
Device Type Distribution 67
Agent Version by OS 68
Team 69
Members 70
Invite Members 74
Inviting Members Manually 74
Inviting Members Using an Identity Provider 74
Member Roles and Permissions 75
Roles 75
User 75
Permissions 75
Restrictions 75

Admin ... 75
Permissions ... 76
Manager ... 76
Permissions ... 76
Restrictions ... 76
User Manager ... 76
Permissions ... 76
Restrictions ... 77
Network Manager ... 77
Permissions ... 77
Restrictions ... 77
Security Manager ... 77
Permissions ... 77
Restrictions ... 78
Billing ... 78
Permissions ... 78
Restrictions ... 78
Managing Members ... 79
Changing Member Role ... 80
Unblocking Members ... 84
Generating Sign-Out and Uninstall Code ... 84
Resetting a Member Password ... 85
Resetting Google Authenticator Two-Factor Authentication for a Member ... 85
Adding Licenses ... 87
Groups ... 89
Creating a Group ... 89
User Configuration Profiles ... 92
Adding a Configuration Profile ... 92
Web Platform Configuration ... 92
General Configuration ... 93

Agent Configuration ... 93
General Configuration ... 93
Agent Upgrades ... 94
Network Configuration ... 95
Windows ... 100
Use VPN Interface DNS ... 100
Notify Reconnect ... 101
Android / Chromebook ... 101
Default Protocol ... 101
Mac ... 101
Use VPN Interface DNS ... 101
iOS ... 102
Auto Reconnect ... 102
Device Isolation ... 102
Use Case ... 104
Devices ... ***105***
Device Inventory ... 106
OS Distribution ... 106
Posture Status ... 106
Device Inventory Details ... 107
Logging Out the Device ... 108
Removing Device ... 108
Posture Check ... 109
Supported Posture Requirement Checks ... 109
Specifying the Device Posture Check Requirements ... 110
Downloads ... 118
Downloading and Deploying the SASE Agent ... 118
Downloading the Certificate ... 120
Deploying the SASE Agent ... 121
Prerequisites ... 121

Deploying the Agent Manually ... 122
Deploying the Agent Using an MDM Application ... 122
Transparent Internet Access Installation ... 122
Common Commands ... 124
MDM Deployment of the SASE MacOS Agent with Internet Security ... 131
Deploying the Agent through MDM ... 131
Downloading the Certificate ... 131
Deploying the Content Filter and System Extension ... 131
Installing SASE on Chromebook ... 132
Using the SASE Agent ... 135
Troubleshooting System Extension Installation on macOS ... 141
SASE Agent - Optimized Performance with Minimal Resource Impact ... 144
Performance Efficiency ... 144
Typical Resource Usage ... 144
Remote Sign-In of Linux Devices to Private Access ... 144
Prerequisites ... 145
Use Case ... 145
Using the Linux Agent CLI for Private Access Login and Troubleshooting ... 145
Pre-Login Tunnel Connection for Windows ... 146
Use Cases ... 146
Prerequisites ... 146
Limitations and Technical Notes ... 146
Enabling Pre-Login Tunnel Connection ... 147
Multiuser and User Switching on Shared Devices (Windows only) ... 149
User Identification and Policy Assignment ... 150
Uninstalling the SASE Agent ... 150
Windows ... 150
macOS ... 151
Linux ... 152
Ubuntu ... 152

Android / iOS 152
Collecting Logs Manually 153
Windows 153
macOS 154
Linux 155
Networks 156
High-Level Procedure 156
Regions and Point-of-Presence 157
Gateways 160
Private Gateways 160
[DEPRECATED] Shared Gateways 160
Tunnels 163
IPSec Site-2-Site VPN Tunnel 163
WireGuard Connector Tunnel 164
OpenVPN Tunnel 165
Internal Network Subnet 165
Dynamic IP Tunnels 165
Creating a Network 166
Defining a Network 167
Adding Gateways to an Existing Network 169
Deactivating a Gateway 170
Enhanced Network 173
Benefits 173
Supported Regions 173
Creating an Enhanced Network 174
Adding a Tunnel 176
Choosing Tunnel Type 179
Dynamic Routing 180
Static Routing 184
Managing a Network 188

Editing a Network ... 188
Adding Regions ... 189
Managing Access ... 190
Managing Tunnels ... 192
Editing a Tunnel ... 192
Viewing Tunnel Details ... 195
Deleting a Tunnel ... 196
Adding a Tunnel ... 198
IPsec Site-to-Site VPN Tunnel ... 199
Prerequisites ... 199
IPSec Handshake ... 199
Phase I (IKE or Gateway) ... 199
Phase II (ESP or Tunnel): ... 199
Policy-Based and Route-Based IPSec Connection ... 200
Supported Integrations ... 201
High-Level Procedure ... 202
WireGuard Connector Tunnel ... 205
Prerequisites ... 205
For High Availability (Optional) ... 206
Configuring a WireGuard Connector Tunnel ... 206
Configuring the Connector in the Check Point SASE Administrator Portal ... 206
Installing the WireGuard Connector on a Linux Server ... 209
Configuring High Availability (Optional) ... 210
Overview ... 210
Setup Flow ... 210
How Failover Works ... 211
Verifying the Setup ... 212
For HA deployments: ... 212
Removing the WireGuard Connector ... 212
For HA deployments ... 213

OpenVPN Tunnel ... 214
Configuring the OpenVPN Tunnel in the Check Point SASE Administrator Portal ... 214
Installing a VPN and Configuring the OpenVPN Tunnel on the Device ... 216
Verifying the Setup ... 222
Verifying the Setup ... 222
Managing a Network ... 223
Editing a Network ... 223
Adding Regions ... 224
Managing Access ... 225
Firewall Rules ... 226
Split Tunneling ... 226
Private DNS ... 229
DNS Filtering ... 232
Routes Table ... 235
Deleting a Network ... 238
Segmenting Networks ... 239
Interconnectivity (Cloud-Agnostic) ... 241
IPSec Based Connections ... 241
Policy-based IPSec Tunnels ... 242
WireGuard Connector Based Connections ... 243
Interconnectivity Using AWS EC2 Instance ... 244
Integrating On-premises Firewall / Router or Cloud based Resources ... 245
High-Level Procedure ... 245
Prerequisites ... 247
Configuring the Tunnel in the Check Point SASE Administrator Portal ... 247
On-premises Firewall - Configuring the Tunnel in the Management Portal ... 257
Barracuda Firewall ... 258
Check Point Firewall ... 268
Pre-requisites ... 268
Configuration Steps ... 268

Creating Interoperable Device Object in the Check Point SmartConsole 268
Adding SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object 269
Creating VPN Start Community 273
Additional settings in Check Point SmartConsole 279
Cisco Firepower 279
Pre-requisites 279
Configuring IPsec Tunnel 280
Configuring the Tunnel in Cisco Firepower 285
Configuring the Static Route in the Cisco Firepower 293
Configuring Firepower Policies Allowing Traffic Flow 299
Configuring Check Point Cluster VIP Redundant IPsec Tunnel 300
Prerequisites 301
High Level Procedure 301
Part 1 - Configuration in SmartConsole 301
Step 1: Create Interoperable Device Object in the Check Point SmartConsole 301
Step 2: Add SASE Gateway IP Address and Remote Subnet to the Interoperable Device Object 303
Step 3: Create VPN Start Community 309
Step 4: Additional settings in Check Point SmartConsole 315
Step 5: Configure VPN Tunnel Interface and BGP 315
Step 6: Configure BGP Configuration 317
Part 2 - Configuration in the SASE Administrator Portal 320
Step 1: Configure Tunnel and Routes Table 320
Step 2: Verify the Setup 326
Configuring Check Point Redundant IPsec Tunnel 326
Pre-requisites 326
Part 1 - Configuration in SmartConsole 327
Step 1: Creating Interoperable Device Object in the Check Point SmartConsole 327

Step 2: Adding SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object ... 331
Step 3: Creating VPN Start Community ... 336
Step 4: Additional settings in Check Point SmartConsole ... 345
Step 5: Configuring VPN Tunnel Interface and BGP Configuration ... 345
Part 2 - Configuration in SASE Administrator Portal ... 350
Step 1: Configuring Tunnel and Routes Table ... 350
Step 2: Verifying the Setup ... 356
Configuring Check Point Maestro VSX Redundant IPsec Tunnel ... 356
Introduction ... 356
Prerequisites ... 356
Part 1 - Configuration in SmartConsole ... 357
Step 1: Create Interoperable Device Object in the Check Point SmartConsole 357
Step 2: Adding SASE Gateway IP Address and Remote SubnetTo The Interoperable Device Object ... 359
Step 3: Creating VPN Star community ... 365
Step 4: Additional settings in Check Point SmartConsole ... 372
Step 5: Configuring VPN Tunnel Interface and BGP Configuration ... 373
Part 2 - Configuration in SASE Administrator Portal ... 375
Step 1 : Configuring Tunnel and Routes Table ... 375
Step 2: Verifying the Setup ... 381
Cisco ASA Firewall ... 382
Cisco Meraki Router ... 396
D-Link DSR Series Router ... 398
DrayTek Vigor2862 Router ... 405
DrayTek Vigor3900 Router ... 407
EdgeMax Router ... 414
FortiGate Next Generation Firewall ... 416
Juniper Networks ScreenOS Firewall ... 420
Juniper (JunOS) SRX Firewall ... 426
Linksys Router ... 429

Netgear BR500 Router ... 432
Palo Alto Firewall ... 439
Palo Alto Redundant Tunnel ... 446
Pre-requisites ... 446
Configuration in Palo Alto WebGUI ... 446
Step 1: Configure Tunnel Interfaces ... 446
Step 2: Configure IKE Crypto Profile ... 448
Step 3: Configure IKE Gateway ... 449
Step 4: Configure IPsec Crypto Profile ... 451
Step 5: Configure IPsec Tunnels ... 452
Step 6: Configure BGP ... 452
Add BGP Peer Group and Peers (for redundancy) ... 453
Step 7: Configure Redistribution Profile and BGP Import Rules ... 456
Redistribution Profile ... 456
BGP Import Rules ... 457
Step 8: Configure Security Policies ... 460
Configuring the tunnel in the Management Platform ... 460
Step 1 : Configuring Tunnel and Routes Table ... 460
Step 2: Verifying the Setup ... 465
pfSense Firewall ... 466
SonicWall Firewall ... 472
Sophos XG Firewall ... 482
UniFi USG Firewall ... 488
WatchGuard Firewall ... 494
Zyxel USG Firewall ... 500
On-premises Router - Configuring the Tunnel in the Management Portal ... 505
Cisco Meraki Router ... 506
D-Link DSR Series Router ... 509
DrayTek Vigor2862 Router ... 516
DrayTek Vigor3900 Router ... 519

EdgeMax Router 526
Linksys Router 528
Netgear BR500 Router 532
Configuring the Cloud-based Resources 538
High-Level Procedure 538
Using the Configuration File for Tunnel Configuration 538
Uploading the Configuration File in the Check Point SASE Administrator Portal 539
Microsoft Azure 541
Tunnel Values 543
Uploading the Configuration File in the Check Point SASE Administrator Portal 543
Alibaba Cloud 546
Prerequisites 546
Step 1 - Configurations in Alibaba Cloud 546
Setting Up a Tunnel 546
Setting Access Rules in Alibaba Security Groups 547
Setting Routes in Alibaba Cloud 547
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal 548
AWS Virtual Gateway 555
Prerequisites 556
Step 1 - Configuring the Tunnel in the AWS Management Console 556
Configuring a Virtual Private Gateway 558
Creating a Virtual Private Network Connection 563
Configuring the Routing Rules to the Default Gateway 566
Configuring the Tunnel 567
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal 569
AWS Transit Gateway 575
Prerequisites 575
Step 1 - Configurations in the AWS Management Console 576
Creating the Transit Gateway and Transit Gateway Attachments 576
Creating the Transit Gateway Attachments 578

Creating the Transit Gateway VPC Attachments ... 578
Creating the Transit Gateway VPN Attachment ... 581
Configuring the Tunnel ... 583
Configuring the Routing ... 584
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal ... 586
AWS Redundant Tunnels - Virtual Private Gateway ... 592
Prerequisites ... 592
Step 1 - Configurations in the AWS Management Console ... 593
Creating a Virtual Private Gateway ... 593
Creating Two Customer Gateways ... 594
Creating Two Site-to-Site VPN Connections ... 596
Creating Static Routes ... 597
Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal ... 599
AWS Redundant Tunnels - Transit Gateway ... 606
Prerequisites ... 606
Step 1 - Configurations in the AWS Management Console ... 607
Creating a Transit Gateway ... 607
Creating Two Site-to-Site VPN Connections ... 608
Creating Static Routes ... 613
Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal ... 615
Azure Virtual Network Gateway ... 623
Prerequisites ... 623
Step 1 - Configurations in the Azure Management Portal ... 624
Creating a Gateway Subnet ... 625
Creating a Virtual Network Gateway ... 629
Creating a Local Network Gateway ... 634
Creating the IPSecTunnel Connection ... 638
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal ... 642
Verifying the VPN Connection in the Azure Management Portal ... 648
Azure Virtual Network Gateway Redundant Tunnels ... 649

Azure Redundant Tunnels - Virtual Network Gateway ... 650
Prerequisites ... 650
Step 1 - Configurations in the Azure Management Portal ... 650
Creating Local Network Gateways ... 652
Creating a Connection ... 654
Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal ... 660
Azure Virtual WAN Redundant Tunnels ... 667
Prerequisites ... 667
Azure Redundant Tunnels - Virtual WAN ... 667
Prerequisites ... 667
Step 1 - Configurations in the Azure Management Portal ... 668
Creating a Virtual Hub ... 669
Creating a Site ... 672
Connecting the Site to your Virtual Hub ... 675
Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal ... 680
Google Cloud Platform ... 687
Prerequisites ... 688
Step 1 - Configurations in the GCP Console ... 688
Creating a Virtual Private Gateway ... 688
Creating a Tunnel ... 689
Configuring the Routing Rules to the VPC Network ... 691
Allowing Incoming Connections from Check Point SASE Local Network Using Firewall Rules ... 692
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal ... 694
Google Cloud Platform (GCP) Redundant Tunnels ... 700
Prerequisites ... 700
Step 1 - Configurations in the GCP Console ... 701
Creating a VPN Gateway ... 701
Adding a Redundant VPN Tunnel ... 702
Configuring Border Gateway Protocol (BGP) Routes ... 707

Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal ... 710
Verifying the Setup in GCP Console ... 717
Google Cloud VPC Peering ... 718
Google Cloud DNS ... 719
Prerequisites ... 719
Enabling Private DNS with SASE Gateway ... 719
Heroku Enterprise ... 722
Prerequisites ... 722
Configuration Steps ... 722
IBM Cloud ... 723
Prerequisites ... 723
Step 1 - Configuring a VPN Gateway at the IBM Cloud Console ... 724
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal ... 728
Verifying the Setup in IBM Cloud Console ... 734
Verifying the Setup ... 735
Private Access ... 736
Firewall ... 737
Use Case ... 737
Prerequisite ... 737
Access Rules Order ... 737
Creating a Firewall Access Rule ... 737
Enabling or Disabling Firewall Logs ... 739
Applications ... 741
Use Case ... 741
Prerequisites ... 742
Adding an Application ... 742
Adding an HTTP/HTTPS Zero Trust Application ... 744
Adding an RDP Zero Trust Application ... 749
Prerequisite ... 749
Known Limitation ... 749

Adding an RDP ZTA ... 749
RDP Server Access Based on IdP ... 755
Additional Registry Configuration ... 756
Windows 7 ... 756
Windows Server 2016 ... 756
Windows Server 2019 ... 756
Troubleshooting ... 756
Upstream Error ... 756
Additional Troubleshooting Steps ... 757
Adding a SSH Zero Trust Application ... 759
Prerequisite ... 759
Adding a VNC Zero Trust Application ... 764
Prerequisite ... 764
Providing Application Access to Members ... 768
Application Policies ... 770
Creating an Application Access Policy ... 770
Assigning a Policy to an Application ... 773
Internet Access ... **775**
High-level Procedure ... 775
Unified Internet Access Policy with Check Point Firewall ... 776
Internet Access Speed ... 776
Factors Affecting Remote User Internet Speed ... 777
Access Policy ... 778
Application Policy ... 779
Support ... 779
Creating an Access Policy ... 779
Creating a Bypass Rule ... 790
Bypass Rules for Certificate Pinning ... 800
Default Bypass Rules ... 804
Finding the Process Name of an Application ... 815

Tenant Restrictions ... 817
Configuration Requirements for Tenant Restrictions ... 818
Supported Applications ... 819
Creating a Tenant Restriction ... 819
End User Behavior ... 822
Threat Prevention Policy ... **823**
Threat Prevention Components ... 823
Malware Protection ... 824
Threat Emulation ... 824
Threat Emulation receives files through these methods of delivery ... 825
Anti-Bot ... 825
Risk Calculation ... 825
Configuring and Managing Threat Prevention Policy ... 826
Logs and Monitoring ... 829
Threat Prevention Exceptions ... 830
Example Use Case ... 830
Key Concept ... 830
Key Principles ... 830
URL Exceptions ... 831
Creating URL Exceptions ... 831
File Exceptions ... 833
Creating File Exceptions ... 833
Managing Exceptions ... 835
Exception Properties Reference ... 835
Data Loss Prevention ... **836**
Use Case ... 836
Actions in DLP Rules ... 836
Known Limitations ... 836
Operations ... 836
File Upload ... 836

File Download ... 837
Creating a DLP Rule ... 839
Data Type Manager ... 850
Creating a Custom Data Type ... 851
Creating a Custom Data Type Group ... 856
Adding an existing Data Type to a Group ... 858
Managing a Data Type or Group ... 860
Managing Microsoft Sensitivity Labels for DLP ... 864
Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview ... 865
Step 2 - Creating Microsoft Sensitivity Labels in SASE ... 866
Step 3 - Assign Sensitivity Labels to DLP Rules ... 871
DLP Logs ... 871
SaaS API ... ***872***
Enterprise Browser ... ***874***
Key Capabilities ... 874
Use Case ... 875
Prerequisites ... 875
Configuring Enterprise Browser ... 875
Step 1: Creating an Application Access Policy ... 875
Step 2: Defining Application Policy ... 877
Step 3: Accessing the Admin Console of Enterprise Browser ... 879
Step 4: Downloading the Enterprise Browser ... 880
Monitor & Logs ... ***881***
Security Events ... 881
Supported Events ... 882
Statistics ... 883
Events ... 884
Card ... 886
Operational Events ... 887

Supported Events ... 887
Statistics ... 888
Events ... 889
Card ... 890
Active Sessions ... 892
Action ... 893
Member Activity ... 895
Web Activity ... 897
Insights ... 897
Web Events Blocked ... 897
Top Web Categories ... 898
Events Per User ... 898
All Web Activities ... 898
Malware Protection ... 900
Insights ... 900
Incidents Blocked ... 900
Malware Types ... 901
Blocked Malware Per User ... 901
All Malware Activities ... 901
Admin Activity ... 903
Tunnels Status ... 907
Firewall Events ... 908
Objects ... **910**
Addresses ... 911
Creating an Address Object ... 911
Managing Addresses ... 912
FQDN-based Firewall Objects ... 914
FQDN Wildcards ... 914
Multi-Level Sub-domains ... 914
Important Considerations ... 914

Limitations ... 914
Services ... 916
Creating a Service Object ... 916
Managing Services ... 919
Custom URLs ... 920
Creating a Custom URL Object ... 920
Managing Custom URLs ... 922
Updatable Objects ... **923**
How Updatable Objects Work ... 923
Where Updatable Objects Are Supported ... 923
Supported Vendors ... 923
Settings ... **924**
Integrations ... 925
Security Information and Event Management (SIEM) Integrations ... 925
Professional Services Automation (PSA) Integrations ... 925
Splunk Cloud ... 925
Integrating Splunk Cloud ... 925
Step 1 - Setting Up the HTTP Event Collector ... 925
Step 2 - Enabling an HTTP Event Collector ... 925
Step 3 - Creating an Event Collector Token ... 926
Configuring the Splunk Integration in the Check Point SASE Administrator Portal ... 927
Troubleshooting ... 929
Microsoft Sentinel ... 930
Configuring the Integration in the Microsoft Azure Portal ... 930
Step 1 - Setting up a Log Analytics Workspace ... 930
Step 2 - Linking the Log Analytics Workspace to Microsoft Sentinel ... 931
Step 3 - Finding your Log Analytics Workspace ID and Primary Key ... 932
Configuring the Microsoft Sentinel Integration in the Check Point SASE Administrator Portal ... 933
Troubleshooting ... 934

Amazon S3 ... 934
Prerequisites ... 934
Configuring the Integration in the AWS Management Console ... 935
Step 1 - Creating a New Bucket ... 935
Step 2 - Creating a New IAM Policy ... 937
Step 3 - Creating an AWS User ... 939
Step 4 - Creating an AWS Access Key ... 939
Configuring the Amazon S3 Integration in the Check Point SASE Administrator Portal ... 941
Troubleshooting ... 942
ConnectWise PSA ... 943
Generating API Key in ConnectWise PSA ... 943
Configuring the Integration in the Check Point SASE Administrator Portal ... 947
Mapping Customers and Agreements ... 948
Identity Providers ... 950
SAML 2.0 ... 951
Generic SAML ... 951
Prerequisites ... 951
High-Level Procedure ... 951
Step 1 - Configure the SAML Identity Provider ... 951
Step 2 - Configure the Check Point SASE Administrator Portal ... 952
Active Directory Federation Services (AD FS) ... 954
Prerequisites ... 954
High-Level Procedure ... 954
Step 1 - Configure the AD FS Management Portal ... 955
Create a Relying Party Trust ... 955
Edit Claim Issuance Policy ... 959
Export the Signing Certificate ... 961
Step 2 - Configure the Check Point SASE Administrator Portal ... 962
Auth0 ... 964

Prerequisites ... 964
High-Level Procedure ... 964
Step 1 - Configure the Auth0 Management Portal ... 964
Step 2 - Configure the Check Point SASE Administrator Portal ... 968
Keycloak ... 970
Prerequisites ... 970
Integration Procedure ... 971
OneLogin ... 980
Prerequisites ... 980
High-Level Procedure ... 980
Step 1 - Configure the OneLogin Management Portal ... 980
Step 2 - Configure the Check Point SASE Administrator Portal ... 987
PingOne for Enterprise ... 989
Prerequisites ... 989
High-Level Procedure ... 989
Step 1 - Configure the PingOne Management Portal ... 989
Step 2 - Configure the Check Point SASE Administrator Portal ... 993
PingFederate ... 995
Prerequisites ... 995
High-Level Procedure ... 995
Step 1 - Configure the PingFederate Management Portal ... 995
Step 2 - Configure the Check Point SASE Administrator Portal ... 996
Rippling ... 998
Prerequisites ... 998
High-Level Procedure ... 998
Step 1 - Configure the Rippling Management Portal ... 999
Step 2 - Configure the Check Point SASE Administrator Portal ... 1005
JumpCloud ... 1007
Step 1 - Configure your JumpCloud Management Portal ... 1007
Step 2 - Configure the Check Point SASE Administrator Portal ... 1011

Okta with SAML 1013
Supported Features 1013
Prerequisites 1013
High-Level Procedure 1014
Step 1 - Configure the Okta Management Portal 1014
Step 2 - Configure the Check Point SASE Administrator Portal 1016
Step 3 - Assign the App 1018
Step 4 - Verify SP-initiated SSO 1019
Supported SAML Attributes 1019
Google Applications with SAML 2.0 1020
Prerequisites 1020
Step 1 - Configuring the Application in the Google Admin Console 1020
Step 2 - Configure the Check Point SASE Administrator Portal 1024
Google Services 1026
Prerequisites 1026
High-Level Procedure 1026
Step 1 - Generate the Google Client ID and Client Secret 1027
Step 2 - Enable the Admin SDK Service 1034
Step 3 - Configure the Check Point SASE Administrator Portal 1034
Microsoft Entra ID (formerly Azure AD) (SAML 2.0) 1036
Configure Microsoft Azure Portal 1036
Configure the Check Point SASE Administrator Portal 1044
Preventing User Duplication in Microsoft Entra ID 1046
Microsoft Entra ID (formerly Azure AD) (Enterprise Application) 1050
Registering Application through the Microsoft Azure Portal 1051
Configuring the Permissions for the Application 1056
Configuring the Key 1059
Configuring IDP Connection in SASE 1061
Assigning Users and Groups in Microsoft Azure 1065
Microsoft Entra ID (formerly Azure AD) (App Registration) 1067

Registering Application through the Microsoft Azure Portal 1067
Configuring the Permissions for the Application 1073
Configuring the Key 1076
Configuring IDP Connection in SASE 1078
Assigning Users and Groups in Microsoft Azure 1082
System for Cross-domain Identity Management (SCIM) 1085
Okta (SCIM) 1085
Prerequisites 1085
Enabling SCIM on Okta Management Portal 1086
Microsoft Entra ID (formerly Azure Active Directory) (SCIM) 1092
High-Level Procedure 1092
Part 1: Configure Entra ID 1092
Step 1 - Creating an application in Entra ID 1092
Step 2 - Configuring API Permissions 1101
Step 3 - Configuring Secret Key for the Application 1104
Part 2: Configuring SASE IDP 1105
Part 3: Configuring SCIM 1109
On-Premises Active Directory 1117
Enabling Active Directory/LDAP Connection 1118
Link to SASE and LDAP 1122
Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions 1129
Two-Factor Authentication 1129
Activating Two-Factor Authentication 1129
Configuring Duo Security for Two-Factor Authentication 1130
Deactivating Two-Factor Authentication 1131
Certificate Manager 1133
Uploading Domain SSL Certificates 1133
URL Aliasing for Zero-Trust Applications on SASE 1136
Support Access 1138
Granting the Support Access Role 1138

Access History 1139
Using Model Context Protocol (MCP) Server with SASE 1140
Features 1140
Supported Actions 1140
Security Guidelines 1141
SASE MCP Server Configuration 1141
Prerequisites 1141
High-Level Procedure 1141
Step 1 - Generate API Credentials 1141
Step 2 - Configure Bypass Rule for the AI Client 1144
Step 3 - Configure the AI Client 1145
Supported Client 1145
Management Host and Origin 1145
Configuring Claude Desktop 1146
Configuring Visual Studio (VS) Code 1147
Configuring Windsurf 1148
Configuring Cursor 1149
Step 4 - Install and Access the SASE MCP Server 1150
Managing SASE MSSP Tenants in Check Point Portal 1152
Prerequisites 1152
Onboarding a SASE Child Tenant 1152
Create a Child Tenant 1152
Add the SASE Service to the Child Tenant 1153
Supported PAYG SKUs 1153
User Management 1153
MSSP Parent Users 1154
Supported Roles 1154
Not Supported 1154
Grant Additional MSSP Parent Users Access to the Child Tenant 1154
Child Tenant SASE Members 1155

Usage and Billing 1155
Overview 1155
My Clients 1156
Member Licenses 1156
Gateway Licenses 1157
Organizations 1157
Adding an Organization 1157
Invoices 1161
Managing Billing 1162
Overview 1163
My Clients 1164
Member Licenses 1164
Gateway Licenses 1165
Organizations 1165
Adding an Organization 1165
Invoices 1169
Managing Billing 1170
Billing 1172
Manage Plan 1173
Updating the Subscription Plan 1173
Modifying Member Licenses 1175
Modifying Gateway / Application Licenses 1177
Adding a Payment Method 1179
Cancelling Subscription 1180
Invoices 1181
Billing Details 1181
Managing SASE MSSP Tenants in Check Point Portal 1183
Prerequisites 1183
Onboarding a SASE Child Tenant 1183
Create a Child Tenant 1183

Add the SASE Service to the Child Tenant ... 1184
Supported PAYG SKUs ... 1184
User Management ... 1184
MSSP Parent Users ... 1185
Supported Roles ... 1185
Not Supported ... 1185
Grant Additional MSSP Parent Users Access to the Child Tenant ... 1185
Child Tenant SASE Members ... 1186
Usage and Billing ... 1186
How-To and Troubleshooting References ... **1187**
How-To References ... 1187
Troubleshooting References ... 1187
Release Notes ... **1189**
Check Point SASE Administrator Portal ... 1190
2026 ... 1190
March ... 1190
February ... 1193
January ... 1195
2025 ... 1197
December ... 1197
November ... 1199
October ... 1201
September ... 1201
August ... 1202
July ... 1203
June ... 1204
May ... 1205
April ... 1207
March ... 1209
February ... 1210

January 1211
2024 1212
December 1212
November 1212
October 1213
September 1213
August 1214
July 1214
June 1215
May 1215
April 1215
March 1216
February 1216
January 1216
Check Point SASE Agent 1217
Windows 1218
12.7.4.14246 1218
12.4.2.14245 1218
12.7.3.13958 1218
12.7.0.13190 1218
12.6.0.12786 1219
12.5.0.11894 1220
12.4.1.12192 1220
12.4.0.10709 1221
12.3.0.10330 1221
12.2.0.9608 1222
12.1.0.9079 1222
12.0.0.8750 1222
11.7.0.2606 1223
11.6.0.2555 1223

11.5.0.2501 ... 1224
11.2.1.2378 ... 1224
11.1.0.2248 ... 1225
11.0.11.2205 ... 1225
11.0.10.2177 ... 1225
11.0.1.2083 ... 1225
11.0.0.2050 ... 1226
10.5.2.1979 ... 1226
10.5.1.1790 ... 1226
10.5.0.1760 ... 1227
10.4.3.1672 ... 1227
10.4.2.1645 ... 1228
MacOS ... 1229
12.7.4.9577 ... 1229
12.7.3.9355 ... 1229
12.7.0.8565 ... 1229
12.6.0.8419 ... 1230
12.5.1.8141 ... 1231
12.3.0.7524 ... 1231
12.2.0.6683 ... 1232
12.1.0.6369 ... 1232
12.0.0.6063 ... 1233
12.0.0.6019 ... 1233
11.7.0.5477 ... 1233
11.7.0.5310 ... 1234
11.6.1.4855 ... 1234
11.6.0.4498 ... 1234
11.5.0.4178 ... 1235
11.2.1.3411 ... 1235
11.0.10.2696 ... 1236

11.0.1.2339 ... 1236
11.0.0.2227 ... 1236
10.5.0.1476 ... 1237
10.4.2.1198 ... 1237
Linux ... 1238
10.0.6.996 ... 1238
10.0.5.962 ... 1238
10.0.4.947 ... 1238
10.0.3.933 ... 1238
10.0.2.915 ... 1239
10.0.1.885 ... 1239
10.0.0.879 ... 1239
9.0.1.843 ... 1239
9.0.0.832 ... 1240
8.1.0.778 ... 1240
iOS ... 1242
8.4.1.5570 ... 1242
8.4.0.4488 ... 1242
8.3.0.2600 ... 1242
8.2.0.1934 ... 1242
8.1.0.1831 ... 1243
8.0.0.1730 ... 1243
7.0.6.1 ... 1243
Android / Chromebook ... 1245
8.2.0.3395 ... 1245
8.1.3.3382 ... 1245
8.1.2.3355 ... 1245
8.1.0.3337 ... 1245
8.0.0.3276 ... 1246
7.1.9.2577 ... 1246

Glossary 1247

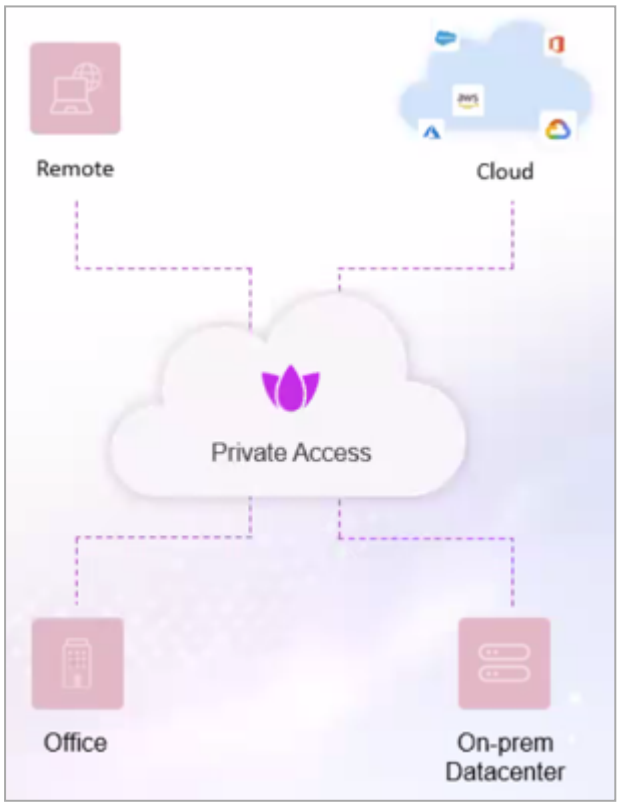
Introduction to Check Point SASE

Check Point SASE is a cloud-based Secure Access Service Edge (SASE) solution that provides secure private and internet access to your remote and branch office users.

Private Access

Private access includes:

- Complete Zero-Trust Network Access to all your corporate resources (on-premises and cloud data centers) to your remote or office workforce.

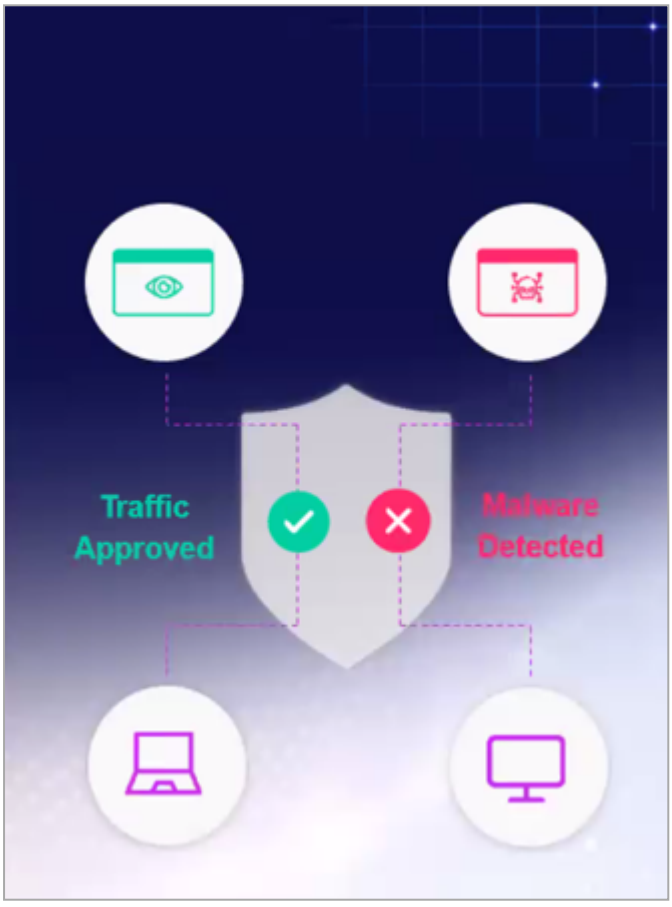


- Agentless access to only specific applications only to authorized members (also known as Application Access), for example, users with BYOD and contractors. The supported types of applications include:

Protocol	Sample Application
HTTP/HTTPS	Bitbucket
RDP	My Desktop
SSH	Staging Web Server
VNC	Build PC

Internet Access

Internet access includes safe access to all the web traffic to to your remote or office workforce.



SASE Agent

SASE Agent is an application that is installed on desktops or mobile devices to enforce safe private and internet access.

Note - The agent is not required for application access.

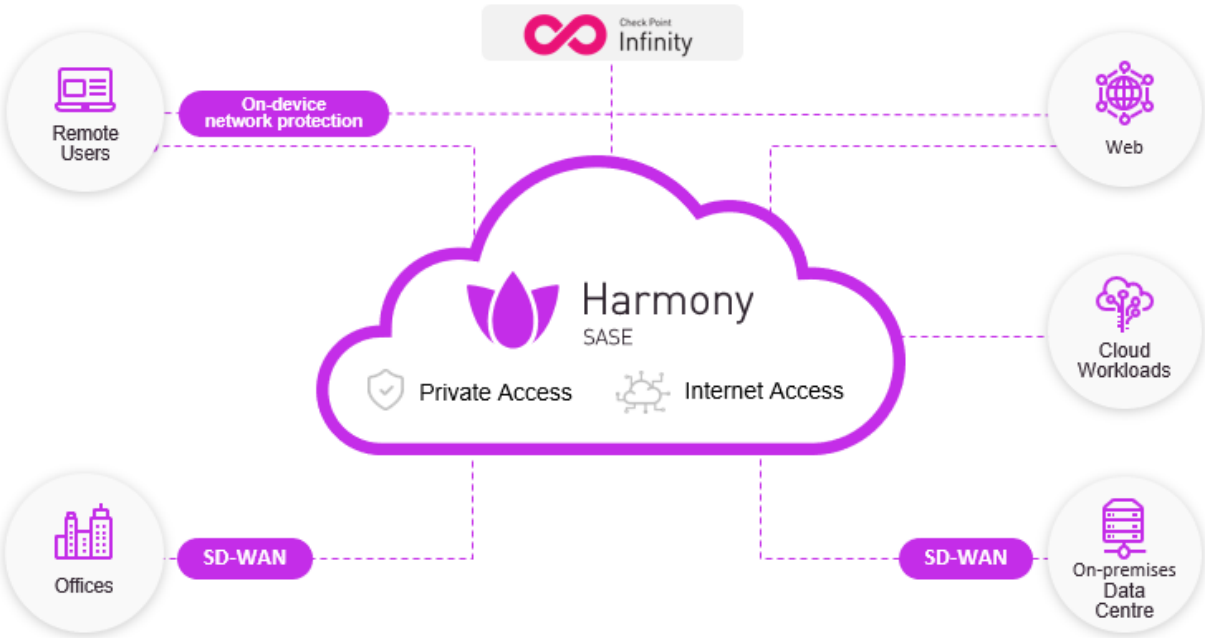
Supported Devices and Operating Systems

Operating System	Version	Action
Desktops and Servers		
Windows EXE	Windows 10 or later	EXE file is downloaded. For example, Perimeter81_ 10.1.1.1438.exe.
Windows MSI	Windows 10 or later	MSI file is downloaded. For example, Perimeter81_ 10.1.1.1438.msi.
macOS	macOS 11 or later	PKG file is downloaded. For example, Perimeter81_ 10.3.0.601.pkg
Ubuntu	Ubuntu 20.04 or later	Deb file is downloaded. For example, Perimeter81_ 8.0.4.735.deb.
Red Hat	RedHat 7 or later	RPM file is downloaded. For example, Perimeter81_ 8.0.4.735.rpm.
Fedora	Fedora 30 or later	RPM (Fedora) file is downloaded. For example, Perimeter81_ 8.0.4.735-fedora.rpm tar.xz.
Linux - Others	Linux 7.0 or later	tar.xz file is downloaded. For example, Perimeter81_ 8.0.4.735.tar.xz.
Mobile Devices		
Android / Chromebook	Android 8.1.0 or later	Redirected to Google play.
iOS	iOS 15 or later	Redirected to App store.

How it Works

SASE's cloud-gateway integrates with your SD-WAN (edge) devices in your branch offices or data centers. Its primary function is to process the private access rules, such as firewall rules and application rules. This gateway connects to the SASE Agent to provide a secure full network access. It also connects to a web portal (agentless) to provide secure application access.

For secure internet access, the SASE uses the in-built Secure Web Gateway (SWG) equipped with a Malware Protection Engine (On-device Network Protection capability) in the SASE Agent to process the *"Access Policy" on page 778* without requiring a separate gateway.



Use Cases

- You want to provide secure internet access to your remote workforce.
- You want to provide zero-trust network access to your remote workforce.
- You want to provide secure access to only particular corporate applications (not entire private access) to your temporary workforce, such as contractors.
- You want to provide both secure internet and private access to your workforce operating from your offices.

Benefits

- Easy-to-deploy SASE solution.
- 2x faster internet security with on-device protection.
- Improved privacy
- Accurate location services
- Web filtering
- Malware protection and traffic inspection
- Automatically detect and protect non-secure WiFi traffic
- Zero-trust access to network and SaaS
- Full mesh any-to-any connectivity to your private network.
- A SASE solution that also integrates with your on-premises or cloud SD-WAN infrastructure.
- Secure access to internal corporate applications (SSH, RDP, Web, Tunnel, and Database) residing in the data center, public or private clouds. Ideal for BYOD and third-party users with no agent installation or management required.

Data Residency

Data residency refers to the physical location where your data is stored and managed.

Data residency encompasses management plane and user information, which includes policy rules, settings, logs, and reports.

SASE supports data residency in these regions:

- EU
- US
- Australia
- India
- Canada

Note - Data Residency in EU ensures that data processing and storage occur entirely within the EU and it meets GDPR requirements for data storage and processing.

API Support

You can use SASE API to create, manage, and control network security aspects, including networks, gateways, regions, tunnels, users, and groups.

For more information about SASE API, see app.swaggerhub.com.

Getting Started

To get started with Check Point SASE:

1. Access the SASE workspace:
   - If you use the SASE workspace in the Check Point Portal:
     a. *"Creating an Account in the Check Point Portal" on the next page*.
     b. *"Accessing the SASE Administrator Portal" on the next page*.
   - If you use the SASE (Perimeter 81) workspace:
     a. Create an account in the SASE portal.
     b. Activate the Perimeter 81 subscription.
2. Invite members.
3. To provide a secure private access:
   a. Define your network.
   b. "Firewall" on page 737
   c. Deploy the Check Point SASE Agent on members' devices.
4. To provide a secure application access:
   a. Define your network.
   b. Define the application.
   c. Create application access rule.
5. To provide a secure internet access:
   a. Define access Policy.
   b. Define the bypass rules.
   c. Deploy the Check Point SASE Agent on members' devices.
6. Monitor:
   - Active sessions
   - Member activity
   - Web activity
   - Malware protection

- Admin activity
- Tunnel status
- Firewall events

Check Point SASE Workspace in the Infinity Portal

Creating an Account in the Check Point Portal

Check Point Portal is a web-based interface that hosts the Check Point security SaaS services.

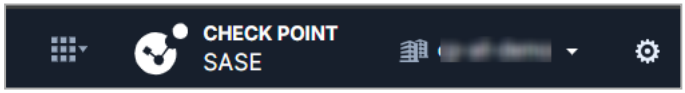
With Check Point Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Check Point Portal account, see the Check Point Portal Administration Guide.

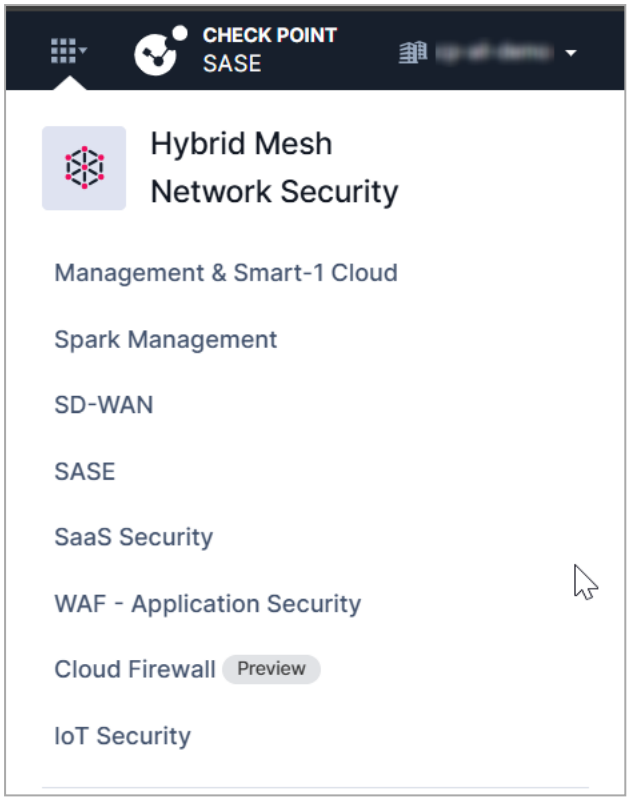
Accessing the SASE Administrator Portal

To access the SASE Administrator Portal:

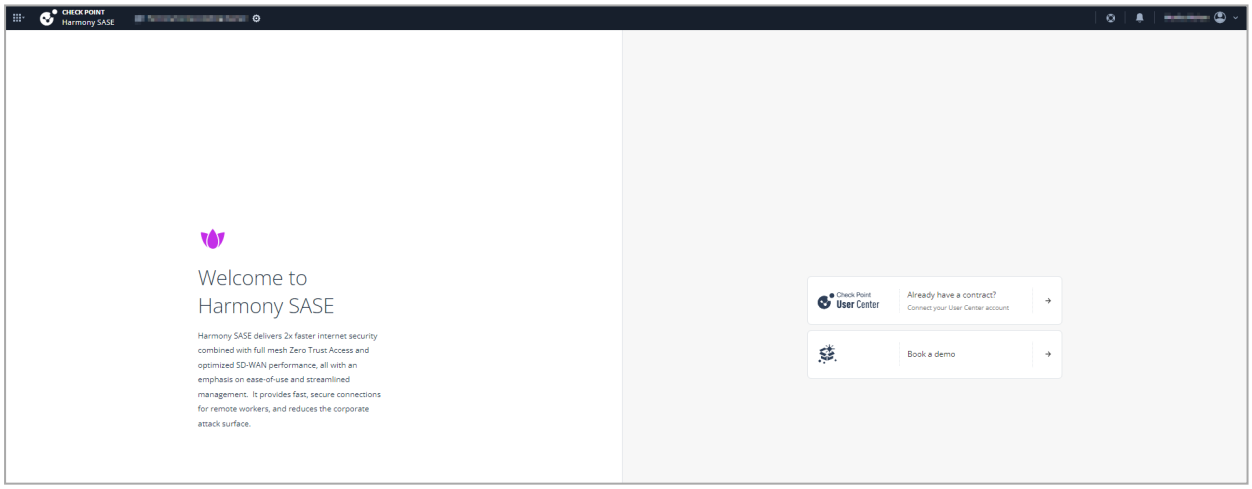
1. Sign in to Check Point Infinity Portal.
2. Click the **Menu** icon in the top left corner.



3. In the **Hybrid Mesh Network Security** section, click **SASE**.



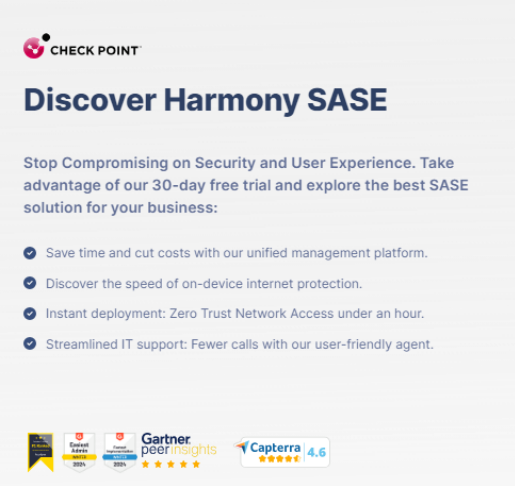
4. If you are accessing the portal for the first time, do one of these:



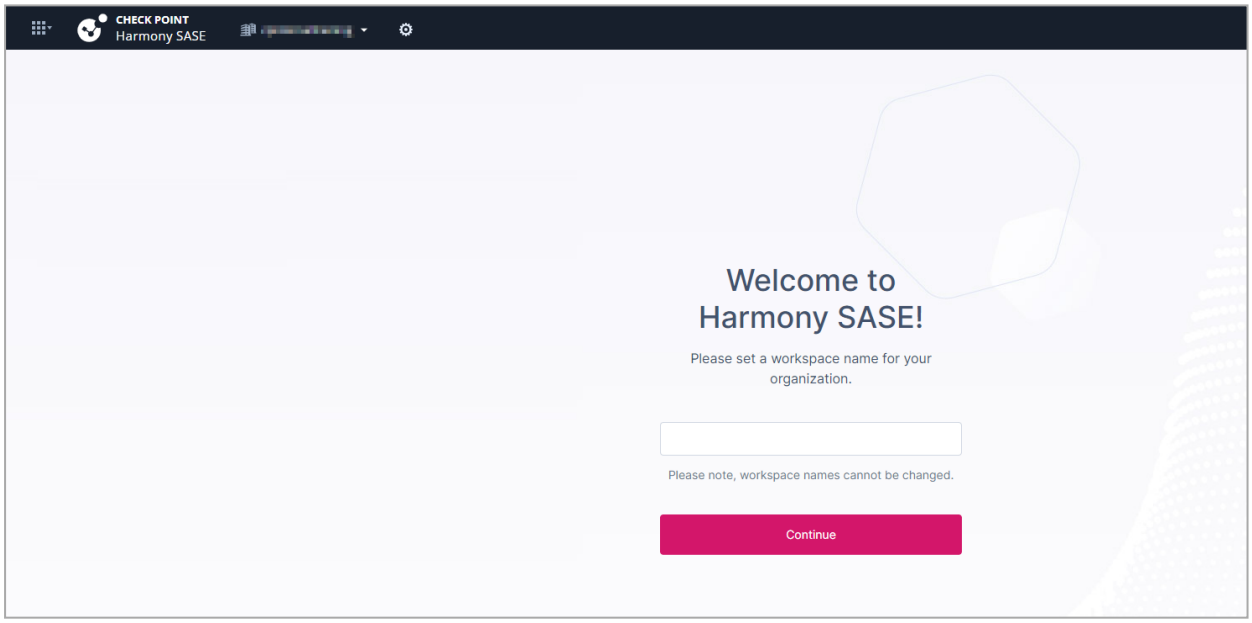
   - If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in Infinity Portal Administration Guide.

- If you want to trial the product, click **Book a demo**.

  Fill and submit the form. An email is sent with the trial status and further instructions to proceed.

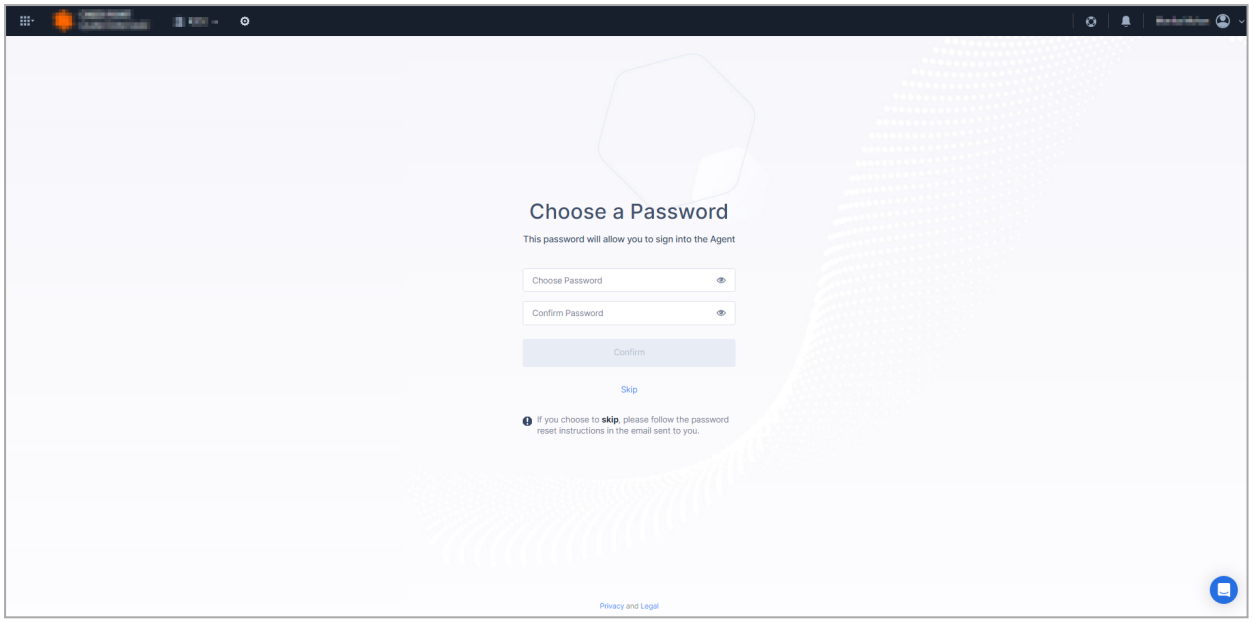


5. Once you fill and submit the form, or If you have already attached the contract with the product, the **Welcome to Check Point SASE** page appears.



6. Enter a name for your workspace. This is used when signing in to the SASE Agent and when accessing Zero Trust Architecture (ZTA) applications.
7. Click **Continue**.

   The **Choose a Password** page appears.



8. (Optional) Enter the credentials to log in to the SASE Agent.

   The password must be at least eight characters long with at least one:

   a. Upper case letter

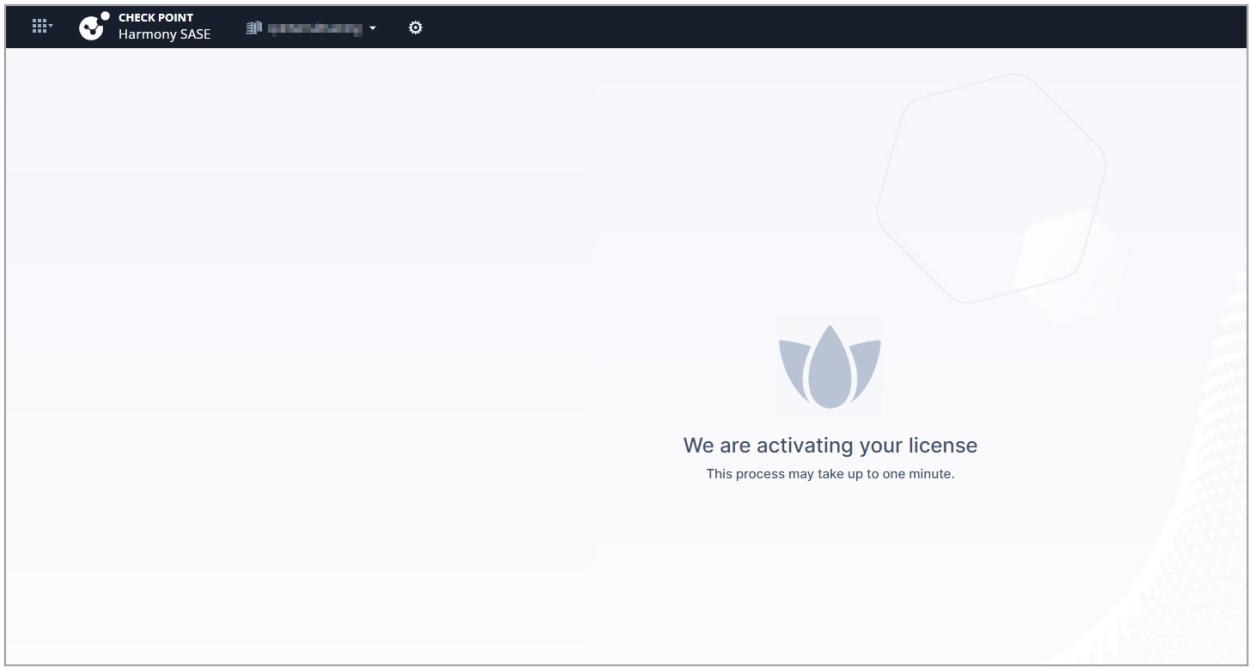
   b. Lower case letter

   c. Number 0-9

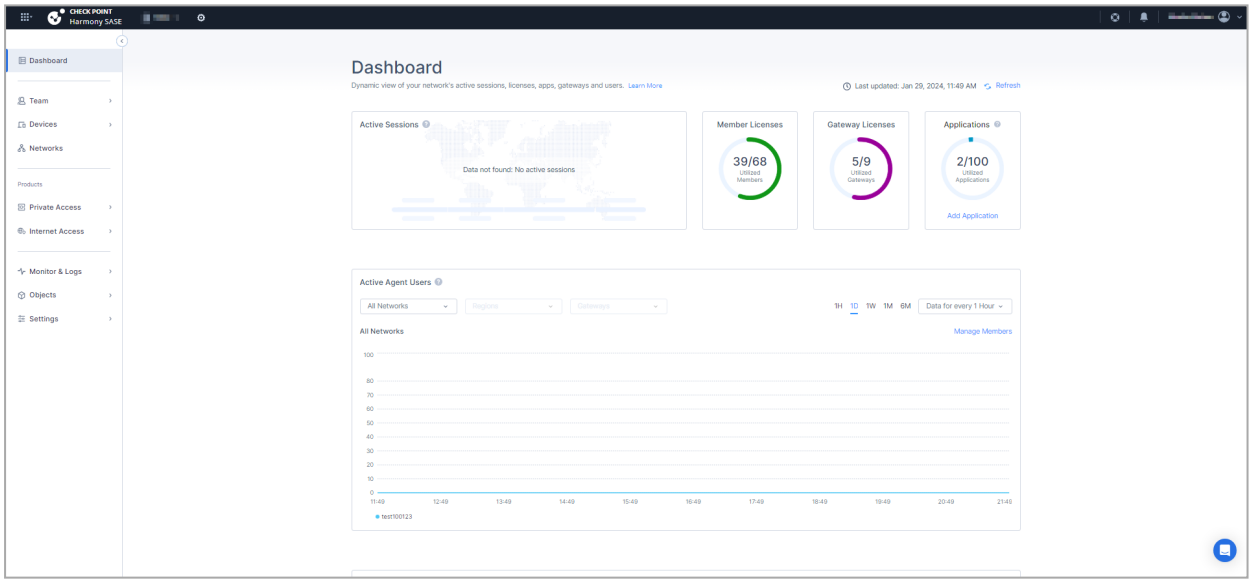
   d. Character !*#%$

   Notes - You can click **Skip** to skip this step. The system sends an email with instructions to reset the password.

9. Click **Confirm**.



The license gets activated and the Dashboard page appears.



Licensing the Product

When you create an account in the Check Point Portal and access the service, you get a free 30-day trial. After the 30-day trial period, you must purchase a software license to use the product. To purchase a license, you must create a Check Point User Center account. For instructions, see sk22716.

After you create a User Center account, contact your Check Point sales representative to purchase a license.

If you have licensed the product, you can view your current contract (license) information from the **Check Point Portal** > **Account Settings** > **Services & Contracts** page.

Specific Service Roles

SASE supports specific service roles. The specific service roles are in addition to the global roles and do not override them. For more information, see Specific Service Roles in the *Infinity Portal Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

Service Roles	Description
Admin	Provides read and write access to full application.
Read-Only	Provides full visibility across your Infinity Account.

Check Point SASE (Perimeter 81) Workspace

Creating an Account in SASE (Perimeter 81)

To create an account in Perimeter 81:

1. Go to Check Point SASE portal.

   The home page appears.

2. Click **Get Started**.
3. Enter:
   - **Name**
   - **Work Email address**
4. Click **Next**.
5. In the **Company Name** field, enter the name of your company.
6. From the **Company Size** list, select the approximate number of employees in your company.
7. Click **Next**.

   Perimeter 81 sends a confirmation code to your registered email address.

8. Enter the confirmation code.
9. Enter the workspace URL to log in to your tenant. For easy identification, Perimeter 81 recommends adding your organization's name in the URL.

   For example, if you enter the workspace URL as CompanyABC, then SASE creates the workspace URL as *https://CompanyABC.perimeter81.com*

   Note - You cannot change the workspace name after you create it.

10. Click **Next**.
11. Create a password to log in to your workspace.
12. Click **Get Started**.

    SASE creates the account and sends you a confirmation email.

    The dashboard page of your workspace appears.

    Note - Optionally, you can click **Get Started** in the confirmation email to go to your workspace's dashboard page.

Activating SASE (Perimeter 81) Subscription

Note - This is available only for the accounts in the Perimeter 81 workspace.

To activate your SASE (Perimeter 81) subscription:

1. Log in to your SASE (Perimeter 81) workspace.
2. In the **Dashboard** page, click **Activate Subscription**.
3. In the **Activate Your Plan** page, choose the billing plan.
4. Click **Continue to Payment** and complete the payment.

   Note - If you have issues to activate your subscription, contact *Check Point Support*.

SASE Pilot Checklist

A structured pilot helps validate your configuration, processes, and readiness to scale before a full rollout. This chapter provides a detailed checklist to help you run a successful SASE pilot.

Defining the Pilot

1. Select 10 to 50 users representing a mix of roles, device types, and locations.
2. Identify the specific resources (servers and applications) that pilot users need to access.
3. Set a timeline for the pilot, typically 2 to 4 weeks.
4. Define success criteria upfront, such as:
   - Percentage of active sessions by the first week
   - Support ticket volume
   - User feedback scores

Preparing the Environment

1. Create a network and establish IPSec tunnels from the network to required resources. See *"Defining a Network" on page 167*.
2. Remove or disable legacy VPN clients on all pilot devices.
3. Deploy the **Check Point SASE Agent** to managed devices via MDM (silent installation). See *"Deploying the SASE Agent" on page 121*.
4. For BYOD and contractor users, configure agentless Zero Trust Application access. See *"Applications" on page 741*.
5. Verify IdP integration and SCIM synchronization for all pilot users.

Configuring Policies

1. Create a dedicated group for pilot users in the SASE Administrator Portal. See *"Creating a Group" on page 89*.
2. Define cloud firewall rules (Private Access), starting with least privilege. See *"Creating a Firewall Access Rule" on page 737*.
3. If applicable, configure agentless application access rules (HTTP/HTTPS, RDP, SSH, VNC). See *"Application Policies" on page 770*.
4. Set up device posture profiles, if required by your organization.
5. Audit all firewall rules to ensure users can access the correct resources.

Notifying Users

Inform pilot users about the following:

1. What is changing
2. Why they were selected
3. What to expect on their devices
4. How to report issues
5. Timeline for the pilot

Running the Pilot

Week 1:

1. **Monitor**:

   Track these on a daily basis:

   - Active sessions
   - Device inventory
   - Firewall events

2. **Troubleshooting**:

   - Address low adoption by ensuring users are aware of the new system.
   - Identify users who are still using a legacy VPN or experiencing authentication issues.

After Week 2:

1. **Watch for edge cases**:

   - Identify unusual networks
   - Unanticipated applications
   - Device conflicts

2. **Validate with users (5 questions, 5 minutes)**:

   - Confirm whether the system is working as expected.
   - Ask whether performance is faster or slower.

- Identify any access gaps.
- Verify whether users are still using the legacy VPN.

Evaluating and Deciding Rollout

1. Compare pilot results against your predefined success criteria.
2. Proceed to rollout if all these conditions are met:
   - Majority of users have active sessions
   - Open issues are resolved
   - Support ticket volume is manageable
   - User feedback positive
3. Run another pilot iteration if any of these occur:
   - A significant number of users never connected
   - Policy gaps require substantial changes
   - Recurring issues remain unresolved

Preparing for Full Rollout

1. Document all issues encountered and how they were resolved.
2. Apply policy and firewall changes from the pilot.
3. Brief your help desk with the pilot issue log.
4. Plan the rollout sequence:

   Expand the rollout department by department. See SASE User Rollout.

Help Options

- Sent an email to SASE support or start a live chat.
- Reach out to your **Technical Account Manager*** for assistance.

  ** Available for qualifying plans only*

SASE User Rollout

This chapter describes the steps to roll out Check Point SASE to the workforce. Make sure the initial setup is complete, networks are configured, resources are connected, the team is invited, and agents are deployed.

Note - If running a small pilot, see *"SASE Pilot Checklist" on page 57*.

Configuring Access Policies and Firewall Rules

Before bringing users online, translate organizational security requirements into Check Point SASE configuration.

1. **Set up cloud firewall rules (Private Access):** Define which users and groups can access each internal resource, such as on-premises servers, cloud data centers, or SaaS applications. Start with least-privilege access and expand as required. See *"Private Access" on page 736*
2. **Configure agentless access (Zero Trust Application Access):** For BYOD users, contractors, or temporary workers, configure browser-based access to specific applications (HTTP/HTTPS, RDP, SSH, VNC). Do not require the full agent or network-level access. See *"Applications" on page 741*.
3. **Configure device posture checks:** Set up device posture profiles to verify that devices meet security requirements before access is granted. See *"Posture Check" on page 109*

Preparing Devices

1. **Remove legacy VPN clients:** Running a VPN with the Check Point SASE Agent can cause connectivity conflicts. Disable or uninstall legacy VPN software.
2. **Confirm agent deployment:** If the agent is not distributed through MDM with silent installation, deploy it. See the silent installation guide for token-based deployment.
3. **Verify Identity Provider (IdP) and SCIM provisioning:** If an Identity Provider is used, confirm that SCIM synchronization is active. This ensures that user and group memberships remain synchronized with the directory.

Rolling Out in Phases

1. **Start with a small group:** Select a department or team that can provide useful feedback. Monitor the user experience before expansion.
2. **Expand department by department:** After the initial group is stable, bring the next group online. Each group acts as a mini-pilot and requires validation.
3. **Validate at each stage:** Before expansion, confirm that policies work, users connect successfully, and no access issues remain unresolved.

Communicating with Users

Send a short message to each rollout group. Include:

- What is changing
- When it takes effect
- How to connect
- Where to get help
- Keep the message short and non-technical.

Monitoring the Deployment

Use the Check Point SASE Administrator Portal to monitor the rollout:

- **Dashboard:** Monitor active sessions, licenses, agent counts, bandwidth, and operating system and device distribution
- **Active Sessions:** View agent connections and Zero Trust Application access sessions
- **Device Inventory:** Verify agent installation status across devices
- **Logs and Activity Reports**: Review member activity, web activity, firewall events, and administrator activity

Watch for:

- Low adoption (agents deployed but few sessions - check user communication and legacy VPN status)
- Connection failures (review tunnel status and firewall events)
- Recurring support tickets (commonly authentication issues or VPN conflicts)

Help Options

- Sent an email to SASE support or start a live chat.
- Reach out to your **Technical Account Manager*** for assistance.

  ** Available for qualifying plans only*

Migrating the SASE (Perimeter 81) Workspace to Check Point Portal

Note - This is applicable only for the users with an existing SASE (formerly Perimeter 81) workspace and who want to migrate and access it through the Check Point Portal.

To migrate and access an existing SASE (formerly Perimeter 81) workspace through the Check Point Portal:

1. Create an account in the Check Point Portal.
2. If you already have a Check Point Portal account, make sure that the data residency of the account matches the data residency of the SASE (Perimeter 81) workspace. If the data residency does not match, then do one of these:
   - Contact *Check Point Support* to migrate the SASE (Perimeter 81) workspace to the same data residency region as your Check Point Portal account.
   - Create a new Check Point Portal account with the same data residency as the SASE (Perimeter 81) workspace.
3. To associate the Check Point Portal account with the SASE workspace, send a request to Check Point SASE support with these information:
   - SASE (Perimeter 81) workspace name
   - Check Point Portal account ID
   - Check Point Portal data residency region
4. To verify, access the SASE Administrator Portal from the Check Point Portal.

Using Check Point User Center for Billing and Subscription

After migration to Check Point Portal, you can continue to use the current billing process to manage subscription. However, you can optionally use User Center to manage licenses and subscription that allows you to use other Check Point products.

To create a User Center account and associate it with your Check Point Portal account:

1. Create a User Center account. See sk22716.
2. Obtain licenses for Check Point products. See sk22564.

3. Link the Check Point Portal account with the User Center account. See Associated Accounts.

Dashboard

The **Dashboard** page shows statistical data on:

- *"Active Sessions" below*
- *"Member Licenses" on the next page*
- *"Gateway Licenses" on the next page*
- *"Applications" on page 66*
- *"Active Agent Users" on page 66*
- *"Users Bandwidth" on page 67*
- *"OS Distribution" on page 67*
- *"Device Type Distribution" on page 67*
- *"Agent Version by OS" on page 68*

To view the **Dashboard** page, access **Check Point SASE** and click **Dashboard**.

Active Sessions

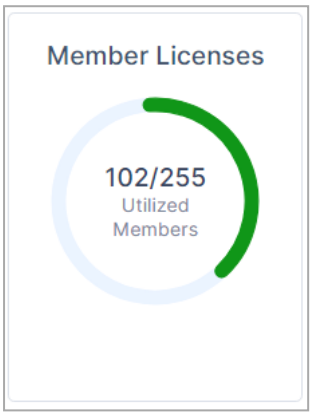
The **Active Sessions** widget shows:

- **Agent Sessions**: The number of users connected to a network through the Check Point SASE Agent.
- **App Sessions**: The number of users accessing the Zero Trust Applications.
- **Total Sessions**: Total number of Agent and Application sessions.

For example, if a member is connected to a network through the Check Point SASE Agent, and is accessing two Zero Trust Applications, then the **Active Sessions** widget shows three active sessions, one **Agent Session** and two **App Sessions**.

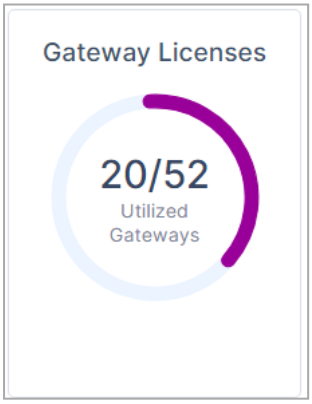
To view the detailed information, click **Expand**. The system redirects to the *"Active Sessions" on page 892* page.

Member Licenses



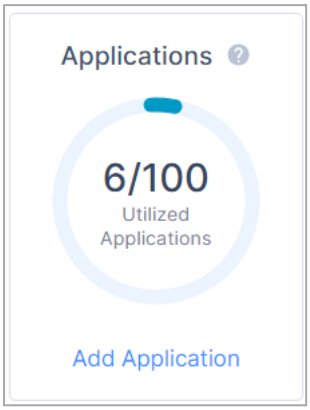
The **Member Licenses** widget shows the number of member licenses utilized out of the purchased licenses.

Gateway Licenses



The **Gateway Licenses** widget shows the number of gateway licenses utilized out of the purchased licenses.

Applications



The **Applications** widget shows the number of applications accessed out of the applications created by you.

To add an application, click **Add Application**. For more information, see *"Applications" on page 741*.

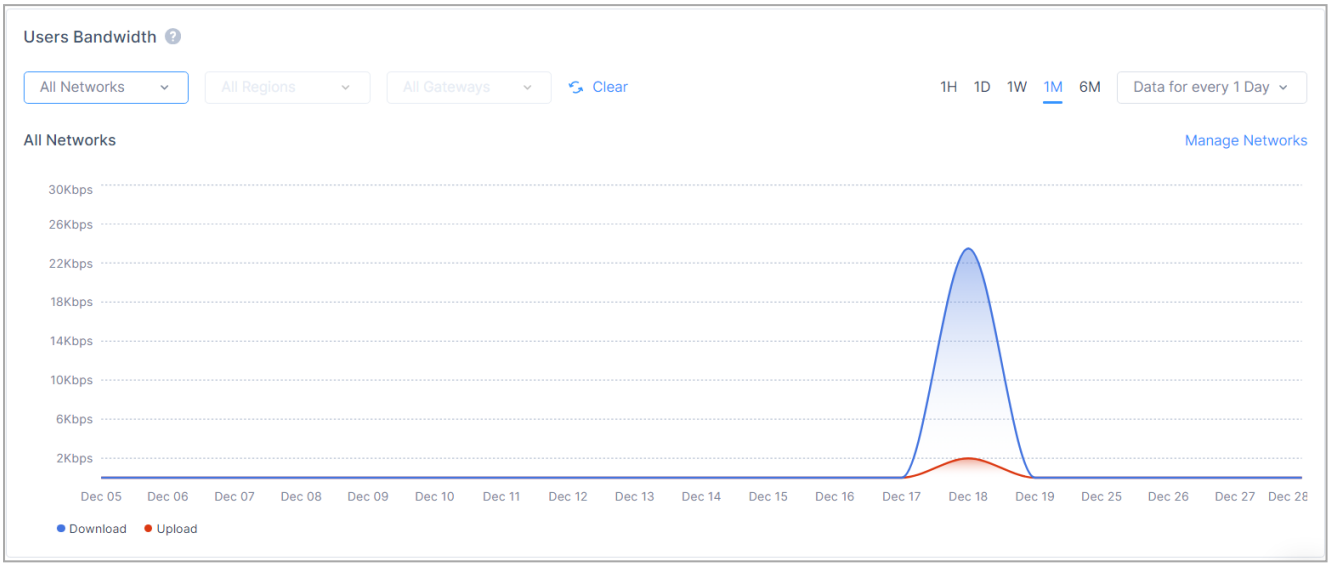
Active Agent Users

The **Active Agent Users** widget shows the live and historical data of members connected to a network through the Check Point SASE Agent.

You can filter the data by **Network**, **Region**, **Gateway**, time frame and scale.

For a network and region, you can compare the data for up to three gateways.

Users Bandwidth

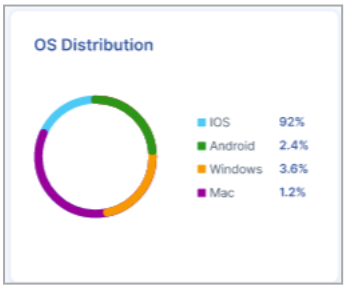


The **Users Bandwidth** widget shows the live and historical bandwidth used (upload and download) by members connected to the Check Point SASE Agent.

You can filter the data by **Network**, **Region**, **Gateway**, time frame and scale.

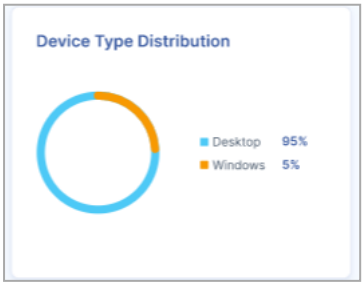
For a network and region, you can compare the data for up to three gateways.

OS Distribution



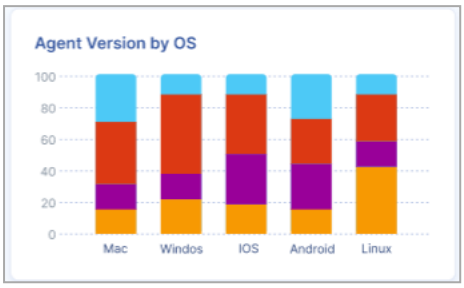
The **OS Distribution** widget shows the distribution of devices by operating systems.

Device Type Distribution



The **Device Type** widget shows the distribution of devices by type.

Agent Version by OS



The **Agent Version by OS** widget shows the distribution of Check Point SASE Agent across different operating systems.

Team

The **Team** page allows you to manage:

- *"Members" on page 70*
- *"Groups" on page 89*
- *"User Configuration Profiles" on page 92*

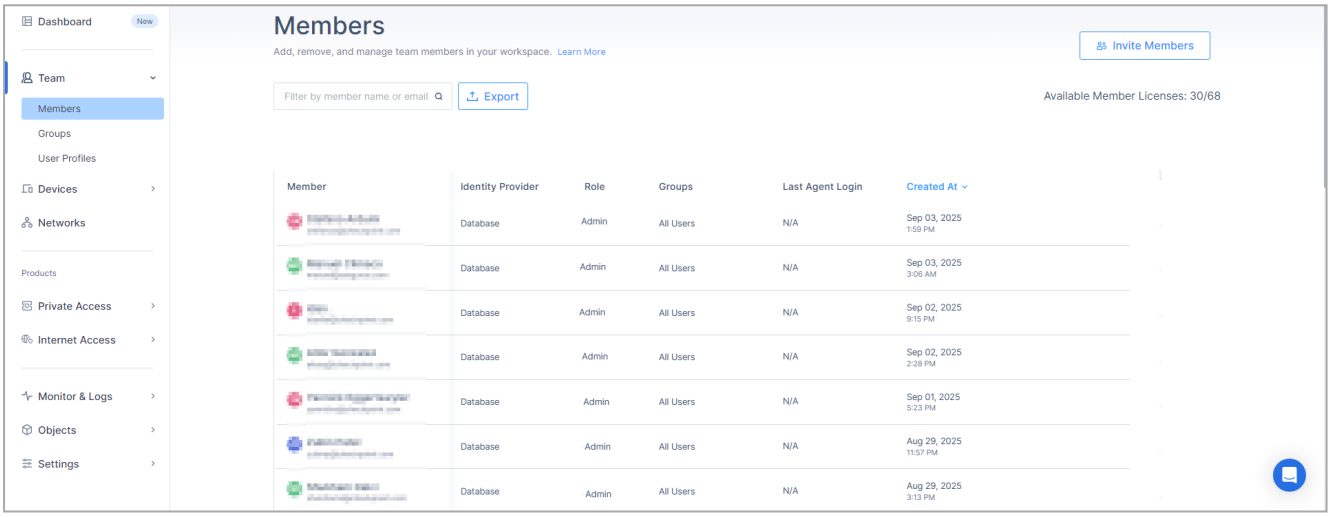
Members

Members are either administrators that manage the SASE Administrator Portal or end-users that you want to provide safe private and internet access.

The **Members** page allows you to:

- Invite members
- Manage members

To view the **Members** page, access **Check Point SASE** Administrator Portal and click **Team** > **Members**.

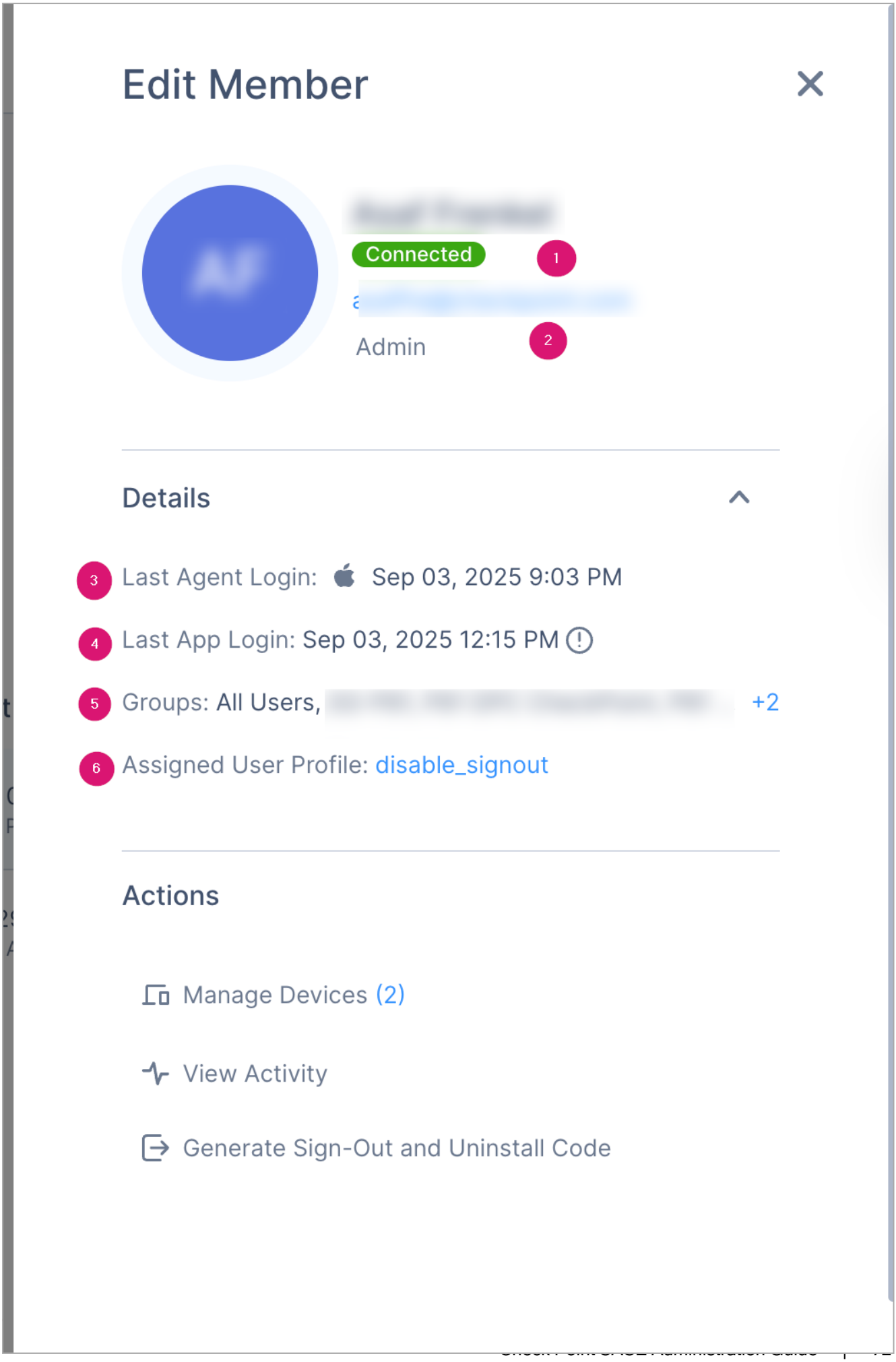


Column	Description
Member	Full name and email address of the member.
Identity Provider	Configured Identity Providers (IdP) for the member. **Database** means that the member is invited from the SASE Administrator Portal. See *"Invite Members" on page 74*.

Column	Description
Role	Role of the member: ■ **User** – End user with access to assigned applications and secure private and Internet access. ■ **Admin** – Full privileges and permissions across system settings, users, networks, and configurations. ■ **Manager** – Manage networks, applications, members, groups, and monitor activity. ■ **User Manager** – Manage members, on-boarding, device settings, and user configurations. ■ **Network Manager** – Manage networks, gateways, tunnels, routes, and network related configurations. ■ **Security Manager** – Manage Internet Access, DLP policies, security events, and security objects. ■ **Billing** – Manage billing information, invoices, licenses, and payment methods. **Note** - Admin and Billing roles and permissions are only for Perimeter 81 customers. For permissions associated with each role, see *"Member Roles and Permissions" on page 75*.
Groups	Group(s) to which the member is assigned.
Last Agent Login	Date and time of the last connected session.
Created At	Date and time when the member was created.

To view more details about the member, click the member row.

The **Edit Member** window appears


Edit Member
Connected
1
Admin
2
Details
3 Last Agent Login: Sep 03, 2025 9:03 PM
4 Last App Login: Sep 03, 2025 12:15 PM
5 Groups: All Users, +2
6 Assigned User Profile: disable_signout
Actions
Manage Devices (2)
View Activity
Generate Sign-Out and Uninstall Code

Legends	Description
1	Indication if the user is currently connected through the agent or application: ■ Connected ■ Offline
2	Role of the member.
3	Date and time of the last Agent login.
4	Date and time of the last application login, and the name of the application when you hover over .
5	Group(s) to which the member is assigned.
6	User configuration profile assigned to a user based on their group membership and the priority among configuration profiles.

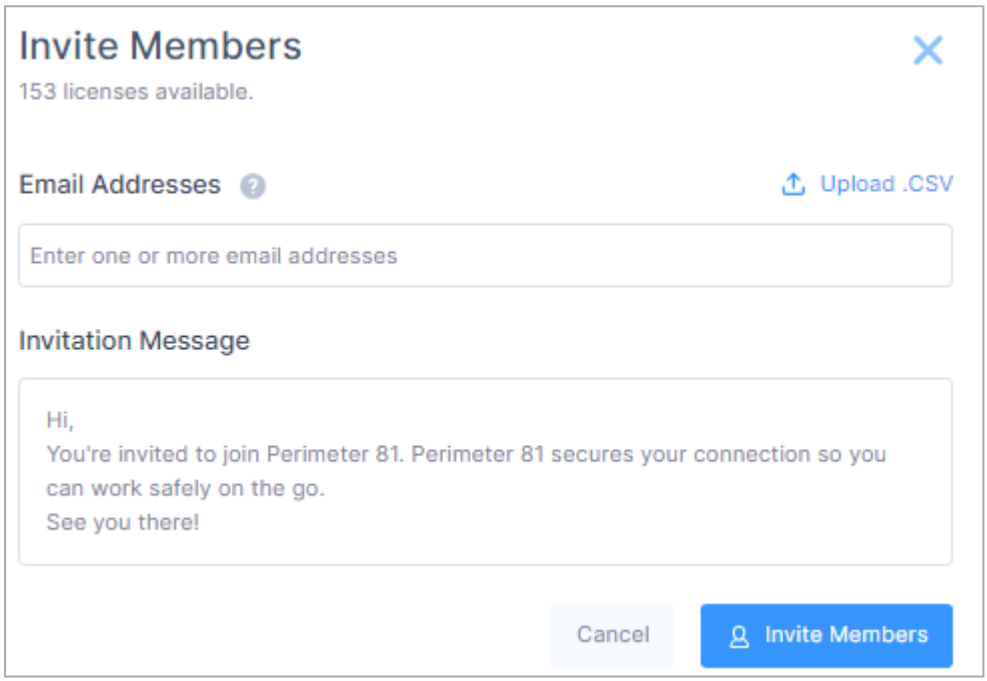
Invite Members

You can invite members either manually or using an Identity Provider (IdP).

Inviting Members Manually

1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Click **Invite Members**.

   The **Invite Members** window appears.



3. In the **Email Addresses** field, specify the email address of the member.
   - To invite multiple members, enter the email addresses separated by a comma or space.
   - If you have a CSV file with a list of email addresses (maximum 100), click **Upload.CSV** and upload the file.
4. (Optional) In the **Invitation Message** field, edit the email message.
5. Click **Invite Members**.

   The system sends an email to members with a link to accept the invite and download the Check Point SASE Agent. The invitation is valid for 30 days. If the invitation expires, you must resend the invitation. For more information, see *"Managing Members" on page 79*.

Inviting Members Using an Identity Provider

See *"Identity Providers" on page 950*.

Member Roles and Permissions

The predefined roles streamline administrative tasks by assigning specific permissions and restrictions to team members, ensuring operational efficiency and enhanced security.

Note - To change member role, see *"Managing Members" on page 79*.

Roles

- **User**
- **Admin**
- **Manager**
- **User Manager**
- **Network Manager**
- **Security Manager**
- **Billing**

Note - Admin and Billing roles and permissions are only for Perimeter 81 customers.

User

The User role allows access only to assigned applications and end-user features.

Permissions

Use the System: Access all features necessary for personal use of the platform.

Restrictions

- Cannot manage or configure other users, networks, or system settings.
- No visibility or access to other administrative areas within the system.
- No access to Billing settings or activity logs.
- Cannot modify Admin or Billing roles.

Admin

The Admin role allows full access to configure system settings, manage users, and assign roles across the platform.

Permissions

- **User Management**: Full control over user roles and permissions.
- **Network Management**: Full access to network configurations, including creation and modification of networks.
- **Billing Management**: Access to billing information and subscription details.
- **System Configuration**: Modify system settings and integrations.
- **Activity Logs**: View all system activity logs.

Manager

The Manager role allows managing network, member, and application configurations, with restricted access to billing and administrative functions.

Permissions

- **User Management** - Can manage user roles but cannot modify Admin or Billing roles.
- **Network Management** - Full access to manage network configurations.
- **System Configuration** - Modify application settings and user groupings.
- **Activity Logs** - View network and user activity logs.

Restrictions

- No access to Billing settings.
- Cannot assign or modify Admin roles.
- Limited access to administrative settings beyond network and member management.

User Manager

The User Manager role allows administrators to focus on managing members and device-related settings. This role is ideal for team members responsible for onboarding, monitoring, and managing user and device configurations.

Permissions

- **Access to Members and Devices interfaces**: Full visibility and control over user and device-related settings.
- **User Management**:

    - Invite and delete users.
    - Assign roles to users (except Admin and Billing roles).
- **Device Management**:
    - Configure device posture settings.
    - Manage user configuration profiles.
- **Activity Logs**: View logs related to Member Activity.

Restrictions

- No visibility or access to other administrative areas within the system.
- Cannot modify roles for Admin or Billing.
- Limited access strictly to member and device management.

Network Manager

The Network Manager role grants team members the ability to manage network configurations, including creating, updating, and deleting networks. This role is ideal for team members responsible for maintaining network infrastructure.

Permissions

- **Network Management**:
    - Access to all network management tools.
    - Create, modify, and delete networks, gateways, tunnels, and routes.
- **Activity Logs**: View logs associated with network activity.

Restrictions

- No access to other system management areas.
- Limited visibility especially to the network related configurations.

Security Manager

The Security Manager role allows monitoring and managing security-related configurations and events across the platform, without access to user, network, or billing administration.

Permissions

- **Internet Access**: Manage all Internet access settings.
- **Data Loss Prevention**: Configure and monitor DLP policies.

- **Security Events**: View and investigate security events.
- **Objects: Objects**: Manage security objects such as Addresses and Custom URLs.

Restrictions

- No access to User or Member management.
- No access to Network configuration.
- No access to system-wide administrative settings.

Billing

The Billing role allows to access financial and license related operations within the system.

Permissions

- **License Management**: Allocate, revoke, and monitor licenses.
- **Billing Settings**: Manage subscriptions, invoices, and payment methods.

Restrictions

- No access to user management, network configuration, activity logs, or system settings.
- No role assignment capabilities beyond license and billing scope.

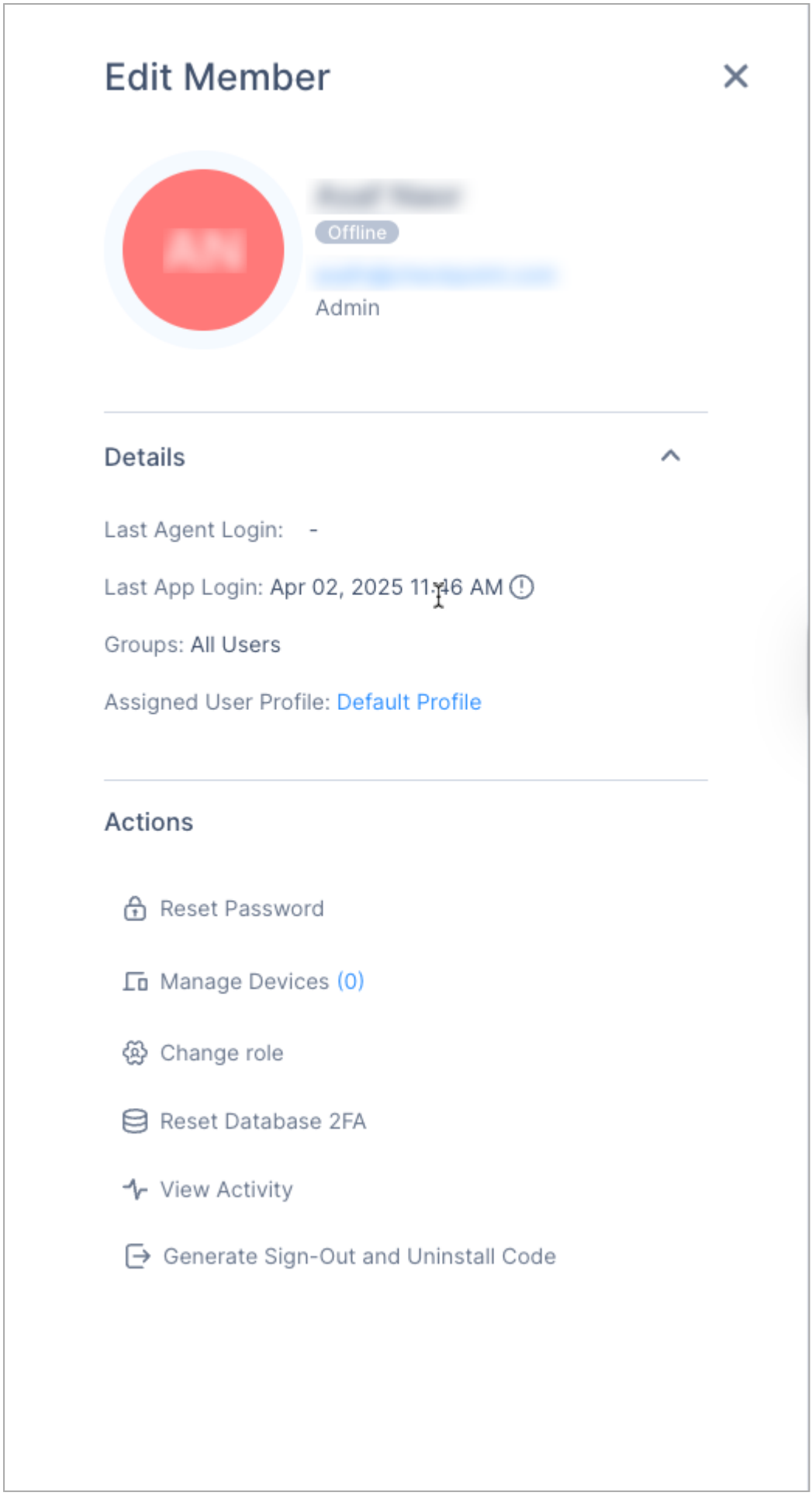
Managing Members

1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Click the member row.
3. To resend the invitation to members that did not accept the invitation within the validity period, click **Resend Invite**.
4. To reset the password, click **Reset Password** and in the confirmation pop-up that appears, click **Reset Password**.
5. To manage the devices of the user, click **Manage Devices**. The system redirects to the **Device Inventory** page. For more information, see *"Device Inventory" on page 106*.
6. To change member role, click **Change role**. For more information, see *"Changing Member Role" on the next page*.
7. To view the activity of a member, click **View Activity**. The system redirects to the **Member Activity** page. See *"Member Activity" on page 895*.
8. To delete a member, click **Delete Member** and in the confirmation pop-up that appears, click **Delete Member**.

Changing Member Role

1. Access the SASE Administrator Portal and click **Team** > **Members**.

2. Click the member row for which you want to change the role.


Edit Member
Offline
Admin
Details
Last Agent Login: -
Last App Login: Apr 02, 2025 11:46 AM
Groups: All Users
Assigned User Profile: Default Profile
Actions
Reset Password
Manage Devices (0)
Change role
Reset Database 2FA
View Activity
Generate Sign-Out and Uninstall Code

The **Edit Member** window appears.

3. Select the role:
   - User
   - Admin
   - Manager
   - User Manager
   - Network Manager
   - Security Manager
   - Billing
4. Click **Save**.

Unblocking Members

SASE blocks members if there are multiple failed login attempts into the SASE Agent. Blocked members are greyed-out with a lock icon.

To unblock a members:

1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Search and select the member row whose account is blocked.

   The **Edit Member** window appears.
3. Click **Unblock User**.

Generating Sign-Out and Uninstall Code

You can prevent members from unauthorized sign-out of the SASE Agent. The sign-out is authorized only after the member enters a sign-out code generated by you.

To generate the sign-out and uninstall code:

1. Access the SASE Administrator Portal.
2. Ensure that *"Disable Sign-Out" on page 93* is enabled for the member or group.
3. Go to **Team** > **Members**.
4. Search and select the member row for which you want to Generate Sign-Out and Uninstall Code.
5. Click **Generate Sign-Out and Uninstall Code**.

A pop-up appears with the sign-out code.

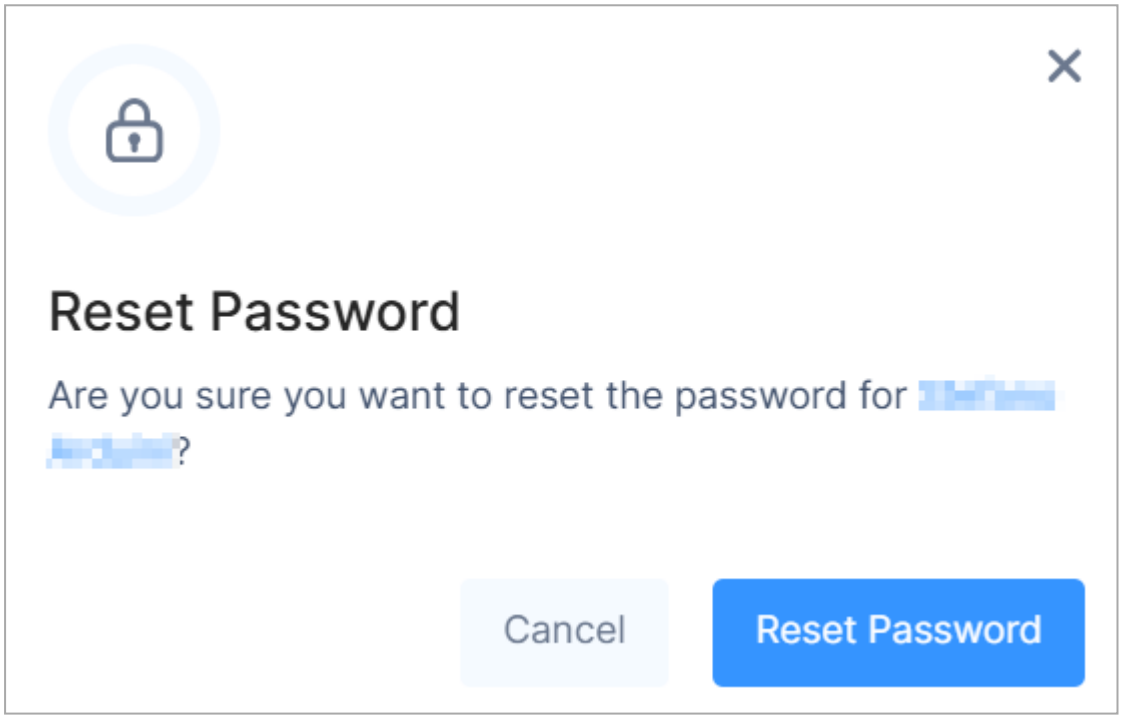
6. Copy the code and share it with the member.

Resetting a Member Password

1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Click the member row for which you want to reset password.

   The **Edit Member** window appears.
3. Click **Reset Password**.

   The **Reset Password** window appears.



4. Click **Reset Password**.

Resetting Google Authenticator Two-Factor Authentication for a Member

When a member changes the device that has Google Authenticator used for Two-Factor Authentication, they must reconfigure it on the new device. To do that, the administrator must reset their Two-Factor Authentication.

To reset Two-Factor Authentication for a member:

1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Click the member row for which you want to reset Two-Factor Authentication (2FA).

The **Edit Member** window appears.

3. Click **Reset Database 2FA**.
4. Click **Reset** in the confirmation pop-up that appears.

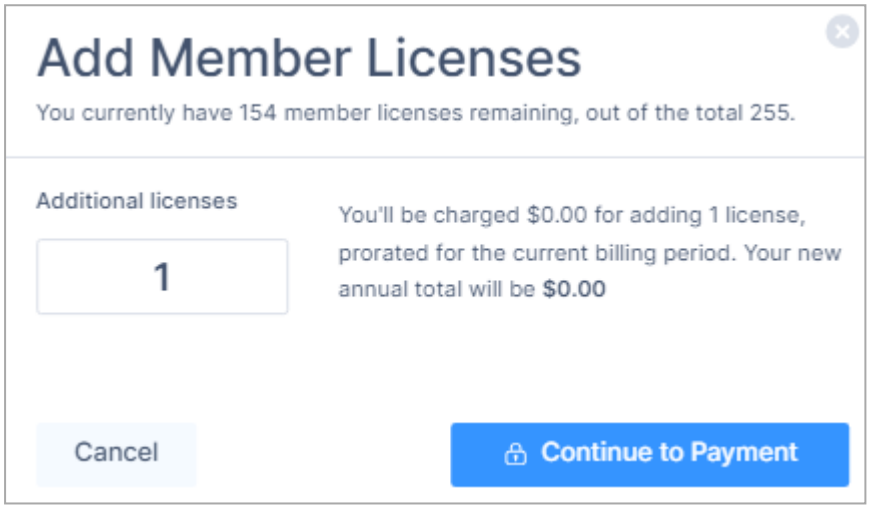
   The member receives a confirmation email for the Two-Factor Authentication reset and a link to re-activate it.

Adding Licenses

Note - This option is available only for the Legacy Perimeter 81 workspace accounts.

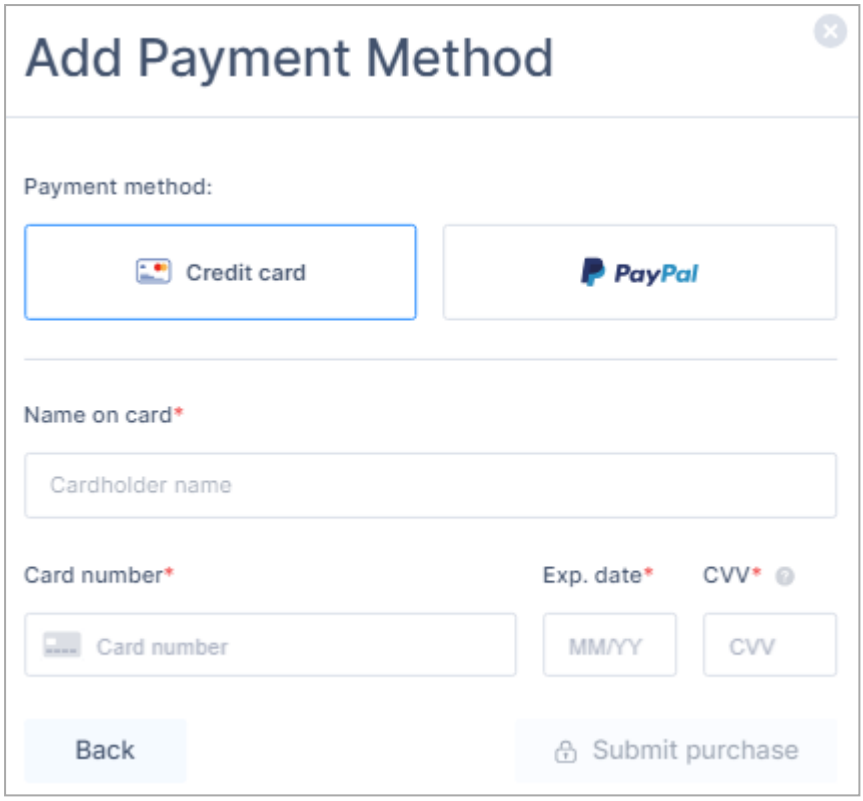
1. Access the SASE Administrator Portal and click **Team** > **Members**.
2. Click **Add Licenses**.

   The **Add Member Licenses** window appears.
3. In the **Additional licenses** field, enter the number of licenses you want to add.



4. Click **Continue to Payment**.

   The **Add Payment Method** window appears.



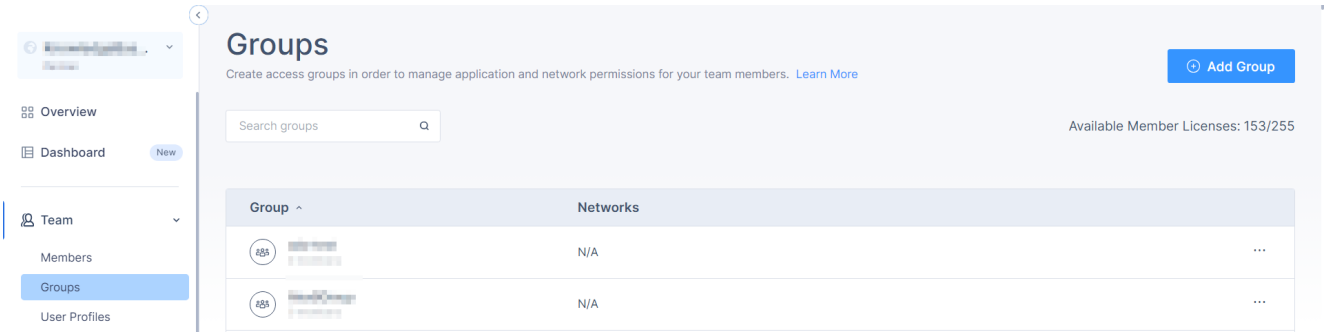
5. Enter the payment details and click **Submit purchase**.

Groups

The **Groups** page allows you to create groups of members, based on roles and locations. For example, it allows you to apply a Policy to multiple members or restrict access only to a segment of the network.

Note - Segmenting networks uses the Software Defined Perimeter (SDP) technology. This isolates sensitive data and reduces the attack surface, minimizing the impact during security breaches.

To view the **Groups** page, access the SASE Administrator Portal and click **Team** > **Groups**.



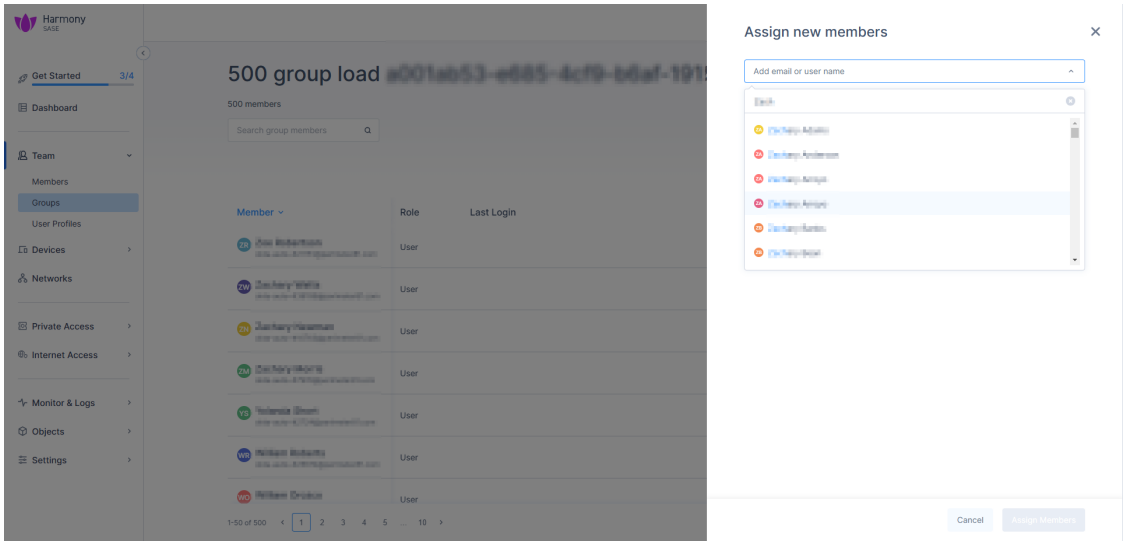
Column	Description
Group	Group name.
Networks	Name of the networks assigned to the group.

Creating a Group

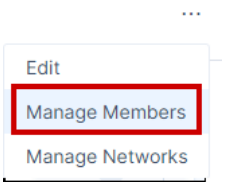
1. Access the SASE Administrator Portal and click **Team** > **Groups**.
2. Click **Add Group**.

   The **Create new group** window appears.

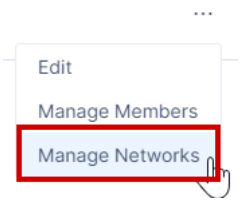
Note - You can search and select users in the **Assign new members** section in the right-pane.



3. Enter the group name and click **Create Group**.
4. To add members to the group:
   a. Click the ··· icon in the last column of the group and then select **Manage Members**.



   b. In the **Assign new members** section, click **+** and select the required members.
5. To add networks to a group or to grant access to a network segment:
   a. Click the ··· icon in the last column of the group and then select **Manage Networks**.



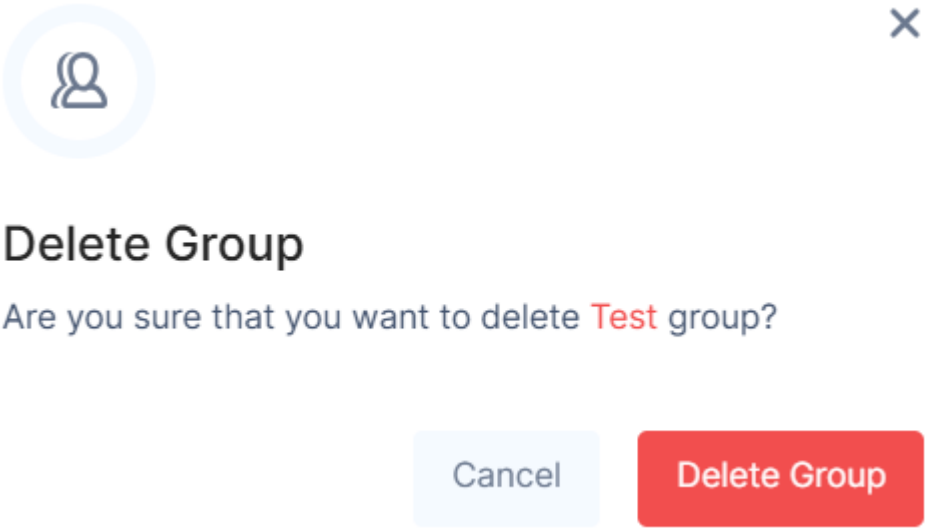
   The **Assign Network to Group** pop-up appears.

b. Select the network and click **Done**.

The members can access only the selected networks from the Check Point SASE Agent.

6. To delete a group, hover over the group that you want to delete and click .

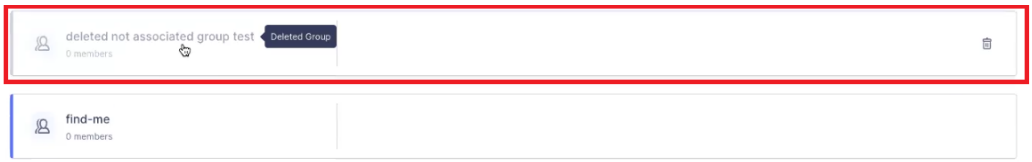
The **Delete Group** window appears.



7. Click **Delete Group**.

Notes:

- A group can also be automatically created as a result of an IDP sync over SCIM, and associate users with it.
- When a group is deleted in the Identity Provider (for example, Okta), it remains in any policies or configurations where it was previously used. It appears greyed out and when you hover over it, **Deleted Group** message is displayed.



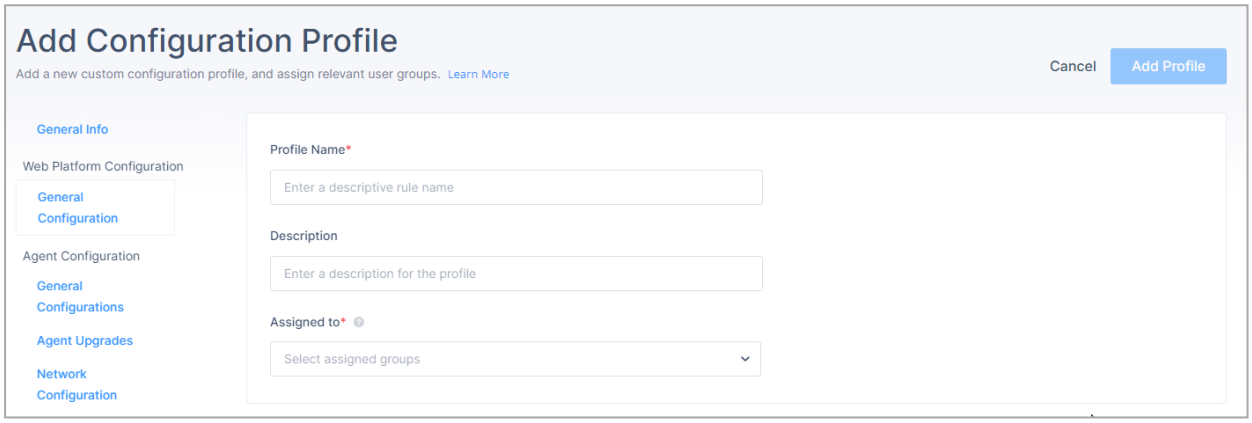
- You cannot add the deleted group in any policies, but it can be removed from the existing policies.
- When the deleted group is re-enabled, it is restored without any members. To add members again, you must manually assign them through the IdP.

User Configuration Profiles

User Configuration Profiles allows you to create profiles with custom settings and apply them to member groups and devices.

Adding a Configuration Profile

1. Access the SASE Administrator Portal and click **Team** > **User Profiles**.
2. Click **Add Configuration Profile**.
3. In the **Profile Name** field, enter a name for the profile.



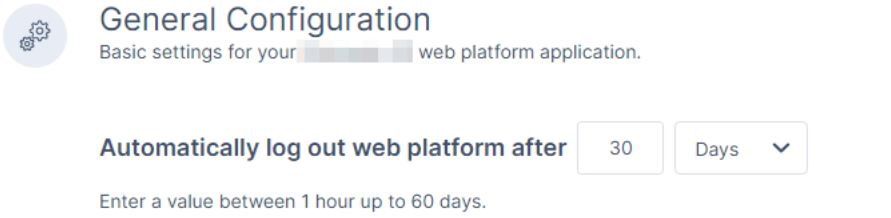
4. (Optional) In the **Description** field, enter a description for the profile.
5. In the **Assigned to** field, select the member groups.
6. Configure *"Web Platform Configuration" below* and *"Agent Configuration" on the next page*.
7. Click **Add Profile**.

The order of the profile indicates its priority. For example, Profile #1 has higher priority than Profile #2.

Web Platform Configuration

The **Web Platform Configuration** settings allows the administrators to configure settings for the Check Point SASE Administrator Portal.

General Configuration



In the **Automatically log out web platform after** field, enter the duration after which the system automatically logs out the member from the SASE Administrator Portal. The supported duration is one hour to 60 days.

Agent Configuration

The **Agent Configuration** settings allows the administrators to configure settings for the Check Point SASE Agent.

General Configuration

From the **General Configuration** section of the **Agent Configuration**, you can configure the basic settings for your Check Point SASE Agent.

Setting	Description
Disable Sign-Out	Prevents members from signing out of the SASE Agent without the sign-out code. The administrator must generate the sign-out code and share it with the member to successfully sign-out from the SASE Agent. See *"Generating Sign-Out and Uninstall Code" on page 84*.
Automatically Log Out Agent After	Logs out the member from the SASE Agent automatically after the specified duration. The supported duration is one hour to 180 days.

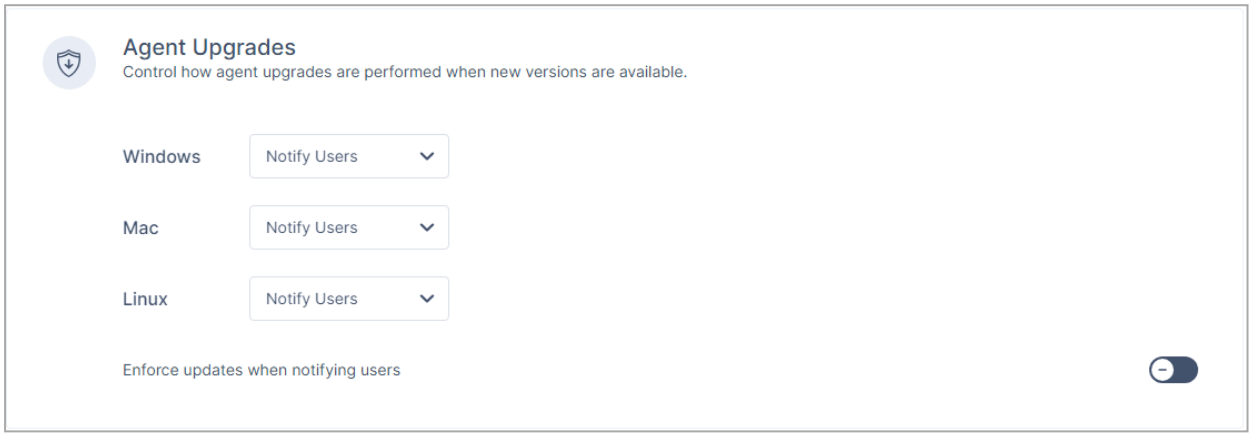
Setting	Description
Automatically sign out non-active user after	Automatically signs out a member from the Check Point SASE Agent if their device remains unattended for the specified duration. The supported duration is 20 min to 60 min. When the **Automatically sign out non-active user after** toggle is enabled, the **Always-On VPN** is bypassed by default. **Note** - The system monitors user activity, such as keyboard and mouse inputs, to determine whether the device is active. If no activity is detected for a prolonged period, the system may automatically sign you out.
[DEPRECATED] Shared Network	Allows members to connect to shared Check Point SASE gateways. This enhances speed and performance if the member's physical location is far from your private gateway location. For more information about shared networks, see *" [DEPRECATED] Shared Gateways " on page 160*.
Connect on Launch	Automatically starts the Check Point SASE Agent when the device starts and connects to the most recent network location. **Notes**: ▪ This setting applies only to Windows and macOS devices. ▪ The member can modify this setting from their device.
Connect / Disconnect Notification	Shows a pop-up notification on the device when the SASE Agent connection status changes. **Notes**: ▪ This setting applies only to Windows and macOS devices. ▪ The member can modify this setting from their device.
Snowplow Report	Allows you to send the Snowplow (user tracking) data to SASE.

Agent Upgrades

Agent Upgrades allows you to control how to perform Check Point SASE Agent upgrades when new versions are released.

To control how to perform Check Point SASE Agent upgrade:

1. Go to **Team** > **User Profiles**.
2. Open a user profile with the required group of members or create a new user profile. See *"Adding a Configuration Profile" on page 92*.
3. Scroll-down to the **Agent Upgrades** section.



4. Select the option required for **Windows**, **Mac**, and **Linux**.
   - **Automatic Silent**: Automatically upgrades the Check Point SASE Agent when new version is available.
   - **Notify Users**: Notifies the user about the new version.
   - **Disabled**: Does not upgrade the Check Point SASE Agent.
5. To automatically upgrade the SASE Agent while notifying the member, turn on the **Enforce updates when notifying users** toggle button.
6. Click **Apply**.

Network Configuration

Network Configuration allows you to configure the network settings for your Check Point SASE Agent.

Feature	Description
Block LAN traffic while connected to a Private network [2]	Prevents a device from accessing or being accessed by other devices on the local network while connected to the VPN, enhancing security against lateral threats. See *"Device Isolation" on page 102*.
Automatic VPN Connection [1]	Automatically connects to the VPN when an internet connection is available.
Always-On VPN	Automatically connects to the VPN when an internet connection is available.
Kill Switch [1]	Automatically disconnects internet connection when the VPN disconnects.
Trusted Environments (Always-On Exceptions) [1]	Bypasses SASE VPN if you have a trusted router and connects directly to your network. To configure a Trusted Environment, use the router's LAN MAC address. You can use the scripts available under Add Trusted Router to assist with setup. You can also run the command `ARP -a` on Windows or `ip neigh show` on macOS and Linux to get the correct LAN MAC address.

Feature	Description
Agent Security in Trusted Network [1]	System administrators can enable or disable security engines in trusted environments. This feature is designed for scenarios where network inspection is already implemented, minimizing redundancy while ensuring control over security posture. Requires Agent version 11.6 or higher.

Feature	Description
Trusted Web Server [1]	Specify a list of one or more HTTPS web servers that are available only in your internal trusted network. A trusted web server can be defined by FQDN or IP Address. Requires Agents of version 11.1 or higher. **To add trusted web server:** 1. Click **Add Trusted Environment**. 2. Select **Trusted Web Server**. 3. In the **Name** field, enter a name. 4. In the **HTTPS Server** field, enter the HTTPS server domain or IP address. 5. In the **TLS Certificate** field, upload the public TLS certificate of the web server, to allow secure validation of the web server. 6. Click **Add**. 7. To add multiple web servers, repeat steps 1 to 5. 8. Click **Apply**.

Feature	Description
Trusted Routers	Specify a list of one or more MAC addresses of a router you own or trust. Connecting to the internet through these routers do not trigger the **Always on VPN** feature, and manually connects and disconnects from the network. **To add trusted routers:** 1. Click **Add Trusted Environment**. 2. Select **Trusted Router**. 3. In the **Name** field, enter the router name. 4. In the **Router MAC Address** field, enter the router MAC address. 5. Click **Add**. 6. To add multiple routers, repeat steps 1 to 4. 7. Click **Apply**.
Automatic Wi-Fi Security [1]	The SASE Agent automatically connects to SASE VPN if the device connects to an unsecured Wi-Fi.

Feature	Description
Trusted Wireless Networks (Automatic Wi-Fi Security Exceptions) [2]	SASE Agent does not enable **Automatic Wi-Fi Security** if the device connects to a trusted Wi-Fi network. **To add trusted Wi-Fi network:** 1. Click **Add Wi-Fi Network**. 2. In the **Name** field, enter the SSID of the network. 3. Click **Add**. 4. To add multiple trusted Wi-Fi networks, repeat steps 1 to 3. 5. Click **Apply**.

[1] The member can modify this setting on their device.

[2] This setting applies only to Windows and macOS devices.

Windows

Allows you to define the settings for Windows devices running the SASE Agent.

To configure the default protocol:

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

Use VPN Interface DNS

Sets the device DNS server as the SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface.

If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers.

Note - The member can modify this setting on their device.

Notify Reconnect

The SASE Agent automatically notifies upon reconnecting with the network.

Note - The member can modify this setting on their device.

Android / Chromebook

From the **Android / Chromebook** settings, the administrators can control the settings for the Check Point SASE Agent running on Android or Chromebook devices.

Default Protocol

To configure the default protocol:

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

Mac

From the **Mac** settings, the administrators can control the settings for the Check Point SASE Agent running on macOS.

To configure the default protocol:

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

Use VPN Interface DNS

Sets the device DNS server as the SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface.

If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers.

Note - The member can modify this setting on their device.

iOS

From the **iOS** settings, the administrators can control the settings for the Check Point SASE Agent running on iOS devices.

Auto Reconnect

Automatically reconnects all the iOS agents to the VPN if the session disconnects or the device connects to Wi-Fi or 3G networks that do not require login credentials.

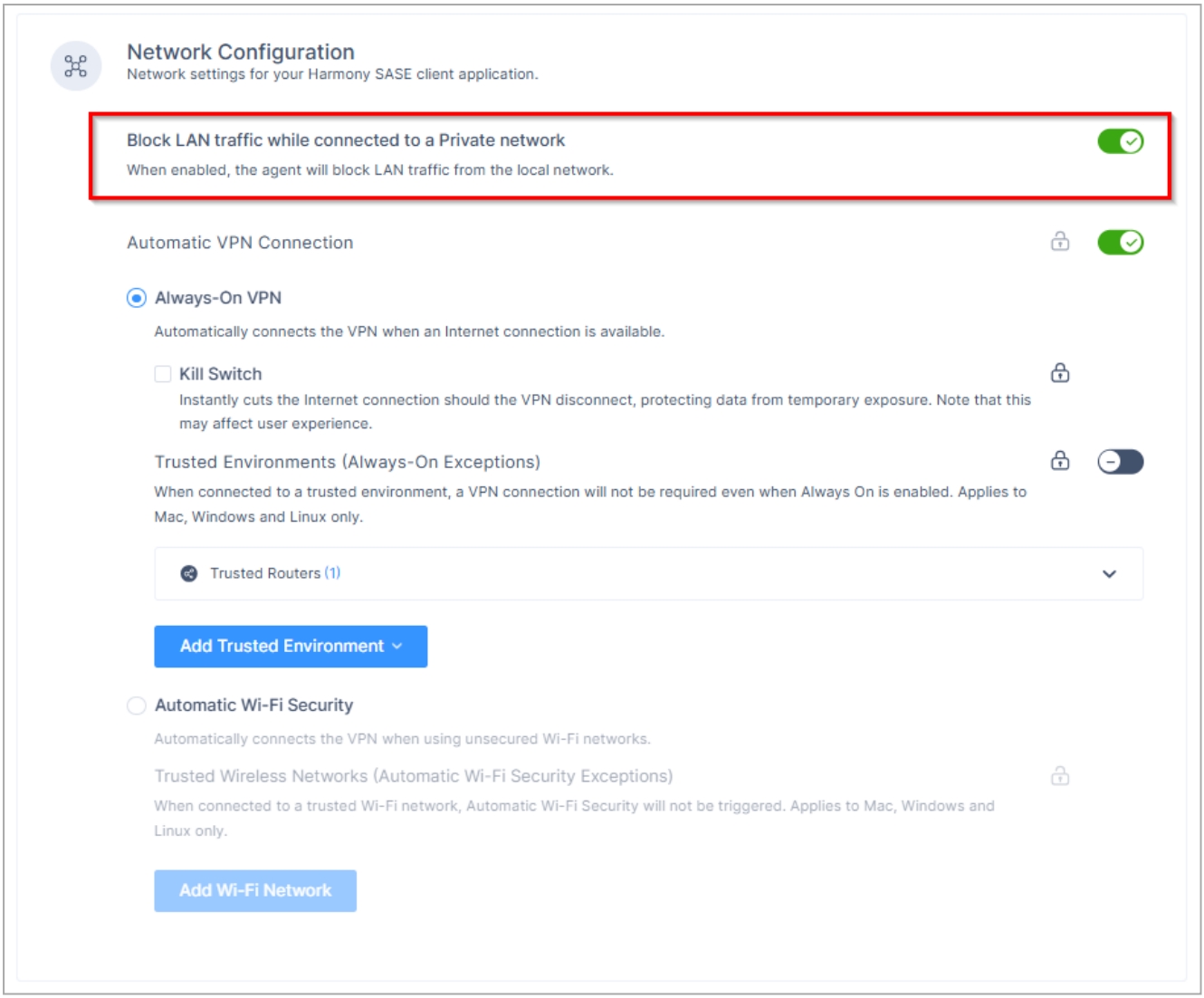
Note - The member can modify this setting on their device.

Device Isolation

The Device Isolation feature provides a preventive layer of protection by restricting a device from communicating with other devices on the local network (LAN) while connected to the VPN (organizational private resources).

To do that:

1. Access the Check Point SASE Administrator Portal and click **Team** > **User Profiles**.
2. Click **Add Configuration Profile**.
3. Go to the **Network Configuration** section.
4. Turn on the **Block LAN traffic while connected to a Private network** toggle button.



By enabling this feature, the device is protected from potentially unsafe or untrusted local traffic, reducing exposure to risks while still allowing secure communication with external resources and the public internet.

Notes:

- This setting applies only to Windows and macOS devices.
- Supported Agent Version - 11.6 and higher.

When Device Isolation is turned on:

- **All local network traffic is blocked** - The device cannot send or receive traffic from any local network traffic (only while connected to the VPN), for example, printers, shared folders, or local servers.
- **Internet and external VPN traffic remains unaffected** - Outbound traffic is still routed through the VPN to external destinations, allowing continued access to organizational and public internet resources.

Use Case

Enable Device Isolation in high-security environments or scenarios where:

- Devices are operating in potentially untrusted networks, for example, public Wi-Fi.
- You want to enforce stricter lateral movement prevention.
- Reducing the attack surface within the internal network is a priority.

Devices

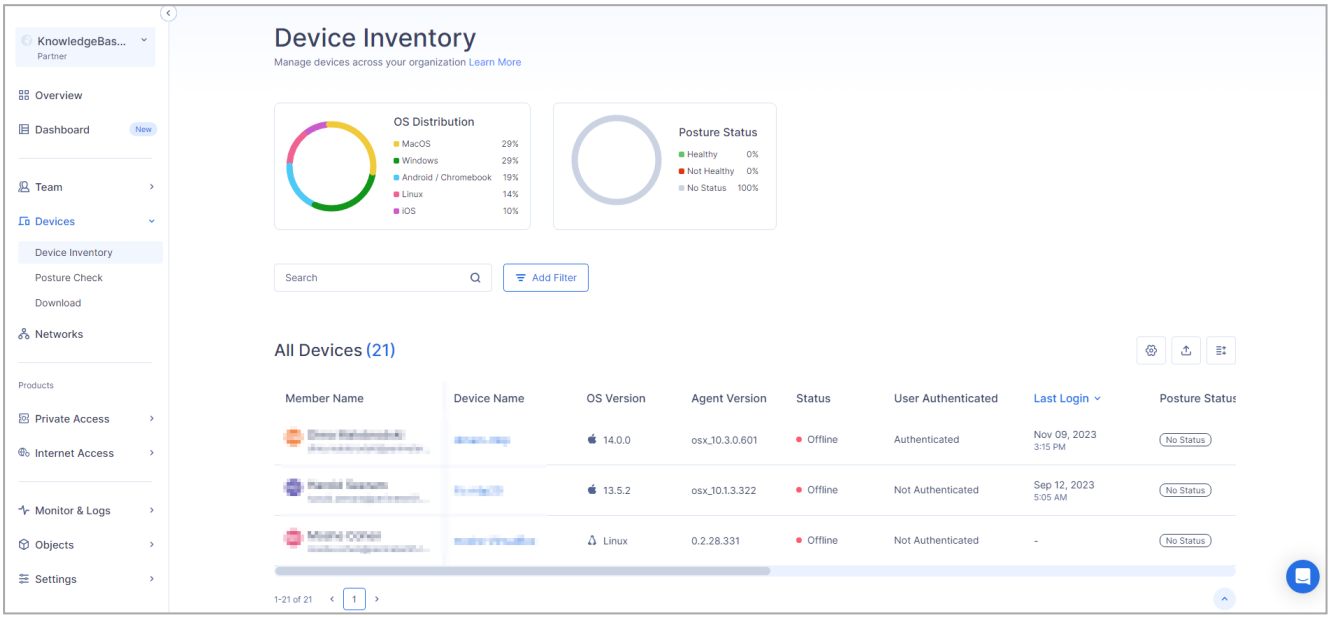
In the **Devices** page, you can:

- View inventory details about your devices
- Configure device posture check profiles
- Download the Check Point SASE Agent

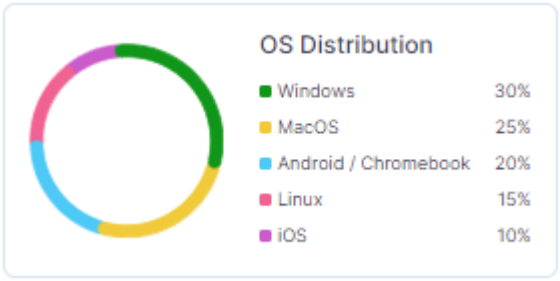
Device Inventory

The **Device Inventory** page provides inventory details about your devices.

To view the **Devices** page, access **Check Point SASE** and click **Devices** > **Device Inventory**.

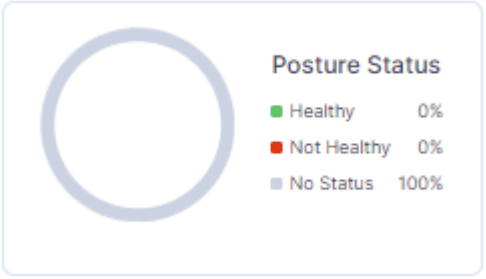


OS Distribution



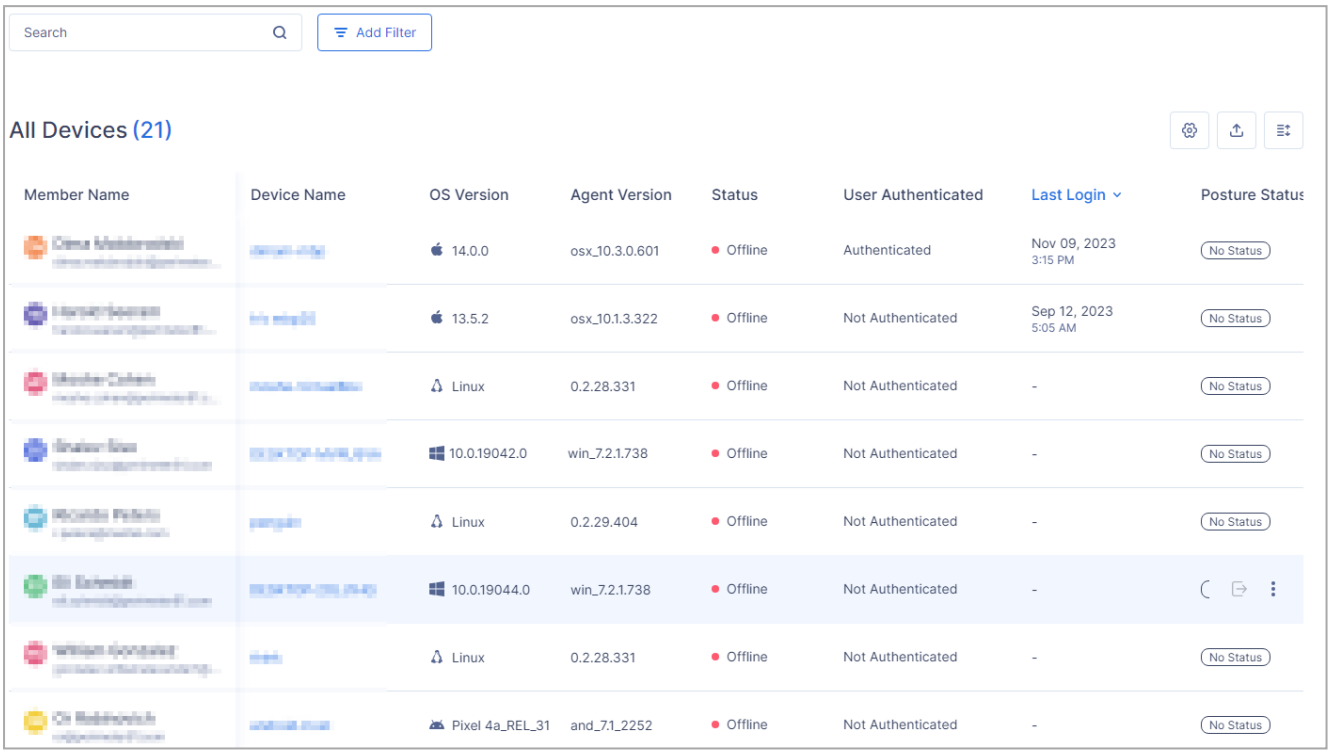
The **OS Distribution** widget shows the distribution of operating systems across devices by percentage.

Posture Status



The **Posture Status** widget shows the posture status of your devices by percentage. For more information, see Manage DPC.

Device Inventory Details



Column	Description
Member Name	User of the device.
Device Name	Name of the device.
OS Version	Operating System and version of the device.
Agent Version	Agent version installed on the device.
Status	The last known device status. ■ **Online** - Agent is running and the user is signed in but not connected to the VPN. ■ **Offline** - Device is turned off or not connected to the internet. ■ **Connected** - Agent is connected to the VPN.
User Authenticated	User authentication status. ■ **Authenticated** - User has signed in to the agent with valid credentials. ■ **Not Authenticated** - User authentication has expired or invalid credentials entered.

Column	Description
Last Login	Date and time of the last login.
Posture Status	Device Posture Check (DPC) status. ■ **Healthy** - Device is compliant with the DPC policy. ■ **Not Healthy** - Device is not compliant with the DPC policy. ■ **No Status** - User has not signed in since the DPC policy assignment or no DPC policy assigned to the device.
Security Warning	Reason for the failed DPC. For example, Missing Anti-Virus software on the device.
Last Posture Check	Date and time when the posture check was last done.
Posture Policy	DPC policy applied to the device.
Device Serial / ID	Unique identifier of the device. For macOS, it is the serial number generated by macOS. For other operating systems, it is generated by Check Point SASE.
Device Type	Type of the device. ■ Desktop ■ Mobile

Logging Out the Device

1. For the device you want to log out, scroll to the end of the row and click ⋮.
2. Go to **Actions** and click **Logout Device**.

Removing Device

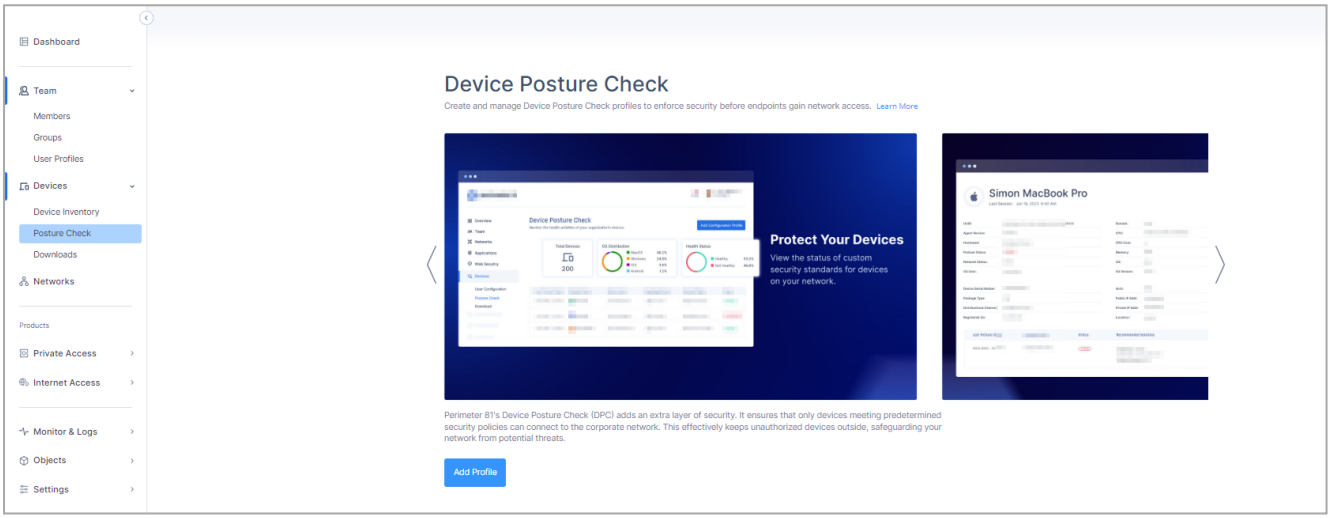
1. For the device you want to remove, scroll to the end of the row and click ⋮.
2. Go to **Actions** and click **Remove Device**.

Posture Check

The **Posture Check** page allows you to specify the posture requirements for the device. If the device does not meet the specified posture requirement, then the SASE Agent blocks private access.

The posture check is performed periodically while the device connected to a network or every time when the device connects to the network.

To view the **Posture Check** page, access the SASE Administrator Portal and click **Devices** > **Posture Check**.



Supported Posture Requirement Checks

Posture Requirement	Windows	macOS	Linux
Specific or any Endpoint Security software is active and up to date on the device.*	Yes	Yes	Yes
Specific or any firewall or Windows Security Center is active and up to date on the device.	Yes	No	No
The device has the specific OS installed and running on the device.	Yes	Yes	No
Check for required or banned specific files on the device.	Yes	Yes	Yes
Check for required or banned registry keys and values on the device.	Yes	No	No
Check for required or banned processes on the device.	Yes	Yes	Yes

Posture Requirement	Windows	macOS	Linux
Hard drive on the device is encrypted.	Yes	Yes	No
Valid device certificate is installed trusted by a CA.	Yes	Yes	No
The user has signed in to a specified AD domain.	Yes	Yes	No

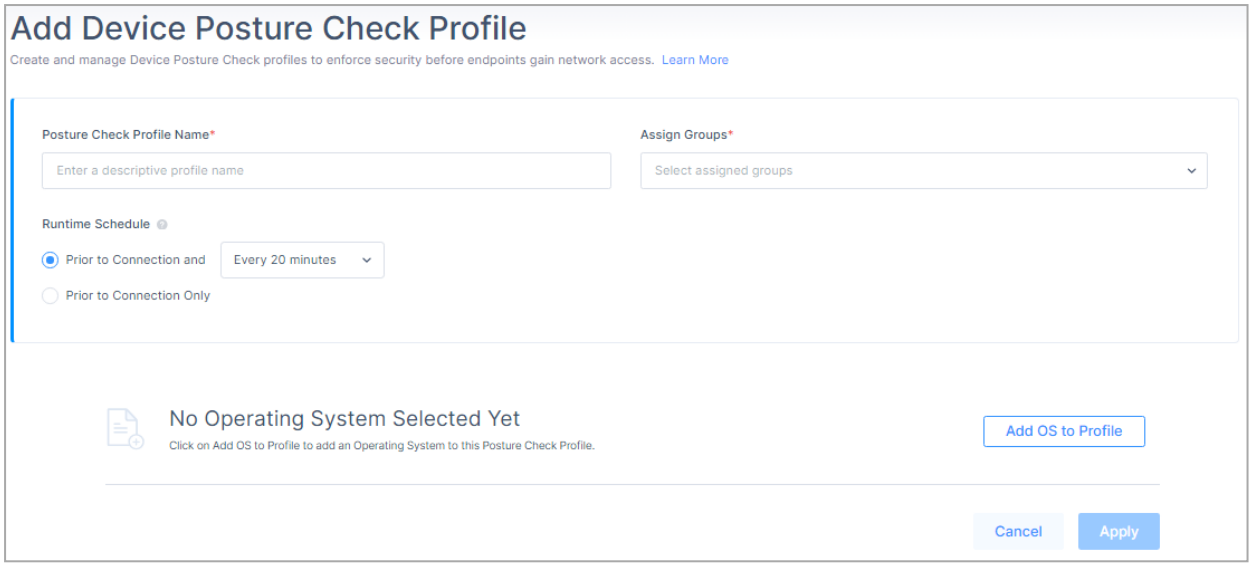
The supported Endpoint Security products include:

- Avast
- Bitdefender Total Security
- Check Point Endpoint Security
- ClamAV
- Crowdstrike Falcon
- ESET NOD32
- Kaspersky
- Malwarebytes
- McAfee
- SentinelOne
- Symantec Norton
- Webroot
- Windows Defender

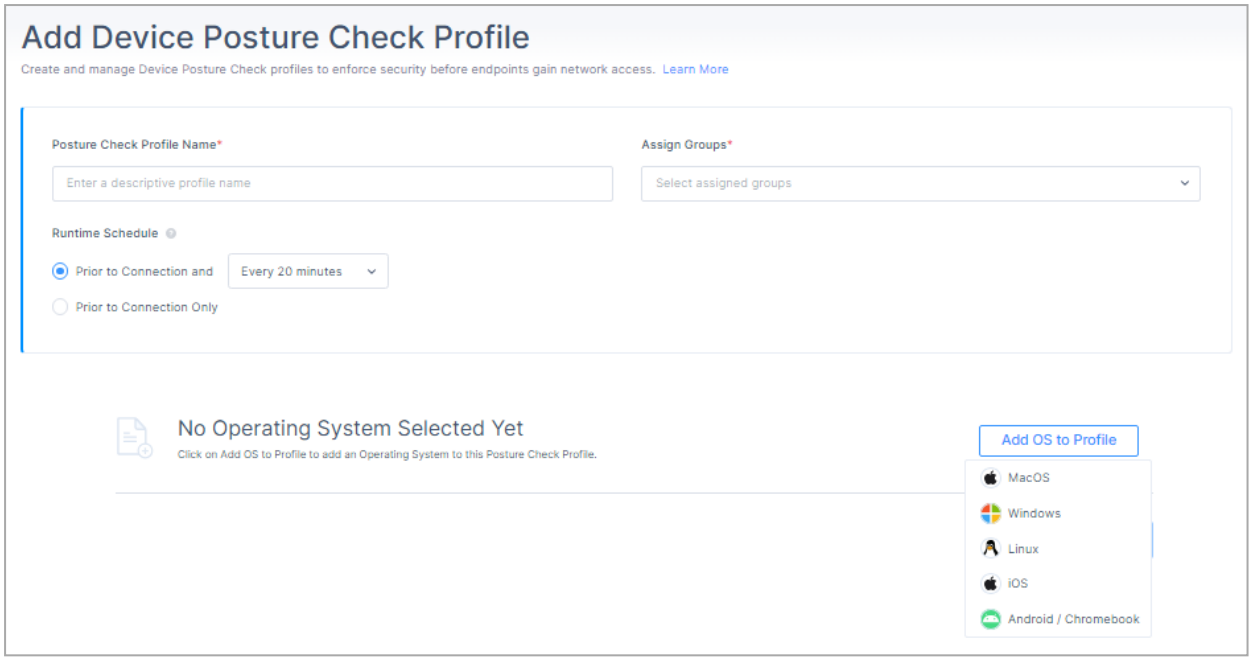
Specifying the Device Posture Check Requirements

1. Access the SASE Administrator Portal and click **Devices** > **Posture Check**.
2. Click **Add Profile**.

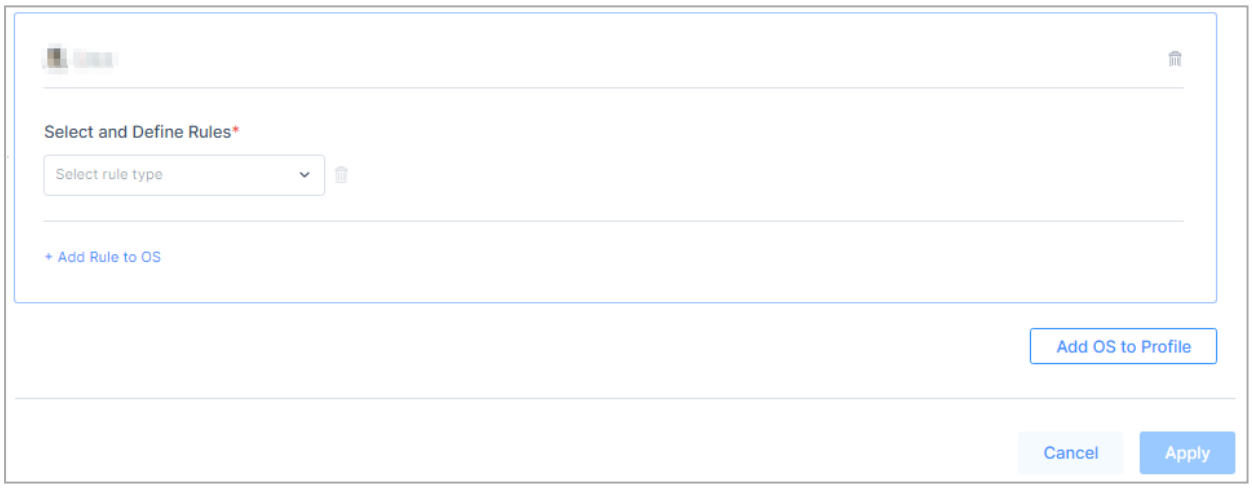
   The **Add Device Posture Check Profile** window appears.



3. In the **Posture Check Profile Name** field, enter a profile name.
4. From the **Assign Groups** list, select the member group(s) to which you want to apply the posture check.
5. In the **Runtime Schedule** section, select when to run the device posture check:
   - **Prior to Connection** and select the interval:
     - **Every 20 minutes**
     - **Every 40 minutes**
     - **Every 60 minutes**
   - **Prior to Connection Only**
6. To add operating system, click **Add OS to Profile**.
7. Select the Operating System from the list:
   a. **MacOS**
   b. **Windows**
   c. **Linux**
   d. **iOS**
   e. **Android / Chromebook**



8. From the **Select and Define Rules** list, select the rule type:



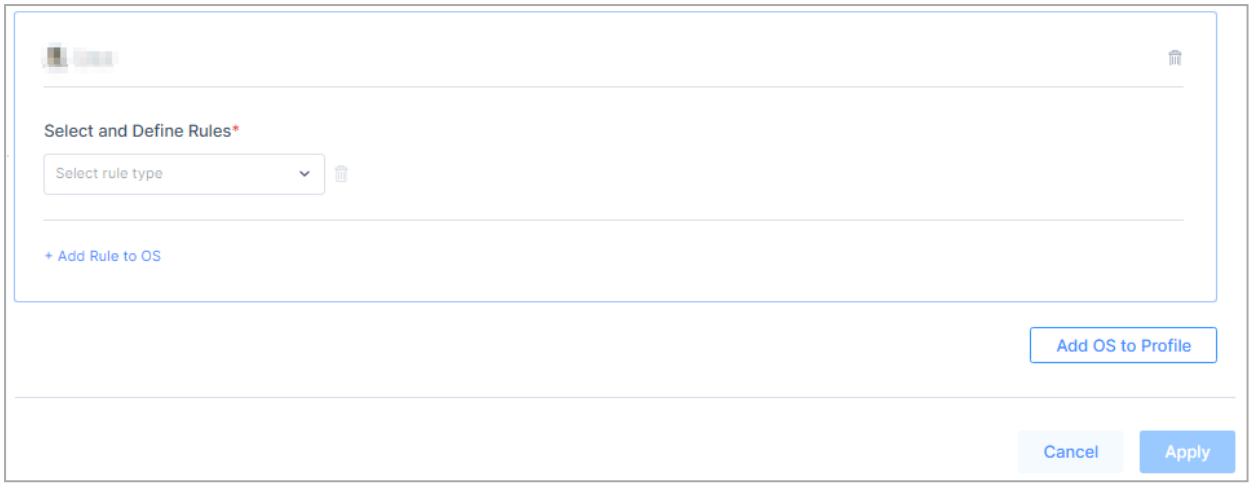
Posture Check Requirement	Description	Action
Endpoint Security	Verifies if the specified Endpoint Security Solution is installed, up-to-date and running.	Select the Endpoint Security software products from the list.
File Exists	Verifies if certain file exist or do not exist (banned) in the specified path.	Enter the path with forward slash. For example, `C:/user/testing`
Disk Encryption	Verifies that the OS hard drives are encrypted.	N/A

Posture Check Requirement	Description	Action
Certificate Issuer & CA	Verifies that the device holds the appropriate certificate.	a. Click **Upload Certificate (PEM)** to upload the certificate. The system validates the certificate. **Notes**: ■ Supports **PEM** certificates only. ■ The maximum file size allowed is 50KB. ■ Supported from Agent version 12.0. b. From the list, select the certificate issuer to validate. c. (Optional) Select the **Verify matching private key on device** checkbox to perform an additional check. This verifies that the certificate is valid, matches the expected issuer, and that the corresponding private key is present on the device. **Note** - The Agent automatically validates the certificate issuer's validity and check for the Root CA even without selecting this checkbox. The checkbox simply adds an extra layer of validation for the private key.
Certificate subject	Verifies that a specific certificate is installed on the device (Mac Keychain).	Enter the certificate name.

Posture Check Requirement	Description	Action
Process Running	Verifies that certain processes are running or not running (banned) on the device.	Enter the process name with the extension *.exe*. For example, `winload.exe`. To get the process name, see Certificate Pinning. This can also be used to check Anti-viruses which are not pre-defined under the Anti-virus category.
Operating System version	Verifies if the specified OS version or higher is running.	Select the operator and then enter the OS version number. For example, `10`, `10.0` or `10.0.19045`.
Registry	Verifies if the specific registry key exists or do not exist (banned).	■ In the **Enter registry key in HKEY_format** field, enter registry key name that must start with HKEY and must not end with \. For example, `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\New Key`). ■ (Optional) In the **Value** field, enter the value of the registry key.

Posture Check Requirement	Description	Action
Windows Security Center	Verifies if the specified Firewall, Endpoint Security, or Windows Security Center is installed and active.	Select a list: ■ **Endpoint Security** ■ **Firewall** ■ **Windows Security Center Service**
Active Directory Association	Verifies if the user is signed in to a specified AD domain.	Enter the domain name. You can add ten domains by adding `OR` between the domain names.
Define Access Permission	Allows or blocks the network access to the device. Default is **Allow**.	Select an action from the **Define Access Permission** list: ■ To allow mobile devices to access networks, select **Allow**. ■ To block mobile devices from accessing networks, select **Deny**. ■ To allow chromebook and prevent android devices to access networks, select **Allow Chromebook only**.

9. To add more rules to OS, click **Add Rule to OS** and repeat step 8.



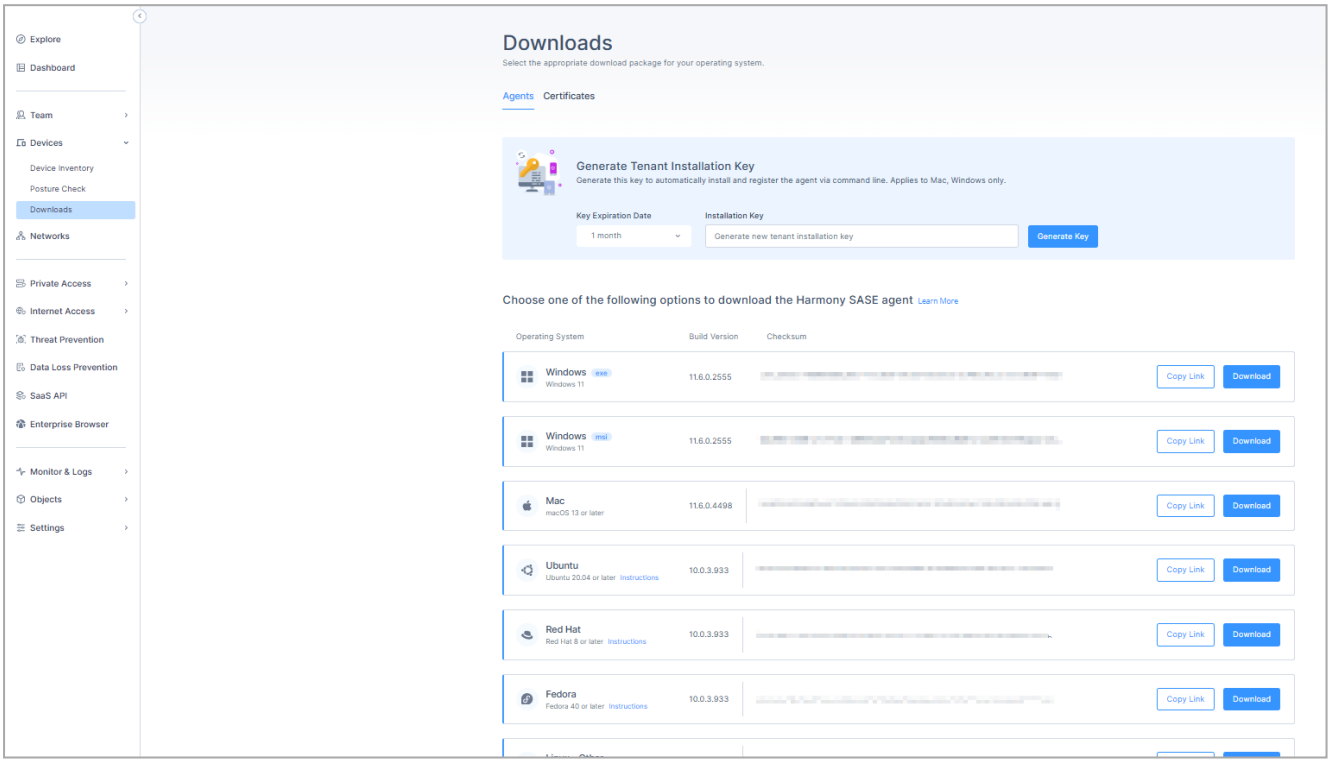
10. Click **Apply**.

    The Device Posture Check profile is created.

Downloads

In the **Downloads** page, you can download the SASE Agent and Certificate.

To view the **Downloads** page, access the Check Point SASE Administrator Portal and click **Devices** > **Downloads**.



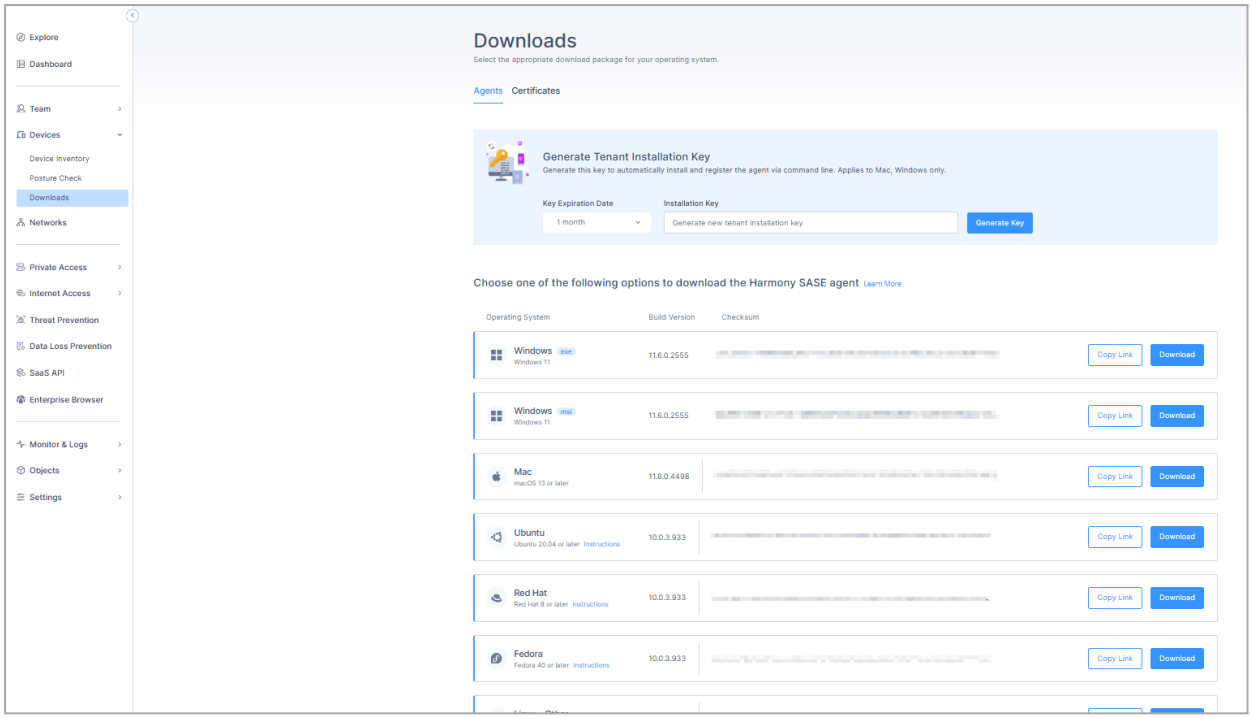
Note - The versions on this page may be newer than the default version for some customers, as a gradual rollout is in progress.

Downloading and Deploying the SASE Agent

Notes -

- For the latest SASE Agent versions, see sk182466.
- The SASE Agent is supported on devices with ARM processor in Private Access mode only.

1. Access the SASE Administrator Portal and click **Devices** > **Downloads**.
2. Click the **Agents** tab.



3. Do one of these:

- Click **Download**.

  The system downloads the file.

Operating System	Version	Downloaded File
Windows EXE	Windows 11	Downloads an exe file.
Windows MSI	Windows 11	Downloads a MSI file.
Mac	macOS 13 or later	Downloads a PKG file.
Ubuntu	Ubuntu 20.04 or later	Downloads a Deb file.
Red Hat	RedHat 8 or later	Downloads a RPM file.
Fedora	Fedora 40 or later	Downloads a RPM (Fedora) file.
Linux - Others	Linux 8.0 or later	Downloads a tar.xz file.
Android / Chromebook[1]	Android 12.1 or later	Redirects to Google Play Store.
iOS	iOS 15 or later	Redirects to Apple App Store.

  [1]To install SASE on Chromebook, see *"Installing SASE on Chromebook" on page 132*.

- Click **Copy Link** to copy the download link. Share the link with members.

4. To verify that the downloaded file is authentic, use the **Checksum**.
5. *"Deploying the SASE Agent" on the next page*.

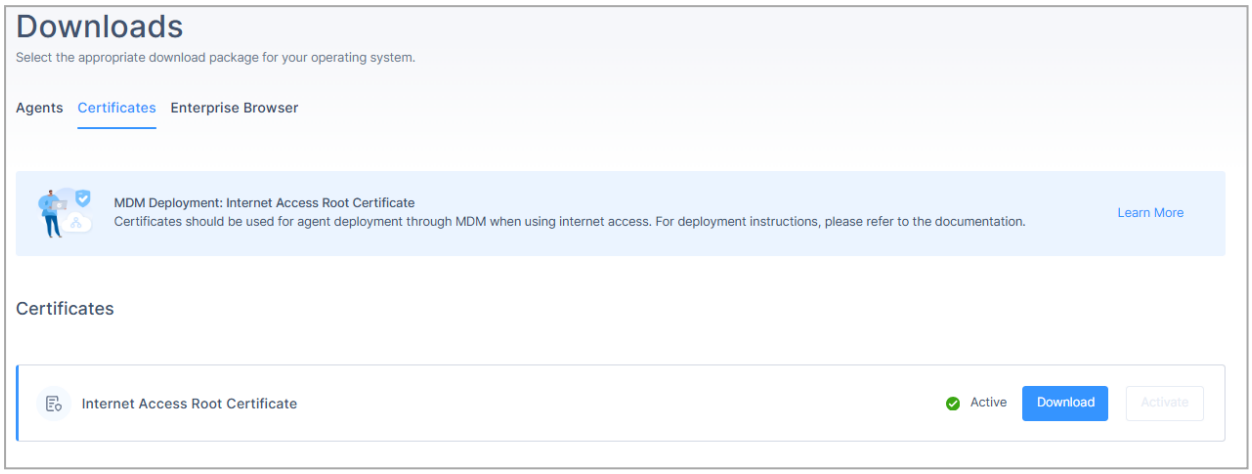
Downloading the Certificate

You can download Secure Web Gateway (SWG) root certificate and install it on macOS devices either manually or using an MDM application. The SWG root certificate is required for Internet Access.

Note- It is supported only with the macOS SASE Agent version 10.4 and higher.

To download the Internet Access Root Certificate:

1. Access the SASE Administrator Portal and click **Devices** > **Downloads**.
2. Click the **Certificates** tab.



3. Click **Activate** to activate the SWG root certificate.
4. When the certificate is active, click **Download**.

   The system downloads a PEM file.
5. Install the certificate on macOS devices either:
   - Manually
   - Using an MDM application. Refer to the MDM's documentation.

     Best Practice - Configure the required app permissions in the MDM so that it is installed without user intervention.

Deploying the SASE Agent

You can deploy the SASE Agent manually or using a Mobile Device Management (MDM) provider.

Prerequisites

- Network connectivity to required SASE Agent service URLs.
- Firewall access for required inbound and outbound traffic.
- Open ports based on the configured VPN protocol and tenant region.

For the complete list of required URLs, ports, and protocol details, see

sk182251

Deploying the Agent Manually

To deploy the agent manually:

- *"Invite Members" on page 74*

  The system sends an email to members with a link to accept the invite and download the Check Point SASE Agent. The invitation is valid for 30 days. If the invitation expires, you must resend the invitation.

- Download the agent and distribute it manually, for example, through email.
- Copy the agent download link and share it manually, for example, through email.

Deploying the Agent Using an MDM Application

You can deploy the agent using any of these popular Mobile Device Management (MDM) applications:

- Cisco Meraki
- JAMF Cloud
- ManageEngine
- Microsoft Intune
- Microsoft System Center Configuration Manager (SCCM)
- MobileIron
- VMWare AirWatch

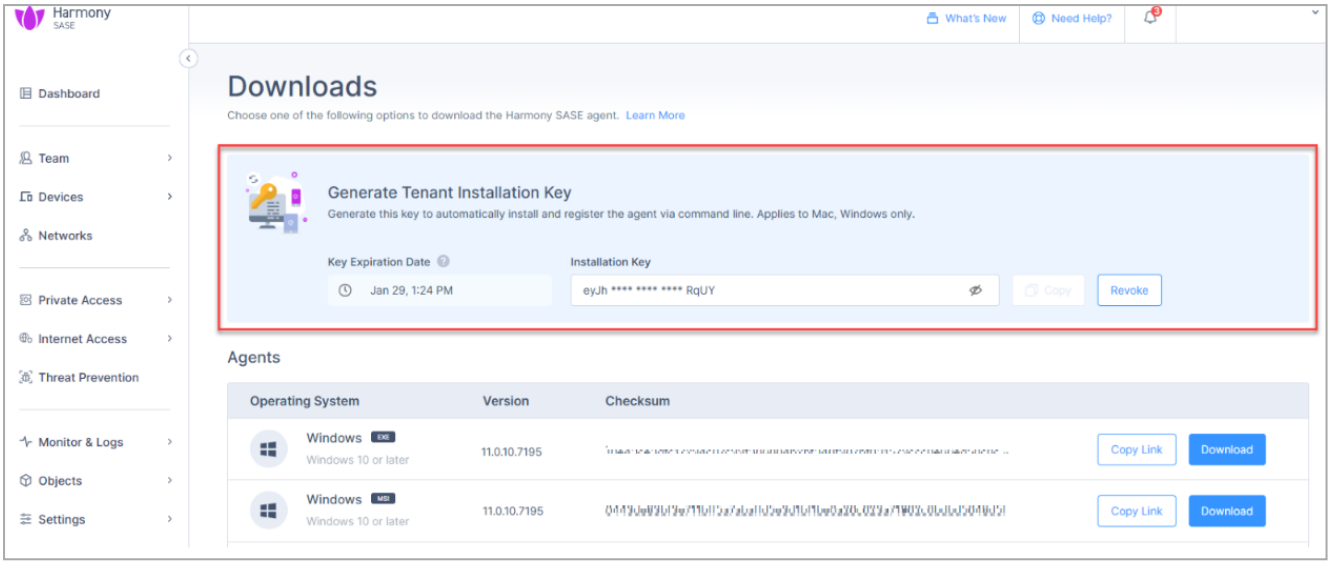
Transparent Internet Access Installation

Note - Applies to SASE Agent version 11.5 and higher.

The Transparent Internet Access enforces internet security immediately upon agent installation, without requiring any end-user interaction.

The remote installation process bypasses both device and member registration while ensuring that users receive the latest security policies, even if they have not signed in to the agent.

You can generate a unique installation key from the platform download page. This key is visible only to Admin users. Once generated, the key validity cannot be modified.



Note - Private Access remains restricted until the user authenticates and registers on the platform.

Seamless Internet Access installation requires sending a combination of these command line parameters during the agent installation process:

- `REGION`
- `WORKSPACE`*
- `TENANT_TOKEN`
- `EMAIL`*

  **Optional*

  Note - EMAIL is optional for Windows and mandatory for macOS.

Common Commands

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Silent Installation	`msiexec /quiet /i Harmony_SASE_ x.x.x.xxx. msi` To know the installation status after the silent installation, run: 1. `start /wait msiexec /quiet /i "Harmony_ SASE_ x.x.x. xxx.msi"` 2. `echo %errorlevel%`	`msiexec /quiet /i Perimeter81_ x.x.x.xxx. msi` To know the installation status after the silent installation, run: 1. `start /wait msiexec /quiet /i "Perimeter81_ x.x.x. xxx.msi"` 2. `echo %errorlevel%`	▪ **For version 11.0.10 and above**: `$ sudo installer -pkg Harmony_SASE_ x.x.x.xxx.pkg -target /` ▪ **For legacy versions (up to 11.0.10)**: `$ sudo installer -pkg Perimeter81_ x.x.x.xxx.pkg -target /` To change the agent permissions after the installation, run: 1. `$ sudo chown -R $(stat -f%Su /dev/console) "/Applications/ Perimeter 81.app"` 2. `$ chmod -R u=rwx "/Applications/ Perimeter 81.app"`	

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):

Pre-populating the tenant or workspace name	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name"`	`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name"`	`$ sudo defaults write com.perimeter81d workspace workspace_name`
			To remove pre-populated workspace/tenant name, run:
			`$ sudo defaults delete com.perimeter81d workspace`
			This is supported only with agent version 8.0.4.116 and higher.
				To pre-populae the workspace name, run:
				`/opt/Perimeter81/perimeter81 ctl set-prepopulate-tenant-id workspace_name`
				Replace "`workspace_name`" with your actual workspace

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Pre-populating the data residency region	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet REGION="EU, US, AU, or IN"` For `REGION`: ■ `"EU"` - Europe ■ `"US"` - America ■ `"AU"` - Australia ■ `"IN"` - India	`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet REGION="EU, US, AU, or IN"` For `REGION`: ■ `"EU"` - Europe ■ `"US"` - America ■ `"AU"` - Australia ■ `"IN"` - India	`$ sudo defaults write com.perimeter81d region "EU, US, AU, or IN"` For `REGION`: ■ `"EU"` - Europe ■ `"US"` - America ■ `"AU"` - Australia ■ `"IN"` - India	

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):

Pre-populating the tenant or workspace name and data residency region	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name" REGION="EU, US, AU, or IN"`
	
	For `REGION`:
	■ `"EU"` - Europe
	■ `"US"` - America
	■ `"AU"` - Australia
	■ `"IN"` - India
		`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name" REGION="EU, US, AU, or IN"`
		
		For `REGION`:
		■ `"EU"` - Europe
		■ `"US"` - America
		■ `"AU"` - Australia
		■ `"IN"` - India
			To pre-populating the tenant or workspace name, run:
			`$ sudo defaults write com.perimeter81d workspace workspace_name`
			To pre-populating the data residency region, run:
			`$ sudo defaults write com.perimeter81d region "EU, US, AU, or IN"`
			
			For `REGION`:
			■ `"EU"` - Europe
			■ `"US"` - America
			■ `"AU"` - Australia
			■ `"IN"` - India	

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Transparent user registration using tenant installation token (**applies for version 11.5 and above**)	`msiexec /quiet /i "Harmony_SASE_XX.XX.XX.XXXX.msi" REGION="EU, US, AU, or IN" TENANT_TOKEN="Installation Token"`			

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
	Note - If the device username does not match the user email address (verify by running whoami /upn from the command line), the email address must be provided as an explicit parameter: `msiexec /quiet /i "Harmony_SASE_XX.XX.XX.XXXX.msi" REGION="EU, US, AU, or IN" TENANT_TOKEN="Installation Token" EMAIL="user email address"`			

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Transparent user registration, using tenant installation and user installation (applies for version 11.3 and higher)			■ `$ sudo defaults write com.perimeter81 d REGION "EU, US, AU, or IN"` ■ `$ sudo defaults write com.perimeter81 d INSTALLATION_ PARAMETERS - dict TENANT_ TOKEN "Installation Token"` **Note** - For organizations using Active Directory (AD), you can pre-populate the user email address by adding the following to the command: `EMAIL $(stat - f%Su /dev/console)@% CompanyDomain%. com` ■ `$ sudo defaults write com.perimeter81 d EMAIL "User@email.co m"`	

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Uninstallation	`msiexec /x "Harmony_SASE_x.x.x.xxx.msi"`	`msiexec /x "Perimeter81_x.x.x.xxx.msi"`	Run the uninstall script.	

MDM Deployment of the SASE MacOS Agent with Internet Security

The SASE system includes **Web Security** features. When Internet Security is enabled on the workspace, the system deploys a locally installed extension, content filter, and certificate to perform SSL decryption. These components are typically installed post-login, requiring user approval. Administrators can pre-deploy these configurations to eliminate the need for user approval and prevent potential misconfigurations of web security components.

Deploying the Agent through MDM

Downloading the Certificate

1. For information on how to download the certificate, see Downloads.
2. Once the certificate is downloaded, add it to the deployment through MDM.

Deploying the Content Filter and System Extension

- Download the .mobileconfig file and certificate for deployment through MDM:

  Harmony SASE.mobileconfig

- Alternatively, a Workspace Administrator can manually configure the Content Filter and System Extension for deployment through MDM.

  Note - Each vendor may assign different names to these values.

- Deploy a **Content Filter**:
  - **Filter Type**: Plug-in
  - **Connection Name**: SASE
  - **Identifier**: com.safervpn.osx.smb
  - **Filter Webkit traffic**: Yes
  - **Filter Socket Traffic**: Yes
  - **Socket Filter Bundle ID**: com.safervpn.osx.smb
  - **Socket Requirement**: identifier "com.safervpn.osx.smb" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = "924635PD62"
  - **Filter Network Pockets**: Yes
  - **Pocket Bundle ID**: com.safervpn.osx.smb
  - **Packet Requirement**: identifier "com.safervpn.osx.smb" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = "924635PD62"
  - **Filter Grade**: Firewall
- Deploy a **System Extension**:
  - Navigate to where you add the VPN Payload Profiles and add a **MacOS** profile and context **Device Profile**.
  - **Allow User Overrides**: Yes
  - **Allowed System Extension Types**: Network
  - **Team ID**: 924635PD62
  - **Bundle Identifier**: com.safervpn.osx.smb.proxy

Installing SASE on Chromebook

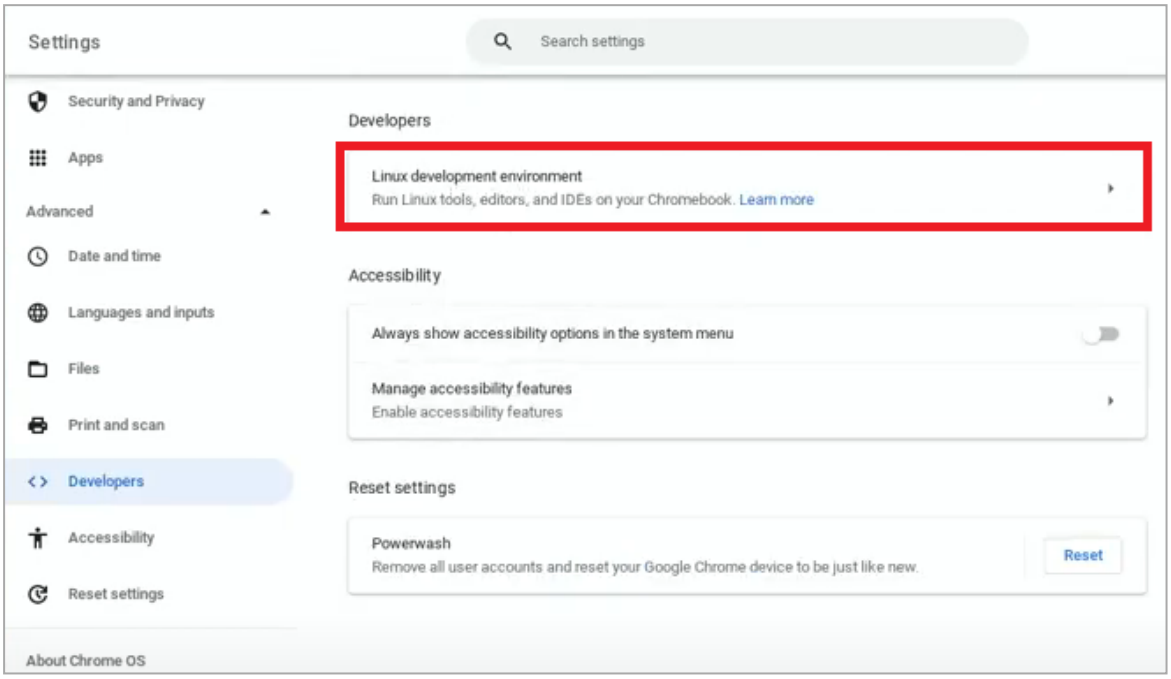
1. Download the **Check Point SASE** Agent. For more information, see Downloads.
2. To enable **Developer Mode**:
   a. Restart your Chromebook.
   b. Press **Esc** + **Refresh button** + **Power button** simultaneously during restart.

c. Press **Ctrl** + **D** when a warning is displayed.

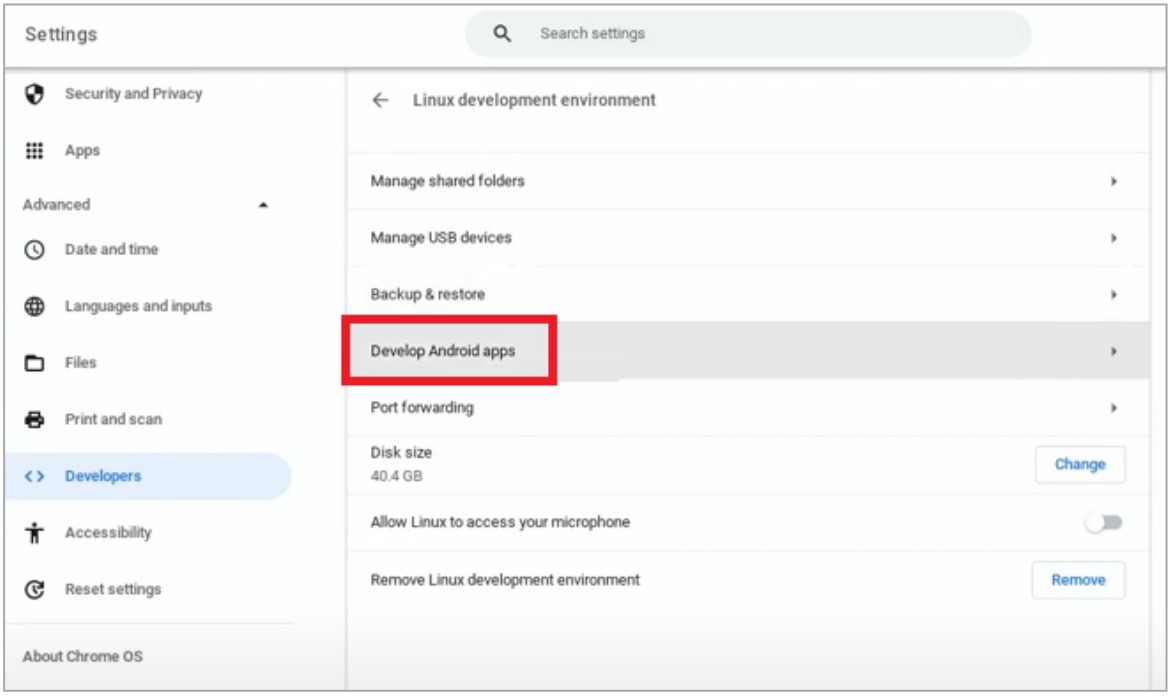
The **Developer Mode** is enabled.

3. To enable **ADB debugging**:

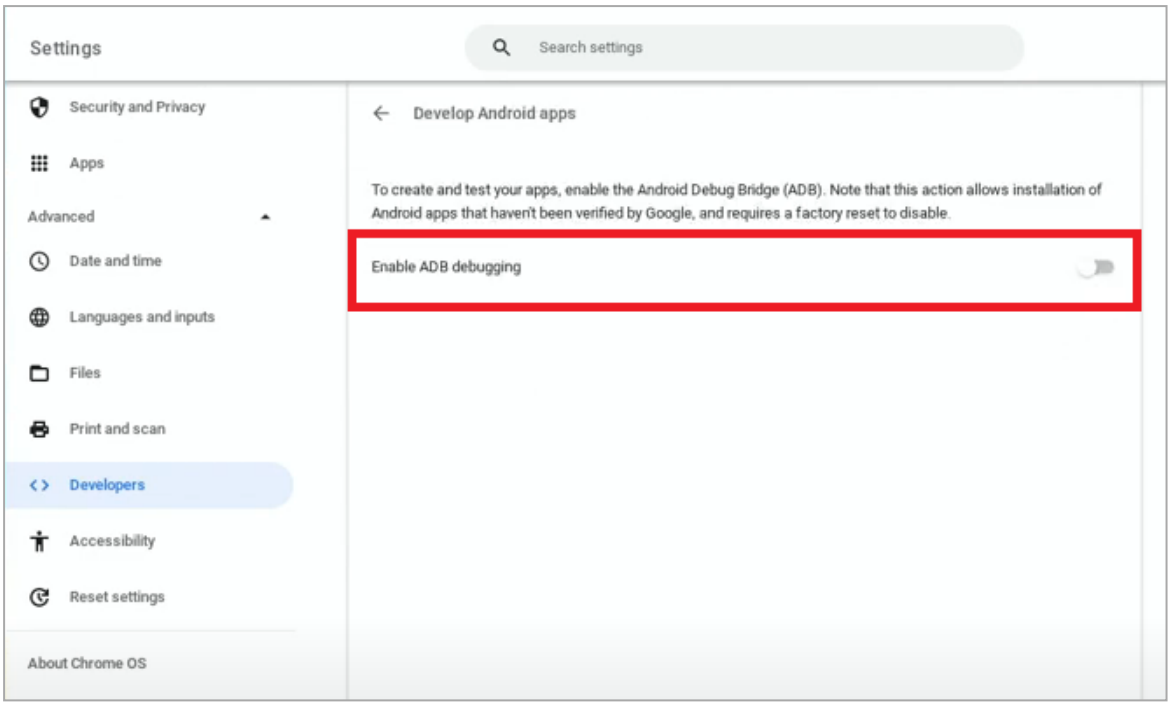
a. Go to **Settings** > **Advanced** > **Developers**.



b. Click **Linux development environment** > **Develop Android apps**.



c. Turn on the **Enable ADB debugging** toggle button.



The **Enable ADB debugging** window appears.

d. Click **Restart and continue**.

e. Click **Allow**.

The **ADB debugging** is enabled and the Chromebook restarts.

4. To install the ADB platform tools, go to your **Linux apps** folder and open **Terminal**.
5. Click **penguin** to open a Linux terminal and run:

```
sudo apt-get install android-tools-adb -y
```

The Android Package Kit (APK) file gets downloaded.

6. Navigate to **Linux** > **My files** > **Linux files**.
7. Drag and drop the downloaded APK file to the **Linux files** folder. This creates a new directory in the Linux terminal.
8. To check the default location where the new directory is created, go to the penguin Linux terminal and run:

```
df -h /boot/
```

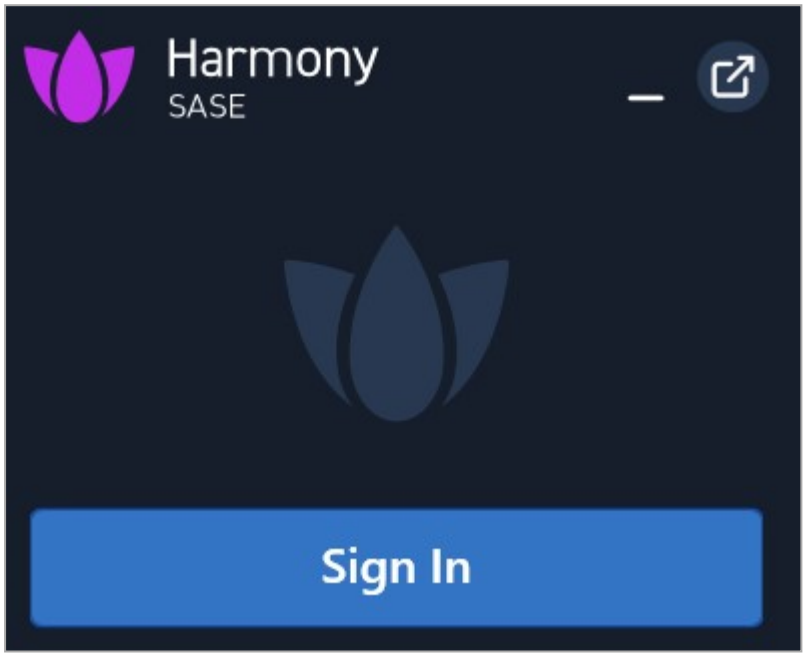
9. Navigate to the file system `cd /dev/hda1` should be the default folder where the API file is located at.
10. To install SASE Agent, run:

```
adb install <filename>.apk
```

Using the SASE Agent

Before you begin, contact your System administrator for your workspace URL.

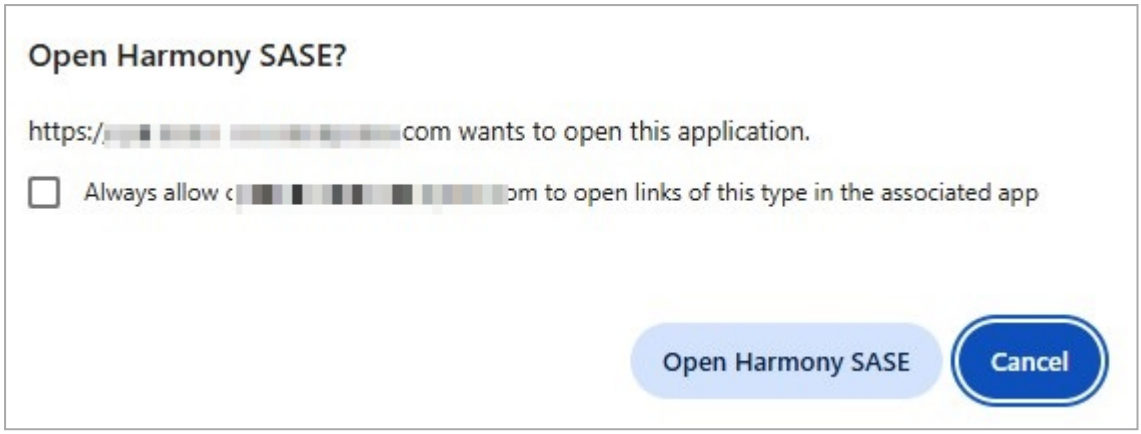
1. Open the SASE Agent.
2. Click **Sign In**.



   The system opens a web browser for authentication.
3. In the **Workspace URL** field, enter the workspace URL and click **Continue**.
4. Enter your credentials and click **Sign In**.

   If you do not know your credentials, contact your System Administrator.

   A prompt appears.
5. Click **Open SASE**.

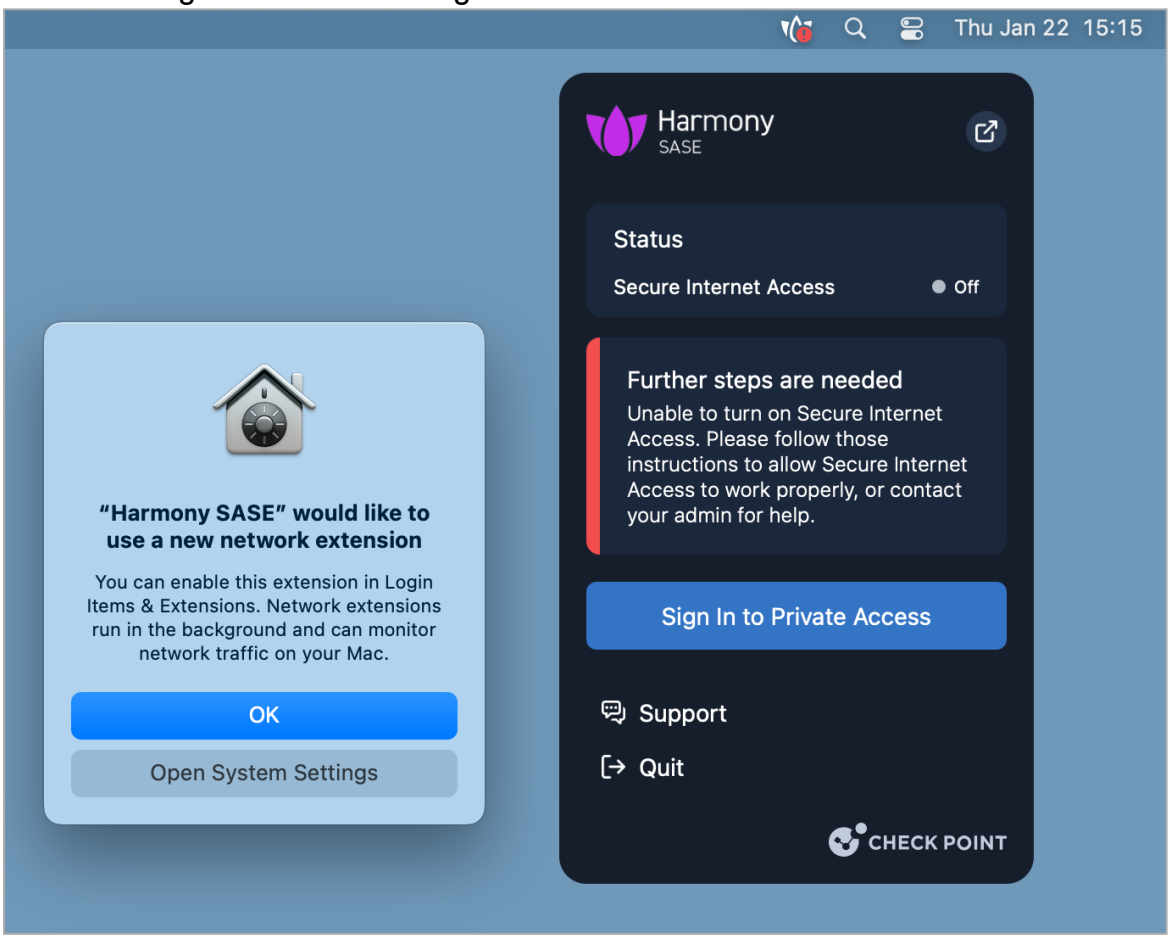


The SASE Agent opens and automatically connects to a **Network**.

6. For macOS devices, if internet access is enabled, then do these (otherwise, skip the step):

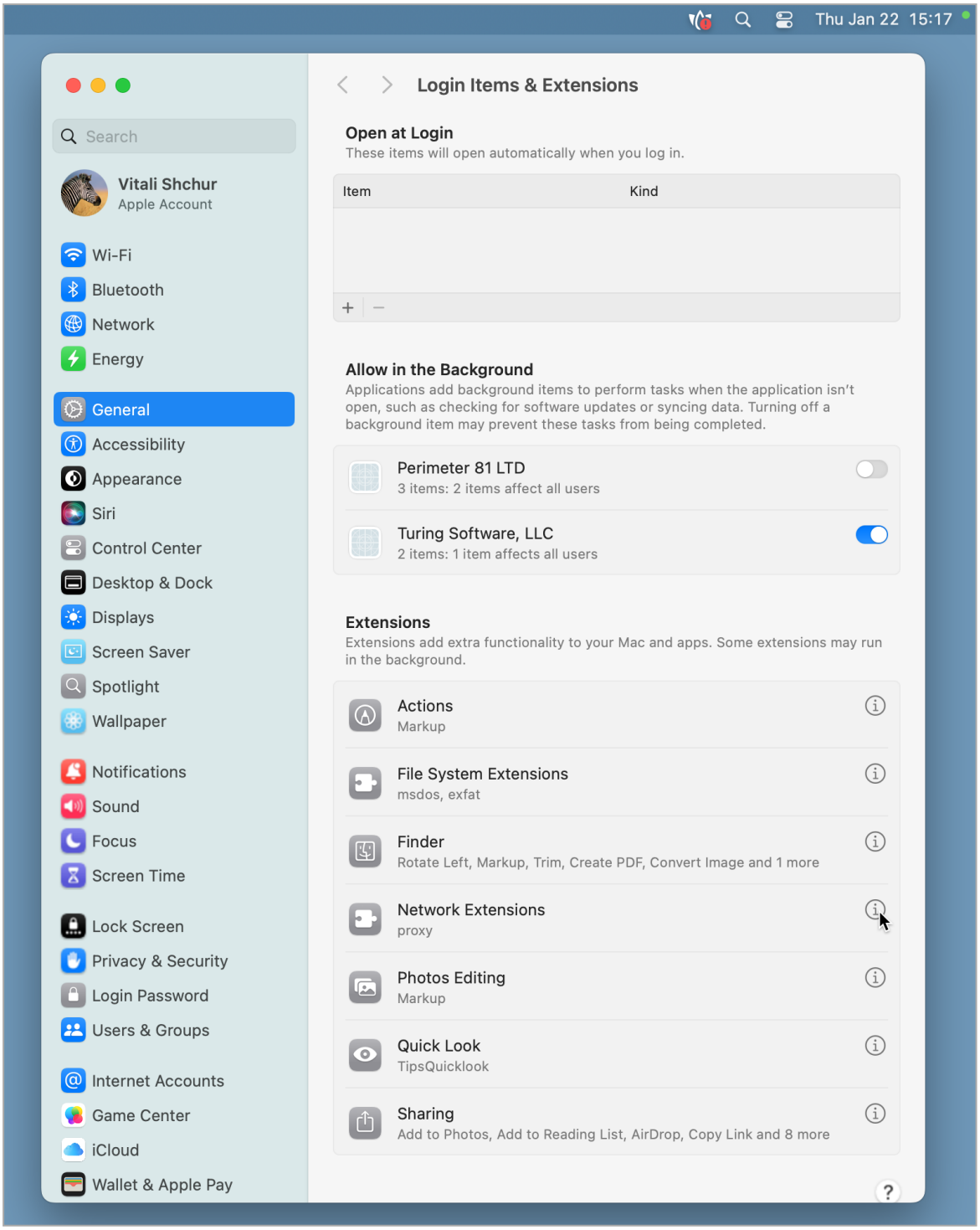
   Note - If you download the Secure Web Gateway (SWG) root certificate, skip the step. For more information, see Certificates.

   a. Install and sign in to the SASE Agent.

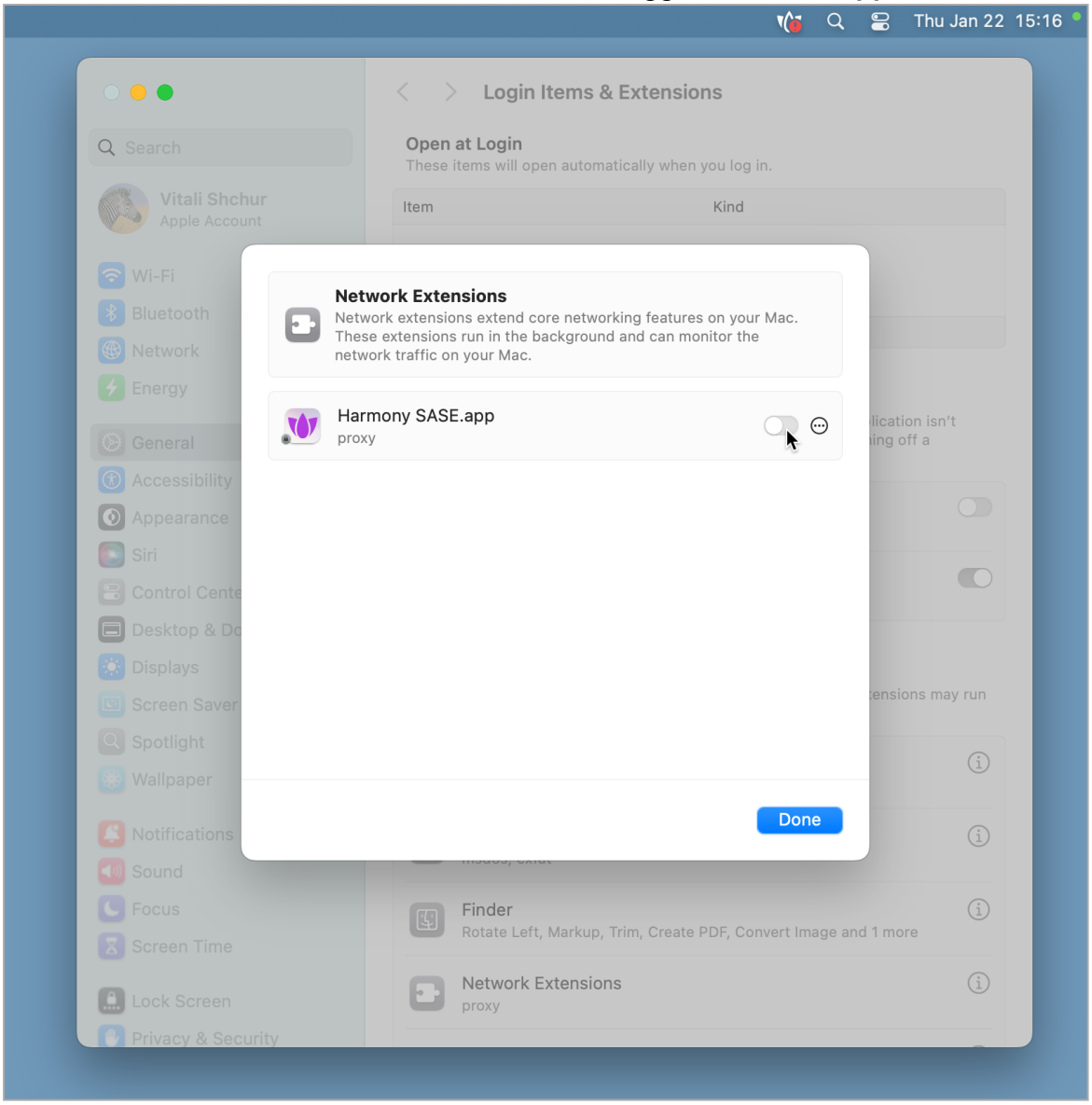


"Check Point SASE" would like to use a new network extension popup appears.

b. Click **Open System Settings**.
Alternatively, go to: **System Settings** > **General** > **Login Items & Extensions** > **Network Extensions**.

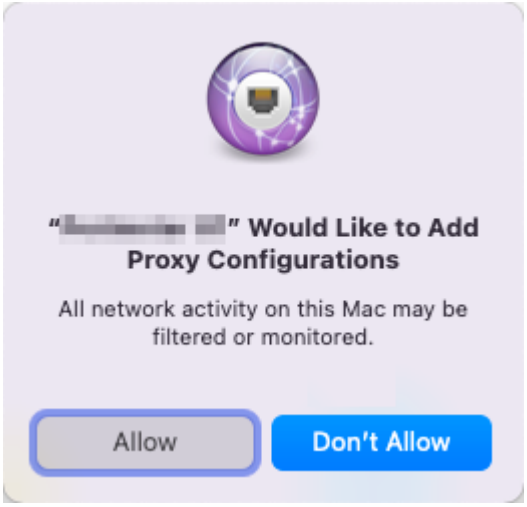


c. In the **Network Extensions** section, enable the toggle for **SASE.app**.

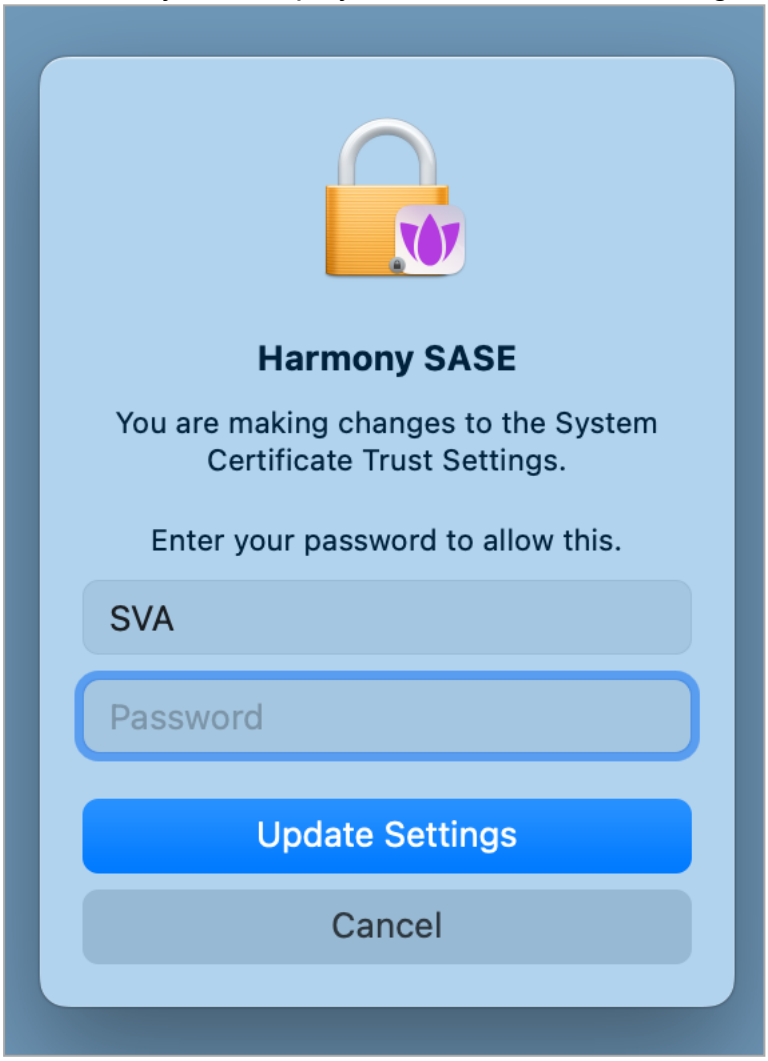


d. Click **Done**.

e. At this prompt, click **Allow**.



f. When the system displays the certificate trust dialog, enter your macOS password.



g. Enter your device credentials and click **Update Settings**.

7. To connect to a specific network, on the **Home** tab, click **Change Network** and then select a network.
8. To make changes to the SASE Agent, click the icon at the bottom left.

Setting	Description
General tab	
Connect of Launch	Automatically starts the SASE Agent when the device starts and connects to the most recent network.
Enable Notifications when Connected/Disconnected	Shows a pop-up notification on the device when the SASE Agent connection status changes.
Enable Notification when Reconnecting	Shows a pop-up notification on the device when the SASE Agent reconnects with the network.
Check For Updates	Checks and shows the latest version of SASE Agent if available.
Automatic Updates	Automatically upgrades to the latest version of the SASE Agent. **Note** - Available only if the System Administrator has enabled it. See *"Agent Upgrades" on page 94*.
Snowplow report.	Sends the Snowplow (user tracking) data to SASE.
Use VPN Interface DNS	Sets the device DNS server as the SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface. If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers.
Network tab	
Always-On VPN	Automatically connects to the VPN when an internet connection is available.
Automatic Wi-Fi Security	The SASE Agent automatically connects to SASE VPN if the device connects to an unsecured Wi-Fi.

Setting	Description
Trusted Wi-Fi Networks	The SASE Agent does not enable **Automatic Wi-Fi Security** if the device connects to a trusted Wi-Fi network. **Note** - This option shows only the trusted networks added by the administrator. See *"Network Configuration" on page 95*.
Protocols tab	
Default	Automatically connects to the network using a protocol configured by the administrator. See *"Network Configuration" on page 95*.
WireGuard	Connects to the network using WireGuard protocol.
OpenVPN	Connects to the network using OpenVPN protocol.

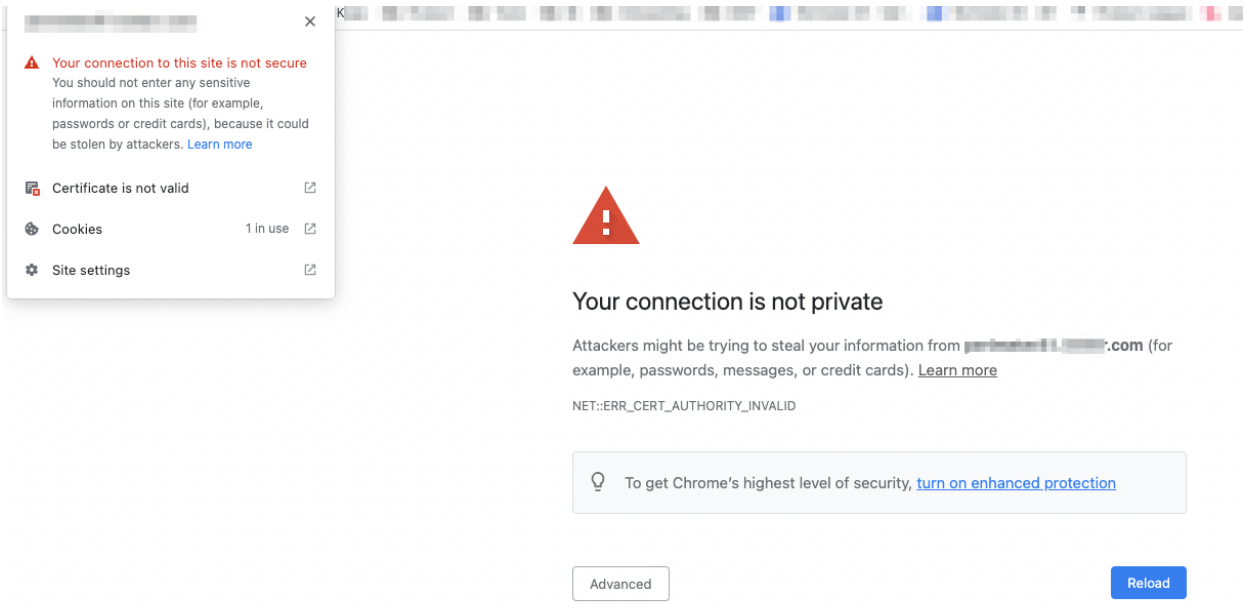
9. Go the **Support** tab and do these:
   - To reset the agent, click **Reset Agent**.
   - To view the documentation, click **User Guides**.
   - To start a live chat with a SASE expert, click **Live Chat**.
   - To run a quick health check and send the results to SASE, click **Send Logs to Support**.
10. To sign out of the agent, click the icon.

    If this option is disabled by the administrator, the agent prevents the member from signing out without a sign-out code. For more information, see *"Disable Sign-Out" on page 93*.
11. To exit the agent, click the icon. This disables the agent and stops the secure private and internet access.

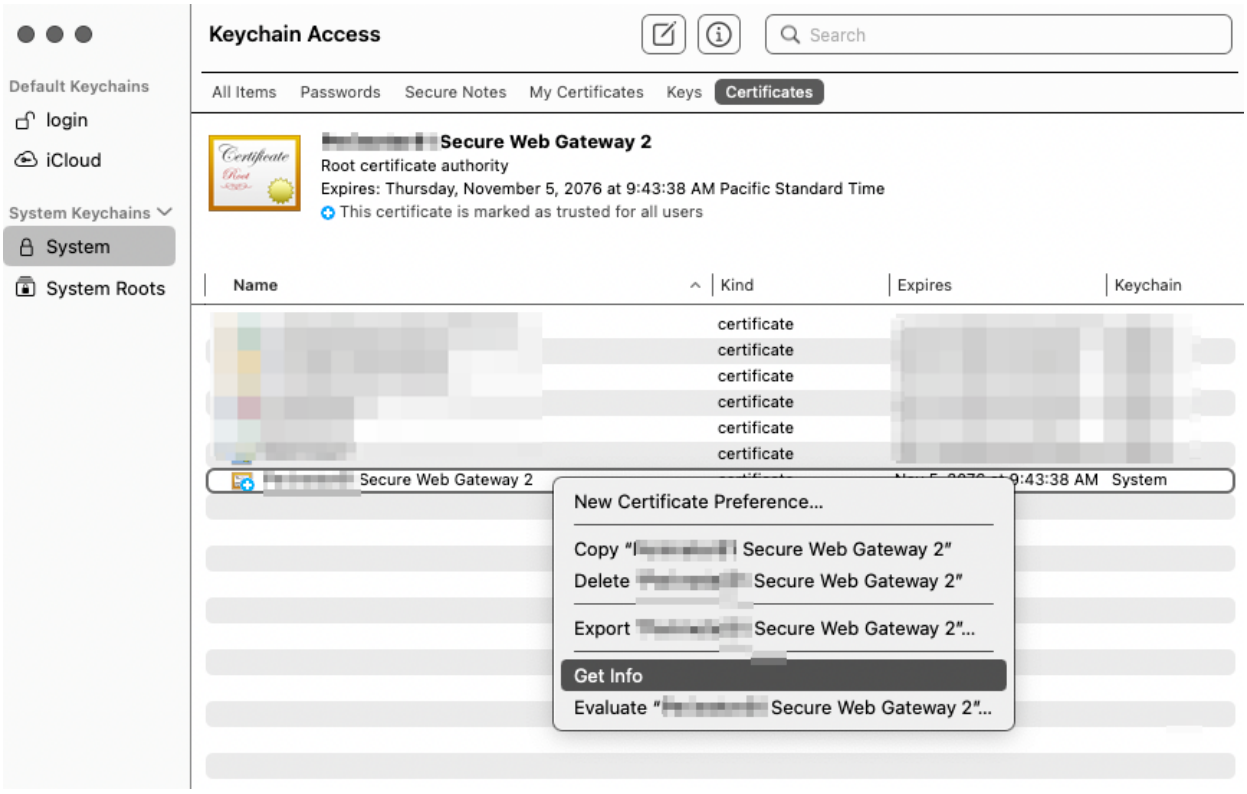
Troubleshooting System Extension Installation on macOS

If the member does not complete the system extension installation during the agent installation:

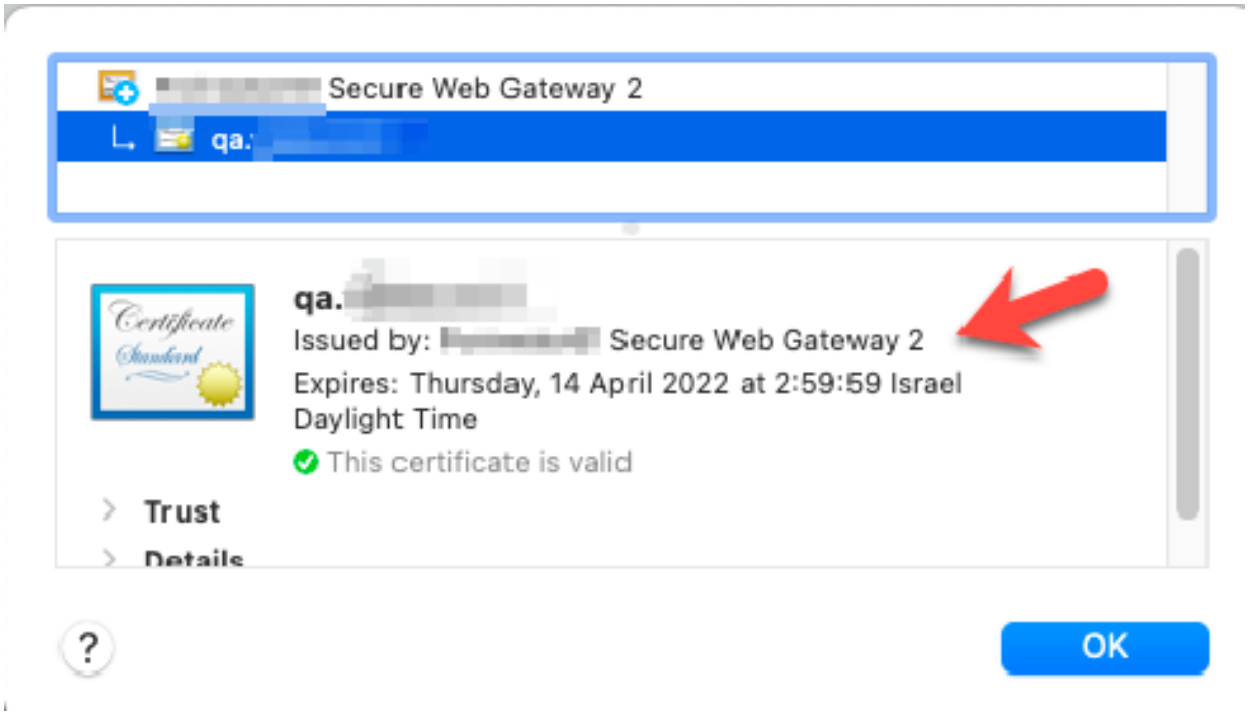
1. Sign out and sign in to the agent.
2. If the Secure Web Gateway certificate installation is blocked, then this error message appears.



3. Open **Keychain Access** (Press Cmd + Space, then search for Keychain Access).



4. Right click **SASE Secure Web Gateway 2** certificate and click **Get Info**.
5. Modify the permission to **Always trust**.



Refresh the web page. The site should load without certificate warnings.

SASE Agent - Optimized Performance with Minimal Resource Impact

SASE Agent is designed for optimal performance, ensuring your device stays fully operational while maintaining robust security. The agent uses minimal resources across all platforms, providing a smooth experience with little impact on system performance.

Performance Efficiency

- **Minimal CPU Usage**: SASE Agent is designed to use minimal CPU resources, enabling users to perform tasks without disruption, even during heavy network traffic.
- **Optimized Memory Usage**: The agent efficiently manages system memory, ensuring minimal resource consumption while maintaining high performance.

Typical Resource Usage

Applicable to Windows 10 or higher and macOS 11 or higher:

Component	Typical Usage*	CPU Utilization
Private Access	Approximately 150 MB	0-5%
Internet Access	Approximately 600 MB	0-5%
Private + Internet Access	Approximately 750 MB	0-5%

The values above reflect typical usage during standard operations. However, resource consumption may temporarily increase during intensive tasks, such as heavy browsing or large file downloads.

Remote Sign-In of Linux Devices to Private Access

This allows administrators to remotely sign in Private Access users on Linux devices using command-line interface (CLI) tools, even during or immediately after installation.

It enables user authentication to the SASE Agent, so the device can access private resources as defined in your Zero Trust Network Access policies.

Prerequisites

- Install the Linux version 10.0.3.933 or higher.
- Users are fully registered to the tenant with both email and password.

Use Case

This feature enables administrators to remotely register and sign in Linux devices to Private Access (PA) using CLI commands, without requiring any user interaction. This helps manage unattended or remotely located devices.

Using the Linux Agent CLI for Private Access Login and Troubleshooting

After installation, the Linux agent runs as a background service. You can access its control interface through these commands:

1. Login to Private Access:

   ```
   /usr/bin/p81-helper-daemon ctl login TENANT_ID USERNAME PASSWORD
   ```

   Replace,

   `TENANT_ID` with your tenant ID.

   `USERNAME` and `PASSWORD` with the user's login credentials.

   Note - The provided `TENANT_ID` must have database identity provider enabled.

2. To view CLI help:

   ```
   /usr/bin/p81-helper-daemon ctl --help
   ```

3. To view login-specific help:

   ```
   /usr/bin/p81-helper-daemon ctl login --help
   ```

4. If login fails, the CLI displays a descriptive error message. For support, collect and provide:

   a. The full command used, excluding the password.

   b. CLI output or a screenshot of the error.

   c. Files from this location, compressed into .zip or .tar:

   ```
   /var/log/perimeter81helper*.log
   ```

Pre-Login Tunnel Connection for Windows

Pre-Login Tunnel Connection allows users to establish a secure SASE tunnel before signing in to the Windows operating system. This capability enables access to private organizational resources, such as on-premises Active Directory (AD), even when users are outside the corporate network and have not yet signed in to the device.

When enabled, the SASE Agent authenticates the user and creates a secure tunnel directly from the Windows login screen. This ensures that required Private Resources are available during the Windows sign-in process.

Note - This feature is available in Early Availability (EA). For access, contact Check Point Support.

Use Cases

New Device Provisioning for Remote Users: Remote users who receive a new PC might need access to an on-premises Active Directory domain defined as a Private Resource. Because AD access requires an active secure tunnel, Pre-Login Tunnel Connection enables the tunnel to be established before the first Windows sign-in.

Remote Troubleshooting and IT Support: If users cannot sign-in to Windows or require assistance before sign-in, Pre-Login Tunnel Connection enables secure connectivity to Private Resources. This allows IT teams to access required systems and provide troubleshooting support securely.

Prerequisites

- SASE Agent version 12.5 or higher is installed on the endpoint.
- The SASE Agent is connected to the organizations workspace.
- Pre-Login Tunnel Connection is enabled at the tenant level.
- Users have access to a secondary authentication device, such as a mobile phone for multi-factor authentication approval.

Limitations and Technical Notes

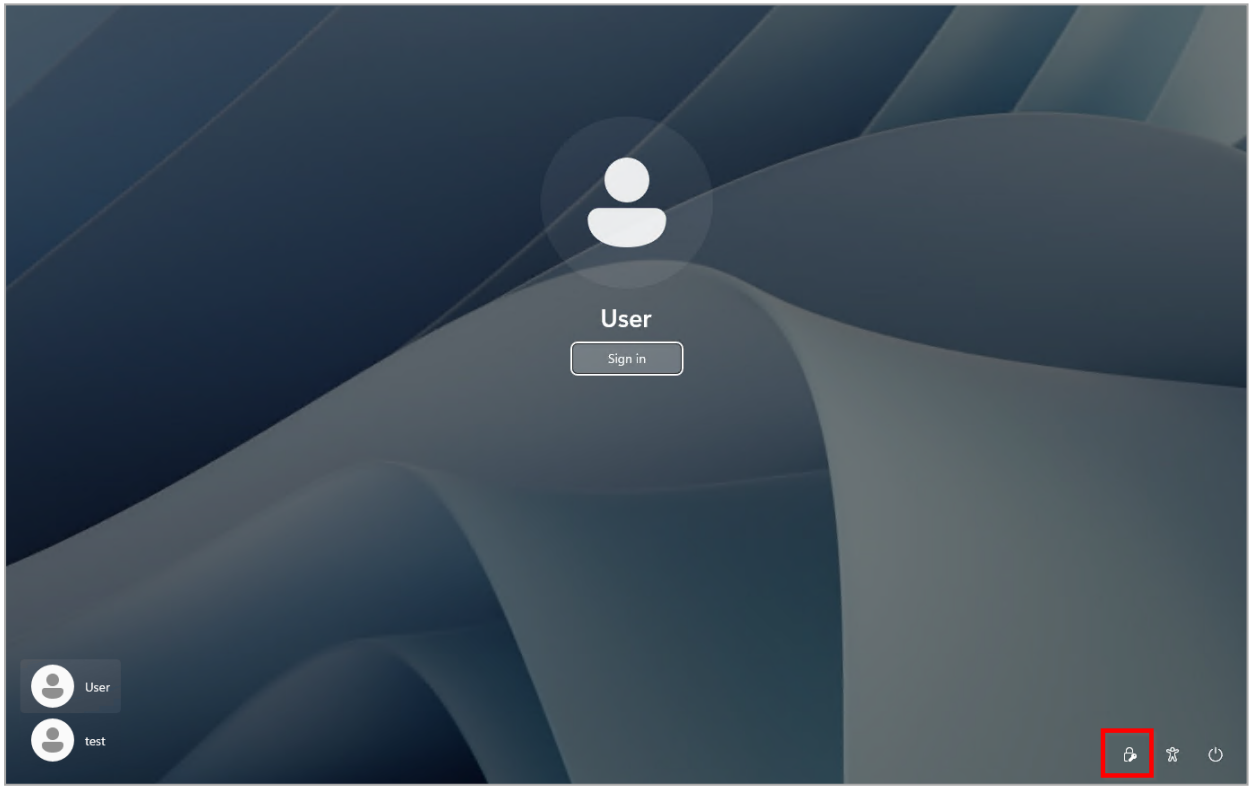
- **Shared Device Protection (Multi-User Environments)**: If Shared Device Protection is enabled, Pre-Login Tunnel Connection is not supported.
- **Device Posture Check (DPC)**: Device Posture Check is not performed while no user is signed in to the operating system. DPC runs automatically after the user signs in to Windows.

- **Agent Upgrade Enforcement**: Agent upgrades cannot be enforced while no user is signed in to the operating system. Any pending upgrade enforcement occurs immediately after Windows login.
- **Network Selection**: Manual network selection is not available in pre-login mode. The agent connects automatically to the last connected network, or to the default network on the first connection.
- **Trusted Network Detection**: Trusted Network Detection is disabled during pre-login mode and resumes after Windows login.
- **Internet Access Only License**: Users with an Internet Access only license cannot use the pre-login Tunnel feature.

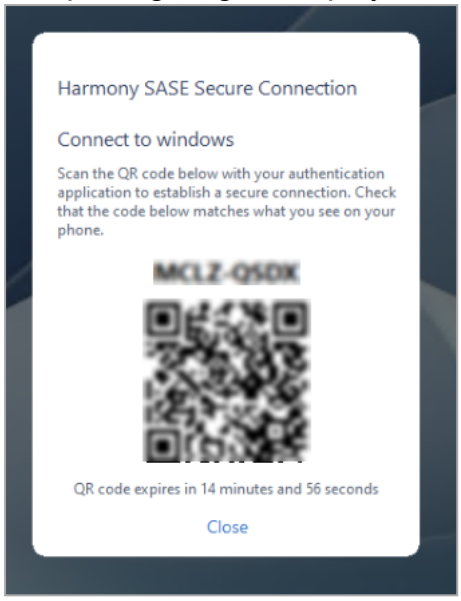
Enabling Pre-Login Tunnel Connection

Pre-Login Tunnel Connection is controlled at the tenant level and applies to all users in the tenant.

1. Turn on the Windows device.
2. On the Windows sign-in screen, click the Network icon.

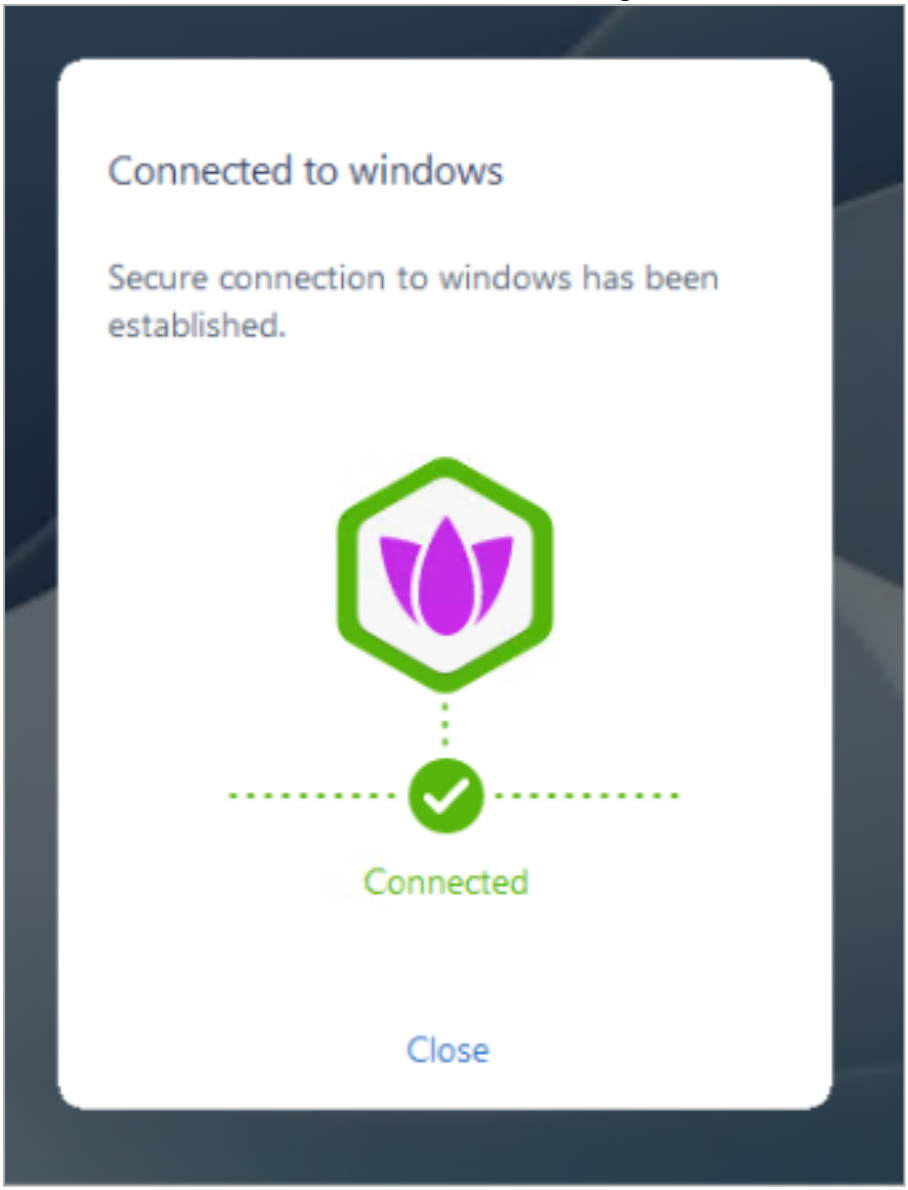


The pre-login agent displays a QR code.



3. Use a secondary device to scan the QR code.
4. On the secondary device, verify the matching code and complete authentication.

5. After successful authentication, the SASE Agent establishes a secure tunnel.



Note - The name represents your organizations configured tenant. For example, “Connected to <Tenant Name>” based on the tenant configuration.

6. Sign in to Windows.

   The device can access required Private Resources, such as Active Directory, and the secure session continues uninterrupted.

Multiuser and User Switching on Shared Devices (Windows only)

SASE Agent version 11.7 enhances security on shared Windows devices by detecting when users switch accounts and applying Internet Access policies specific to each user.

The agent ensures each monitored device receives user-specific security by enforcing individual policies, browsing restrictions, and private resource access based on group membership. Security events are logged under the active user's account for accurate tracking. This provides administrators with clear visibility and control over user activity on all monitored devices.

User Identification and Policy Assignment

- For Domain and Active Directory or Entra Synced Users:
  1. The agent automatically detects the domain user using the User Principal Name (UPN).
  2. The device is reassigned to the detected user.
  3. User-specific policies and restrictions are applied immediately.
- For Local or Non-Domain Users (UPN Unavailable):
  1. A new user account is automatically created in the SASE Administrator Portal.

     Note - Local users are created in the `%username%.%devicename%@%tenantname%.local` format. Each local user account uses an additional user license.
  2. The new user is assigned to the default group policy named All users.
  3. The device remains protected by this policy.

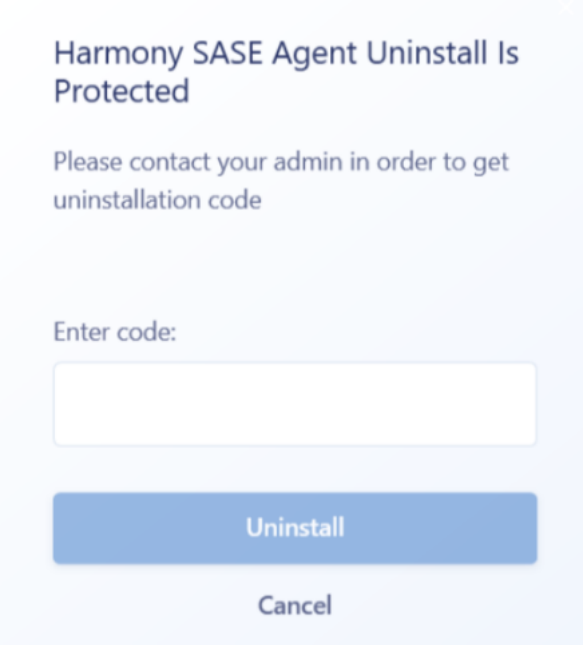
     Important - Access to private resources (for example, VPN connections) is not available for local users.

Uninstalling the SASE Agent

Windows

Follow the computer's procedure to uninstall the agent.

Note -
If the administrator blocked the agent uninstallation, the **Check Point SASE Agent Uninstall is Protected** window appears:



1. In the **Enter Code** field, enter the uninstallation code. To get the code, contact your administrator.
2. Click **Uninstall**.

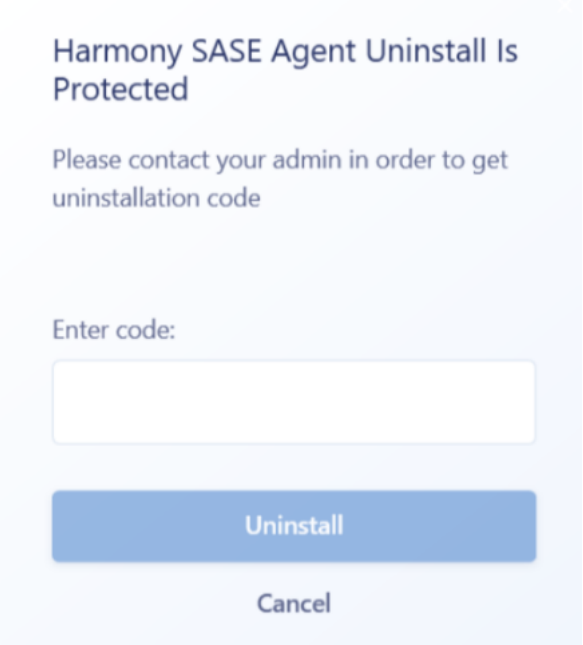
macOS

- Follow the computer's procedure to uninstall the agent.
- Run this command in the terminal to automatically download and execute the uninstall script:

```
curl
https://supportbucketshare.s3.amazonaws.com/Knowledge+Base/uninstall.sh | sudo bash
```

Notes:

- If you use SASE Secure Web Gateway (SWG), deploy the SWG-enabled agents in the presence of your Customer Success Engineer.
- If the administrator blocked the agent uninstallation, the **Check Point SASE Agent Uninstall is Protected** window appears:



a. In the **Enter Code** field, enter the uninstallation code. To get the code, contact your administrator.
b. Click **Uninstall**.

Linux

Ubuntu

To uninstall the SASE Agent, run:

```
CLICLIsudo apt remove --purge <Perimeter 81 package name>
sudo rm -Rf /etc/Perimeter81
sudo rm -Rf $HOME/.config/Perimeter81
sudo rm -Rf /opt/Perimeter81
```

Android / iOS

Follow the device's procedure to uninstall the agent.

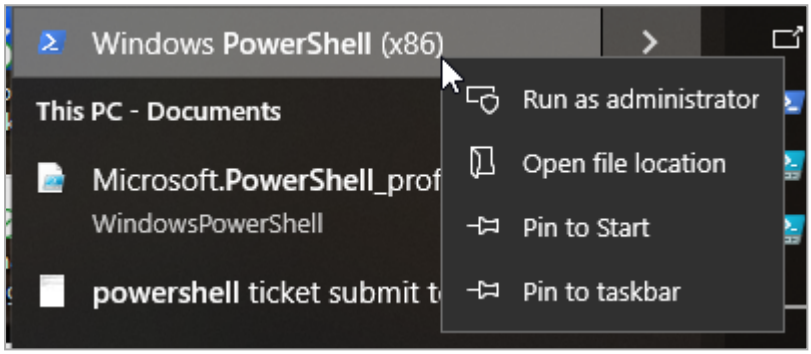
Collecting Logs Manually

If the SASE Agent fails to perform automatic log collection, you can manually collect and send the logs using scripts.

Note - This option is available only for the Perimeter 81 workspace accounts.

Windows

1. Right-click Windows PowerShell and click **Run as administrator**.



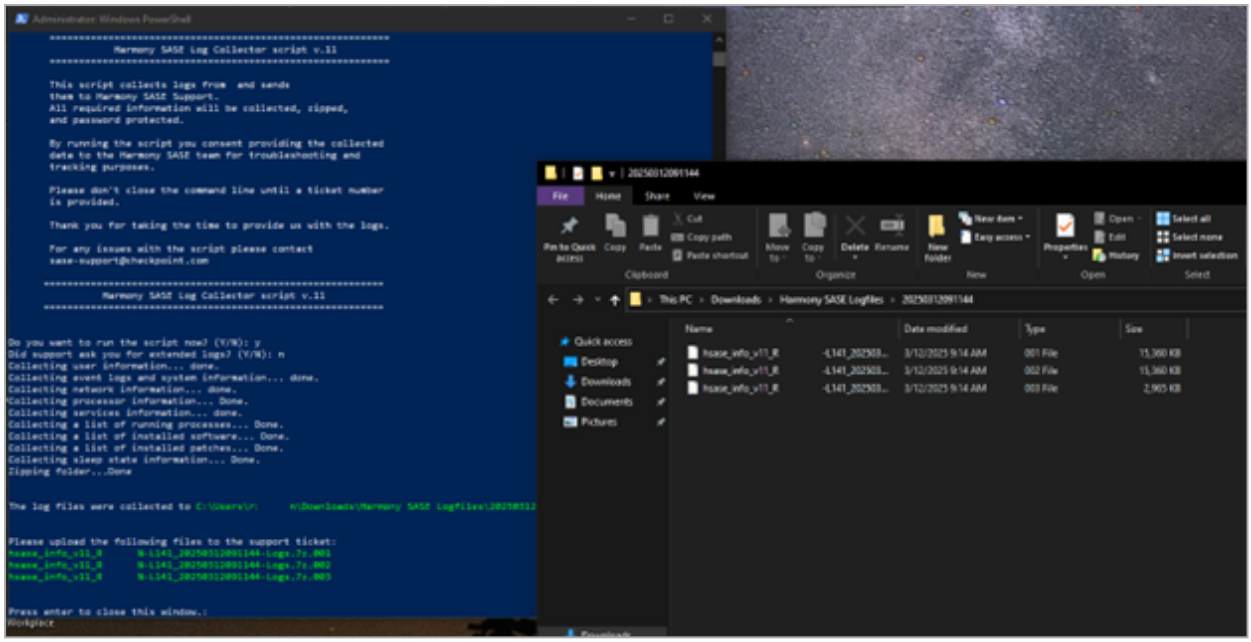
2. Run:

```
Invoke-Expression ((New-Object
System.Net.WebClient).DownloadString
('https://supportbucketshare.s3.us-east-
1.amazonaws.com/Custom+Scripts/Log+Collector/Log+Collector+PS.ps
1'))
```

3. When prompted, enter **Y**. If support requests extended logs, enter **Y** again.

   Note - Enable extended logs only if instructed by support, as they are significantly larger.

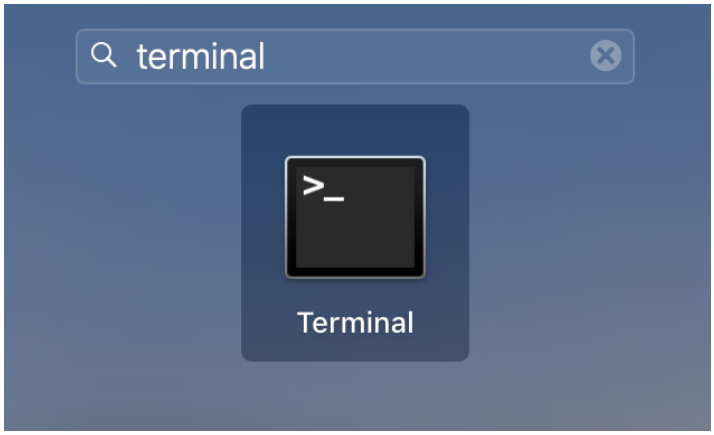
4. Once the script completes, an Explorer window opens with the log files.



5. Submit the required files to your support ticket.
6. Once the support confirms receipt, manually delete the **Check Point SASELogfiles** directory from the **Downloads** folder.

macOS

1. On your Mac machine, open the **Terminal** application.



2. Copy and run:

```
curl -s "https://supportbucketshare.s3.us-east-1.amazonaws.com/Custom+Scripts/Log+Collector/Log+Collector+SH.sh" -o temp.sh;sudo bash temp.sh;rm temp.sh
```

3. Once the script completes, a Finder window opens with the log files.
4. Submit the .zip file to your support ticket. Older runs are saved under **Previous Runs**.

5. Once support confirms receipt, manually delete the **SASE Logfiles** directory from the *Downloads* folder.

Linux

1. On your Linux machine, open the **Terminal** application and run:

   ```
   /opt/Perimeter81/perimeter81 collect-logs
   ```

2. Send the log file to *Check Point Support*.

Networks

The **Networks** page allows you to specify your network for private access. A network consists of three basic components:

- *"Regions and Point-of-Presence" on page 157*
- *"Gateways" on page 160*
- *"Tunnels" on page 163*

High-Level Procedure

"Defining a Network" on page 167.

"Enhanced Network" on page 173

"Adding a Tunnel" on page 198.

"Managing a Network" on page 223.

Regions and Point-of-Presence

Regions are the physical locations of your Check Point SASE gateway(s). You can deploy the Check Point SASE gateway in a single or multiple (Lower latency, redundancy and better performance) regions. SASE automatically connects your members to the nearest Check Point SASE gateway.

North America	EMEA	APAC	LATAM
■ Montreal, Canada (1) ■ Vancouver, Canada (1) ■ Ashburn 1, VA, USA (1) ■ Boston, MA, USA(1) ■ Chicago 1, IL, USA (1) ■ Dallas 1, TX, USA (1) ■ Denver, CO, USA (1) ■ Los Angeles 1, CA, USA(1) ■ New York 1, NY, USA (1) ■ New York 3, NY, USA(1) ■ Silicon Valley 1, CA, USA (1) ■ Toronto 2, Canada ■ Toronto 3, Canada ■ Ashburn 2, VA, USA ■ Atlanta 1, GA, USA ■ Atlanta 2, GA, USA ■ Chicago 2, IL, USA ■ Dallas 2, TX, USA ■ Fremont, CA, USA ■ Honolulu, HI, USA ■ Los Angeles 2, CA, USA ■ Miami, FL, USA	■ Vienna, Austria (1) ■ Brussels 1, Belgium (1) ■ Frankfurt 1, Germany (1) ■ Tel Aviv 1, Israel (1) ■ Stockholm 1, Sweden (1) ■ Zurich 1, Switzerland (1) ■ Istanbul, Türkiye (1) ■ Dubai, UAE (1) ■ London 1, UK (1) ■ London 3, UK (1) ■ Manchester 1, UK (1) ■ Helsinki, Finland ■ Helsinki 2, Finland ■ Paris, France ■ Paris 2, France ■ Frankfurt 3, Germany ■ Frankfurt 4, Germany ■ Tel Aviv 2, Israel ■ Milan, Italy ■ Amsterdam 2, Netherlands ■ Amsterdam 4, Netherlands ■ Warsaw 1, Poland ■ Warsaw 2, Poland ■ Johannesburg, South Africa ■ Madrid 1, Spain ■ Madrid 2, Spain ■ Madrid 3, Spain	■ Perth, Australia(1) ■ Hong Kong, China(1) ■ Auckland, New Zealand (1) ■ Taipei 1 (1) ■ Melbourne, Australia ■ Melbourne 2, Australia ■ Sydney 1, Australia ■ Sydney 2, Australia ■ Bangalore 1, India ■ Bangalore 2, India ■ Chennai, India ■ Mumbai 1, India ■ Mumbai 2, India ■ New Delhi, India ■ Jakarta, Indonesia ■ Osaka, Japan ■ Osaka 2, Japan ■ Tokyo 1, Japan ■ Tokyo 2, Japan ■ Singapore 2 ■ Singapore 3 ■ Seoul, South Korea	■ Sao Paulo 2, Brazil ■ Sao Paulo 3, Brazil ■ Santiago, Chile ■ Mexico City, Mexico

North America	EMEA	APAC	LATAM
■ Miami 2, FL, USA ■ New Jersey 1, NJ, USA ■ New Jersey 2, NJ, USA ■ New York 2, NY, USA ■ San Francisco, CA, USA ■ Seattle, WA, USA ■ Seattle 2, WA, USA ■ Silicon Valley 2, CA, USA	■ Stockholm 2, Sweden ■ London 2, UK ■ London 4, UK ■ Manchester 2, UK		

Notes -

- (1) Data centers managed by Check Point SASE. All other data centers are managed by trusted cloud service providers.
- Each listed location represents a distinct Region.
- If you cannot find a suitable region, contact *Check Point Support*.

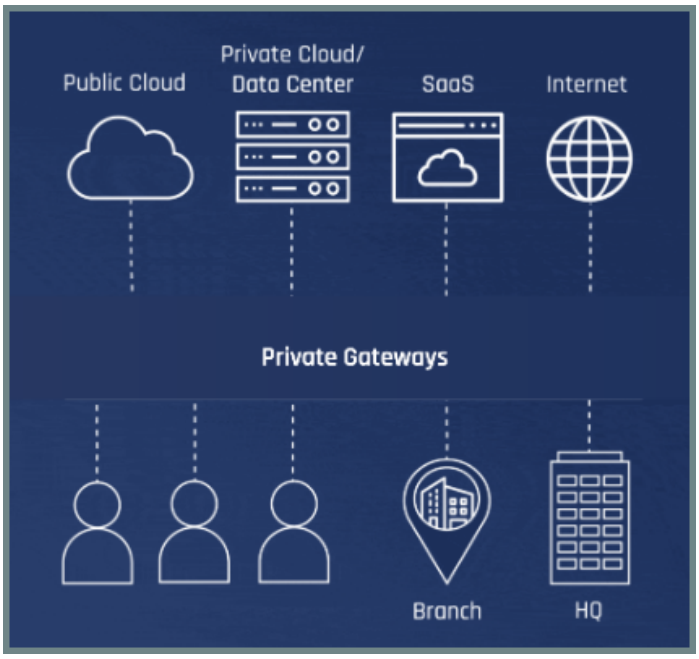
Gateways

Gateways are the cloud-based Check Point SASE servers deployed in the region you select. Each gateway is assigned a unique static IP address that can be connected to your on-premises or cloud resources through tunnels. You can deploy multiple gateways for redundancy, and load balancing. Check Point SASE supports two types of gateways:

- *"Private Gateways" below*
- *"[DEPRECATED] Shared Gateways " below*

Private Gateways

Private gateways are the dedicated gateways deployed for you. By default, all gateways are deployed as private. If you deploy multiple gateways, then at least one gateway must be private.



Note - The default gateway is of the type private. Every Check Point SASE network must consist of at least one private gateway.

[DEPRECATED] Shared Gateways

Shared gateways are shared among customers. They are suitable if you cannot find a private gateway in your preferred region.

SASE supports shared gateways in these regions:

- Austria
- Argentina

- Australia
- Belgium
- Brazil
- Canada
- Cyprus
- Denmark
- Finland
- France
- Germany
- Hong Kong
- India
- Ireland
- Israel
- Italy
- Japan
- Mexico
- The Netherlands
- New Zealand
- Poland
- Portugal
- Romania
- Russia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- USA East
- USA West

- The United Kingdom

Notes:

- By default, all gateways are deployed as private. If you want to deploy a shared gateway, at least one gateway must be private.
- Shared gateways support only internet access. They do not support private access.

To allow members to connect to a shared gateway, see *"[DEPRECATED] Shared Network" on page 94*.

Tunnels

Tunnels are encrypted secure connections between the SASE gateway and your SD-WAN device (on-premises or cloud) on your network. You can connect all your branches to a network using a single or multiple tunnels.

Check Point SASE supports three types of tunnels:

- *"IPSec Site-2-Site VPN Tunnel" below*
- *"WireGuard Connector Tunnel" on the next page*
- *"OpenVPN Tunnel" on page 165*

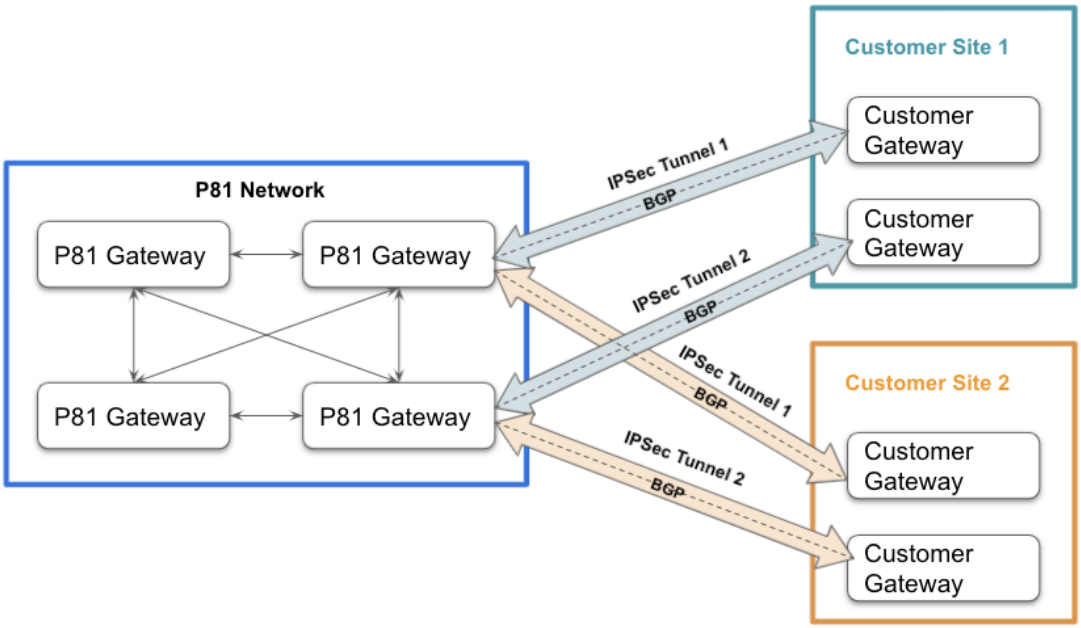
IPSec Site-2-Site VPN Tunnel

IPSec (IP Security) is a protocol suite designed to secure data communication over IP networks to ensure integrity, confidentiality, and authentication. It uses the IKE VPN protocol to establish a secure communication between networks. An IPSec tunnel connects your Check Point SASE gateway with your local network.

You can configure either a **single IPSec Site-2-Site VPN tunnel** or **redundant tunnels**.

With a single tunnel, all the traffic is routed through this tunnel.

With redundant tunnels, traffic is routed through multiple tunnels. This offers high network availability, redundancy, better performance by routing traffic to the closest tunnel.



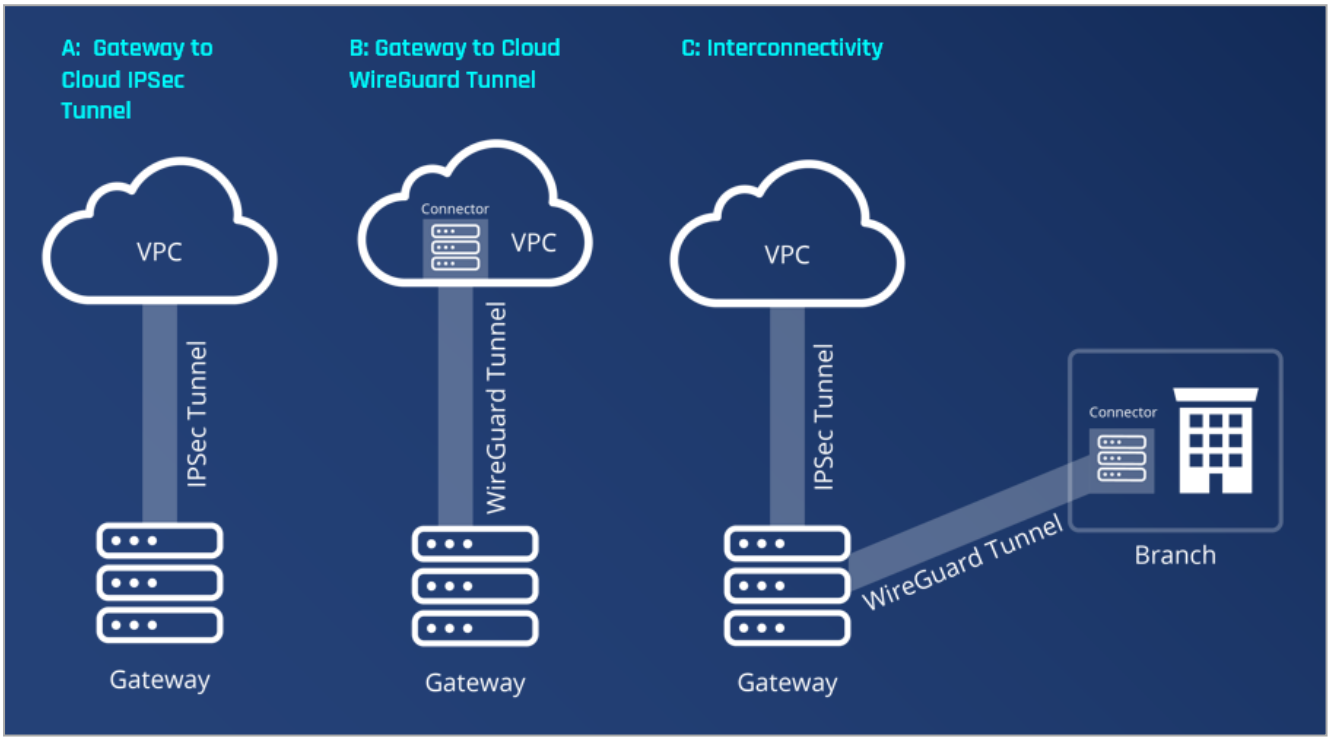
Best Practice - For redundancy, we recommend that you deploy the gateways in different regions depending on users' location.

To configure an IPSec Site-2-Site VPN Tunnel, see *"IPsec Site-to-Site VPN Tunnel" on page 199*.

WireGuard Connector Tunnel

WireGuard Connector is a fast and modern VPN that utilizes state-of-the-art cryptography. It is designed as a general-purpose VPN to run on embedded interfaces and super computers alike.

This shows an example of tunnel usage in a network.



This table shows a comparison between Wireguard connector and IPSec tunnels.

	Wireguard Connector	IPSec Tunnel
Site-to-Site Implementation	Wireguard	strongSwan
VPN Protocol	Wireguard	IKE
Internet Protocol	UDP	Any
Setup Environment	Linux	Any
Stability	High	High
Chipers Design Date	00's-10's	90's-00's
Code Length	4k	400k-60k lines

To configure a Wireguard connector, see *"WireGuard Connector Tunnel" on page 205*.

OpenVPN Tunnel

The OpenVPN protocol creates secure and private site-to-site connections using the SSL encryption. It is suitable in these scenarios:

- Incompatible operating system. For supported operating systems, see *"Downloading and Deploying the SASE Agent" on page 118*.
- You want to create a dedicated Check Point SASE connection with a single machine.
- The device does not support the Check Point SASE Agent.

Caution - The OpenVPN tunnel does not offer advanced security as the agent, such as Split Tunneling, DNS Filtering, Configuration Profiles, Firewall, Activity, SWG, DPC, and Single Sign-On.

To configure a OpenVPN Tunnel in the Check Point SASE Administrator Portal, see *"OpenVPN Tunnel" on page 214*.

Internal Network Subnet

The Check Point SASE SASE network is designed according to internationally acknowledged standards and follows the RFC conventions regulated by the American internet authorities. To successfully incorporate Check Point SASE in your architecture, make sure that:

1. Your internal network follows industry-accepted design patterns.
2. Virtual Private Cloud (VPCs) or Data Centers (DC) with overlapping subnets do not reside in the same network.
3. Your Check Point SASE network subnet does not overlap with your network subnet.
4. (Highly Recommended) All subnet masks are either class B or C.
5. (Recommended) Your internal network has a static public IP.

   Caution - 192.168.1.0/24 and 10.0.0.0/24 are the most commonly used subnets for IoT applications.
   If you connect to a site with this CIDR from a typical home location, it causes an IP conflict. Use 192.168.81.0/24 or 10.81.0.0/24 as the subnet to connect your site to Check Point SASE.

Dynamic IP Tunnels

In order to establish a site-to-site tunnel (IPSec or WireGuard) between your SASE gateway and a firewall or router with a dynamic public IP address, you need to apply some modifications to the tunnel creation process. Follow the instructions in:

- *"IPsec Site-to-Site VPN Tunnel" on page 199*
- *"WireGuard Connector Tunnel" on page 205*

Notes:

- This option is not supported by cloud IaaS providers (AWS, GCP, or Azure).
- Only a single dynamic IP IPSec tunnel is supported per each Cloud Gateway.

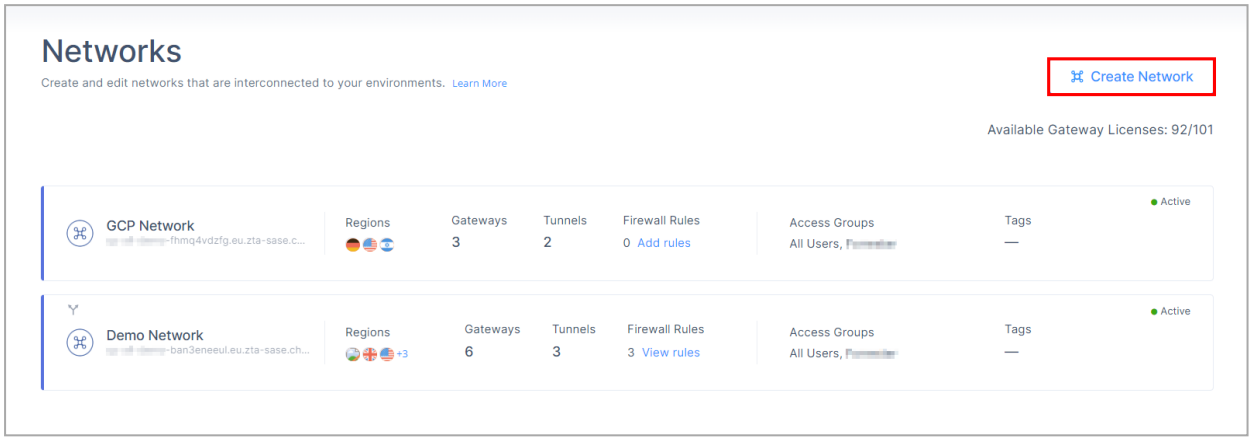
Creating a Network

To protect the cloud infrastructure using SASE, you must define the network, add gateways, and create tunnels.

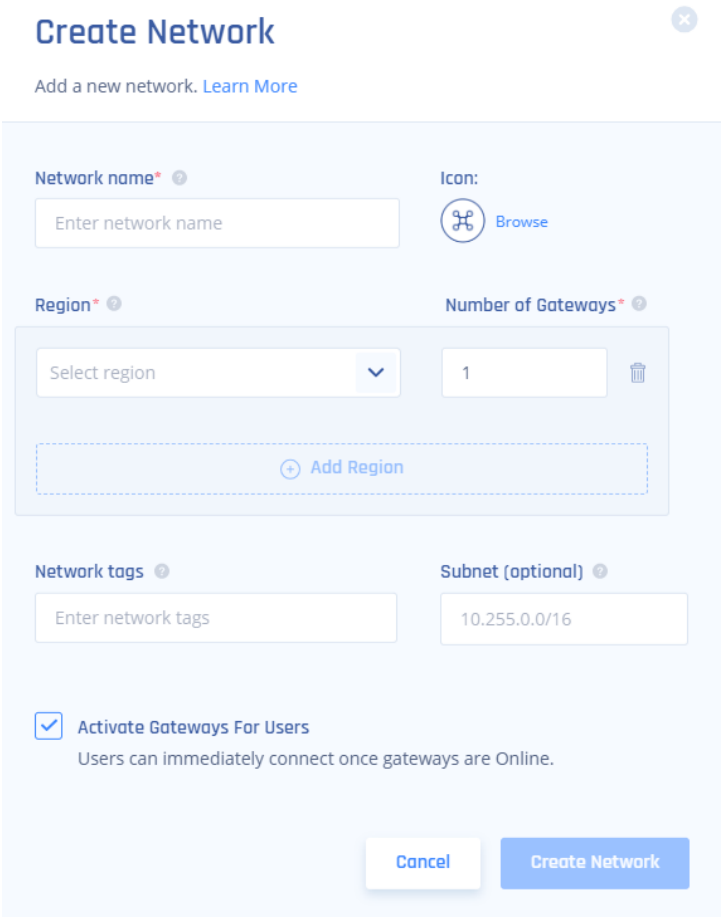
- Step 1 - Define a network
- Step 2 - Add a tunnel
- Step 3 - Verify the tunnel setup
- Step 4 - Manage the network

Defining a Network

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click **Create Network**.



3. Enter the network details:



a. **Network name** - Name for your network. For example, HQ, Finance, or Staging.

b. **Icon** - Icon for your network.

   The default is . To change the icon, click **Browse** and select the icon.

c. **Region** - Region to deploy the Check Point SASE gateway.

   We recommend that you choose a region closest to your members.

d. (For Standard Network) **Number of Gateways** - The number of private gateways you want to deploy in the region.

   Make sure that the number does not exceed the purchased licenses.

e. To add another region, click **Add Region** and repeat steps c and d.

f. **Network Tags** - Network tags to identify the different purposes and/or teams that your Network supports.

g. **(Optional) Subnet** - Your network subnet IP address. The default is 10.255.0.0/16. For information on possible subnets and bit masks, see sk182225.

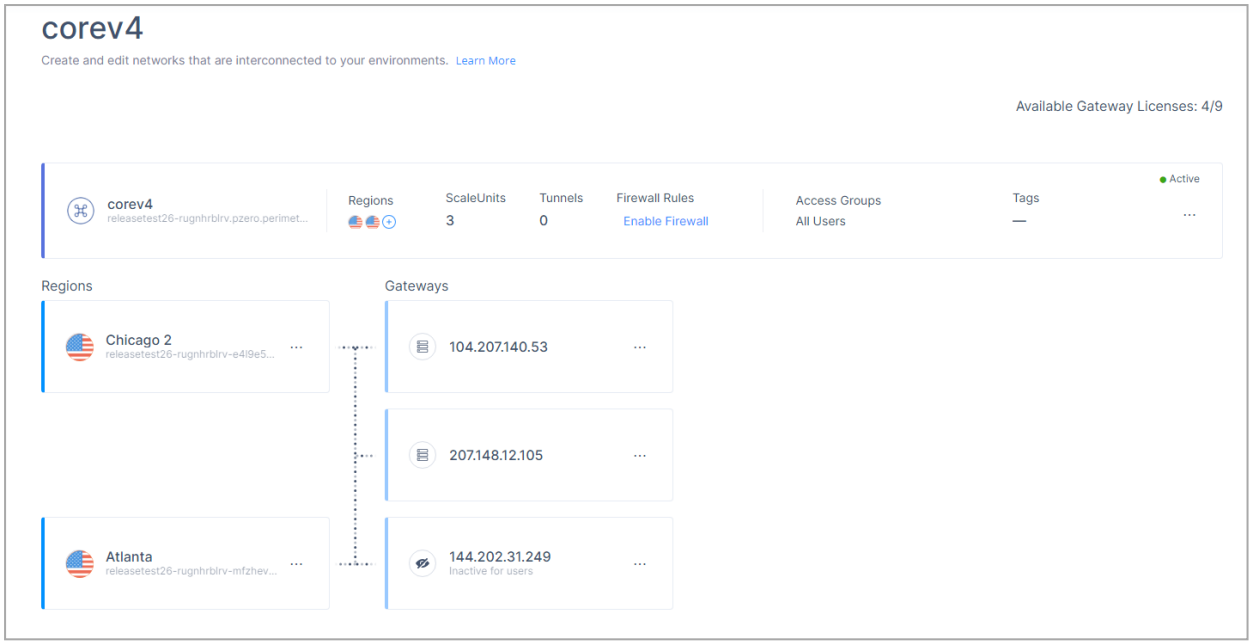
   Warning - You cannot change your subnet after you create your network. Make sure that the subnet does not overlap with your SD-WAN device's subnets.

4. The **Activate Gateways For Users** checkbox is selected by default. Clear it if you want to deactivate the gateway.

5. Click **Create Network**.

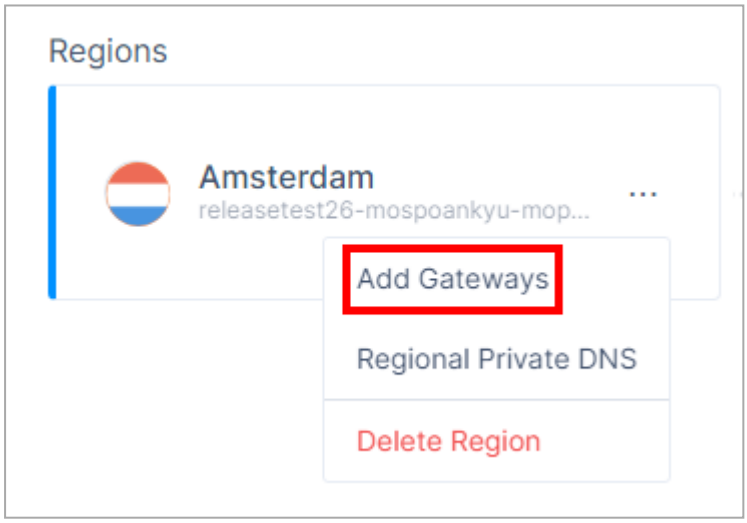
   The system creates the network and it is listed in the **Networks** page.

6. To view the network architecture, click the network name.

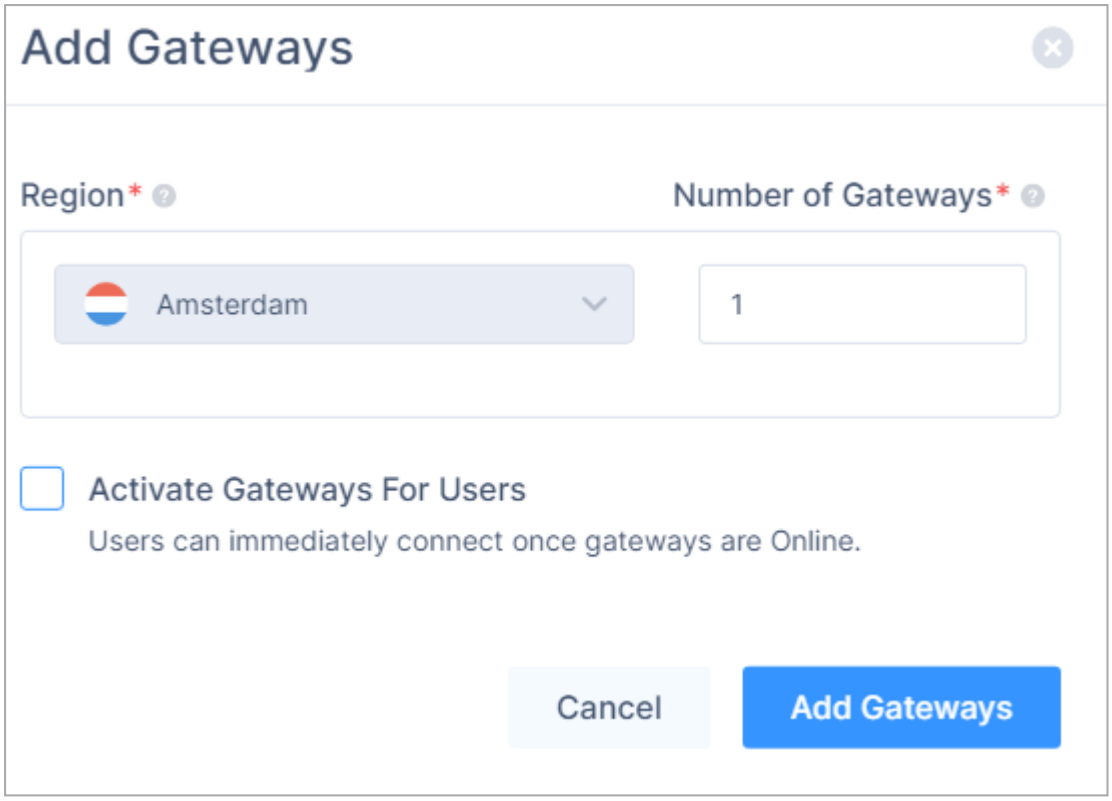


Adding Gateways to an Existing Network

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· on your Region and then click **Add Gateways**.



The **Add Gateways** window appears.



The gateway is inactive by default.

4. To activate the gateway, select the **Activate Gateways For Users** checkbox.
5. Click **Add Gateways**.

Deactivating a Gateway

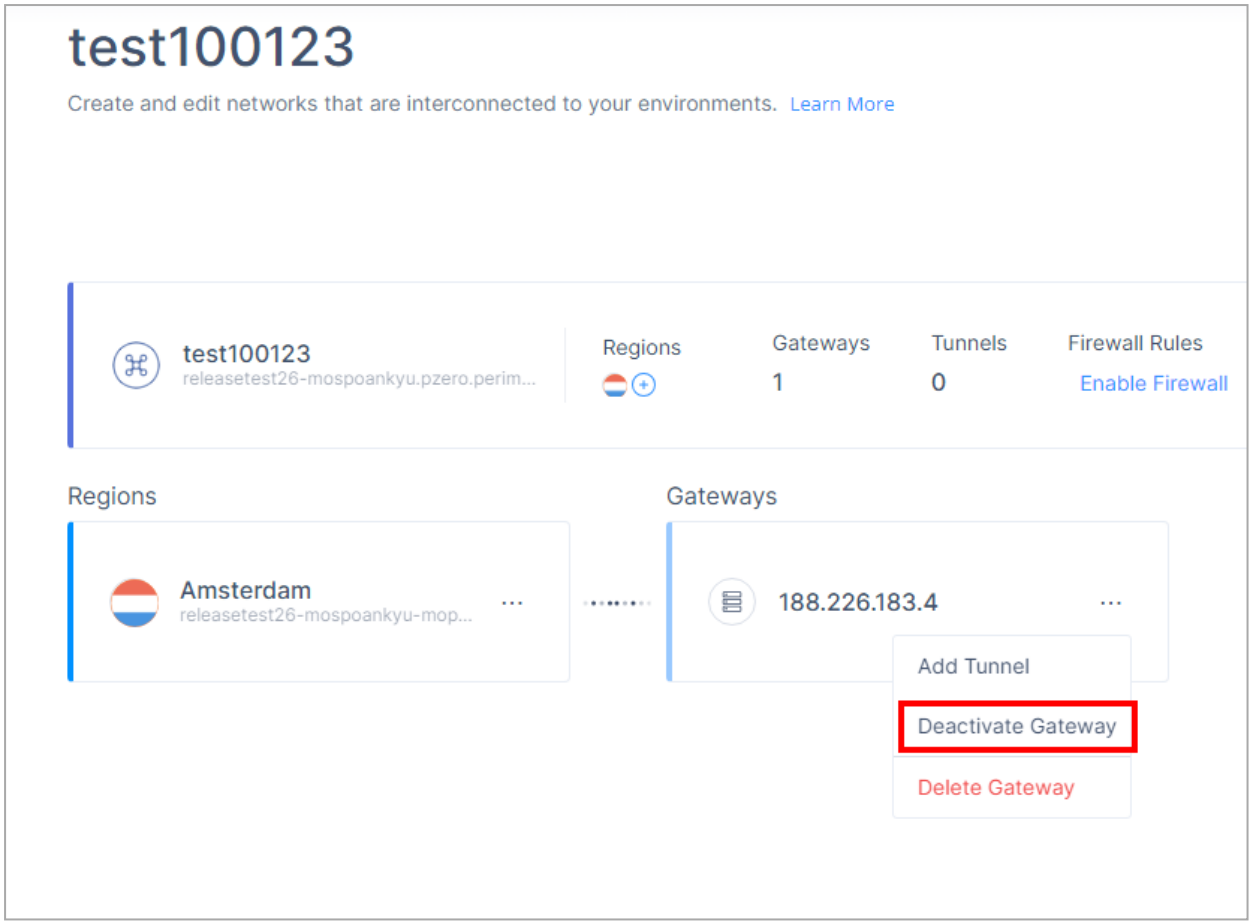
You can deactivate a gateway to block members from accessing the network resources (including Zero trust Applications) connected to the gateway. However, the gateway remains operational and configurable.

When you deactivate a gateway:

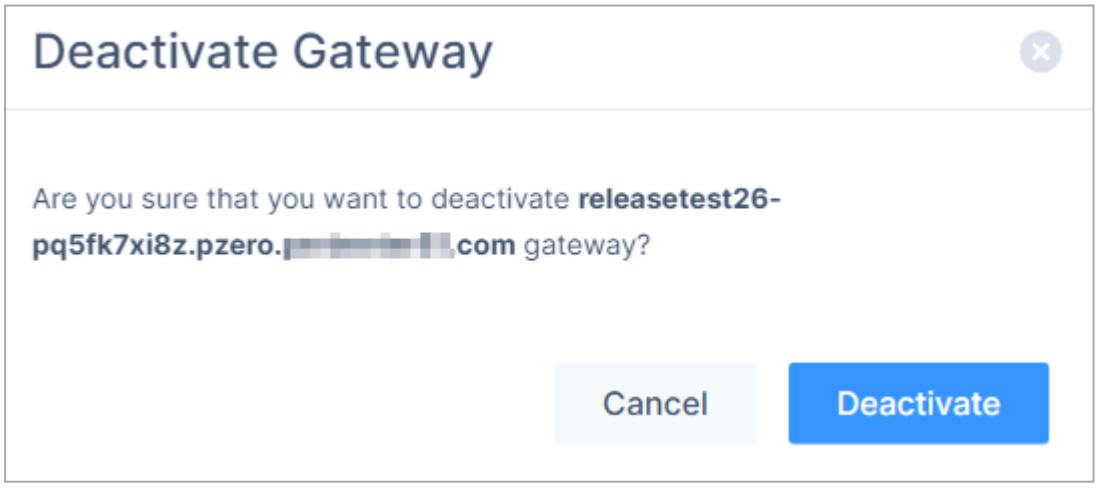
- Members and applications cannot connect to the gateway and are redirected to alternate gateways (if available).
- Members already connected to the gateway stay connected until they disconnect. After which, they are connected to an alternate gateway (if available).

To deactivate a gateway:

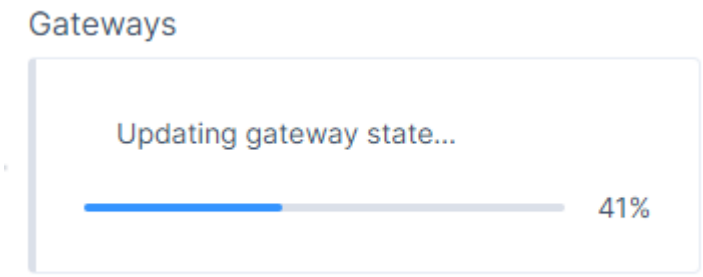
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· on your gateway and then click **Deactivate Gateway**.



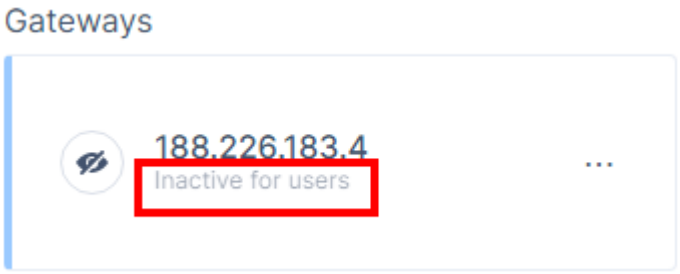
4. Click **Deactivate**.



The system shows the progress of the gateway status.



After the gateway is deactivated, it is marked as **Inactive for users**.



5. To re-activate your gateway, click ··· and then click **Activate Gateway**.

Enhanced Network

An Enhanced Network offers better scalability and easier management.

Benefits

- **Improved scalability:**
  - Support for more users per network
  - Higher throughput per tunnel
  - Up to **eight** parallel terminations for redundant IPsec tunnels. This offers better resiliency, load sharing, and overall scale compared to Standard Networks, which support only two parallel terminations.
- **Simplified management:**
  - Each region uses a single public IP address, regardless of scale. This removes the need to manage multiple public IP addresses.
  - Capacity in a region can be quickly adjusted by adding or removing **Scale Units**, the virtual equivalent of gateways in Standard Networks.
- **Enhanced user interface:**

  Improved network management interface, making it easier to create and maintain IPsec tunnels.
- **Early access to features:**

  New features and bug fixes are released first or exclusively to Enhanced Networks.

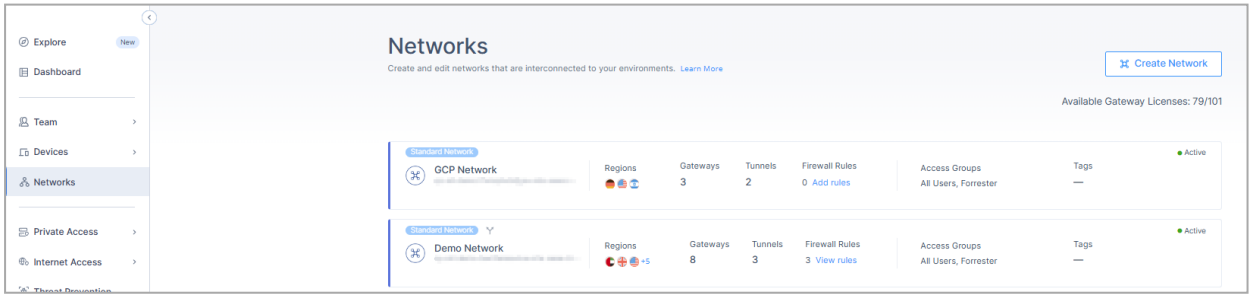
Supported Regions

Enhanced Networks are supported in these regions:

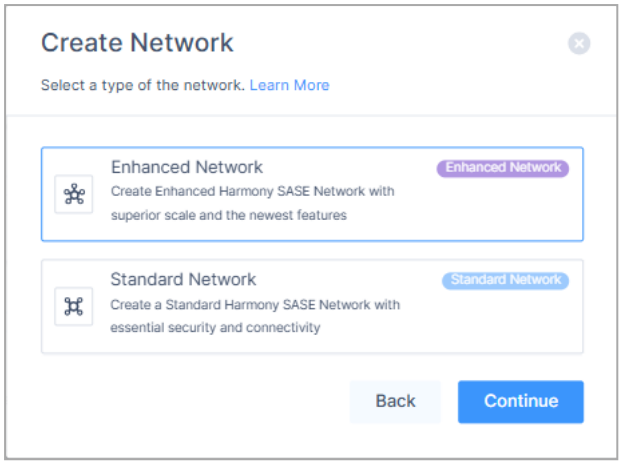
North America	EMEA	APAC	LATAM
■ Ashburn ■ Atlanta ■ Boston ■ Chicago 2 ■ Dallas ■ Dallas 2 ■ Denver ■ Honolulu ■ Los Angeles 1 ■ Los Angeles 2 ■ Miami ■ New Jersey ■ New York 1 ■ New York 3 ■ Seattle ■ Silicon Valley 1 ■ Silicon Valley 2 ■ Toronto 3 ■ Vancouver	■ Amsterdam 2 ■ Brussels 1 ■ Dubai ■ Frankfurt 1 ■ Frankfurt 4 ■ Israel 1 ■ Israel 2 ■ Istanbul ■ Johannesburg ■ London 1 ■ London 3 ■ London 4 ■ Madrid 2 ■ Manchester 1 ■ Manchester 2 ■ Paris ■ Stockholm 2 ■ Vienna ■ Warsaw 2 ■ Zurich	■ Auckland ■ Bangalore 2 ■ Hong Kong ■ Melbourne 1 ■ Mumbai 2 ■ New Delhi ■ Osaka ■ Perth, Australia ■ Seoul ■ Singapore 3 ■ Sydney 1 ■ Taipei ■ Tokyo 1	■ Mexico City ■ Santiago 1 ■ Sao Paulo 2

Creating an Enhanced Network

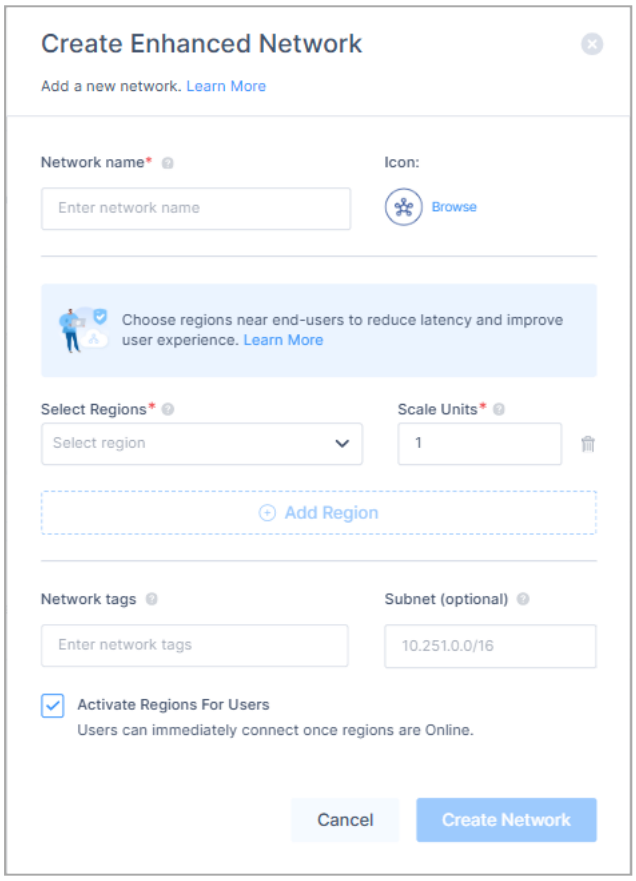
1. Access the SASE Administrator Portal and click **Networks**.
2. Click **Create Network**.



3. Select **Enhanced Network** and click **Continue**.



4. Enter the network details:



   a. **Network name**: Name for your network. For example, HQ, Finance, or Staging.

   b. Icon: By default the network icon is applied. If you do not choose one, click **Browse** to select an icon.

   c. **Region**: Region to deploy the SASE gateway.

   Note - Recommended to choose a region closest to your sites and members.

d. **Scale Units:** The number of gateways you want to deploy in the region.

Notes -

- Scale Unit is a virtual network component that allows defining the expected capacity in each network region.
- One Scale Unit's expected capacity is similar to the capacity of a single Standard Network Gateway.
- Each Scale Unit consumes one Gateway License.

e. (Optional) **Add Region**: To add more regions, click **Add Region** and repeat steps c and d.

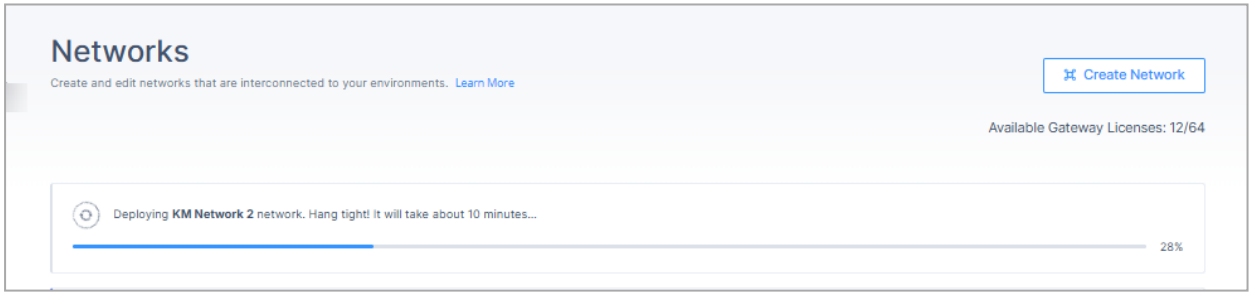
f. (Optional) **Network Tags**: Add tags to identify the purpose or team.

g. (Optional) **Subnet**: By default the network Subnet IP address is 10.255.0.0/16. For information on possible Subnet and bit masks, see sk182225.

Note - You cannot change the Subnet after creation. Ensure it does not overlap with SD-WAN device Subnets.

h. By default the **Activate Regions For Users** checkbox is selected. If you want to deactivate the region, disable it.

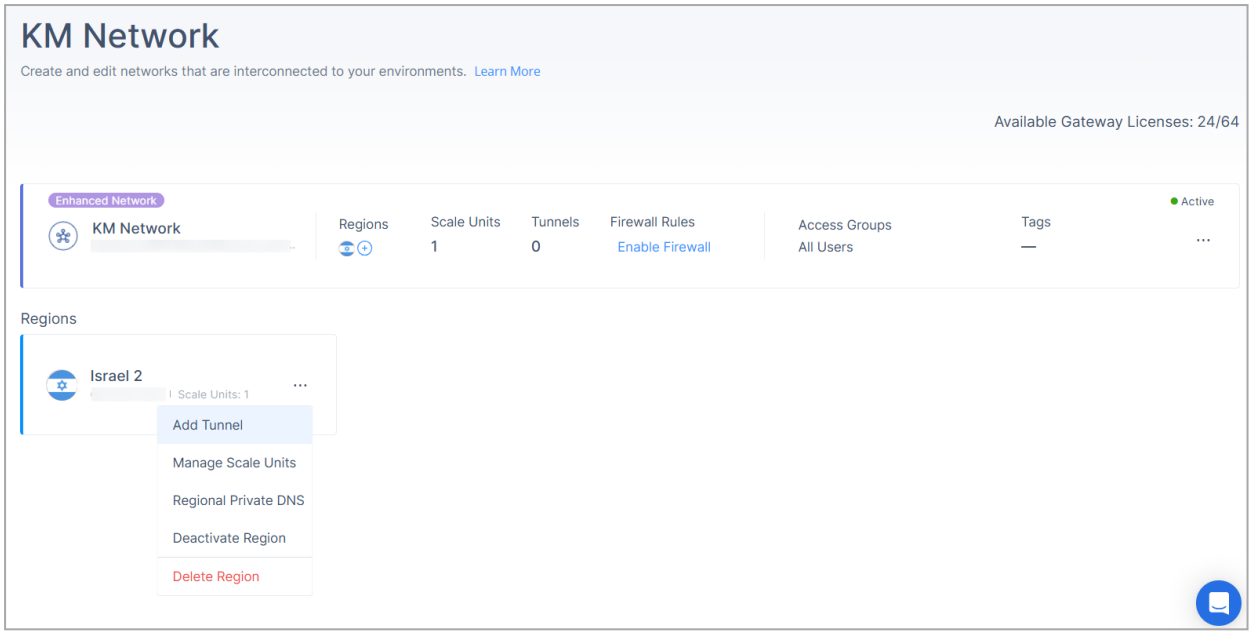
5. Click **Create Network**.



The system shows the progress of the network status on the Networks page. After the network is created, proceed with Adding a Tunnel.

Adding a Tunnel

1. In the **Networks** page, select your Enhanced Network.
2. For the region to which you want to add the tunnel, click ··· and click **Add Tunnel**.



3. Enter these details:

   a. **Tunnel Name**

   b. **Add Short Tunnel description**

   c. **Add Tunnel Estimated Maximum Bandwidth**

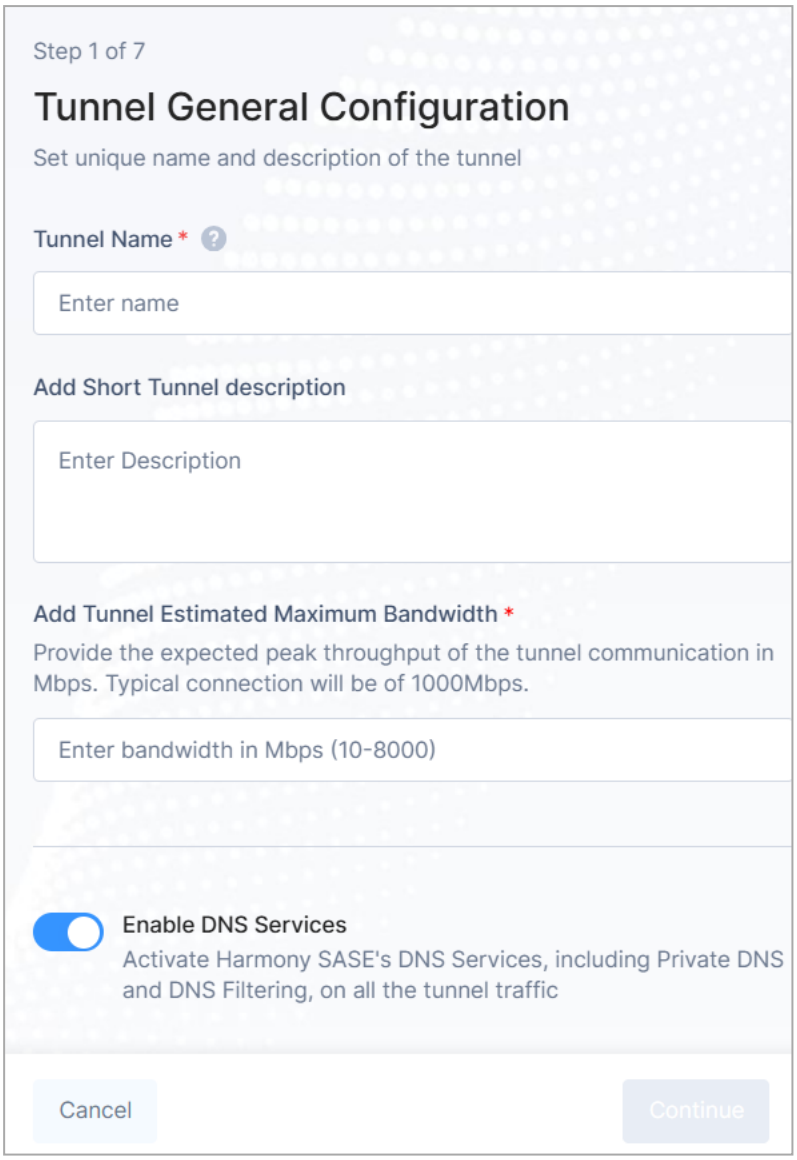
      Specify the expected peak throughput of the tunnel communication in Mbps.

      - **Range**: 10-8000 Mbps
      - **Typical connection**: 1000 Mbps

   d. By default the **Enable DNS Services** is enabled. Disable if you want to deactivate the DNS services.

      - Enable: Activates SASE's DNS services, including Private DNS and DNS Filtering on all tunnel traffic.

- Disable: No DNS services for Site to Site tunnel traffic.



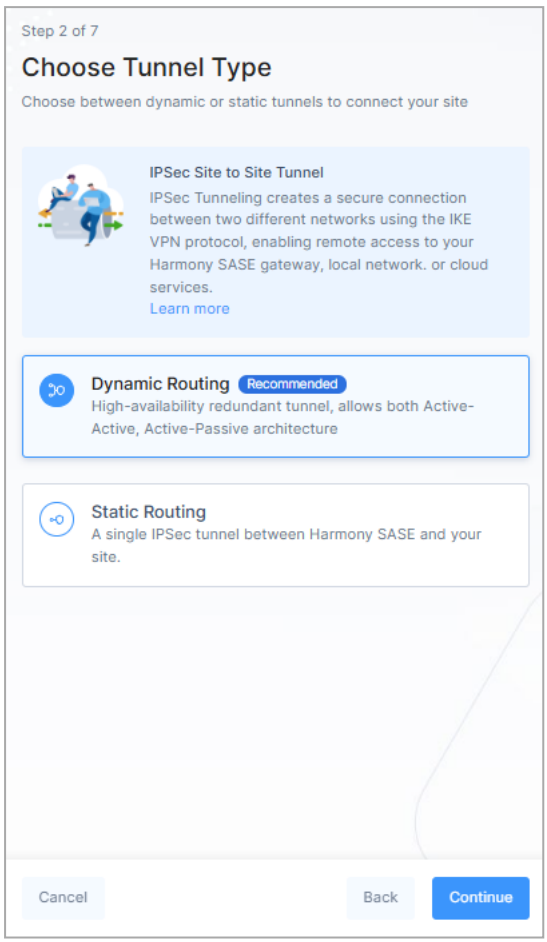
4. Click **Continue**.

   The **Choose Tunnel Type** window appears.

5. Select your preferred Tunnel Type.

Choosing Tunnel Type

1. In the **Choose Tunnel Type** window, select one of these:



   - **Dynamic Routing (Recommended)**:
     - High availability, active-active architecture.
     - Requires at least two regions.
     - Supports up to eight IPsec terminations for resiliency and load sharing.
   - **Static Routing**:

     Single IPsec tunnel between SASE and your site.

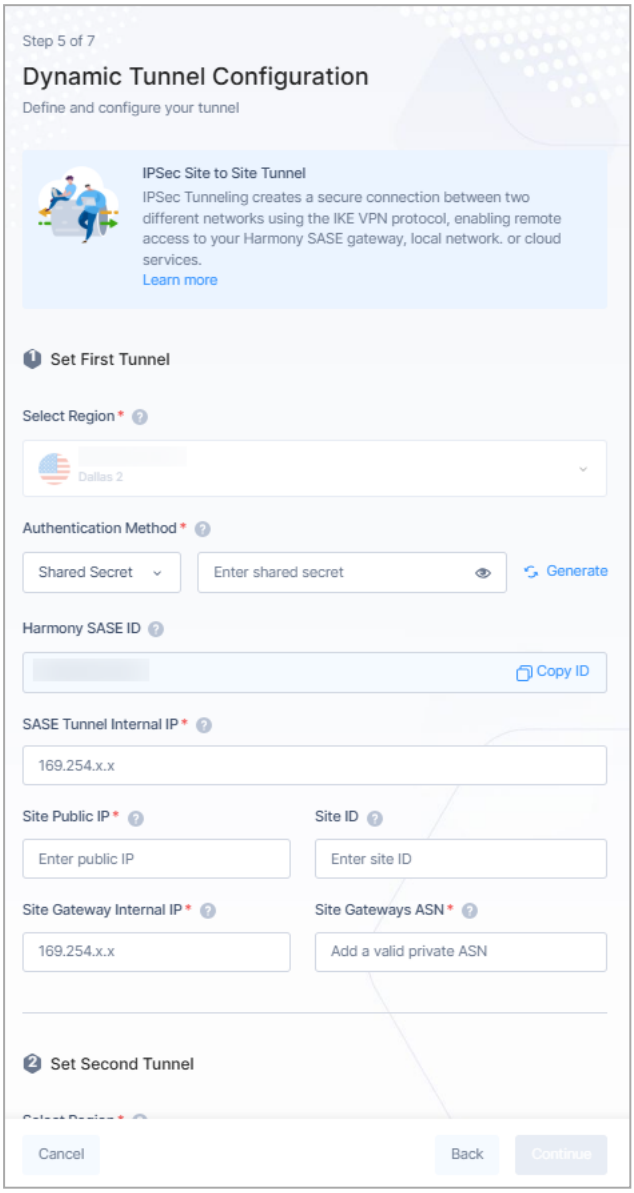
2. Click **Continue**.

   Refer:

   - *"Dynamic Routing" on the next page*
   - *"Static Routing" on page 184*

Dynamic Routing

1. In **Dynamic Tunnel Configuration** window, Select **Region** section:
   - For the first tunnel, the Region is selected by default.
   - For the second tunnel, select the Region from the list.



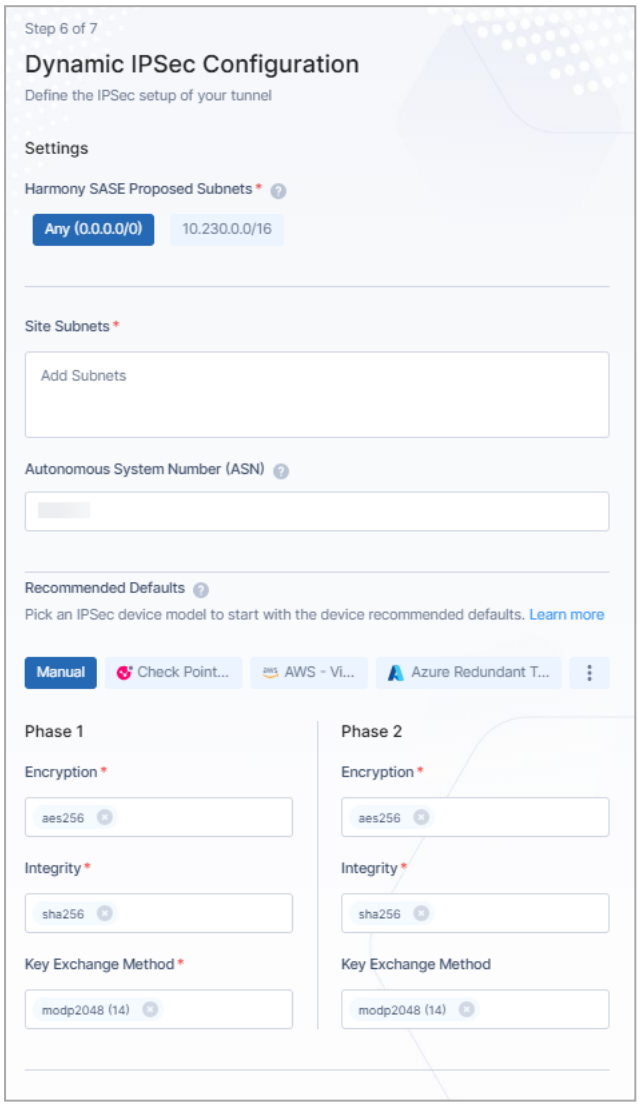
   You can add up to eight parallel IPsec terminations for resiliency and load sharing.
2. Make sure **Authentication Method** is **Shared Secret** and enter **Shared Secret** key.
3. Enter these details:
   a. **SASE Tunnel Internal IP**
   b. **Site Public IP**: Public IP address of the second end of the tunnel.

c. **Site ID**: In most cases, the ID of the tunnel is its public IP. However, it must be configured to the same value on both ends.

d. **Site Gateway Internal IP**

e. **Site Gateways ASN**

4. Click **Continue**.



The **IPsec Configuration** window appears.

5. By default **SASE Proposed Subnets** is **Any (0.0.0.0/0)**.

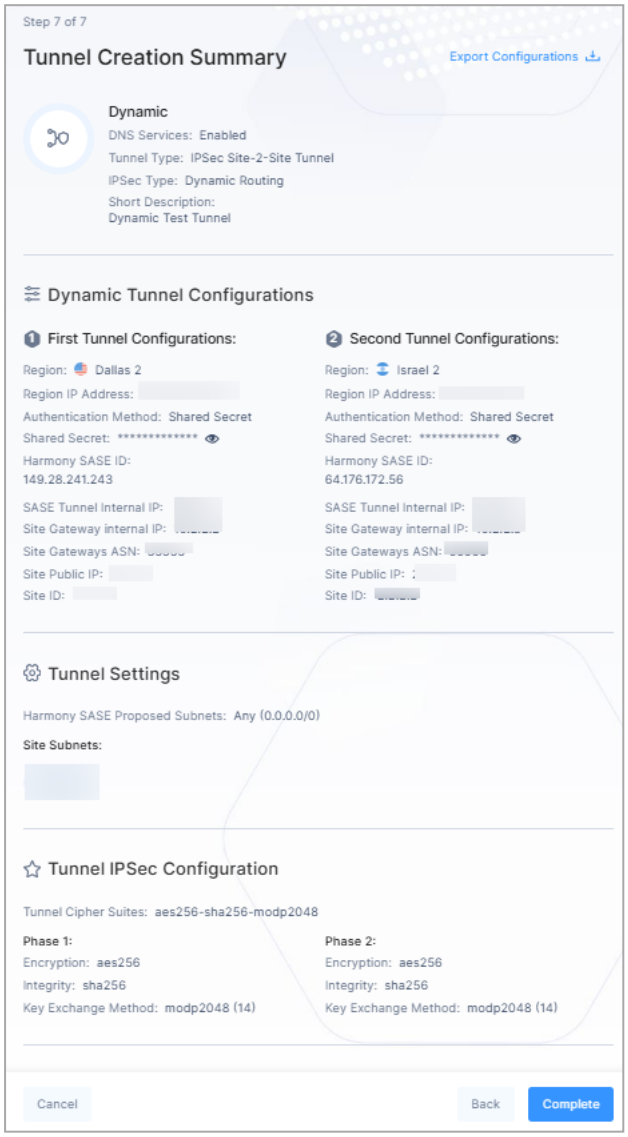
Note - The IPsec network selector should be configured to the same value at both ends of the tunnel.

6. Enter **Site Subnets**.

7. Enter **Autonomous System Number (ASN)**.

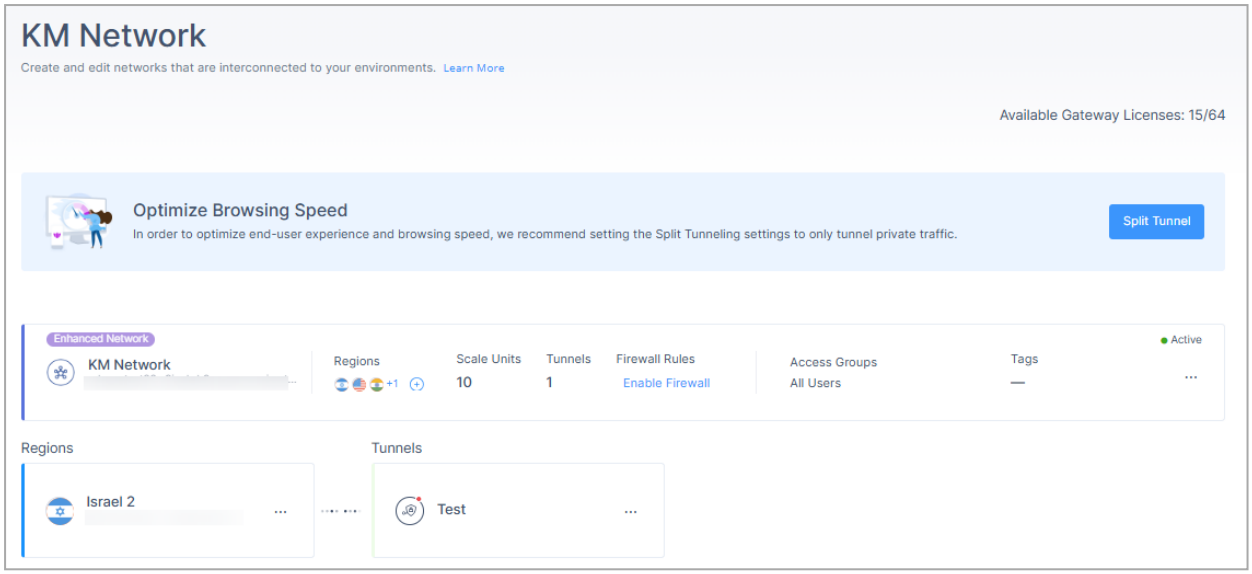
Note - The Autonomous System Number (ASN) is required for the Border Gateway Protocol (BGP).

8. In **Recommended Defaults**, the values are by default based on the service provider. For more details, refer Connect Cloud Resources and Connect On-Prem Resources.
9. Click **Continue**.



The **Tunnel Creation Summary** window appears. You can see all the configuration details.

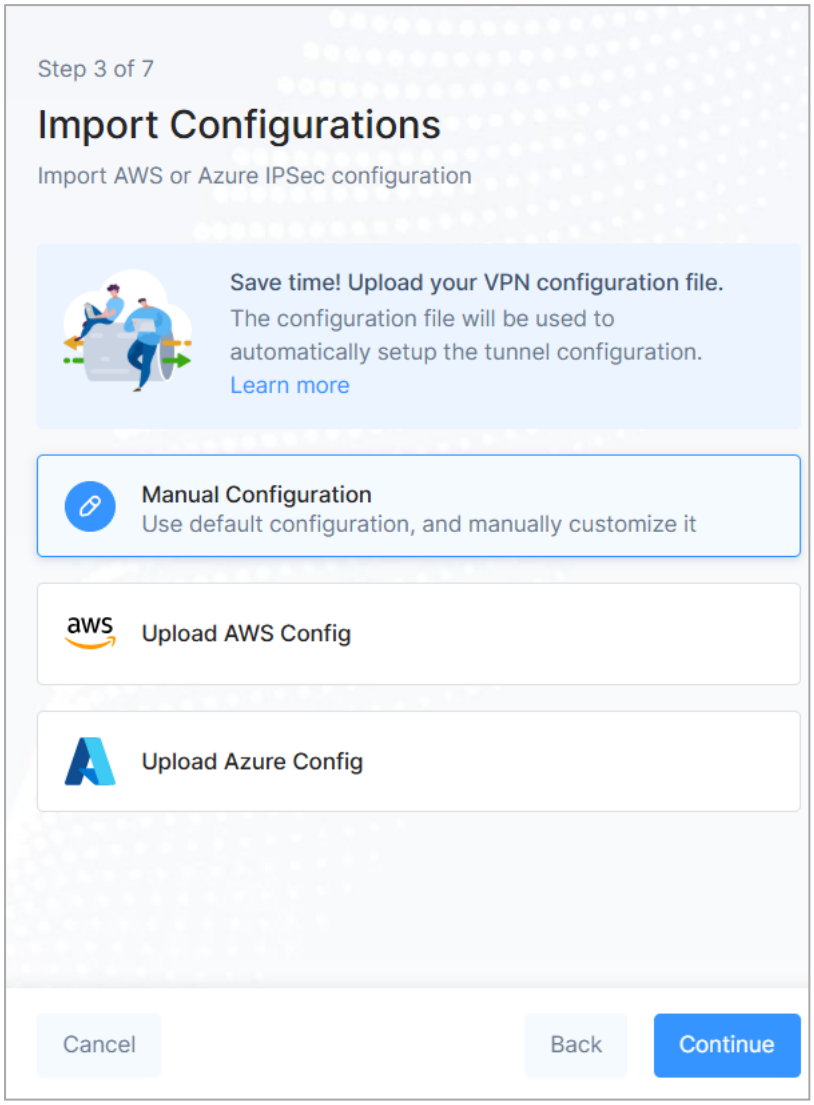
10. (Optional) Click **Export Configurations** to download configuration JSON file.
11. Click **Complete**.



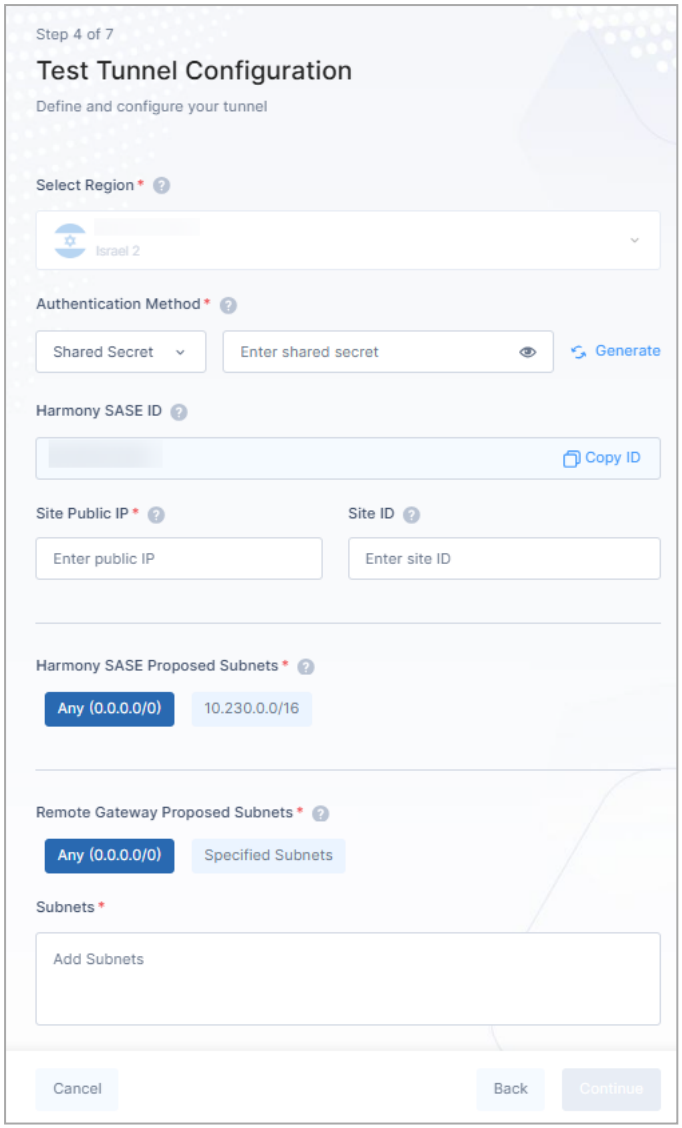
The tunnel is created and listed in your **Networks** page.

Static Routing

1. In the **Import Configurations** window, select **Manual Configuration** and click **Continue**.

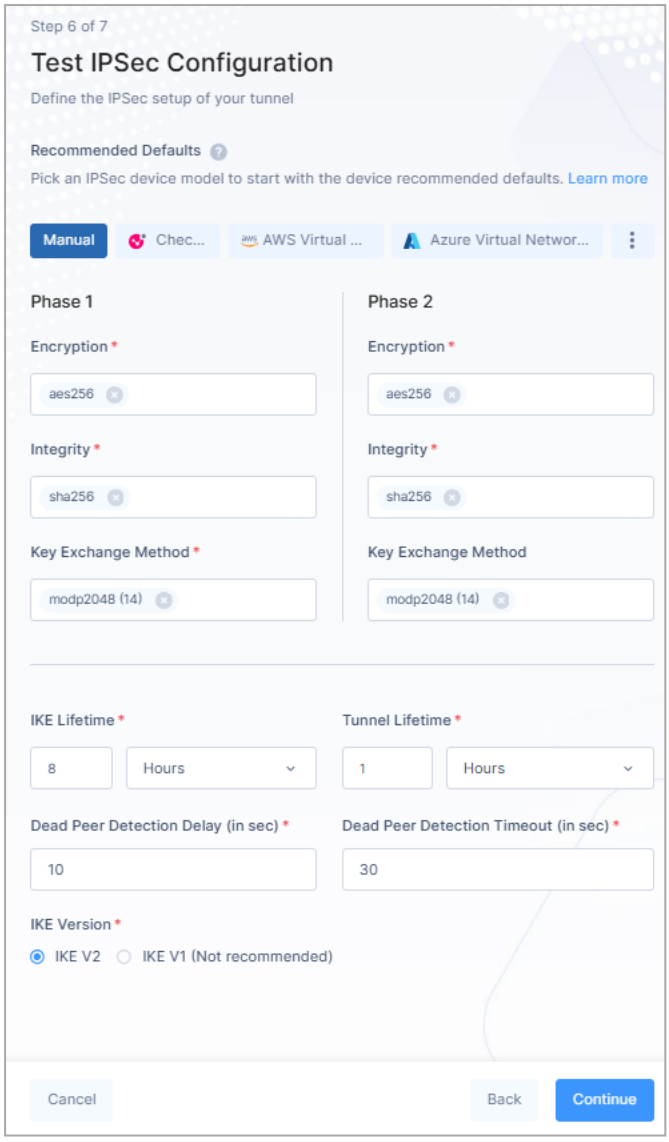


2. In the Tunnel Configuration window, the **Authentication Method** is selected as **Shared Secret** by default.

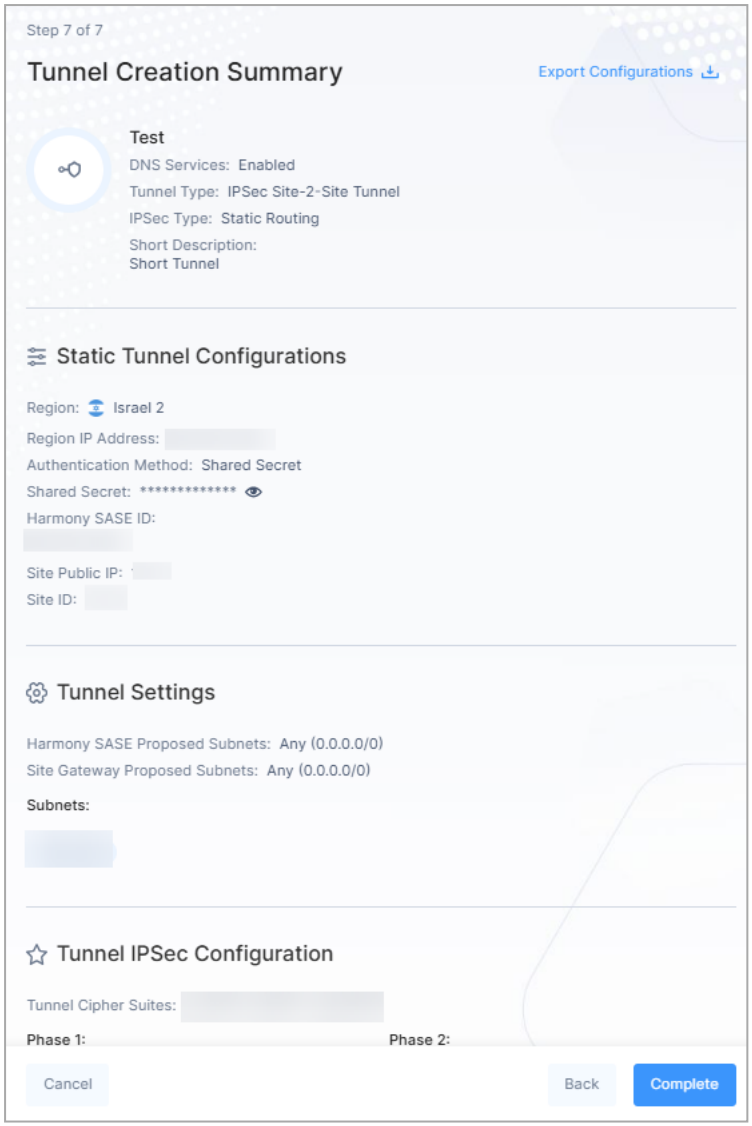


3. Click **Generate** to get the Shared Secret key.
4. Enter **Site Public IP**: It is the Public IP address of the second end of the tunnel.
5. (Optional) **Site ID**: In most cases, the ID of the tunnel is its public IP. However, it must be configured to the same value on both ends.
6. By default **SASE Proposed Subnets** is selected as **Any (0.0.0.0/0)**.
7. By default **Remote Gateway Proposed Subnets** is **Any (0.0.0.0/0)**.

   Note - It is not recommended to use Specified Subnets or Policy Based Routing. Consider using **Any (0.0.0.0/0)**, Route Based instead.
8. Enter **Subnets**.
9. Click **Continue**.

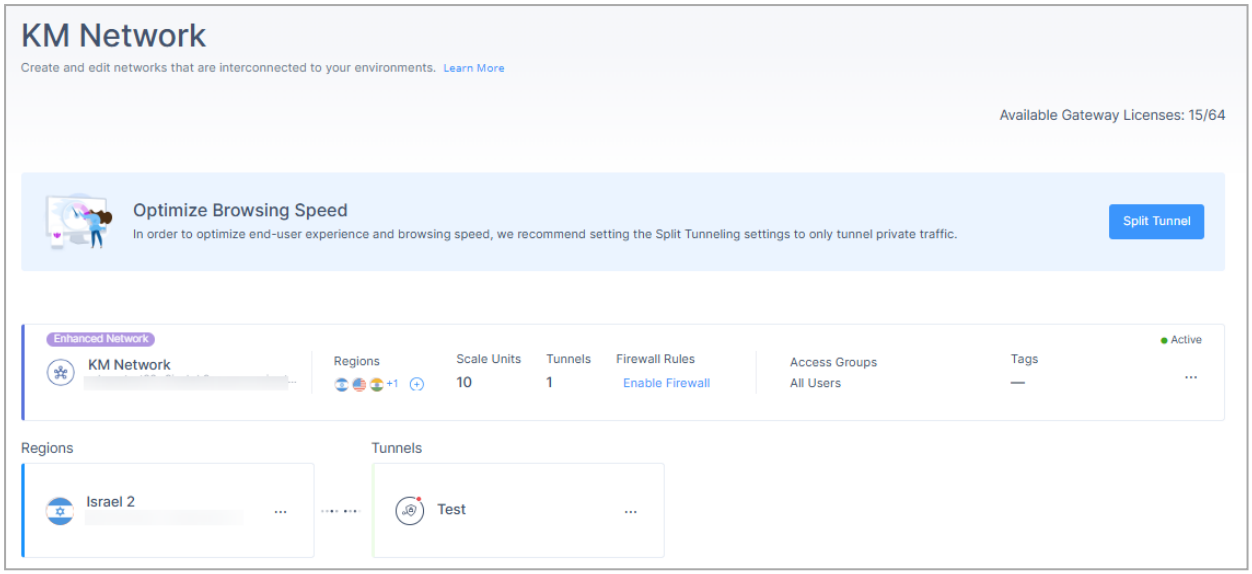


10. In **IPsec Configuration** window, the values are by default based on the service provider. For more details, refer Connect Cloud Resources and Connect On-Prem Resources.
11. Click **Continue**.



The **Tunnel Creation Summary** window appears. You can see all the configuration details.

12. (Optional) Click **Export Configurations** to download configuration JSON file.
13. Click **Complete**.

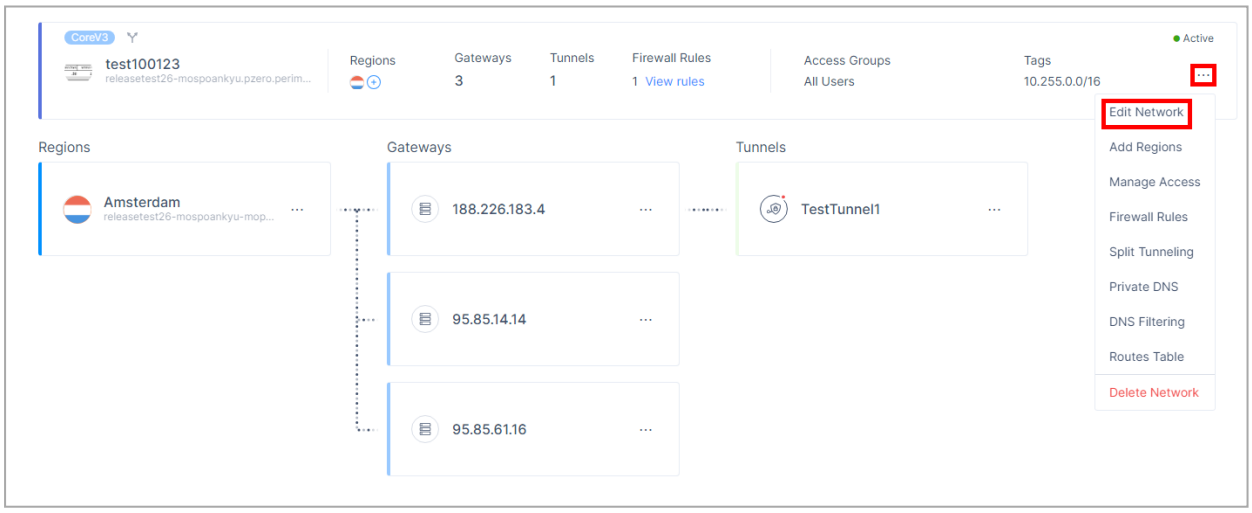


The tunnel is created and listed in your Networks page.

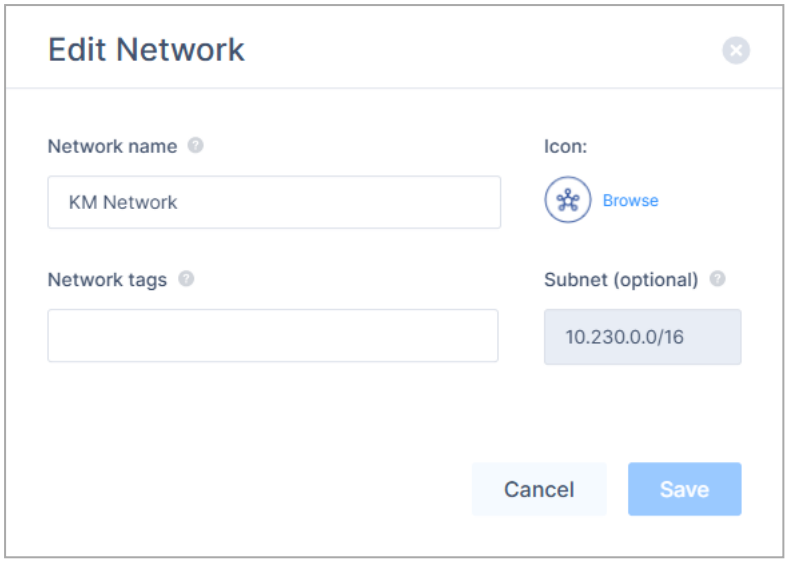
Managing a Network

Editing a Network

1. Access the SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Edit Network**.



The Edit Network window appears.

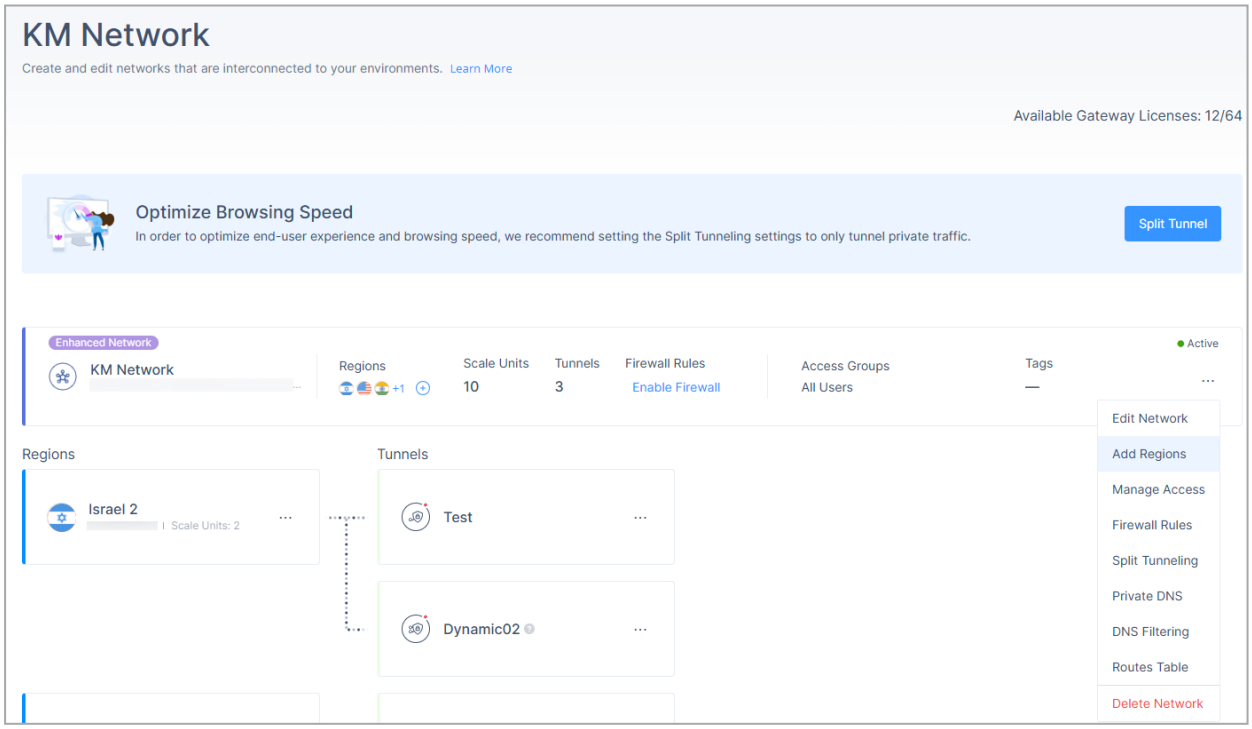


4. Make the required changes (**Network name**, **Network tags**, **Icon**) and click **Save**.

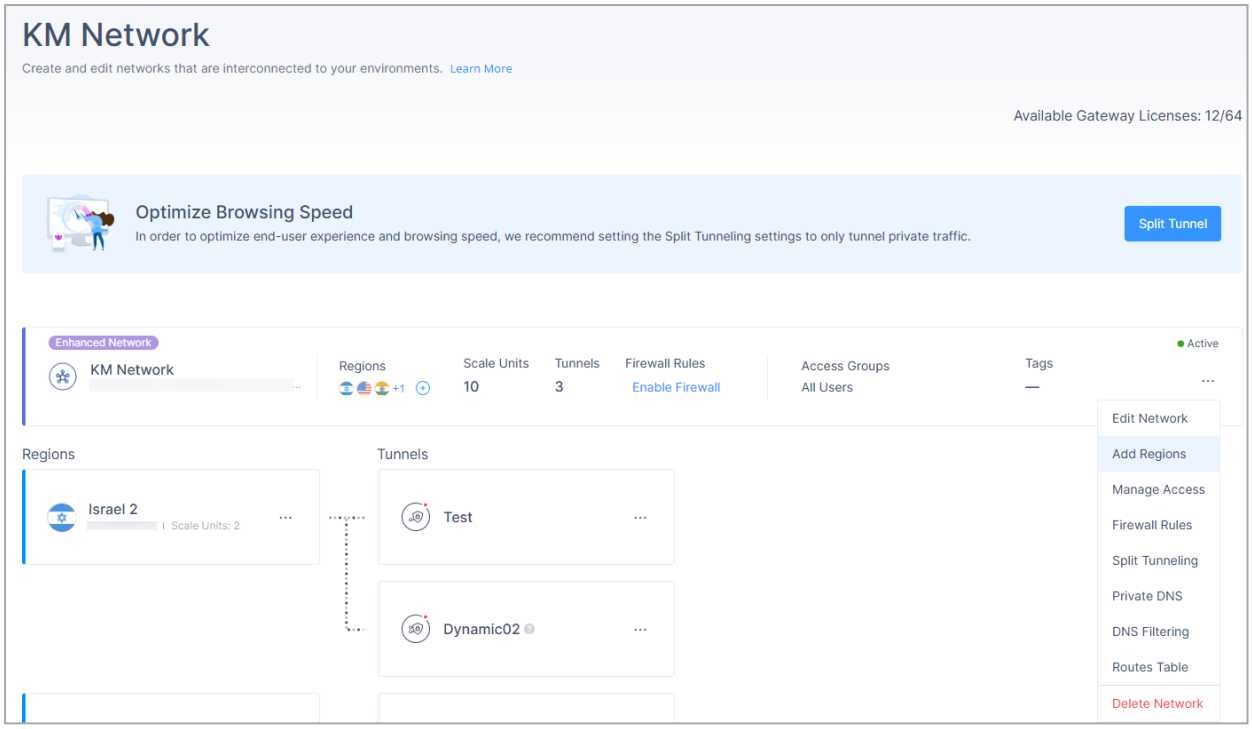
   Note - You cannot change the Subnet after network creation.

Adding Regions

1. Access the SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Edit Network**.



4. The **Add Region** window appears.



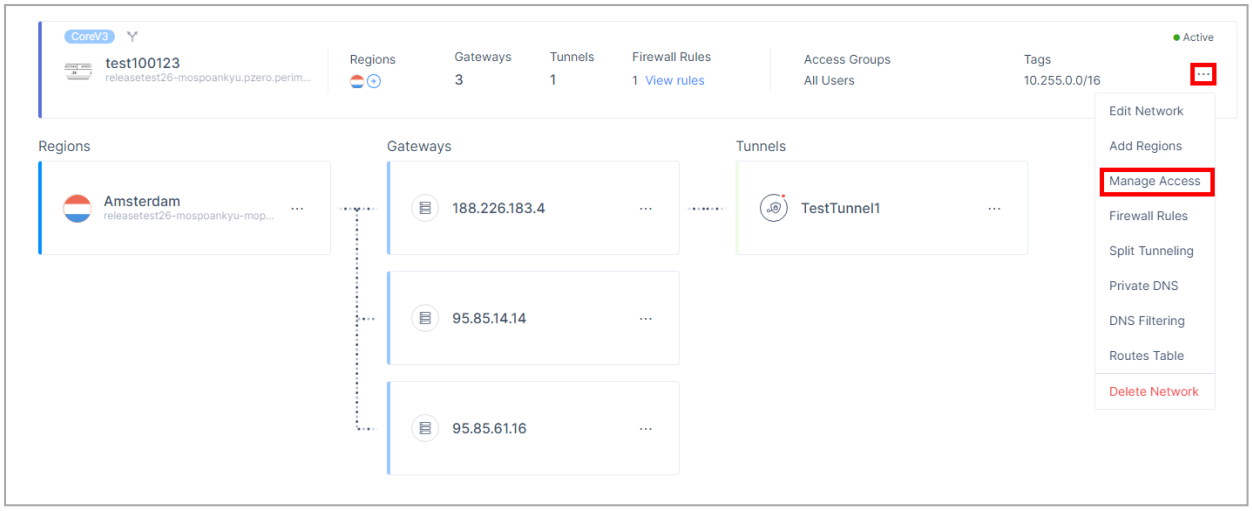
5. From the **Region** list, select the region to deploy the SASE gateway.
6. In the **Scale Units** field, enter the number of gateways you want to deploy in the region.
7. To add more regions, click **Add Region** and repeat steps 4 and 5.
8. To activate the region for users, select the **Activate Regions For Users** checkbox.
9. Click **Add Region**.

Managing Access

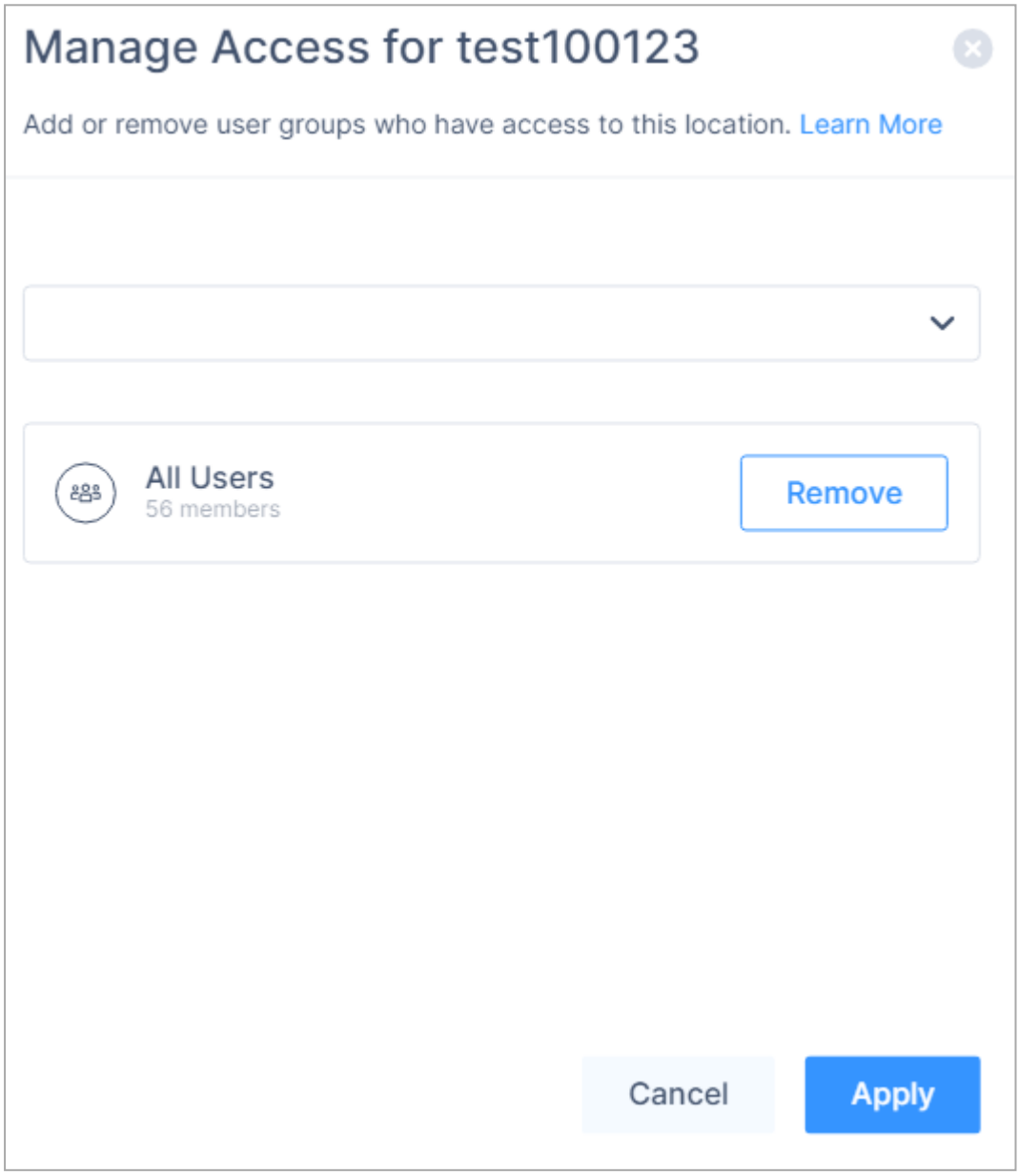
Manage Access allows you to select the member groups who can access the network.

To manage access to a network:

1. Access the SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ... and then click **Manage Access**.



The **Manage Access** window appears.



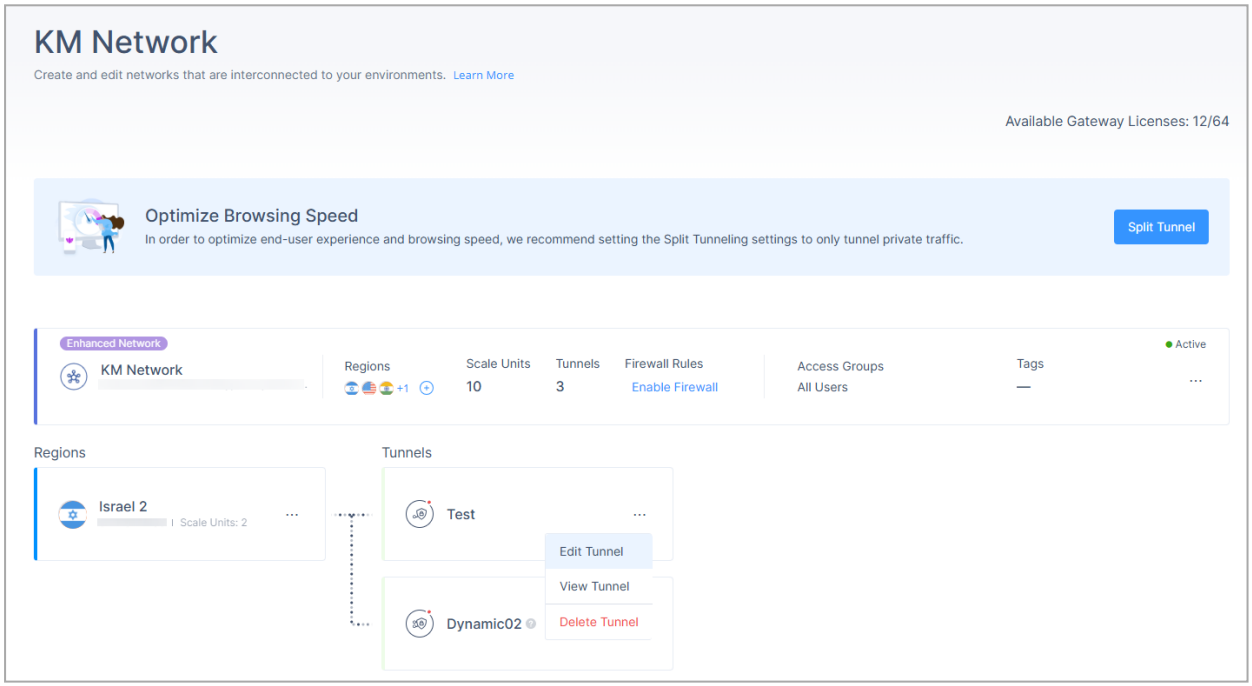
4. From the list, select the member groups who can access the network.
5. To remove a member group, click **Remove**.
6. Click **Apply**.

Managing Tunnels

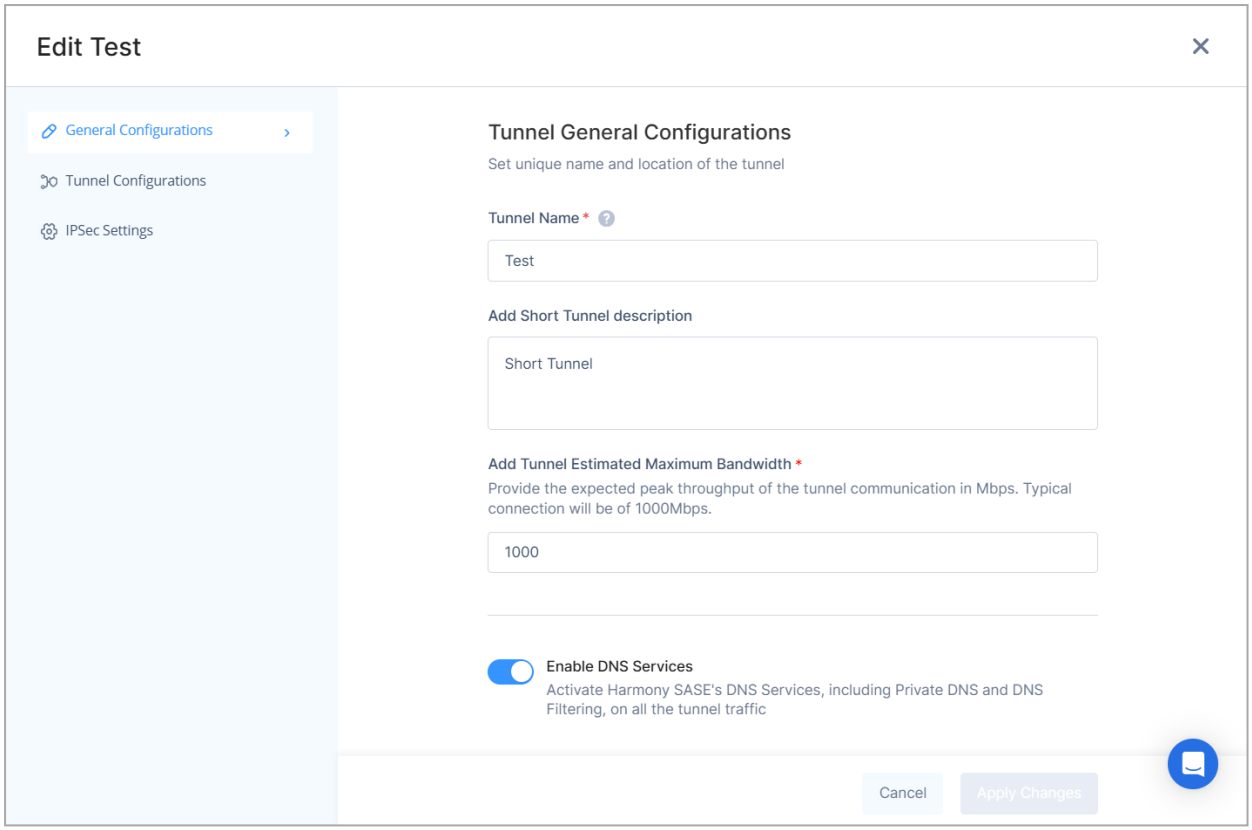
In Enhanced Networks, all tunnel operations happen at the Region level (not on gateways).

Editing a Tunnel

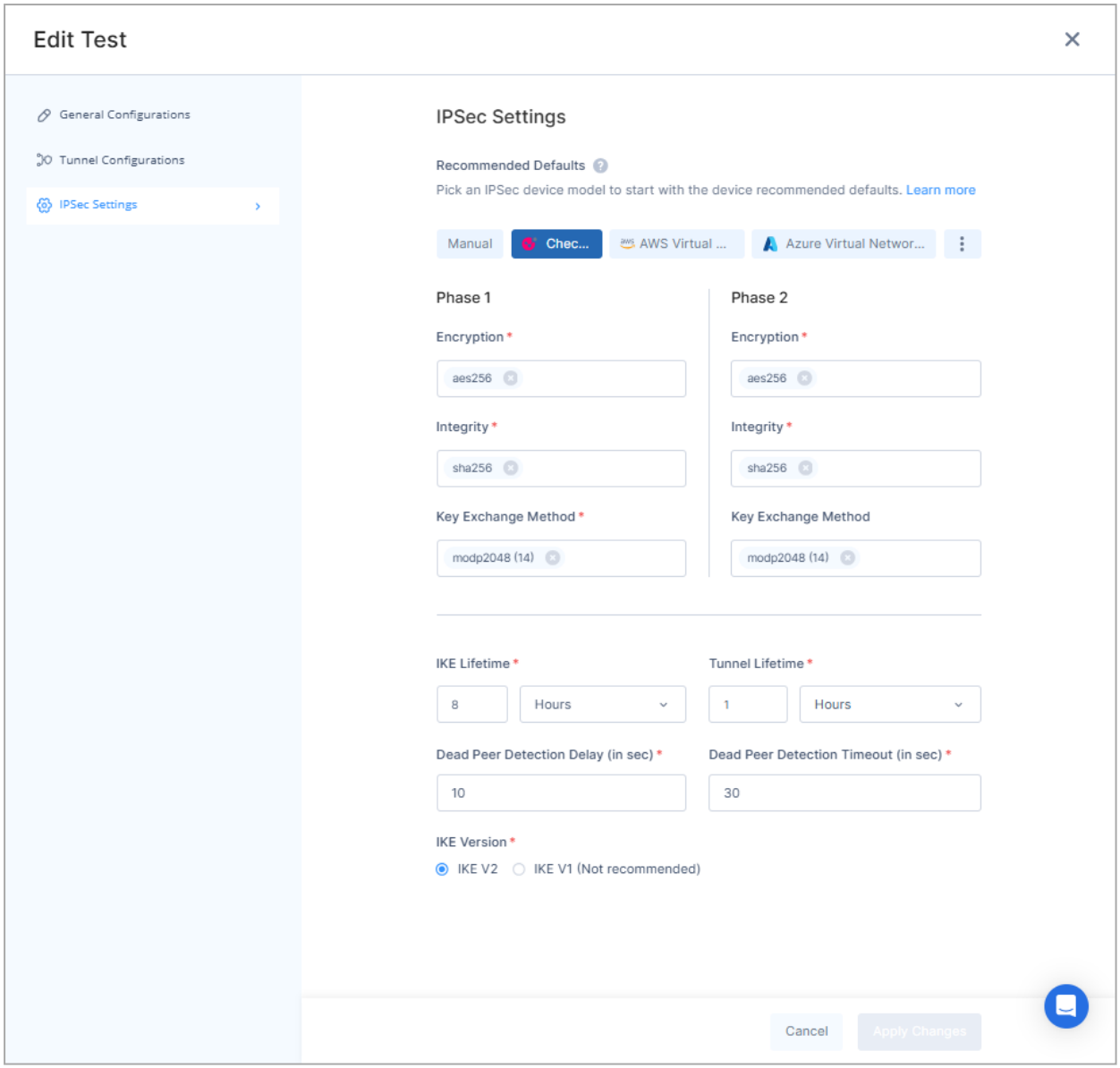
1. In the **Networks** page, select your Enhanced Network.
2. Click ··· and click **Edit Tunnel**.



The **Edit Tunnel** pop up appears.



3. Make the required changes and click **Apply Changes**.



Notes -

For Tunnel Configurations:

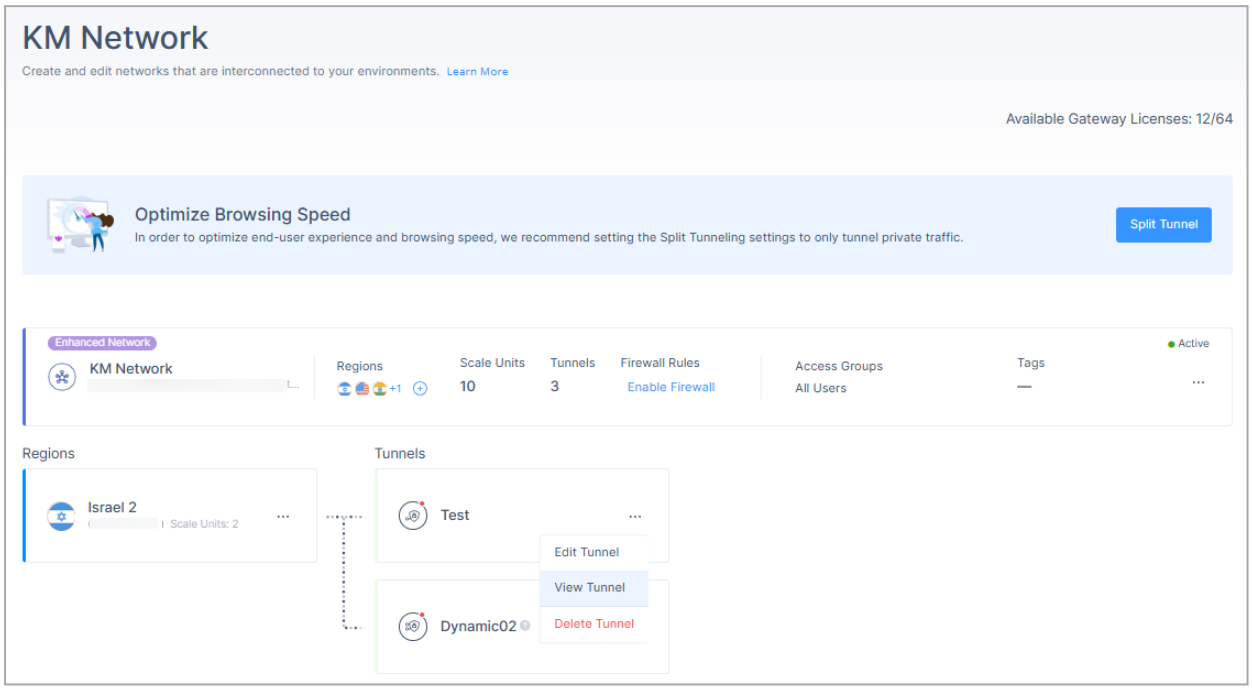
- You cannot add and delete terminations in the same edit session.
- You cannot move a termination to a different region, delete or re-add it.
- Ensure the region has enough Scale Units before adding terminations.

For IPsec settings:

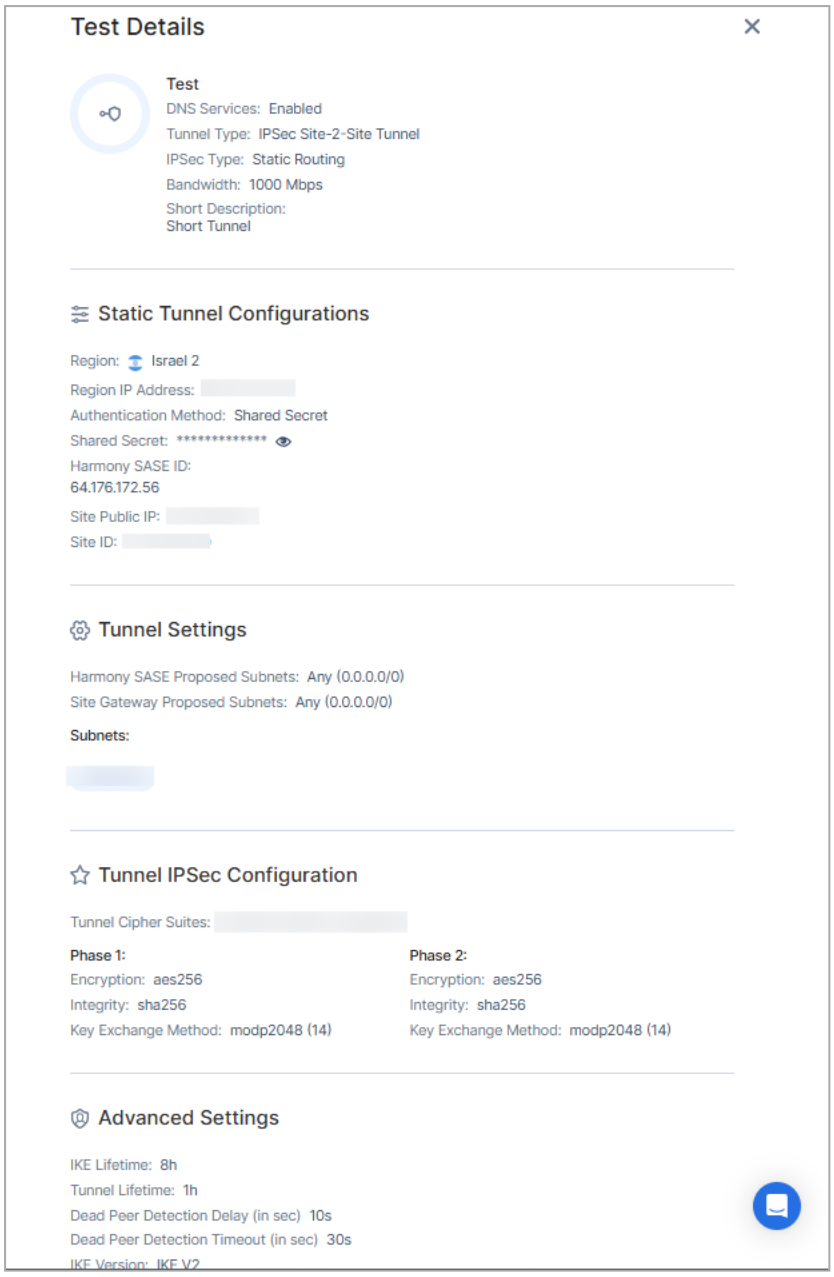
- Use vendor recommendations unless you have a specific compliance requirement.
- Incorrect IPsec settings can cause tunnel failure, validate changes before applying.

Viewing Tunnel Details

1. In the Networks page, select your Enhanced Network.
2. Click ··· and click **View Tunnel**.

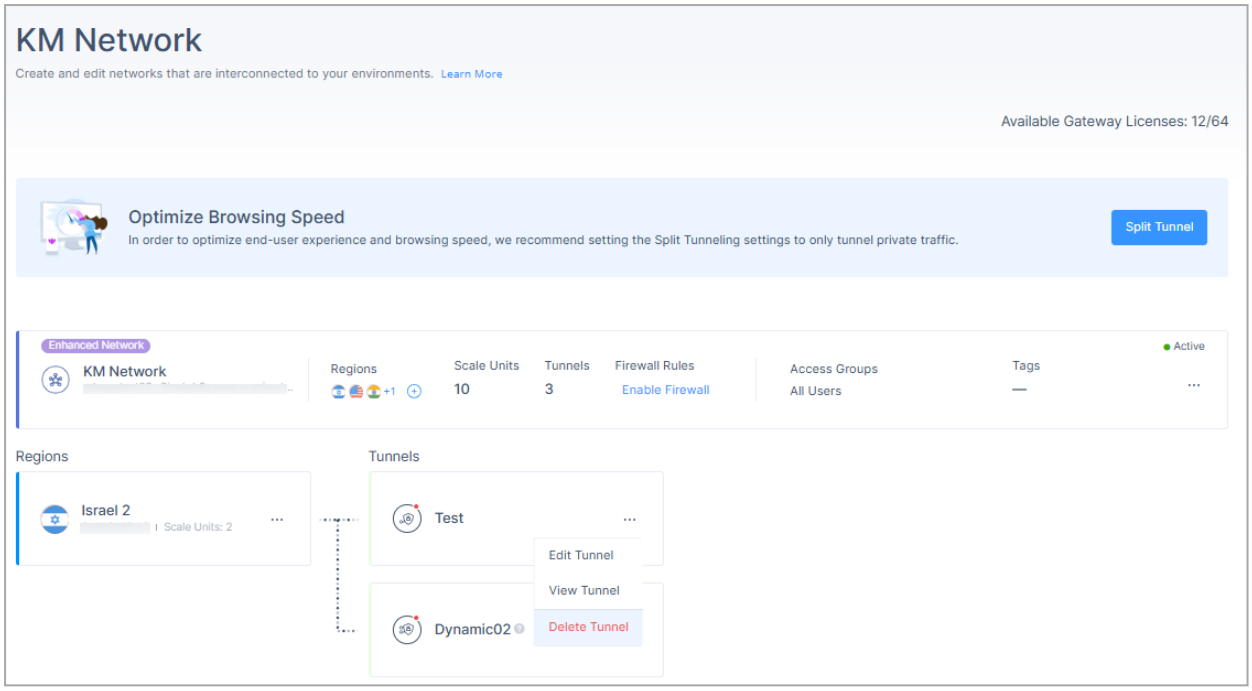


The Tunnel Details pop up appears.

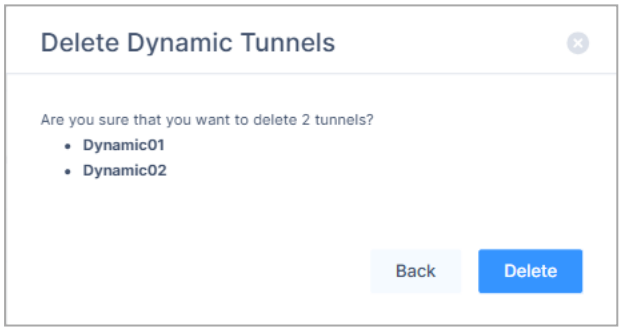


Deleting a Tunnel

1. In the **Networks** page, select your Enhanced Network.
2. Click ... and click **Delete Tunnel**.



The **Delete Dynamic Tunnel** pop up appears.



3. Click **Delete**.

Note -

- Make sure no active traffic depends on the tunnel before you delete it.
- You can delete individual terminations or the entire dynamic tunnel.
- Once you start a delete operation, you cannot add new terminations in the same session.

Adding a Tunnel

Check Point SASE supports three types of tunnels:

- *"IPsec Site-to-Site VPN Tunnel" on page 199*
- *"WireGuard Connector Tunnel" on page 205*
- *"OpenVPN Tunnel" on page 214*

IPsec Site-to-Site VPN Tunnel

Prerequisites

Make sure your edge device (firewall or router) supports IPsec point to point tunnel using IKEv1 or IKEv2 protocols.

IPSec Handshake

The IPSec Site-2-Site VPN tunnel employs a two-phase handshake.

Phase I (IKE or Gateway)

This is the security association responsible for the external IP communication between the Check Point SASE network and the remote IP through the port 500/4500. The following information is required for Phase I. This information must match in both Check Point SASE and the remote side of the tunnel:

- **Shared Secret**
- **Public IP**
- **Remote ID**
- **IKE Version**
- **IKE Lifetime**
- **Encryption (Phase 1)**
- **Integrity (Phase 1)**
- **Key Exchange Method**

Phase II (ESP or Tunnel):

This is the security association responsible for the internal LAN range or subnet handshake after establishing the IKE SA .

The following information is required for Phase II. This information must match in both Check Point SASE and the remote side of the tunnel:

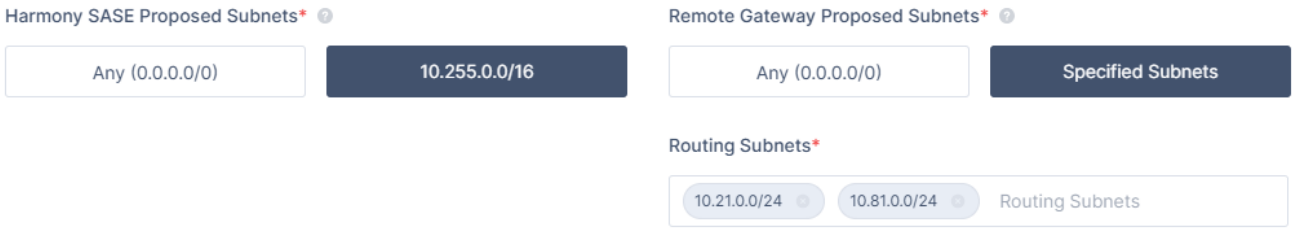
- **Check Point SASE Gateway Proposal Subnets**
- **Remote Gateway Proposal Subnets**
- **Tunnel Lifetime**
- **Dead Peer Detection (DPD)**
- **Encryption (Phase 2)**

- **Integrity (Phase 2)**
- **Key Exchange Method**

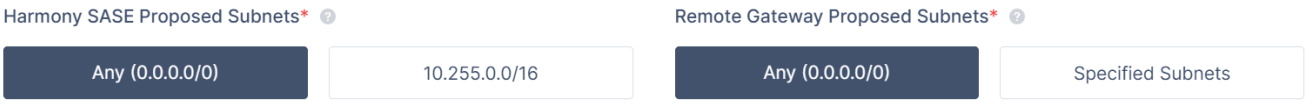
Policy-Based and Route-Based IPSec Connection

Policy-based connection is easier to set up but is more vulnerable to IPSec tunnel value mismatch.

Depending on your device, a single missing subnet may cause the Phase 2 negotiation to fail.



Route-based connection is also known as a Tunnel Interface or VTI.



It is a more modern and stable method of IPSec tunneling. Once established, it uses one subnet (0.0.0.0/0) for the handshake, thereby reducing the chances of an error during renegotiation.

Supported Integrations

On-premises SD-WAN		Cloud-based SD-WAN
Firewall	Router	
■ *"Barracuda Firewall" on page 258* ■ *"Check Point Firewall" on page 268* ■ *"Cisco Firepower" on page 279* ■ *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 300* ■ *"Configuring Check Point Redundant IPsec Tunnel" on page 326* ■ *"Cisco ASA Firewall" on page 382* ■ *"Cisco Meraki Router" on page 506* ■ *"FortiGate Next Generation Firewall" on page 416* ■ *"Juniper Networks ScreenOS Firewall" on page 420* ■ *"Juniper (JunOS) SRX Firewall" on page 426* ■ *"Palo Alto Firewall" on page 439* ■ *"Palo Alto Redundant Tunnel" on page 446* ■ *"pfSense Firewall" on page 466* ■ *"SonicWall Firewall" on page 472* ■ *"Sophos XG Firewall" on page 482* ■ *"UniFi USG Firewall" on page 488* ■ *"WatchGuard Firewall" on page 494* ■ *"Zyxel USG Firewall" on page 500*	■ *"Cisco Meraki Router" on page 506* ■ *"D-Link DSR Series Router" on page 509* ■ *"DrayTek Vigor2862 Router" on page 516* ■ *"DrayTek Vigor3900 Router" on page 519* ■ *"EdgeMax Router" on page 526* ■ *"Linksys Router" on page 528* ■ *"Netgear BR500 Router" on page 532*	**Single Tunnel** ■ *"AWS Virtual Gateway" on page 555* ■ *"AWS Transit Gateway" on page 575* ■ *"Google Cloud Platform" on page 687* ■ *"Azure Virtual Network Gateway" on page 623* **Redundant Tunnels** ■ *"AWS Redundant Tunnels - Virtual Private Gateway" on page 592* ■ *"AWS Redundant Tunnels - Transit Gateway" on page 606* ■ *"Google Cloud Platform (GCP) Redundant Tunnels" on page 700* ■ *"Azure Virtual Network Gateway Redundant Tunnels" on page 649* ■ *"Azure Virtual WAN Redundant Tunnels" on page 667* **Other Cloud Options** ■ *"Alibaba Cloud" on page 546* ■ *"Heroku Enterprise" on page 722* ■ *"IBM Cloud" on page 723*

High-Level Procedure

1. Make sure you have the required prerequisites.
2. Configure the tunnel in the SASE Administrator Portal.

3. Configure the required Firewall / Router / Cloud Management Portal:

On-premises		Cloud-based Resource
Firewall	Router	
■ *"Barracuda Firewall" on page 258* ■ *"Check Point Firewall" on page 268* ■ *"Cisco Firepower" on page 279* ■ *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 300* ■ *"Configuring Check Point Redundant IPsec Tunnel" on page 326* ■ *"Cisco ASA Firewall" on page 382* ■ *"Cisco Meraki Router" on page 506* ■ *"FortiGate Next Generation Firewall" on page 416* ■ *"Juniper Networks ScreenOS Firewall" on page 420* ■ *"Juniper (JunOS) SRX Firewall" on page 426* ■ *"Palo Alto Firewall" on page 439* ■ *"Palo Alto Redundant Tunnel" on page 446* ■ *"pfSense Firewall" on page 466* ■ *"SonicWall Firewall" on page 472* ■ *"Sophos XG Firewall" on page 482* ■ *"UniFi USG Firewall" on page 488* ■ *"WatchGuard Firewall" on page 494* ■ *"Zyxel USG Firewall" on page 500*	■ *"Cisco Meraki Router" on page 506* ■ *"D-Link DSR Series Router" on page 509* ■ *"DrayTek Vigor2862 Router" on page 516* ■ *"DrayTek Vigor3900 Router" on page 519* ■ *"EdgeMax Router" on page 526* ■ *"Linksys Router" on page 528* ■ *"Netgear BR500 Router" on page 532*	**Single Tunnel** ■ *"AWS Virtual Gateway" on page 555* ■ *"AWS Transit Gateway" on page 575* ■ *"Google Cloud Platform" on page 687* ■ *"Azure Virtual Network Gateway" on page 623* **Redundant Tunnels** ■ *"AWS Redundant Tunnels - Virtual Private Gateway" on page 592* ■ *"AWS Redundant Tunnels - Transit Gateway" on page 606* ■ *"Google Cloud Platform (GCP) Redundant Tunnels" on page 700* ■ *"Azure Virtual Network Gateway Redundant Tunnels" on page 649* ■ *"Azure Virtual WAN Redundant Tunnels" on page 667* **Other Cloud Options** ■ *"Alibaba Cloud" on page 546* ■ *"Heroku Enterprise" on page 722* ■ *"IBM Cloud" on page 723*

4. Verify the setup.

WireGuard Connector Tunnel

Prerequisites

A Linux machine with these specifications:

- **Kernel**: Any of these packages installed:
  - Ubuntu (Server/Desktop) 22.04 LTS or higher
  - CentOS 9 or CentOS 10
  - RHEL 9 or RHEL 10
- **Packages installed**:
  - Ubuntu - curl; dig; software-properties-common
  - CentOS - curl, bind-utils
  - RHEL9 or RHEL 10 iptables-nft-services should be installed

    1. To verify that the *iptables* service is enabled and active, run:

       ```
       systemctl status iptables
       ```

       Output:

       ```
       [root@ip-172-31-30-78 ~]# systemctl status iptables
       ● iptables.service - IPv4 firewall with iptables
            Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; preset: disabled)
            Active: active (exited) since Tue 2025-09-09 06:28:27 UTC; 3s ago
           Process: 42295 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
          Main PID: 42295 (code=exited, status=0/SUCCESS)
               CPU: 15ms
       ```

    2. To activate *iptables*, if not enabled and active, run:

       ```
       systemctl enable iptables
       systemctl start iptables
       ```

- 20 GB free disk space
- 2 GB RAM
- Static internal IP address
- Network adapter that supports bridge connection

  Note - For Linux deployed on a Windows host, enable virtualization on Windows BIOS.

For High Availability (Optional)

To configure High Availability, you need:

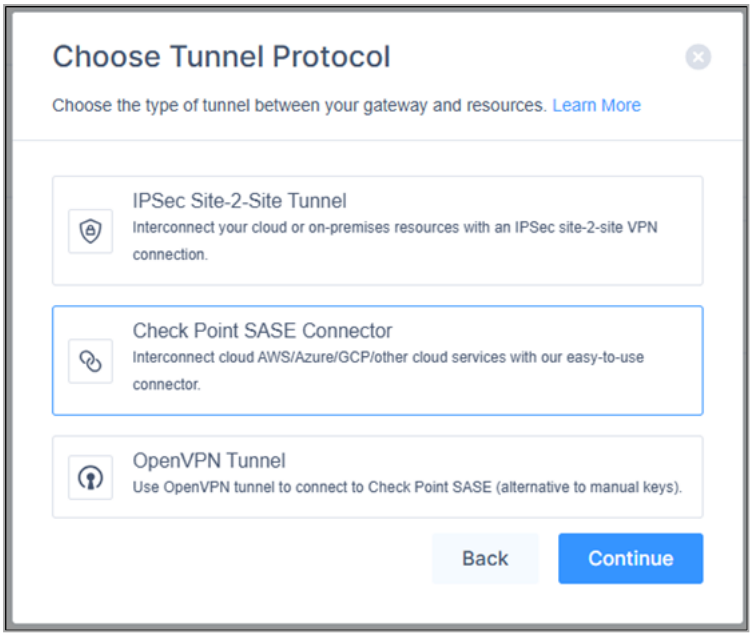
- Two Linux computers on the same local network (same LAN segment).
- Both computers must reach each other through IP.
- VRRP protocol (IP protocol 112) must not be blocked between the two computers.
- The *keepalived* package (the script installs this automatically if it is missing).
- A unique Virtual Router ID (VRID) on the LAN. The default is 81 and the valid range is 1-255.

Configuring a WireGuard Connector Tunnel

Configuring the Connector in the Check Point SASE Administrator Portal

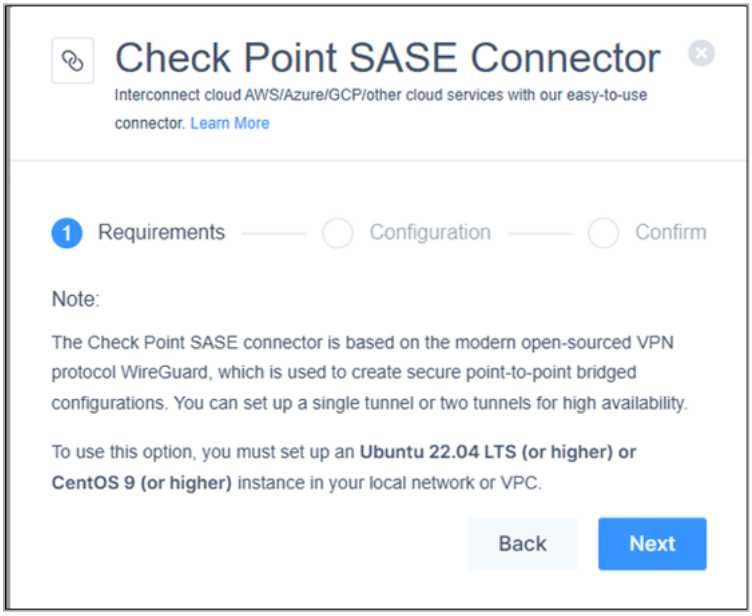
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the WireGuard Connector tunnel, click ··· and click **Add Tunnel**.

The **Choose Tunnel Protocol** window appears.



4. Select **WireGuard Connector** and click **Continue**.

   The **Check Point SASE Connector** window appears.



5. In the **Requirements** section, read the requirements and make sure they are met. Click **Next**.
6. In the **Configuration** section, enter these:

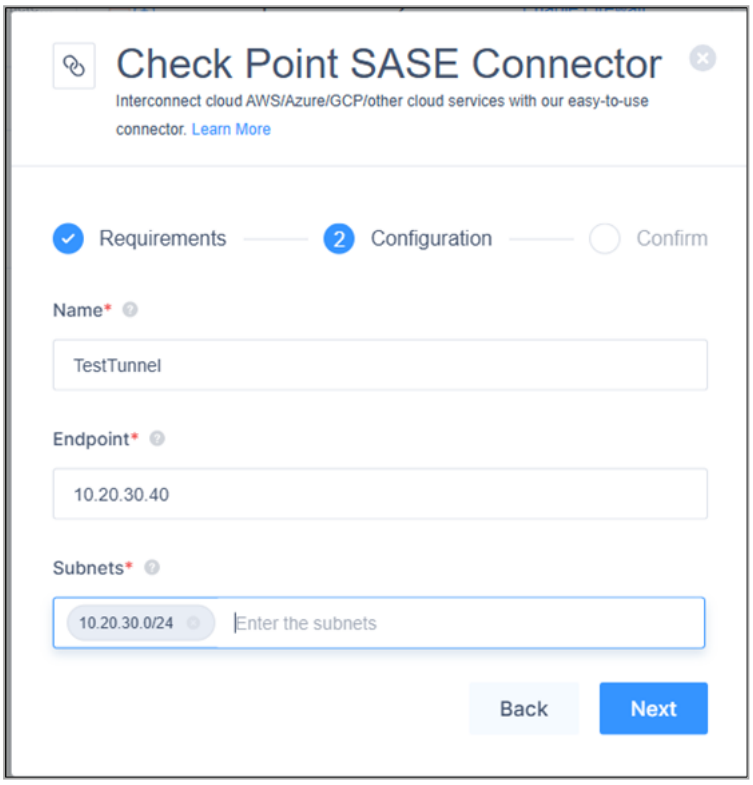
a. **Name** - Name for the connector.

b. **Endpoint** - IP address of the Linux server that has the WireGuard Connector installed.

   If you are using a dynamic public IP address, enter 0.0.0.0

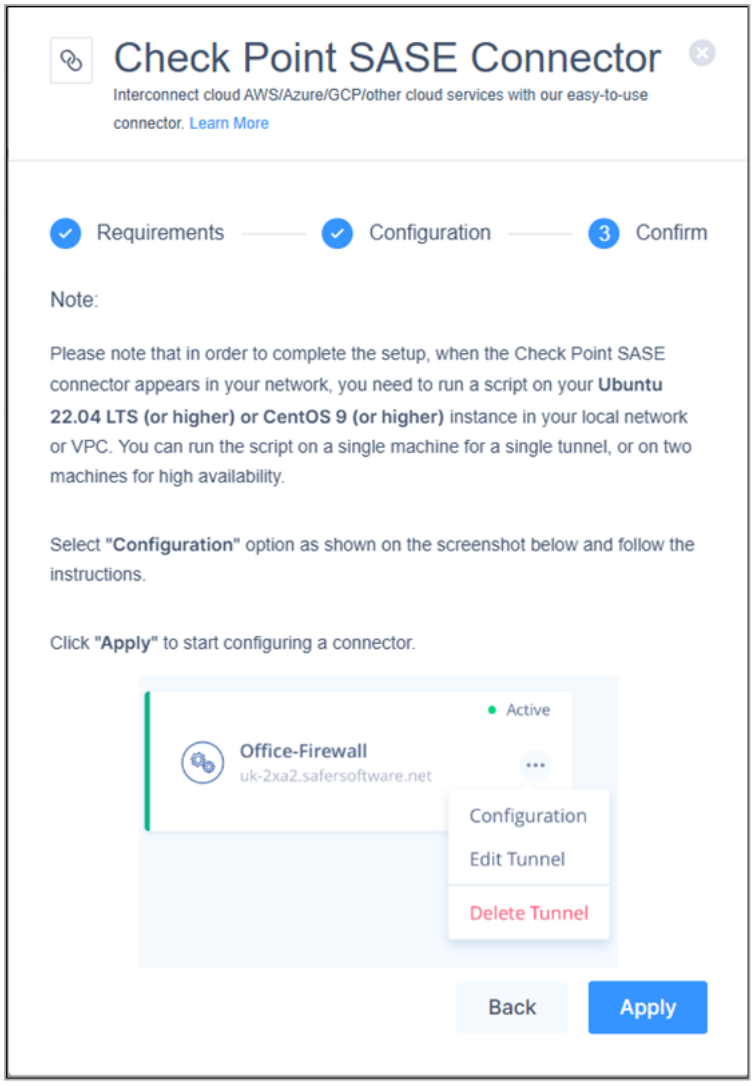
   Note - If you do not know the IP address, query the server by running this command in your Linux terminal:
   `dig +short myip.opendns.com @resolver1.opendns.com`

c. **Subnets** - Subnets of your local network.



d. Click **Next**.

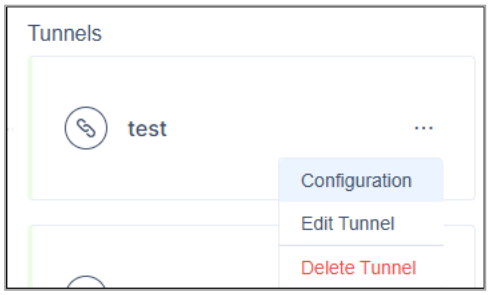
7. In the **Confirm** section, click **Apply**.



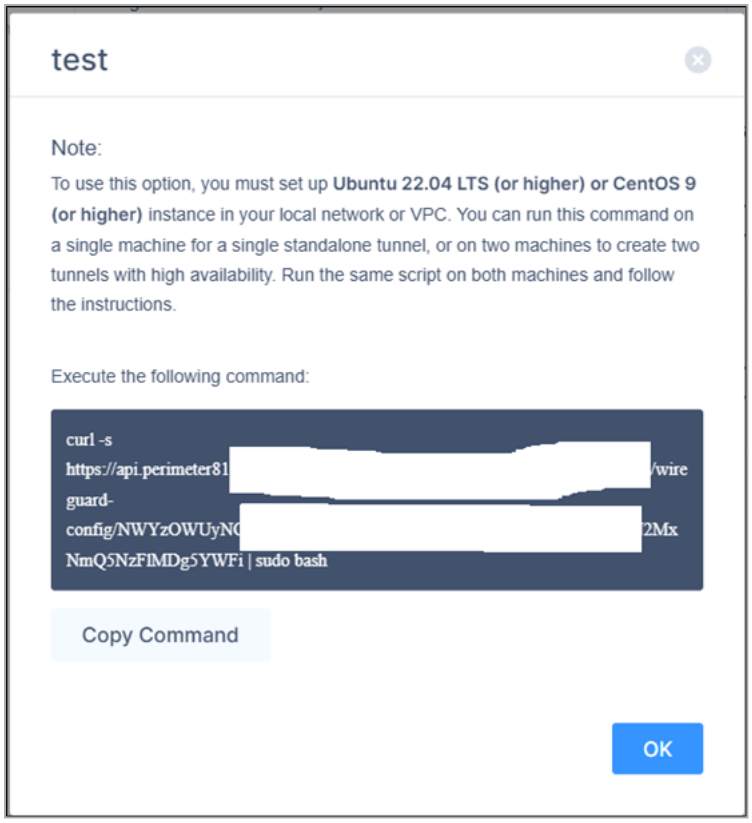
After deployment, the connector appears in the **Networks** page.

Installing the WireGuard Connector on a Linux Server

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click ··· for the WireGuard Connector tunnel that you just configured and then click **Configuration**.



The **Linux Connector** window appears.



3. Click **Copy Command**.

   Note - The command is unique to each connector.

4. Open the Linux terminal and connect as Root user.
5. Run the copied command.
6. Select **Yes** at Stage 4 for access or mode - **Remote Access only** and follow the instructions to install the connector.

Configuring High Availability (Optional)

Overview

WireGuard Connector supports active-passive High Availability using *keepalived* (VRRP). Two computers are configured on the same network one actively runs the tunnel, and the other is on standby. If the active computer fails, the standby automatically takes over the tunnel within seconds. When the failed computer recovers, it becomes the new standby with no pre-emption, ensuring seamless failover without manual intervention.

Setup Flow

Run the same installation script on two computers, one after the other.

Machine 1 (First):

1. Run the installation script (same command from the portal).
2. When prompted "Do you want to enable High Availability (HA) mode?", select **Yes**.
3. Select **1** (first computer).
4. Enter the IP address of the second computer.
5. Note the Virtual Router ID displayed (default: 81). You need this for Machine 2.
6. The script installs and configures *keepalived*, adds firewall rules for VRRP, and starts the tunnel.

Machine 2 (Second):

1. Run the installation script on the second computer.
2. Enable HA and select **2** (second computer).
3. Enter the IP address of the first computer.
4. Enter the Virtual Router ID from Machine 1 (default: 81).
5. The script verifies connectivity to Machine 1, configures *keepalived*, and enters standby mode.

How Failover Works

- Both computers run *keepalived*, which exchanges VRRP heartbeats every second (unicast).
- If the active computer stops responding after 3 missed heartbeats, the standby takes over and starts the WireGuard tunnel.
- When the failed computer recovers, it becomes the new standby. No disruptive switchback occurs.
- Failover completes in approximately 3 seconds.

Important - The WireGuard service is managed by *keepalived* in HA mode. Do not start or stop WireGuard manually with *systemctl*. *keepalived* handles this automatically.

Notes -

- The Virtual Router ID (VRID) must be unique on the LAN. If another *keepalived* instance uses 81, the script detects the conflict and prompts for an alternative.
- Firewall rules for VRRP (protocol 112) are added automatically by the script (*iptables* or *firewalld*).

Verifying the Setup

1. Connect to your network using the Check Point SASE Agent on a device.
2. Open the command line and run:

   ```
   ping <Internal resource IP address>
   ```

3. Make sure that outbound port UDP/8000 is not blocked in your firewall/router, and that you have followed all the steps.
4. If the issue persists, on the Linux server, collect these logs and contact *Check Point Support*. The logs are available in:

   ```
   ##Configuration file
   /etc/wireguard/wg0.conf

   ##Connection logs
   /tmp/p81-wg-connector.log
   ```

For HA deployments:

1. On both computers, run this command to verify that keepalived is running: `systemctl status keepalived`
2. Check the VRRP state by running: `journalctl -u keepalived`

   One computer shows **MASTER** and the other shows **BACKUP**.

Removing the WireGuard Connector

Connect to the command line of Linux server where you have installed the WireGuard Connector and run:

```
# Locate the WireGuard packages # (the output of this command will
show you all wireguard packages installed on the machine)
dpkg -l | grep wireguard

# Delete all packages found that are associated with WireGuard
# (Run this command for each package found, replace  with the output
from the previous command)
apt-get remove --purge # Locate the WireGuard packages # (the output
of this command will show you all wireguard packages installed on the
machine)
dpkg -l | grep wireguard
```

```
# Locate the WireGuard packages # (the output of this command will
show you all wireguard packages installed on the machine)
yum list installed | grep wireguard

# Delete all packages found that are associated with WireGuard# (Run
this command for each package found, replace  with the output from the
previous command)
yum remove # Locate the WireGuard packages # (the output of this
command will show you all wireguard packages installed on the machine)
yum list installed | grep wireguard
```

For HA deployments

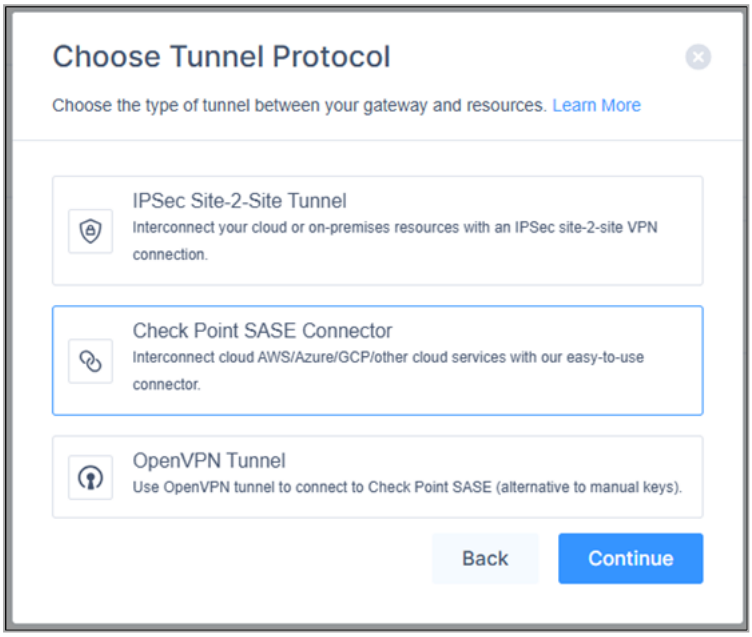
1. Before removing WireGuard, stop and disable keepalived:
   a. `systemctl stop keepalived`
   b. `systemctl disable keepalived`
2. Remove the keepalived configuration and helper scripts:
   a. `rm /etc/keepalived/keepalived.conf`
   b. `rm /usr/libexec/keepalived/p81-wg-*`

OpenVPN Tunnel

Configuring the OpenVPN Tunnel in the Check Point SASE Administrator Portal

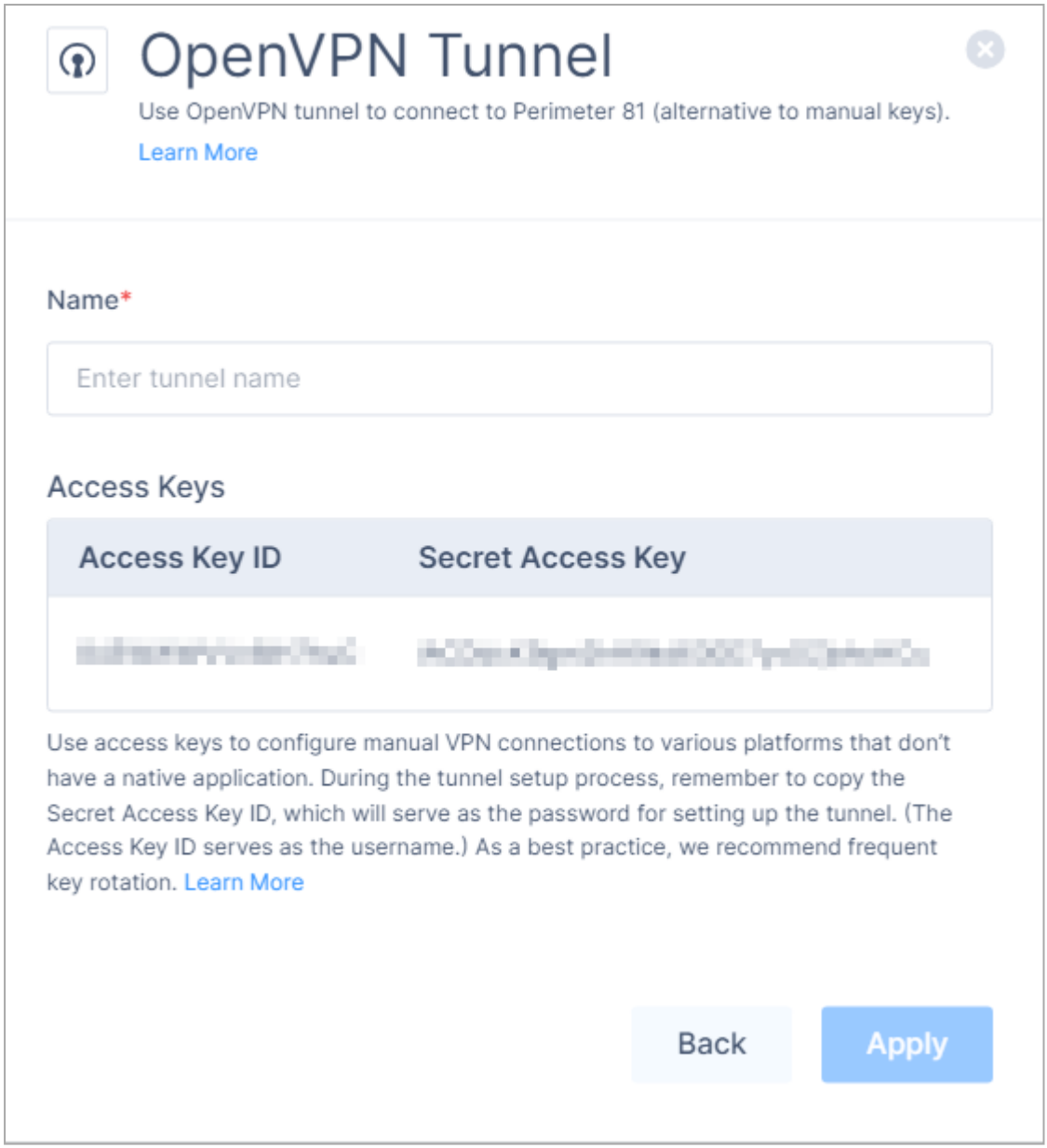
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the OpenVPN tunnel, click ··· and click **Add Tunnel**.

   The **Choose Tunnel Protocol** window appears.



4. Select **OpenVPN Tunnel** and click **Continue**.

   The **OpenVPN Tunnel** window appears.

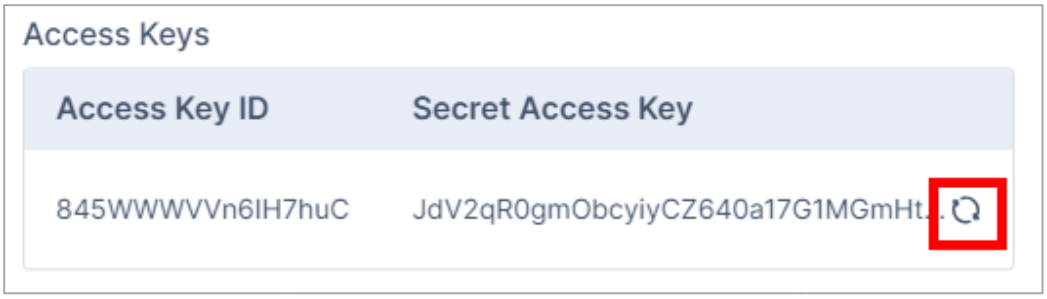


5. In the **Name** field, enter a name for the tunnel.
6. Save the **Access Keys** credentials.

Caution - Save the Access Keys credentials before you click **Apply**. Otherwise, regenerate the Access Keys:

a. To regenerate the Access Keys, in the newly created OpenVPN tunnel, click ··· > **Edit Tunnel**.

b. In the **Access Keys** section, click ↻.

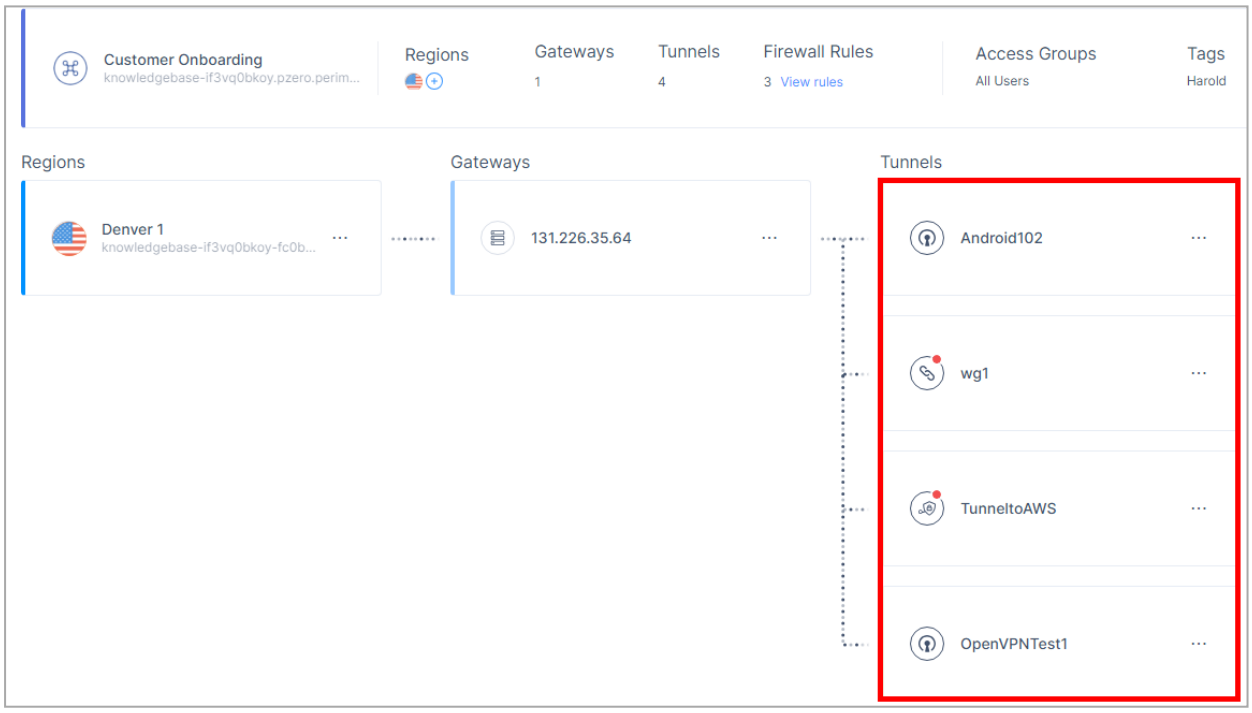


The system regenerates the **Access Key ID** and **Secret Access Key** values.

c. Click **Apply**.

7. Click **Apply**.

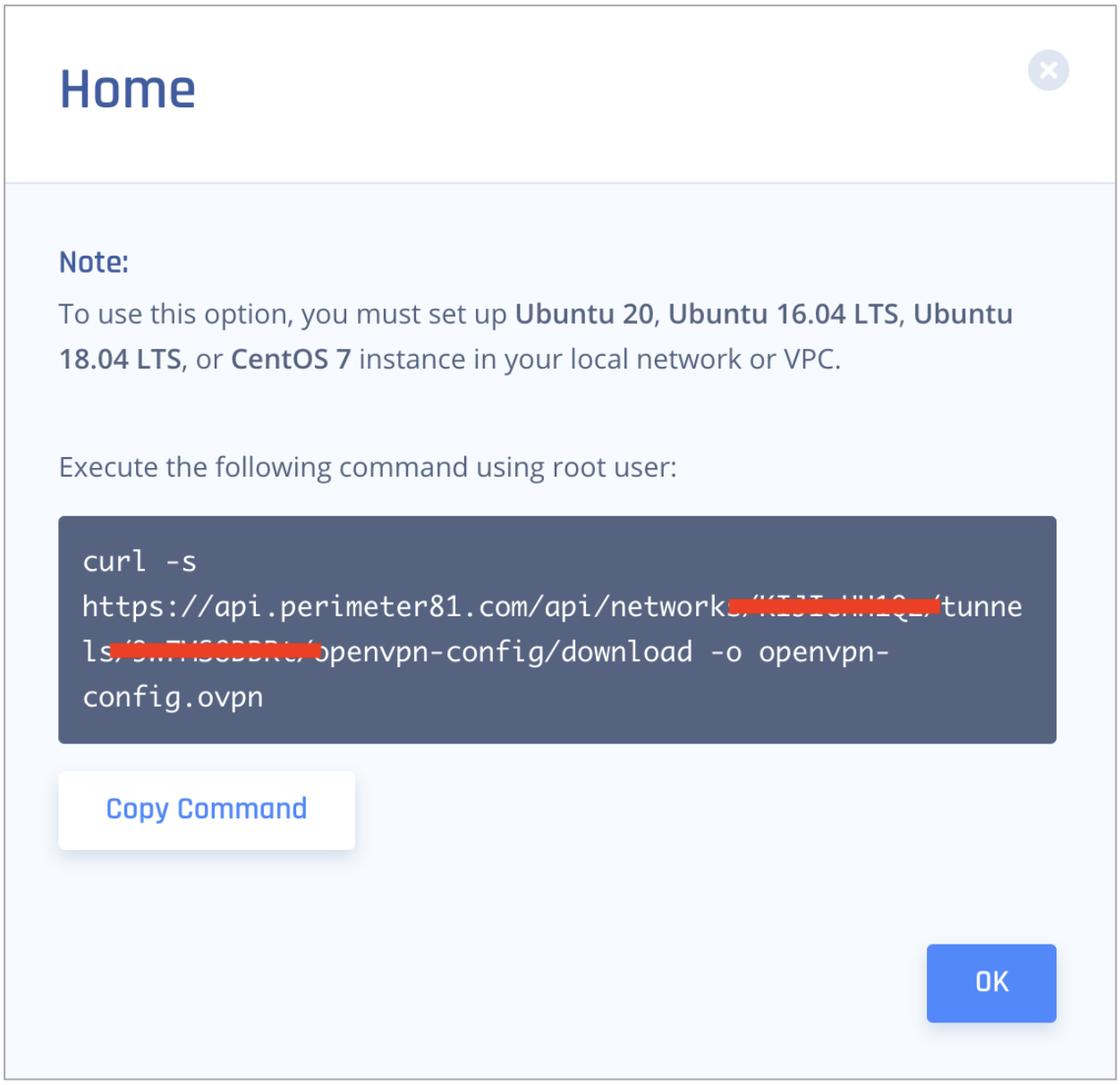
The system creates an OpenVPN tunnel and displays it in the **Tunnels** section.



Installing a VPN and Configuring the OpenVPN Tunnel on the Device

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.

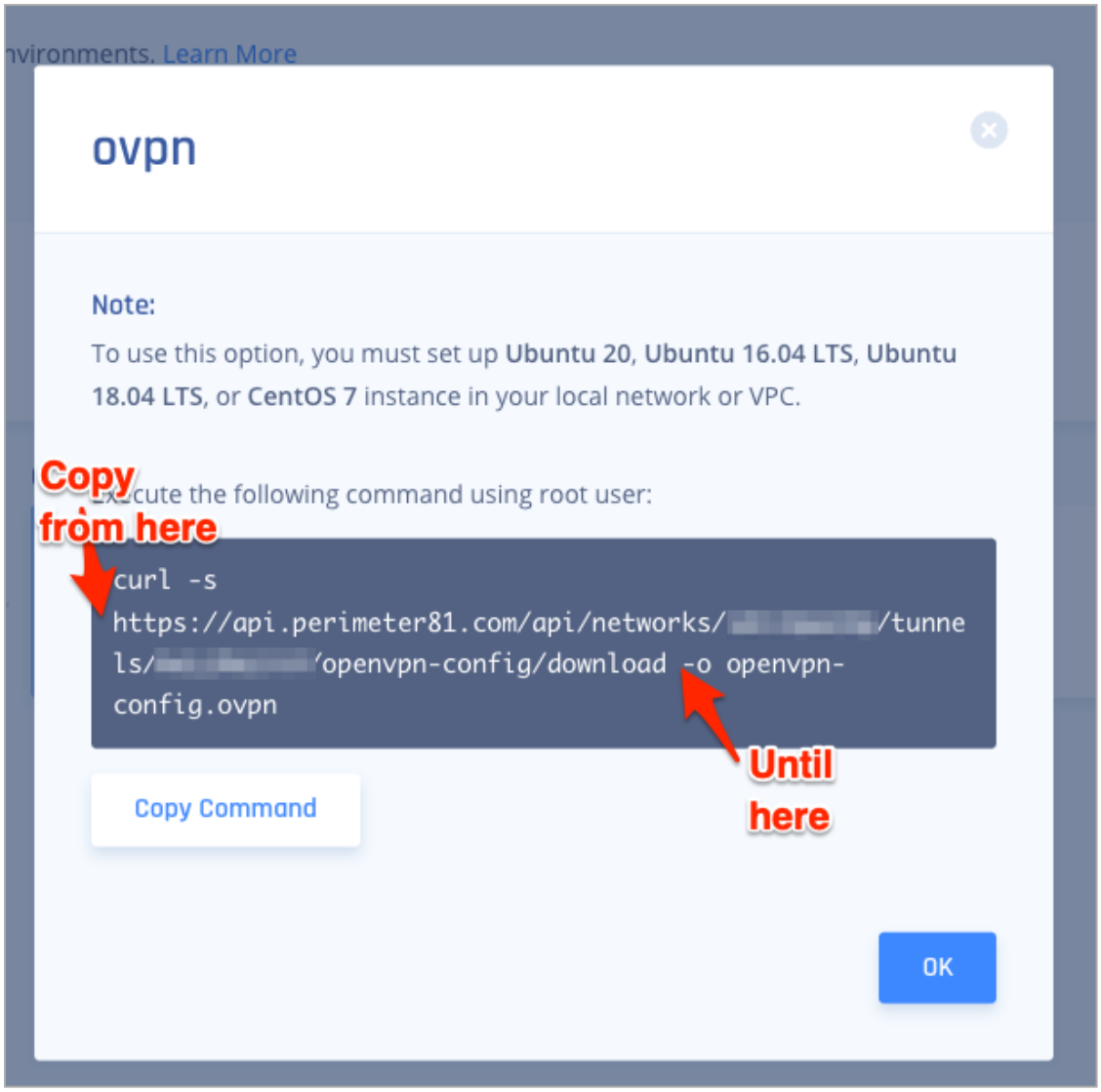
3. In the gateway where you added the OpenVPN tunnel, click ··· and then click **Configuration**.



4. Copy the command and run it in the terminal window on the device.

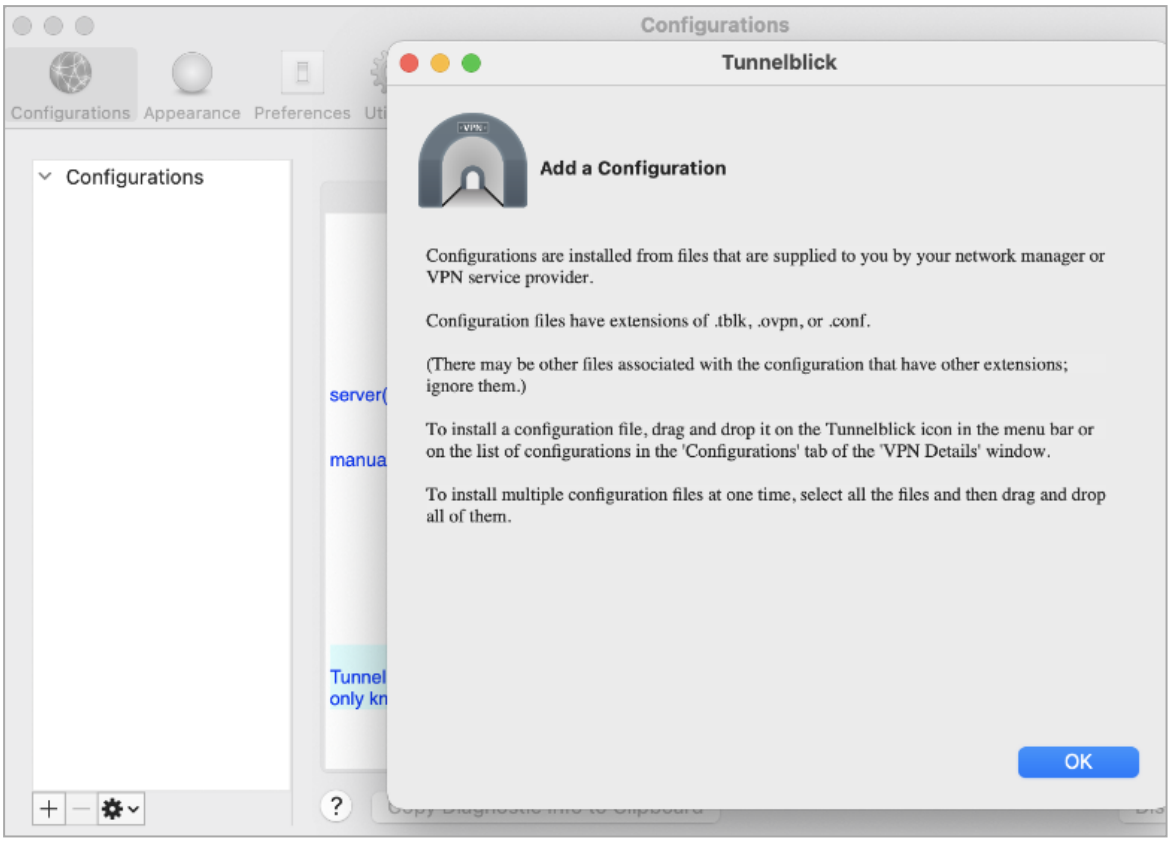
   The system downloads the *saferx-openvpn-client.pvpn* configuration file.

Note - If the device's operating system does not support a terminal window, copy the command from `https` until `download`. Paste the command in a browser address bar and press **Enter**. The system downloads the *saferx-openvpn-client.ovpn* configuration file.



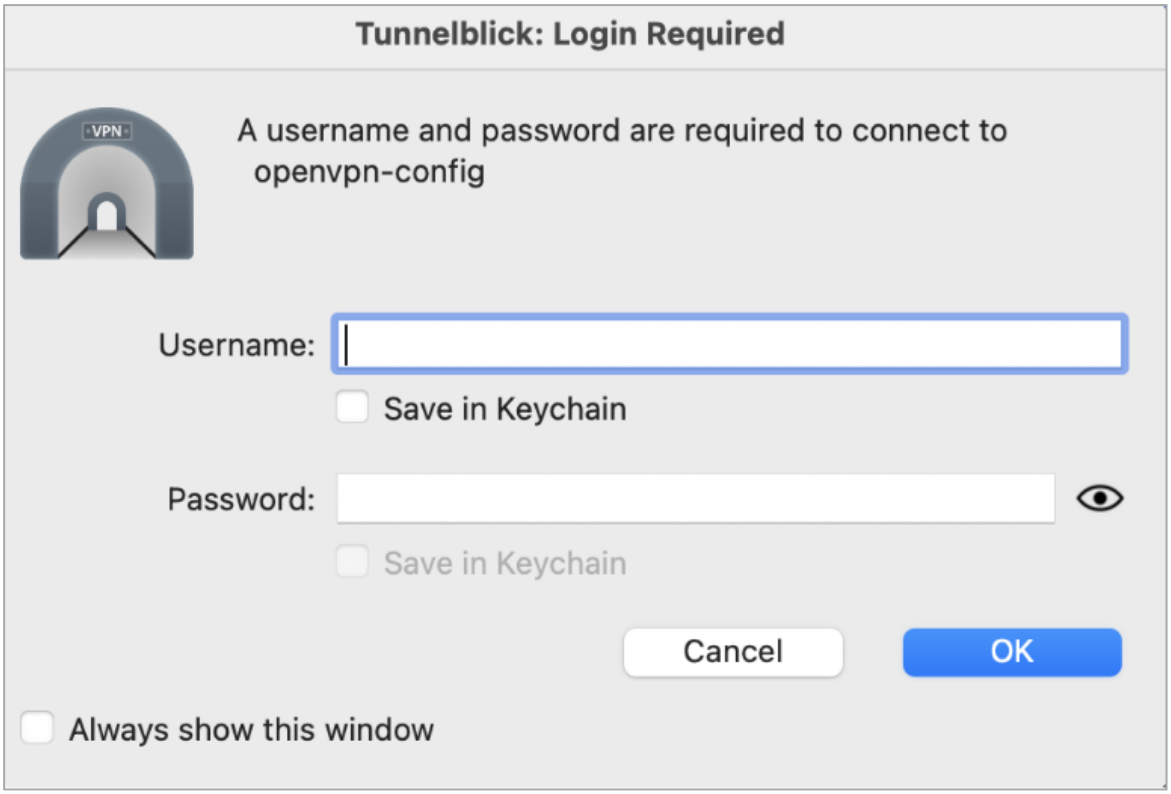
5. On a macOS device:
    a. Download and install a VPN client. Check Point recommends Tunnelblick VPN client.

b. Drag and drop the *openvpn-config.ovpn* file into the client to add the configuration.



c. To connect to the VPN, in the **Username** field, enter the **Access Key ID** that you copied when you created the tunnel.

d. In the **Password** field, enter the **Secret Access Key** that you copied when you created the tunnel.

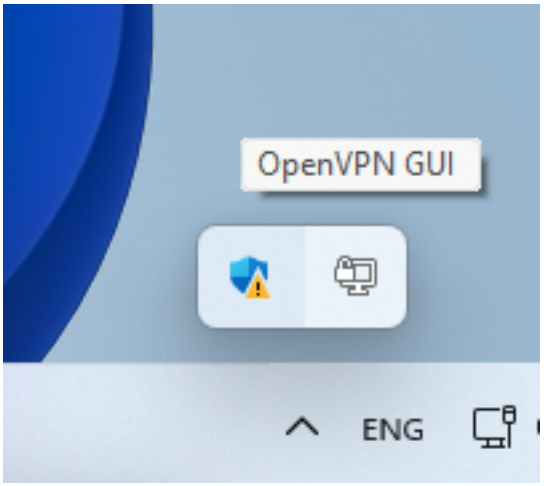


e. Click **OK**.

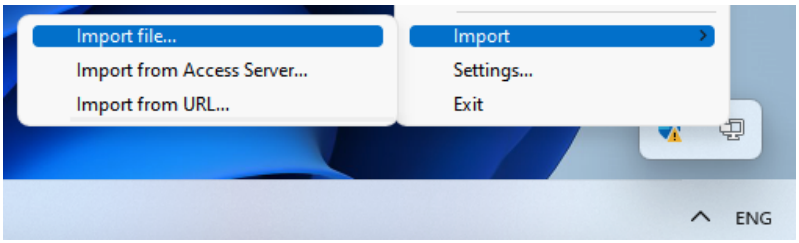
6. On a Windows device:

a. Download and install the OpenVPN Client. Check Point recommends https://openvpn.net/community-downloads/

b. Click the **OpenVPN** icon.



c. Click **Import** > **Import file...**

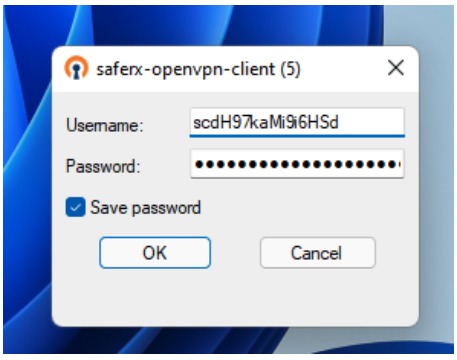


d. Select the downloaded file *saferx-openvpn-client.ovpn*

e. After you import the file, right-click the OpenVPN client and then click **Connect**.

The OpenVPN client window appears.

f. In the **Username** field, enter the **Access Key ID** that you copied when you created the tunnel.



g. In the **Password** field, enter the **Secret Access Key** that you copied when you created the tunnel.

Note - If the **Secret Access Key** starts with *6perimeter81$*, it indicates that the key is encrypted.
Regenerate the access keys. See step 6 in *"Configuring the OpenVPN Tunnel in the Check Point SASE Administrator Portal" on page 214*.

Verifying the Setup

1. In the Check Point SASE Administrator Portal, click **Networks** and verify that the tunnel is up.
2. In the Check Point SASE Agent, connect to the network and access a resource. If you are unable to connect to the resource, contact *Check Point Support*.

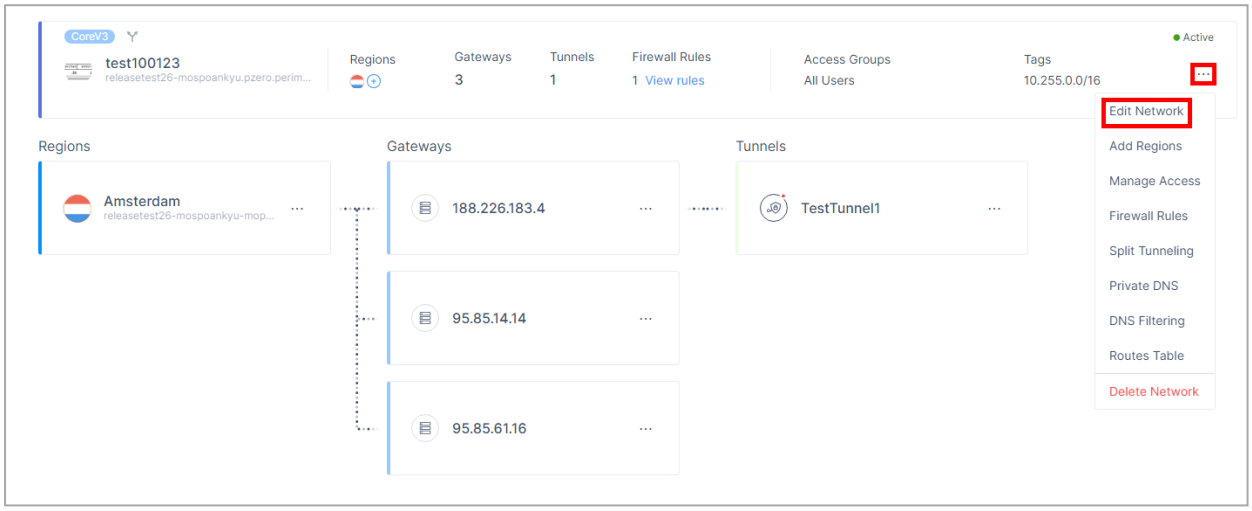
Verifying the Setup

1. In the Check Point SASE Administrator Portal, click **Networks** and verify that the tunnel is up.
2. In the Check Point SASE Agent, connect to the network and access a resource. If you are unable to connect to the resource, contact *Check Point Support*.

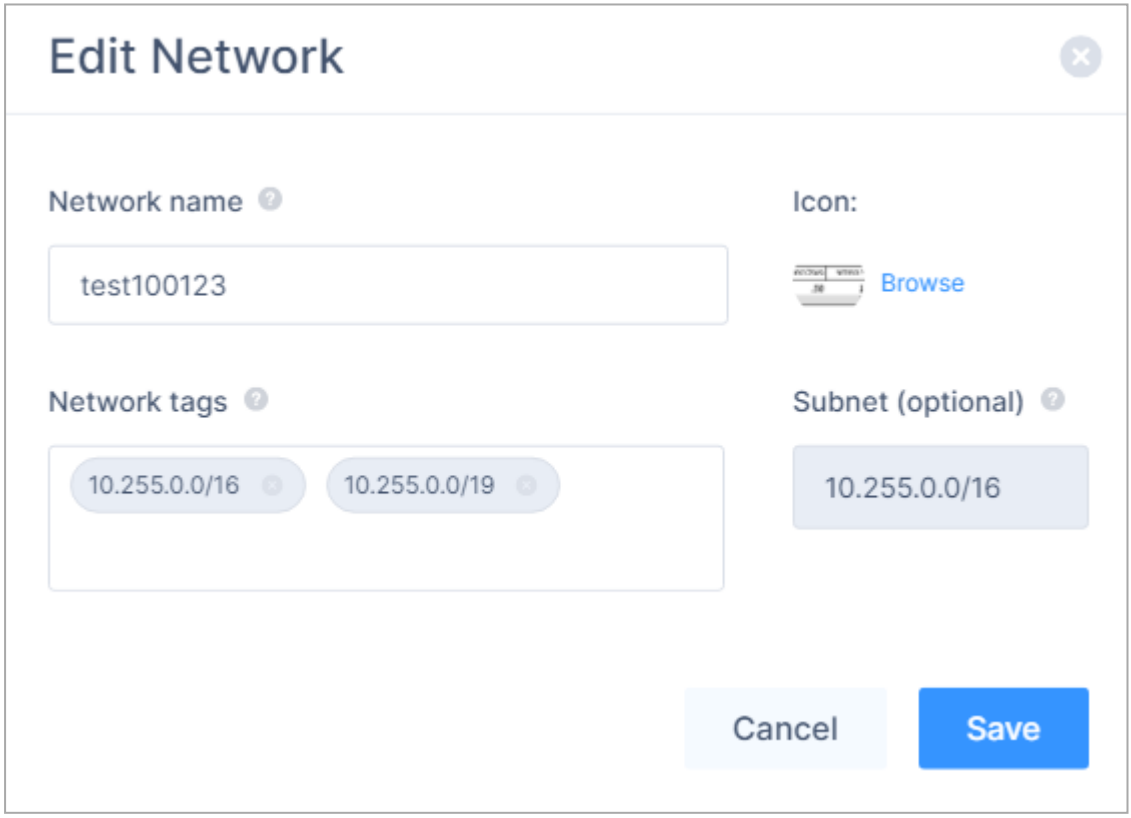
Managing a Network

Editing a Network

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Edit Network**.



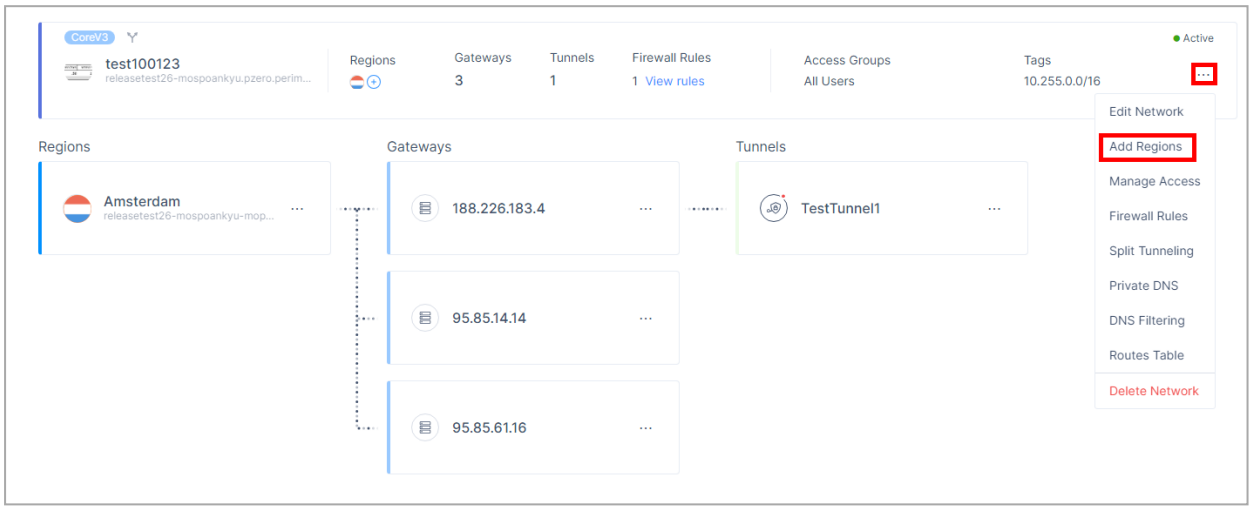
The **Edit Network** window appears.



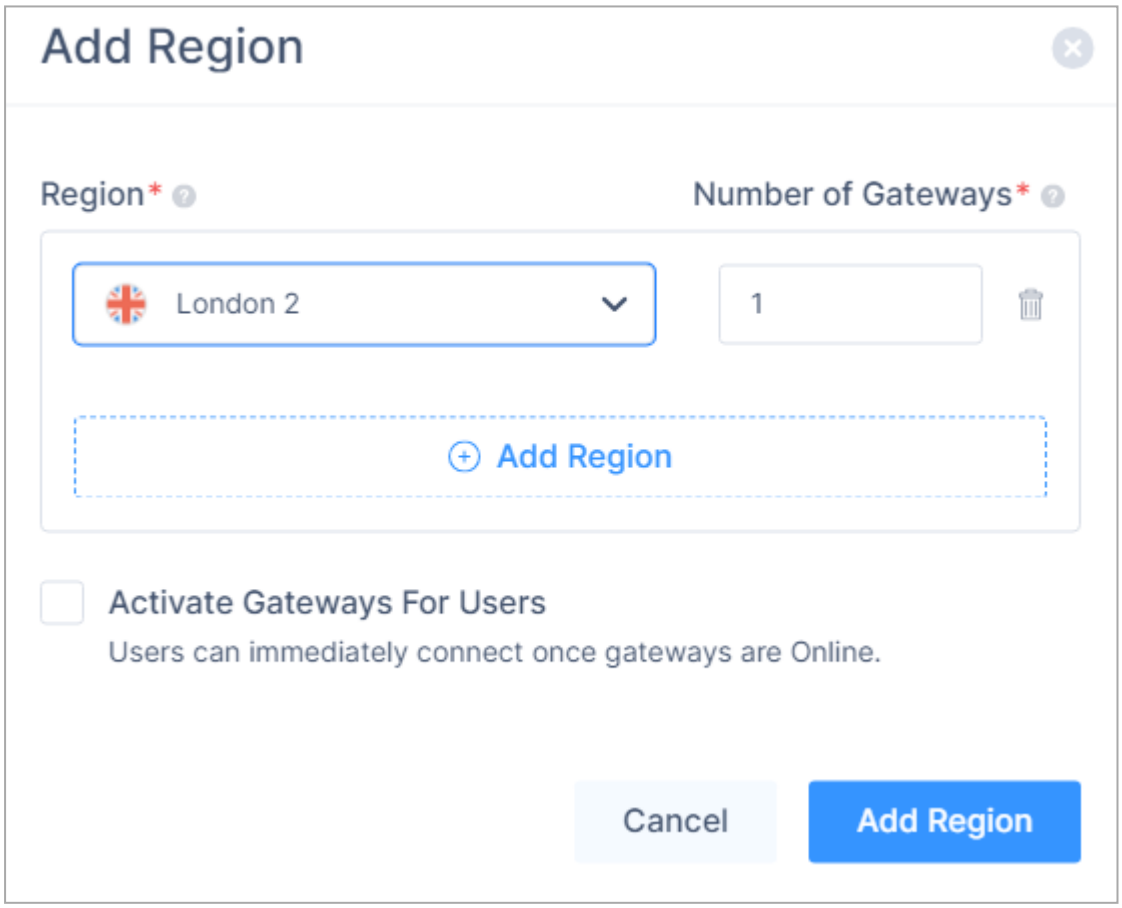
4. Make the required changes and click **Save**.

Adding Regions

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Add Regions**.



The **Add Region** window appears.



4. From the **Region** list, select the region to deploy the Check Point SASE gateway.

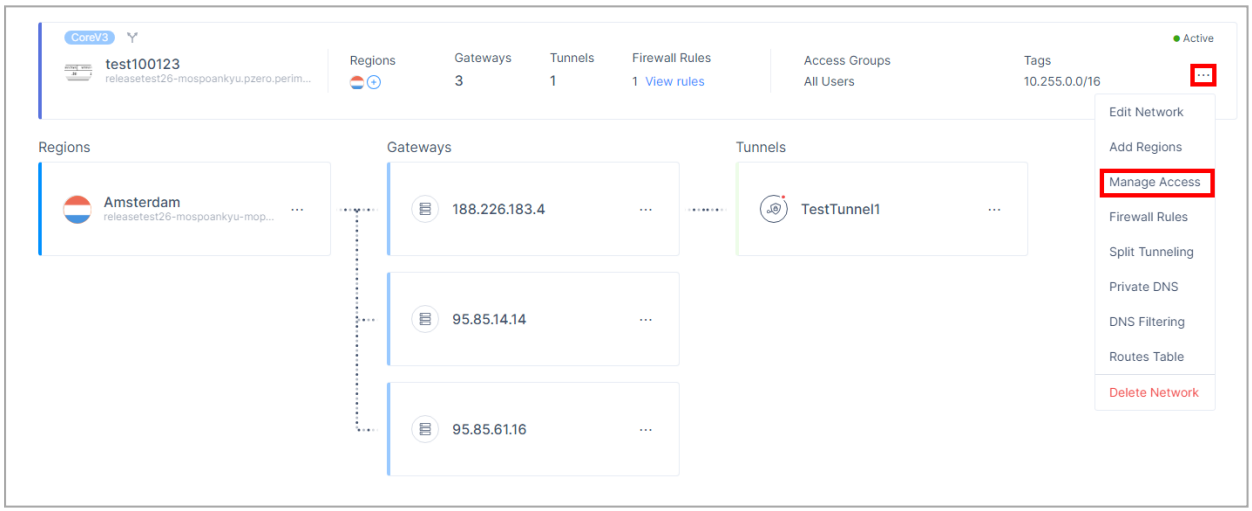
5. In the **Number of Gateways** field, enter the number of private gateways you want to deploy in the region.
6. To add another region, click **Add Region** and repeat steps 4 and 5.
7. To activate the gateway for users, select the **Activate Gateways For Users** checkbox.
8. Click **Add Region**.

Managing Access

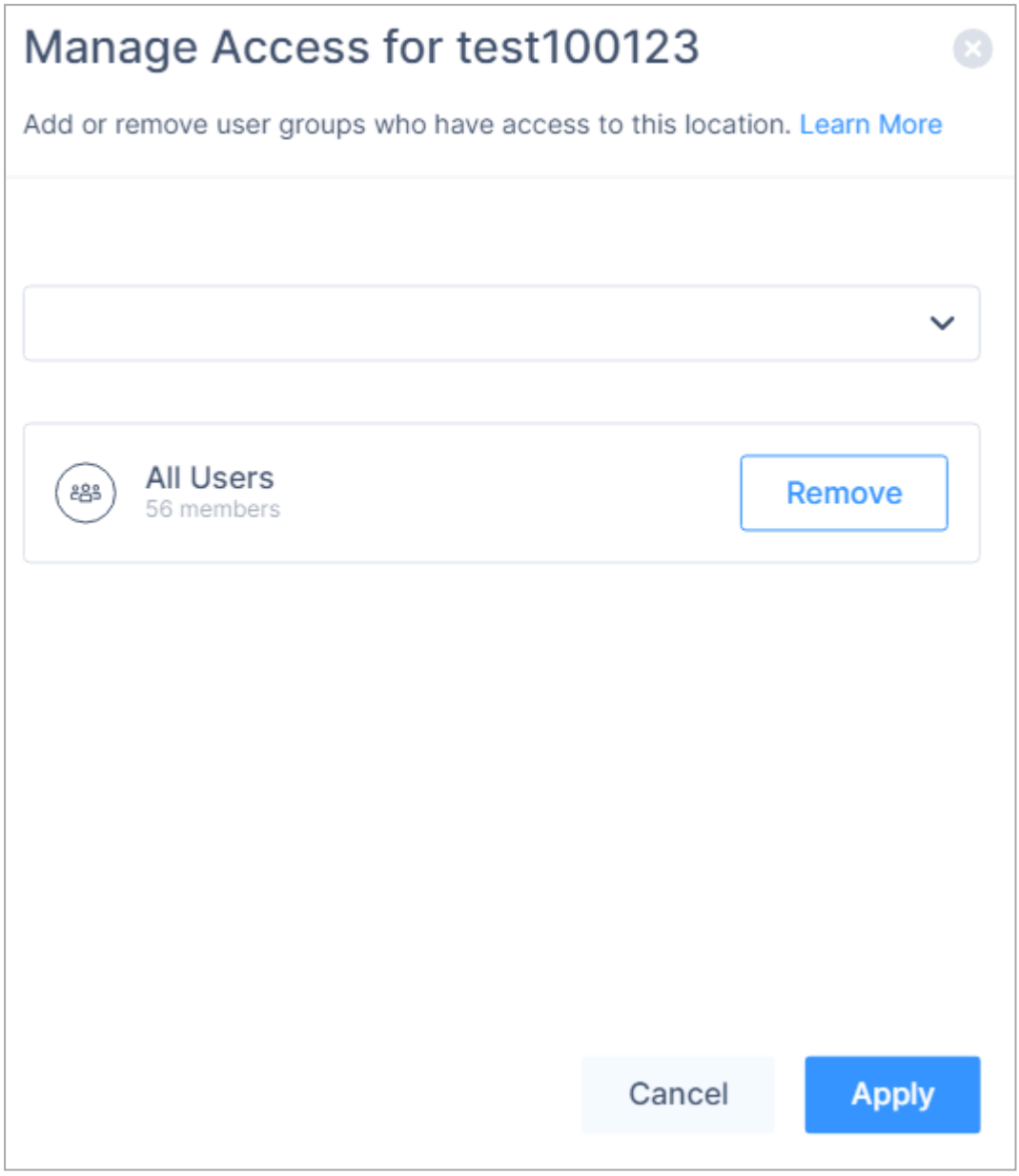
Manage Access allows you to select the member groups who can access the network.

To manage access to a network:

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Manage Access**.



The **Manage Access** window appears.



4. From the list, select the member groups who can access the network.
5. To remove a member group, click **Remove**.
6. Click **Apply**.

Firewall Rules

Firewall Rules allows you to set the firewall access rules for your network.

To set the rules, see *"Creating a Firewall Access Rule" on page 737*.

Split Tunneling

Split tunneling allows you to choose the traffic that should pass through the tunnel and the traffic that should bypass the tunnel and access the resource directly.

Private network traffic is always tunneled through the cloud, based on your network tunnels and routing table settings.

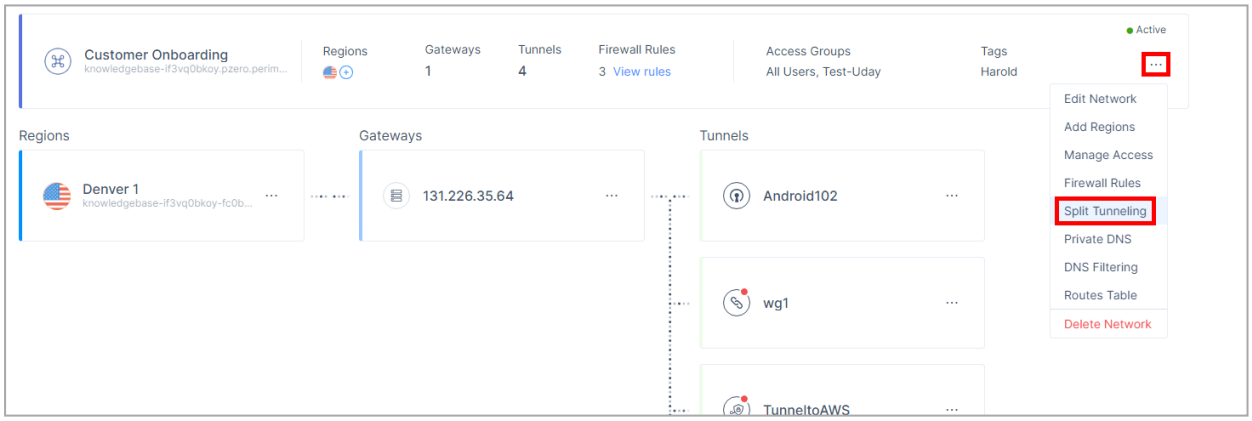
To route additional addresses through the SASE cloud, such as public cloud resources you wish to access through SASE using whitelisting, you must specify them manually.You also need to specify any addresses you want to exclude when routing all internet traffic through the tunnel.

Notes:

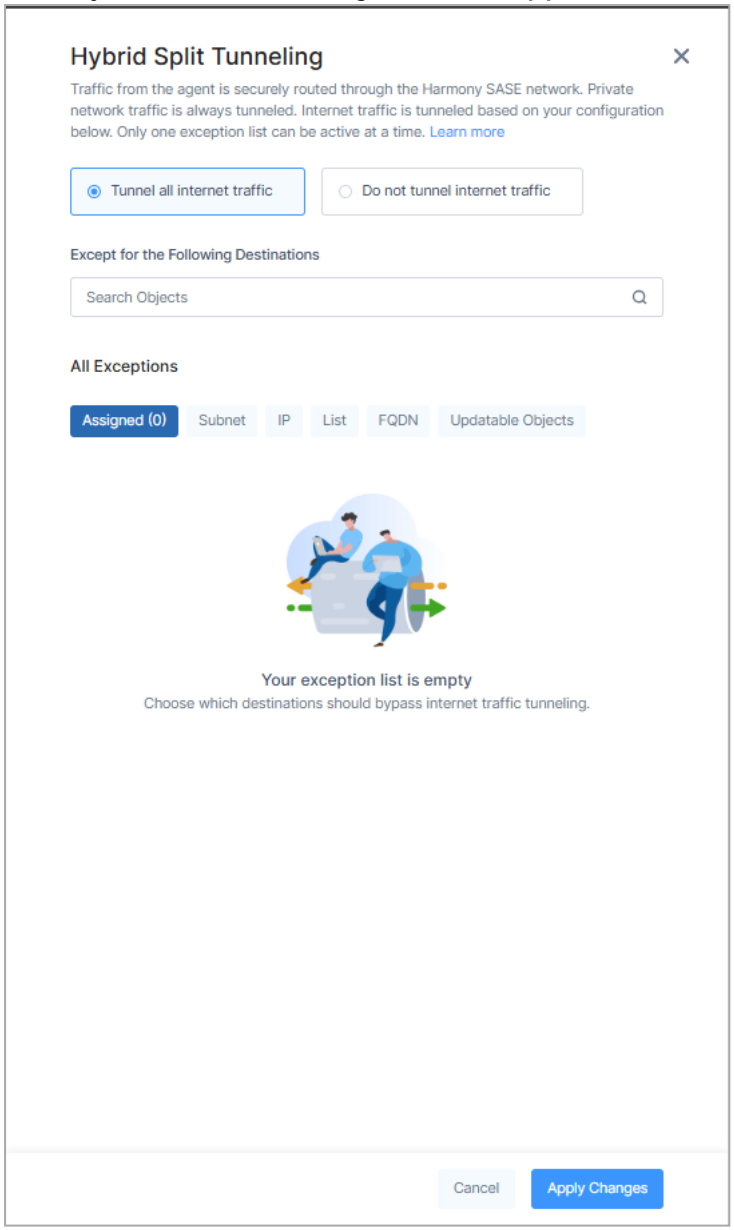
- Split tunneling by FQDN is supported only for Check Point SASE Agents 10.1.x and higher. With older agent versions, split tunneling by FQDN is ignored and reverts to full tunneling.
- The recommended setting is not to tunnel traffic internet through the cloud to minimize latency while keeping connectivity to private resources.

To configure split tunneling for a network:

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select your network.
3. Click ··· and then click **Split Tunneling**.



The **Hybrid SASE Settings** window appears.



4. Select one of these:
   - **Tunnel all internet traffic except**: Routes all internet traffic through SASE, except the destinations you specify. These destinations bypass the tunnel
   - **Do not tunnel any traffic except**: Routes only private network traffic through SASE. Internet traffic is sent directly to the internet, except the destinations you specify. These destinations are tunneled.
5. In the **Except for the Following Destinations**, search for objects.
6. In **All Exceptions**, select the required objects:

a. **Assigned**: Displays the objects currently selected for this network.

b. **Subnet**: Select subnet-based destination objects.

c. **IP**: Select individual IP address objects.

d. **List**: Select predefined lists that contain multiple IPs, subnets, or FQDNs.

e. **FQDN**: Select fully qualified domain name (FQDN) objects for domain-based split tunneling rules.
For more information on creating Subnet, IP, List, and FQDN objects, see *"Addresses" on page 911*.

f. **Updatable Objects**: Select dynamic object groups that automatically update their IP ranges.
For more information, see *"Updatable Objects" on page 923*.
Note - Microsoft Azure services, Amazon Web Services (AWS), and Geolocation-based Updatable Objects are not supported for Split Tunneling.

7. Verify the selected objects under the **Assigned** tab.
8. Click **Apply Changes**.

Note - The processing time depends on the system resource. It takes up to 3 seconds for every 500 subnets.

Private DNS

Notes -

- You cannot enable Regional DNS and Private DNS at the same time.
- Only one DNS option can be active per network or region.

A private DNS allows you to use your local DNS to resolve host names into IP addresses.

Check Point SASE supports DNS at two levels:

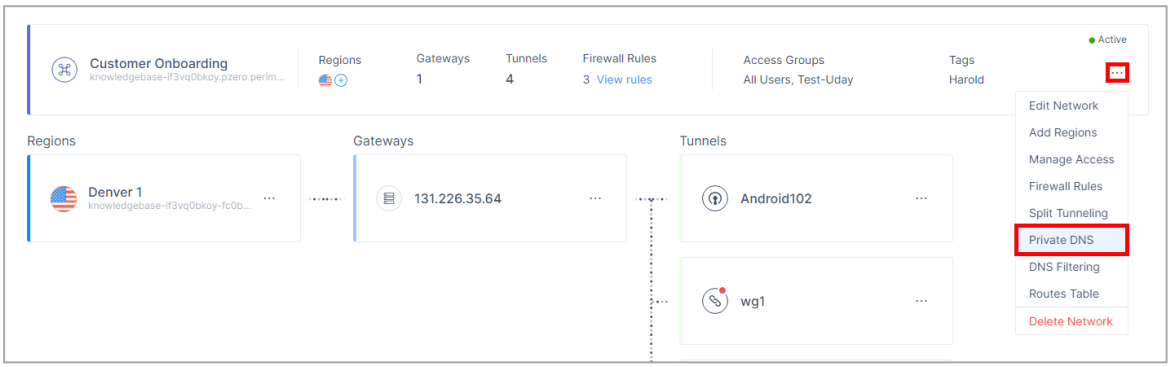
- Network - Allows you to utilize your organization's DNS server and local domain names.
- Region - Allows your users to resolve resources through a local DNS server rather than waiting for a remote server response.

Notes -

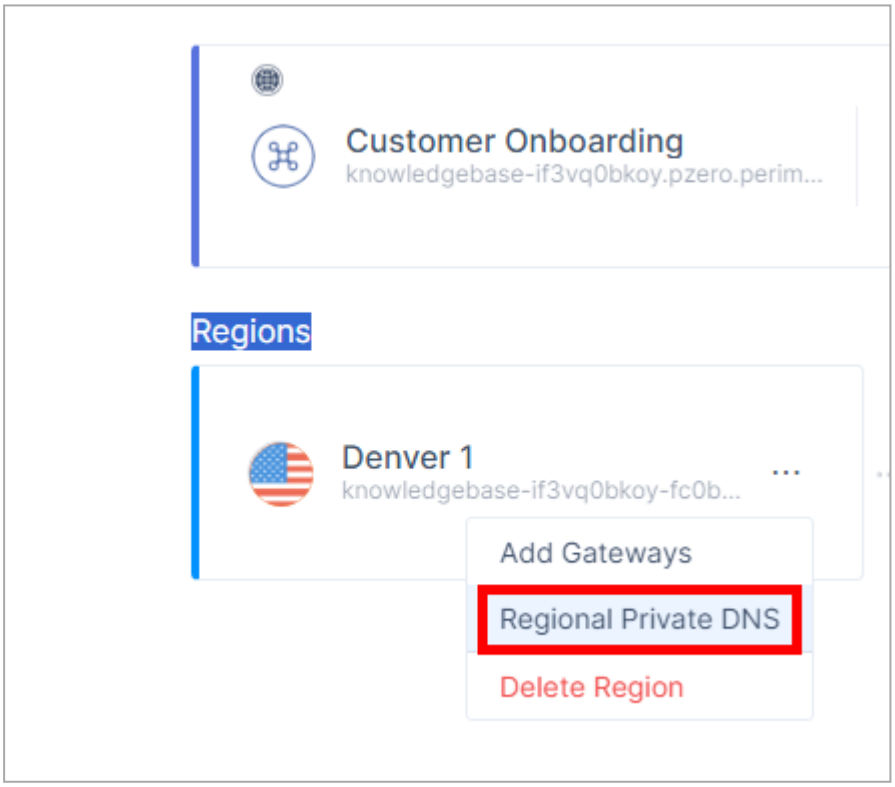
- Do not use Public DNS *8.8.8.8*, *8.8.4.4*, *1.1.1.1*, and *1.0.0.1* for your private DNS.
- If your private DNS server does not have a public IP address, then Check Point recommends to use the IPSec or WireGuard connector tunnel.

To configure a private DNS for a network:

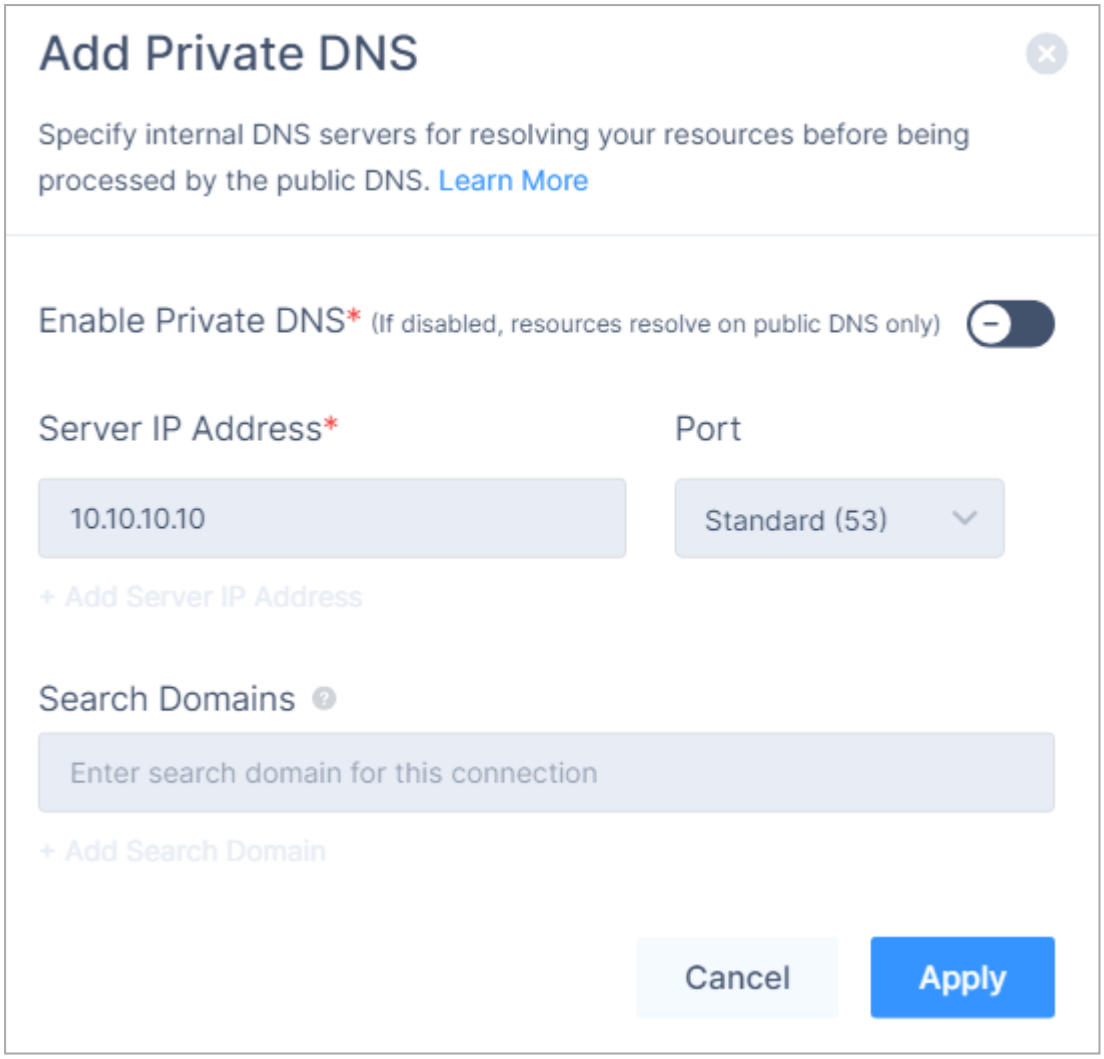
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. To add a private DNS:
   - For a network, click ··· and then click **Private DNS**.



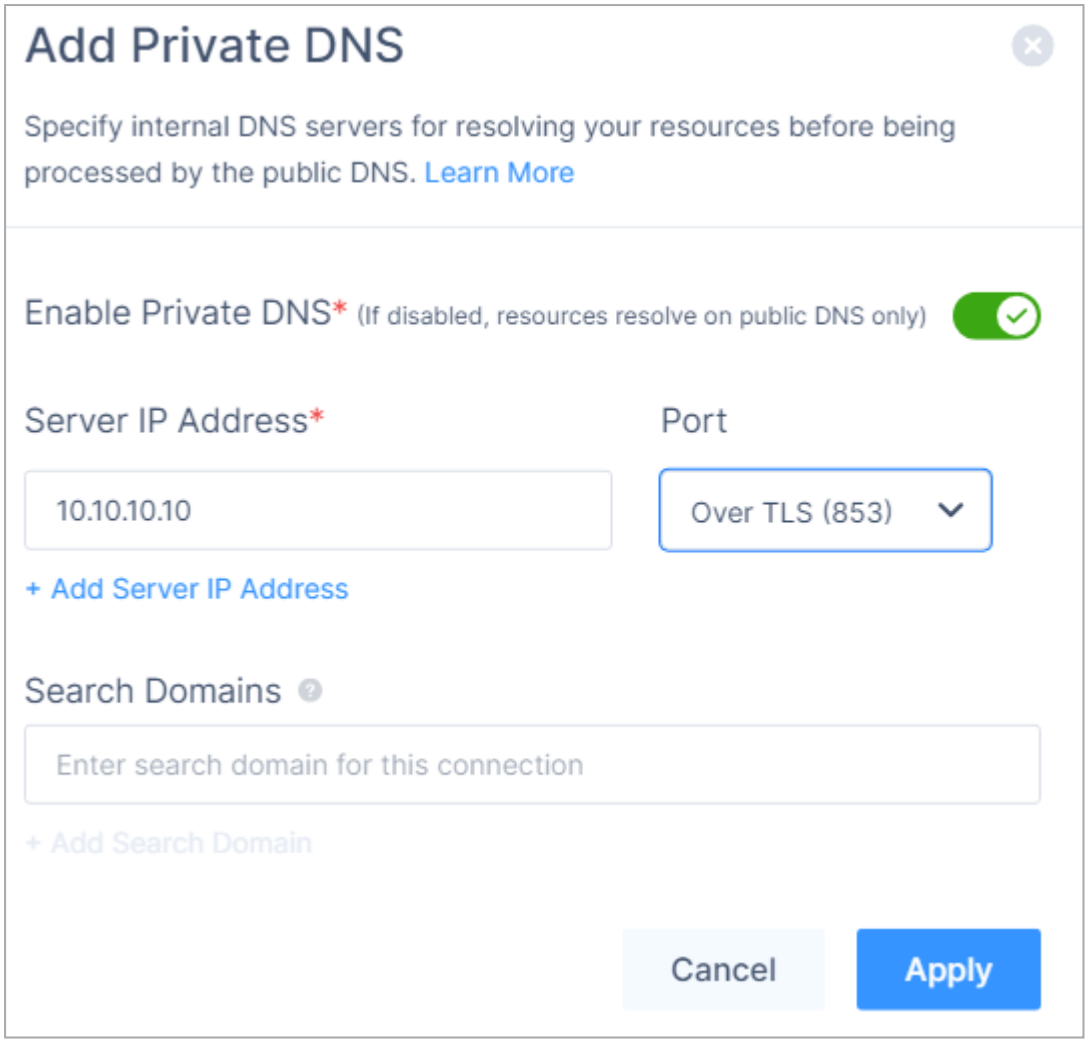
   - For a region, in the **Regions** section, click ··· and then click **Regional Private DNS**.



The **Add Private DNS** window appears.



4. Turn on the **Enable Private DNS** toggle button.
5. If your Private DNS Server(s) supports DoT, from the **Port** list, select **Over TLS** (otherwise your requests are sent over HTTPS).



Note - You can configure multiple private DNS servers for load balancing. Make sure that the DNS endpoint has zone sharing or zone forwarding enabled. This is supported by both cloud-based and on-premises DNS resolvers.

6. In the **Server IP Address** field, enter the IP address of your DNS servers. You can enter up to four IP addresses.
7. In the **Search Domains** field, enter the suffix for the DNS query.

   For example, if the domain is *checkpoint.com*, if your enter *support*, then the system automatically redirects to *support.checkpoint.com*.
8. Click **Apply**.

   Wait for the network status to change from **Deploying...** to **Active**.

DNS Filtering

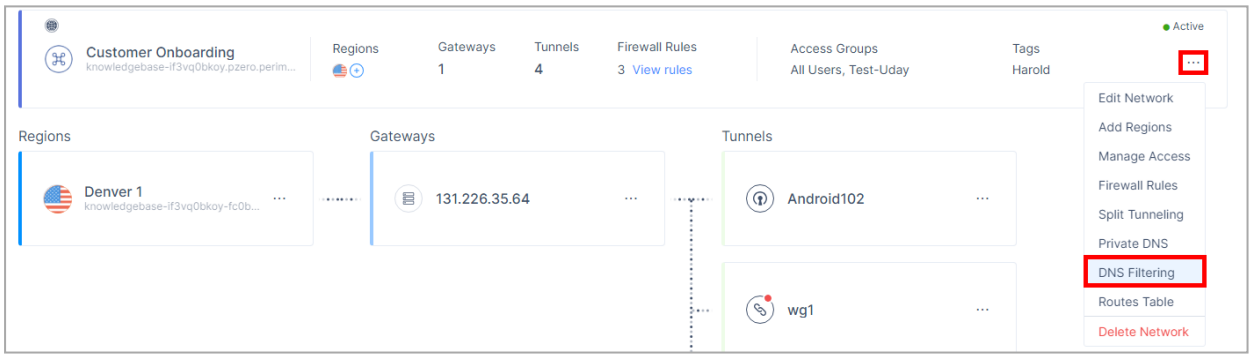
DNS Filtering allows you to manage internet access for members in your network by blocking or allowing websites using allow-list and block-list.

Best Practices -

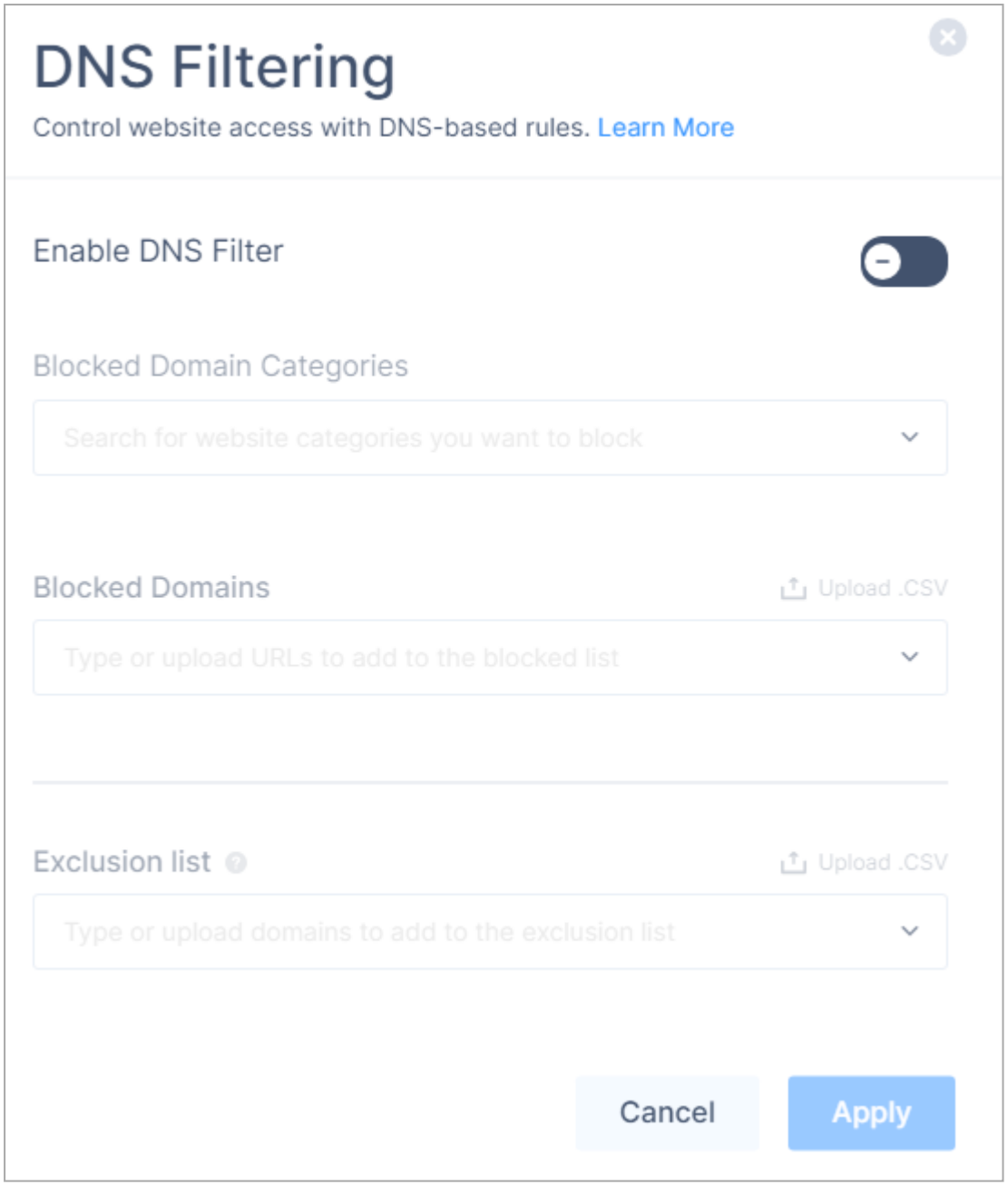
- Make sure that you have the list of URLs to block and allow.
- Make sure that the DNS filter settings work as expected.

To configure DNS filtering for a network:

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **DNS Filtering**.



The **DNS Filtering** window appears.



4. Turn on the **Enable DNS Filter** toggle button.
5. From the **Blocked Domain Categories** list, select the website categories you want to block.
6. In the **Blocked Domains** field, enter the domains you want to block or upload a .CSV file with the domains.

   Make sure that the .CSV file:

   - Contains all the entries in a single column.
   - Each cell contain only one entry.

- The number of entries does not exceed 1000.
- Each entry is in the form *domain.com*, without **www**, **HTTP**, **HTTPs** prefixes.

	A
1	badpineapple.com
2	fakenews.co.uk
3	loveistheanswer.fr

Note - When you block a domain, the system blocks the related sub-domains as well.

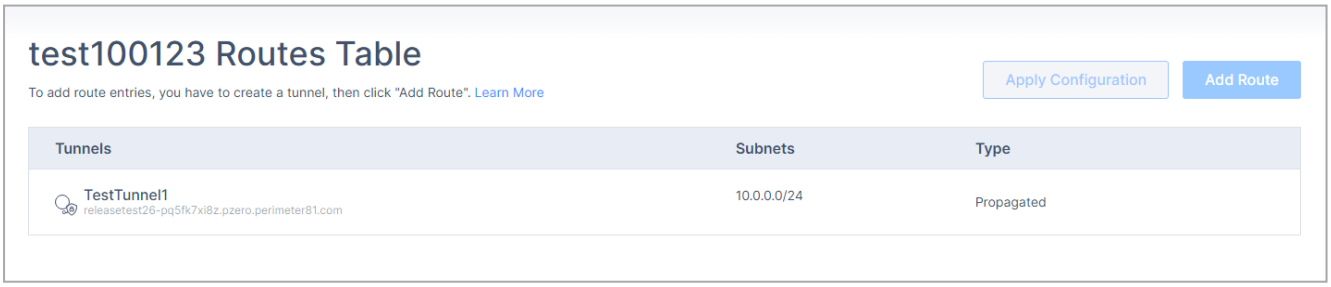
7. In the **Exclusion list** field, enter the URLs you want to exempt from the blocked domains list or upload a .CSV file with the domains.
8. Click **Apply**.

   After the settings are applied, a tooltip shows that DNS filtering is activated in your network.

   The changes are enforced the next time when the member connects to your network using the Check Point SASE Agent.

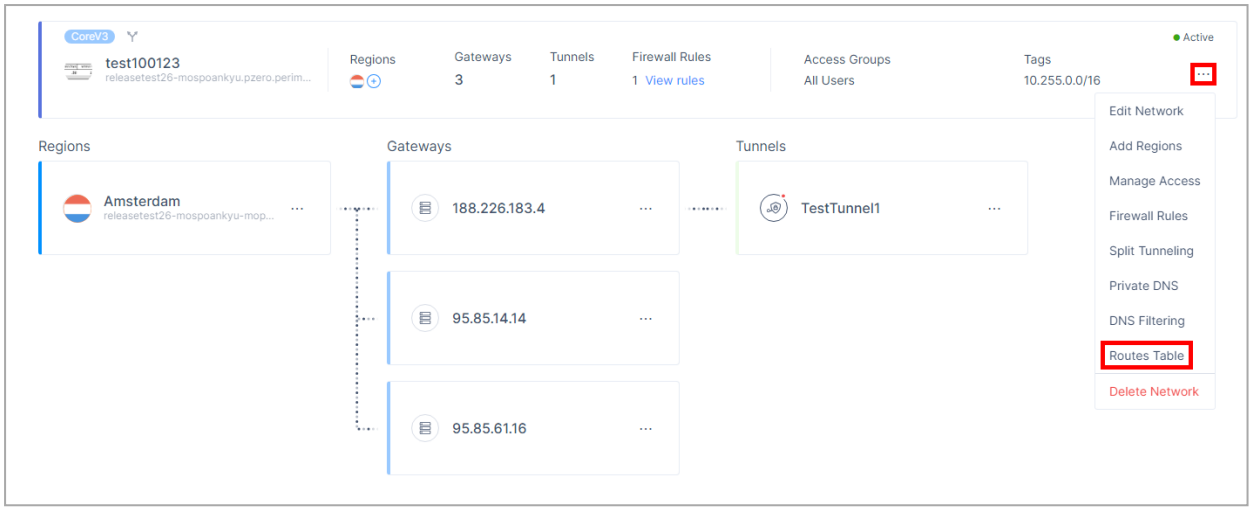
Routes Table

Routes Table shows the routes created for the tunnels in your network.

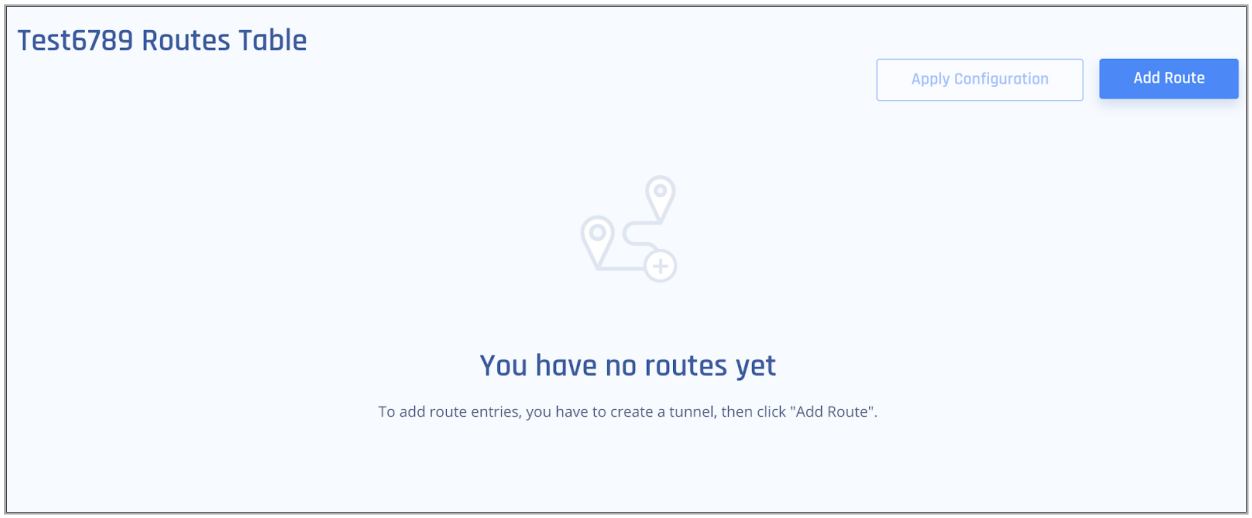


To add a new route to a tunnel in your network:

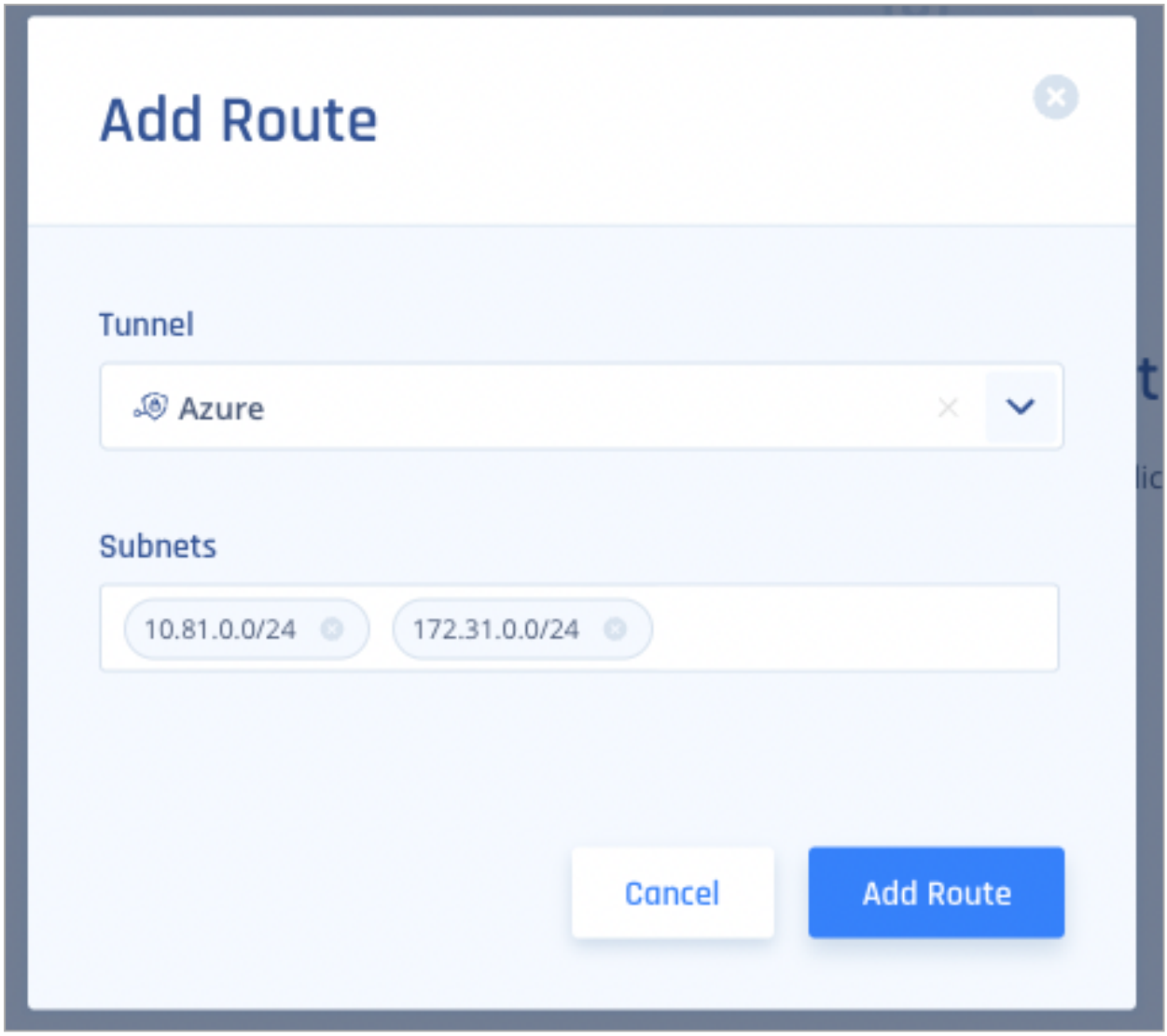
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· at the right end of the network and then select **Routes Table**.



4. Click **Add Route**.

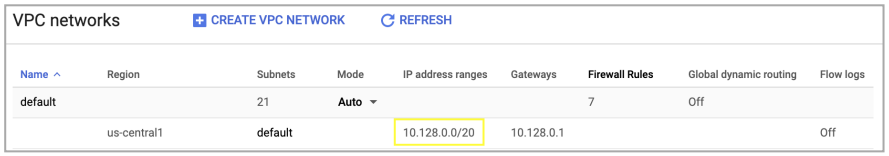


5. Enter all the subnets on the remote side of the tunnel and then click **Add Route**.

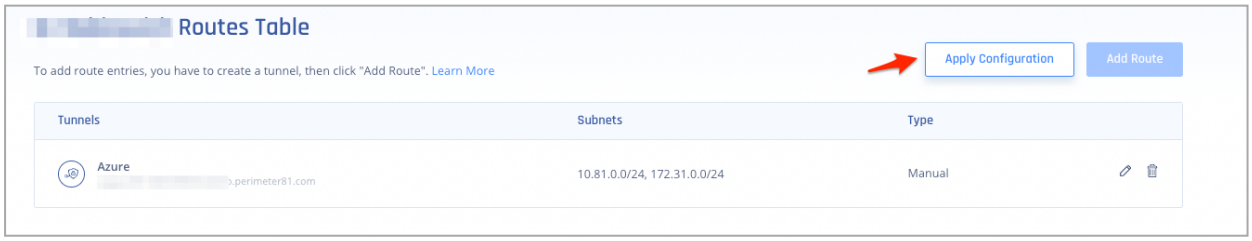


For cloud-based resources, enter these values for your vendor.

Tunnel Type	Subnets
Amazon AWS	
AWS Single Tunnel - Transit Gateway	CIDRs of the attached VPCs (The VPCs to which you want to gain access)
AWS Single Tunnel - Virtual Gateway	Subnets you want to reach on the AWS side of the tunnel.

Tunnel Type	Subnets
AWS Redundant Tunnels - Transit Gateway	Subnets you want to reach on the AWS side of the tunnel. **Note** - Ensure that the added route matches the route transmitted by BGP. Any discrepancies, such as incorrect subnetting or supernetting, are strictly prohibited.
AWS Redundant Tunnels - Virtual Private Gateway	
Google Cloud Platform	
Single Tunnel	From the GCP console, copy the subnets of the regions where your resources are installed. 
Redundant Tunnels	
Microsoft Azure	
Single Tunnel - Virtual Network Gateway	Subnets of the regions where your resources are installed.
Redundant Tunnels - Virtual Network Gateway	
Redundant Tunnels - Virtual WAN	

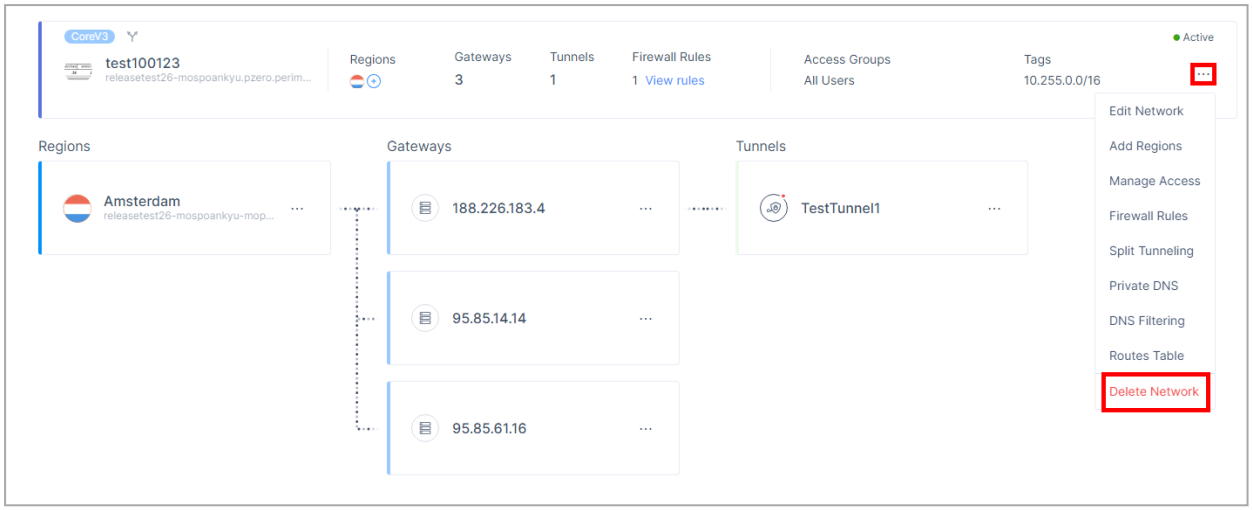
6. Click **Apply Configuration**.



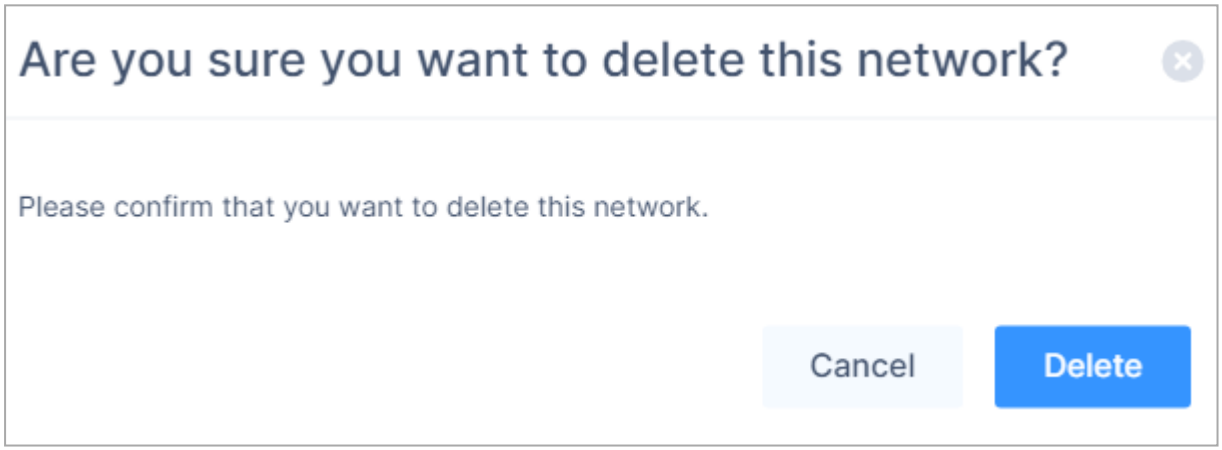
Deleting a Network

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.

3. Click ··· and then click **Delete Network**.



4. Click **Delete**.



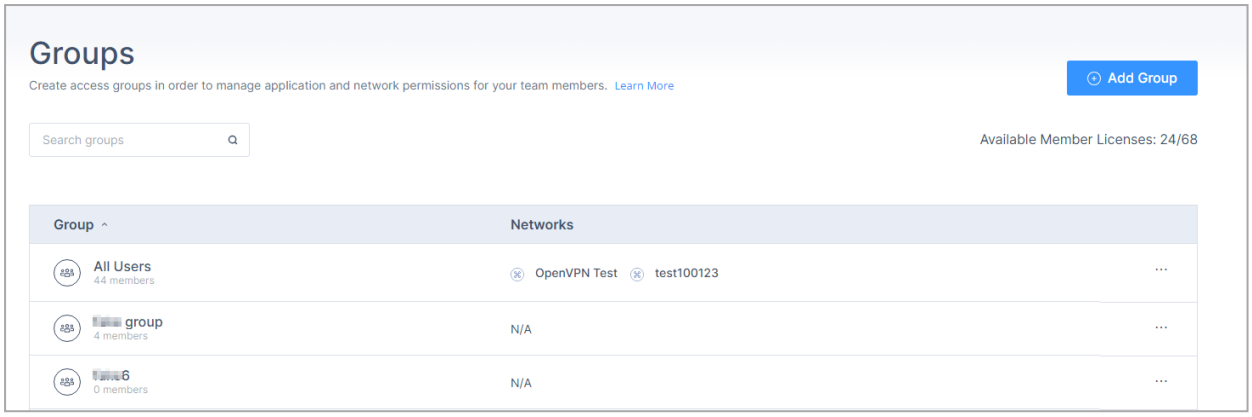
Segmenting Networks

Segmenting networks allows you to limit network access and provide customized member permissions. SASE uses Software-Defined Perimeter (SDP) to segment networks. For example, you can assign member groups to specific parts of a network or only to some of your SDPs.

To segment your network:

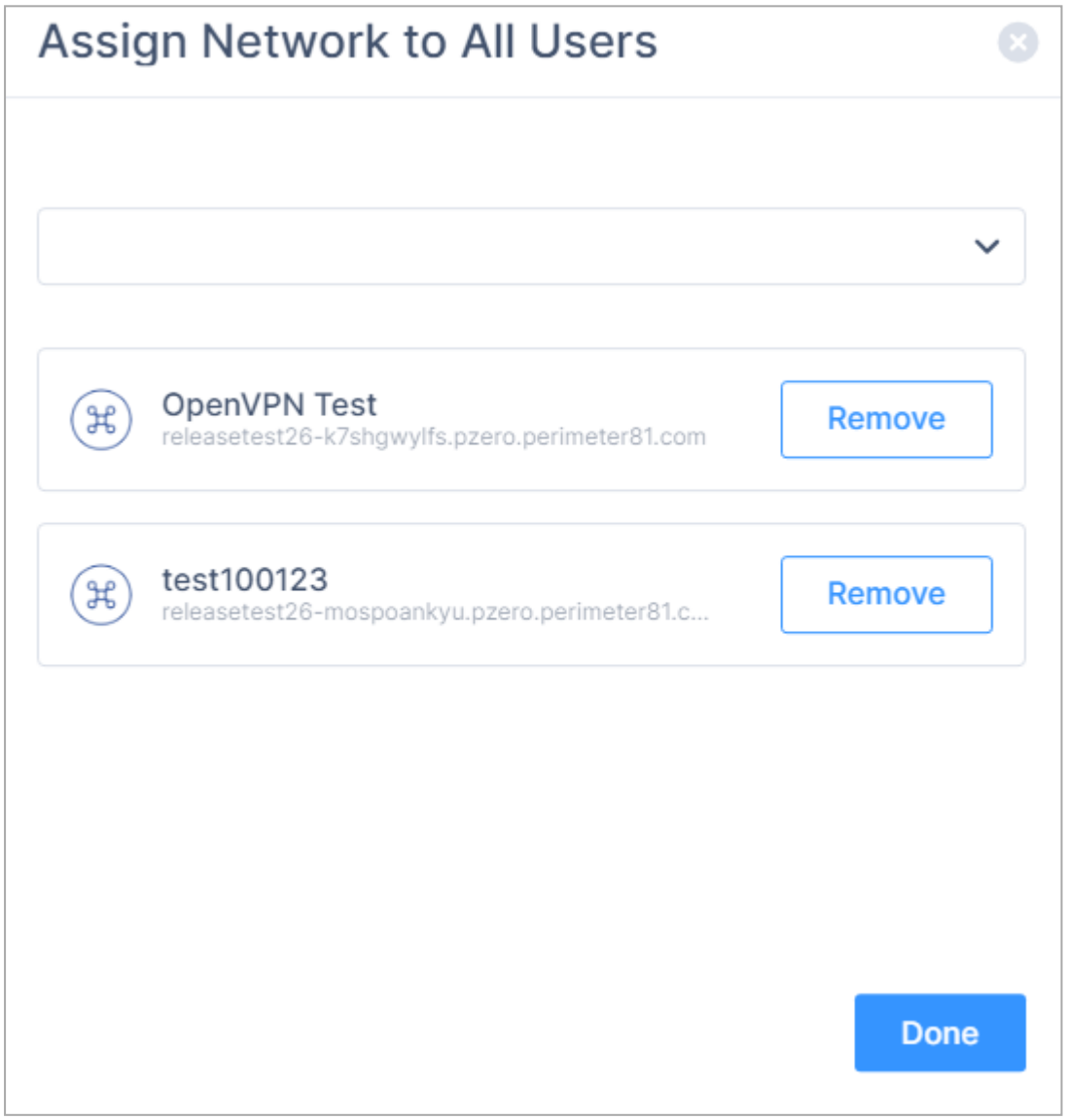
1. Access the SASE Administrator Portal and click **Team** > **Groups**.

   The **Groups** page appears.



2. Click ··· for the group you want to manage the network and then click **Manage Networks**.

   The **Assign Network to Group** window appears.



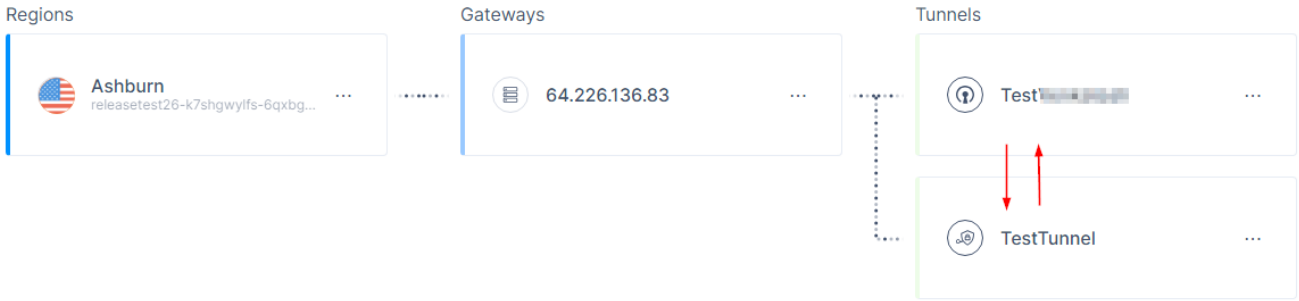
3. From the list, select the networks that the member group can access and click **Done**.

The members can access only the selected network locations when they log in to their client application.

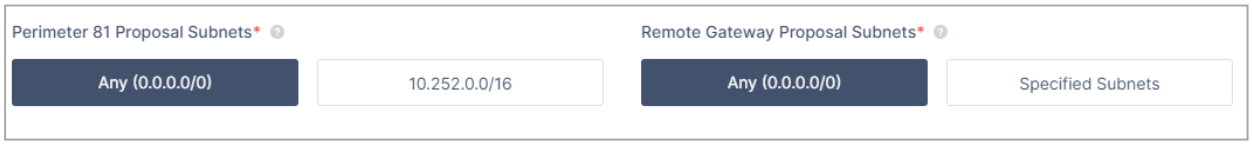
Interconnectivity (Cloud-Agnostic)

This chapter describes how to securely connect sites and cloud resources using Check Point SASE. When two sites are tunneled to your Check Point SASE network, they can securely communicate through this network without the Check Point SASE Agent.

IPSec Based Connections

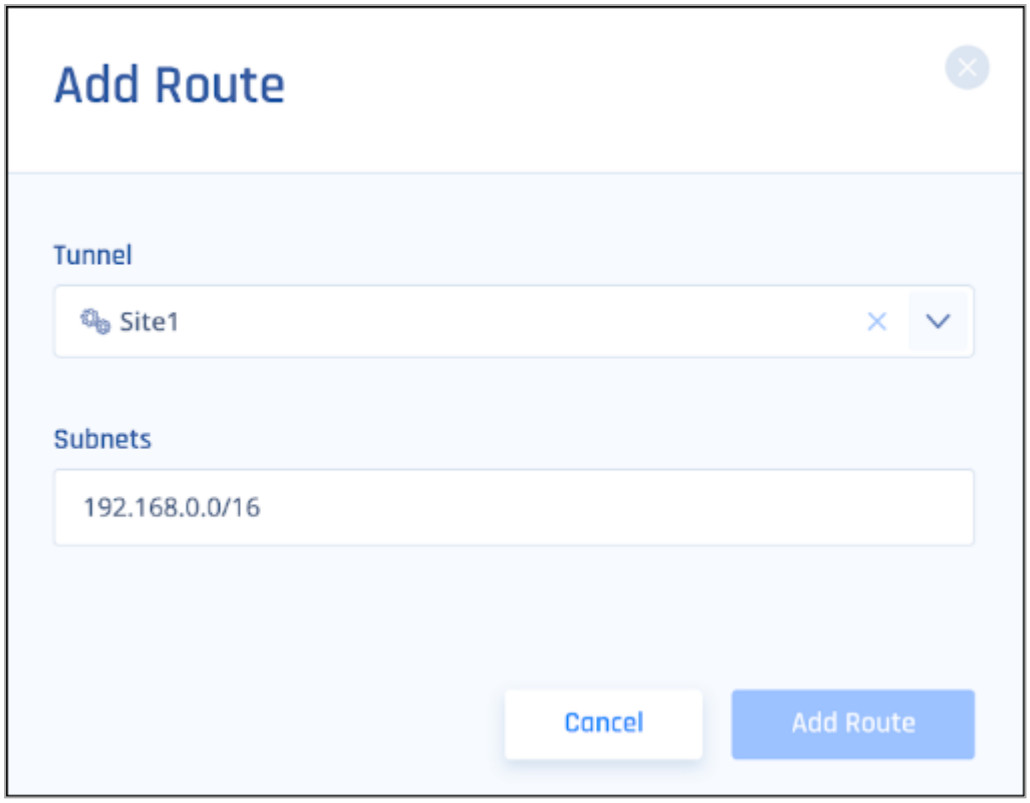


1. Make sure both tunnels are route-based. This means they do not rely on a specific internal subnet for a handshake between sites. Instead, a route is configured on each device's Route Table, to indicate which subnets to send through the tunnel.
2. In the Check Point SASE Administrator Portal, go to your network and set **Perimeter Proposal Subnets** and **Remote Gateway Proposal Subnets** to **ANY (0.0.0.0/0)** for both the tunnels.

   This may make the tunnel go down. Make sure the device you use supports route-based VPN. This means the tunnel is set up to **0.0.0.0/0** and a route is added separately.
3. Make sure the **Routes Table** in the Check Point SASE side has the routes of all of the configured sites.

   To add **Routes Table**, see Adding a route. In the **Subnets** field, add the routing to the internal LAN subnets behind each tunnel.



4. Go to the first site's Routes Table (Site1) and add a route to direct the traffic to the second site's LAN subnet, in addition to the route that indicates all Check Point SASE subnets (usually 10.255.0.0/16) to go through the IPSec Site-2-Site tunnel.
5. Go to the second site's Routes Table (Site2), and set up a static route for both the Check Point SASE LAN Subnet and Site1's LAN subnet to go through the IPSec Site-2-Site tunnel.

Policy-based IPSec Tunnels

To achieve interconnectivity in a Policy-based Site-to-Site environment:

1. Go to the first site's Routes Table (Site1), and ensure that there are two Phase II tunnels:
   - One from Site1's internal subnet to Check Point SASE's subnet.
   - Another from Site1's internal subnet to Site2's internal subnet.
2. Go to the second site's Routes Table (Site2), and ensure that there are two Phase II tunnels:
   - One from Site2's internal subnet to Check Point SASE's subnet.
   - Another from Site2's internal subnet to Site1's internal subnet.

Note - As this feature is not supported by most of the routers, Check Point recommends to use Route-based IPSec tunnels.

WireGuard Connector Based Connections

To establish a connection from one resource to another, you must reinstall the connector, as the default installation (Accessor mode) does not allow it.

1. Uninstall the connector.
   - Ubuntu

     ```
     # Locate the WireGuard packages (the output of this command
     is the full package name)
     dpkg -l | grep wireguard

     # Delete all packages found that are associated with
     WireGuard (replace pkg with the output from the previous
     command)
     apt-get remove --purge pkg
     ```

   - CentOS

     ```
     # Locate the WireGuard packages (the output of this command
     is the full package name)
     yum list installed | grep wireguard

     # Delete all packages found that are associated with
     WireGuard (replace pkg with the output from the previous
     command)
     yum remove pkg
     ```

2. Reboot the machine and execute the connector installation script (the curl command copied from the Check Point SASE Administrator Portal). For more information, see *"Installing the WireGuard Connector on a Linux Server" on page 209*.
3. At Stage 4, select **NO (n)**, which prevents accessor mode installation.
4. To ensure that the default route for the Linux machine is not modified, select **N** for `"Do you want to route whole traffic through connector tunnel? [Y/N]"`.

   Note - In Full Tunnel Mode, the site's entire traffic is sent through the WireGuard connector and the entire firewall is placed behind the Check Point SASE secure network. To operate in this mode:
   a. Select **Y** to override the default route on the machine and forward the traffic through the connector.
   b. Ensure that the Router/Firewall on the network sends all of the route's traffic(0.0.0.0/0) through the internal IP of the WireGuard connector. Follow the instructions below if Linux machine is the router.

5. For `Do you want to enable IP forwarding (router mode)? [Y/N]:`
   - If the Linux server is acting as a firewall, router, or NAT device, select **Y**.
   - For any other device, select **N**.
6. Open the Route Table of the network in which the WireGuard connector is installed (usually your router or firewall).
7. Configure a static route to direct the traffic from your Check Point SASE LAN subnet (10.XXX.0.0/16) and your other desired remote subnet to the IP address of the machine hosting the connector.

   Open the Linux machine terminal that hosts the connector and run:

```
# Temporarily shut the connector down
wg-quick down wg0
# Open the connector's route table.
vi /etc/wireguard/wg0.conf
# Enter the subnets of the resources you'd like to communicate
with each other
set AllowedIPs = <Harmony SASE Subnet>, <Site1 Subnet>,< Site 2
Subnet>
# Turn the connector up
wg-quick up wg0
# Make sure that the desired change has taken place
wg show
```

Interconnectivity Using AWS EC2 Instance

For WireGuard connector installed over AWS EC2 instance, you must disable the source/destination checks.

To disable source/destination checks:

1. Log in to Amazon EC2 console.
2. In the navigation pane, click **Instances** and select the relevant instance.
3. Select **Actions**, **Networking**, **Change source/destination check**.
4. For **Source/destination checking** , select **Stop**.
5. Click **Save**.
6. If the instance has a secondary network interface:
   a. Go to **Networking** tab > **Network interfaces** and select the secondary network interface.

b. Select the interface ID and go to the **Network Interfaces** page.

c. Select **Actions**, **Change source/dest. check**.

d. Clear the **Enable** checkbox.

e. Click **Save**.

Integrating On-premises Firewall / Router or Cloud based Resources

High-Level Procedure

1. Make sure you have the required prerequisites.
2. For on-premises firewall and routers:

a. Configure the tunnel in the SASE Administrator Portal.

b. Configure the required Firewall / Router / Cloud Management Portal:

On-premises	
Firewall	**Router**
■ *"Barracuda Firewall" on page 258* ■ *"Check Point Firewall" on page 268* ■ *"Cisco Firepower" on page 279* ■ *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 300* ■ *"Configuring Check Point Redundant IPsec Tunnel" on page 326* ■ *"Cisco ASA Firewall" on page 382* ■ *"Cisco Meraki Router" on page 506* ■ *"FortiGate Next Generation Firewall" on page 416* ■ *"Juniper Networks ScreenOS Firewall" on page 420* ■ *"Juniper (JunOS) SRX Firewall" on page 426* ■ *"Palo Alto Firewall" on page 439* ■ *"Palo Alto Redundant Tunnel" on page 446* ■ *"pfSense Firewall" on page 466* ■ *"SonicWall Firewall" on page 472* ■ *"Sophos XG Firewall" on page 482* ■ *"UniFi USG Firewall" on page 488* ■ *"WatchGuard Firewall" on page 494* ■ *"Zyxel USG Firewall" on page 500*	■ *"Cisco Meraki Router" on page 506* ■ *"D-Link DSR Series Router" on page 509* ■ *"DrayTek Vigor2862 Router" on page 516* ■ *"DrayTek Vigor3900 Router" on page 519* ■ *"EdgeMax Router" on page 526* ■ *"Linksys Router" on page 528* ■ *"Netgear BR500 Router" on page 532*

3. For cloud-based resource, configure any of these:

Single Tunnel

- *"AWS Virtual Gateway" on page 555*
- *"AWS Transit Gateway" on page 575*
- *"Google Cloud Platform" on page 687*
- *"Azure Virtual Network Gateway" on page 623*

Redundant Tunnels

- *"AWS Redundant Tunnels - Virtual Private Gateway" on page 592*
- *"AWS Redundant Tunnels - Transit Gateway" on page 606*
- *"Google Cloud Platform (GCP) Redundant Tunnels" on page 700*
- *"Azure Virtual Network Gateway Redundant Tunnels" on page 649*
- *"Azure Virtual WAN Redundant Tunnels" on page 667*

Other Cloud Options

- *"Alibaba Cloud" on page 546*
- *"Heroku Enterprise" on page 722*
- *"IBM Cloud" on page 723*

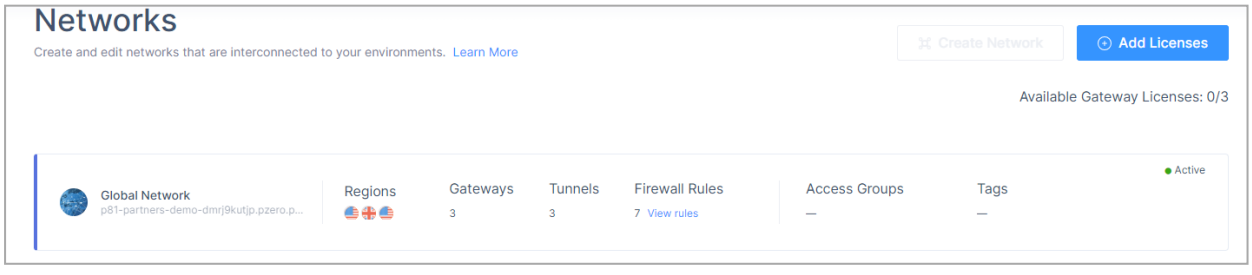
4. Verify the setup.

Prerequisites

- Check Point SASE Administrator Portal account.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account with the Firewall/Router/Cloud Management Portal.

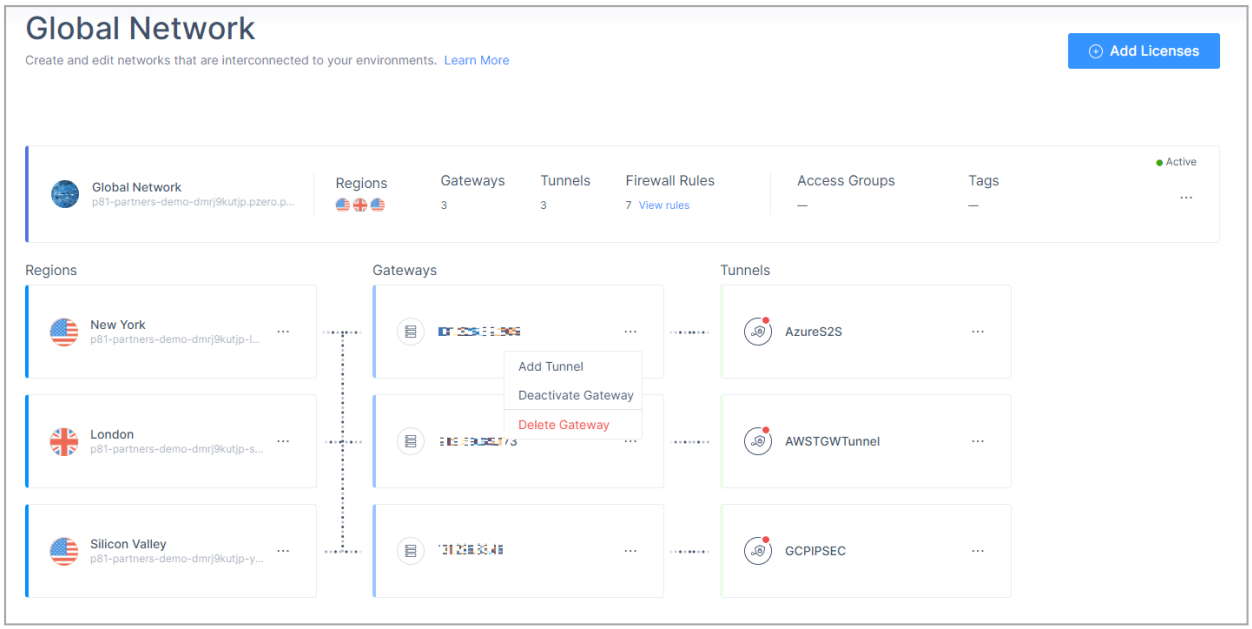
Configuring the Tunnel in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network.

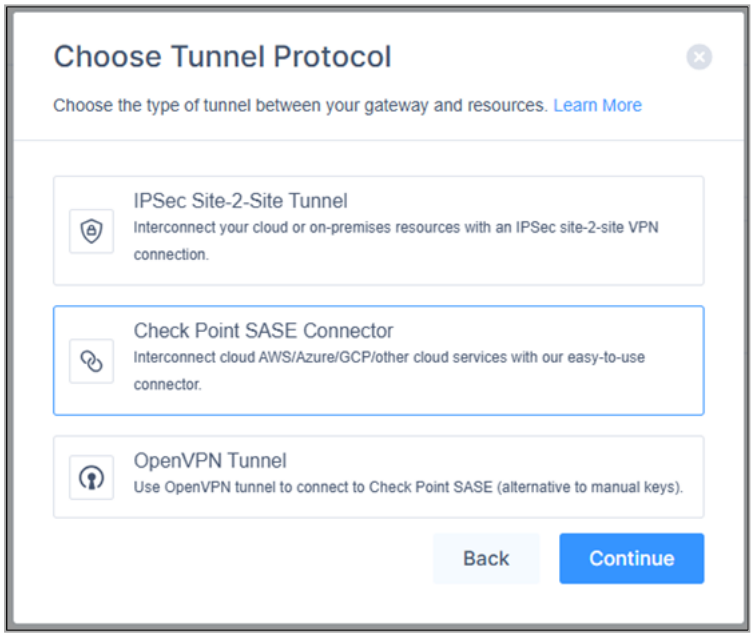


3. Click ... and select **Add Tunnel** for the gateway from which you want to add the IPSec Site-to-Site VPN tunnel.

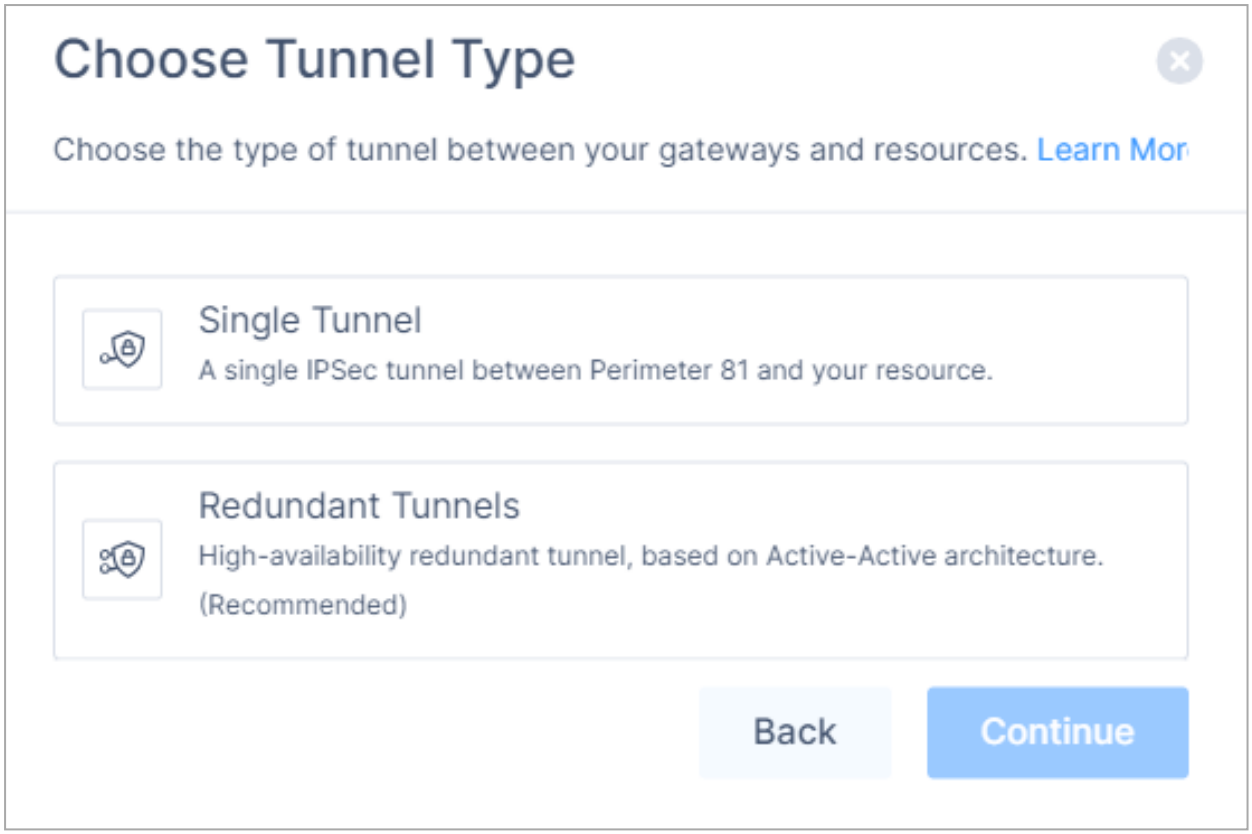
Note - Only a single dynamic IP IPSec tunnel is supported per each Cloud Gateway.



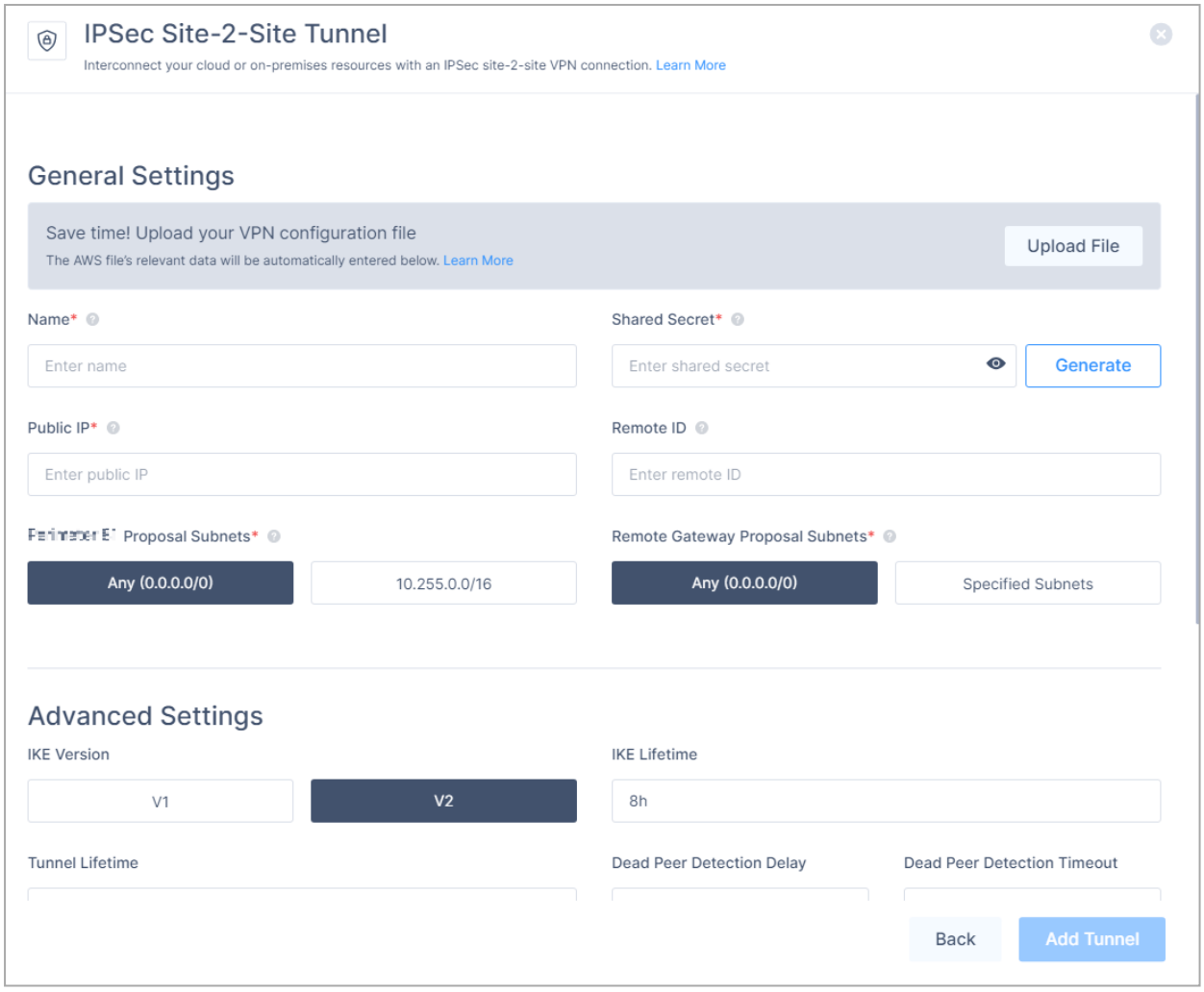
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



6. In the **General Settings** section, enter the relevant details:



Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Check Point SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Barracuda Firewall" on page 258	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Barracuda Firewall Public WAN IP address.	Barracuda Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Barracuda internal LAN subnets.
"Check Point Firewall" on page 268	Name for the tunnel.	Enter the secret key specified in Check Point SmartConsole or click **Generate** to generate it.	Public or Egress IP address of Check Point Firewall	Public or Egress IP address of Check Point	Any (0.0.0.0)	Any (0.0.0.0)

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Check Point SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Cisco ASA Firewall" on page 382	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Cisco ASA Firewall Public WAN IP address.	Cisco ASA Firewall Public WAN IP address.	Any (0.0.0.0)	Any (0.0.0.0)
"Cisco Meraki Router" on page 506	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Cisco Meraki Router Public WAN IP address.	Cisco Meraki Router Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Cisco Meraki internal LAN subnets.
"D-Link DSR Series Router" on page 509	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	D-Link DSR Series Router Public WAN IP address.	D-Link DSR Series Router Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	D-Link DSR Series Router internal LAN subnets.
"DrayTek Vigor2862 Router" on page 516	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	DrayTek Vigor3900 Router Public WAN IP address.	DrayTek Vigor3900 Router Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	DrayTek Vigor internal LAN subnets.
"DrayTek Vigor3900 Router" on page 519	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	DrayTek Vigor2862 Router Public WAN IP address.	Name for the VPN profile on the DrayTek Vigor2862 Router.	Check Point SASE network subnet. The default is 10.255.0.0/16.	DrayTek Vigor internal LAN subnets.
"EdgeMax Router" on page 526	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	EdgeMax Router Public WAN IP address.	EdgeMax Router Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	EdgeMax internal LAN subnets.
"FortiGate Next Generation Firewall" on page 416	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	FortiGate Next Generation Firewall public IP address.	FortiGate Next Generation Firewall remote ID.	Check Point SASE network subnet. The default is 10.255.0.0/16.	FortiGate Next Generation Firewall internal LAN subnets.
"Linksys Router" on page 528	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Linksys public WAN IP address.	Linksys public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Linksys internal LAN subnets.

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Check Point SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Juniper Networks ScreenOS Firewall" on page 420	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Juniper Networks ScreenOS Firewall Public WAN IP address.	Juniper Networks ScreenOS Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Juniper Networks ScreenOS internal LAN subnets.
"Juniper (JunOS) SRX Firewall" on page 426	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Juniper SRX Firewall Public WAN IP address.	Juniper SRX Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Juniper Networks ScreenOS internal LAN subnets.
"Netgear BR500 Router" on page 532	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Netgear BR500 Router Public WAN IP address.	Netgear BR500 Router Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Netgear BR500 internal LAN subnets.
"Palo Alto Firewall" on page 439	Name for the tunnel.	Enter the secret key specified in the Palo Alto Management Portal.	External internal IP address of Palo Alto Firewall. You can obtain this from **Interfaces > Ethernet** in the Palo Alto Management Portal.	External internal IP address of Palo Alto Firewall. You can obtain this from **Interfaces > Ethernet** in the Palo Alto Management Portal. If NAT is configured, then enter the internal LAN IP address of the Palo Alto Firewall.	Any (0.0.0.0)	Any (0.0.0.0)
"pfSense Firewall" on page 466	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	pfSense Firewall Public WAN IP address.	pfSense Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	pfSense internal LAN subnets.

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Check Point SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"SonicWall Firewall" on page 472	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	SonicWall Firewall Public WAN IP address.	SonicWall Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	SonicWall internal LAN subnets.
"Sophos XG Firewall" on page 482	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Sophos XG Firewall Public WAN IP address.	Sophos XG Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Sophos XG internal LAN subnets.
"UniFi USG Firewall" on page 488	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	UniFi USG Firewall Public WAN IP address.	UniFi USG Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	UniFi USG internal LAN subnets.
"WatchGuard Firewall" on page 494	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	WatchGuard Firewall Public WAN IP address.	WatchGuard Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	WatchGuard internal LAN subnets.
"Zyxel USG Firewall" on page 500	Name for the tunnel.	Enter a secret key or click **Generate** to generate it	Zyxel USG Firewall Public WAN IP address.	Zyxel USG Firewall Public WAN IP address.	Check Point SASE network subnet. The default is 10.255.0.0/16.	Zyxel USG internal LAN subnets.

[1]This is the public IP address of the second end of the tunnel.

[2] In most cases, the ID of the remote tunnel is the public IP of the tunnel. However, it must be configured to the same value on both ends.

[3] The IPSec network selector must be configured to the same value at both ends of the tunnel.

7. In the **Advanced Settings** section, enter the relevant details:

Field Firewall/Router	IKE Version[1] [2]	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Barracuda	V2	8h	1h	10s	30s	aes256	aes256	SHA	SHA	modp1024	modp1024
Check Point	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Cisco ASA	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Cisco Meraki	V1	8h	1h	10s	50s	aes256	aes256	sha1	sha1	modp1536	modp1536
D-Link DSR Series Router	V1	8h	1h	30s	10s	aes256	aes256	sha512	sha512	modp1536	modp1536
DrayTek Vigor2862	V2	8h	1h	30s	60s	aes256	aes256	sha1	sha1	modp1024	modp1024
DrayTek Vigor3900	V1	8h	1h	30s	60s	aes256	aes256	sha1	sha1	modp1536	modp1536
EdgeMax	V1	8h	1h	15s	30s	aes256	aes256	sha1	sha1	modp2048	modp2048
FortiGate Next Generation Firewall	V2	8h	1h	10s	30s	Default value	Default value	Default value	Default value	ecp521	ecp521

Field / Firewall/Router	IKE Version[1][2]	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Linksys	V2	8h	1h	30s	10s	aes256	aes256	sha1	sha1	modp1536	modp1536
Juniper Networks ScreenOS	V1	8h	1h	10s	50s	aes256	aes256	sha1	sha1	modp1536	modp1536
Juniper Networks SRX	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Netgear BR500	V2	8h	1h	30s	10s	aes256	aes256	sha1	sha1	modp1536	modp1536
Palo Alto	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
pfSense	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
SonicWall	V2	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Sophos XG	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	modp2048	modp2048
UniFi USG	V2	8h	8h	10s	30s	aes256	aes256	sha1	sha1	ecp521	ecp521
WatchGuard	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Zyxel USG	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048

[1] If **V2** is not supported, select **V1**.

[2] For dynamic IP tunnels, select **V2**.

8. Click **Add Tunnel**.

On-premises Firewall - Configuring the Tunnel in the Management Portal

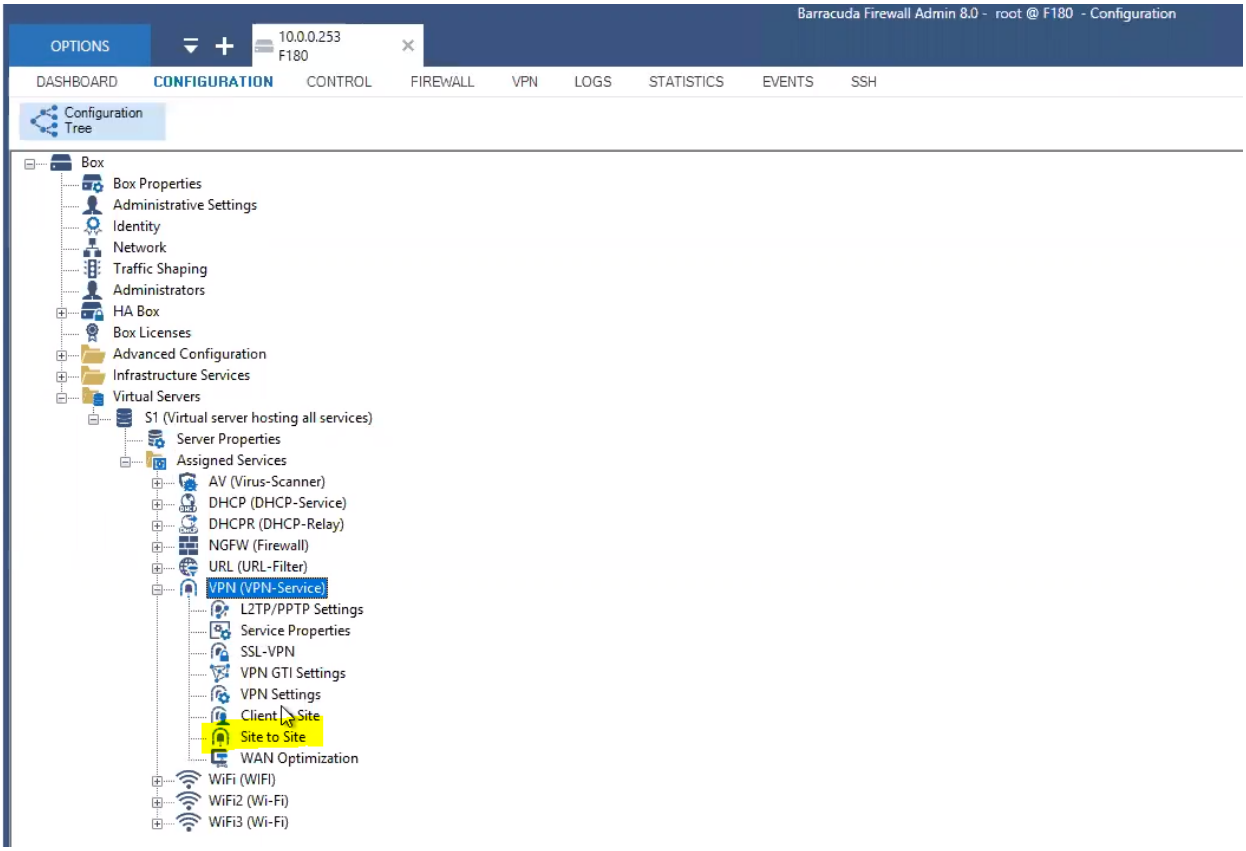
Check Point SASE supports these on-premises firewall devices for the IPSec Site-2-Site VPN tunnel connection with the Check Point SASE gateway:

- *"Barracuda Firewall" on page 258*
- *"Check Point Firewall" on page 268*
- *"Cisco Firepower" on page 279*
- *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 300*
- *"Configuring Check Point Redundant IPsec Tunnel" on page 326*
- *"Cisco ASA Firewall" on page 382*
- *"Cisco Meraki Router" on page 506*
- *"FortiGate Next Generation Firewall" on page 416*
- *"Juniper Networks ScreenOS Firewall" on page 420*
- *"Juniper (JunOS) SRX Firewall" on page 426*
- *"Palo Alto Firewall" on page 439*
- *"Palo Alto Redundant Tunnel" on page 446*
- *"pfSense Firewall" on page 466*
- *"SonicWall Firewall" on page 472*
- *"Sophos XG Firewall" on page 482*
- *"UniFi USG Firewall" on page 488*
- *"WatchGuard Firewall" on page 494*
- *"Zyxel USG Firewall" on page 500*

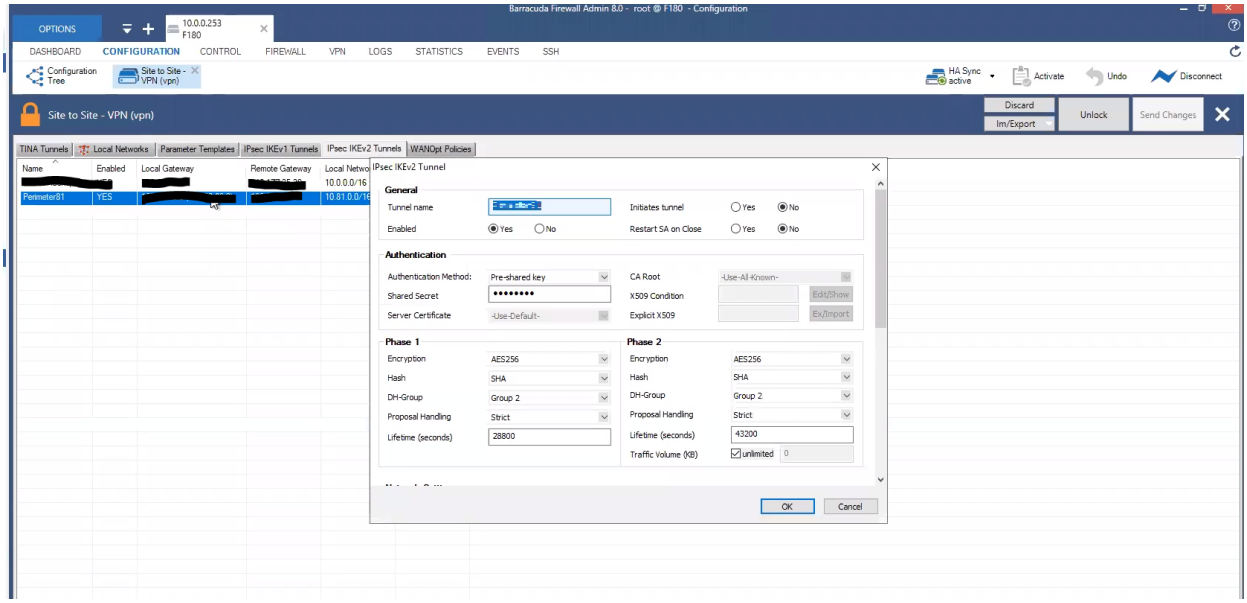
Barracuda Firewall

To configuring the tunnel in the Barracuda Management Portal:

1. Log in to the Barracuda Management Portal with the Administrator account.
2. From the top menu, click **Configuration > Virtual Servers > Your virtual server > Assigned Services > VPN (VPN-Service) > Site to Site**.



3. In the **IPsec IKEv2 Tunnels** tab, create a new tunnel:



a. In the **General** section:

   i. In the **Tunnel Name** field, enter a tunnel name.

   ii. Leave the rest of fields to default settings.

b. In the **Authentication** section:

   i. From the **Authentication Method** list, select Pre-shared key.

   ii. In the **Shared Secret** field, enter the same secret key that you specified in step **6** in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.

   iii. Leave the rest of fields to default settings.

c. In the **Phase 1** section:

Field	Enter
Encryption	AES256
Hash	SHA
Diffie-Hellman Group	2
Proposal Handling	Strict
Lifetime	28800

d. In the **Phase 2** section:

Field	Enter
Encryption	AES256
Hash	SHA
DH-Group	2
Proposal Handling	Strict
Lifetime	3600
Traffic Volume (KB)	Unlimited

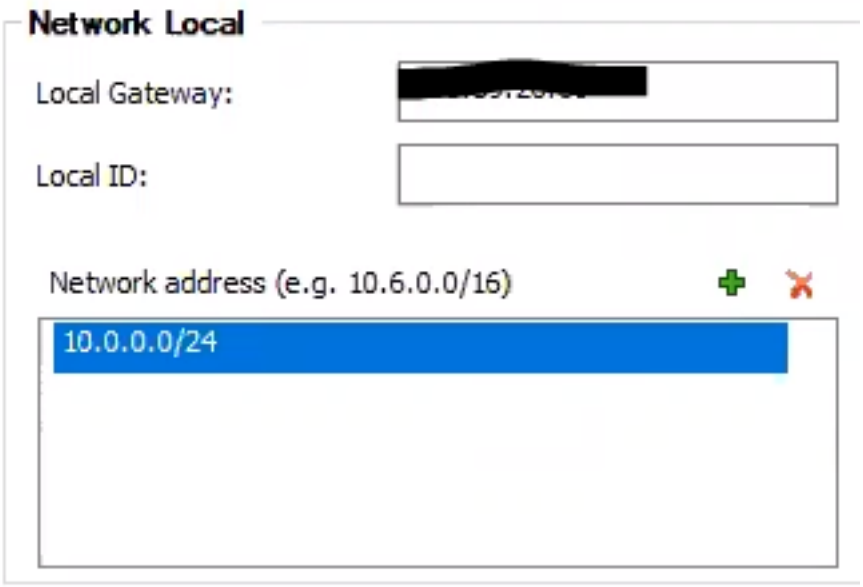
4. Click **Configuration > Site to Site VPN (vpn)**:

a. Create a new site-to-site VPN or edit an existing one.

b. In the **IPSec IKEv2 Tunnel** selection:

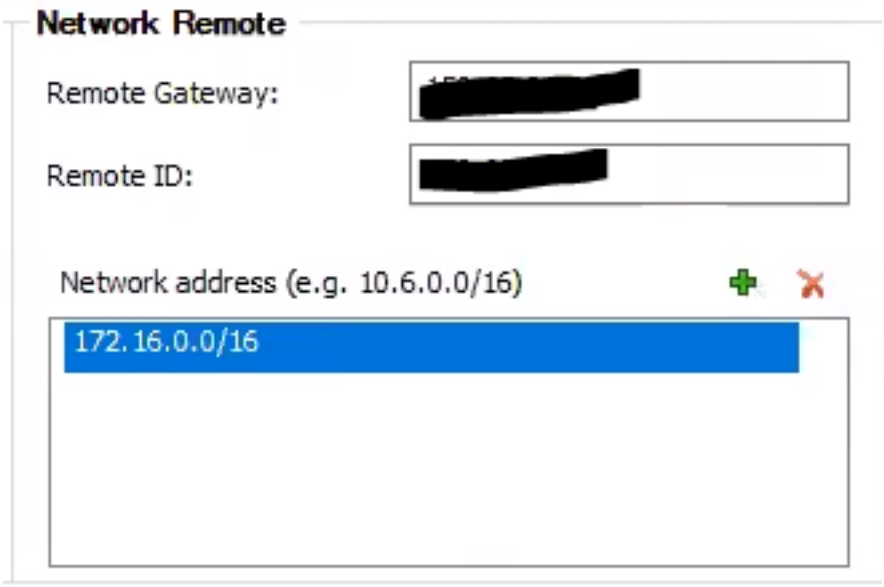
Field	Enter
Endpoint Type	IPv4
One VPN Tunnel per Subnet Pair	Clear
Universal Traffic Selectors	Clear
Force UDP Encapsulation	Clear
IKE Reauthentication	Select
Next Hop Routing	0.0.0.0
Interface Index	0

c. In the **Network Local** selection:



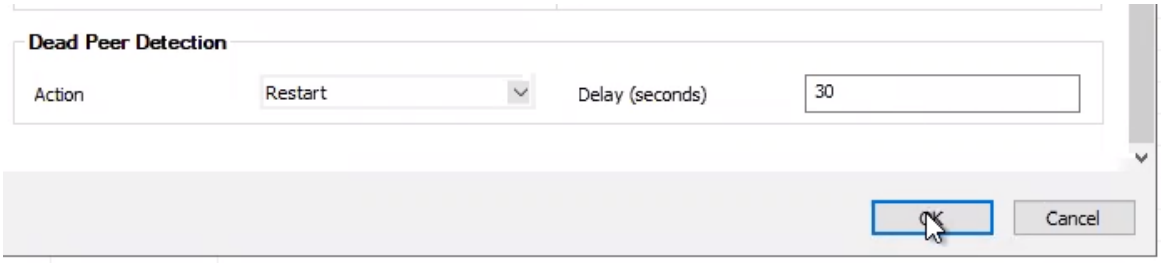
Field	Enter
Local Gateway	Barracuda Firewall Public IP address
Local ID	Barracuda Firewall Public IP address
Network address	Internal network subnets

d. In the **Network Remote** selection:



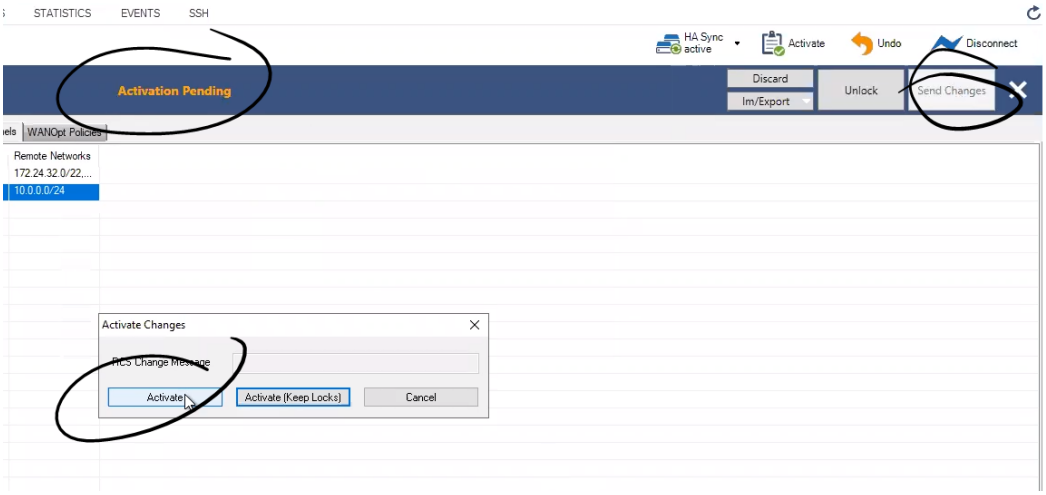
Field	Enter
Remote Gateway	Check Point SASE Public IP address
Remote ID	Check Point SASE Public IP address
Network address	Check Point SASE network subnets

e. In the **Dead Peer Detection** selection:



Field	Enter
Action	Restart
Delay (seconds)	30

f. Click **OK**.

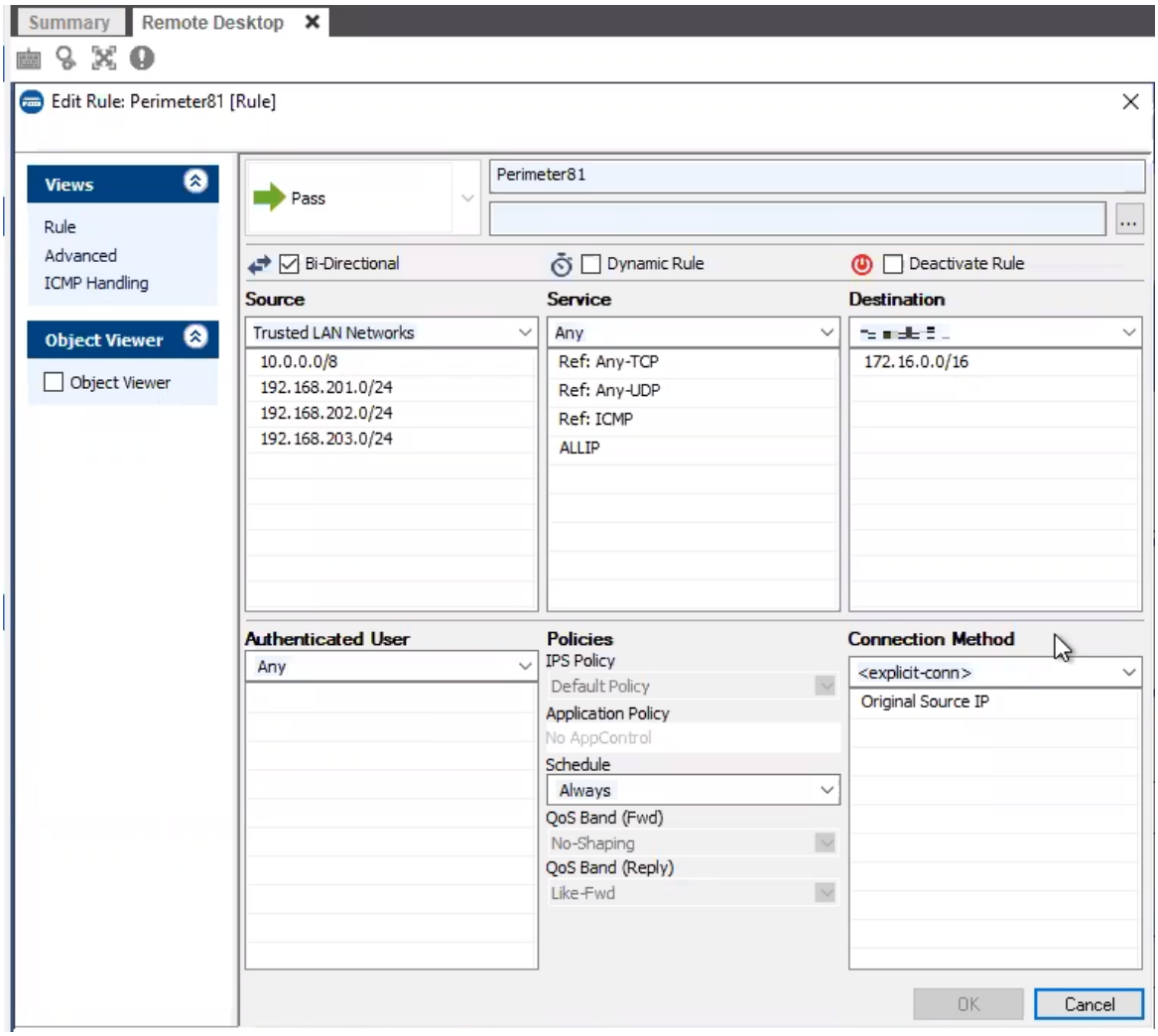


g. Click **Send Changes**.

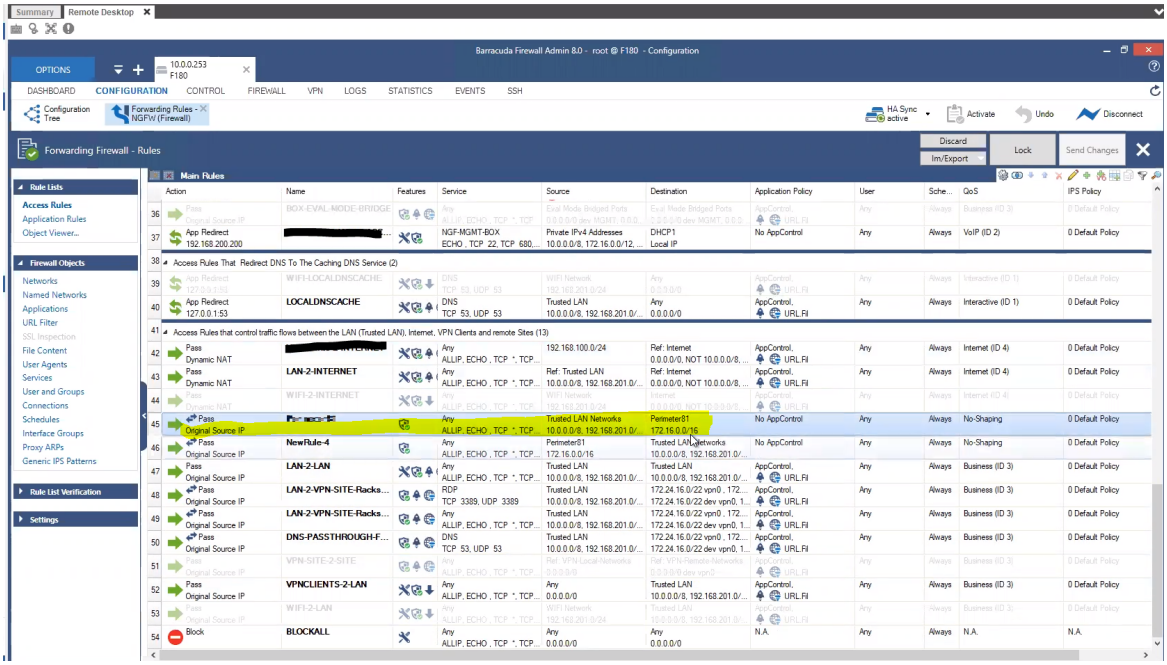
h. Click **Activate**.

5. Click **Firewall > Forwarding Rules**:

a. Add Check Point SASE gateway public IP address to the allow-list.

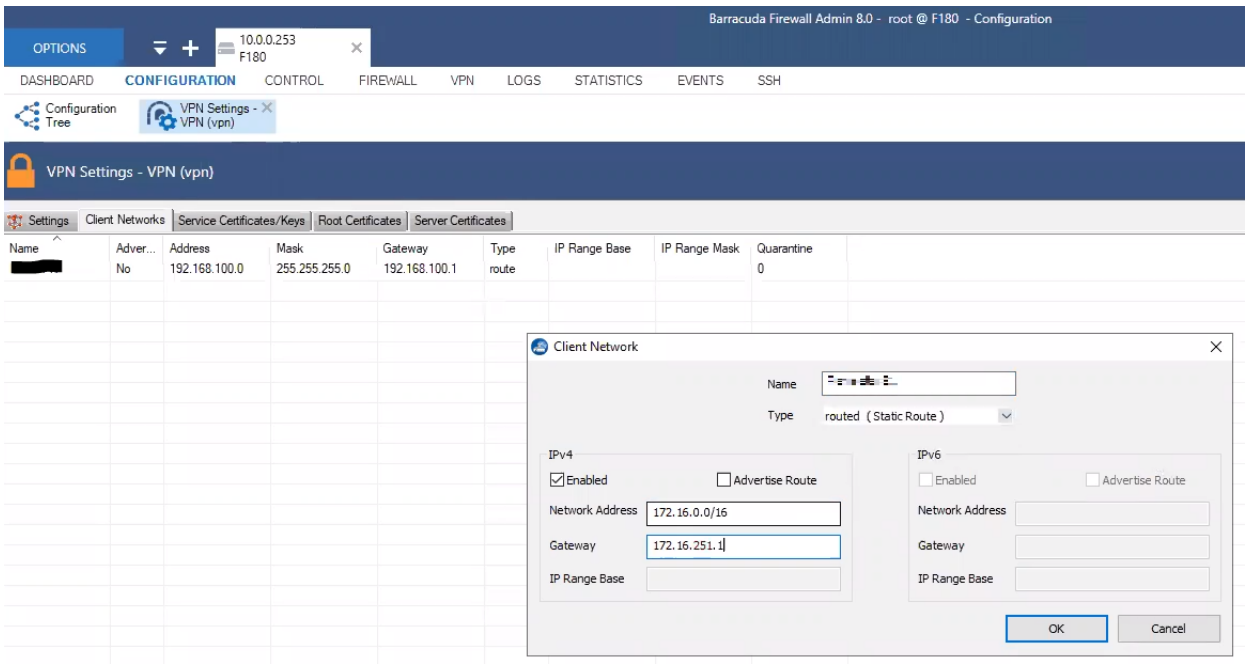


b. Ensure that the Check Point SASE gateway public IP address is listed under the firewall rules.



c. Add the static routes from the Check Point SASE subnet (10.XXX.0.0/16) to the local network and from the local network to the Check Point SASE subnet (10.XXX.0.0/16) through the VPN tunnel gateway.

6. Click **Configuration > Site to Site VPN (vpn)**:

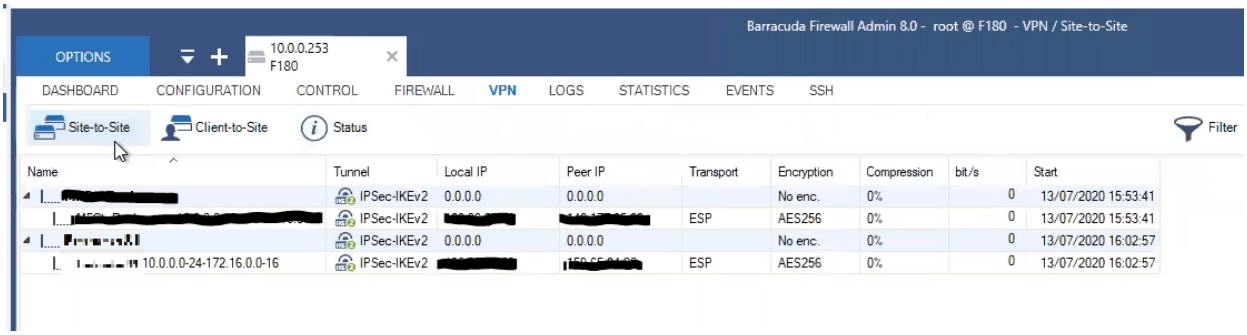


a. In the **Client Networks** tab:

Field	Enter
Network Address	172.xxx.0.0/16 (or relevant subnet0
Gateway	Local Barracuda IP address
Name	Tunnel name.

b. Click **OK**.

7. To verify that the tunnel is up, go to **VPN > Site-to-Site**. If the tunnel is listed in the table, then the tunnel is up.



Check Point Firewall

You can establish a Single Site-to-Site VPN tunnel between your SASE.

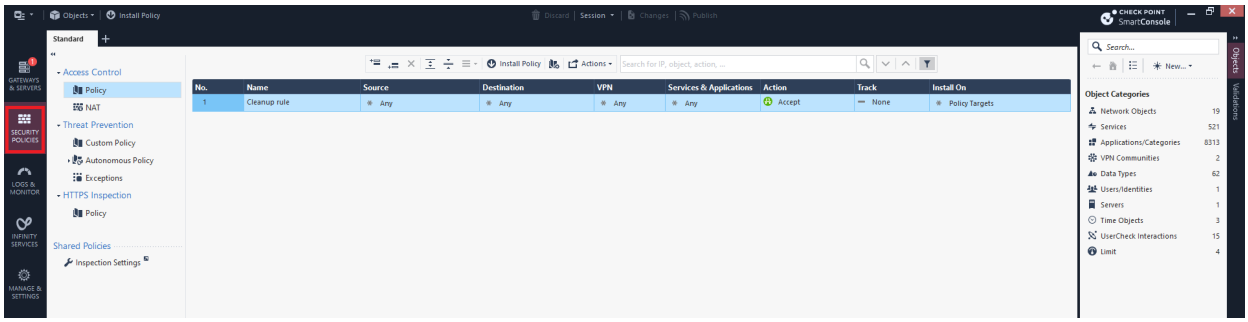
Pre-requisites

- SASE Administrator Portal account.
- Make sure that you have installed the SASE Agent on your device.
- Administrator account with Firewall/Router/Cloud Management Portal.

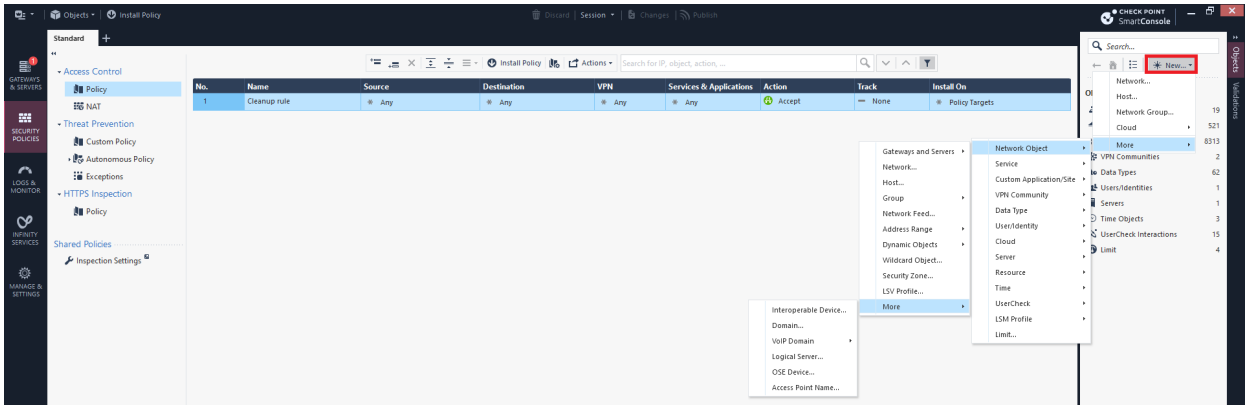
Configuration Steps

Creating Interoperable Device Object in the Check Point SmartConsole

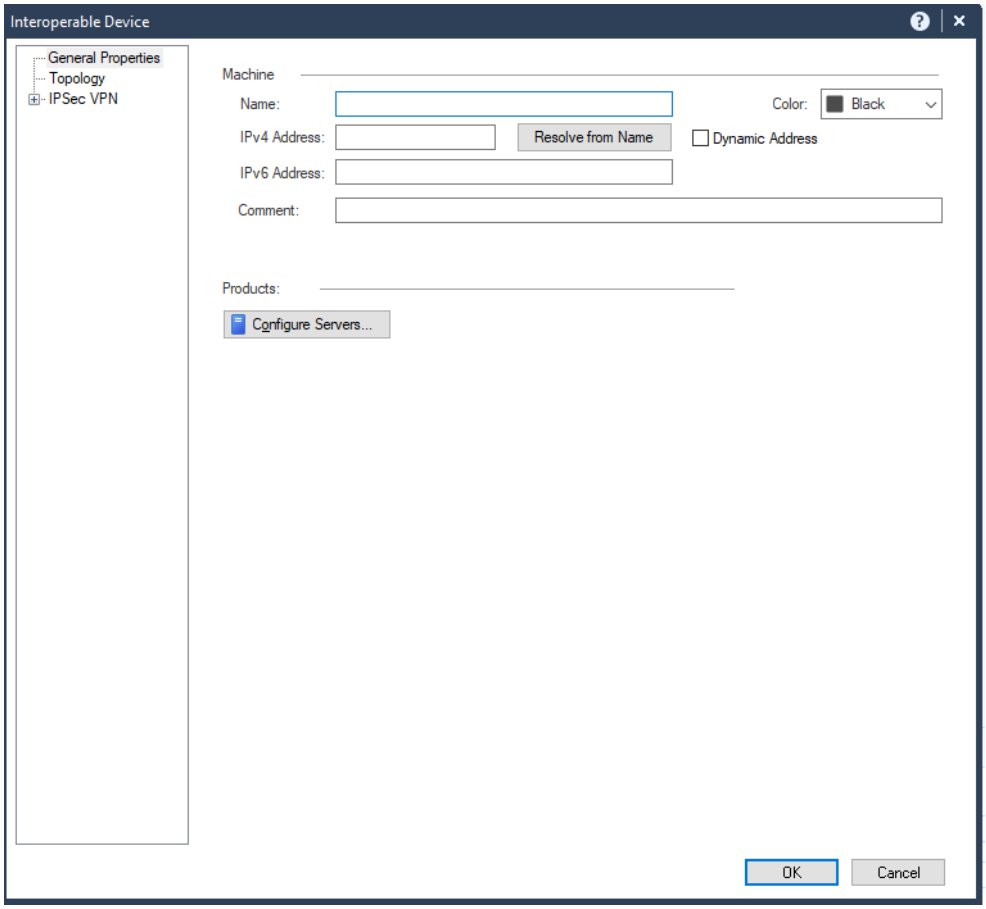
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. On the top right, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



a. In the **Name** field, enter a name for Check Point SASE gateway.

b. In the **IPv4 Address** field, enter the Check Point SASE gateway public IP address.

   To find the SASE Gateway public IP Address:

   i. Access the SASE Administrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

c. Click **OK**.

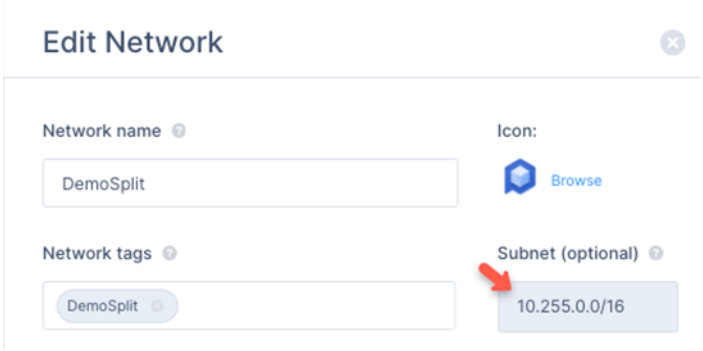
Adding SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object

1. Log in to the SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network. The default value is 10.255.0.0/16.
4. To verify:

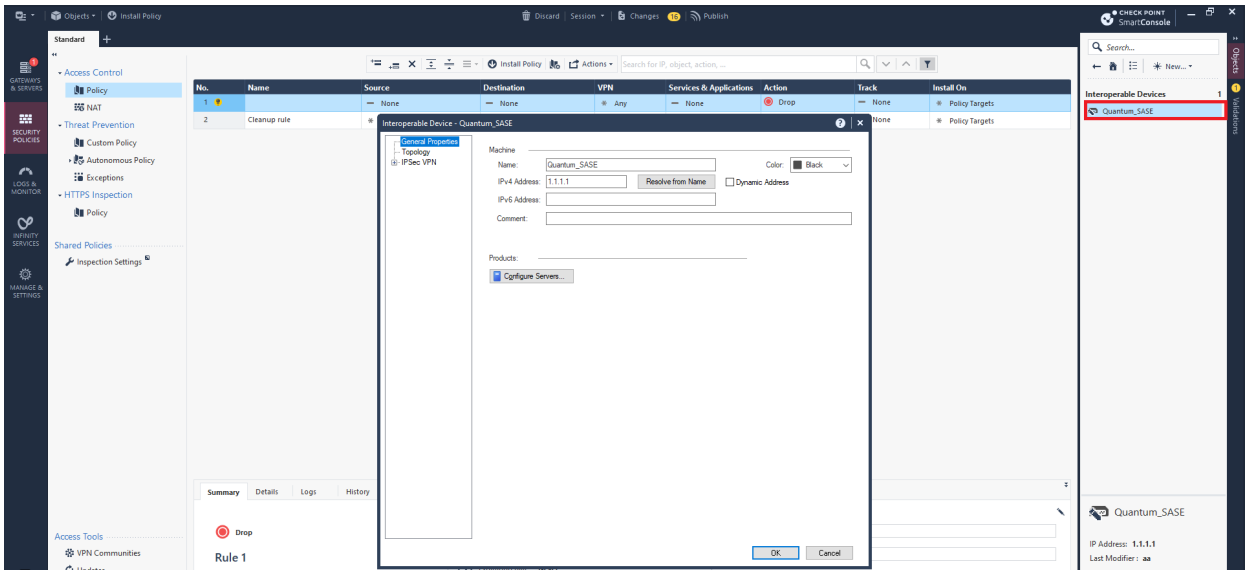
a. Select a network, scroll to the end of the row and click ... .

b. Select **Edit Network.**

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

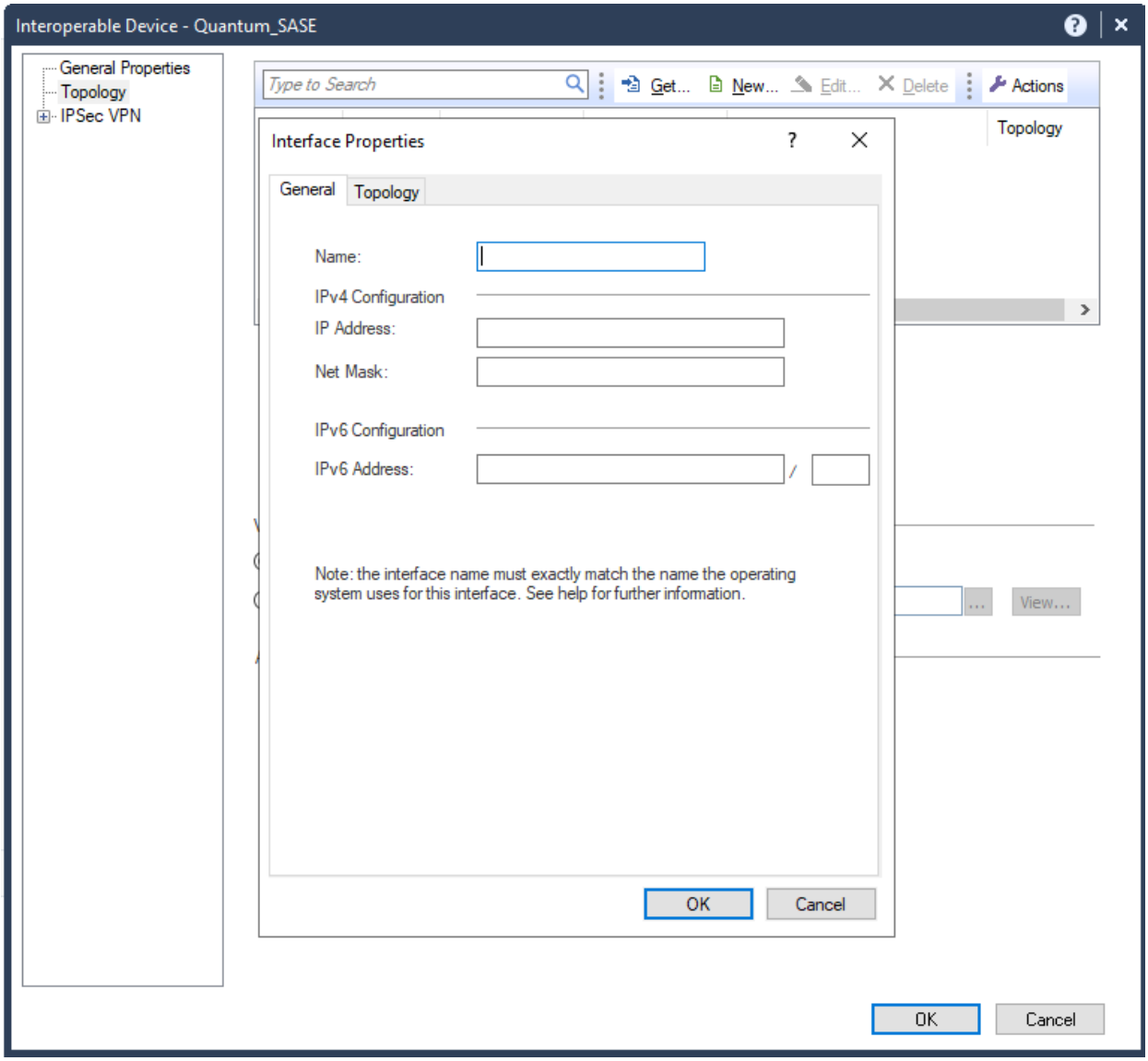


5. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

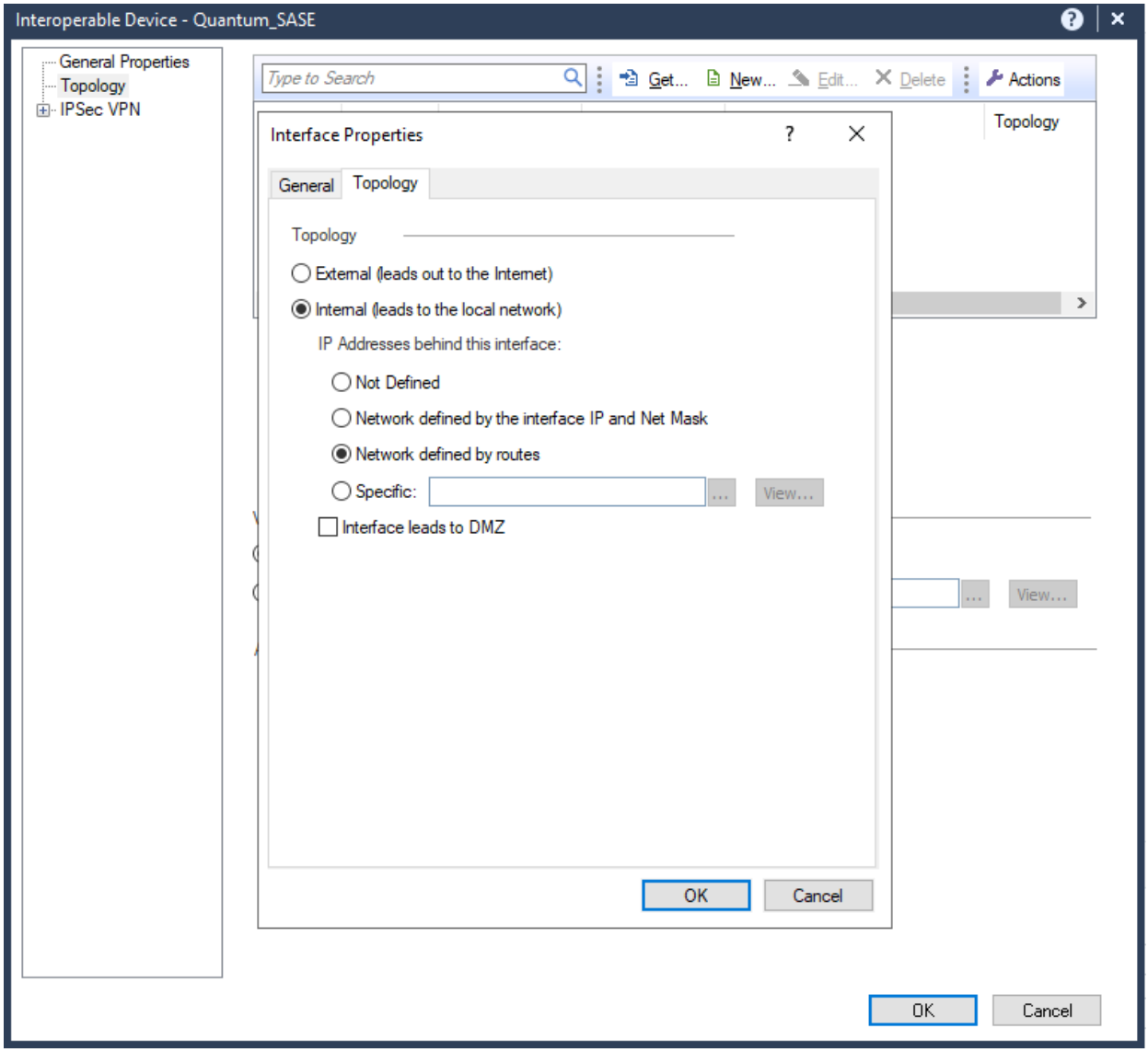
6. Click **Topology > New**.



7. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

8. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



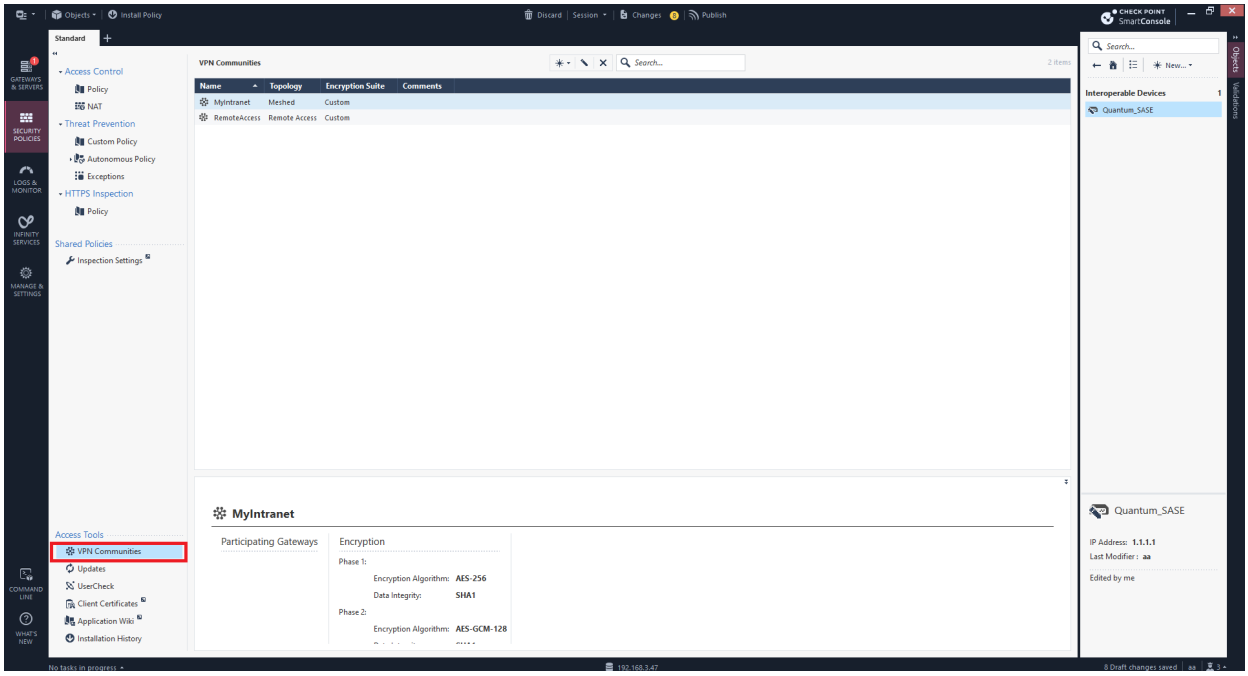
9. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Check Point SASE gateway.
Net Mask	255.255.255.255

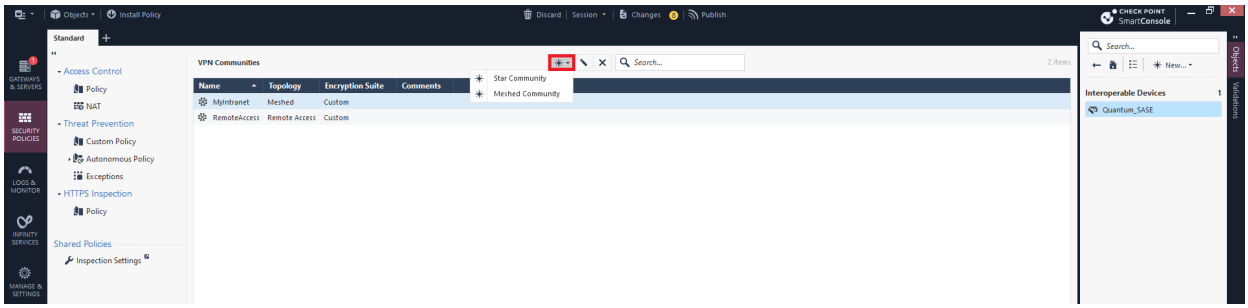
10. In the **Topology** tab, select **External (leads to the local Internet)**.
11. Click **OK**.
12. Click **OK**.
13. Publish and install the policy.

Creating VPN Start Community

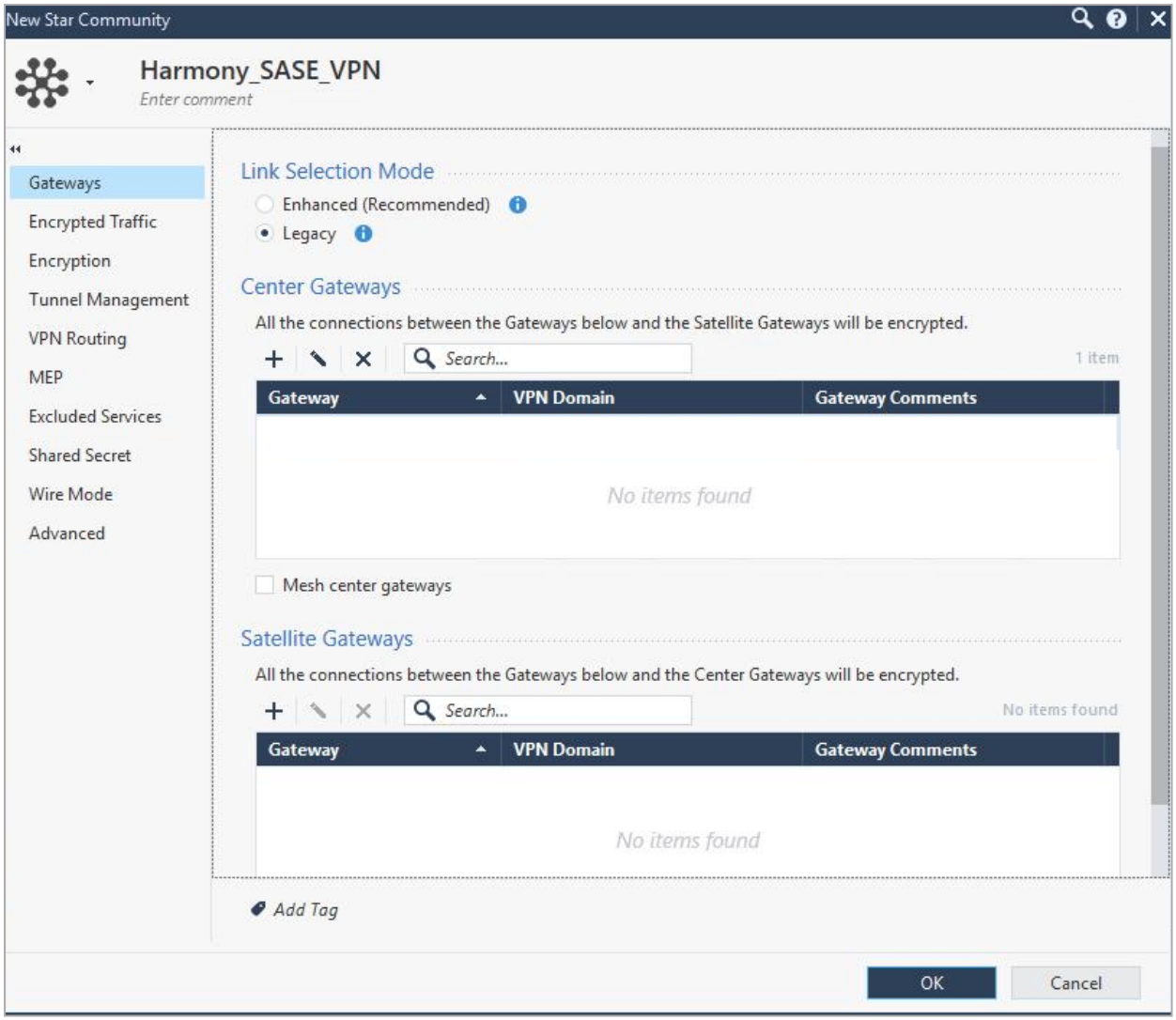
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Click **New** and select **Star Community**.



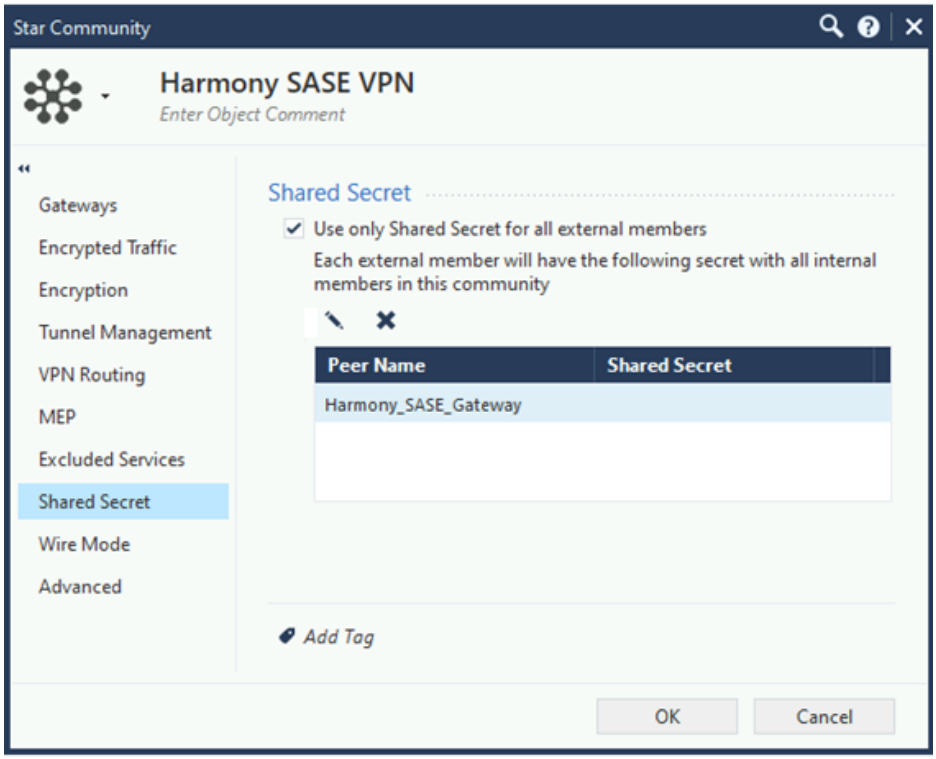
The **New Star Community** window appears.



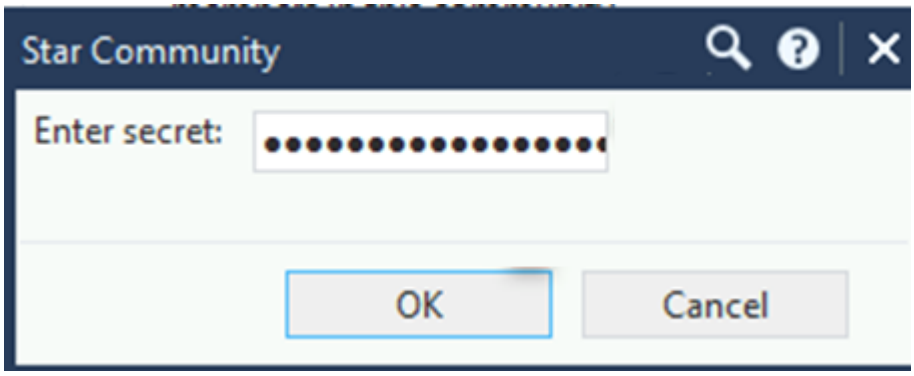
5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, SASE VPN.
6. In the **Link Selection Mode** section, select one of these:
   - **Enhanced (Recommended)** - Uses dynamic, intelligent, probe-based logic to choose the optimal VPN link. It evaluates:
     - Interface status
     - Multiple external IP addresses
     - Multiple ISP circuits
     - Reachability through Next-Hop Probing
     - SLA-like behavior for tunnel selection

- **Legacy** - Uses static or basic logic to select the VPN interface or IP address. Selection is based on:
  - Main IP (default)
  - Selected interface
  - Selected IP
  - IP address determined by topology

7. Under **Center Gateways**, click + and add the Check Point gateway.
8. Under **Satellite Gateways**, click + and add the previously created Interoperable Device Object for the SASE gateway. See step 3.
9. Click **Shared Secret**.
10. To edit the shared key, click ✎.

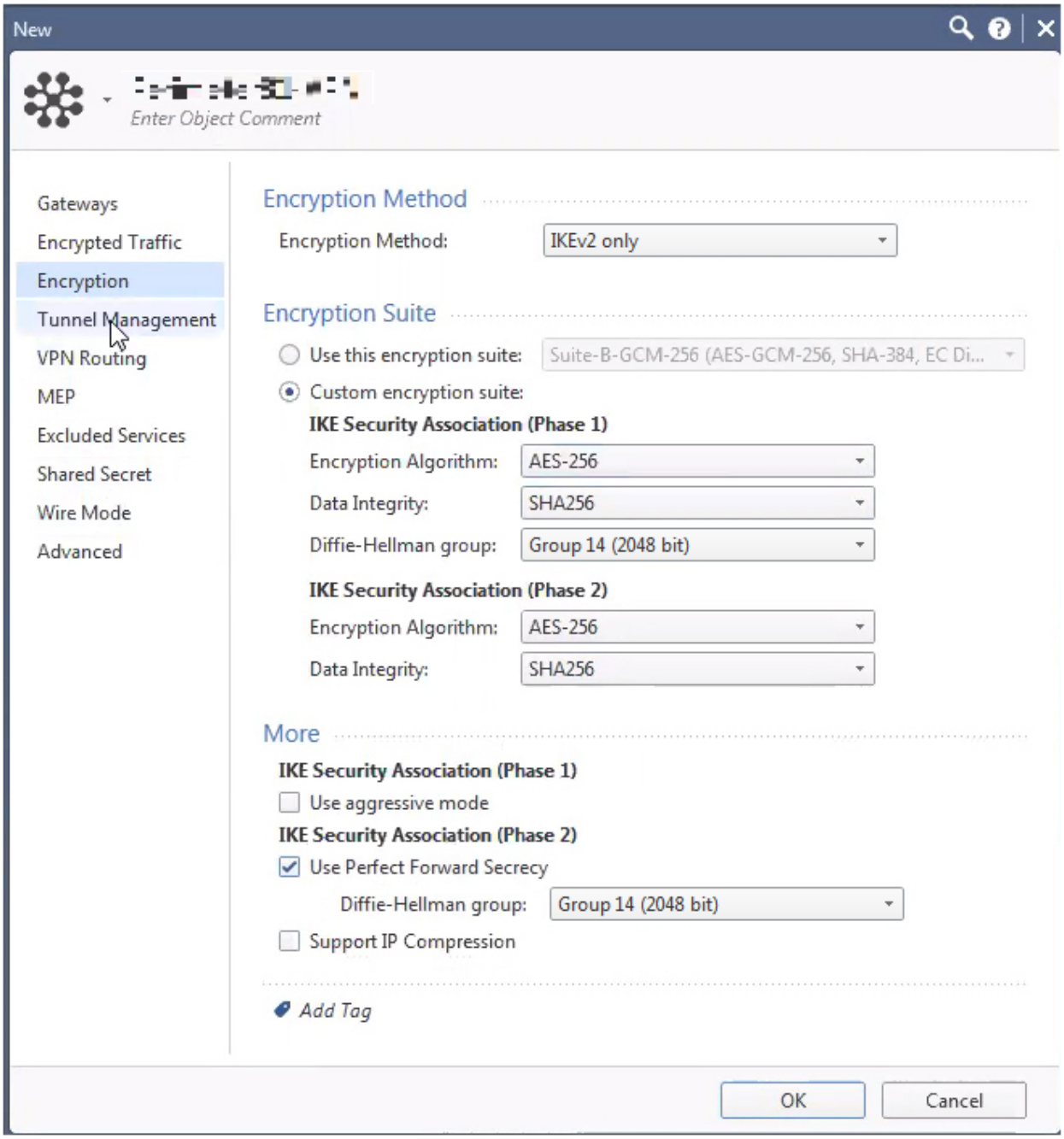


11. In the **Enter secret** field, enter an appropriate key. Make a note of it as it is used while configuring the tunnel in the Check Point SASE Administrator Portal.



Note - Check Point recommends that the share secret key is at least 20 characters in length.

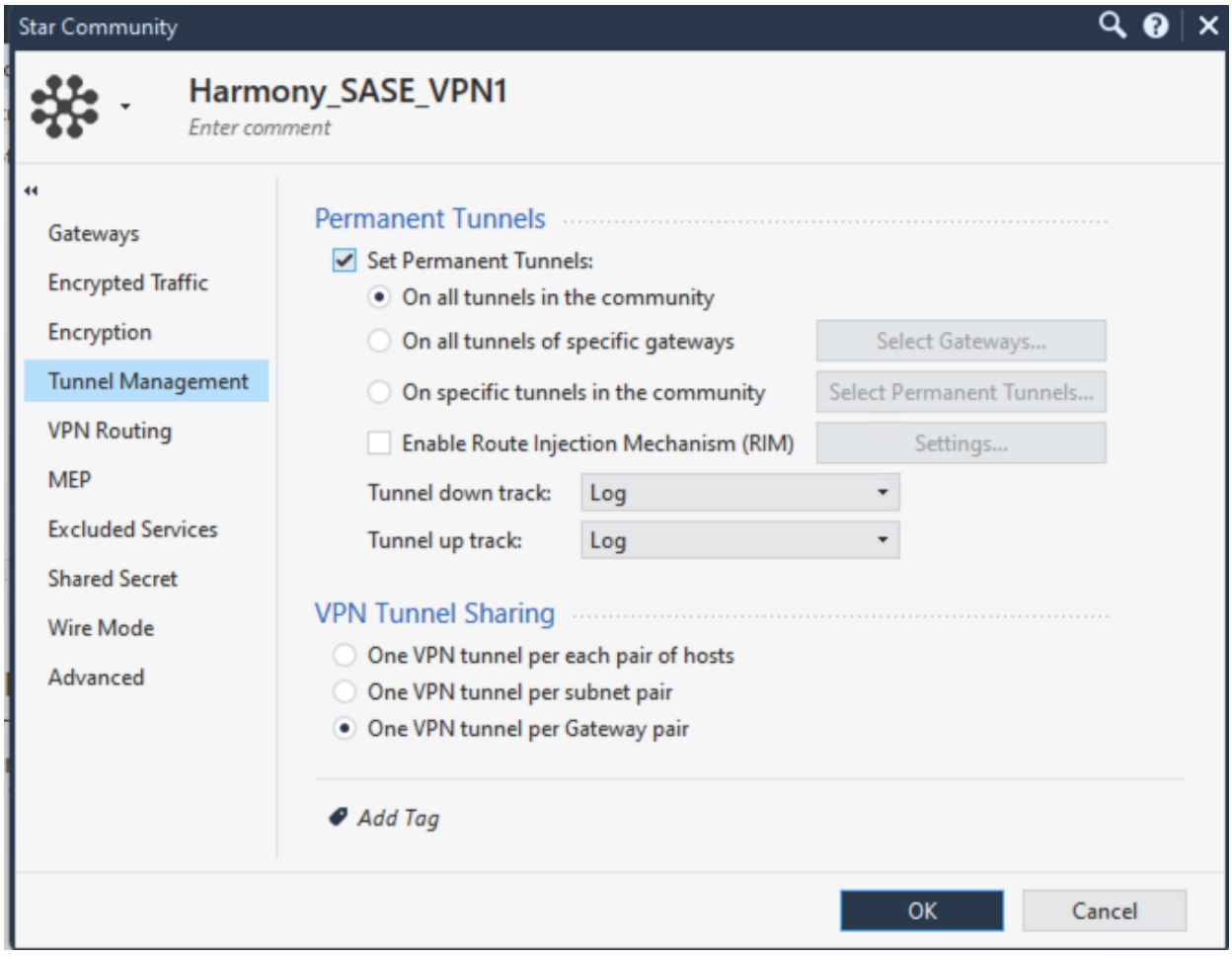
12. Click **OK**.
13. Click **Encryption**:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256

Field	Enter
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

14. Click **Tunnel Management**.
15. In the **Permanent Tunnels** section, select the **Set Permanent Tunnels** checkbox and then select **On all tunnels in the community**.



16. In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

    Important - Make sure that you enter the remote subnets specified here in the Check Point SASEAdministrator Portal. A mismatch can disconnect the tunnel.

17. Click **Advanced**.

    a. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.

    b. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.

18. Click **OK**.

Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Check Point SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Check Point SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

To configure the Tunnel in SASE Administrator Portal, see *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.

To configure the Routes Table in SASE Administrator Portal, see Routes Table.

Cisco Firepower

You can establish a Site-to-Site VPN tunnel between your SASE and the Cisco Firepower device.

Pre-requisites

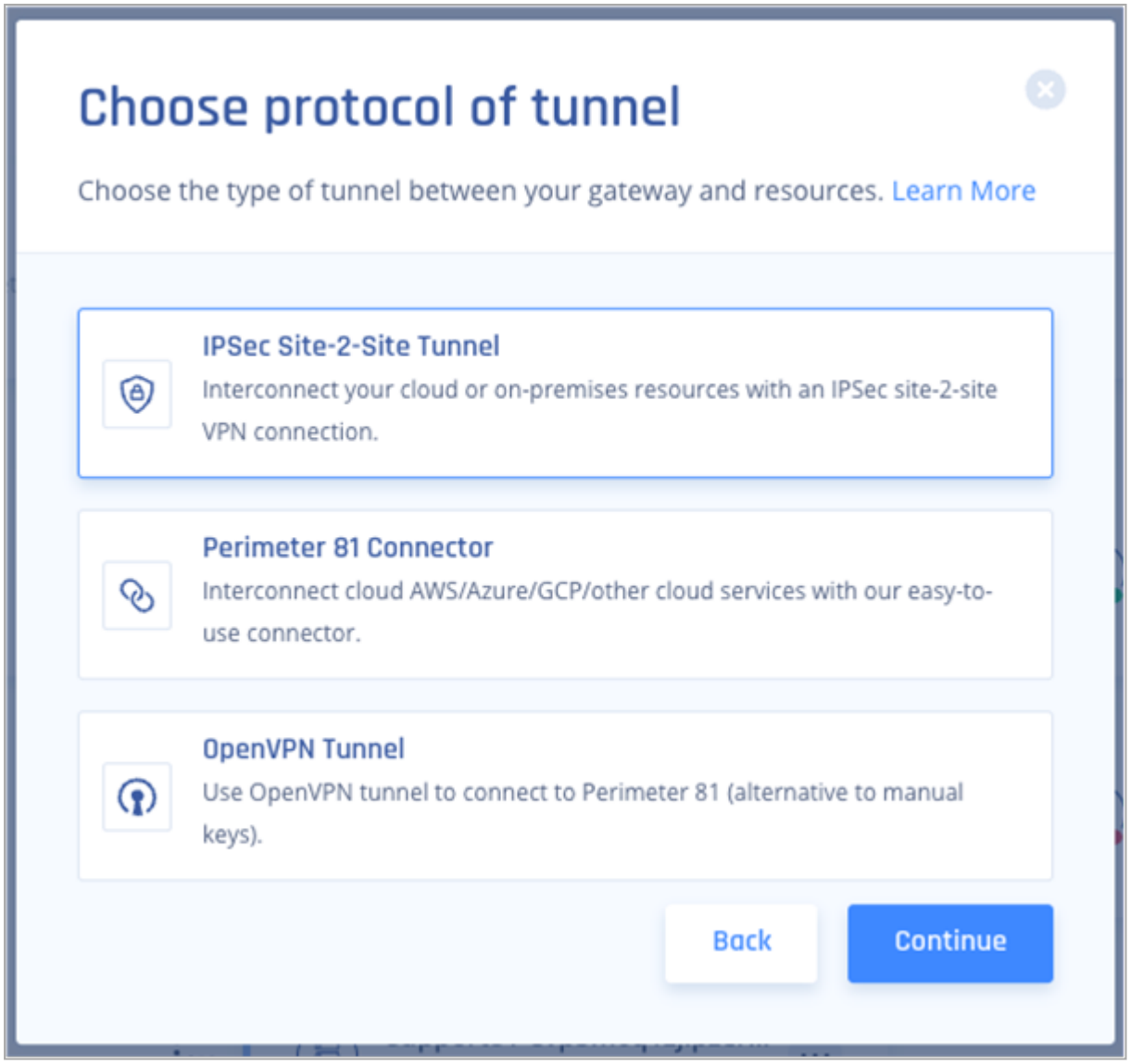
- SASE Administrator Portal account and a configured network.
- Make sure that you have installed the SASE Agent on your device.
- Active and licensed Cisco Firepower device with necessary administrative permissions.

Configuring IPsec Tunnel

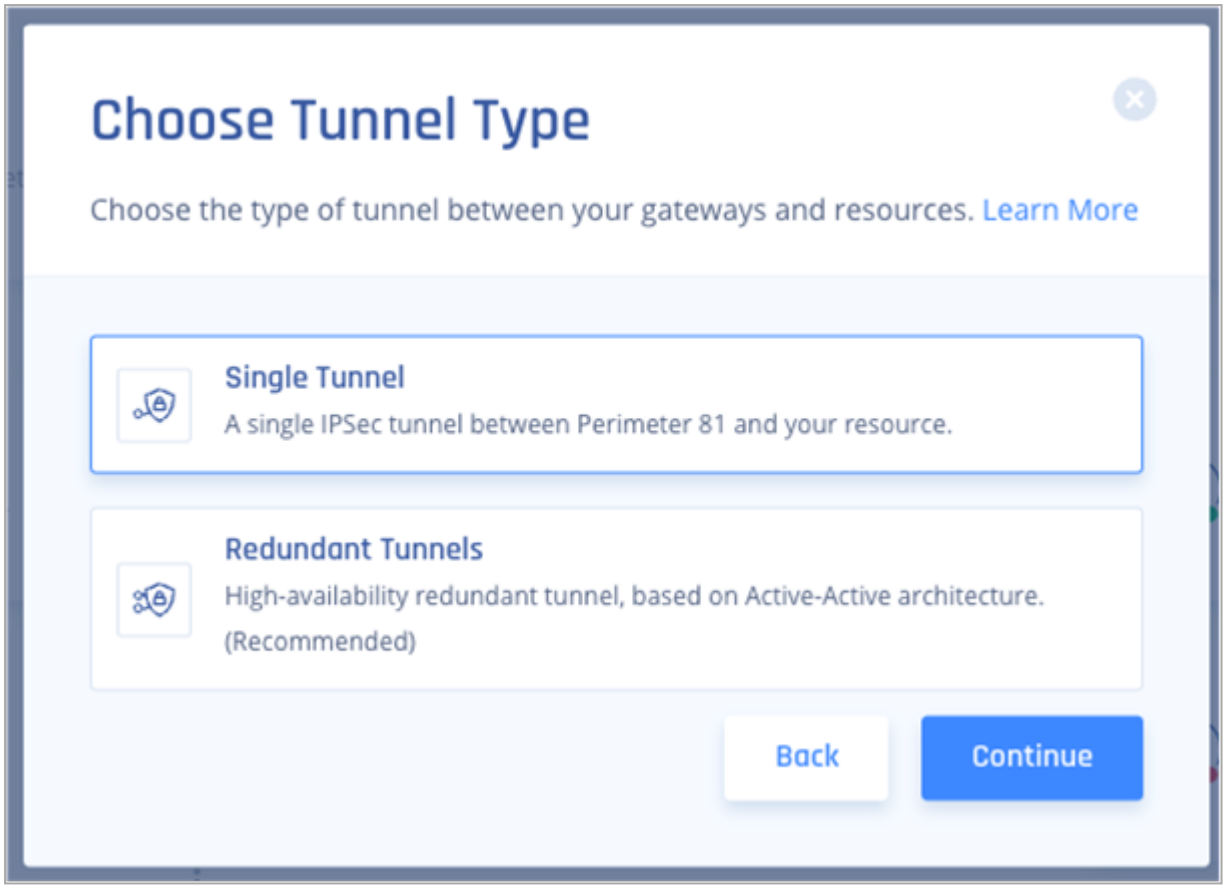
To configure an IPsec tunnel, do these:

1. Log in to the SASE Administrator Portal.
2. Click **Networks**.
3. Select the network from which you want to create the tunnel to the Cisco Firepower.
4. Click ... and select **Add Tunnel**.

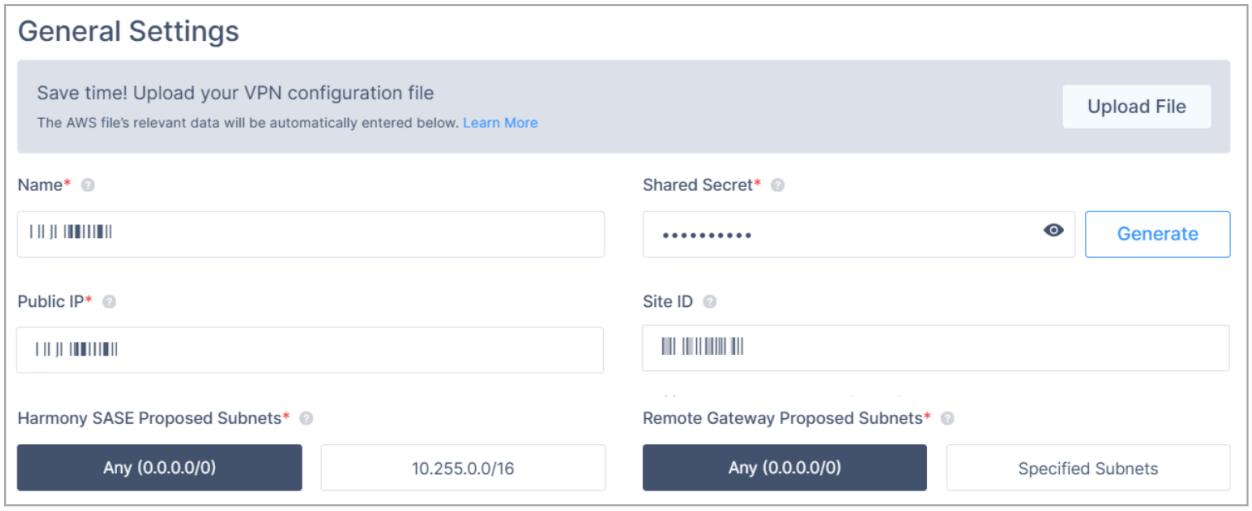
5. Select **IPSec Site-2-Site Tunnel** and click **Continue**.



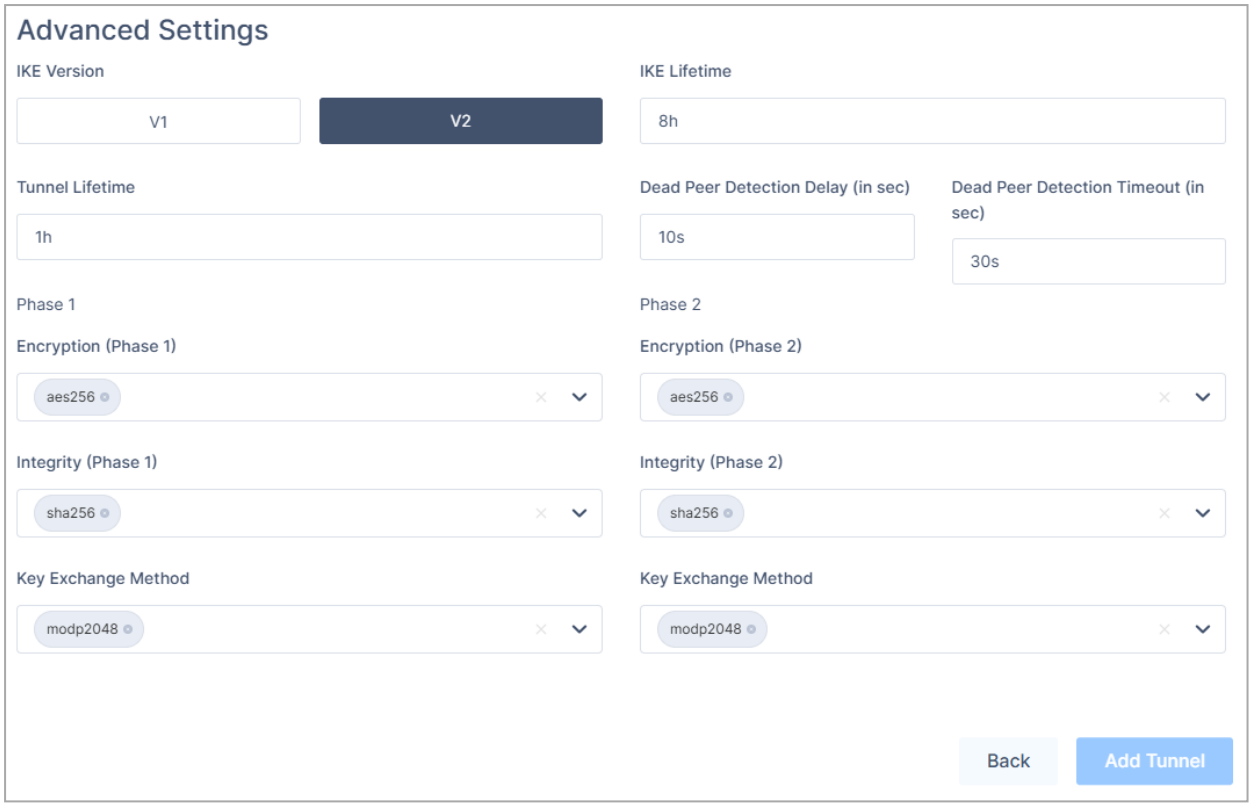
6. Select **Single Tunnel** and click **Continue**.



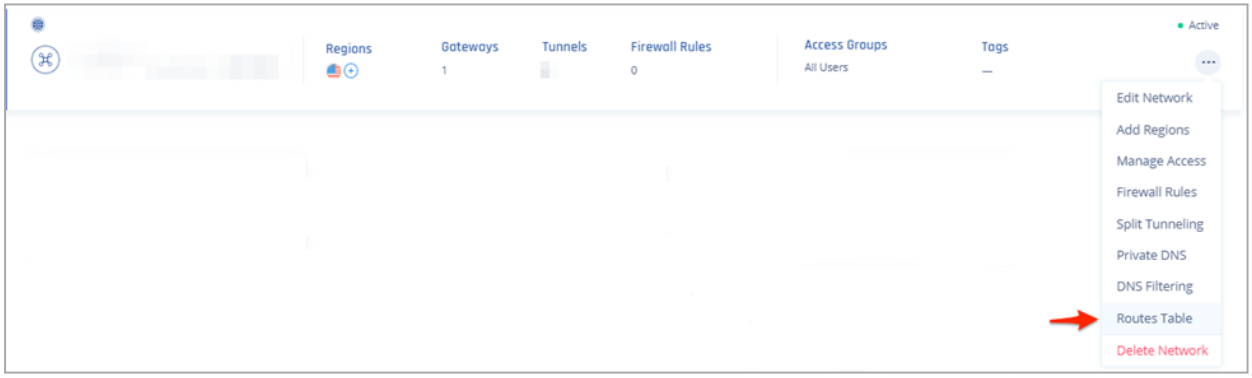
7. In the **General Settings** section:
    a. In the **Name** field, enter a name for the tunnel.
    b. In the **Shared Secret** field, enter a string or click **Generate**.
    c. In the **Public IP** field, enter the public IP of the Firepower device.
    d. In the **Remote ID** field, enter the remote ID of the Firepower device (this is same as Public IP unless the device is behind a NAT, then use the IP of the **outside** interface on the Firepower).
    e. In the **Check Point SASE Gateway Proposal Subnets** section, leave the default value, **Any (0.0.0.0/0)**.
    f. In the **Remote Gateway Proposal Subnets** section, leave the default value, **Any (0.0.0.0/0)**.



8. In the **Advanced Settings** section, specify these:
   - **IKE Version**: V2
   - **IKE Lifetime**: 8h
   - **Tunnel Lifetime**: 1h
   - **Dead Peer Detection Delay**: 10s
   - **Dead Peer Detection Timeout**: 30s
   - **Phase 1**:
     - **Encryption(Phase 1)**: aes256
     - **Integrity (Phase 1)**: sha256
     - **Key Exchange Method**: modp2048
   - **Phase 2**:
     - **Encryption(Phase 2)**: aes256
     - **Integrity (Phase 2)**: sha256
     - **Key Exchange Method**: modp2048

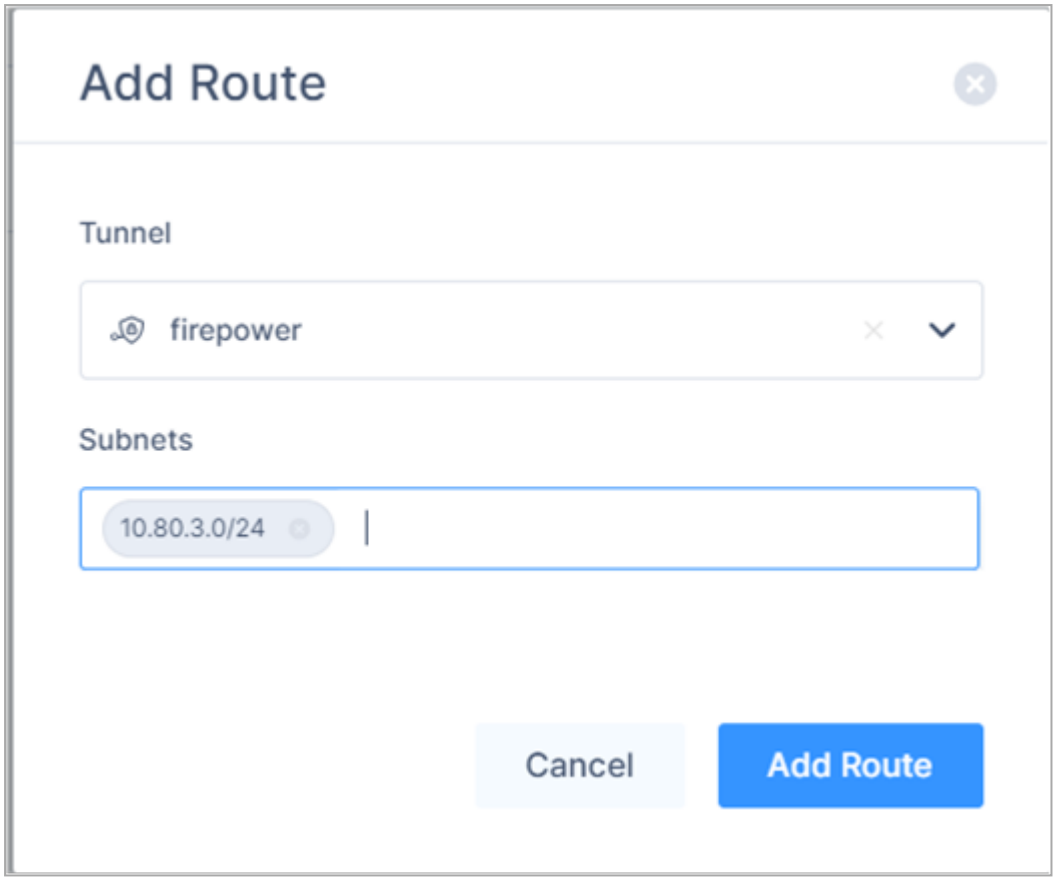


9. On your network, click ... and select **Routes Table**.

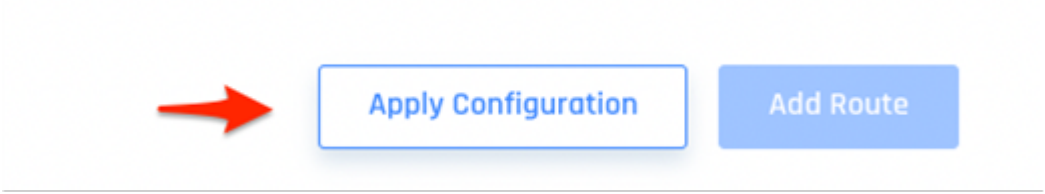


10. Click **Add Route**.

    The **Add Route** window appears.



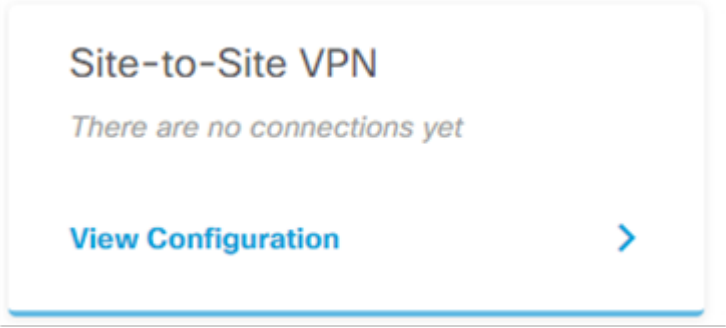
11. Verify the values entered in these:
    a. **Tunnel**
    b. **Subnet**
12. Click **Add Route**.
13. Click **Apply Configuration**.



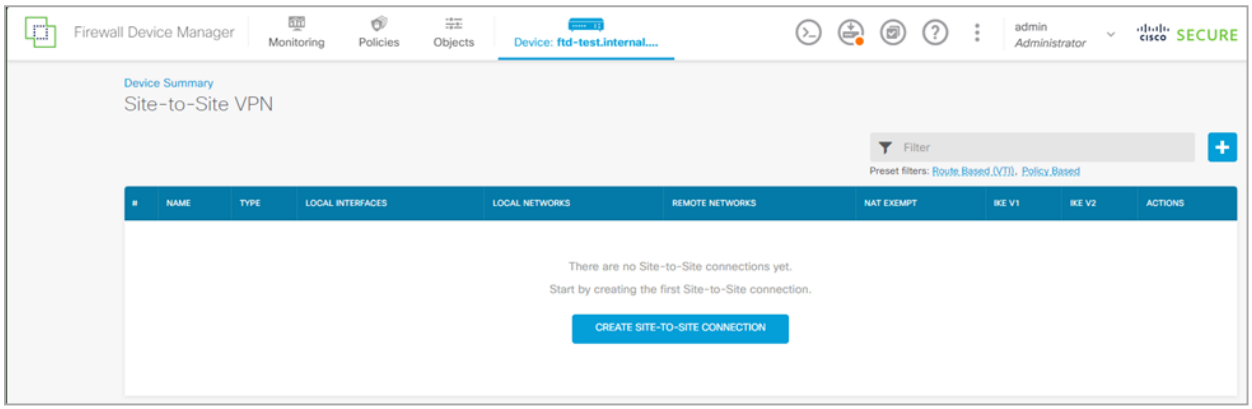
Configuring the Tunnel in Cisco Firepower

1. Login to your Cisco Firepower web console.
2. Select your device.

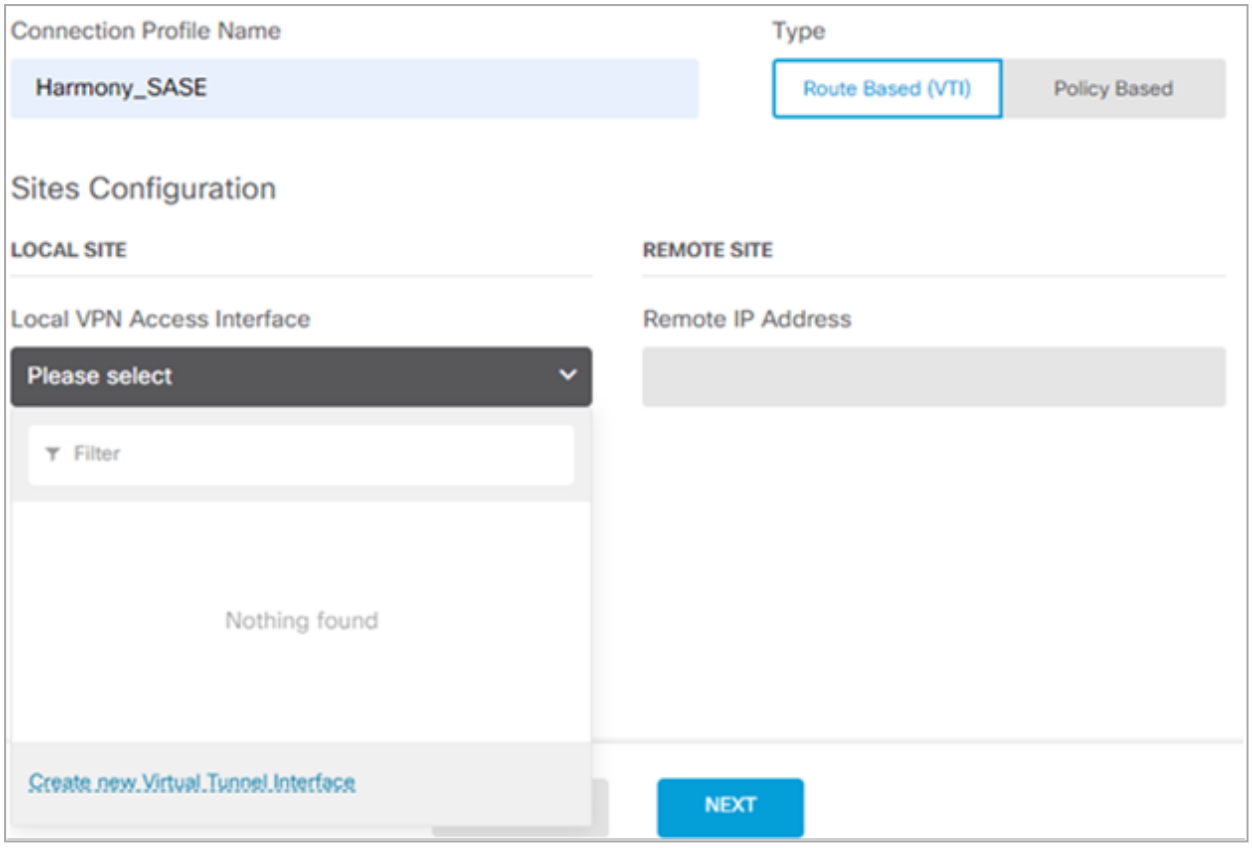
3. Go to Site-to-Site VPN configuration and click **View Configuration**.



4. Click + to create a Site-to-Site Connection.



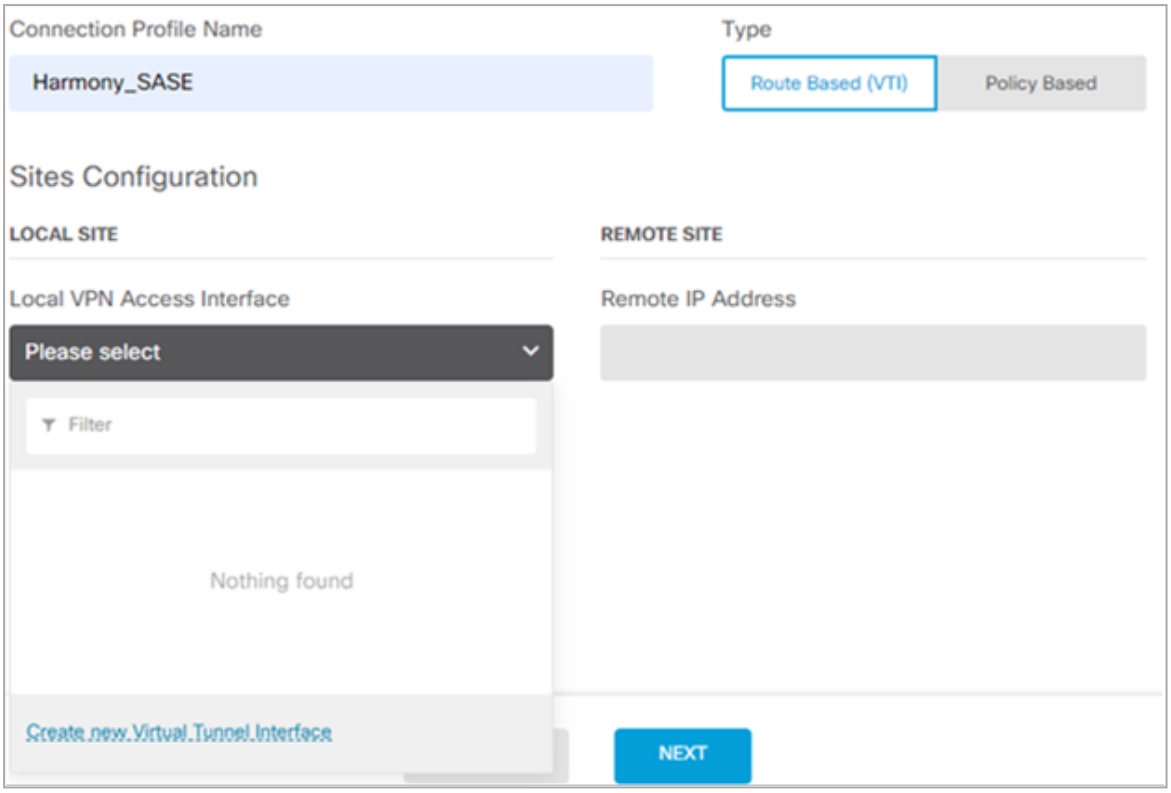
5. Specify these:



a. In the **Connection Profile Name** field, enter a name for your connection.

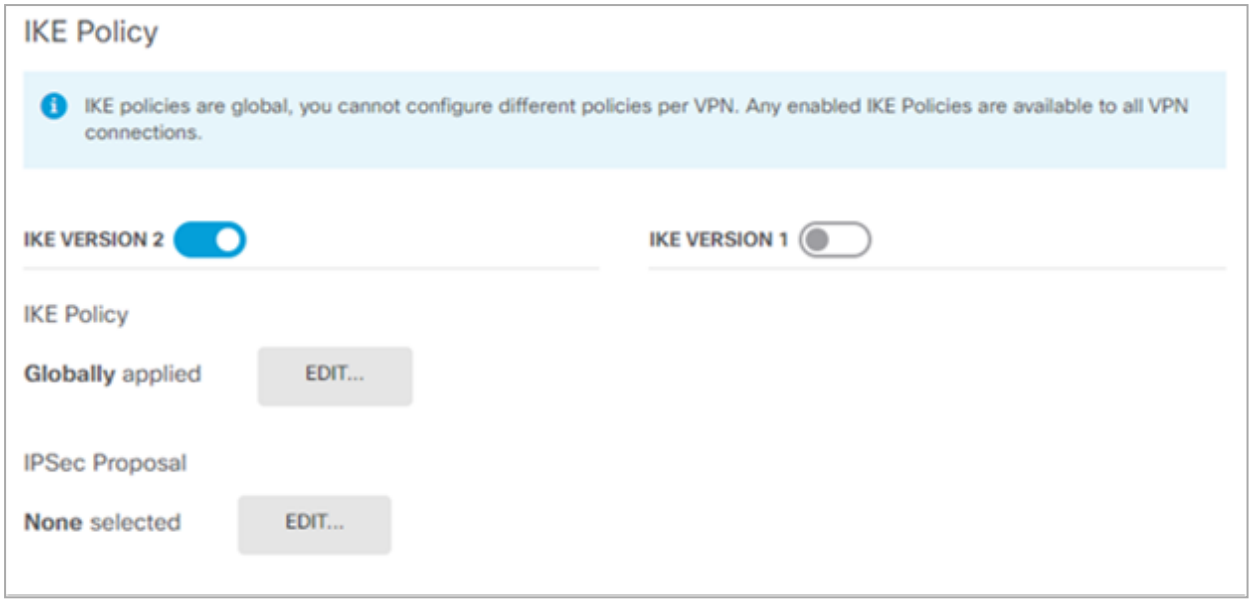
b. In the **Type** section, select **Route Based (VTI)**.

c. Expand **Local VPN Access Interface**, and click **Create new Virtual Tunnel Interface**.

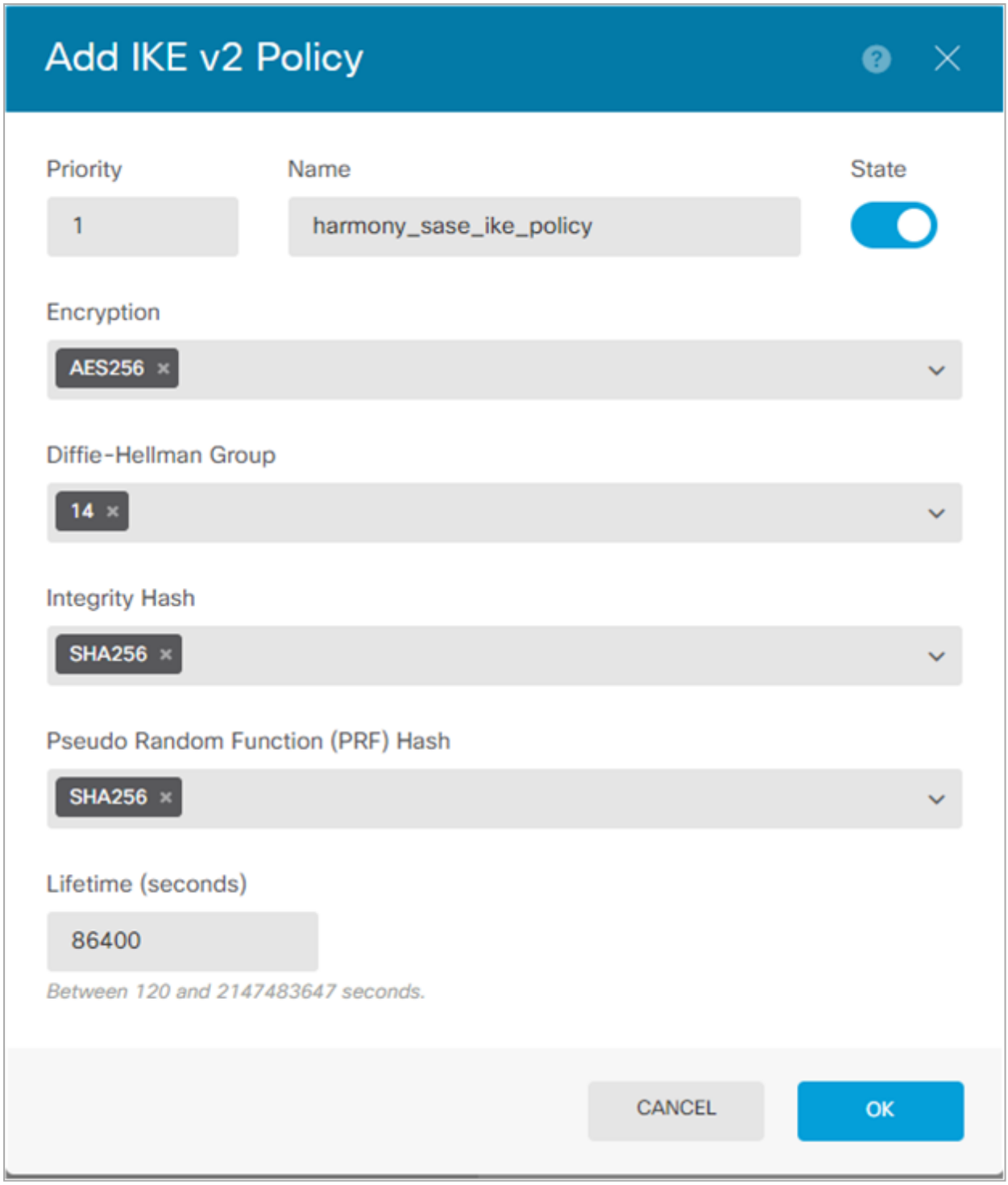


The **Create Virtual Tunnel Interface** window appears.

6. Enter a name for your VTI adapter, for example, harmony_sase_vti.
7. Turn on the **Status** toggle button.
8. Enter a tunnel ID.
9. Set the source to your outside interface.
10. Set the IP and Subnet Mask to `169.254.2.122 / 255.255.255.252`
11. Click **OK**.
12. From the **Create Virtual Tunnel Interface** list, select the newly created VTI object.
13. In the **Remote IP Address** field, enter your Check Point SASE gateway IP address (found in your Check Point SASE Administrator Portal).
14. Click **Next**.



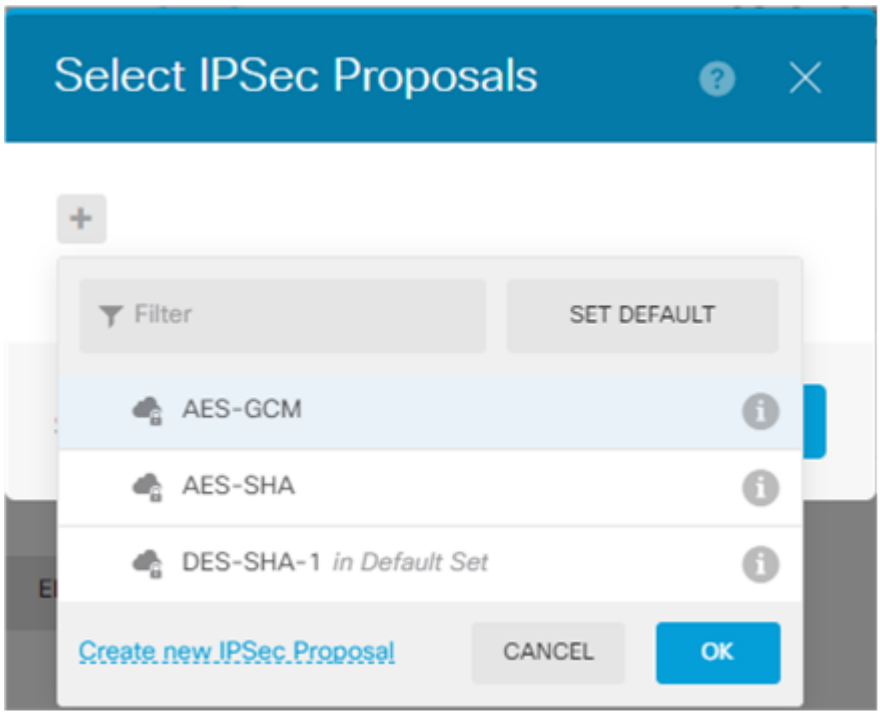
15. Make sure **IKE VERSION 2** is enabled.
16. In the **IKE Policy** section, for **Globally applied**, click **Edit**.
17. Create a new policy with the settings that match the Phase 1 settings on the SASE side. Specify these:



- **Priority**
- **Name**
- **State** - Enable
- **Encryption**: AES256
- **Diffie-Hellman Group**: 14

- **Integrity Hash**: SHA256
- **Pseudo Random Function (PRF) Hash**: SHA256
- **Lifetime**: 28800

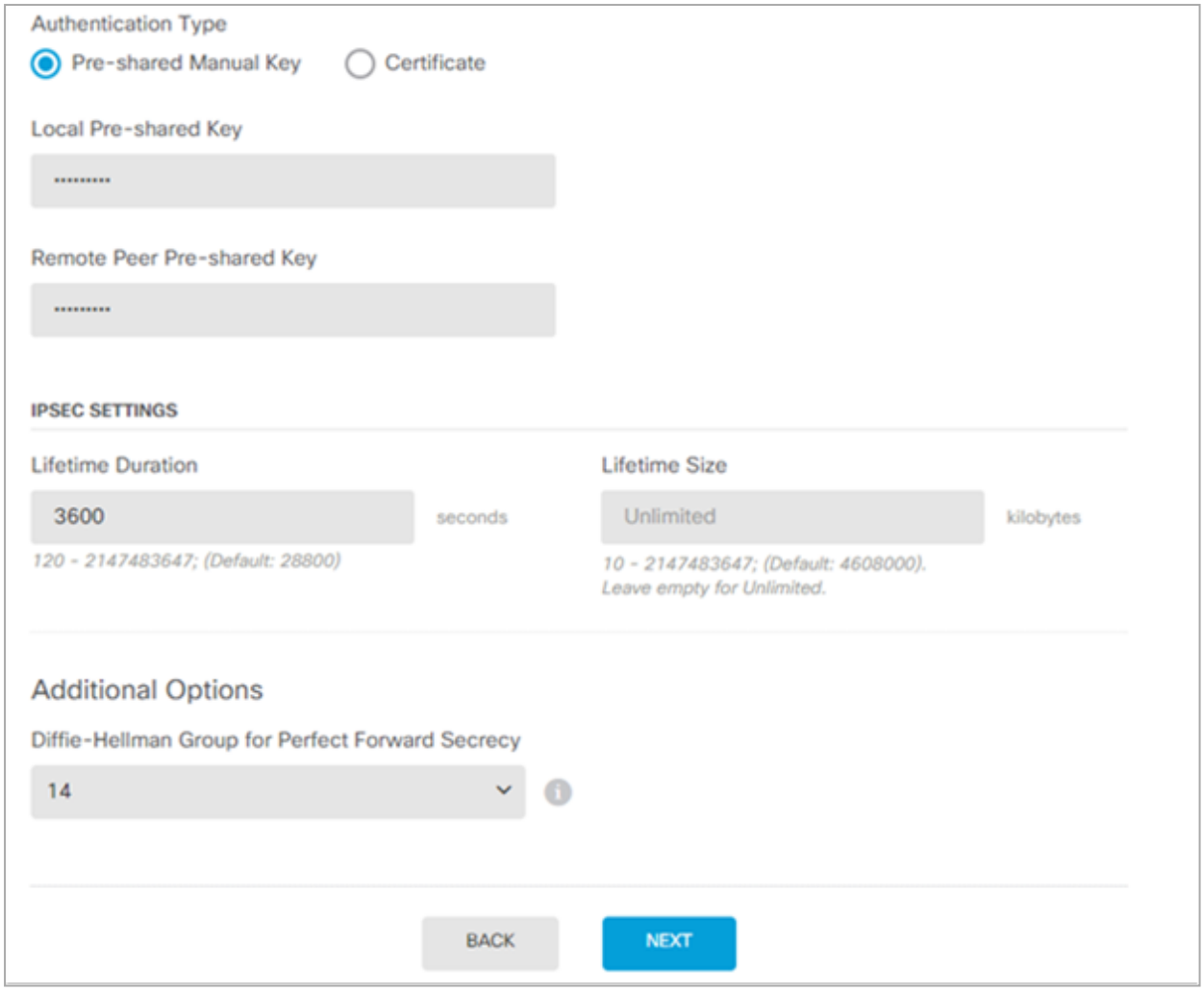
18. Click **OK**.
19. Click **Edit by IPSec Proposal**.



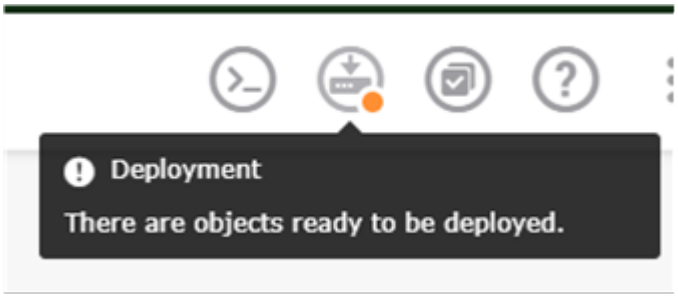
20. Click **Create new IPSec Proposal**.
21. Specify these:
    a. **Name**
    b. **Encryption**: AES256
    c. **Integrity Hash**: SHA256

    Note - Select the Encryption and Integrity Hash to match the SASE side for Phase 2.

22. Click **OK**.
23. In the **Authentication Type** section, select **Pre-shared Manual Key**.



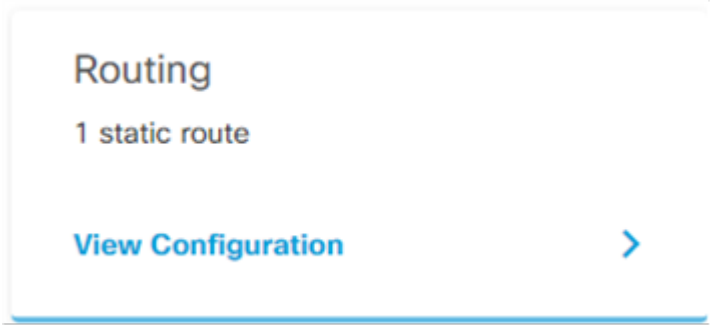
24. In the **Local Pre-shared Key** and **Remote Peer Pre-shared Key** fields, enter the Pre-shared Key that you created on the SASE portal.
25. In the **Lifetime Duration** field, enter **3600**.
26. In the **Diffie-Hellman Group for Perfect Forward Secrecy** field, enter **14**.
27. Click **Next**.
28. Click **Finish**.
29. Click to deploy changes to apply the new tunnel.



Configuring the Static Route in the Cisco Firepower

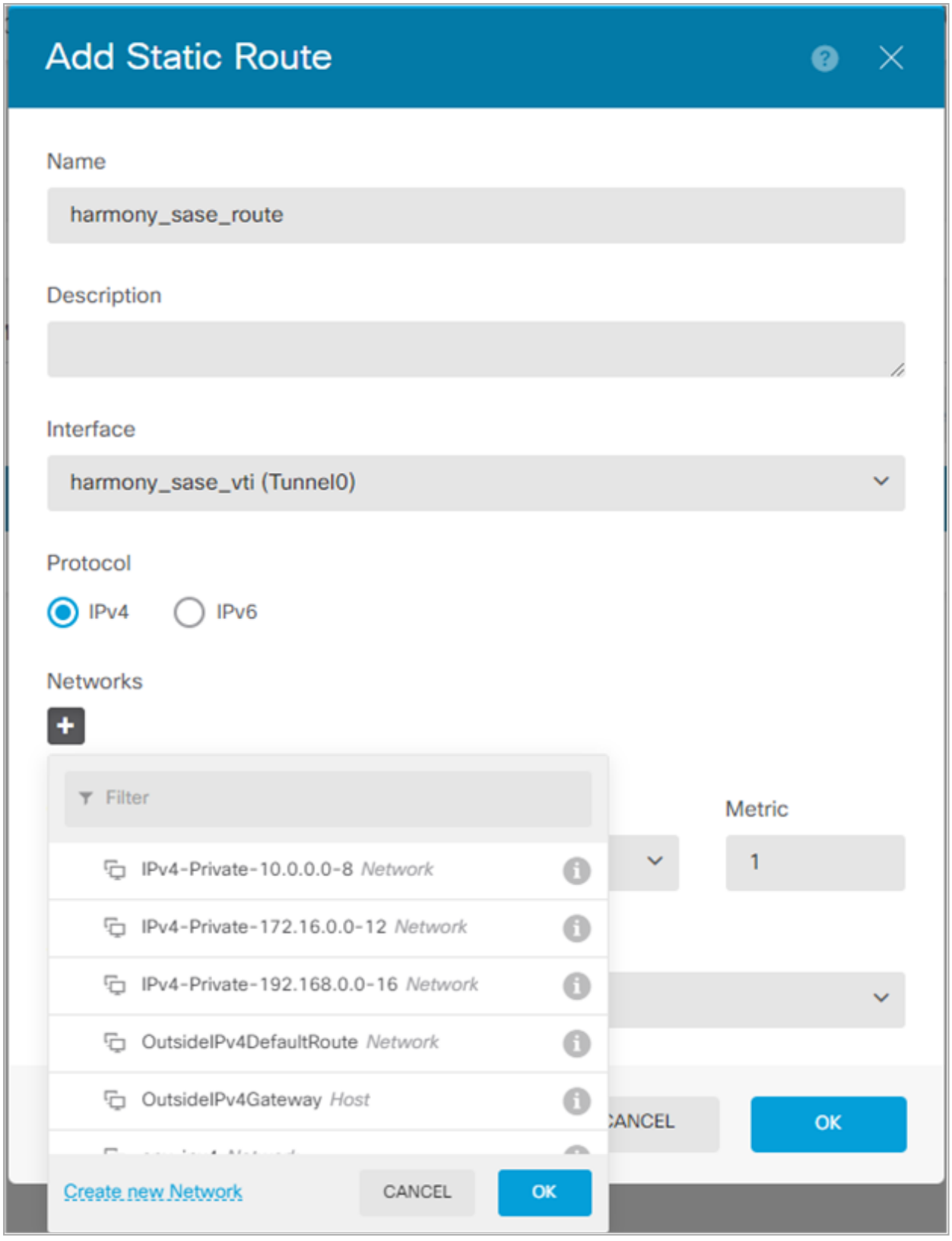
1. Select your device.

2. In the **Routing** section, click **View Configuration**.



3. Click to add a new static route.

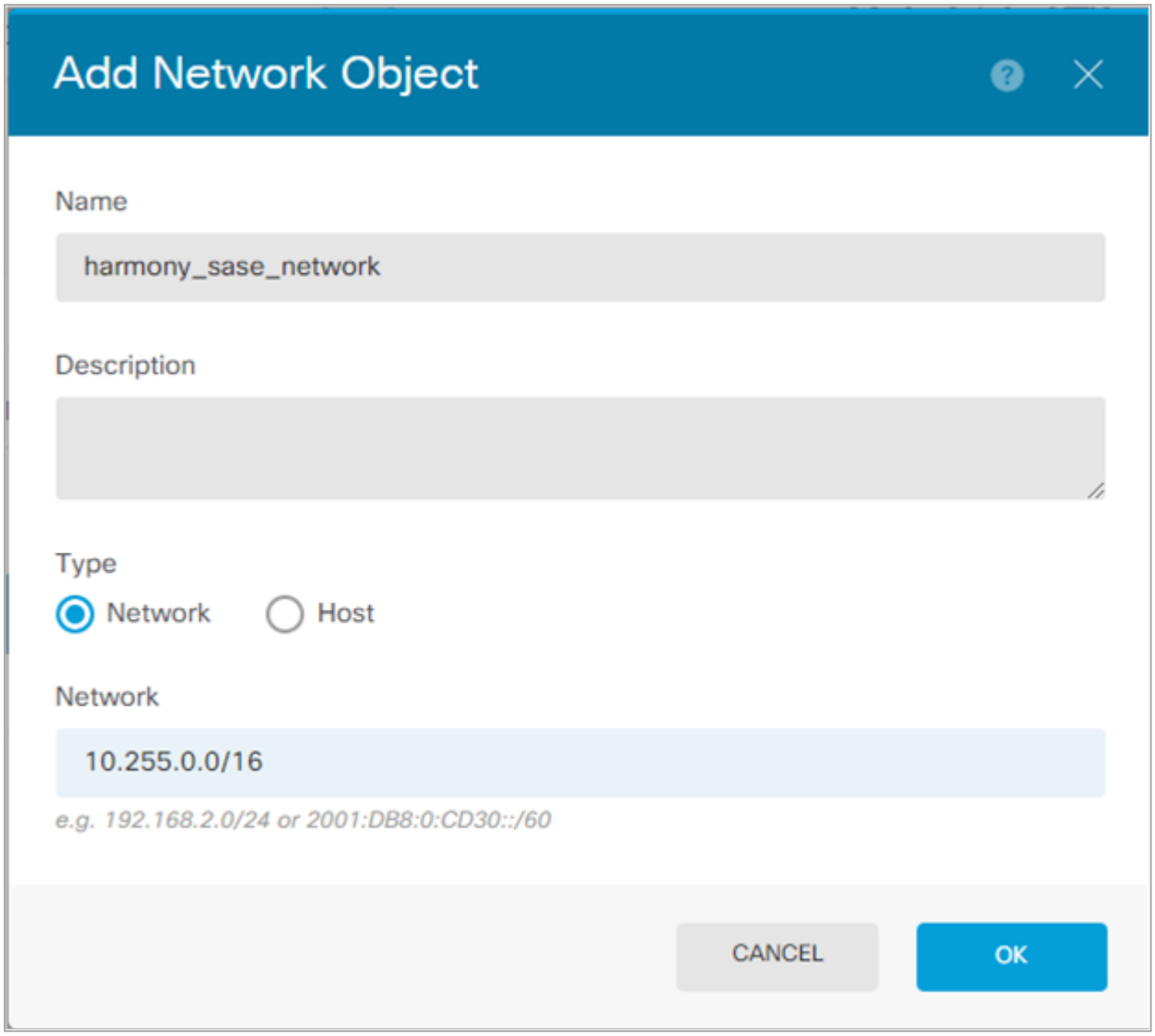
The **Add Static Route** window appears.



4. In the **Name** field, enter a name for your static route.
5. In the **Description** field, enter a description.

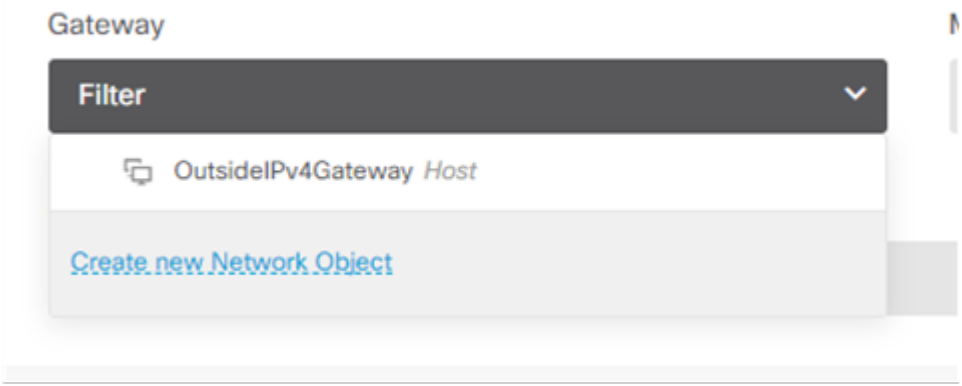
6. From the **Interface** list, select the interface you created in [Configuring the Tunnel in the Cisco Firepower] step 6.
7. In the **Networks** section, click +.
8. Click **Create new Network**.

   The **Add Network Object** window appears.



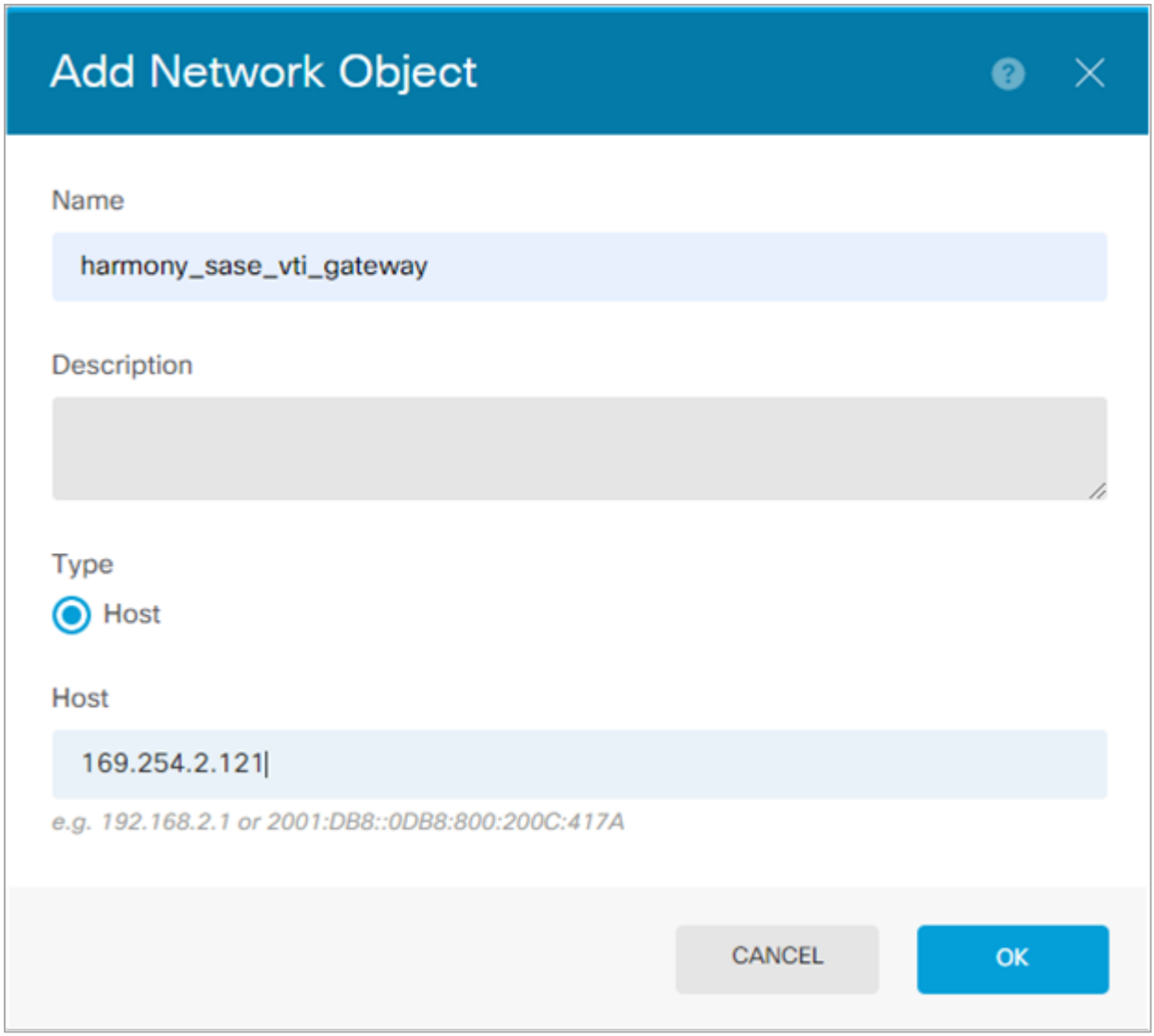
9. Specify these:
   - **Name**
   - **Description**
   - **Type** - Network
   - **Network** - 10.255.0.0/16 (default)
10. Click **OK**.

11. In the **Networks** section, click +.
12. Select the object you just created.
13. In the **Gateway** section, click **Create new Network Object**.



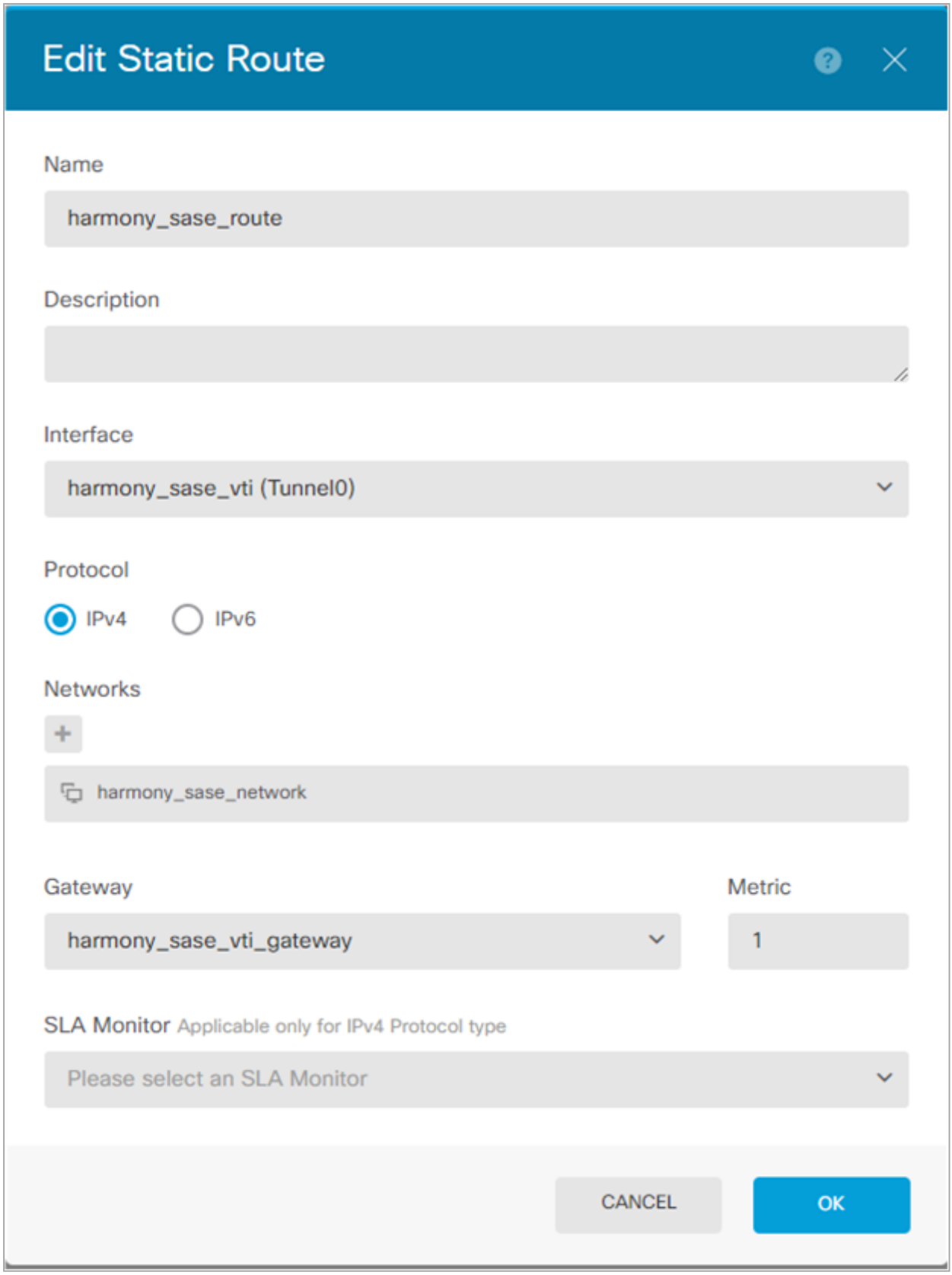
The **Add Network Object** window appears.

14. Specify these:



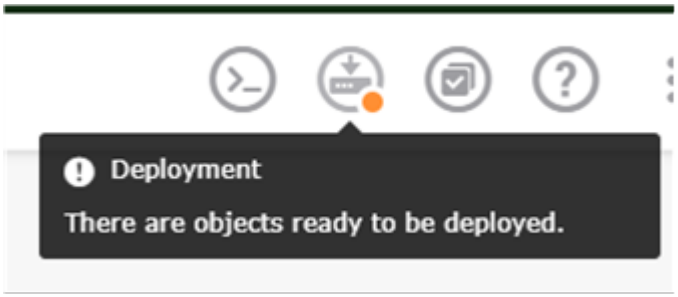
a. Name. For example, harmony_sase_vti_gateway
b. Description
c. Type - Host
d. Network - 169.254.2.121 (this is the corresponding side of your VTI adapter)

15. Click **OK**.



The new route is added.

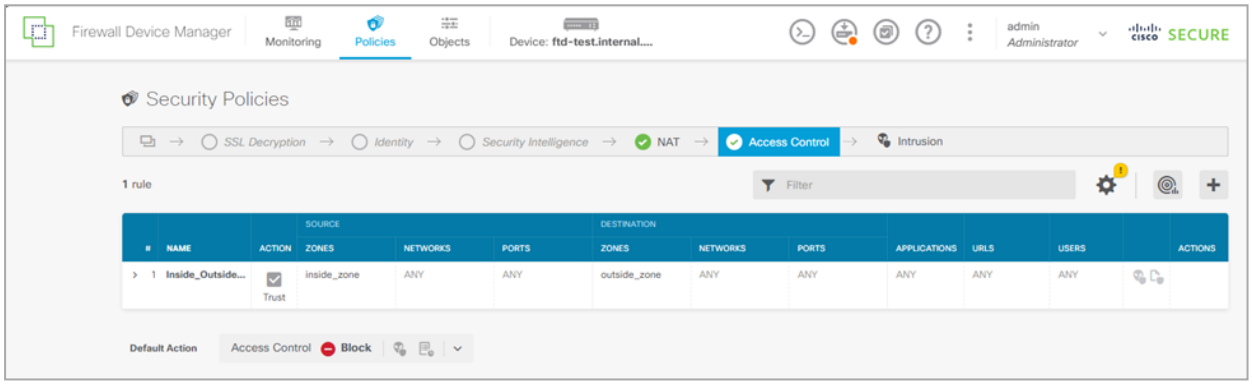
16. Click to deploy changes to apply the new route.



Configuring Firepower Policies Allowing Traffic Flow

To configure Cisco Firepower policies to allow traffic to flow:

1. Go to **Policies** and click + to add a new access rule.



2. Configure either 1 bidirectional rule or 2 unidirectional rules.

   For example: Creating a single bidirectional rule.

   a. Enter an order number. Make sure this rule is not after a block rule that affects this traffic.

   b. Enter a title. For example, harmony_sase_allow.

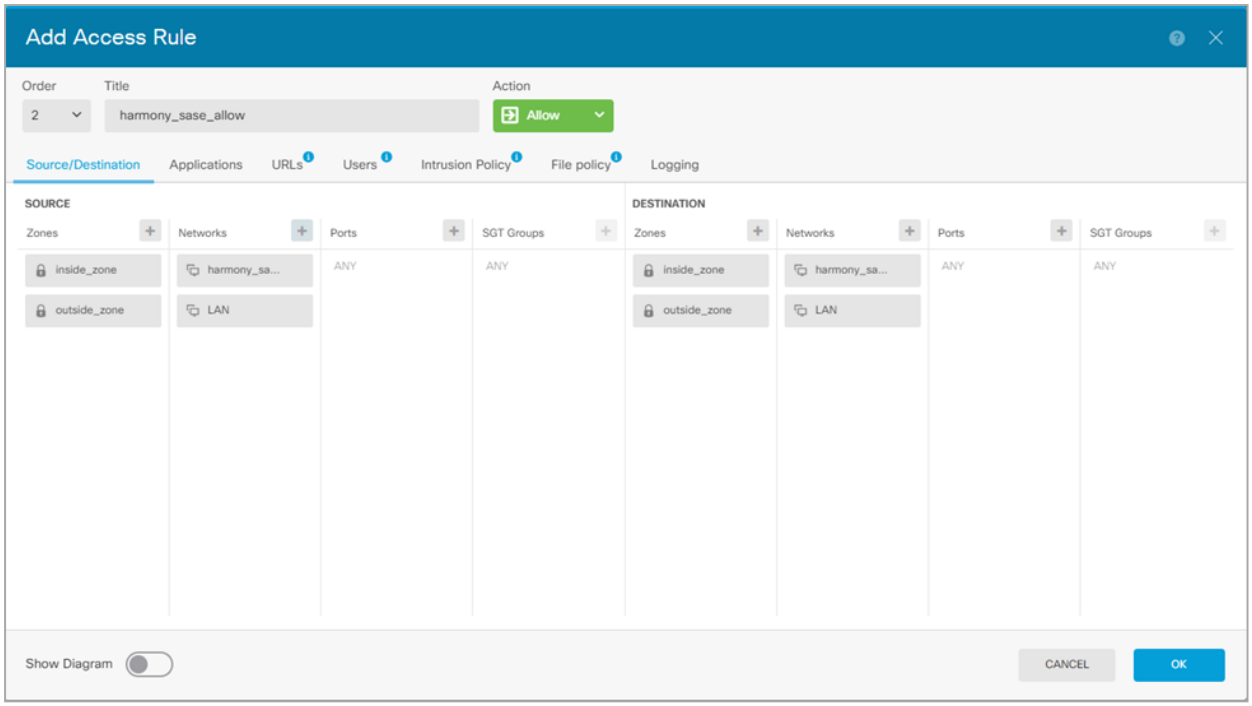
   c. Set your Source zones and Networks.

   d. Add an entry for inside_zone and outside_zone.

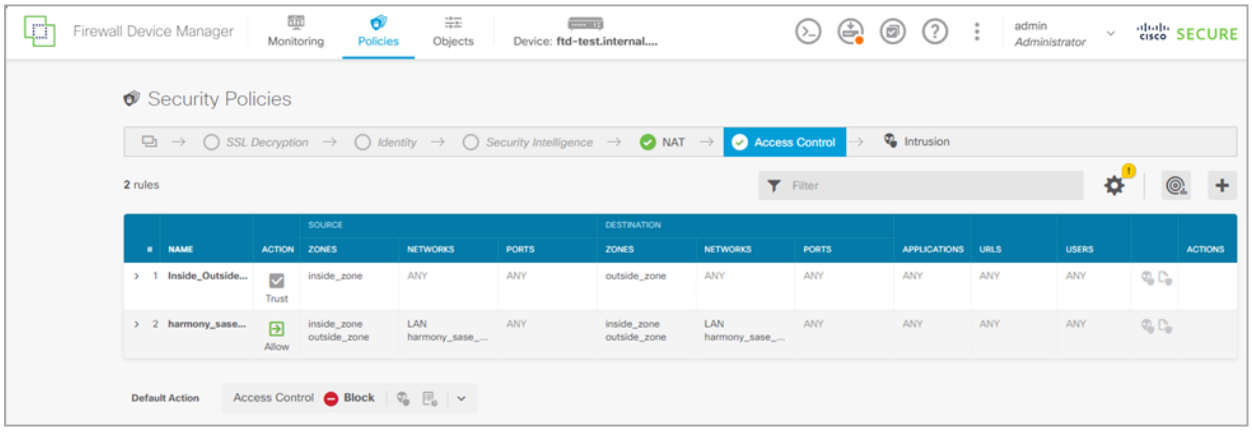
   e. Add a network entry for your harmony_sase_network object.

   f. Repeat the same for the Destination.

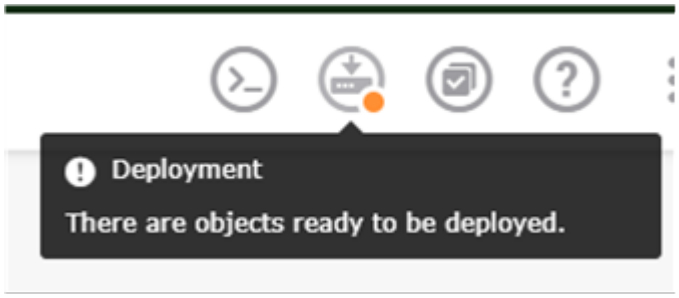
3. Click **OK**.



Once you add the rule, the table should display:



4. Click to deploy changes to apply the new route.



Configuring Check Point Cluster VIP Redundant IPsec Tunnel

This topic explains how to establish a redundant Site-to-Site tunnel between your SASE Network and Check Point Firewall cluster VIP.

Prerequisites

- SASE Administrator Portal account.
- Device with SASE Agent installed.
- Administrator account with Firewall, Router, and Cloud Management Portal.
- A cluster of two Quantum gateways, behind a single VIP.

Note - Configuration with ISP redundancy is not supported.

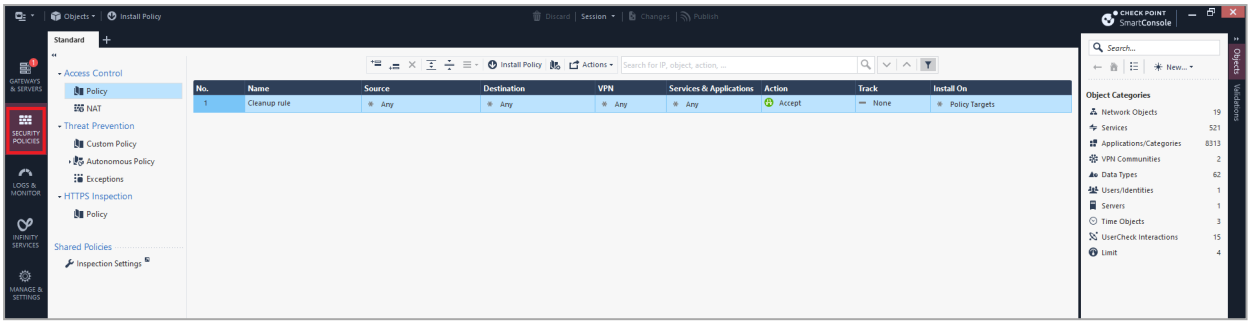
High Level Procedure

- *"Part 1 - Configuration in SmartConsole" below*
  - *"Step 1: Create Interoperable Device Object in the Check Point SmartConsole" below*
  - *"Step 2: Add SASE Gateway IP Address and Remote Subnet to the Interoperable Device Object" on page 303*
  - *"Step 3: Create VPN Start Community" on page 309*
  - *"Step 4: Additional settings in Check Point SmartConsole" on page 315*
  - *"Step 5: Configure VPN Tunnel Interface and BGP" on page 315*
  - *"Step 6: Configure BGP Configuration" on page 317*
- *"Part 2 - Configuration in the SASE Administrator Portal" on page 320*
  - *"Step 1: Configure Tunnel and Routes Table" on page 320*
  - *"Step 2: Verify the Setup" on page 326*

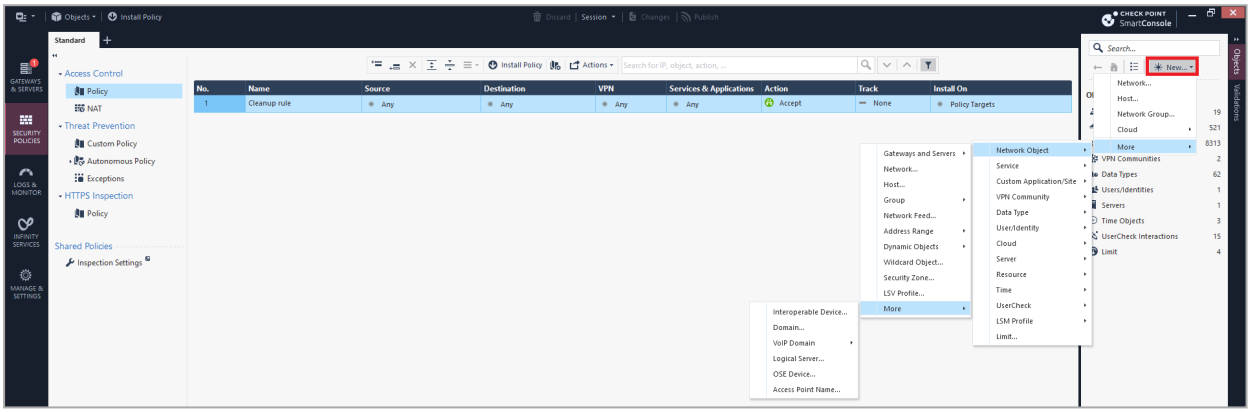
Part 1 - Configuration in SmartConsole

Step 1: Create Interoperable Device Object in the Check Point SmartConsole

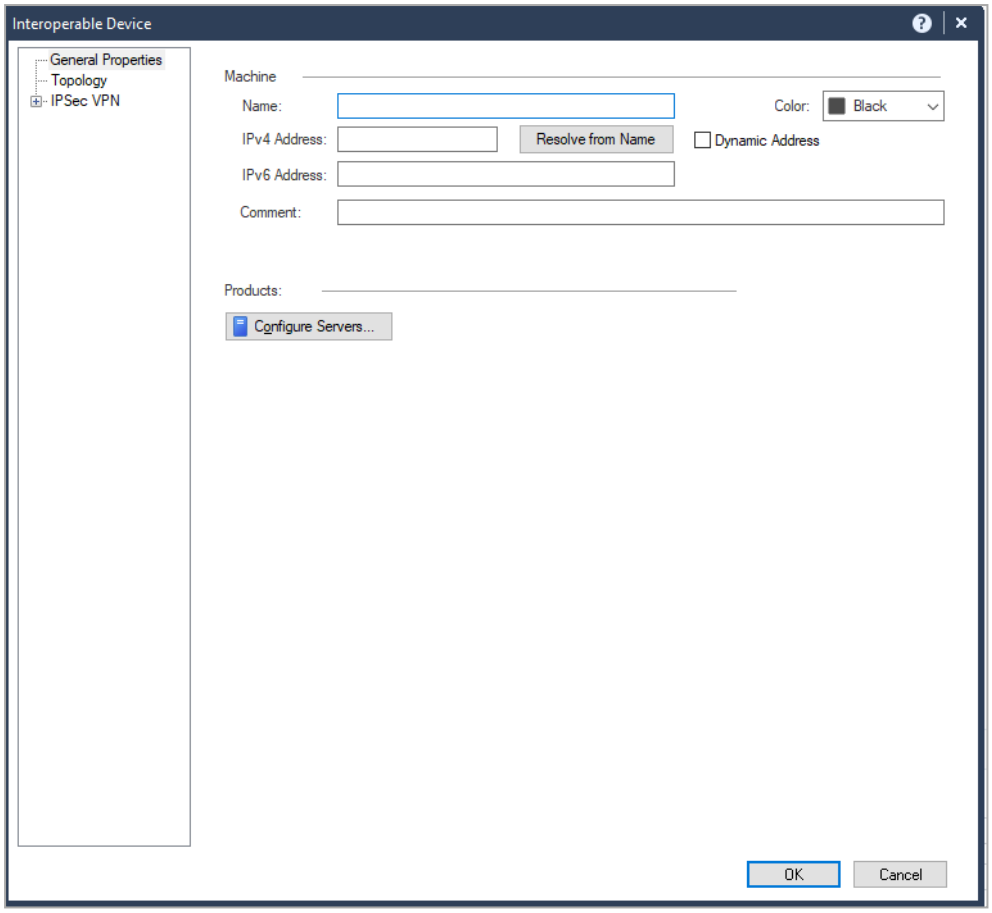
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. In the Objects pane, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



4. Enter these details:
    a. In the **Name** field, enter a name for the Check Point SASE gateway, for example, *Harmony_SASE_Gateway*.
    b. In the **IPv4 Address** field, enter the Check Point SASE gateway public IP address.

        To find the SASE Gateway public IP Address:

        i. Access the SASE Administrator Portal and click **Networks**.
        ii. Select the network.
        iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

    c. Click **OK**.

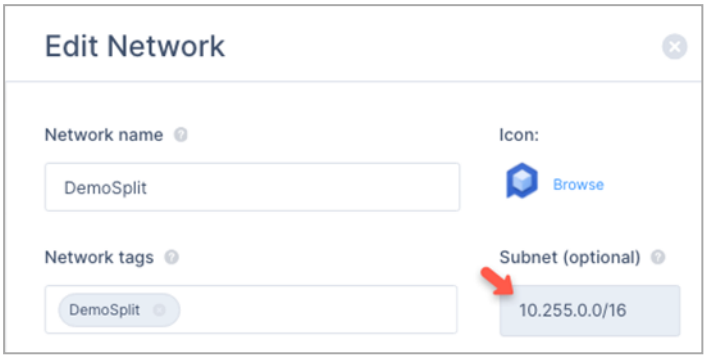
Step 2: Add SASE Gateway IP Address and Remote Subnet to the Interoperable Device Object

1. Log in to the SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network:

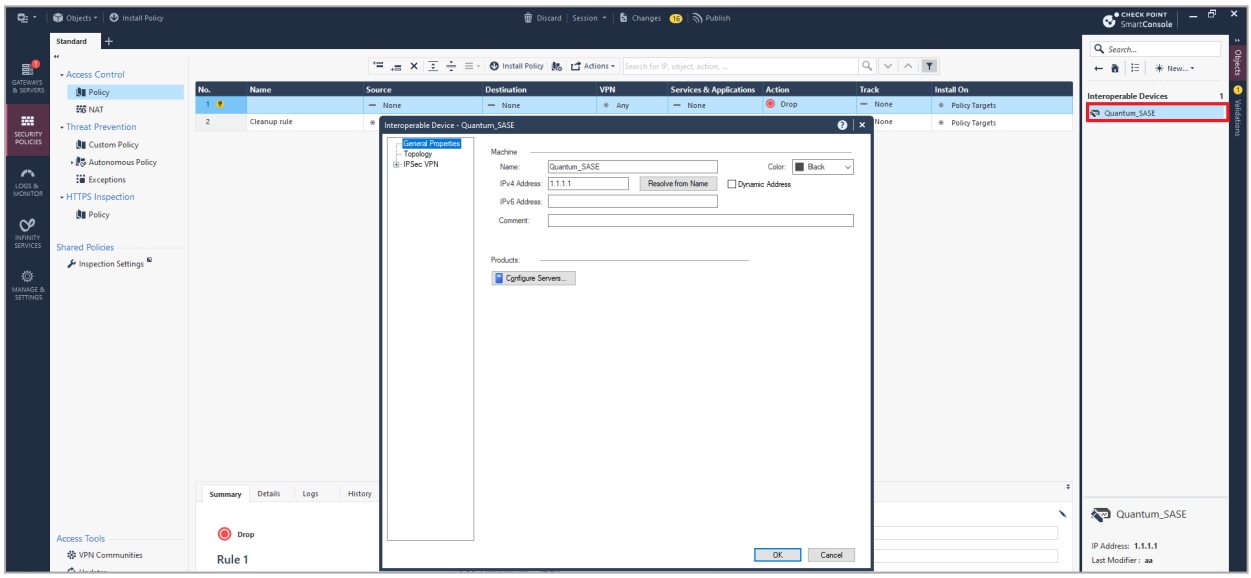
a. Select a network, scroll to the end of the row and click ... .

b. Select **Edit Network**.

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

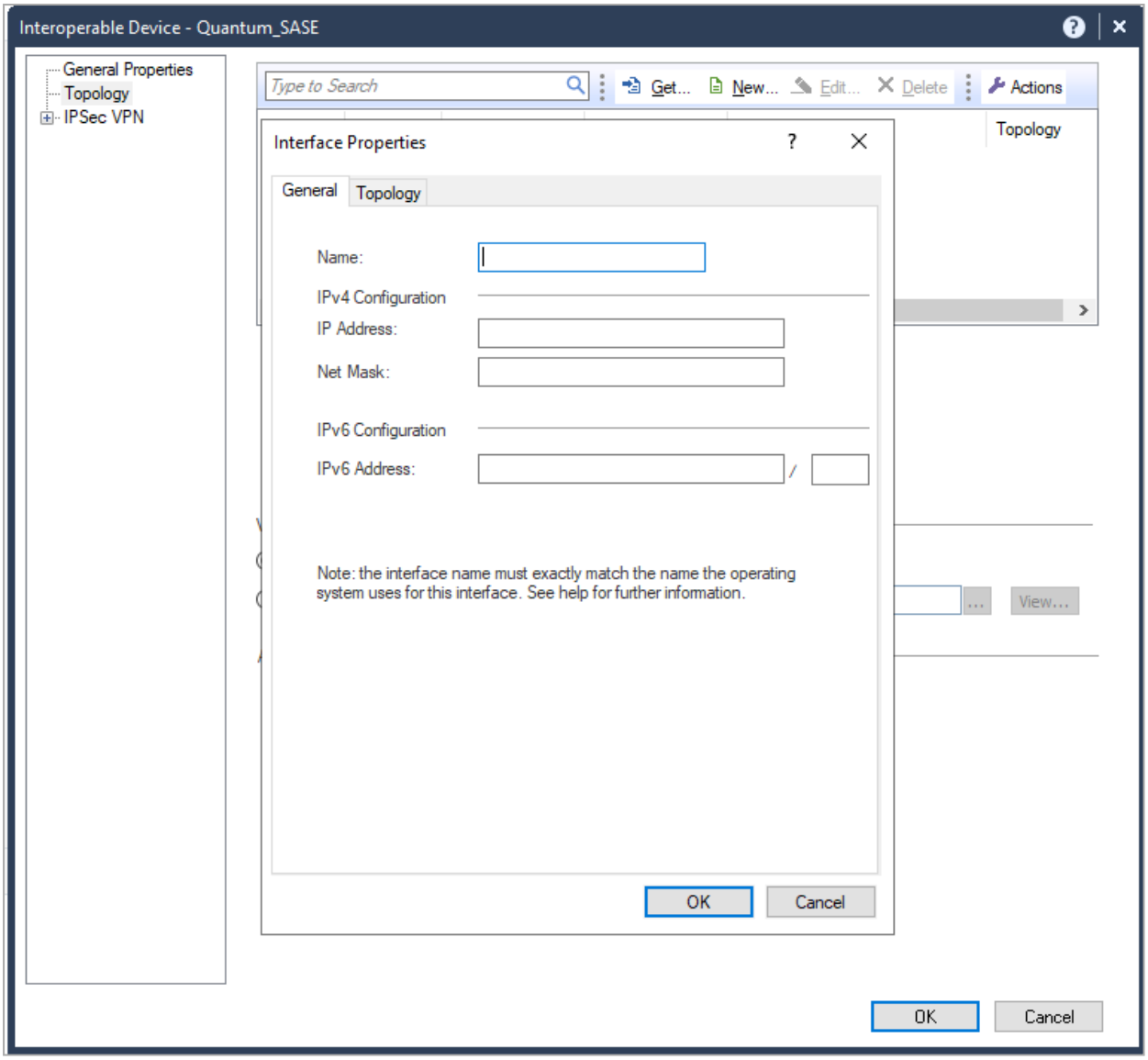


4. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

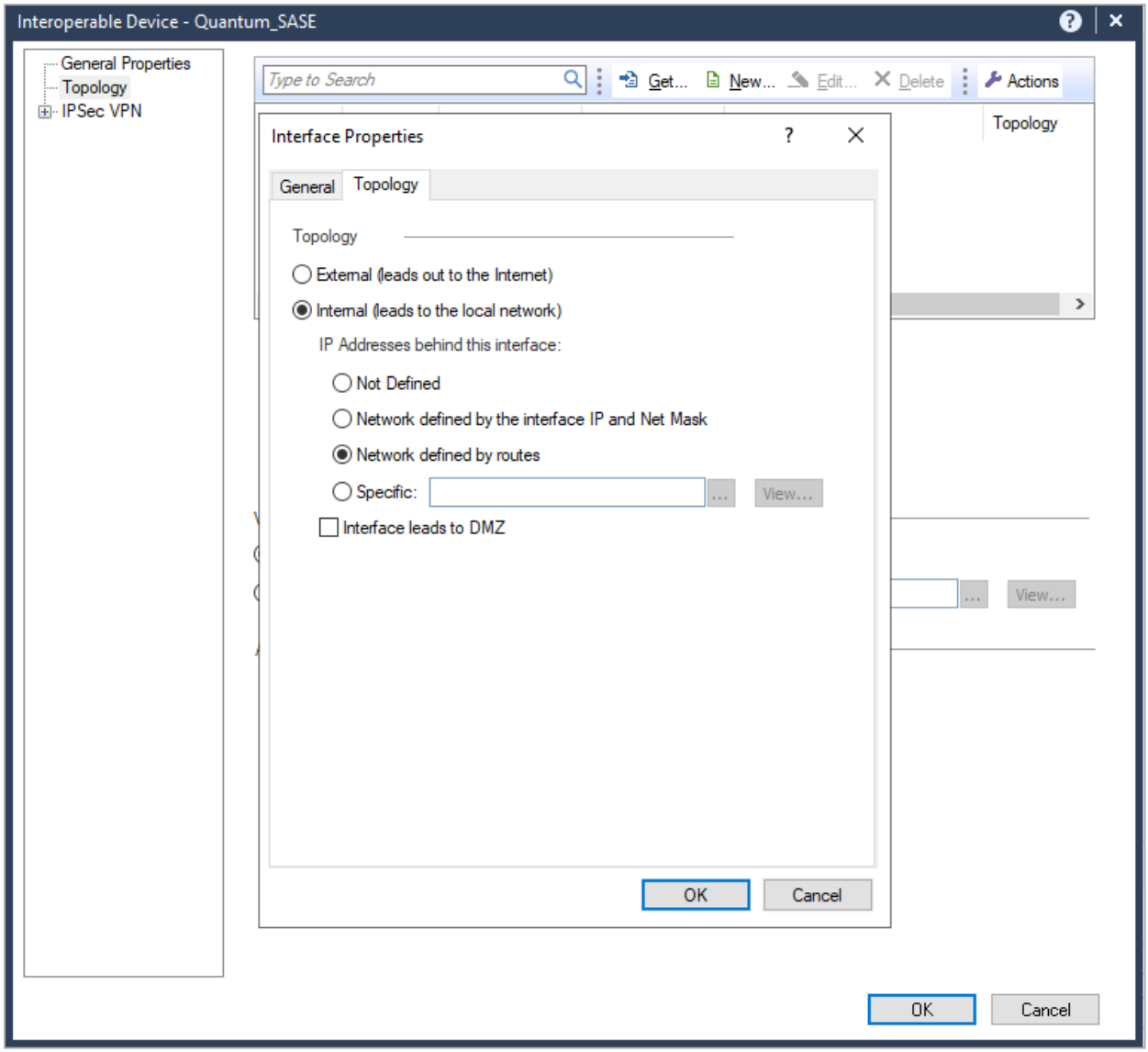
5. Click **Topology > New**.



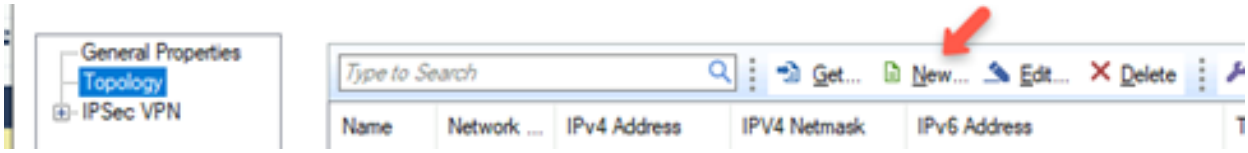
6. In the **General** tab, enter these details:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

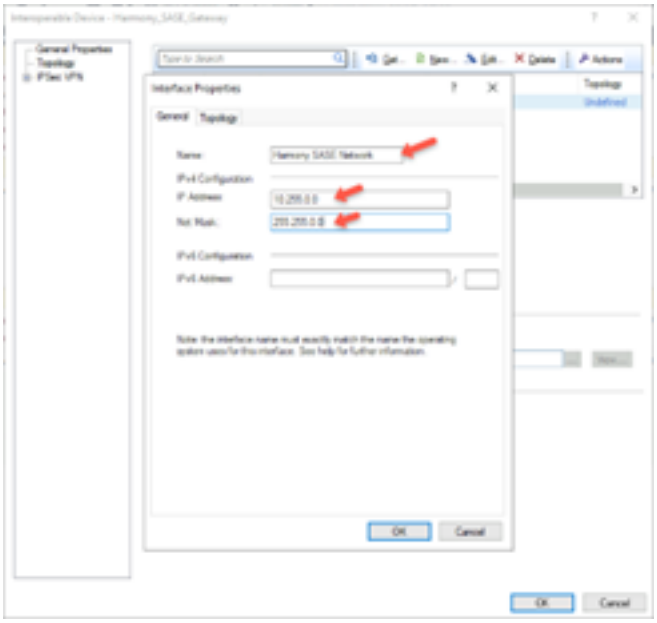
7. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



8. Click **OK**.
9. Click **Topology** > **New**.

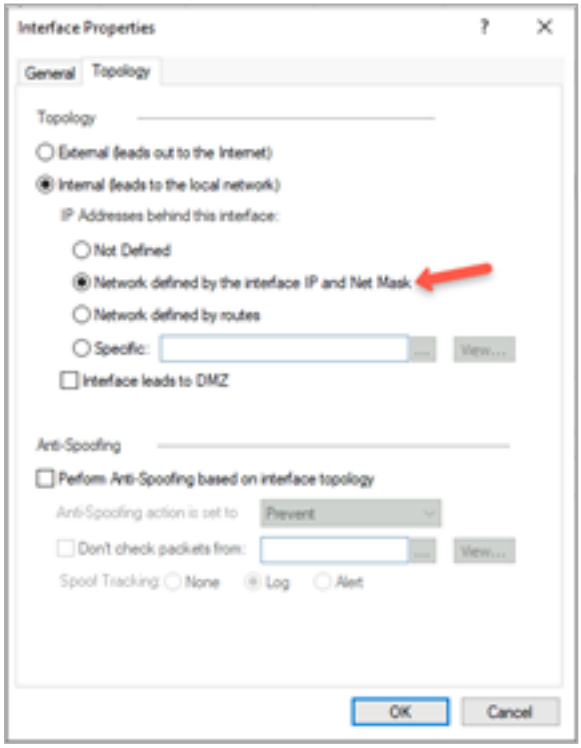


10. In the **General** tab, enter these details:



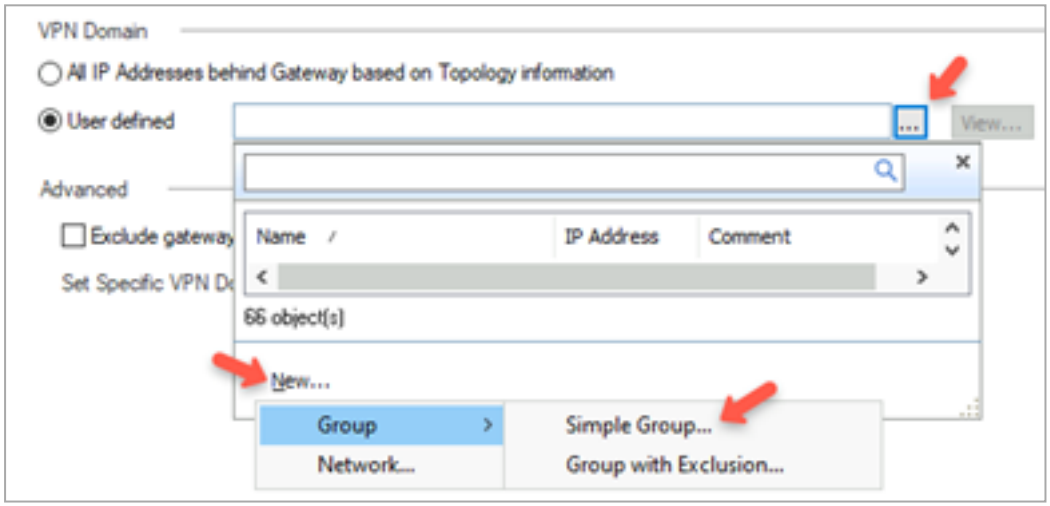
Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Check Point SASE gateway.
Net Mask	255.255.255.255

11. In the **Topology** tab, select **External (leads to the local Internet)**.

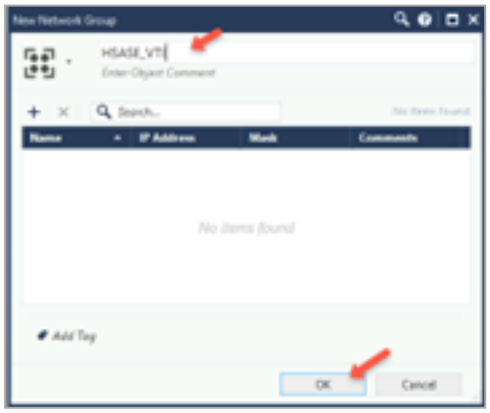


12. Click **OK**.

13. Click **Topology** > **New**.
14. In the **General** tab, enter these:
    a. **Name** - Name for the topology, for example, Harmony_SASE_Gateway.
    b. **IP Address** - Public IP address of the SASE gateway.
    c. **Net Mask** - 255.255.255.255
15. Click the **Topology** tab.
16. Select **External (leads out to the internet)**.
17. Click **OK**.
18. In the **VPN Domain** section, select **User defined** and click ... .
19. Click **New** and go to **Group** > **Simple Group**.



The **New Network Group** window appears.

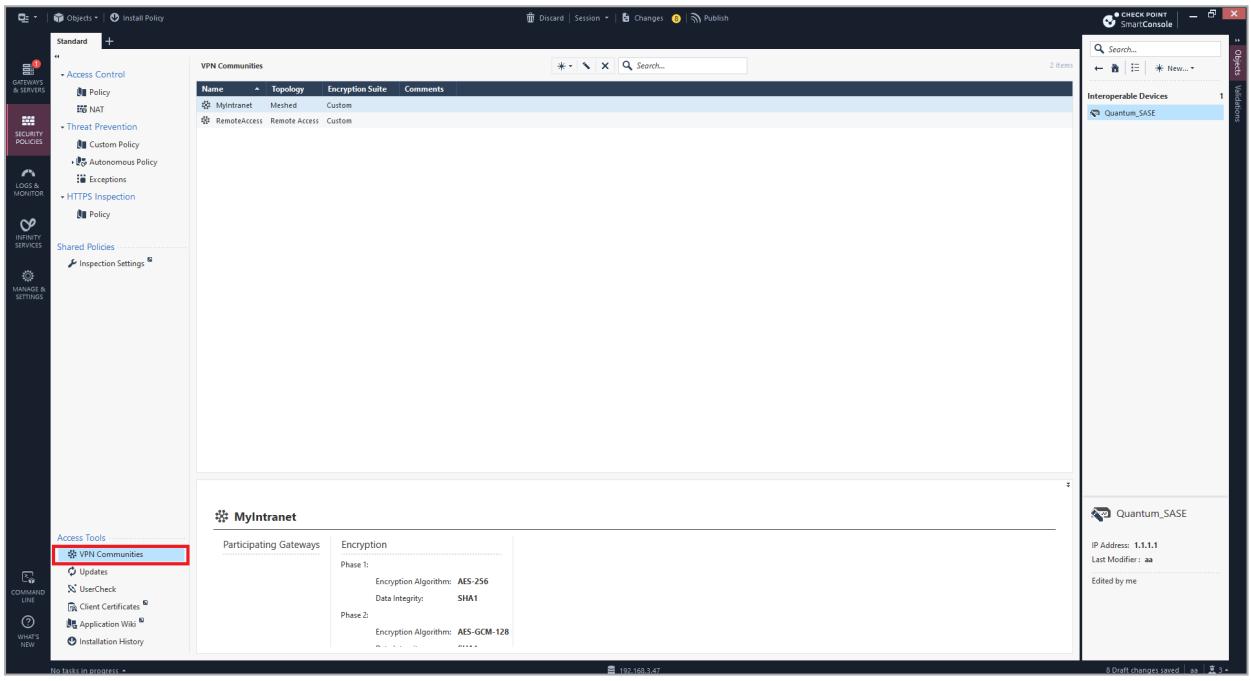


20. In the **Enter Object Comment** field, enter a name, for example, *HSASE_VTI*, and click **OK**.

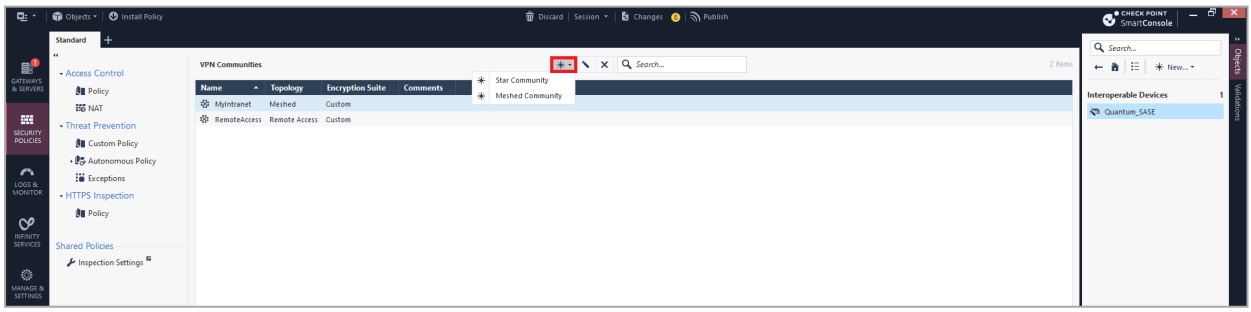
21. For the other SASE gateway and Check Point gateway, follow the same procedure in *"Step 1: Create Interoperable Device Object in the Check Point SmartConsole" on page 301* and *"Step 2: Add SASE Gateway IP Address and Remote Subnet to the Interoperable Device Object" on page 303*.
22. Publish and install the policy.

Step 3: Create VPN Start Community

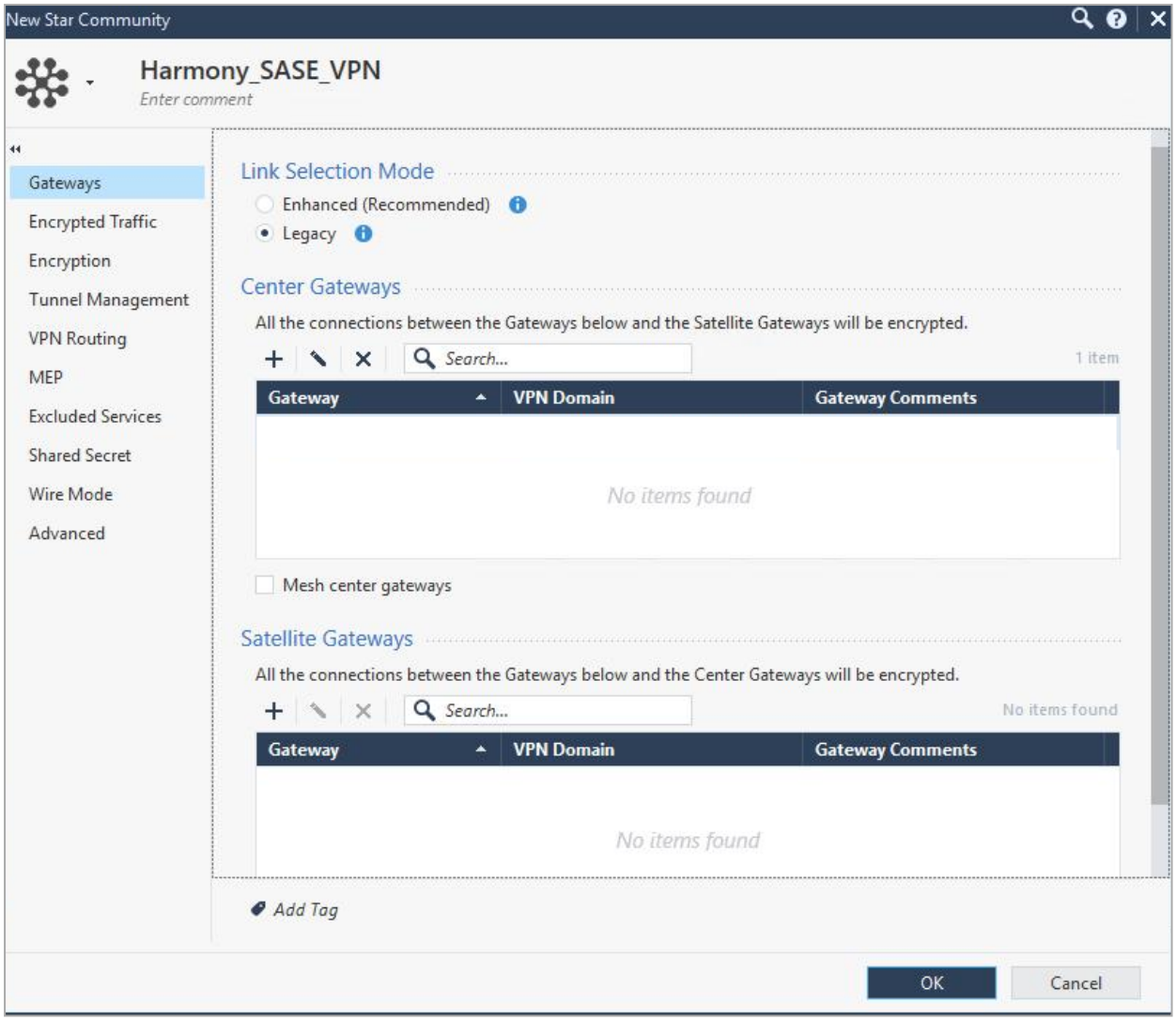
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Select an object, click **New** and go to **More** > **VPN Community** > **Star Community**.



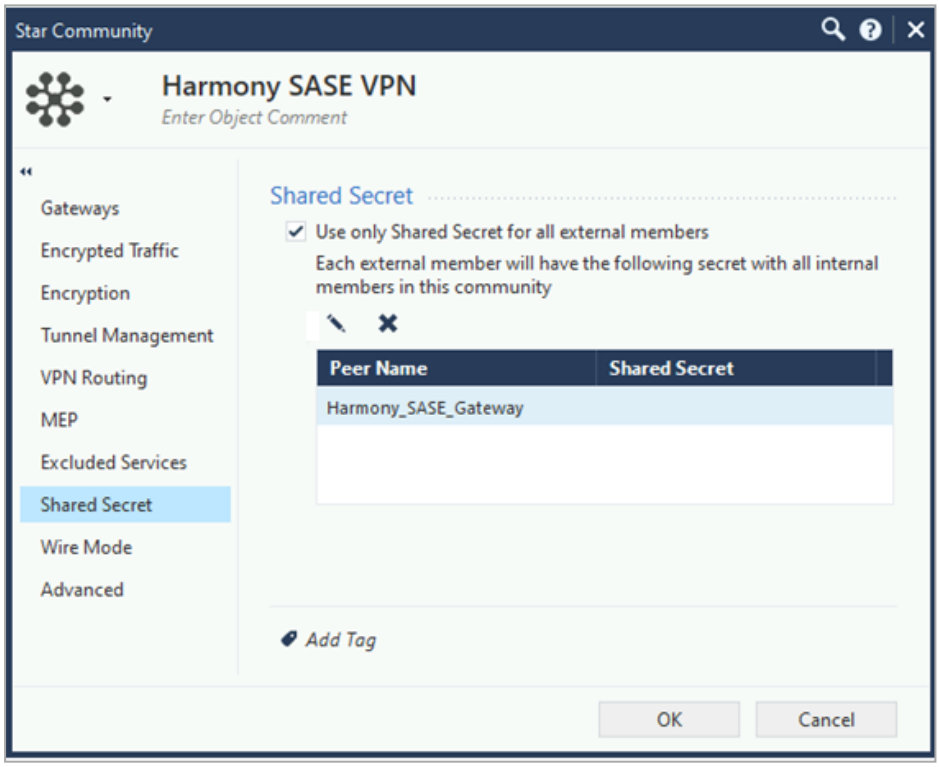
The **New Star Community** window appears.



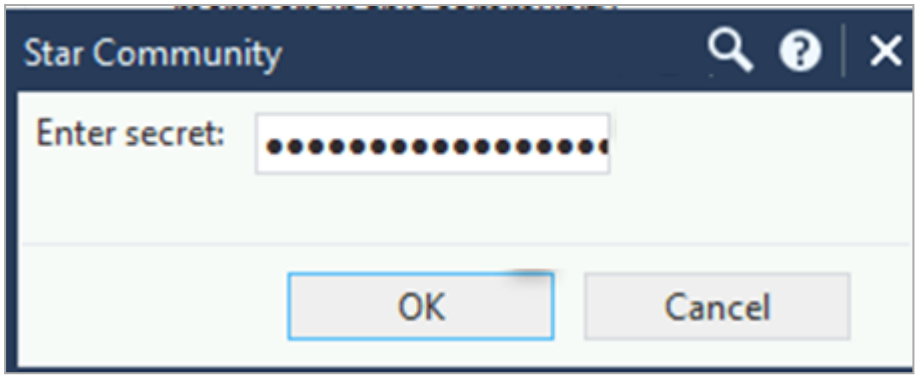
5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, *Harmony_SASE_VPN*.
6. In the **Link Selection Mode** section, select one of these:
   - **Enhanced (Recommended)** - Uses dynamic, intelligent, probe-based logic to choose the optimal VPN link. It evaluates:
     - Interface status
     - Multiple external IP addresses
     - Multiple ISP circuits
     - Reachability through Next-Hop Probing
     - SLA-like behavior for tunnel selection

- **Legacy** - Uses static or basic logic to select the VPN interface or IP address. Selection is based on:
  - Main IP (default)
  - Selected interface
  - Selected IP
  - IP address determined by topology

7. Under **Center Gateways**, click + and add the Check Point Gateway.
8. Under **Satellite Gateways**, click + and add the Interoperable Device Object created for the Check Point Gateway. See *"Step 1: Create Interoperable Device Object in the Check Point SmartConsole" on page 301*.
9. Go to **Shared Secret** and click ✎ to edit the shared key.



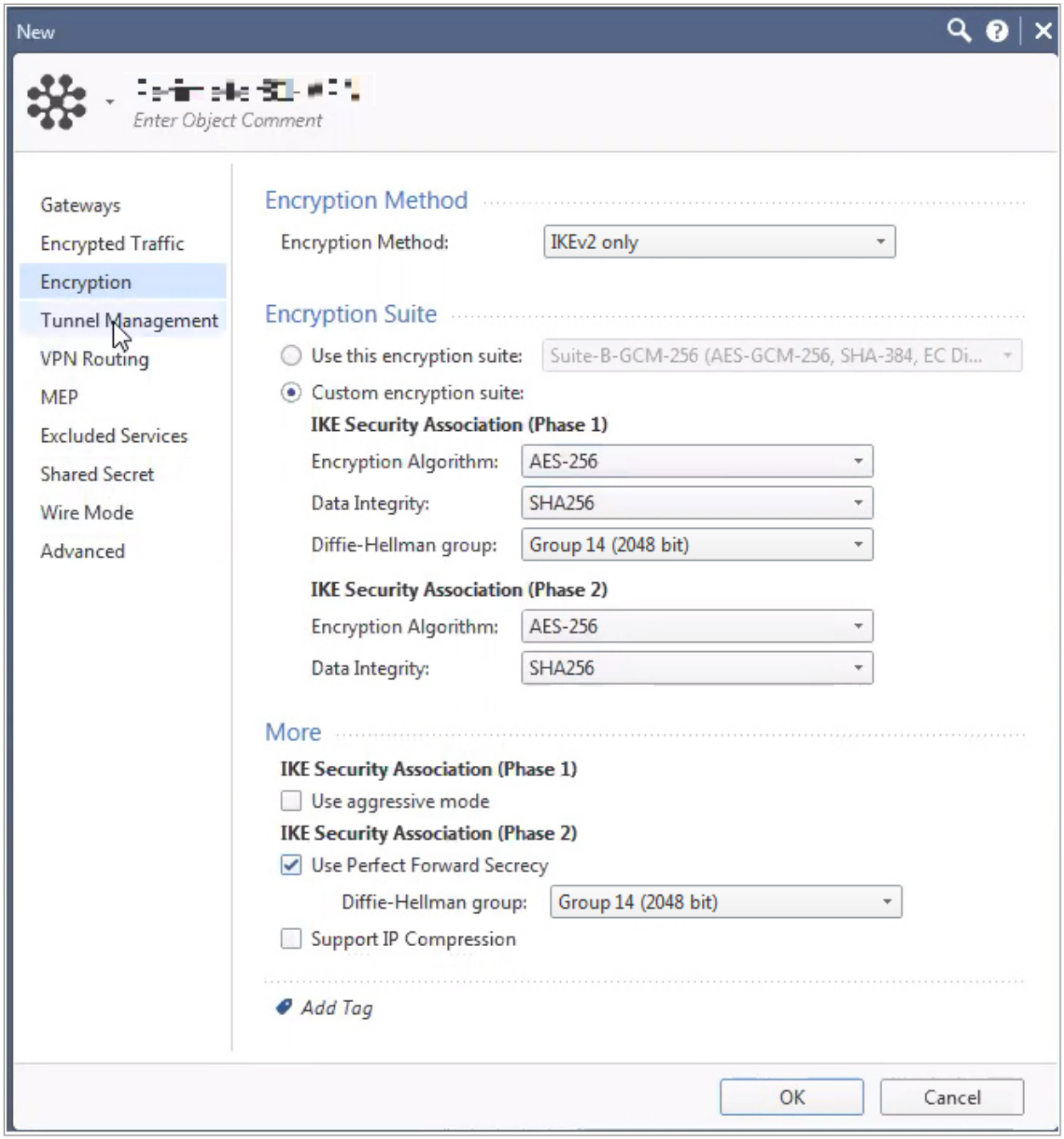
10. In the **Enter secret** field, enter an appropriate key.



Notes:

- Copy the key as it is required while configuring the IPsec Tunnel in the SASE Administrator Portal.
- Check Point recommends that the share secret key is at least 20 characters in length.

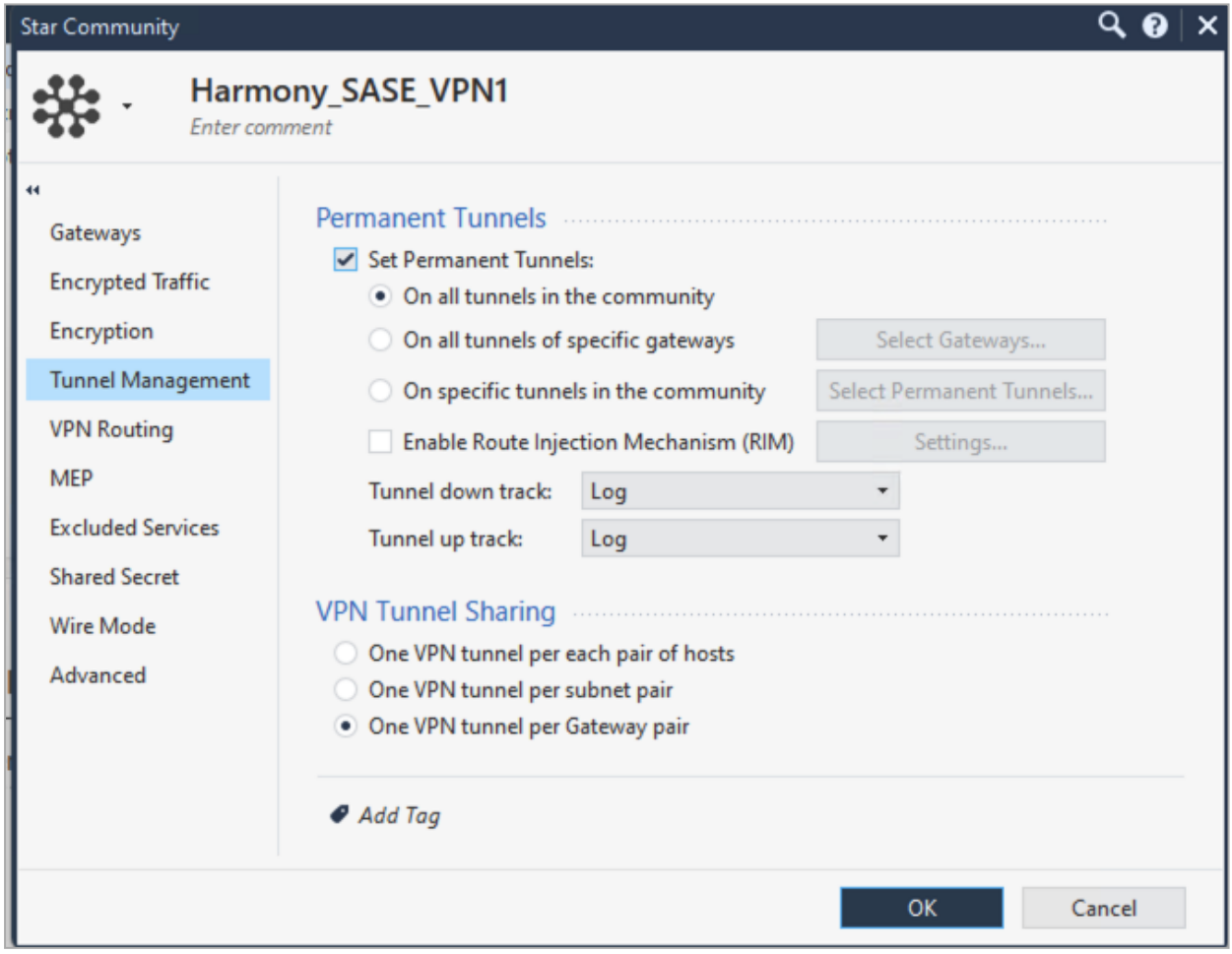
11. Click **OK**.
12. From the left navigation pane, click **Encryption** and enter these:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256

Field	Enter
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

13. Click **Tunnel Management**.
14. In the **Permanent Tunnels** section, select the **Set Permanent Tunnels** checkbox and then select **On all tunnels in the community**.



15. In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

    Important - Make sure that you enter the remote subnets specified here in the Check Point SASEAdministrator Portal. A mismatch can disconnect the tunnel.

16. Click **Advanced**.
    - In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.
    - In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.
17. Click **OK**.
18. Publish and install the policy.

Step 4: Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Check Point SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Check Point SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

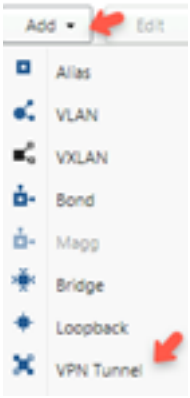
   Note - The network configuration differs if you have not changed the default settings during SASE network creation. For testing purposes, you should initially allow any/any or allow ping before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

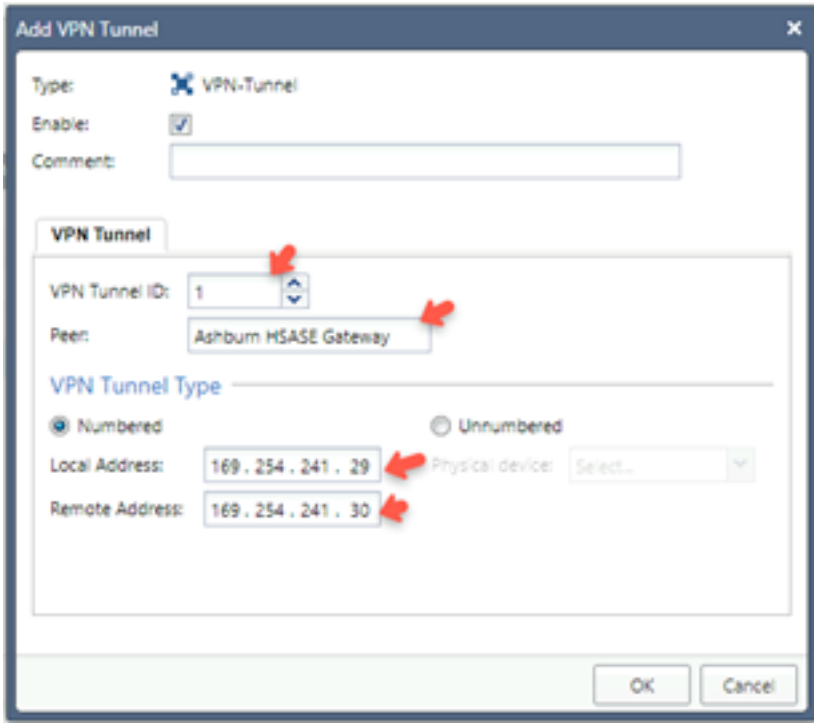
Step 5: Configure VPN Tunnel Interface and BGP

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Click **Network Interfaces**.
3. From the **Add** list, select **VPN Tunnel**.



The **Add VPN Tunnel** page appears.

4. Enter these:

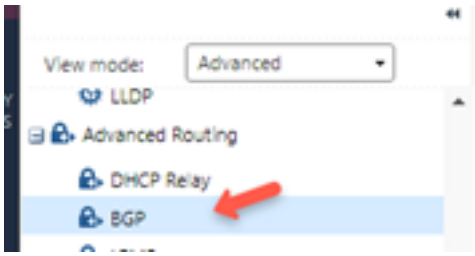


   - **VPN Tunnel ID** - Select a unique ID.
   - **Peer** - Name of the interoperable device previously created for the first SASE Gateway.
   - **VPN Tunnel Type** - Numbered.
   - **Local Address** - Internal address for the Quantum Gateway (within 169.254.x.x/30 ranges).
   - **Remote Address** - Internal address for the SASE Gateway (within 169.254.x.x/30 ranges, corresponding to the above).
5. Click **OK**.
6. Repeat steps 3 through 5 and create the second VPN Tunnel.

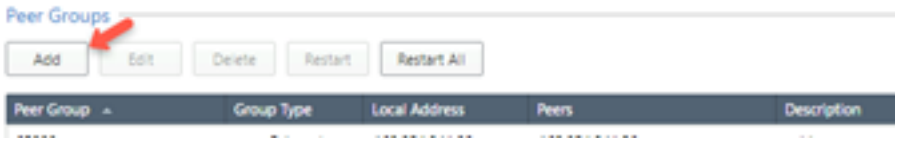
7. Perform steps 1 through 6 on the second Check Point Gateway Gaia Portal.
8. Log in to the Check Point SmartConsole.
9. Open the Gateway Cluster Properties.
10. Go to **Network Management**.
11. From the **Get Interfaces** list, select **Get interfaces Without Topology**.
12. Once the two VPN Tunnel Interfaces are added, click the first tunnel interface.
13. Go to **General**.
14. In the **IPv4** field, add the Virtual IP (VIP) that matches the member IP addresses.
15. Repeat steps 12 through 14 on the second tunnel interface.
16. Publish and install the policy.

Step 6: Configure BGP Configuration

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Go to **Advanced Routing** and select **BGP**.

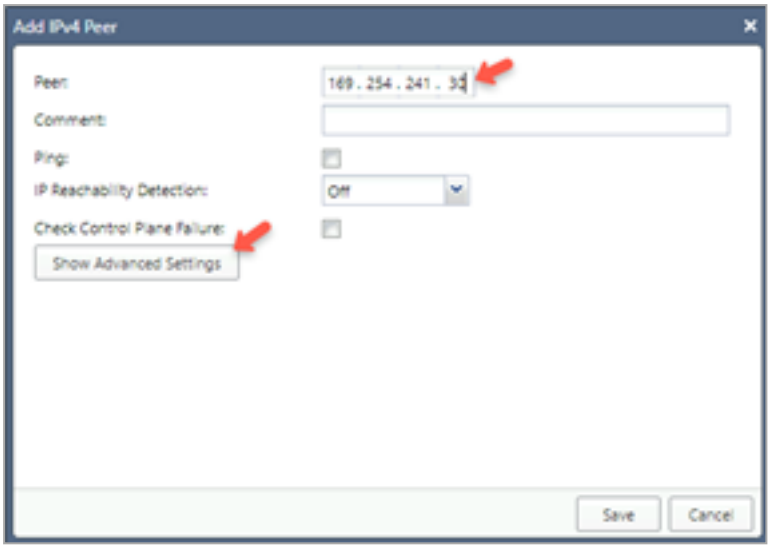


3. In the **Peer Groups** section, click **Add**.

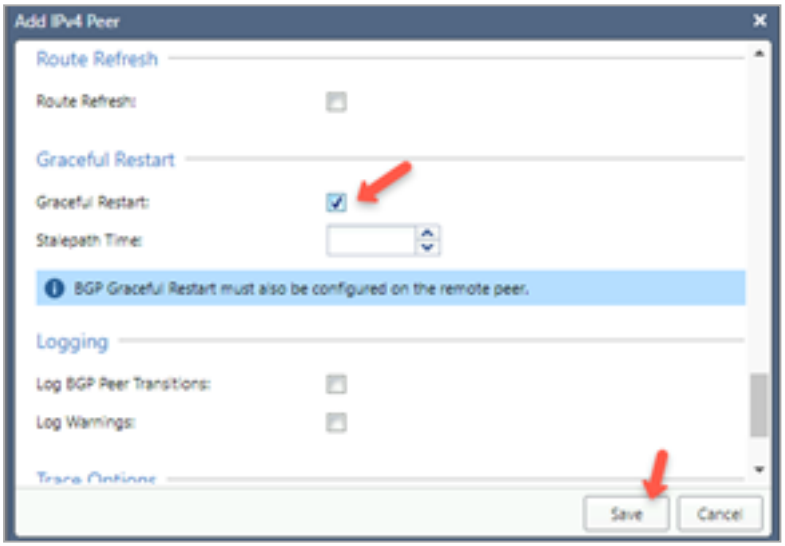


4. Enter these:
   - **Peer AS Number** - The AS Number of the SASE network. If not set already, enter **64512**.
   - **Peer Group Type** - External.
   - **Local Address** - The local address entered while configuring VPN Tunnel Interface. See step 14 in *"Step 5: Configure VPN Tunnel Interface and BGP" on page 315*.
5. Click **Add Peers**.
6. Enter these:

a. In the **Peer** field, enter the Remote Address set under the VTI configuration in Step 4 and click **Show Advanced Settings**.



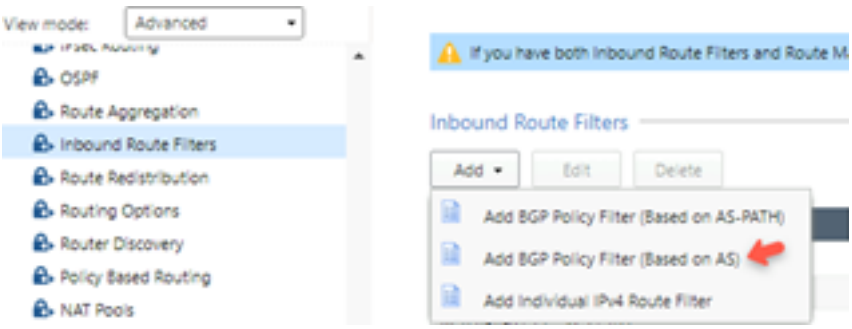
b. Select the **Graceful Restart** checkbox.



c. Select the **eBGP Multihop** checkbox and click **Save**.

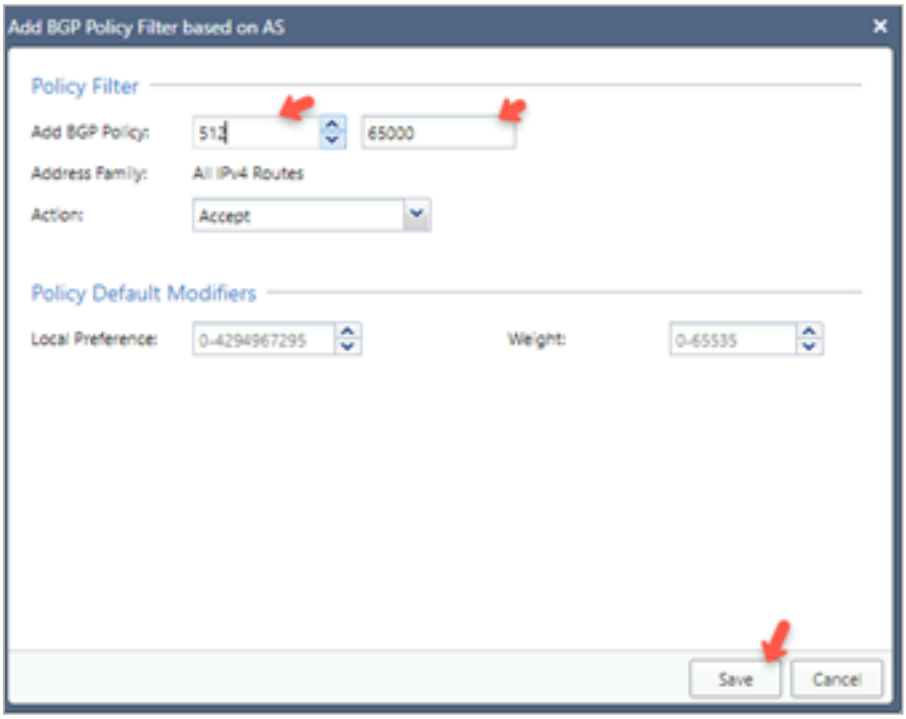
Note - If **eBGP Multihop** is not enabled, the BGP session cannot be established.

7. Repeat step 6 and add the address of the second interface remote address.
8. From the **View mode** list, select **Advanced Routing** and click **Inbound Route Filter**.
9. From the **Add** list, select **Add BGP Policy Filter (Based on AS)**.

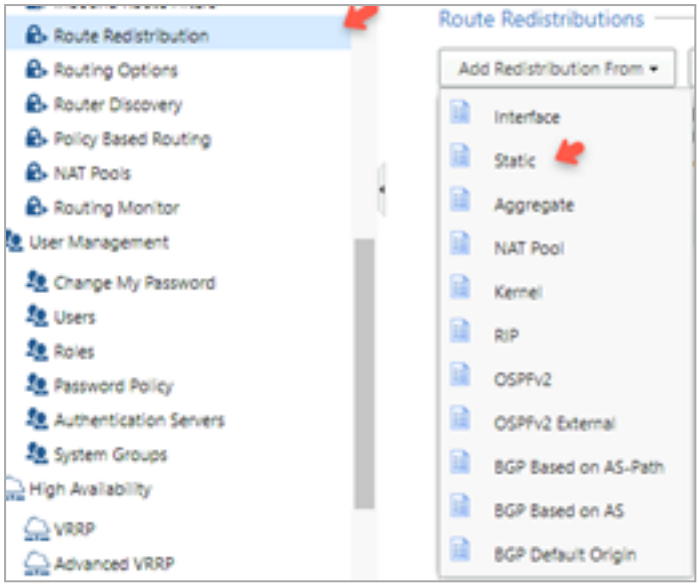


The **Add BGP Policy Filter based on AS** window appears.

10. Specify these:
    a. **Add BGP Policy** - Set a number from the available range.
    b. **AS Number** - Set the AS Number of the SASE Network.
    c. **Action** - Accept



11. Click **Save**.
12. From the **View mode** list, select **Advanced Routing** and then, click **Route Redistribution**.
13. From the list, select **Add Redistribution From**.
14. Select **Static**.



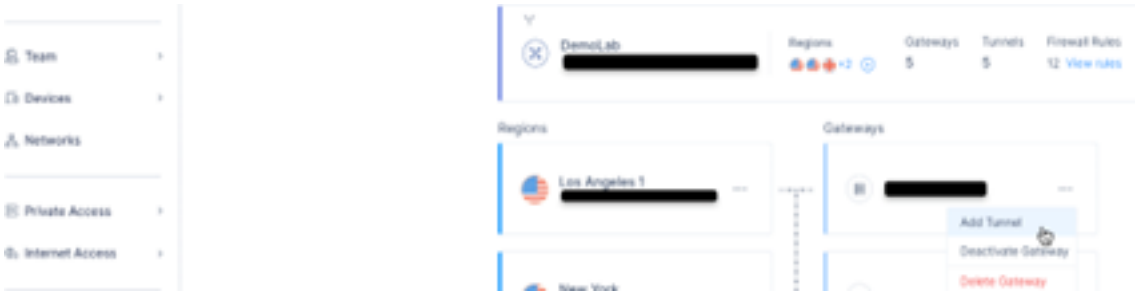
Note - For BGP, no routes are accepted from a peer by default. You must configure an explicit Inbound BGP Route Filter to accept a BGP route from a peer.

15. Repeat the same procedure for the second Check Point Gateway in the Gaia Portal.

Part 2 - Configuration in the SASE Administrator Portal

Step 1: Configure Tunnel and Routes Table

1. Access the SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· .
4. Select **Add Tunnel** for the gateway from which you want to add the IPsec Site-2-Site VPN tunnel.

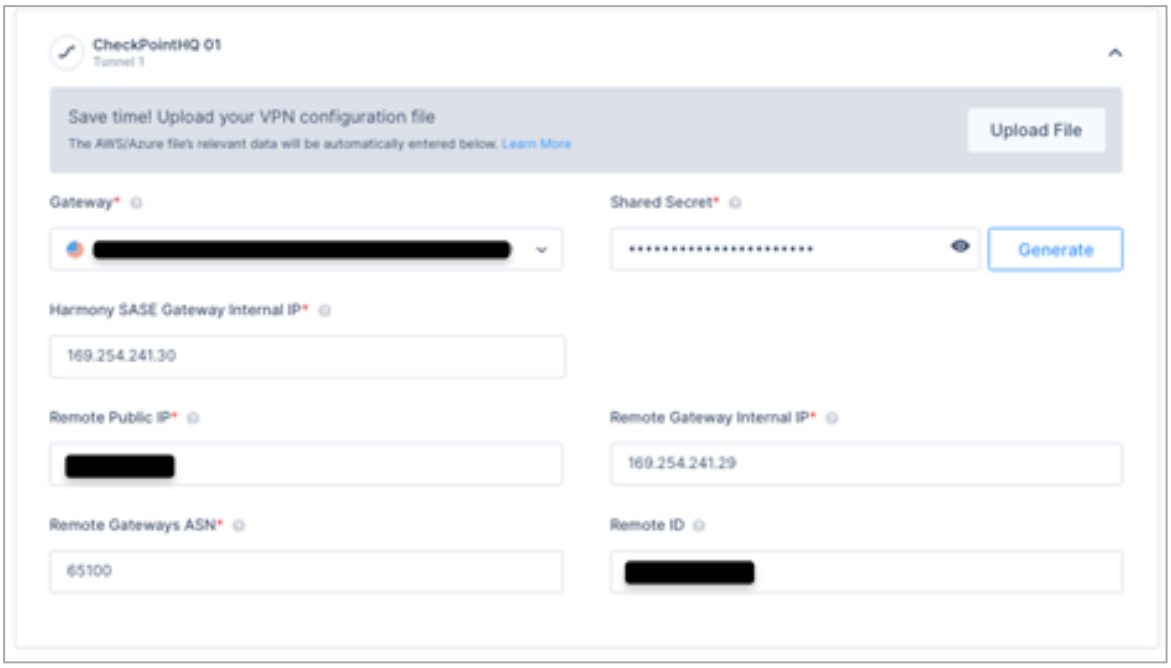


a. Click **IPSec Site-2-Site Tunnel** and click **Continue**.

b. Click **Redundant Tunnels** and click **Continue**.

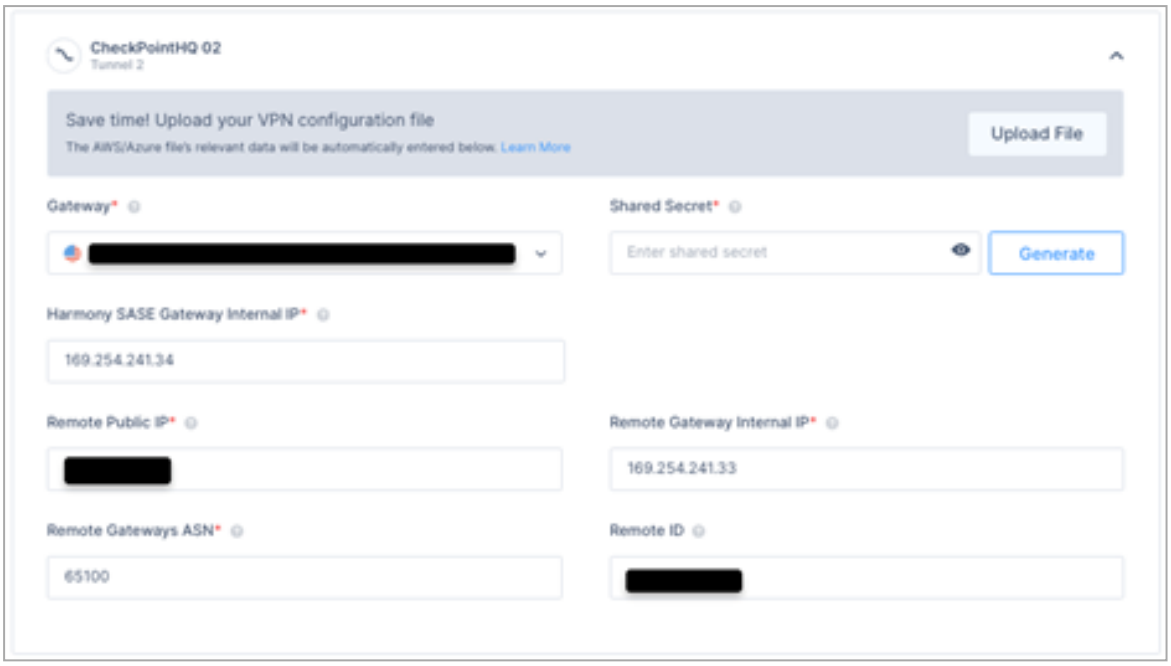
c. In the **Tunnel name** field, enter a logical name.

d. Expand Tunnel 1 and specify these:



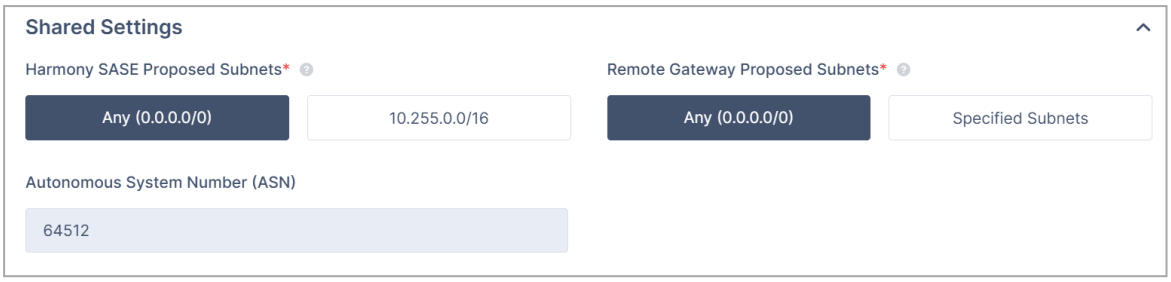
- **Shared Secret** - The value previously set on the first start policy.
- **SASE Gateway Internal IP** - The remote address of the first Check Point Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the first Quantum Gateway.
- **Remote Gateway Internal IP** - The VIP of the first VTI interface.
- **Remote Gateways ASN** - The ASN of the first Quantum Gateway.
- **Remote ID** - The router ID of the first Quantum Gateway used under the BGP settings above.

e. Expand Tunnel 2 and specify these:



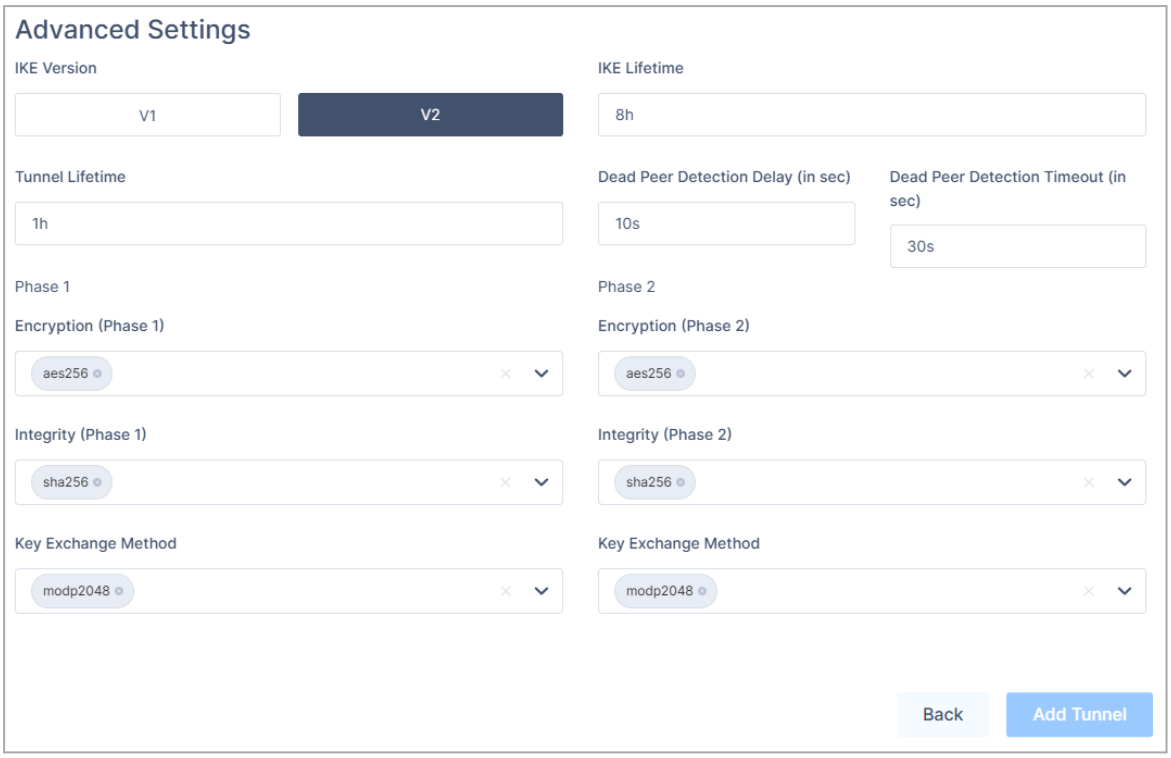
- **Gateway** - Select the second SASE Gateway for the tunnel.
- **Shared Secret** - The value previously set on the second star policy.
- **SASE Gateway Internal IP** - The remote address of the second Quantum Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the second Quantum Gateway.
- **Remote Gateway Internal IP** - The VIP of the second VTI interface.
- **Remote Gateways ASN** - The ASN of the second Quantum Gateway.
- **Remote ID** - The router ID of the second Quantum Gateway used under the BGP settings above.

f. Expand **Shared Settings** and specify these:



- **Check Point SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Autonomous System Number (ASN)** - Default value is **64512**, if not set, enter the AS Number for the Check Point SASE network.

g. In the **Advanced Settings** section, specify these:



- **IKE Version**: V2
- **IKE Lifetime**: 8h
- **Tunnel Lifetime**: 1h
- **Dead Peer Detection Delay**: 10s
- **Dead Peer Detection Timeout**: 30s
- **Phase 1**:
  - **Encryption(Phase 1)**: aes256
  - **Integrity (Phase 1)**: sha256
  - **Key Exchange Method**: modp2048
- **Phase 2**:
  - **Encryption(Phase 2)**: aes256
  - **Integrity (Phase 2)**: sha256
  - **Key Exchange Method**: modp2048

h. Click **Add Tunnel**.

5. Select **Routes Table**:

a. Click **Add Route**.

The **Add Route** window appears.

b. Enter all the subnets on the remote side of the tunnel and then click **Add Route**.

c. Click **Apply Configuration**.

Step 2: Verify the Setup

Once you complete the above steps, your tunnel should be active.

1. Verify the setup in the SASE Administrator Portal:
   a. Click **Networks**.
   b. Locate the tunnel you create, and check the tunnel status.

   It should indicate that the tunnel is **Up**, signifying a successful connection.
2. Verify the setup in the SASE Agent:
   a. Connect to your network using the SASE Agent.
   b. Access one of the resources in your environment.

Configuring Check Point Redundant IPsec Tunnel

This topic explains how to establish a single Site-to-Site tunnel between your SASE Network and Check Point Firewall.

Pre-requisites

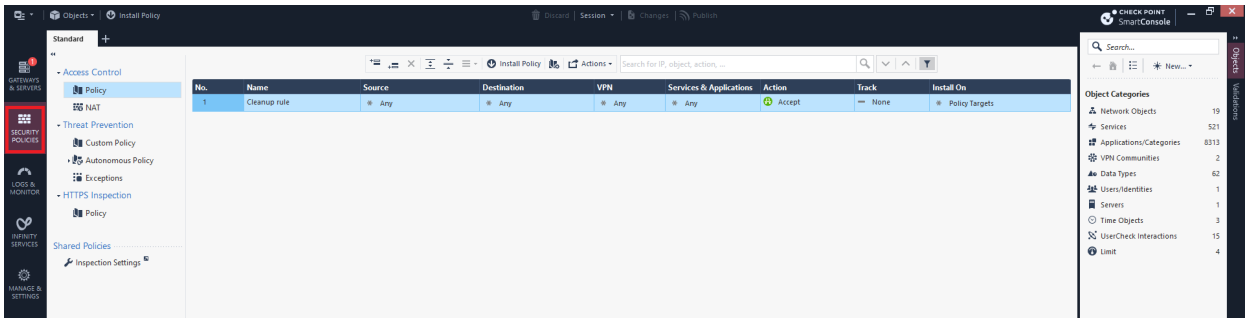
- SASE Administrator Portal account.
- Device with SASE Agent installed.
- Administrator account with Firewall, Router, and Cloud Management Portal.

- A cluster of two Quantum gateways, each with a public IP.
- Configuration with ISP redundancy PMTR-68991 is not supported.

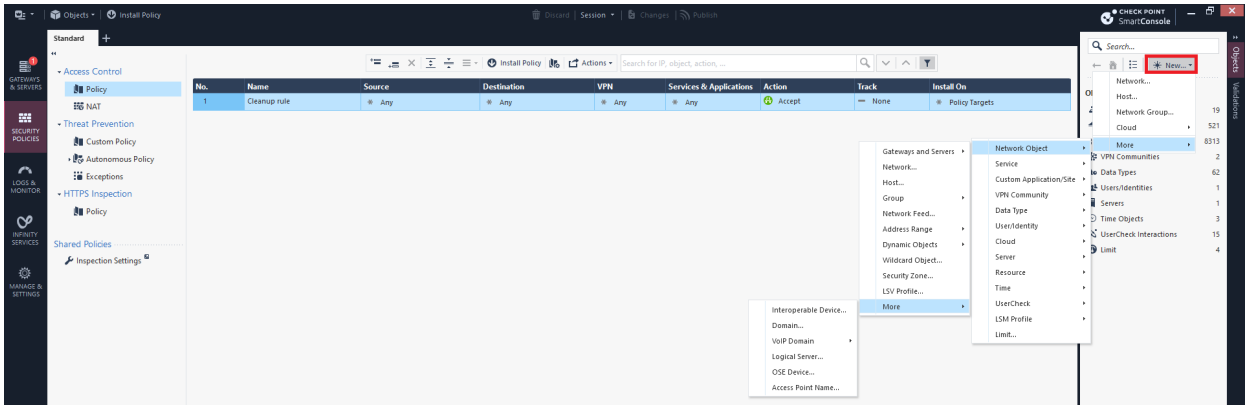
Part 1 - Configuration in SmartConsole

Step 1: Creating Interoperable Device Object in the Check Point SmartConsole

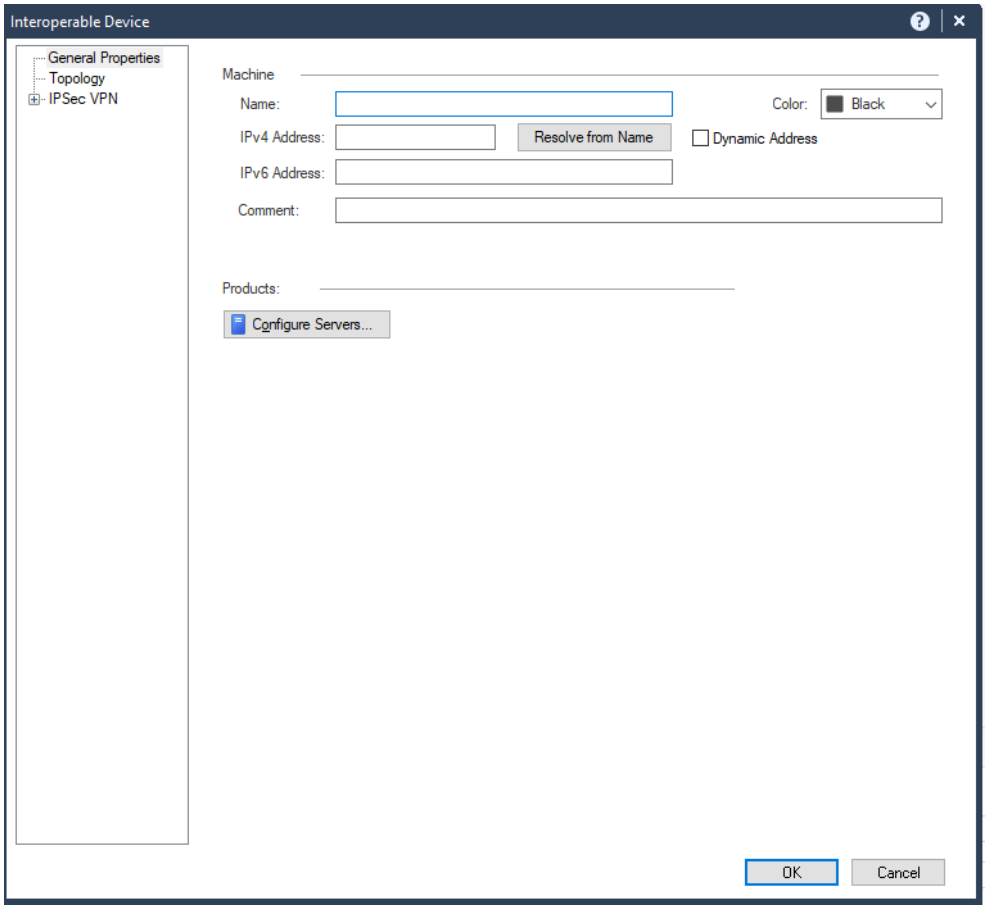
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. In the Objects pane, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



a. In the **Name** field, enter a name for the Check Point SASE gateway, for example, Check Point_SASE_Gateway.

b. In the **IPv4 Address** field, enter the Check Point SASE gateway public IP address.

   To find the SASE Gateway public IP Address:

   i. Access the SASE Administrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

c. Click **OK**.

d. Click on the left top corner of the page.

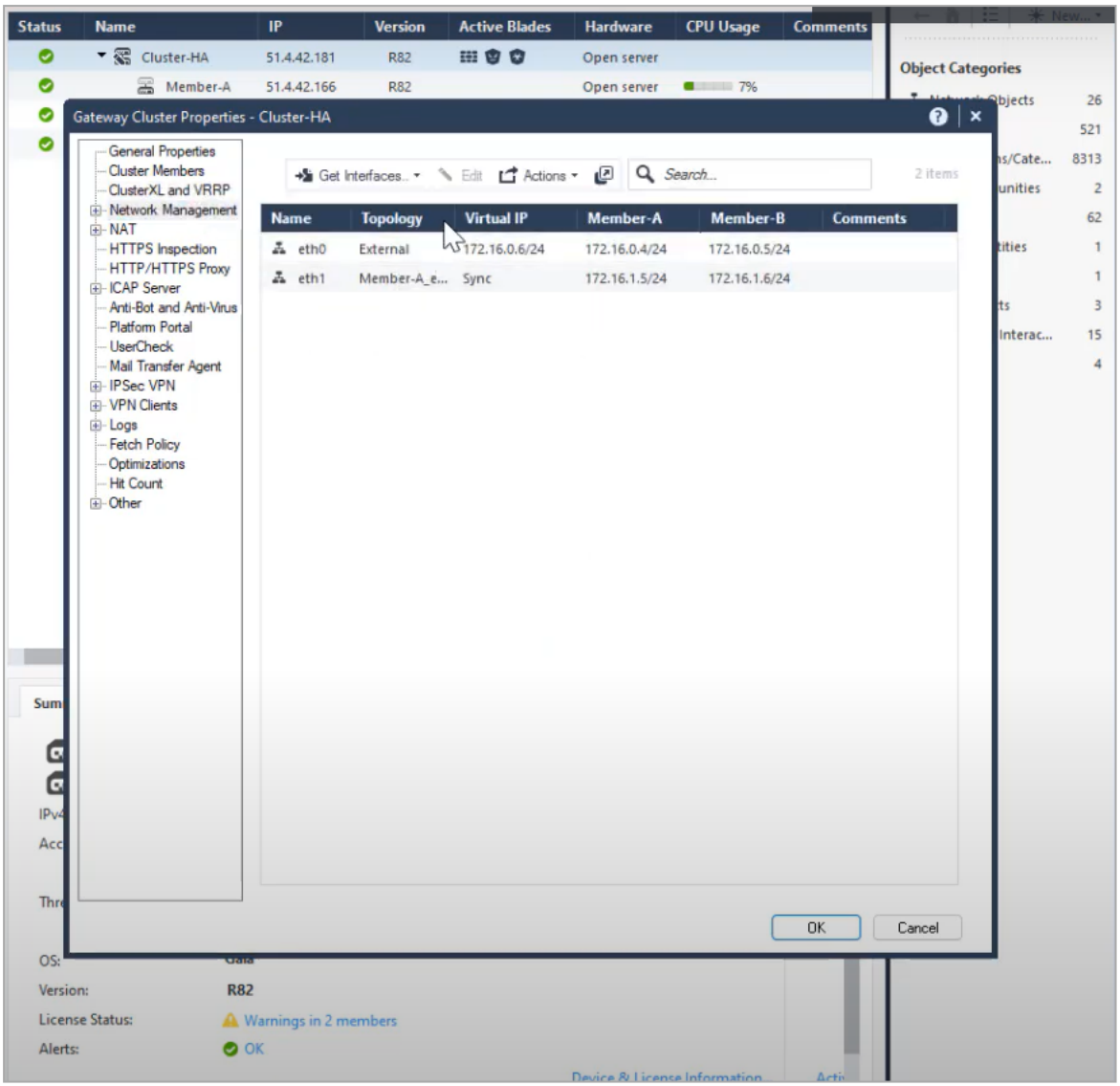
e. Select **Global properties**.

f. Go to **VPN** > **Advanced**.

g. Select the **Enable VPN Directional Match in VPN Column** checkbox.

h. Click **OK**.

i. Select the cluster from the table.



j. Click **General Properties**.

k. Select the **IPSec VPN** checkbox.

l. Click **Network Management**.

m. Click **Get Interfaces**.

n. Select **Get Interfaces With Topology**.

The **SmartConsole** window appears.

o. Click **Yes**.

p. Double-click the Cluster Member 1.

q. In the **IPv4 Address** field, enter the Check Point SASE gateway public IP address.

   To find the SASE Gateway public IP Address:

   i. Access the SASEAdministrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

r. Click **Modify**.

s. In the **Anti-Spoofing** section, unselect the **Perform Anti-Spoofing based on interface topology** checkbox.

t. Click **OK**.

u. Click **OK**.

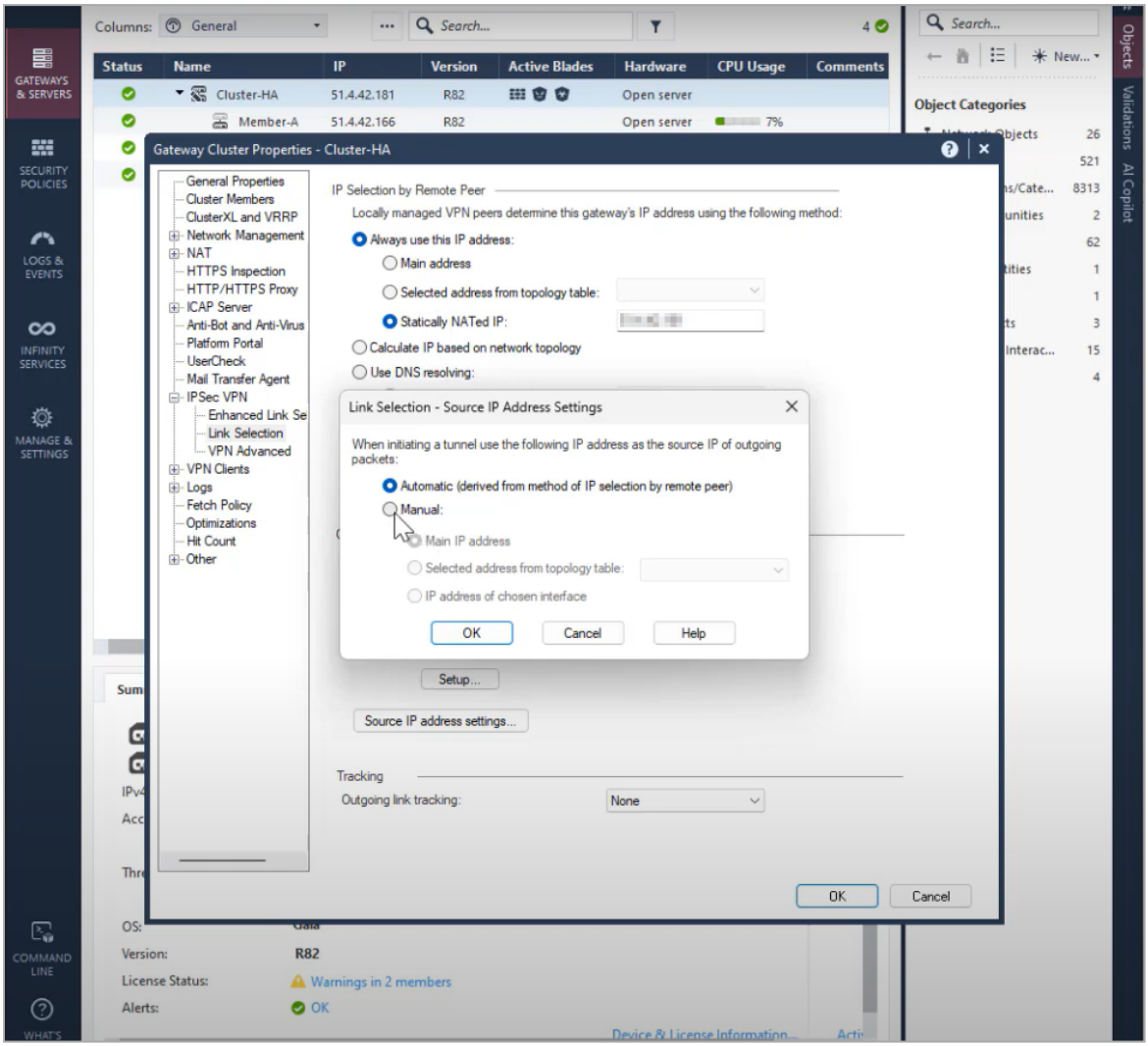
v. Repeat step from **p** through **u** for Cluster Member 2.

w. Go to **IPSec VPN** > **Link Selection**.

x. Select the **Statically NATed IP** checkbox and enter the Check Point SASE gateway public IP address.

y. Click **Source IP address settings**.

The **Link Selection - Source IP Address Settings** window appears.



z. Select **Manual** and then select **Selected address from topology table** checkbox.

aa. From the list, select the private IP address.

ab. Click **OK**.

ac. Click **OK**.

ad. Publish and install the policy.

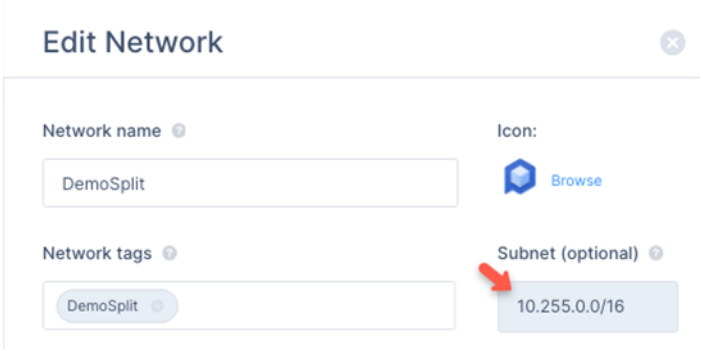
Step 2: Adding SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object

1. Log in to the SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network:

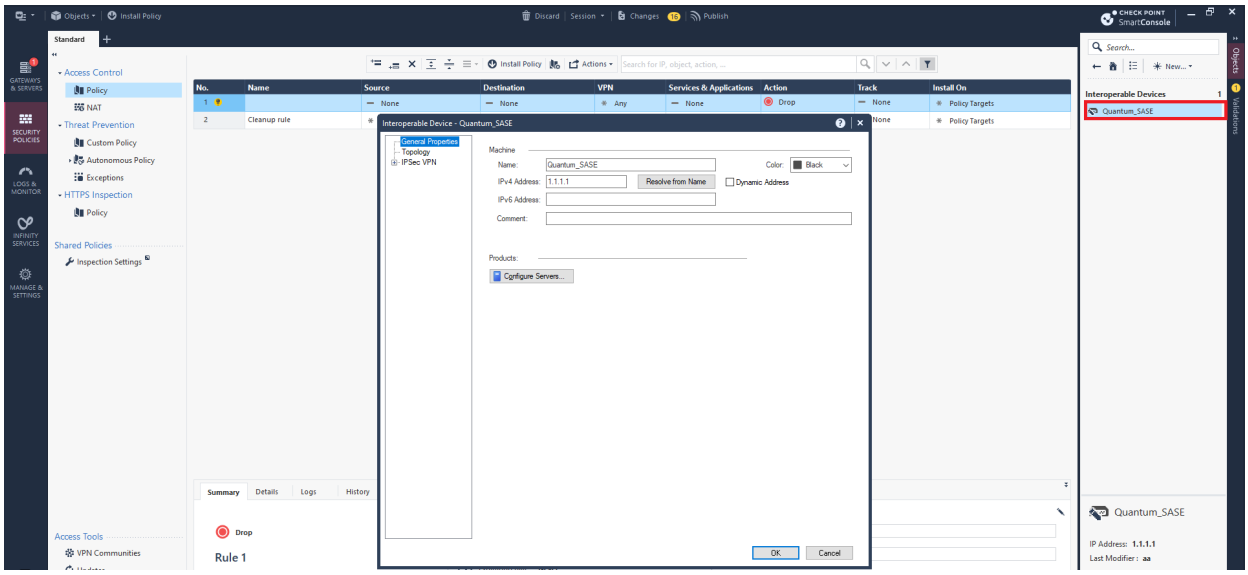
a. Select a network, scroll to the end of the row and click ... .

b. Select **Edit Network.**

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

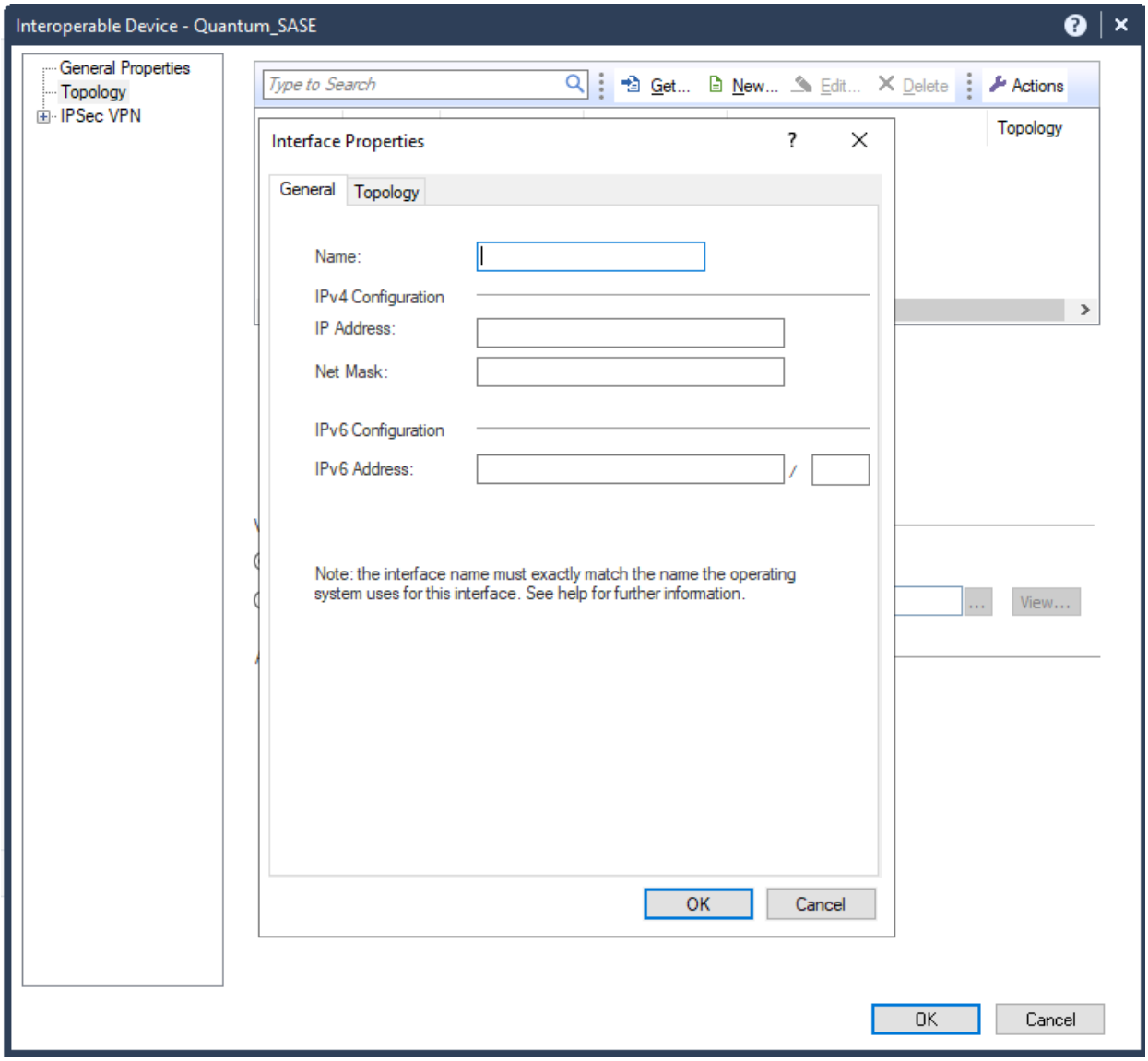


4. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

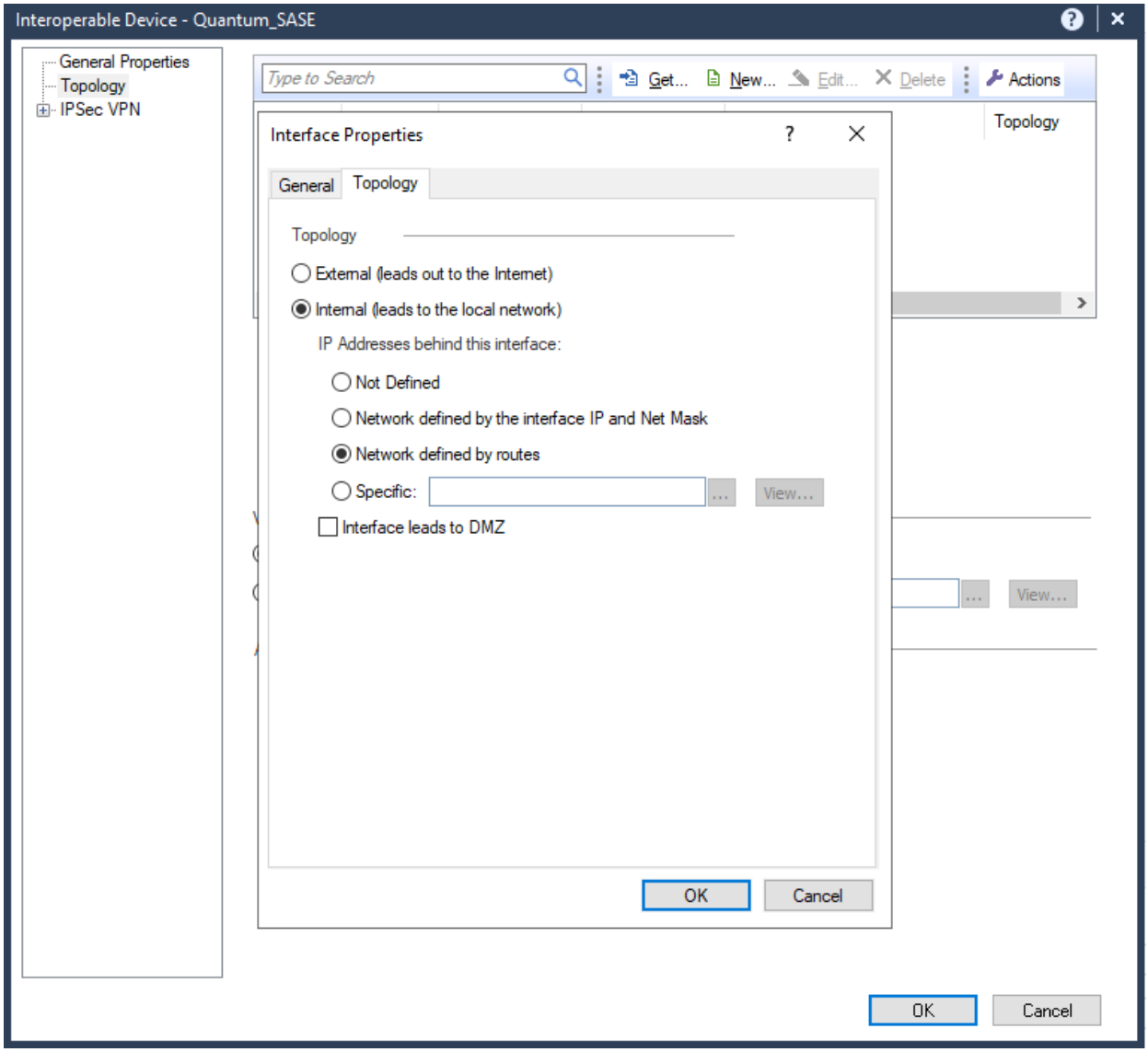
5. Click **Topology > New**.



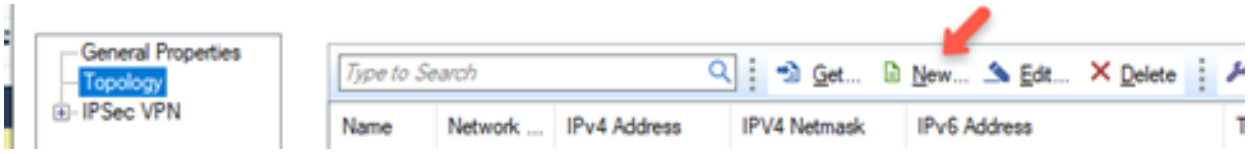
6. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

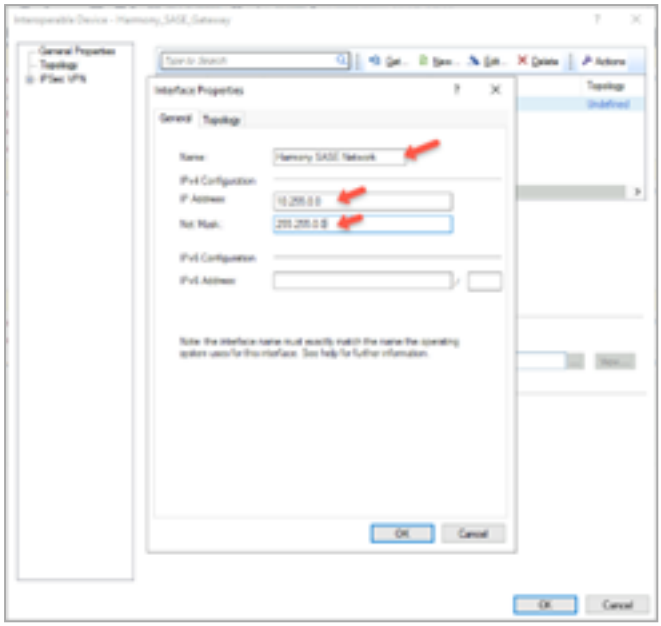
7. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



8. Click **OK**.
9. Click **Topology** > **New**.

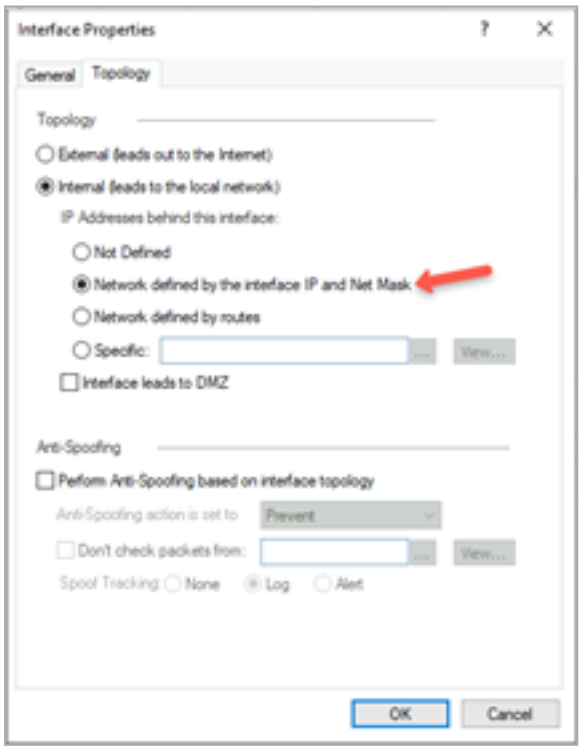


10. In the **General** tab:



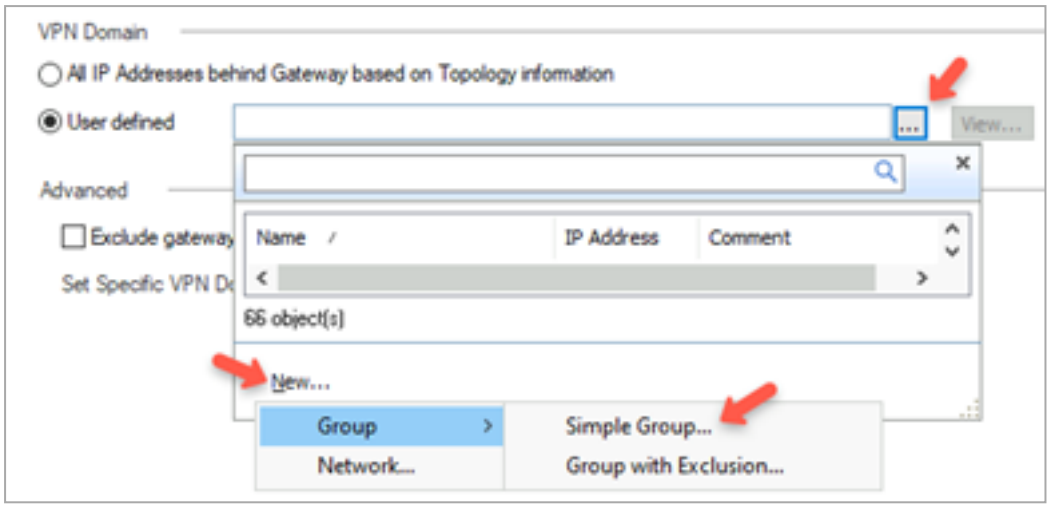
Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Check Point SASE gateway.
Net Mask	255.255.255.255

11. In the **Topology** tab, select **External (leads to the local Internet)**.



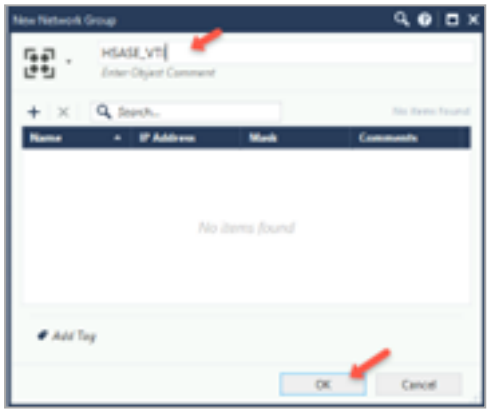
12. Click **OK**.

13. In the **VPN Domain** section, select **User defined** and click ··· .



14. Click **New** and go to **Group** > **Simple Group**.

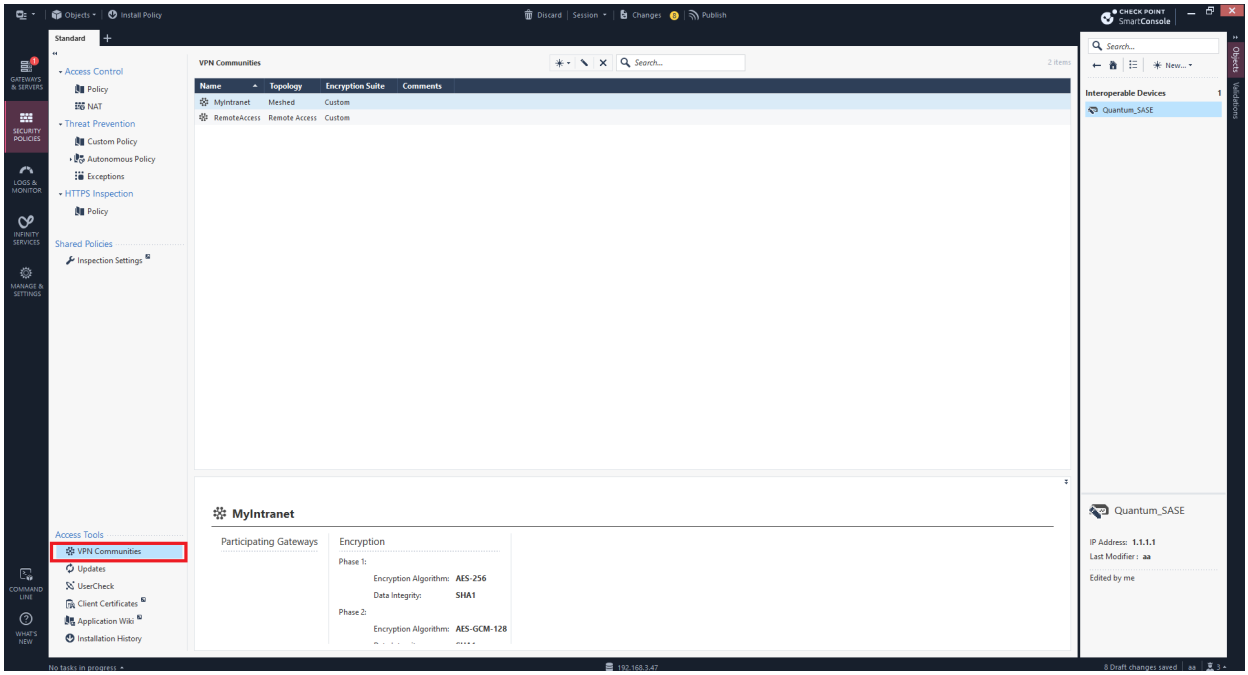
    The **New Network Group** window appears.



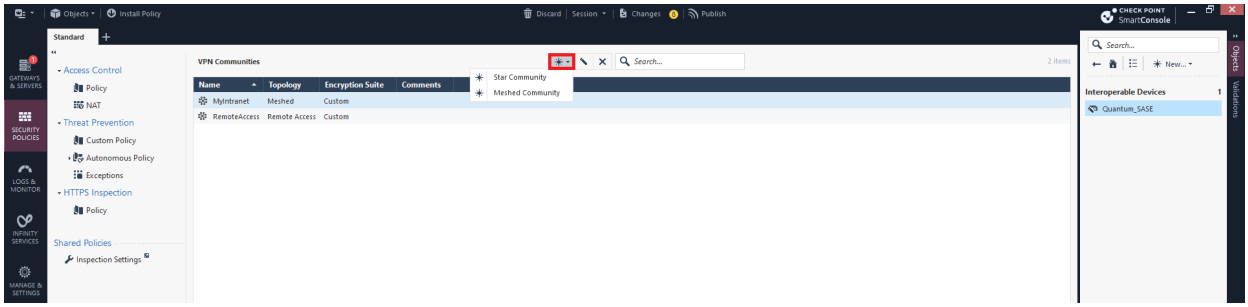
15. In the **Enter Object Comment** field, enter a name, for example, HSASE_VTI, and click **OK**.
16. For the other Check Point SASE Gateway and Check Point Gateway, follow the same procedure in **Creating Interoperable Device Objects in the Check Point SmartConsole** and **Adding SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object sections**.
17. Publish and install the policy.

Step 3: Creating VPN Start Community

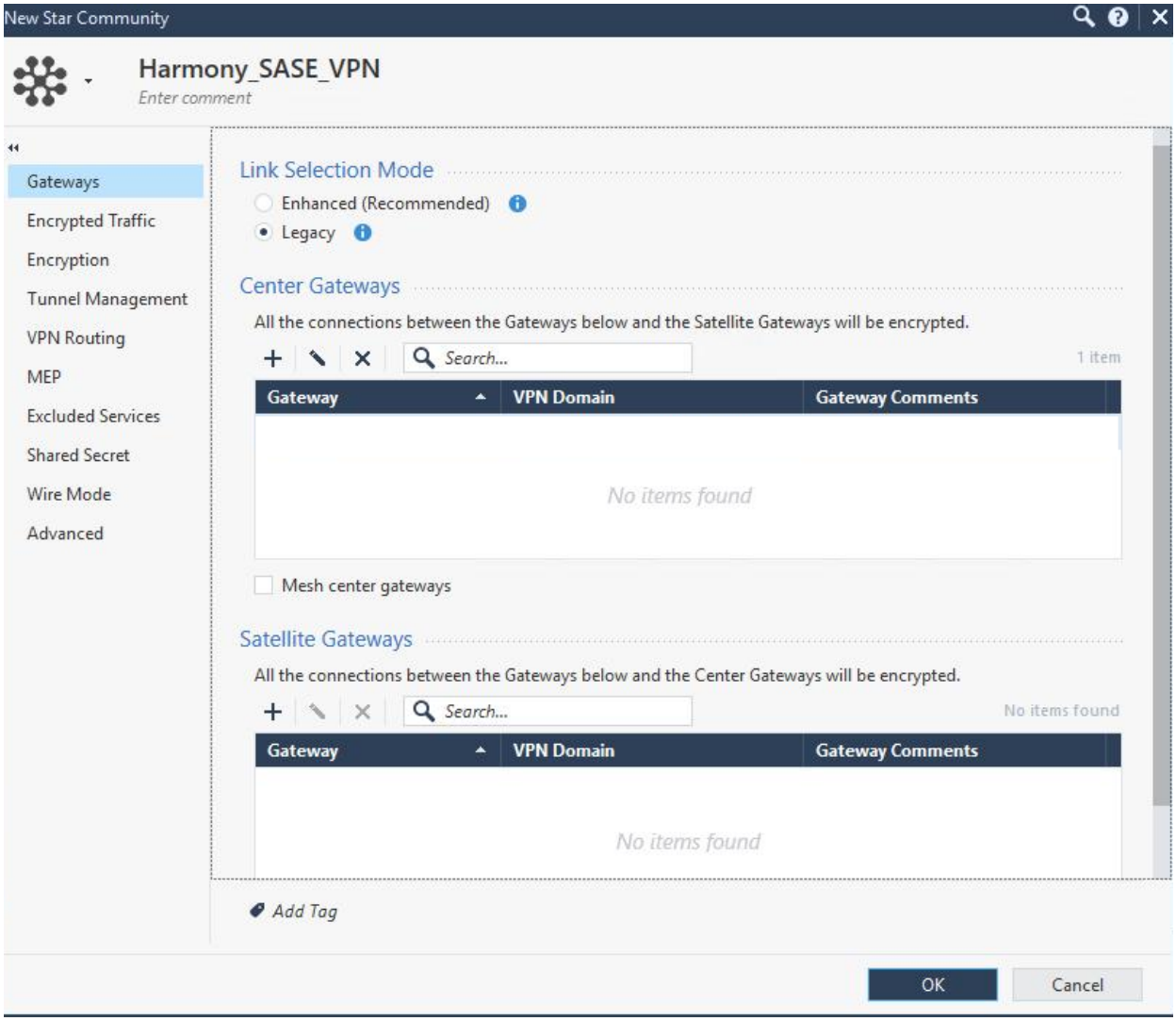
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Select an object, click **New** and go to **More** > **VPN Community** > **Star Community**.



The **New Star Community** window appears.



5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, Check Point_SASE_VPN.
6. In the **Link Selection Mode** section, select one of these:
   - **Enhanced (Recommended)** - Uses dynamic, intelligent, probe-based logic to choose the optimal VPN link. It evaluates:
     - Interface status
     - Multiple external IP addresses
     - Multiple ISP circuits
     - Reachability through Next-Hop Probing
     - SLA-like behavior for tunnel selection

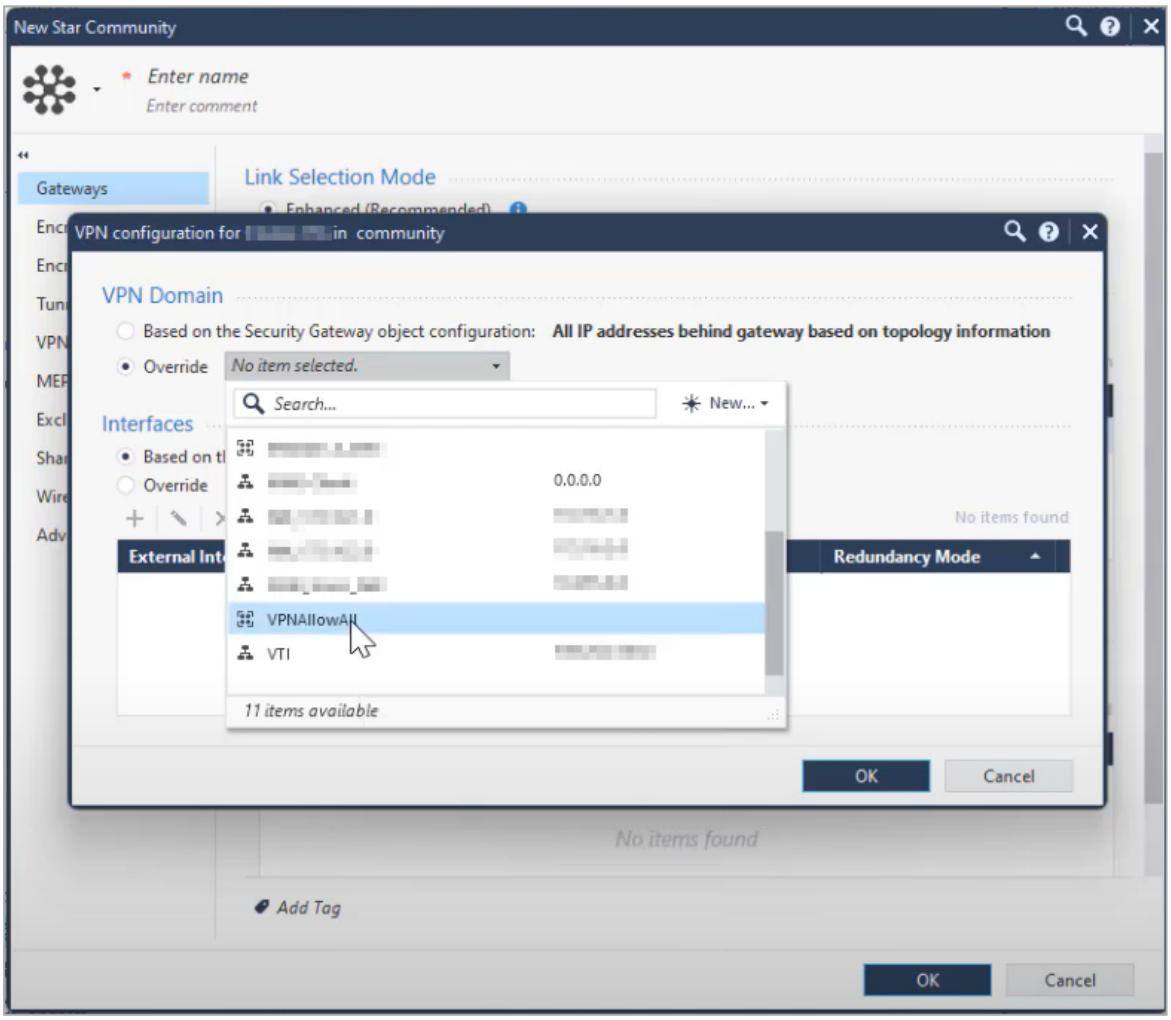
- **Legacy** - Uses static or basic logic to select the VPN interface or IP address. Selection is based on:
  - Main IP (default)
  - Selected interface
  - Selected IP
  - IP address determined by topology

7. Under **Center Gateways**, click + and add the Check Point Gateway:

   The cluster is added to the table.

   a. Double-click the cluster in the table.

   b. In the **VPN Domain** section, select the **Override** checkbox and from the list, select the allow all VPN group.



c. In the **Interfaces** section, select the **Override** checkbox and click +.

   The **Interface Settings** window appears.

d. Specify these:

   i. **External Interface**

   ii. **Static NAT IP Address** - The Check Point SASE gateway public IP address.

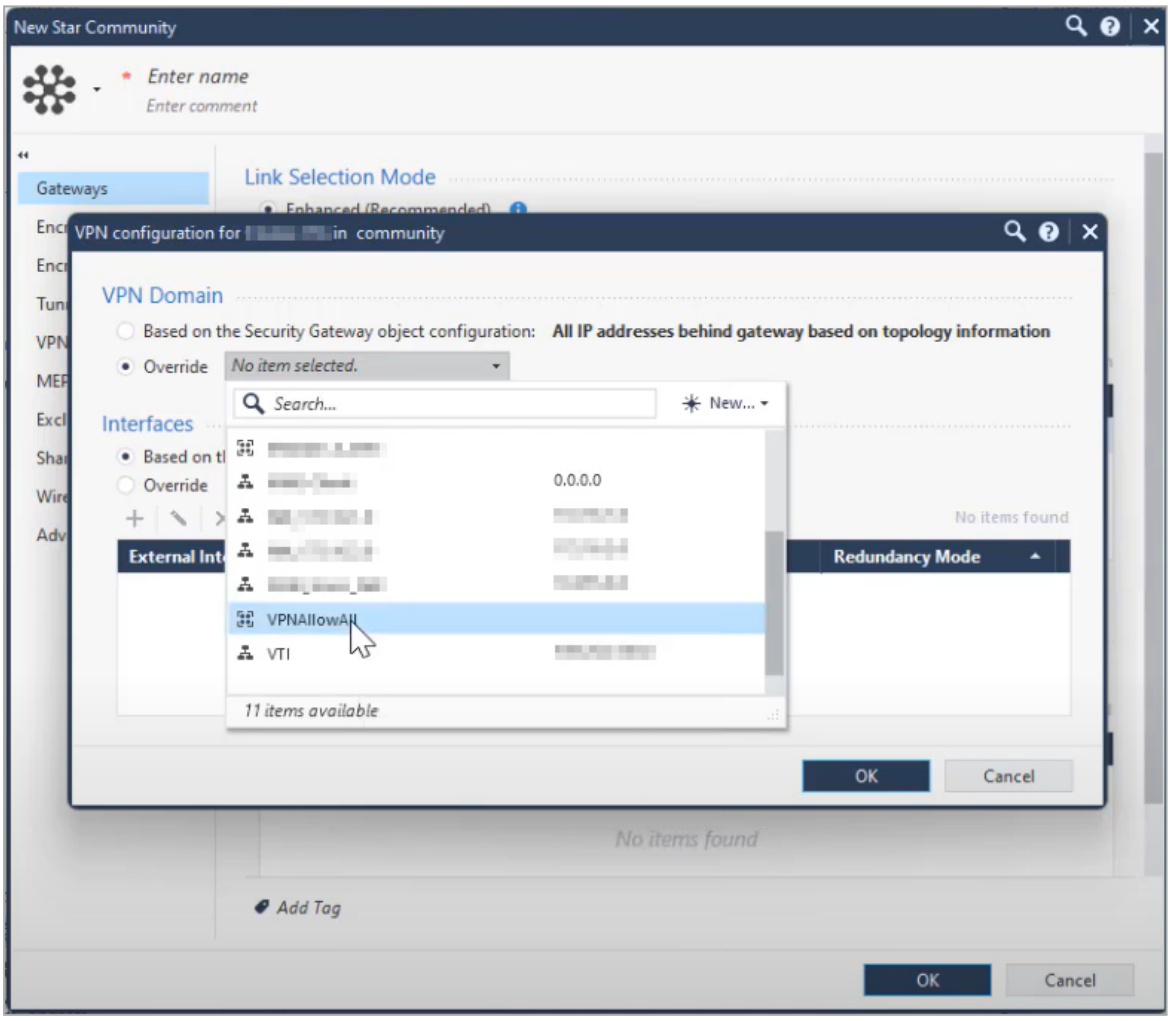
e. Click **OK**.

f. Click **OK**.

8. Under **Satellite Gateways**, click + and add the Interoperable Device Object created for the Check Point Gateway. See Step 1.

   a. From the table, double-click the cluster of the first Quantum Gateway.

   b. In the **VPN Domain** section, select the **Override** checkbox and from the list, select the allow all VPN group.



c. In the **Interfaces** section, select the **Override** checkbox and click +.

The **Interface Settings** window appears.

d. Specify these:

i. **External Interface**

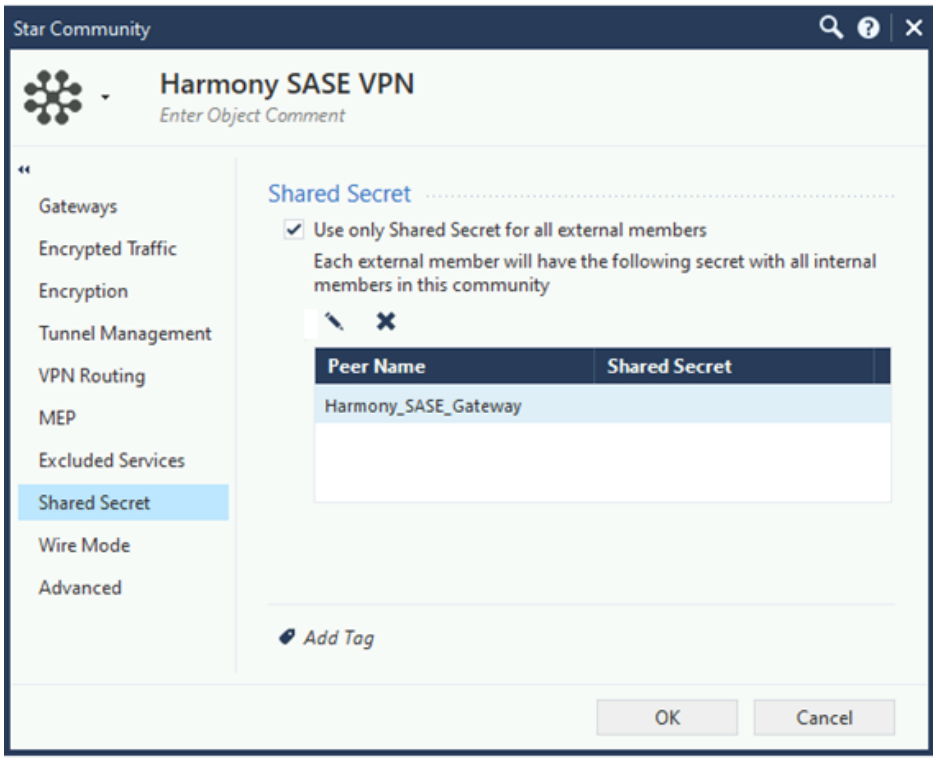
ii. **Static NAT IP Address** - The Check Point SASE gateway public IP address.

e. Click **OK**.

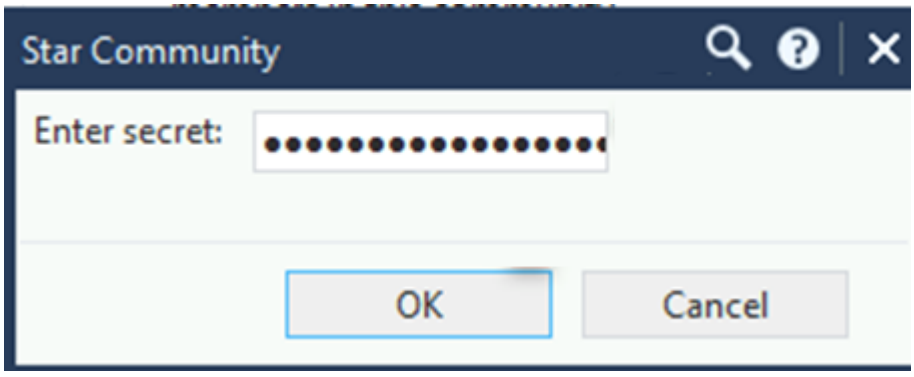
f. Click **OK**.

g. Repeat the steps from **a** through **f** for the cluster of the second QuantumGateway.

9. Go to **Shared Secret** and click ✎ to edit the shared key.



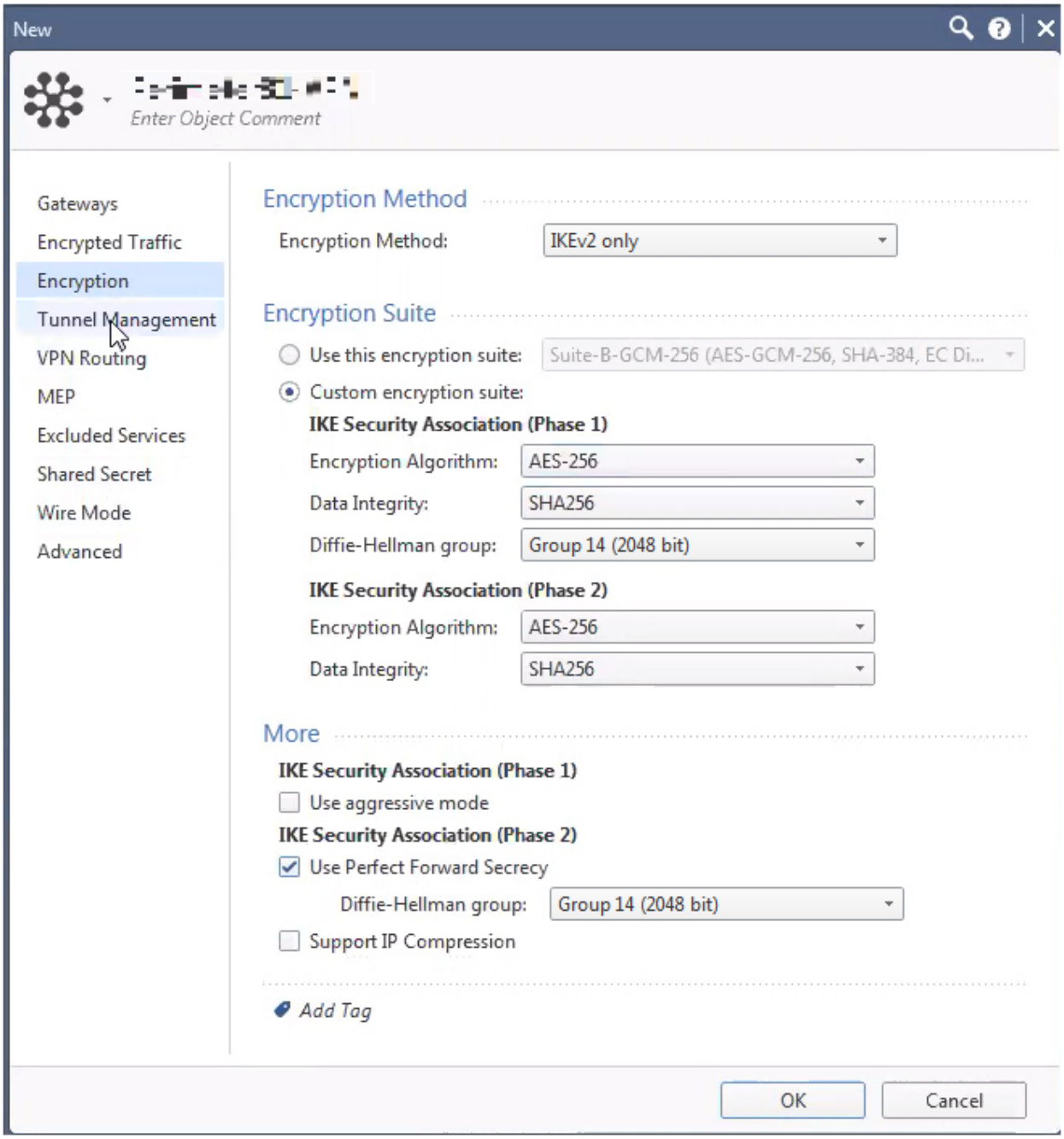
10. In the **Enter secret** field, enter an appropriate key.



Notes:

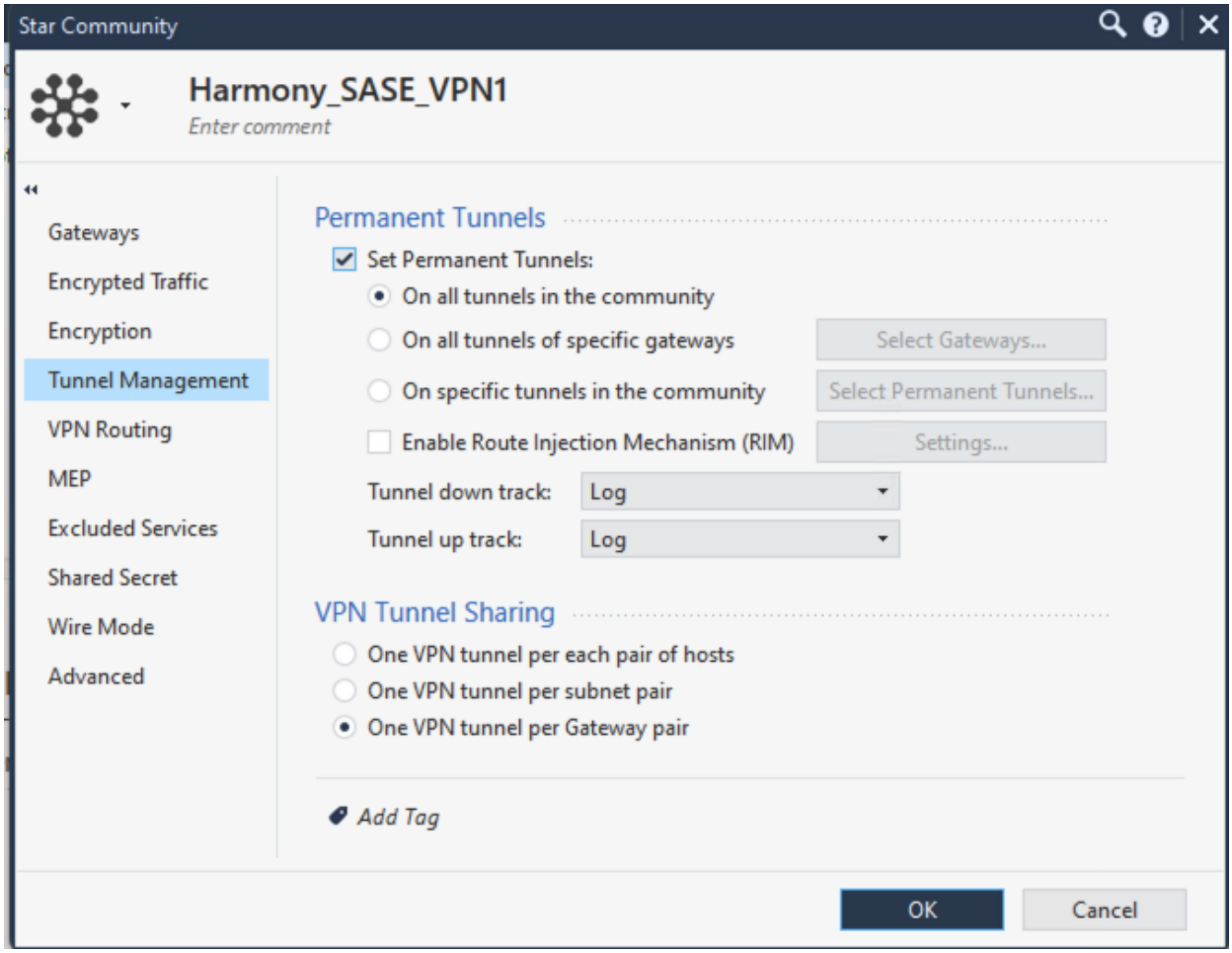
- Copy the key as it is required while configuring the IPsec Tunnel in the SASE Administrator Portal.
- Check Point recommends that the share secret key is at least 20 characters in length.

11. Click **OK**.
12. From the left navigation pane, click **Encryption** and do these:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

13. Click **Tunnel Management**.
14. In the **Permanent Tunnels** section, select the **Set Permanent Tunnels** checkbox and then select **On all tunnels in the community**.



15. In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

    Important - Make sure that you enter the remote subnets specified here in the Check Point SASEAdministrator Portal. A mismatch can disconnect the tunnel.

16. Click **Advanced**.

    a. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.

    b. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.

17. In the **Properties** section, select the **Disable NAT inside the VPN community** checkbox and from the list, select **Both center and satellite** gateways.

18. Click **OK**.

19. Repeat steps **1** to **17** for the other Check Point Gateway and SASE Gateway.

20. Publish and install the policy.

Step 4: Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Check Point SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Check Point SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

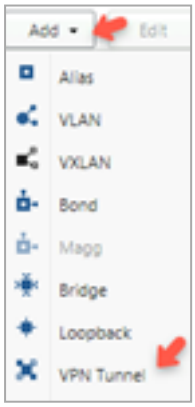
   Note - The network configuration differs if you have not changed the default settings during Check Point SASE network creation. For testing purposes, you should initially allow any/any or allow ping before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

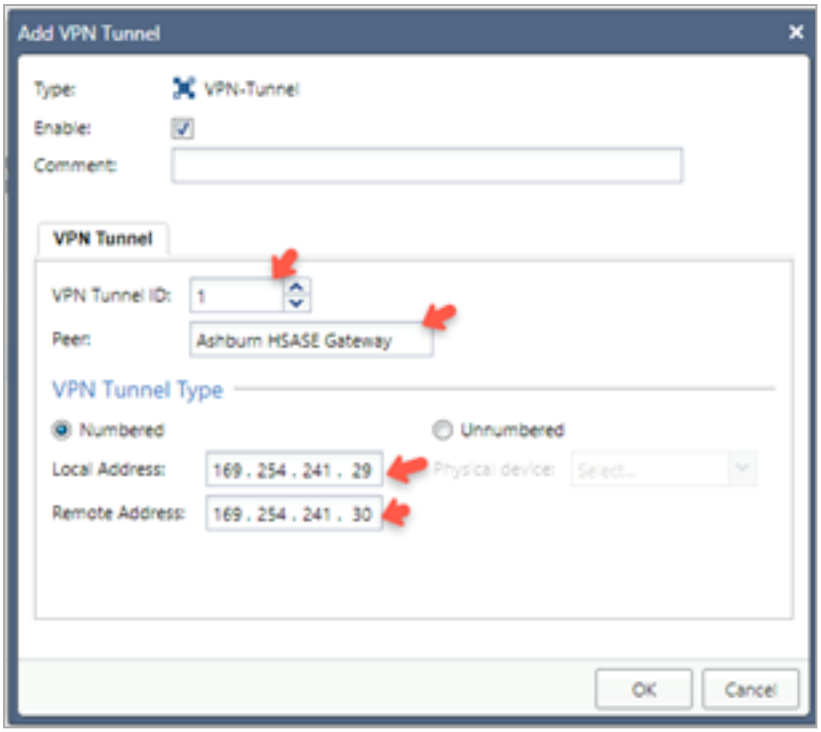
Step 5: Configuring VPN Tunnel Interface and BGP Configuration

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Click **Network Interfaces**.
3. From the **Add** list, select **VPN Tunnel**.



   The **Add VPN Tunnel** page appears.

4. Enter these:



a. **VPN Tunnel ID** - Select a unique ID.

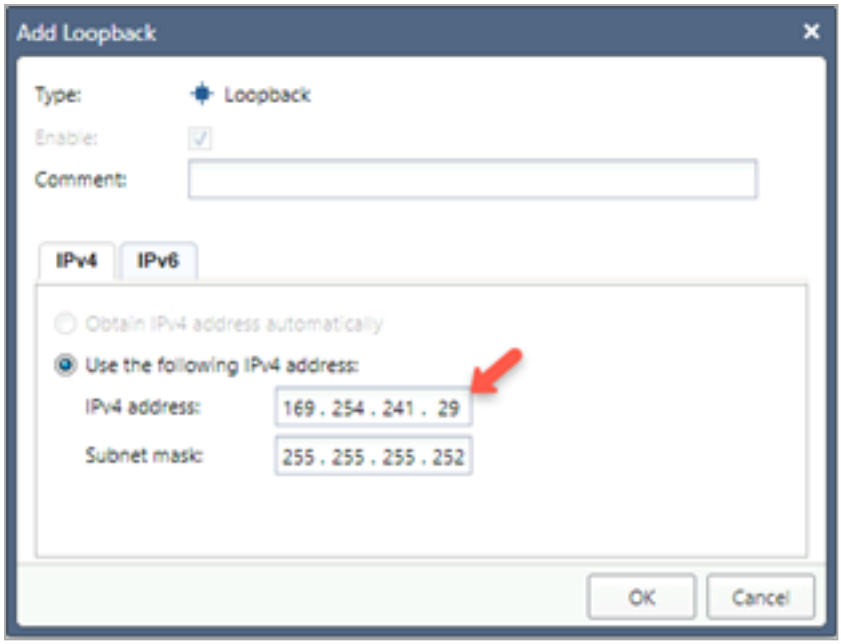
b. **Peer** - Name of the interoperable device previously created for the first SASE Gateway.

c. **VPN Tunnel Type** - Numbered.

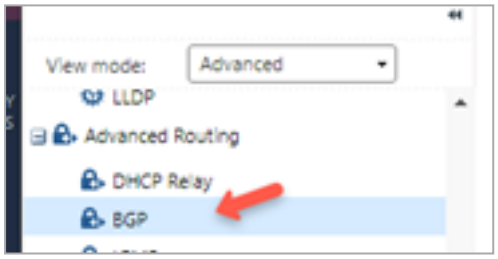
d. **Local Address** - Internal address for the Quantum Gateway (within 169.254.x.x/30 ranges).

e. **Remote Address** - Internal address for the SASE Gateway (within 169.254.x.x/30 ranges, corresponding to the above).

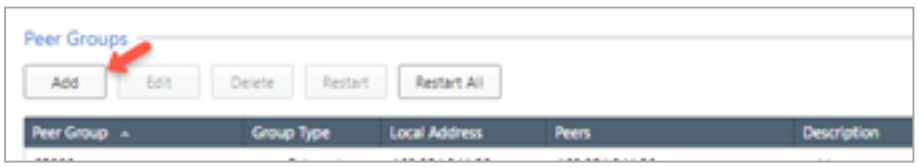
5. Click **OK**.
6. Click **Network Interfaces**, **Add** > **Loopback**.
7. Select **Use the following IPV4 address**.



8. In the **IPv4** field, enter the Local Address entered in step 4 and click **OK**.
9. Go to **Advanced Routing** and select **BGP**.

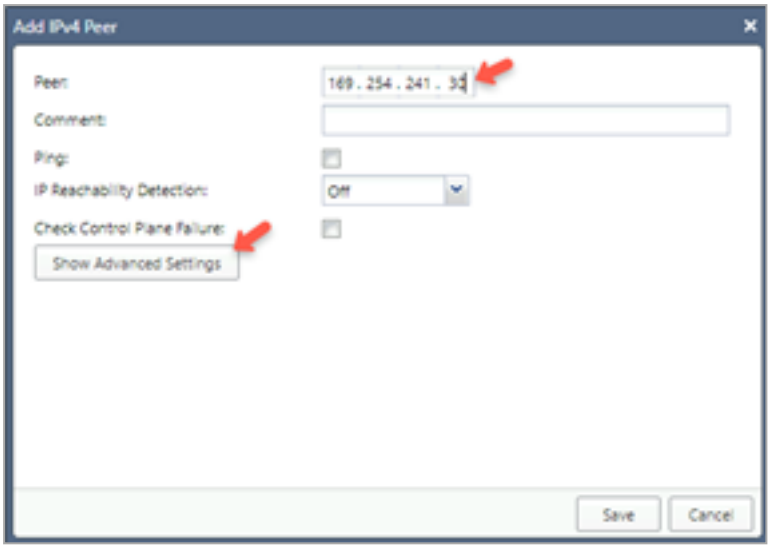


10. In the **Peer Groups** section, click **Add**.

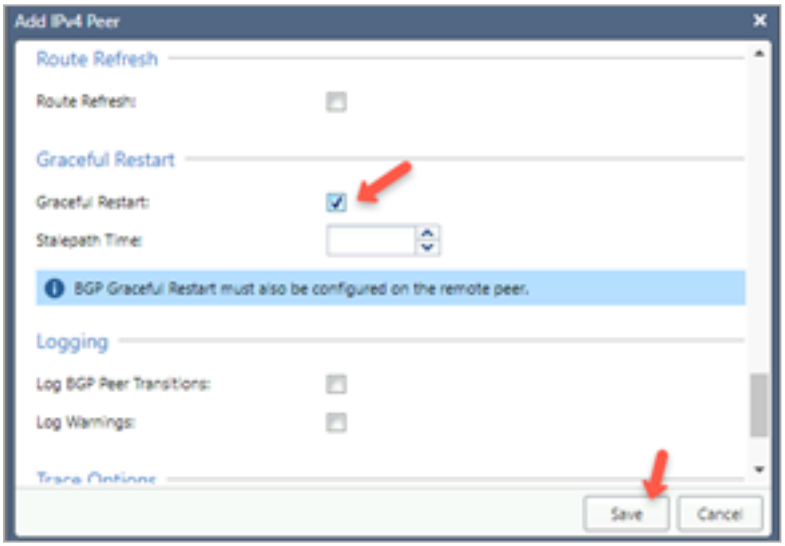


11. Enter these:
    a. **Peer AS Number** - The AS Number of the Check Point SASE network. If not set already, enter 64512.
    b. **Peer Group Type** - External.
    c. **Local Address** - The local address entered in the VTI configuration section Step 4.
12. Click **Add Peers**.
13. Enter these:

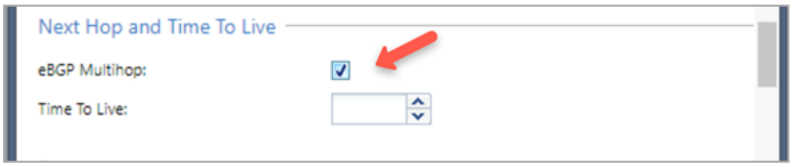
a. In the **Peer** field, enter the Remote Address set under the VTI configuration in Step 4 and click **Show Advanced Settings**.



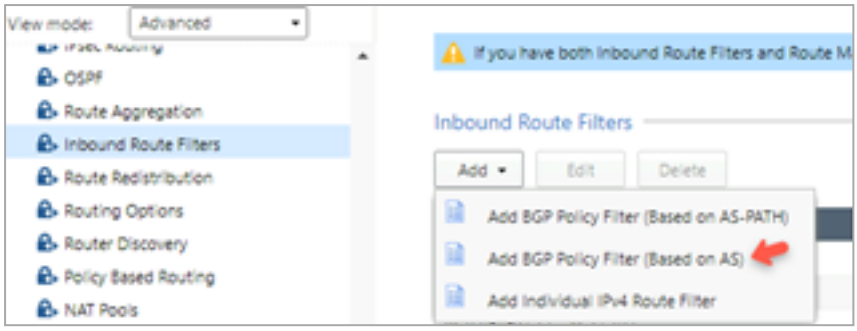
b. Select the **Graceful Restart** checkbox.



c. Select the **eBGP Multihop** checkbox and click **Save**.

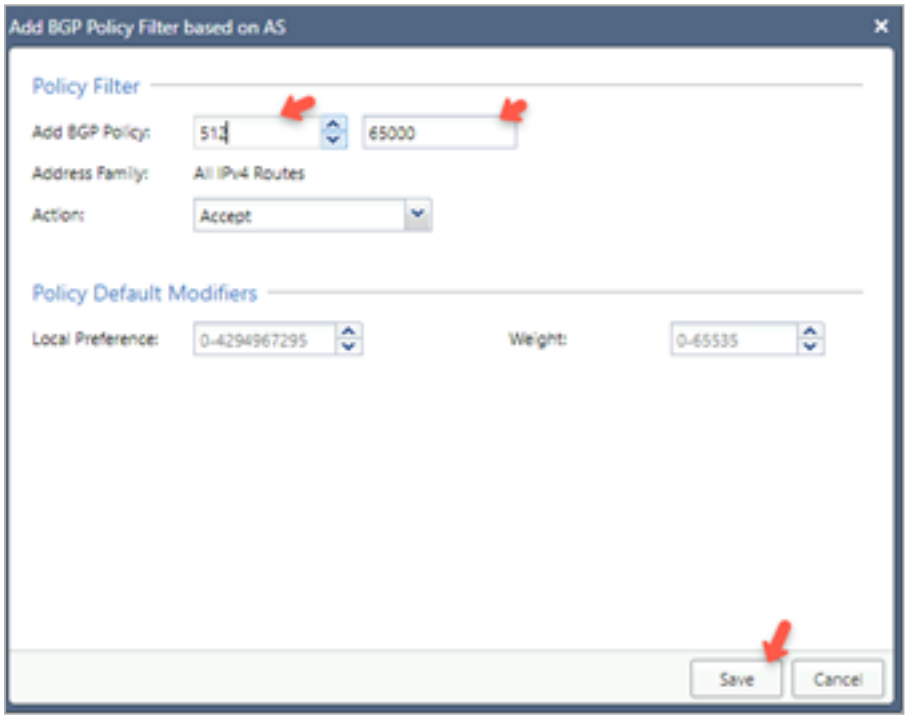


14. From the **View mode** list, select **Advanced Routing** and click **Inbound Route Filter**.
15. From the **Add** list, select **Add BGP Policy Filter (Based on AS)**.

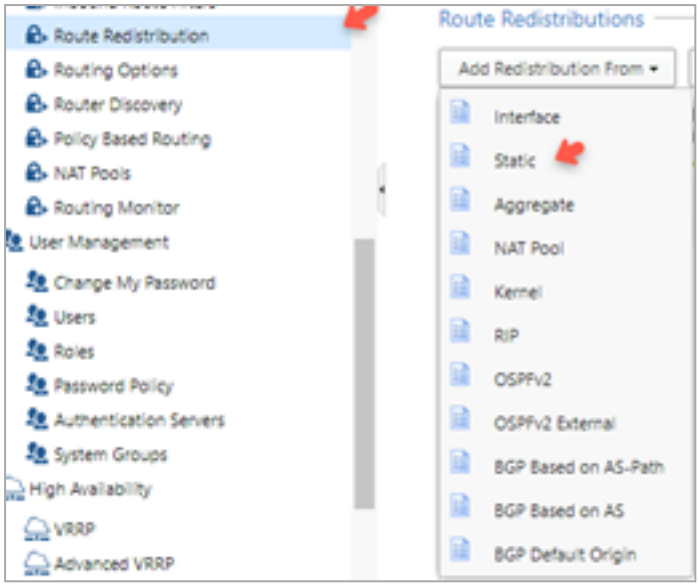


The **Add BGP Policy Filter based on AS** window appears.

16. Specify these:
    a. **Add BGP Policy** - Set a number from the available range.
    b. **AS Number** - Set the AS Number of the SASE Network.
    c. **Action** - Accept



17. Click **Save**.
18. From the **View mode** list, select **Advanced Routing**, click **Route Redistribution**.
19. From the list, select **Add Redistribution From**.
20. Select **Static**.



Note - For BGP, no routes are accepted from a peer by default. You must configure an explicit Inbound BGP Route Filter to accept a BGP route from a peer.

21. Repeat the steps for the second Check Point Gateway and SASE Gateway. Use a different 169.254.x.x/30 range for the local and remote peer IP addresses.

Part 2 - Configuration in SASE Administrator Portal

Step 1: Configuring Tunnel and Routes Table

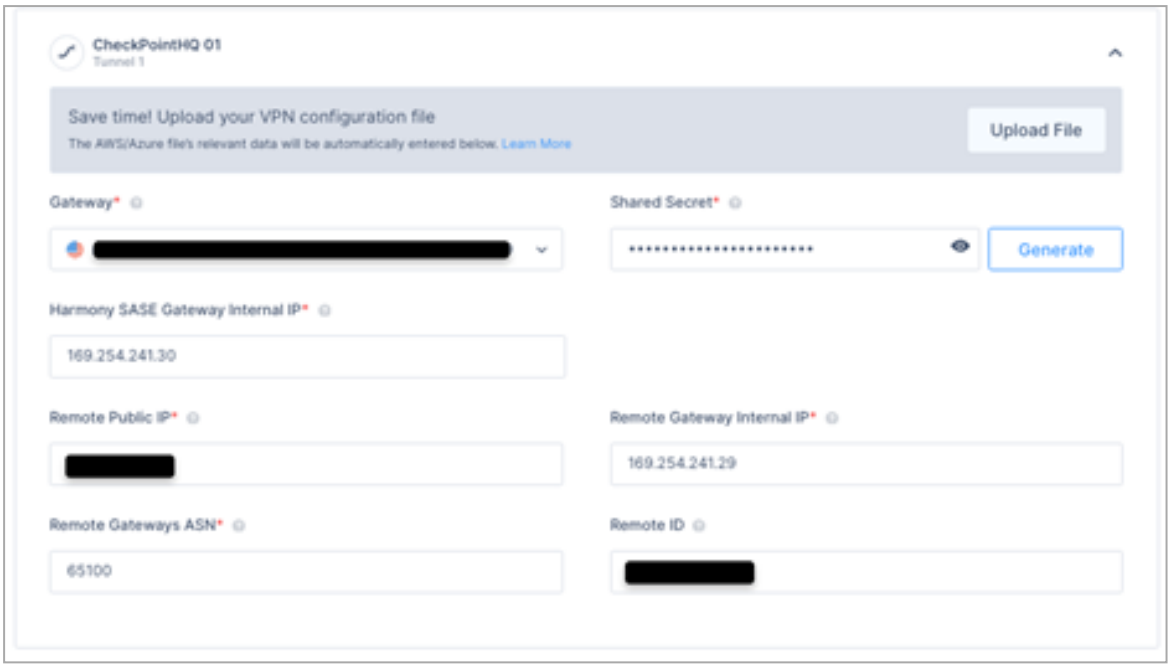
1. Access the SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ⋯ .
4. Select **Add Tunnel** for the gateway from which you want to add the IPSec Site-2-Site VPN tunnel.

a. Click **IPSec Site-2-Site Tunnel** and click **Continue**.

b. Click **Redundant Tunnels** and click **Continue**.

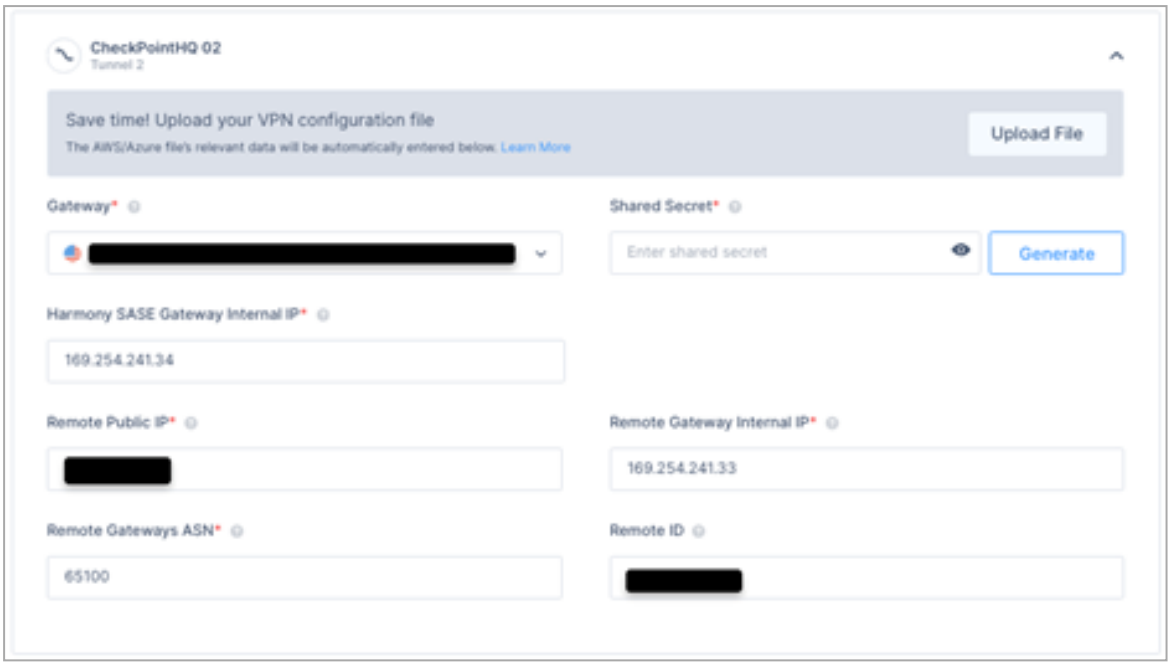
c. In the **Tunnel name** field, enter a logical name.

d. Expand Tunnel 1 and specify these:



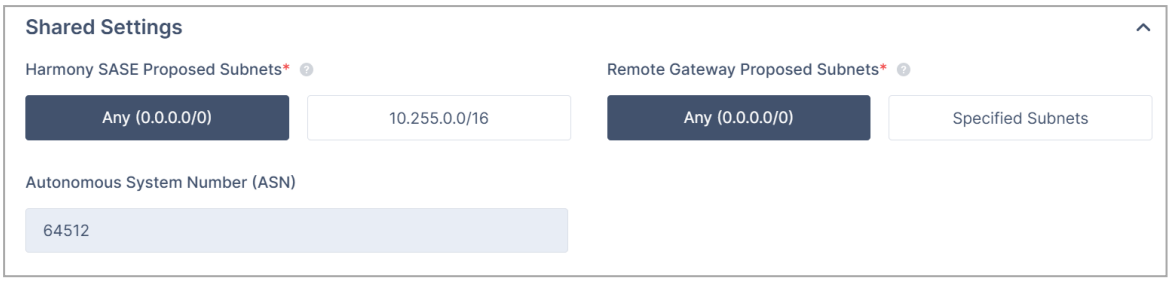
- **Shared Secret** - The value previously set on the first start policy.
- **SASE Gateway Internal IP** - The remote address of the first Check Point Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the first Quantum Gateway.
- **Remote Gateway Internal IP** - The local address of the first Quantum Gateway used under the VTI settings.
- **Remote Gateways ASN** - The ASN of the first Quantum Gateway.
- **Remote ID** - The router ID of the first Quantum Gateway used under the BGP settings above.

e. Expand Tunnel 2 and specify these:



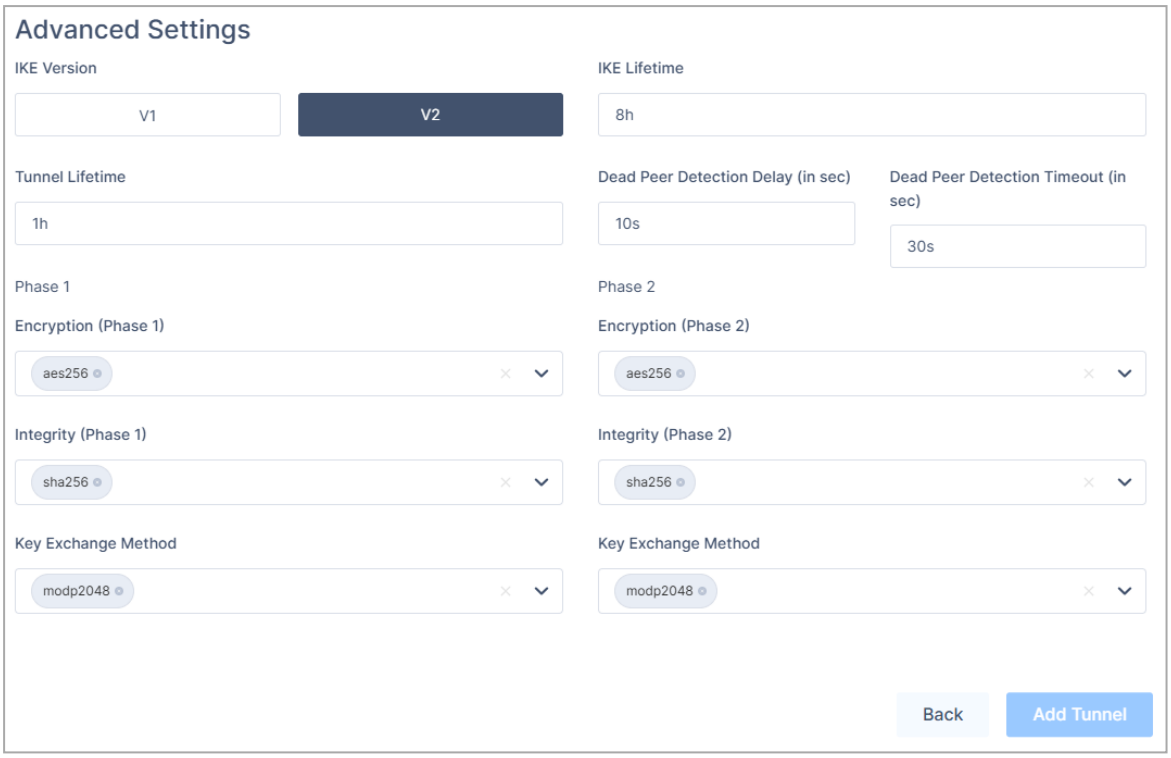
- **Gateway** - Select the second SASE Gateway for the tunnel.
- **Shared Secret** - The value previously set on the second star policy.
- **SASE Gateway Internal IP** - The remote address of the second Quantum Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the second Quantum Gateway.
- **Remote Gateway Internal IP** -The local address of the second Quantum Gateway used under the VTI settings.
- **Remote Gateways ASN** - The ASN of the second Quantum Gateway.
- **Remote ID** - The router ID of the second Quantum Gateway used under the BGP settings above.

f. Expand **Shared Settings** and specify these:



- **Check Point SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Autonomous System Number (ASN)** - Default value is **64512**, if not set, enter the AS Number for the Check Point SASE network.

g. In the **Advanced Settings** section, specify these:



- **IKE Version**: V2
- **IKE Lifetime**: 8h
- **Tunnel Lifetime**: 1h
- **Dead Peer Detection Delay**: 10s
- **Dead Peer Detection Timeout**: 30s
- **Phase 1**:
  - **Encryption(Phase 1)**: aes256
  - **Integrity (Phase 1)**: sha256
  - **Key Exchange Method**: modp2048
- **Phase 2**:
  - **Encryption(Phase 2)**: aes256
  - **Integrity (Phase 2)**: sha256
  - **Key Exchange Method**: modp2048

h. Click **Add Tunnel**.

5. Select **Routes Table**:

a. Click **Add Route**.

The **Add Route** window appears.

b. Enter all the subnets on the remote side of the tunnel and then click **Add Route**.

c. Click **Apply Configuration**.

Step 2: Verifying the Setup

Once you complete the above steps, your tunnel should be active.

1. Verify the setup in the SASE Administrator Portal:
   a. Click **Networks**.
   b. Locate the tunnel you create, and check the tunnel status.

   It should indicate that the tunnel is **Up**, signifying a successful connection.
2. Verify the setup in the SASE Agent:
   a. Connect to your network using the SASE Agent.
   b. Access one of the resources in your environment.

Configuring Check Point Maestro VSX Redundant IPsec Tunnel

Introduction

This topic explains how to establish a redundant Site-to-Site VPN tunnel between your SASE Network and Check PointMaestro VSXFirewall.

Prerequisites

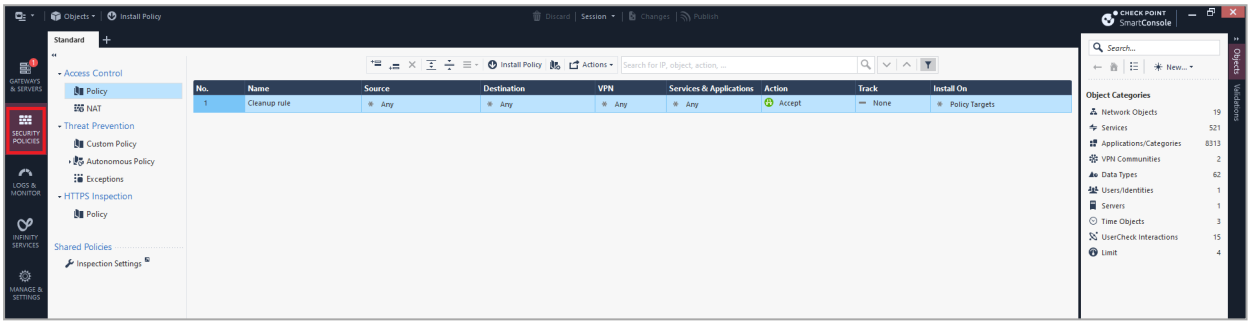
- SASE Administrator Portal account.
- Device with SASE Agent installed.

- Administrator account with Firewall, Router, and Cloud Management Portal.
- A MaestroVSX Cluster with one or two public IPs.

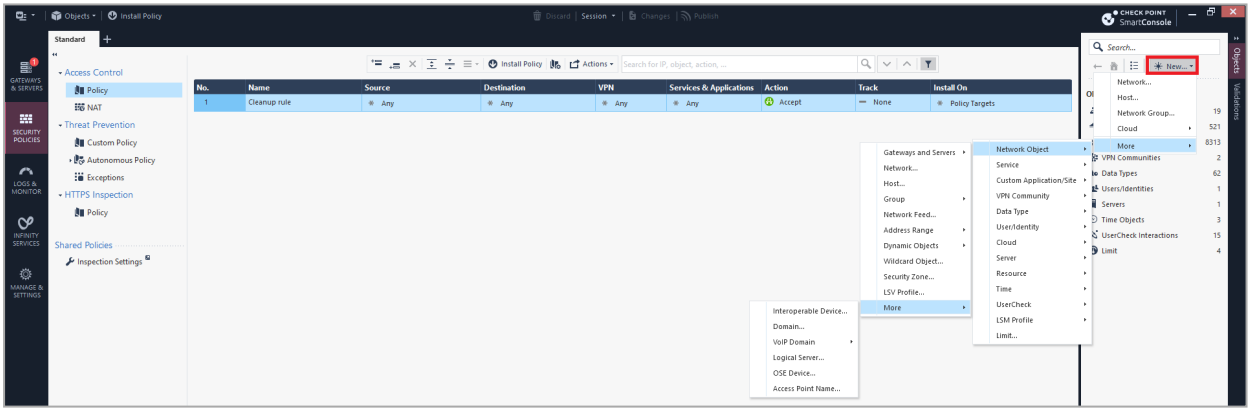
Part 1 - Configuration in SmartConsole

Step 1: Create Interoperable Device Object in the Check Point SmartConsole

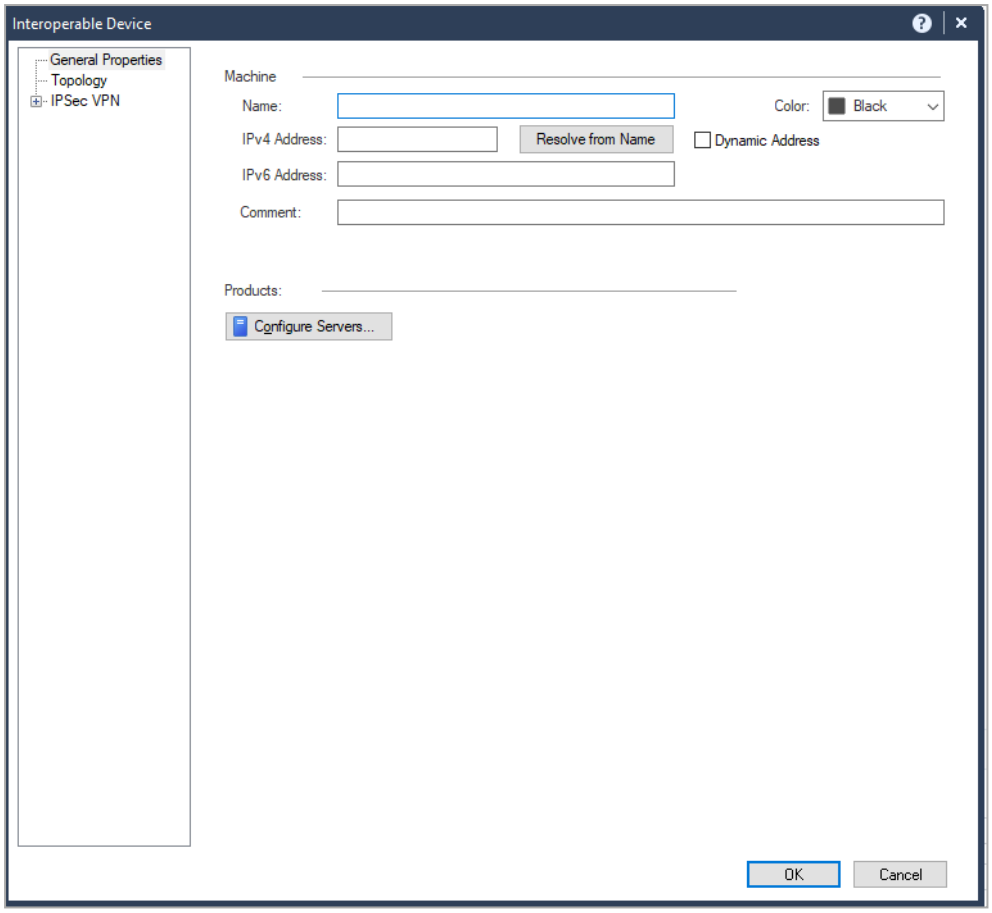
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



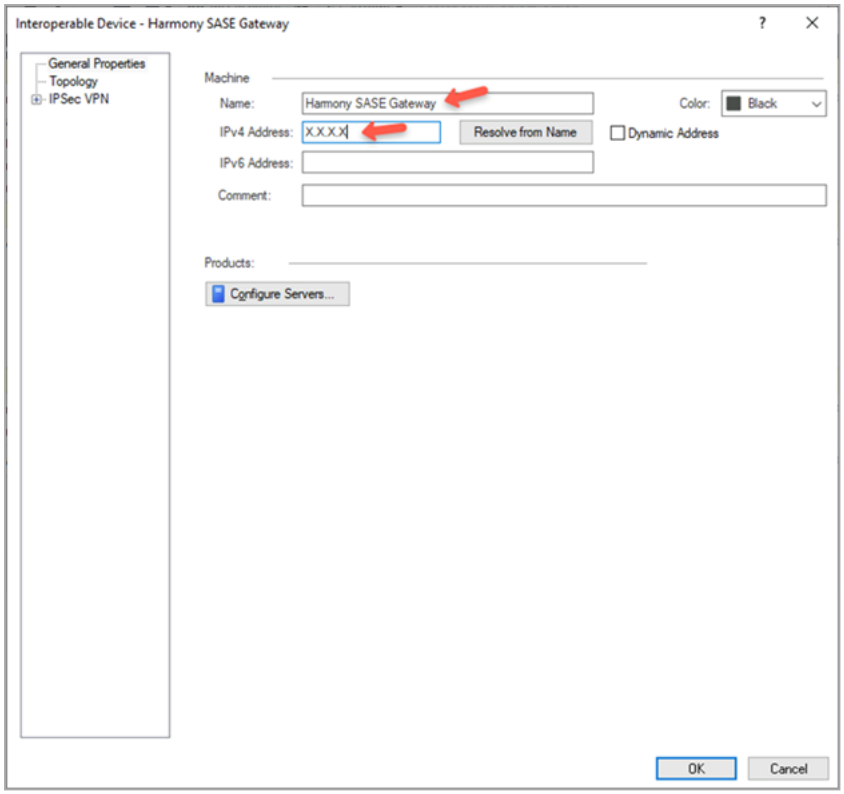
3. In the **Objects** pane, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** popup appears.



4. In the **Name** field, enter a name for the SASEGateway, for example, Harmony_SASE_Gateway.
5. In the **IPv4 Address** field, enter the SASEGateway public IP address.



To find the SASE Gateway public IP Address:

a. Access the SASE Administrator Portaland click **Networks**.

b. Select the network.

c. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

6. Click **OK**.

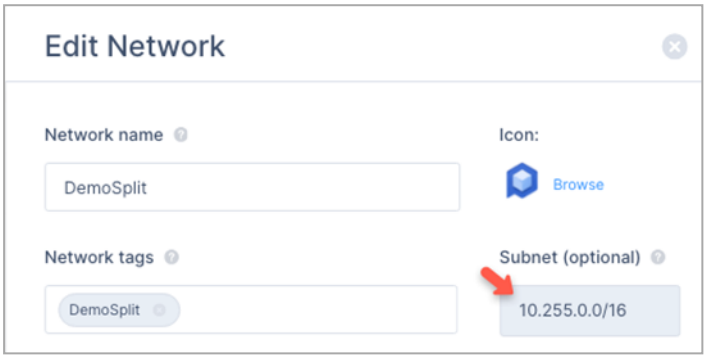
Step 2: Adding SASE Gateway IP Address and Remote SubnetTo The Interoperable Device Object

1. Log in to the SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network:

a. Select a network, scroll to the end of the row and click ... .

b. Select **Edit Network**.

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.



4. Open the Interoperable Device object that you created.

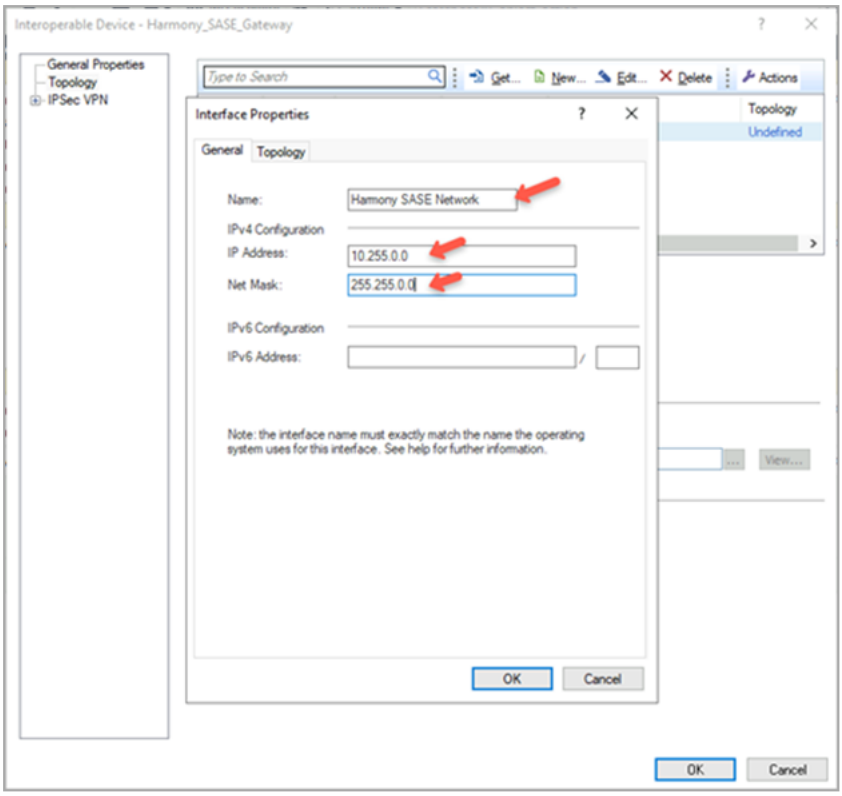
5. Click **Topology > New**.

6. In the **General** tab, enter these:

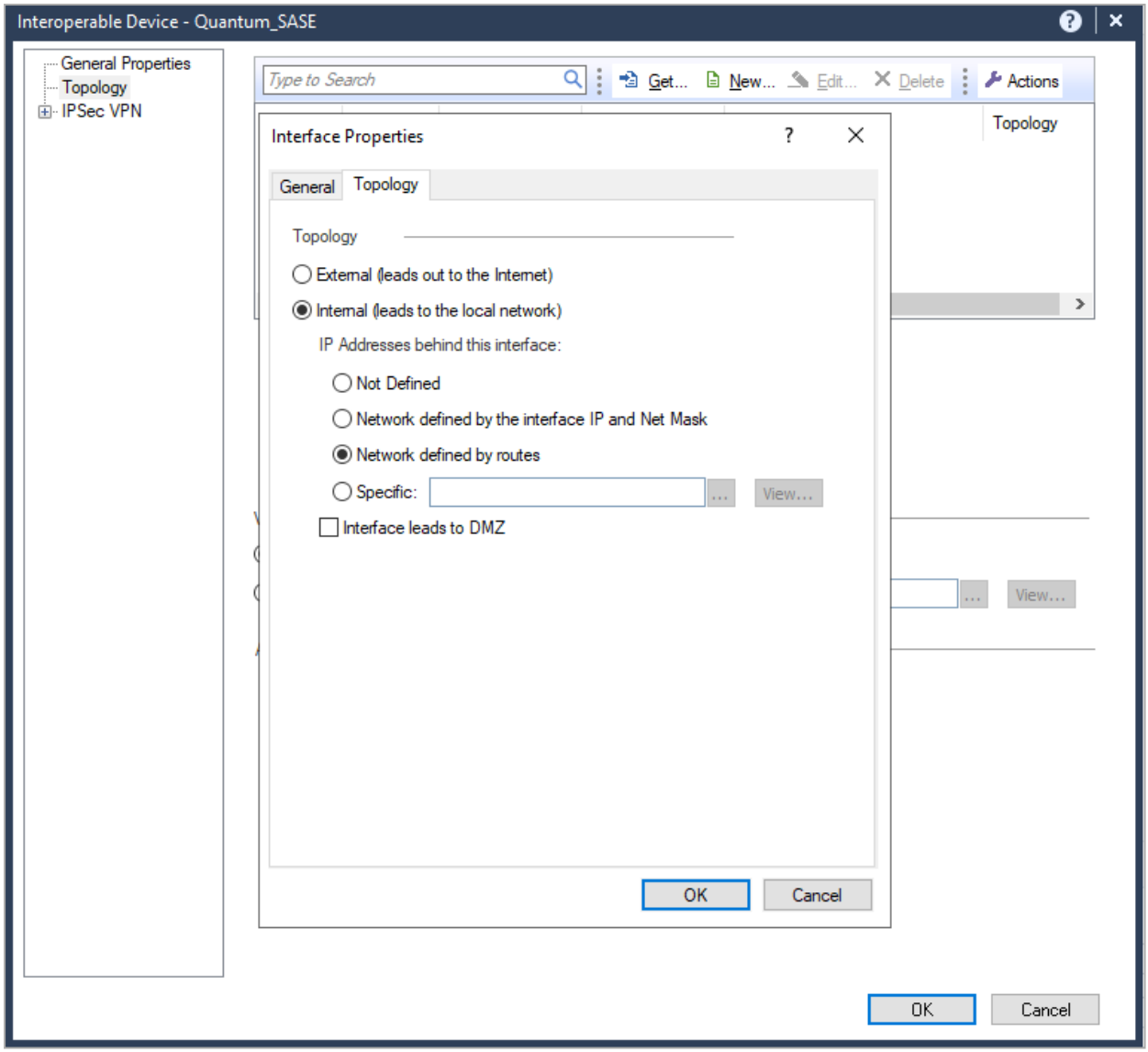
a. **Name** - Name of the topology, for example, SASE Network.

b. **IP Address**- 10.255.0.0

c. **Net Mask**- 255.255.0.0

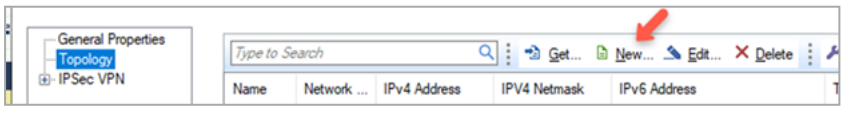


In the **Topology tab**, select **Internal (leads to the local network)** and then select **Network defined by the interface IP** and **Net Mask**.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

7. Click **OK**.
8. Click **Topology > New**.

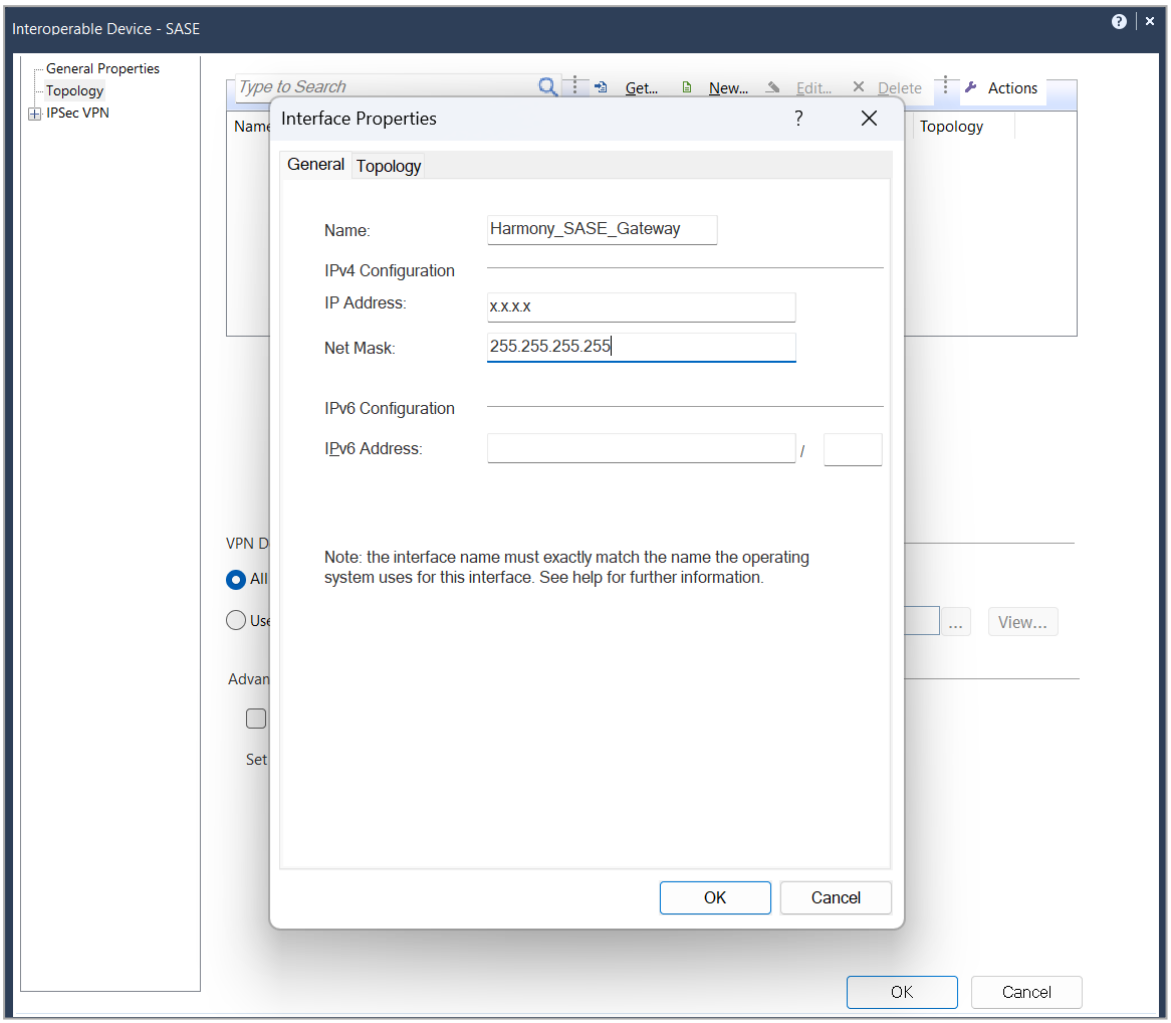


9. In the **General** tab, enter these:

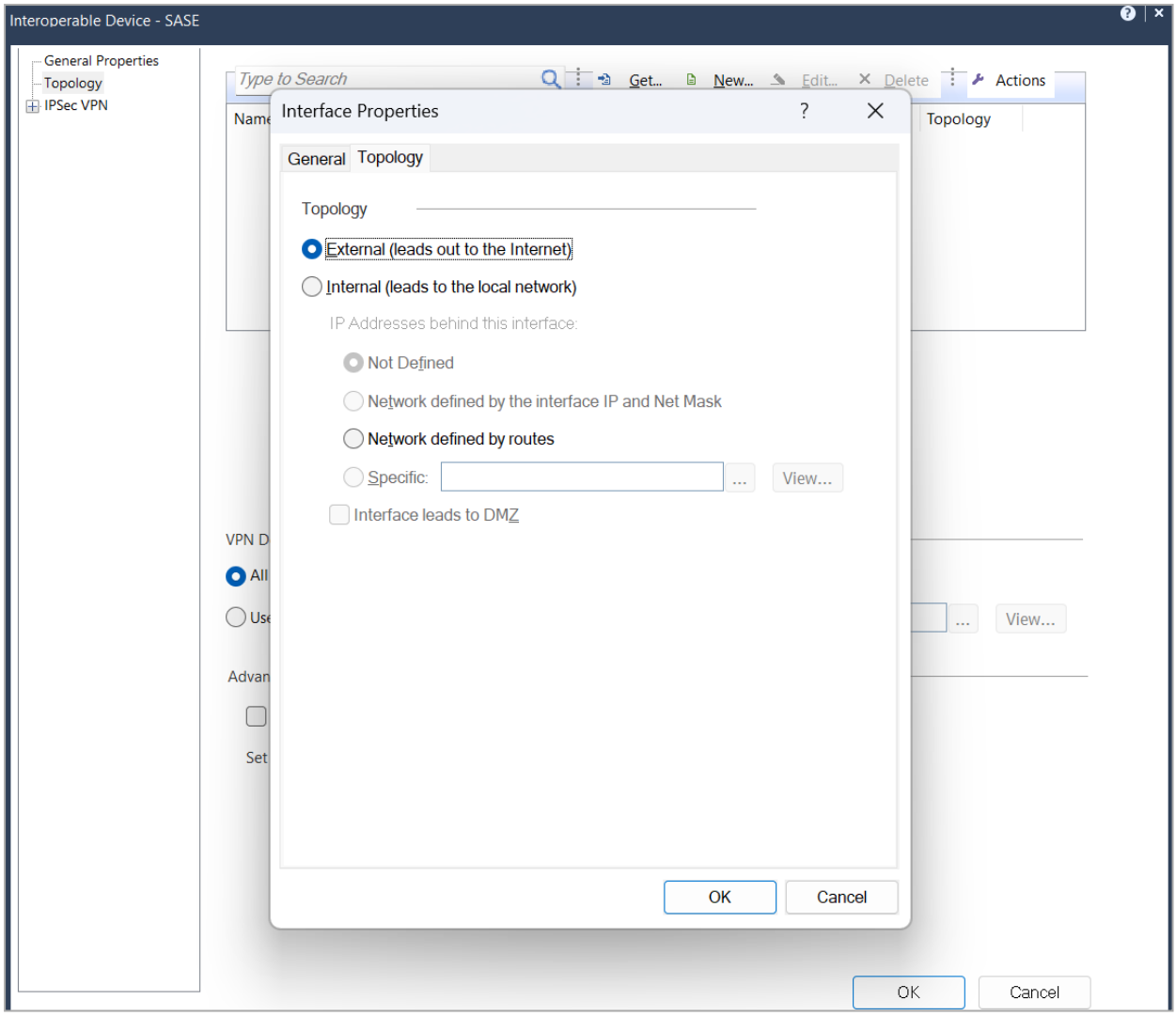
a. **Name** - Name for the topology, for example, Harmony_SASE_Gateway

b. **IP Address** - Public IP address of the Check Point SASE gateway

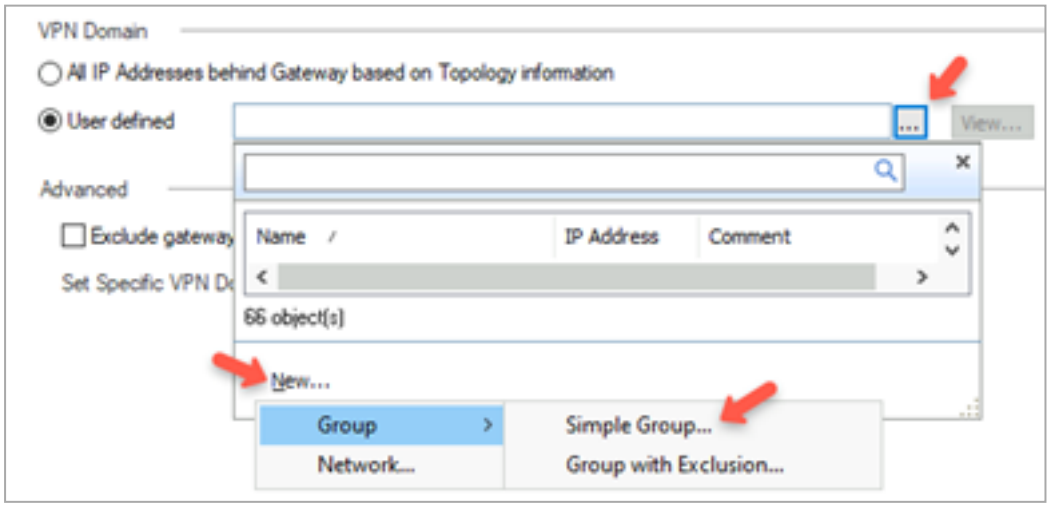
c. **Net Mask** - 255.255.255.255



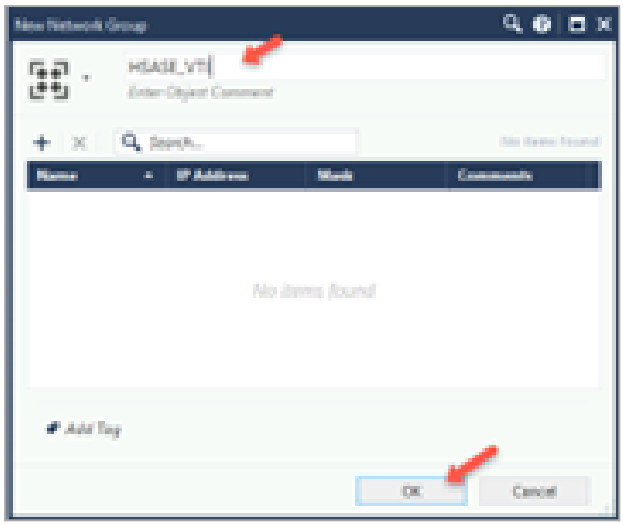
10. Click the **Topology** tab, Select **External (leads out to the internet)**.



11. Click **OK**.
12. In the **VPN Domain** section, select **User defined** and click ... .
13. Click **New** and go to **Group > Simple Group**.



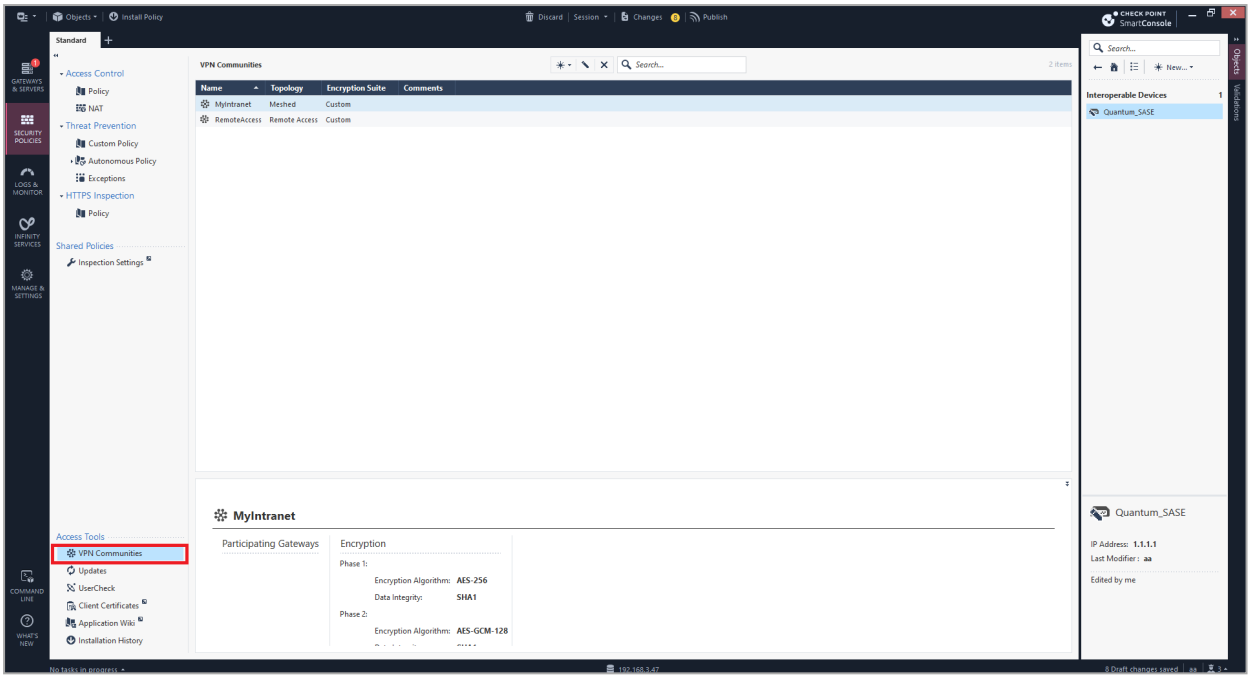
The **New Network Group** popup appears.



14. In the **Enter Object Comment** field, enter a name, for example, HSASE_VTI, and click **OK**.
15. For the other SASE Gateway and Check Point Gateway, follow the same procedure in **Creating Interoperable Device Objects in the Check Point SmartConsole and Adding SASE Gateway IP Address and Remote SubnetTo The Interoperable Device Object** sections.
16. Publish and install the policy.

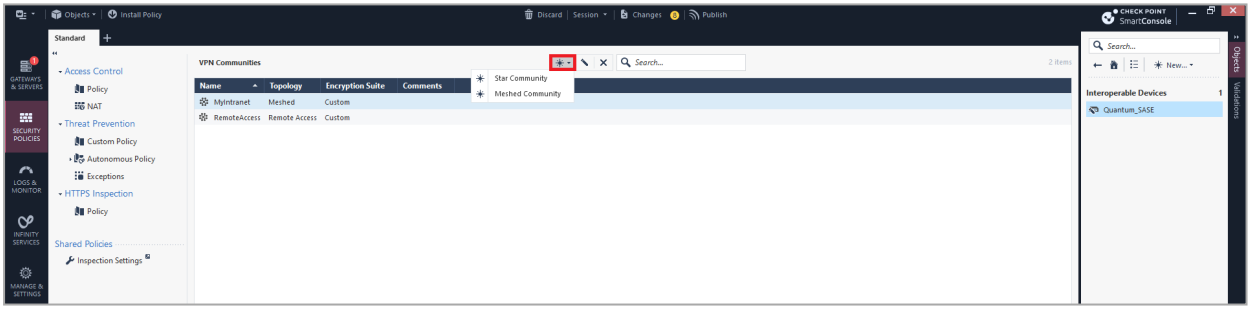
Step 3: Creating VPN Star community

1. Log in to the Check PointSmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools > VPN Communities**

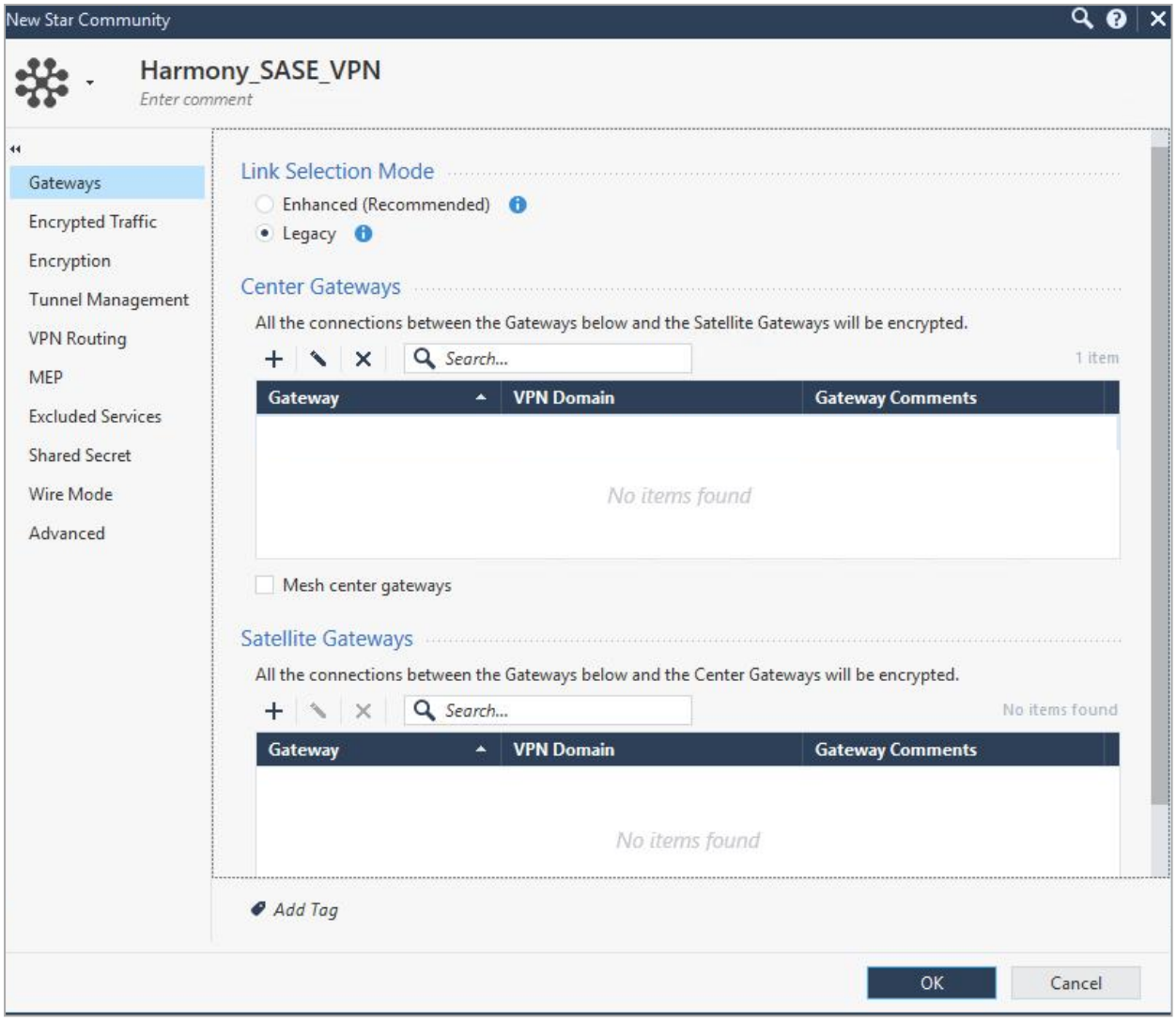


.

4. Select an object, click **New** and go to **More > VPN Communities > Star Community**.



The **New Star Community** popup appears.



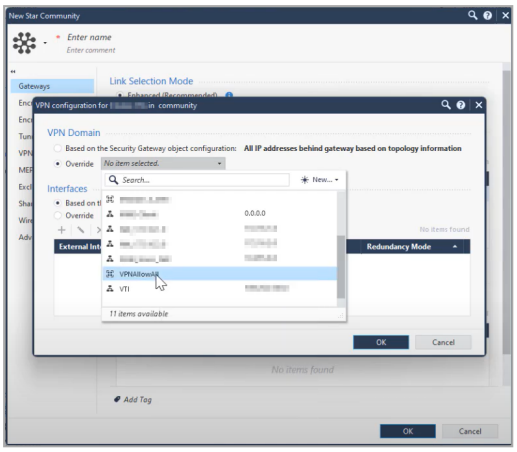
5. In the **Enter Object Name** field, enter an object name for the VPN Star Community, for example, *Harmony_SASE_VPN*.

6. In the Centre Gatewayssection, click + and add the MaestroSecurity Group.

   The Security Group is added to the table.

a. Double-click the Maestro Security Group in the table.

b. In the **VPN Domain** section, select the **Override** checkbox and from the list, select the allow all VPN group.



c. In the **Interfaces** section, select the **Override** checkbox and click + .

The **Interface Settings** popup appears.

d. Specify these:

i. **External Interface**

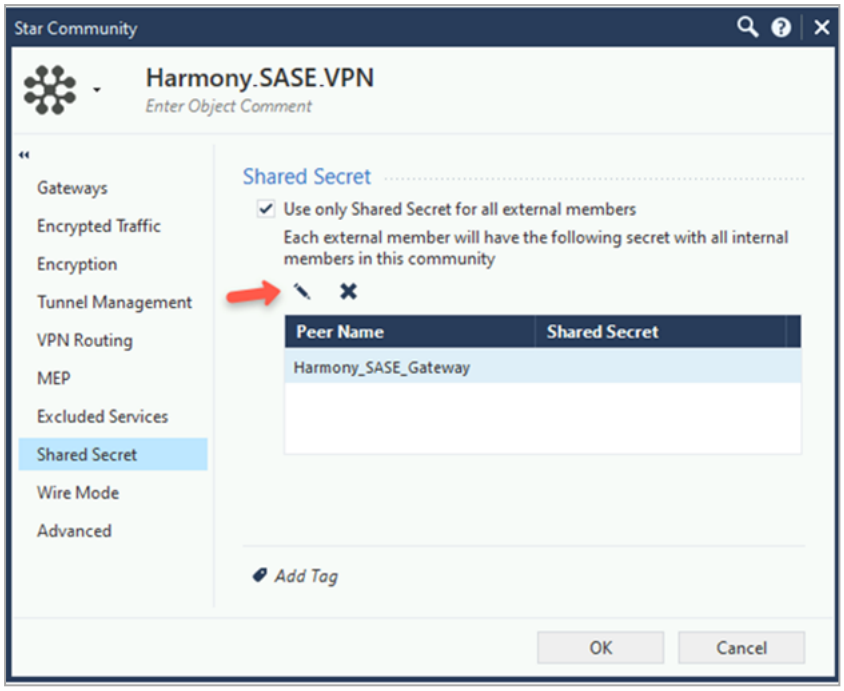
ii. **Static NAT IP Address** - The SASE Gatewaypublic IP address.

e. Click **OK**.

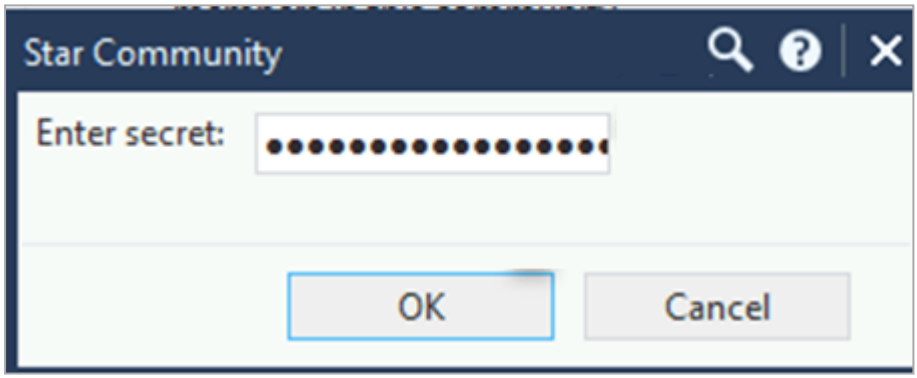
f. Click **OK**.

7. In the **Satellite Gateway** section, click + and add the Interoperable Device Object created for the Check Point Gateway. See Step 1.

8. Go to **Shared Secret** and click ✎ to edit the shared key.



9. In the **Enter secret** field, enter an appropriate key.



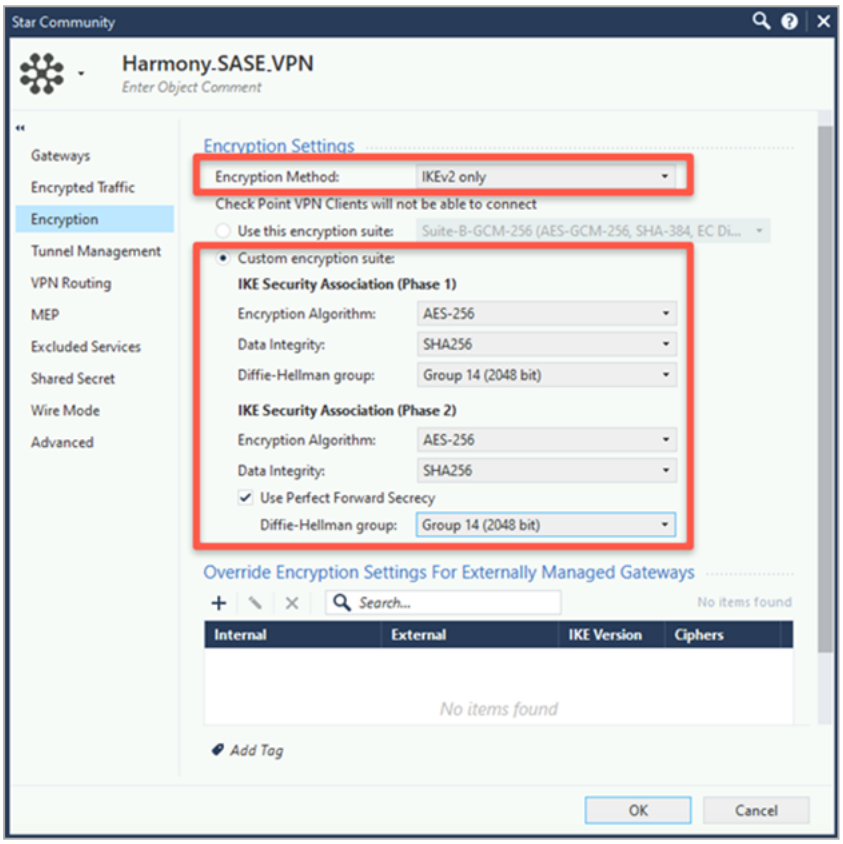
Notes -

- Check Point recommends that the shared secret key is at least 20 characters in length.
- Copy the key as it is required while configuring the IPsec Tunnel in the SASE Administrator Portal.

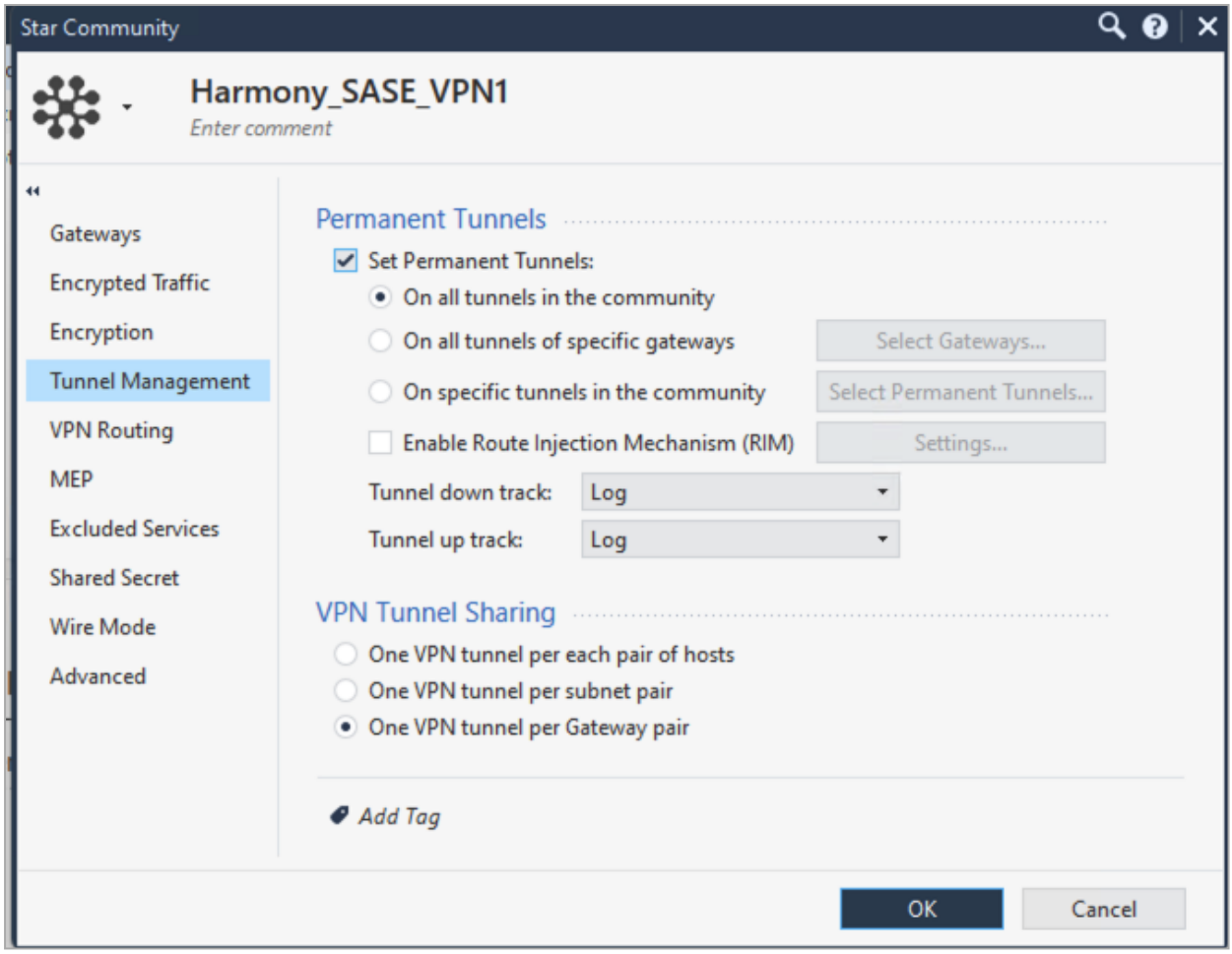
10. Click **OK**.
11. From the left navigation pane, click **Encryption** and do these:
    a. In the **Encryption Settings** section, from the **Encryption Method** list, select **IKEv2 only**.
    b. In the **Encryption Suite** section, select **Custom encryption suite**.

c. In the **IKE Security Association (Phase 1)** section:
   i. From the **Encryption Algorithm** list, select **AES-256**.
   ii. From the **Data Integrity** list, select **SHA256**.
   iii. From the **Diffie Hellman group** list, select **Group 14 (2048 bit)**.

d. In the **IKE Security Association (Phase 2)** section:
   i. From the **Encryption Algorithm** list, select **AES-256**.
   ii. From the **Data Integrity** list, select **SHA256**.
   iii. Select **Use Perfect Forward Secrecy**.
   iv. From the **Diffie Hellman group** list, select **Group 14 (2048 bit)**.



12. Go to **Tunnel Management**.
13. In the **Permanent Tunnels** section, select the **Set Permanent Tunnels** checkbox and then select **On all tunnels in the community**.



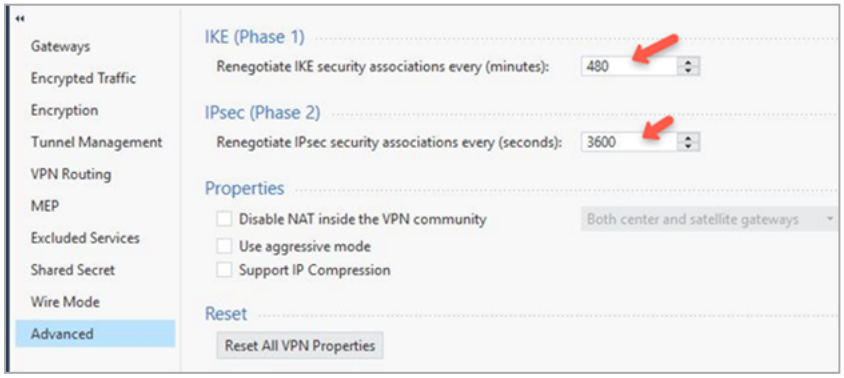
14. In the **VPN Tunnel Sharing** section, select **One VPN tunnel per Gateway pair**.

    Note - Make sure that you enter the remote Subnets specified here in the SASE Administrator Portal. A mismatch can disconnect the tunnel.

15. Go to **Advanced**.

16. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.

17. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security assecurity associations every (seconds)** field to **3600**.



18. Click **OK**.
19. In the **Properties** section, select the **Disable NAT inside the VPN Community** checkbox and from the list, select **Both center and satellite** gateways.
20. Publish and install the policy.

Step 4: Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the SASE Network 10.255.0.0/16 to specific destinations and services.

   Note - The network configuration differs if you have not changed the default settings during SASE network creation. For testing purposes, you should initially allow any/any or allow ping before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

Step 5: Configuring VPN Tunnel Interface and BGP Configuration

1. Log in to Gaia Clish of the MaestroSecurity Group.
   a. Switch to Expert mode.
   b. Write a script for creating two VPN Tunnel Interfaces with these content:

```
transaction begin
add interface vd <Name of Maestro Security Group> vpn_tunnel
numbered peer <Name of Interoperable device of first SASE GW>
local <Tunnel Local IP> remote <Tunnel Remote IP> tunnel_id
<Tunnel ID>
add interface vd <Name of Maestro Security Group> vpn_tunnel
numbered peer < Name of Interoperable device of second SASE
GW > local <Tunnel Local IP> remote <Tunnel Remote IP>
tunnel_id <Tunnel ID>
transaction end
```

   Local Address - Internal address for the **Maestro Security Group** (within 169.254.x.x/30 ranges).

   Remote Address - Internal address for the **SASE Gateway**(within 169.254.x.x/30 ranges, corresponding to the above).

   Example for script content:

```
transaction begin
add interface vd vs-ext vpn_tunnel numbered peer SASE_
Frankfurt_1 local 169.254.254.1 remote 169.254.254.2 tunnel_
id 1
add interface vd vs-ext vpn_tunnel numbered peer SASE_London_
1 local 169.254.254.5 remote 169.254.254.6 tunnel_id 2
transaction end
```

   c. Execute the script through **vsx_provisioning_tool**:

```
vsx_provisioning_tool -s localhost -u <user name> -f <full
path to above script>
```

   d. Verify successful execution of the script.
   e. Exit **expert mode** and connect to the relevant **Maestro Security Group**:

f. Create a peer group by executing these commands:

```
set bgp external remote-as <Peer AS Number> on
set bgp external remote-as <Peer AS Number> peer <remote peer
IP> on multihop on graceful-restart on
set bgp external remote-as <Peer AS Number> peer <remote peer
IP> on multihop on graceful-restart on
```

Peer AS Number - The AS Number of the SASE network. If not set already, enter 64512.

Remote peer IP - Enter remote IP addresses of the two tunnels created in step 3.

g. Create an inbound route filter by executing these command:

```
set inbound-route-filter bgp-policy based-on-as as <AS
Number> on
```

AS Number - The AS Number of the SASE network.

h. Create a routes distribution rule by executing these command:

```
set route-redistribution to bgp-as <AS Number> from static-
route all-ipv4-routes on
```

AS Number - The AS Number of the Check Point SASE network.

i. Save the configuration:

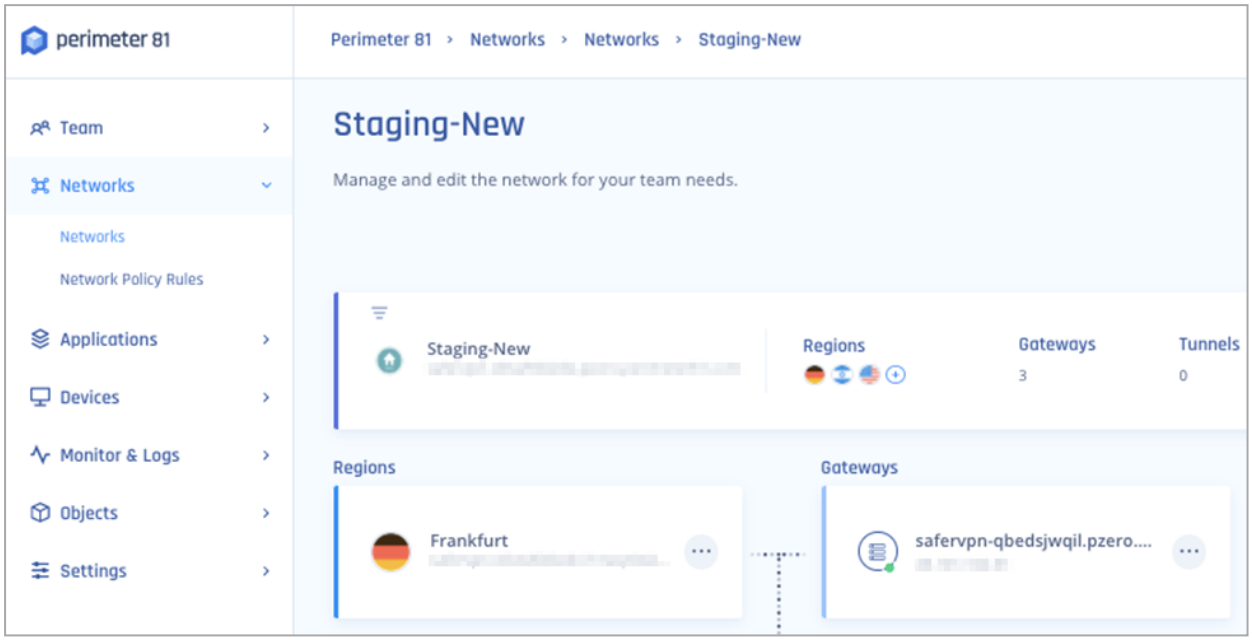
```
save config
```

2. Log in to the **Check Point SmartConsole**.
   a. Open the **Maestro Security Group Properties**.
   b. Go to **Network Management**.
   c. From the **Get Interfaces** list, select **Get interfaces Without Topology**.
   d. Verify that the two VPN Tunnel Interfaces are added.
   e. Publish and install the policy.

Part 2 - Configuration in SASE Administrator Portal

Step 1 : Configuring Tunnel and Routes Table

1. Access the SASE Administrator Portal and click **Networks**.



2. Select the network.
3. Click ··· .
4. Select **Add Tunnel** for the gateway from which you want to add the IPsec Site-2-Site VPN tunnel.
   a. Click **IPsec Site-2-Site Tunnel** and click **Continue**.

b. Click **Redundant Tunnels** and click **Continue**.

c. In the **Tunnel name** field, enter a logical name.

d. Expand **Tunnel 1** and specify these:

   i. **Shared Secret** – The value previously set on the first star policy.

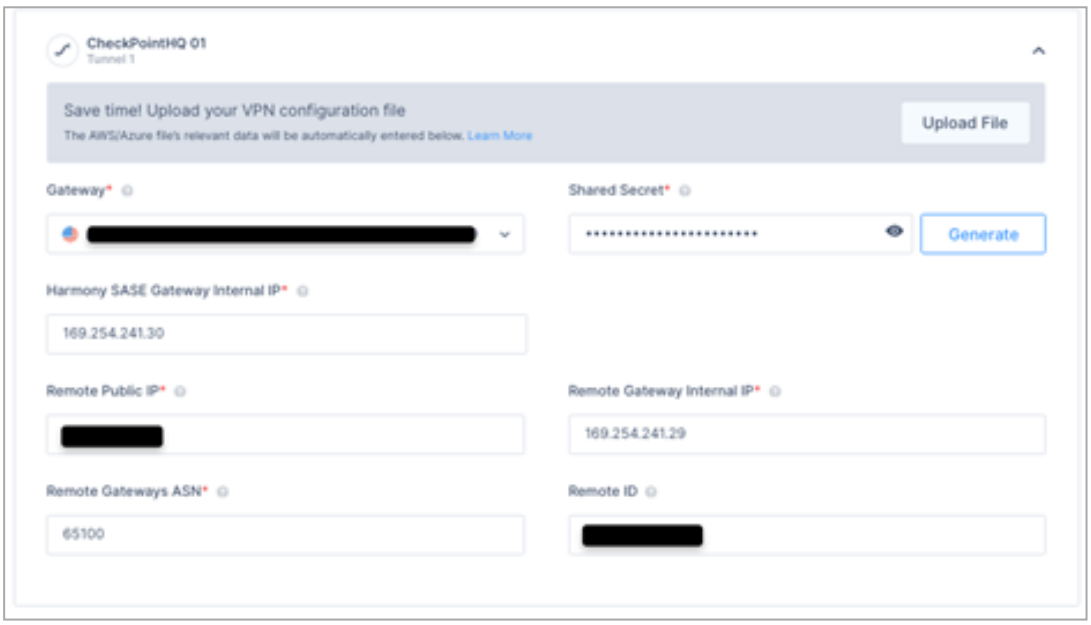
   ii. **SASE Gateway Internal IP** - The remote address of the first Check Point Gateway used under the VTI settings.

   iii. **Remote Public IP** - The public IP of the Maestro Security Group.

   iv. **Remote Gateway Internal IP** -The first local address of the Maestro Security Group under the VTI settings.

   v. **Remote Gateways ASN** - The ASN of the Maestro Security Group.

   vi. **Remote ID** - The router ID of the Maestro Security Group used under the BGP settings above.



e. Expand **Tunnel 2** and specify these:

   i. **Gateway** - Select the second SASE Gateway for the tunnel.

   ii. **Shared Secret** - The value previously set on the second star policy.

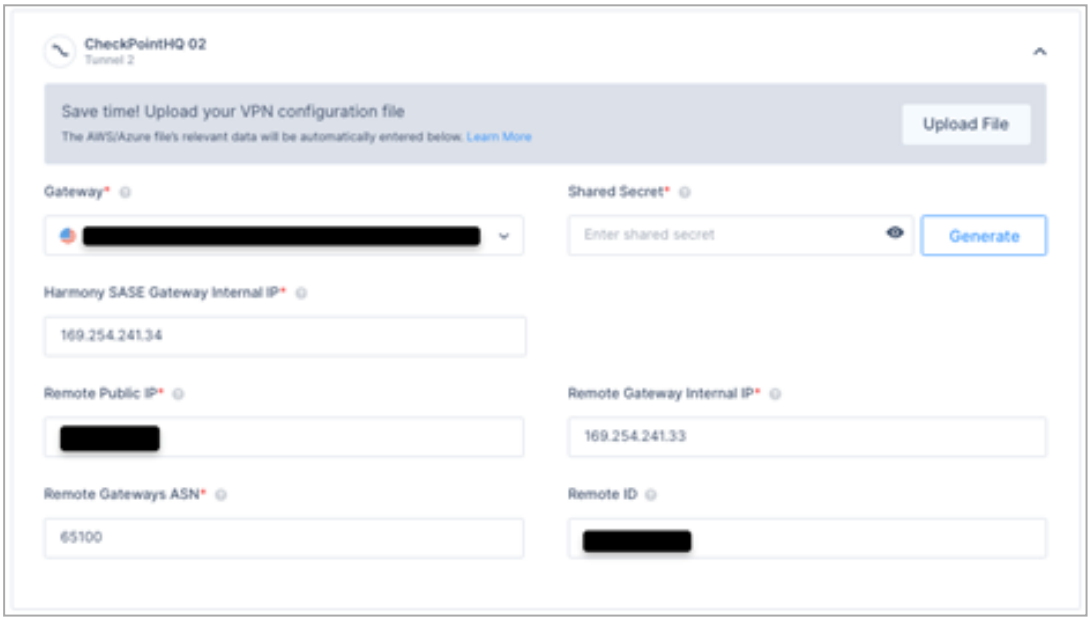
   iii. **SASE Gateway Internal IP** - The remote address of the second SASE Gateway used under the VTI settings.

   iv. **Remote Public IP** - The public IP of the Maestro Security Group.

   v. **Remote Gateway Internal IP** -The second local address of the Maestro Security Group used under the VTI settings.

   vi. **Remote Gateway ASN** - The ASN of the Maestro Security Group.

   vii. **Remote ID** - The router ID of the Maestro Security Group used under the BGP settings above.

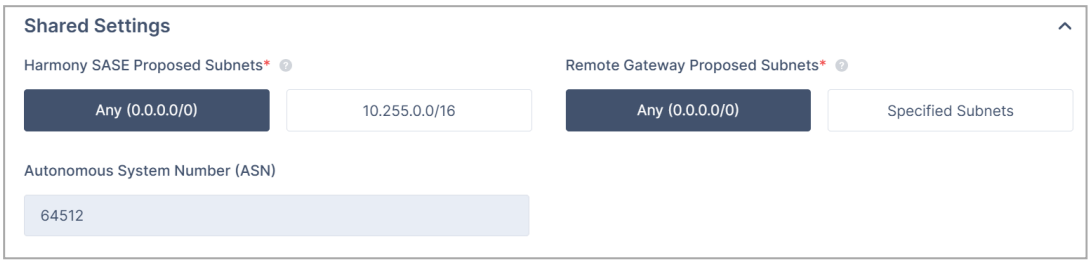


f. Expand **Shared Settings** and specify these:

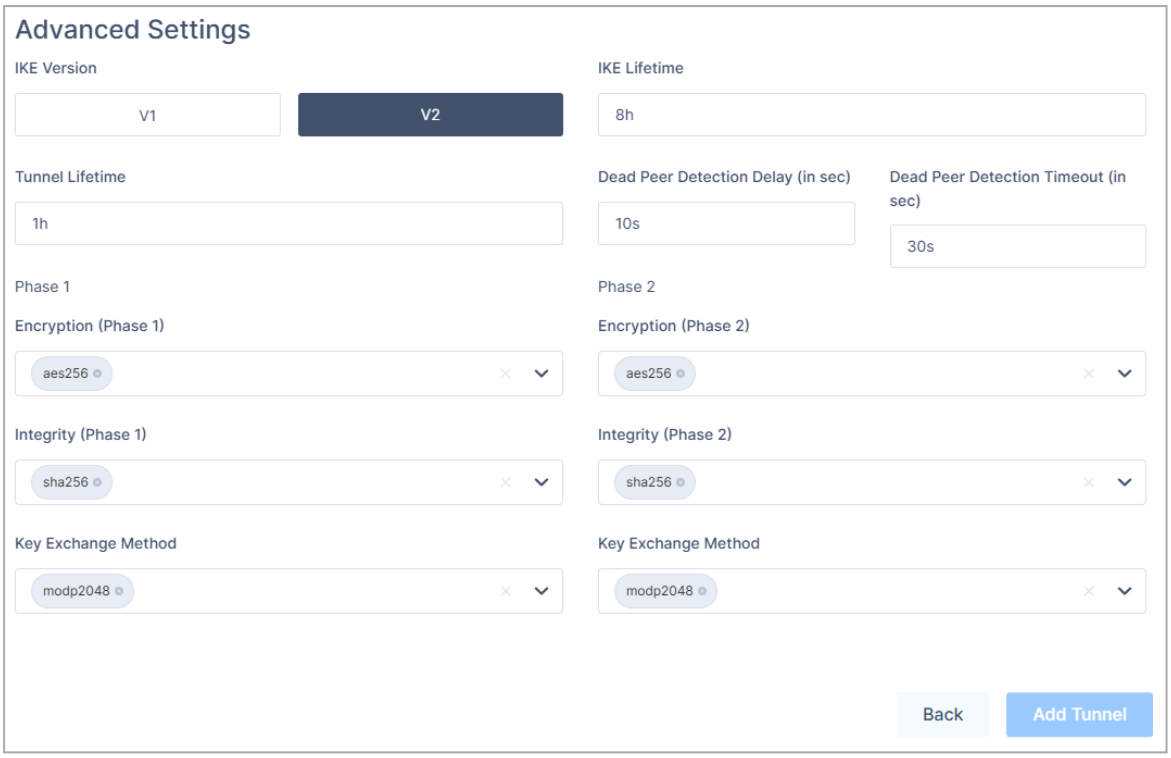
   i. **SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.

   ii. **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.

   iii. **Autonomous System Number (ASN)** - Default value is **64512**, if not set, enter the AS Number for the SASE network.



g. In the **Advanced Settings** section, specify these:



i. **IKE Version:** V2

ii. **IKE Lifetime:** 8h

iii. **Tunnel Lifetime:** 1h

iv. **Dead Peer Detection Delay:** 10s

v. **Dead Peer Detection Timeout:** 30s

vi. **Phase 1:**

   i. **Encryption(Phase 1):** aes256

   ii. **Integrity (Phase 1):** sha256

   iii. **Key Exchange Method:** modp2048

vii. **Phase 2:**

   i. **Encryption(Phase 2):** aes256

   ii. **Integrity (Phase 2):** sha256

   iii. **Key Exchange Method:** modp2048

viii. Click **Add Tunnel**.

5. Select **Routes Table**:

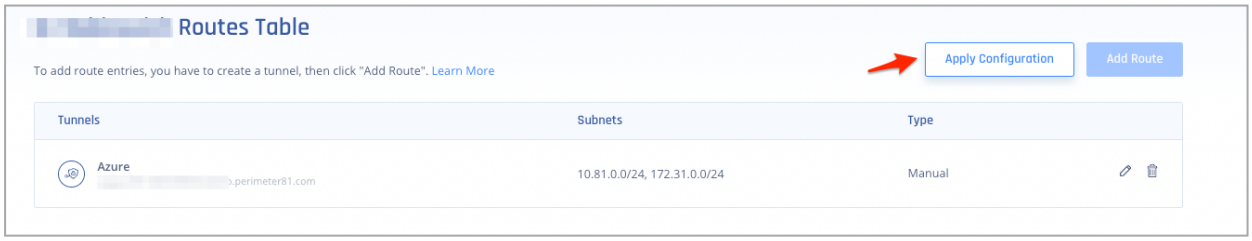
a. Click **Add Route**.

The **Add Route** popup appears.

b. Enter all the Subnets on the remote side of the tunnel and then click **Add Route**.

Note - Make sure that in the Tunnel list, you have selected the previously entered Tunnel name.

6. Click **Apply Configuration**.



Step 2: Verifying the Setup

Once you complete the above steps, your tunnel should be active.

1. Verify the setup in the SASE Administrator Portal:
   a. Click **Networks**.
   b. Locate the tunnel you created, and check the tunnel status.

      It should indicate that the tunnel is **Up**, signifying a successful connection.
2. Verify the setup in the SASE Agent:

a. Connect to your network using the SASE Agent.

b. Access one of the resources in your environment.

Cisco ASA Firewall

You can configure the tunnel in the Cisco Adaptive security Appliance (ASA) firewall either using CLI or ASDM.

To configure the tunnel in Cisco ASA firewall through CLI:

1. Connect to the firewall through SSH with the privilege-15-level account and then enter the enable mode. For example, using PuTTY.
2. Create a tunnel profile and proposal with the values specified in the Check Point SASE Administrator Portal. Run:

```
crypto ipsec ikev2 ipsec-proposal Tun-Prop
 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile Tun-Prof
 set ikev2 ipsec-proposal Tun-Prop
 set pfs group21
 set security-association lifetime seconds 3600
```

3. Create a crypto policy with the values specified in the Check Point SASE Administrator Portal. Run:

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 28800
crypto ikev2 enable outside
```

4. Select IPsec IKEv2 Tunnels and create a new tunnel with the values specified in the Check Point SASE Administrator Portal. Run:

```
group-policy Tun-Grp-Pol internal
group-policy Tun-Grp-Pol attributes
 vpn-tunnel-protocol ikev2
```

```
tunnel-group 131.226.X.X type ipsec-l2l
tunnel-group 131.226.X.X general-attributes
 default-group-policy Tun-Grp-Pol
tunnel-group 131.226.X.X ipsec-attributes
 ikev2 remote-authentication pre-shared-key SuperSecret
 ikev2 local-authentication pre-shared-key SuperSecret
```

5. Create your Virtual Tunnel Interface (VTI). Please be sure to use the IP address in the text. Run:

```
interface Tunnel1
 nameif P81_131.226.X.X
 ip address 169.254.2.122 255.255.255.252
 tunnel source interface outside
 tunnel destination 131.226.X.X
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Tun-Prof
```

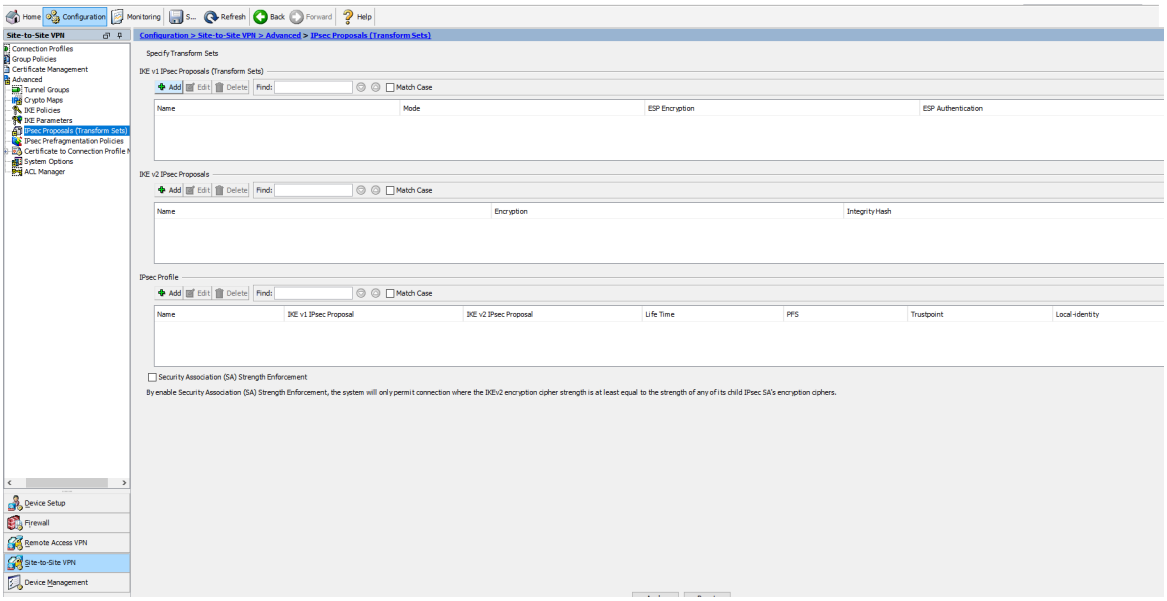
6. Create a route back to the Check Point SASE subnet. Run:

```
route P81_131.226.X.X 10.255.0.0 255.255.0.0 169.254.2.121 1
```

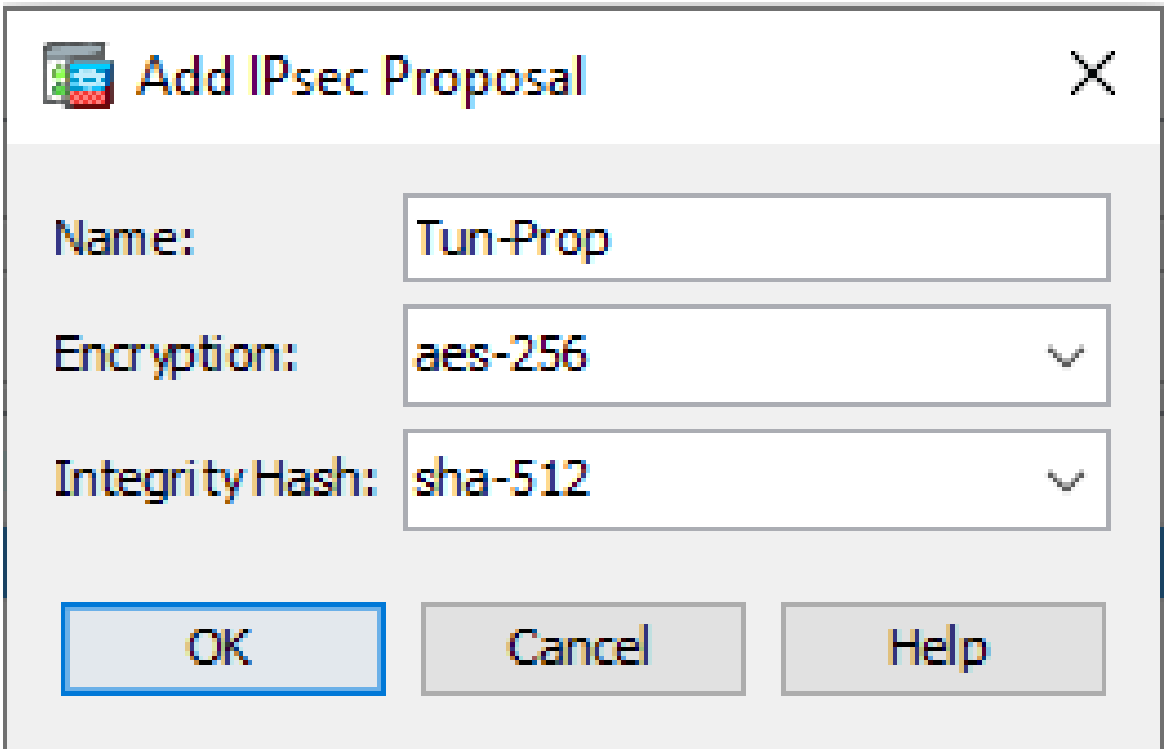
To configure the tunnel with Cisco ASA firewall through Adaptive Security Device Manager (ASDM):

1. Log in to the firewall using ASDM.
2. Create a tunnel profile and proposal with the values specified in the Check Point SASE Administrator Portal:

a. Click **Configuration > Site-to-site VPN > Advanced > IPsec Proposals (Transform Sets)**.

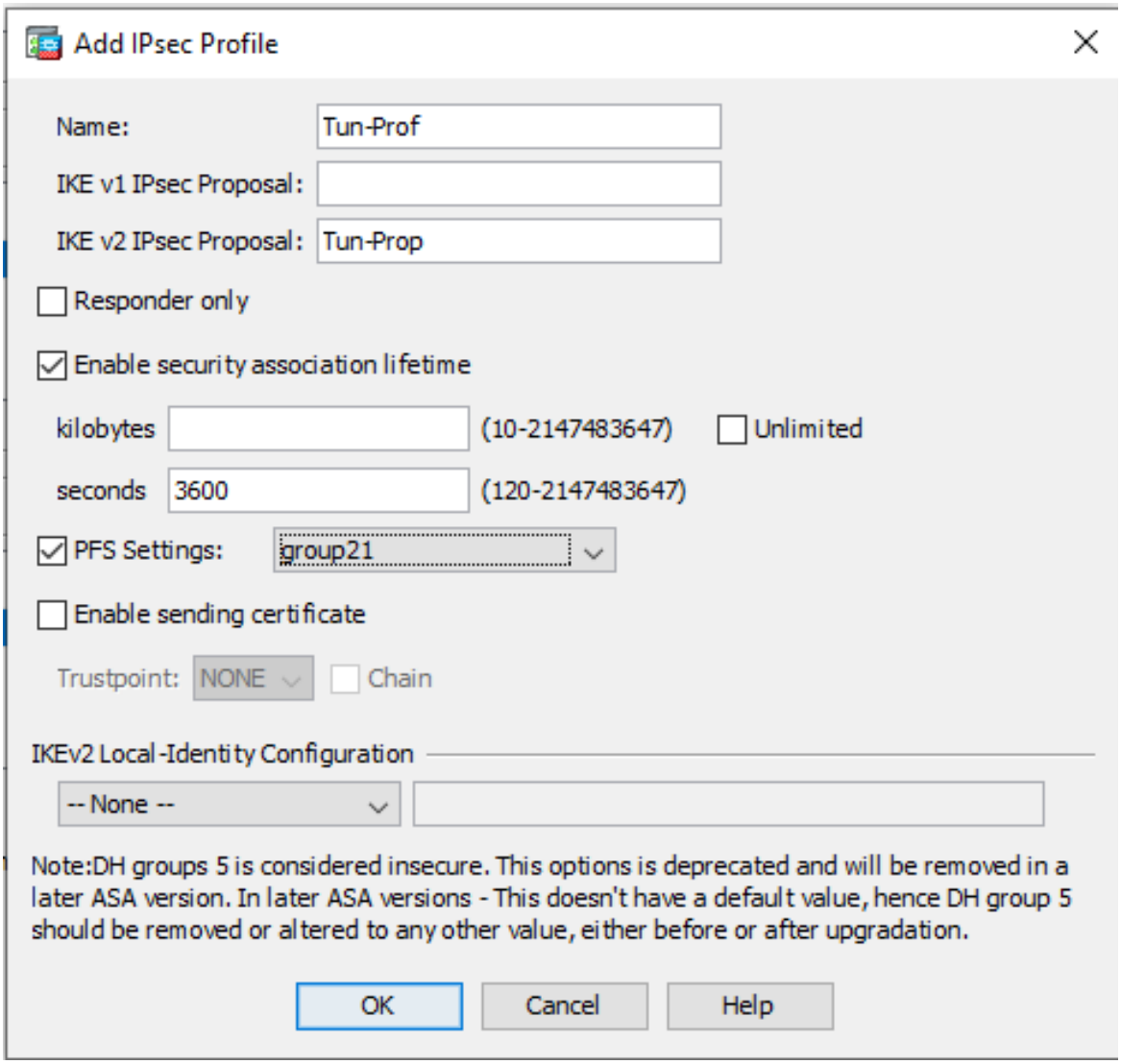


b. In the **IKE v2 IPsec Proposals** section, click **Add**:



Field	Enter
Name	Tun-Prop
Encryption	aes-256
Integrity Hash	sha-512

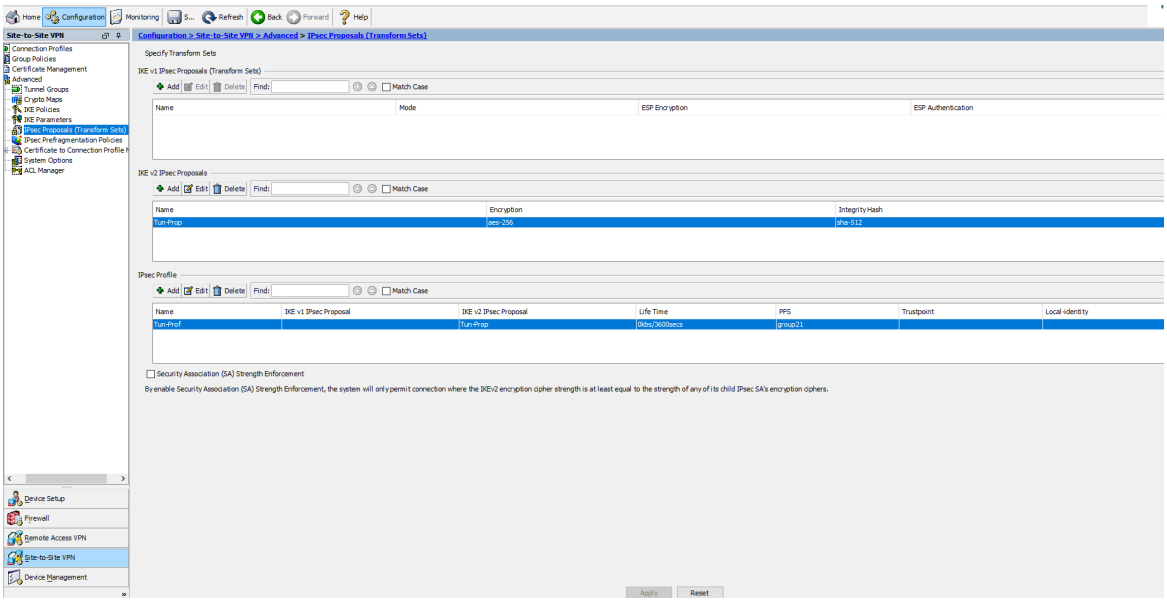
In the **IPsec Profile** section, click **Add**:



Field	Enter
Name	Tun-Prop
IKE v2 IPsec Proposal	Tun-Prop
Enable security association lifetime	Select and leave **kilobytes** blank.
Seconds	3600

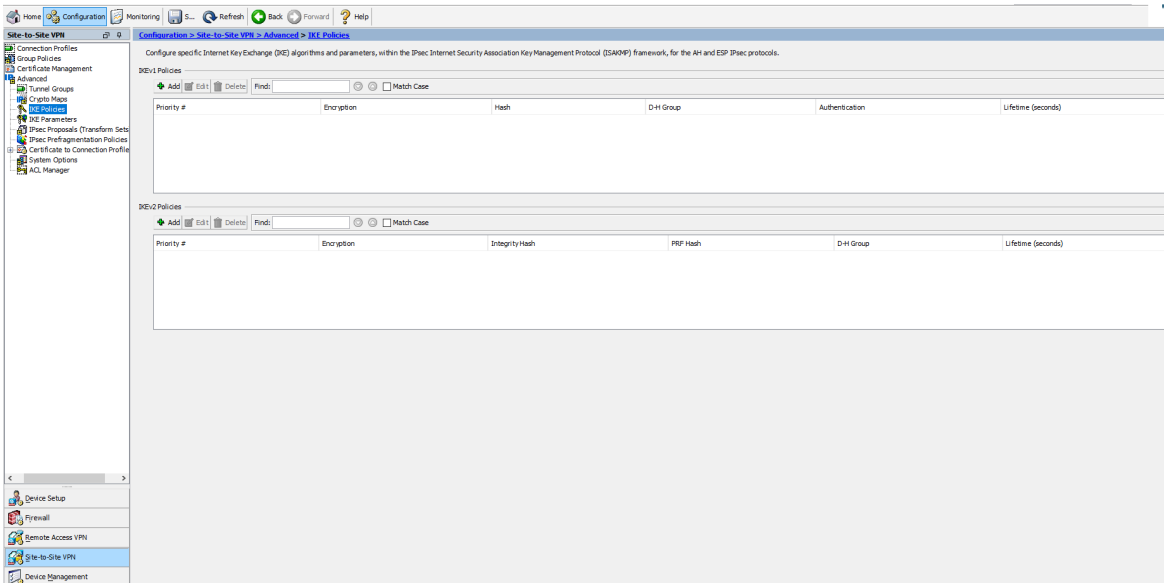
c. Click **OK**.

d. Click **Apply** and **Save**.

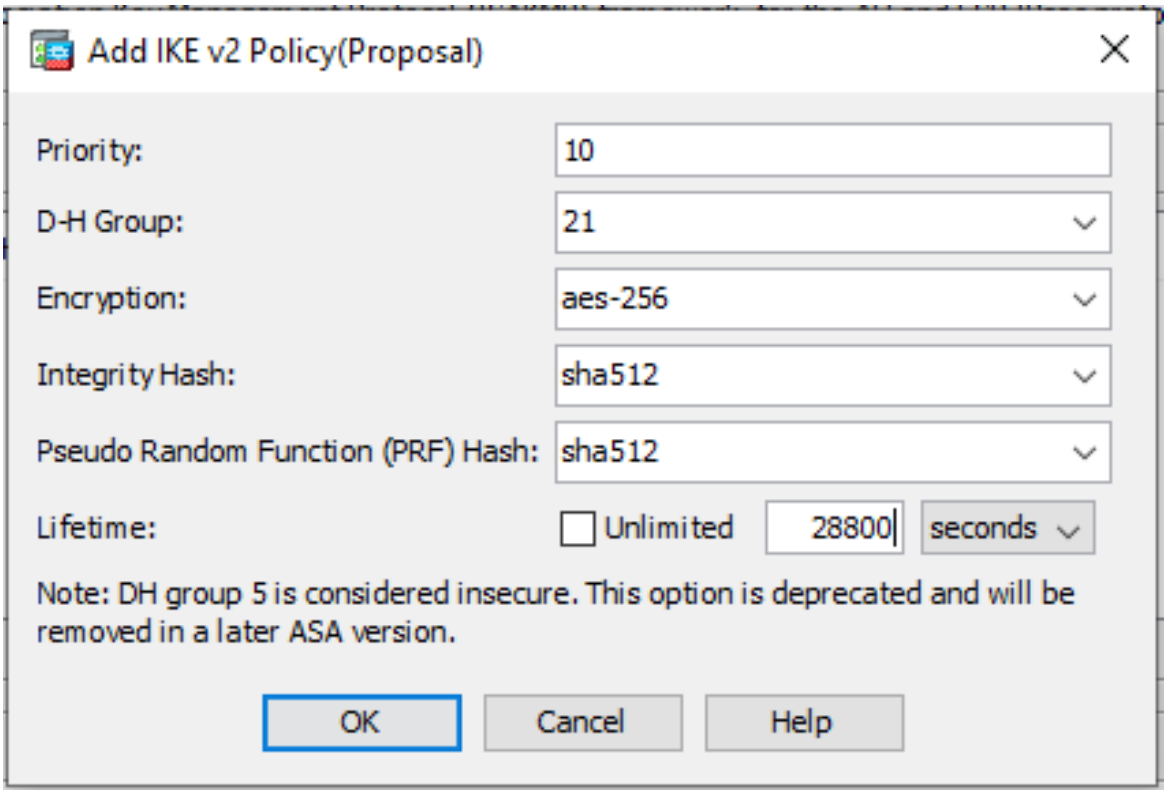


3. Create a crypto policy with the values specified in the Check Point SASE Administrator Portal:

   a. Go to **Configuration > Site-to-Site VPN > Advanced > IKE Policies**.



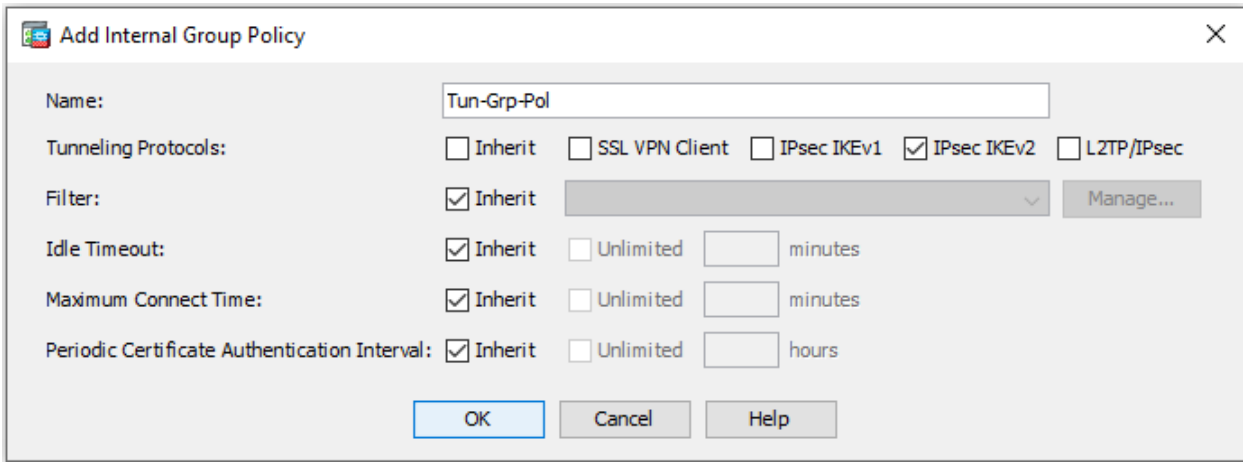
b. In the **IKEv2 Policies** section, click **Add**:



Field	Enter
Priority	10
D-H Group	21
Encryption	AES-256
Integrity Hash	sha256
Pseud0-Random Function (PRF) Hash	sha256
Lifetime	28800 seconds

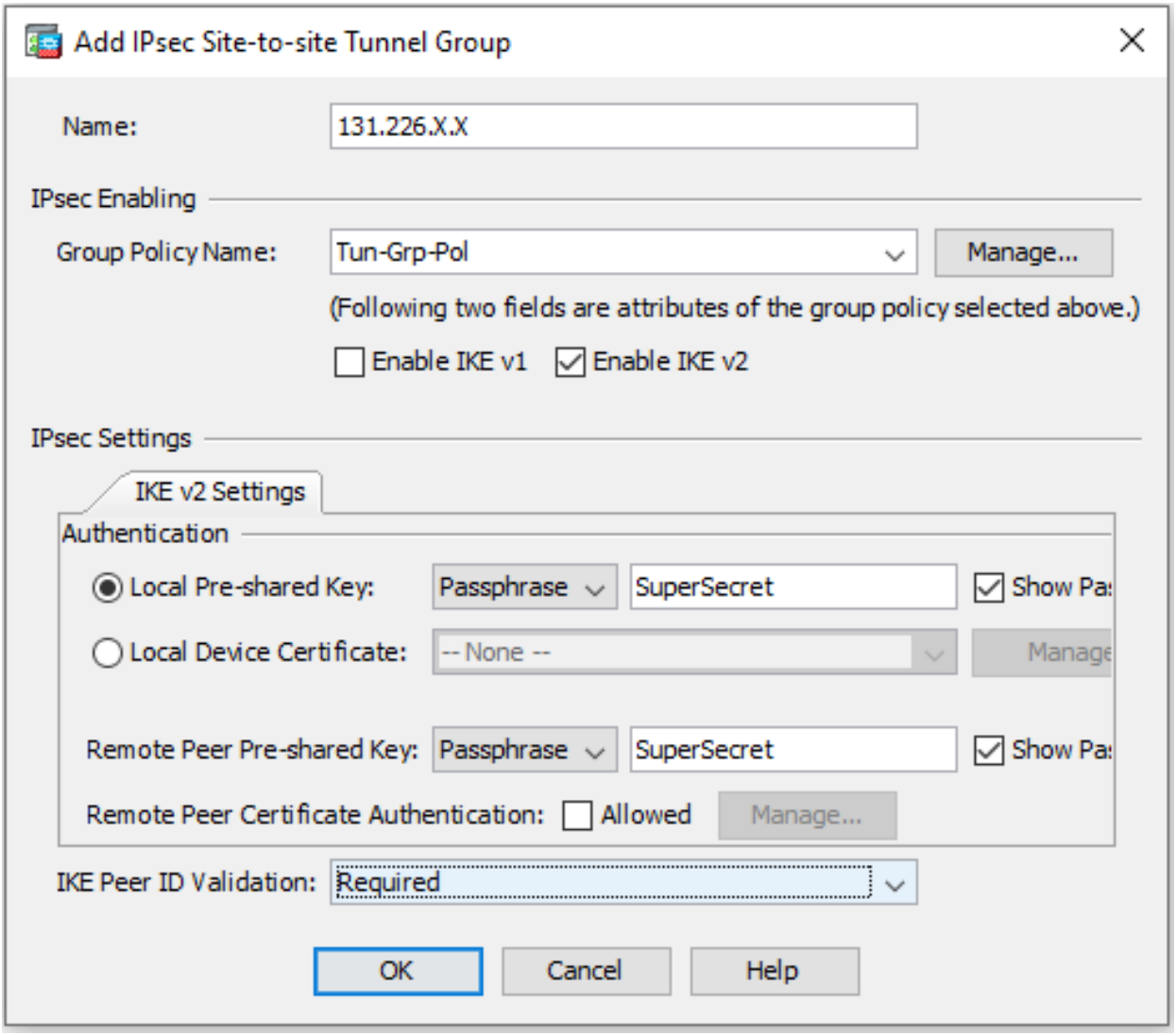
c. Click **OK**.

4. Go to **Configuration > Site-to-Site VPN > Group Policies** and click **Add**:



Field	Enter
Name	Tun-Prop
Tunneling Protocols	IPsec IKEv2

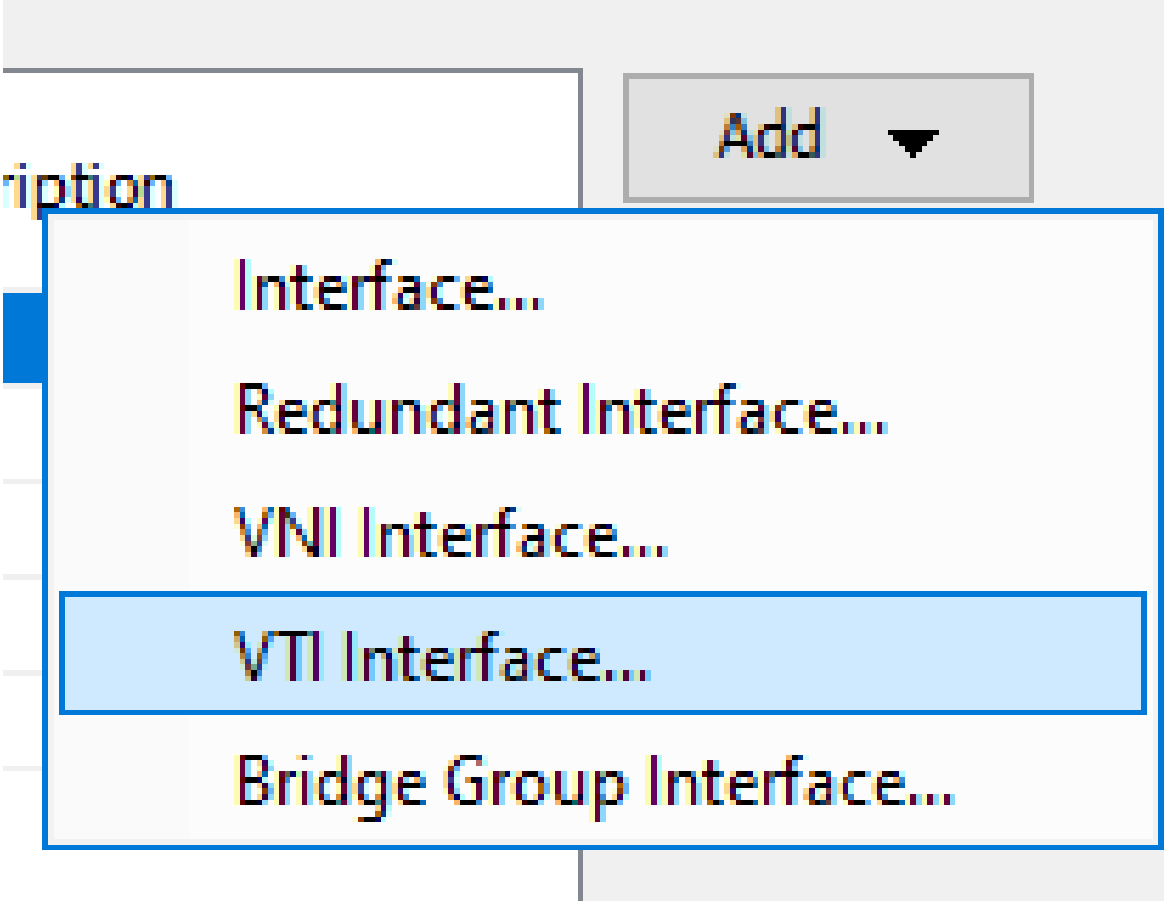
5. Go to **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups** and click **Add**:



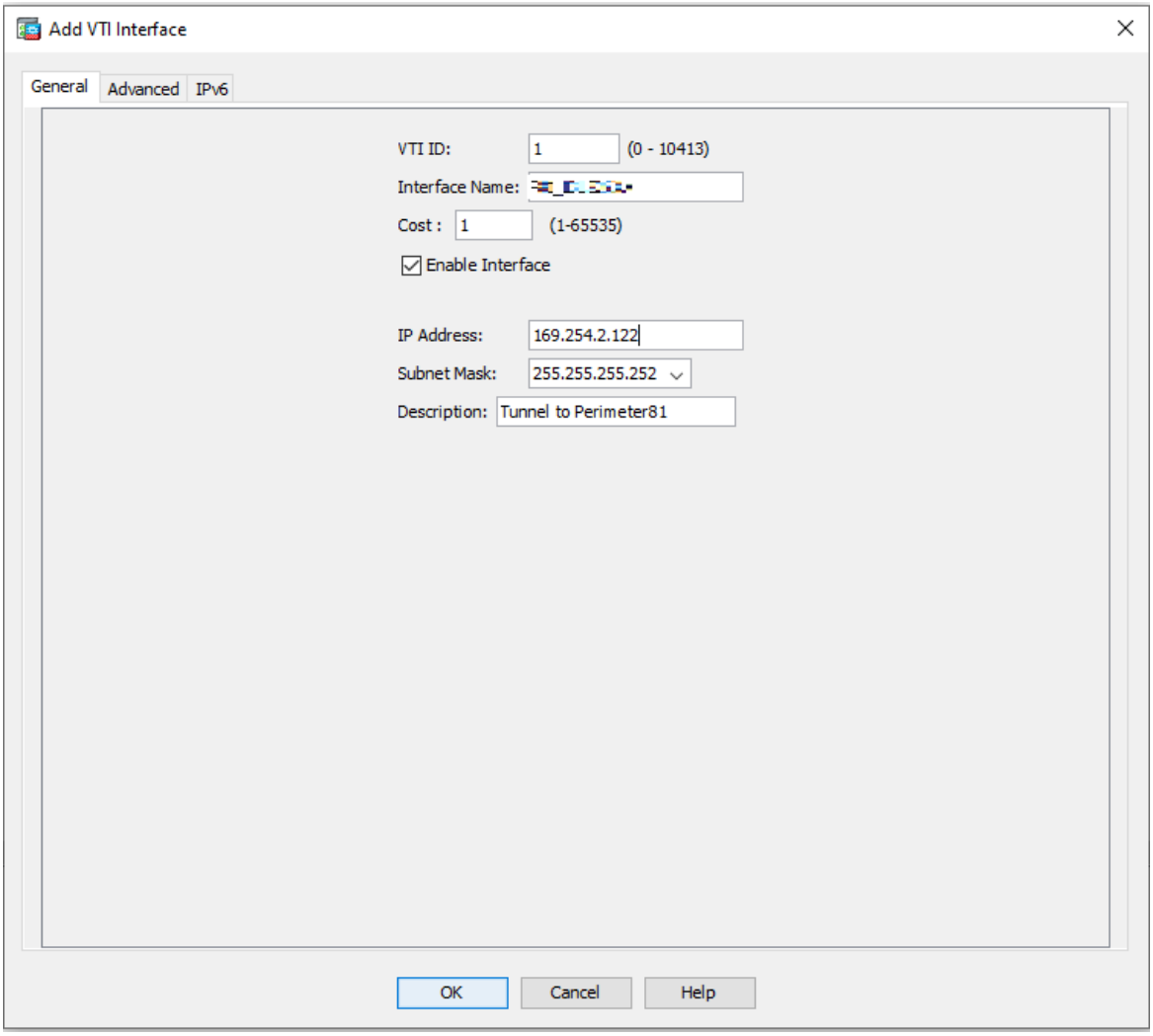
Field	Enter
Name	131.226.x.x. Make sure this is same value specified in the Check Point SASE Administrator Portal.
Group Policy Name	Tun-Grp-Pol
Local Pre-Shared Key	Secret key specified in the Check Point SASE Administrator Portal.
Remote Pre-Shared Key	Secret key specified in the Check Point SASE Administrator Portal.

6. Go to **Configuration > Device Setup > Interface Settings > Interfaces** and click **Add**.

a. Select **VTI Interface**:

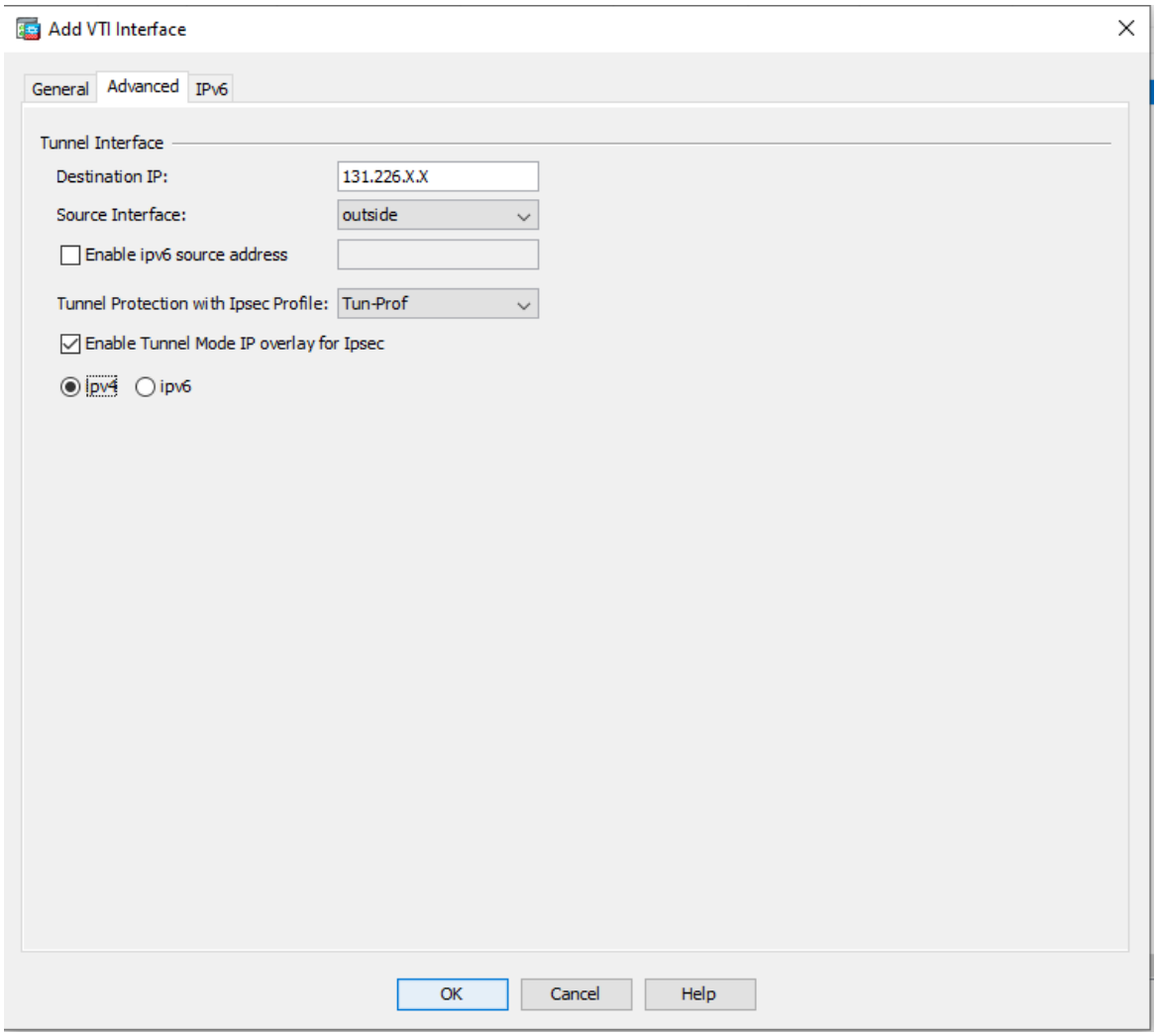


b. In the **General** tab:



Field	Enter
VTI ID	1
Interface Name	Name for the interface.
IP Address	169.254.2.122
Subnet Mask	255.255.255.252
Description	Tunnel to Check Point SASE.

c. In the **Advanced** tab:

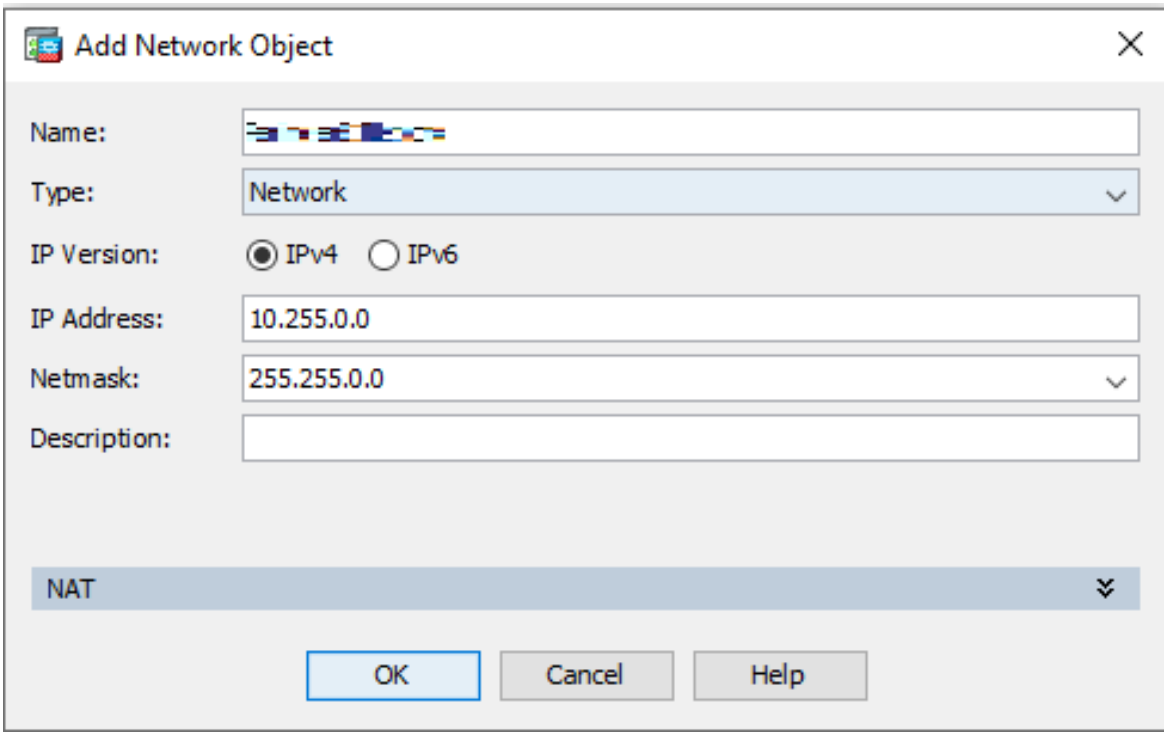


Field	Enter
Destination IP	131.226.x.x. Public IP address of Check Point SASE gateway.
Source Interface	Name for your outside interface.
Tunnel Protection with Ipsec Profile	Tun-Prof
Enable Tunnel Mode IP overlay for Ipsec	Select and select **ipv4**.

7. Create a route back to the Check Point SASE subnet:

a. Go to **Configuration > Firewall > Objects > Network Objects/Groups**.

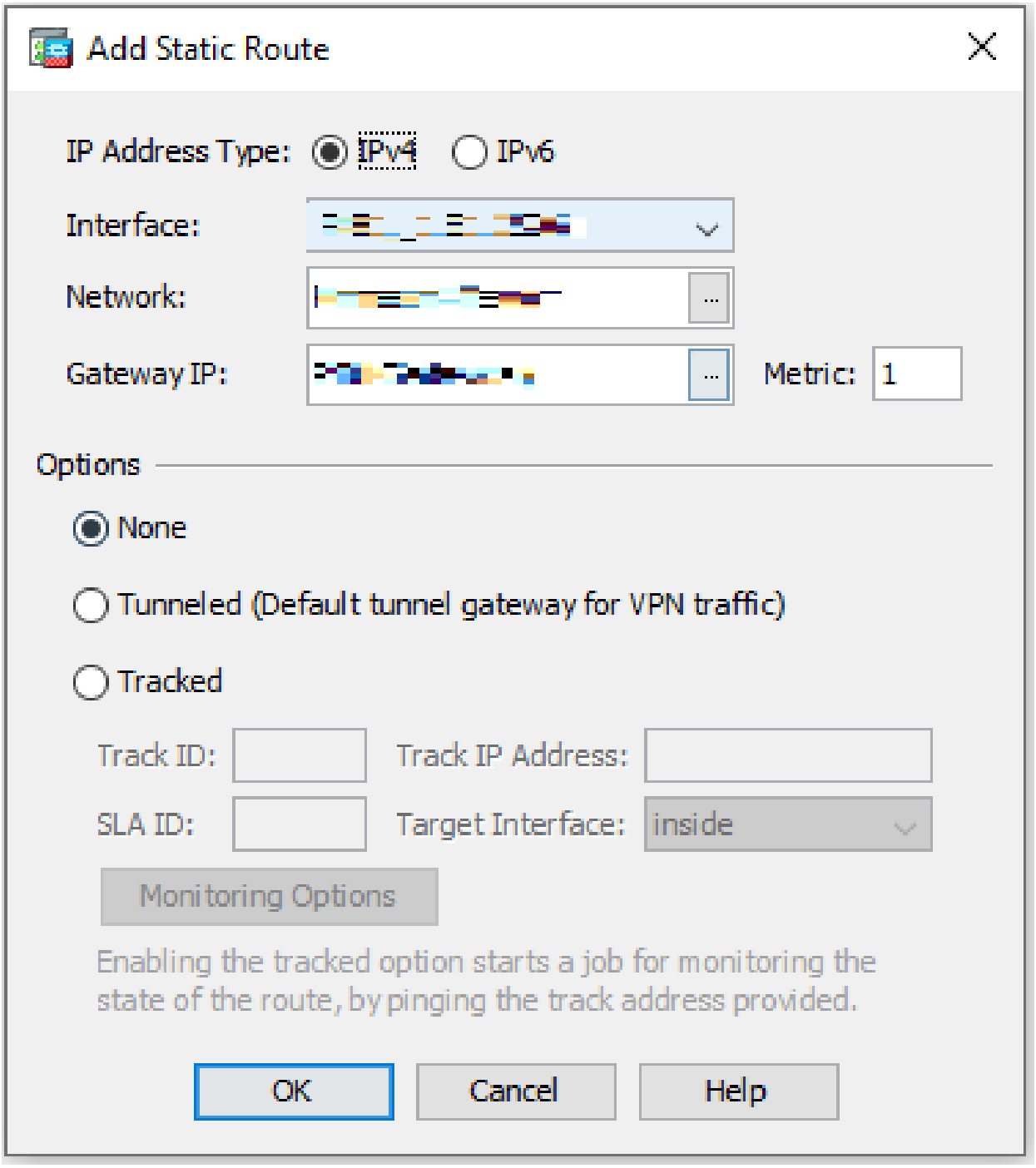
b. Clicking **Add > Network Object**:



Field	Enter
Name	Name for the object.
Type	Host
IP Version	IPv4
IP Address	169.254.2.121

c. Click **OK**.

8. Go to **Configuration > Device Setup > Routing > Static Routes** and then click Add:

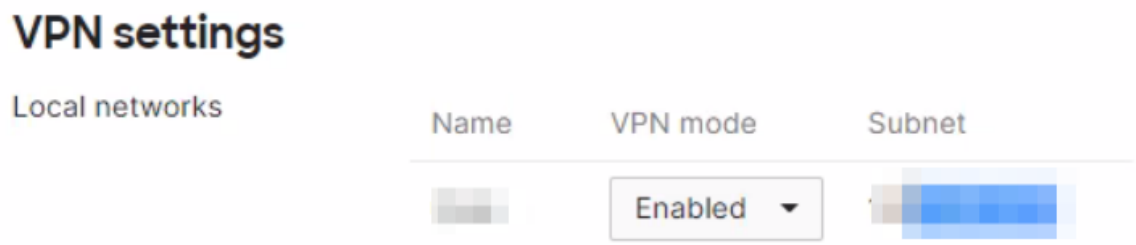


Field	Enter
IP address Type	IPv4
Interface	Interface that you created for the setup.
Network	Network that you created for the setup.
Gateway IP	Gateway that you created for the setup.

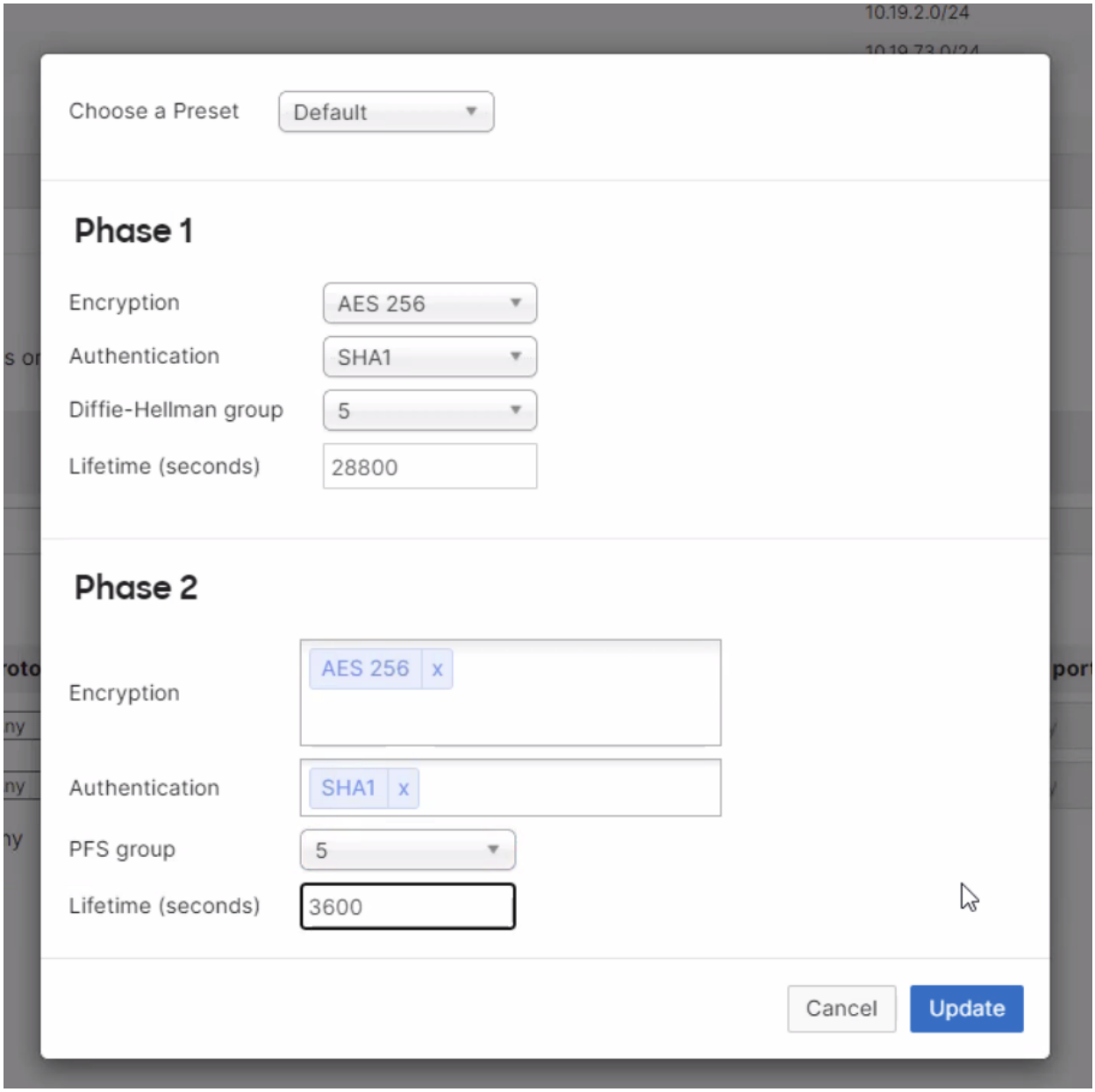
Cisco Meraki Router

To configure the tunnel in the Cisco Meraki Management Portal:

1. Log in to the Cisco Meraki Management Portal with the Administrator account.
2. Go to **Security Appliance > Configure > Site-to-site VPN**.
3. Make sure that the local LAN you want t connect from the Check Point SASE network is participating in the VPN.



4. Scroll down to the **Non-Meraki VPN peers** section.
5. Click **Add a peer**:



Field	Enter
Name	Name for the remote device or VPN.
IKE Version	IKEv1
Public Ip	Public IP address of the Check Point SASE gateway.
Remote ID	Public IP address of the Check Point SASE gateway.
Private subnets	Check Point SASE network subnets. Default is 10.255.0.0/16.
Preshared secret key	Secret key specified in the Check Point SASE Administrator Portal.

Field	Enter
IPsec Policy to use	Custom
Phase 1	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	28800
Phase 2	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	3600

6. Click **Update**.
7. Edit the router rules to allow the traffic through the Check Point SASE tunnel. These rules apply to inbound and/or outbound VPN traffic from all MX appliances in the organization that participate in site-to-site VPN.

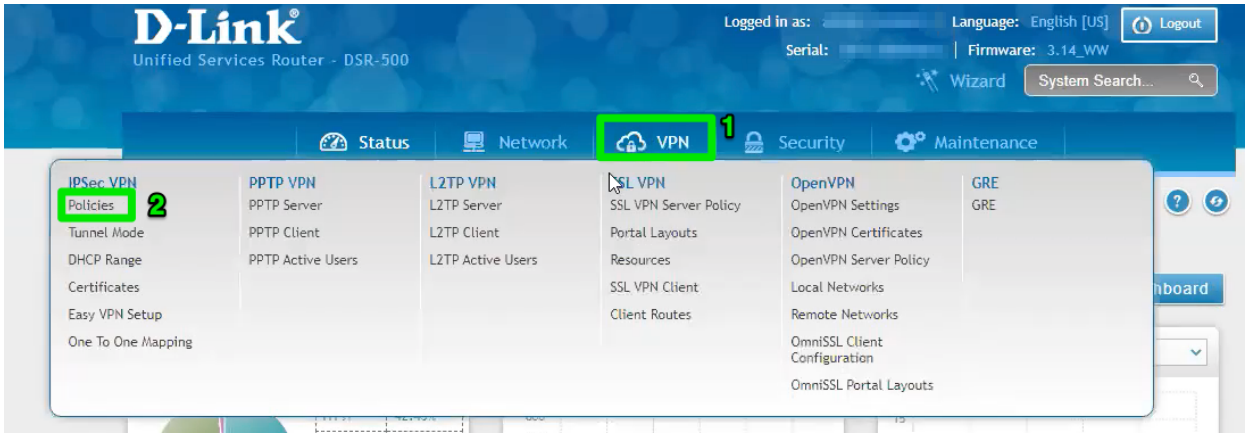
   To create a rule, got to **Security Appliance > Configure > Site-to-site VPN**, in the **Site-to-site firewall** section, select **Add a rule**.

   For reference, see the Layer 3 firewall rules.

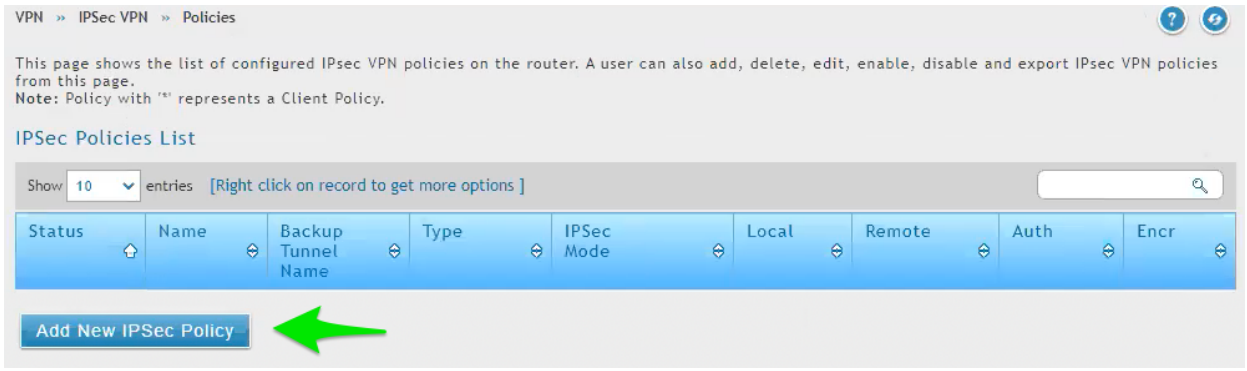
D-Link DSR Series Router

To configure the tunnel in the D-Link DSR Series Router Management Portal:

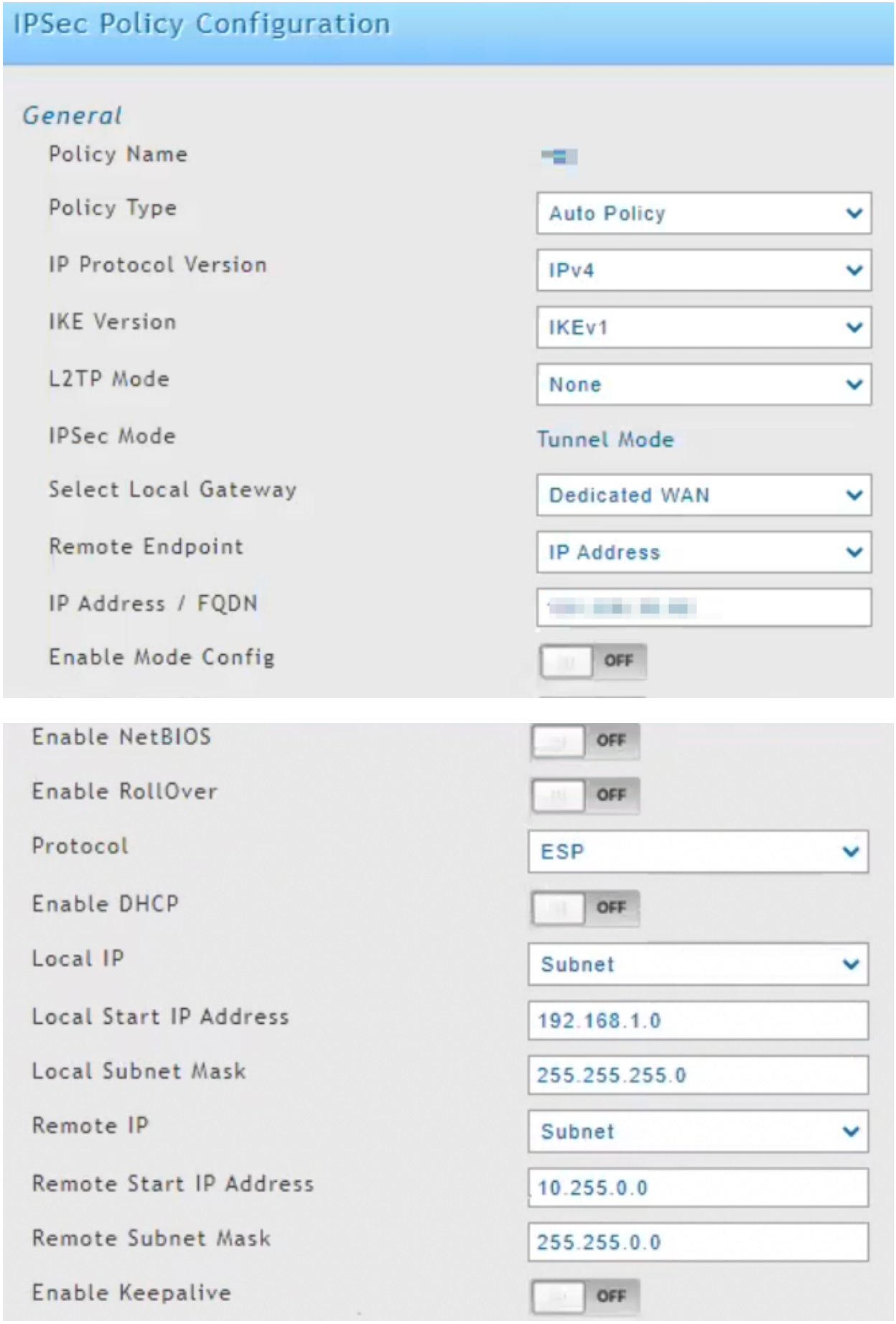
1. Log in to the D-Link DSR Series Router Management Portal with the Administrator.
2. Click **VPN**.



3. Click **IPSec VPN > Policies**.
4. Click **Add New IPSec Policy**.

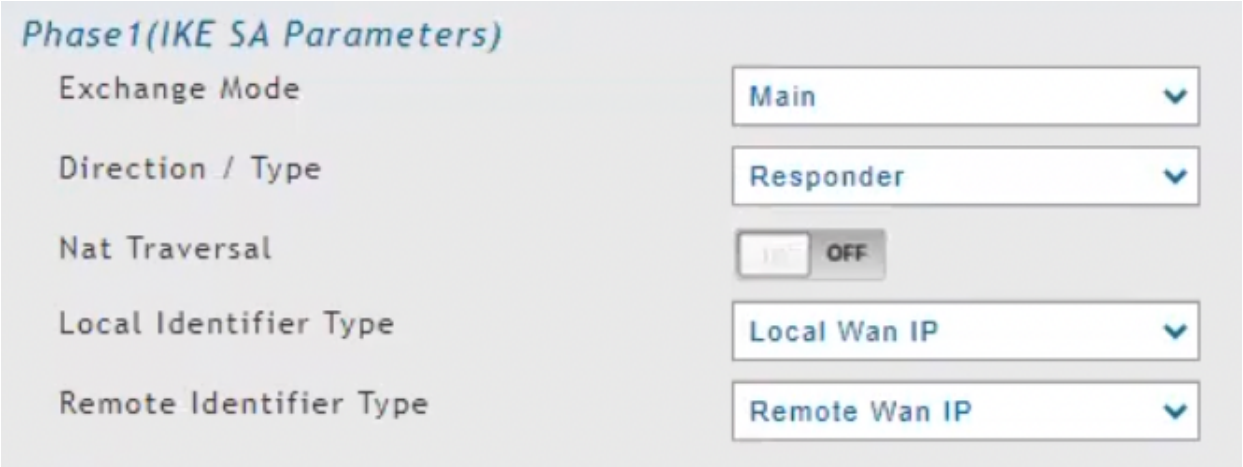


5. In the **General** section:


IPSec Policy Configuration
General
Policy Name
Policy Type
Auto Policy
IP Protocol Version
IPv4
IKE Version
IKEv1
L2TP Mode
None
IPSec Mode
Tunnel Mode
Select Local Gateway
Dedicated WAN
Remote Endpoint
IP Address
IP Address / FQDN
Enable Mode Config
OFF
Enable NetBIOS
OFF
Enable RollOver
OFF
Protocol
ESP
Enable DHCP
OFF
Local IP
Subnet
Local Start IP Address
192.168.1.0
Local Subnet Mask
255.255.255.0
Remote IP
Subnet
Remote Start IP Address
10.255.0.0
Remote Subnet Mask
255.255.0.0
Enable Keepalive
OFF

Field	Enter
Policy Name	Name for the policy.
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address/FQDN	Public IP address of the Check Point SASE gateway.
Enable Config Mode	Off
Enable NetBIOS	Off
Enable RollOver	Off
Protocol	ESP
Enable DHCP	Off
Local IP	Subnet
Local Start IP Address	Your local subnet
Local Subnet Mask	Matching subnet mask
Remote IP	Subnet
Remote Start IP Address	10.255.0.0
Remote Subnet Mask	255.255.0.0
Enable Keepalive	Off

6. In the **Phase1 (IKE SA Parameters)** section:



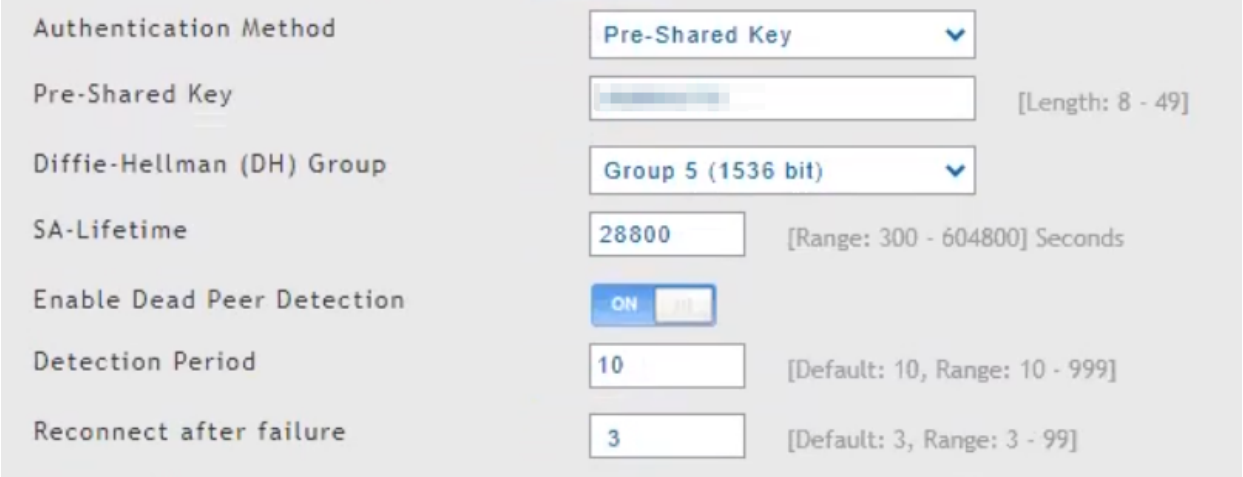
Field	Enter
Exchange Mode	Main
Direction/Type	Responder
NAT Traversal	Off
Local Identifier Type	Local Wan IP
Remote Identifier Type	Remote Wan IP

7. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
AES-128	Off
AES-256	On
Blowfish	Off

Field	Enter
3DES	Off
AES-192	Off

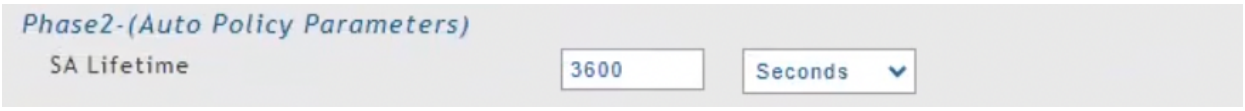
8. In the **Authentication Algorithm** section:



Field	Enter
MD5	Off
SHA2-256	Off
SHA2-512	On
Authentication Method	Pre-Shared Key
Pre-Shared Key	Secret key specified in the Check Point SASE Administrator Portal.
Diffie-Hellman (DH) Group	Group 5
SA-Lifetime	28800

Field	Enter
Enable dead Peer Detection	On
Detection Period	10
Reconnect after failure	3

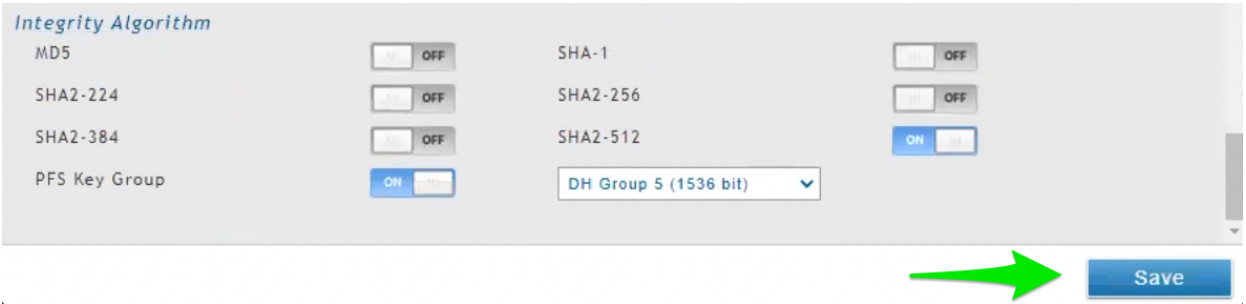
9. In the **Phase2 - (Auto Policy Parameters)** section, in the **SA Lifetime** field, enter **3600 seconds**.



10. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
3DES	Off
AES-192	Off
None	Off
AES-128	Off
AES-256	On

11. In the **Integrity Algorithm** section:



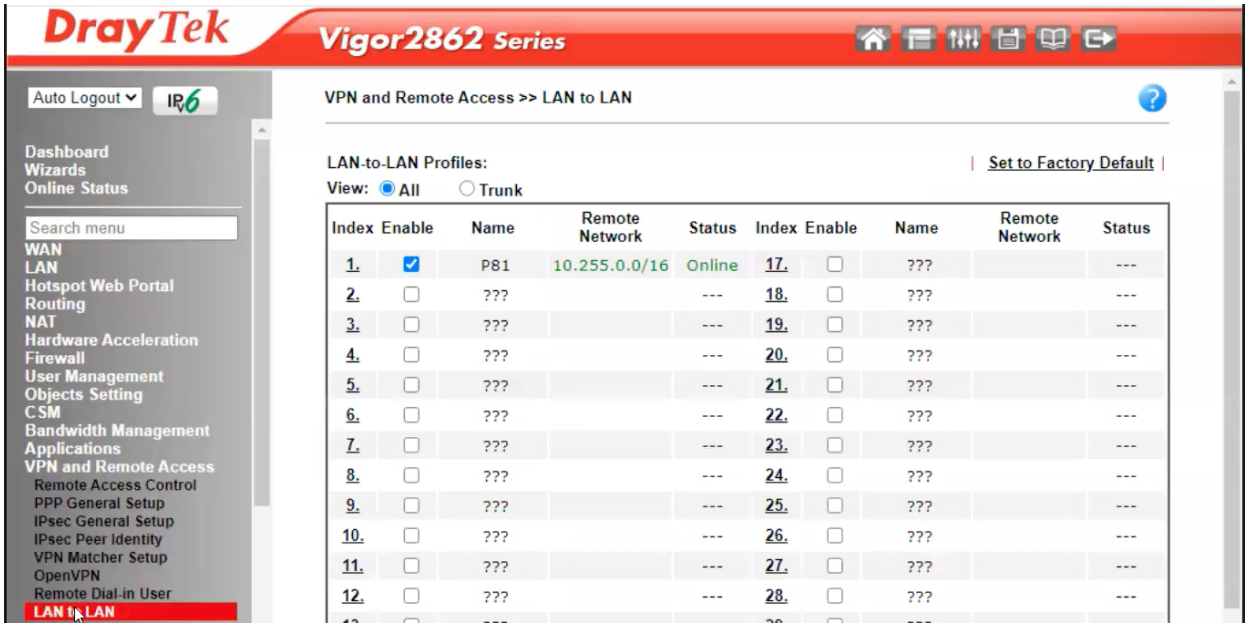
Field	Enter
MD5	Off
SHA-224	Off
SHA2-384	Off
PFS Key Group	On
SHA-1	Off
SHA2-256	Off
SHA2-512	On

12. Click **Save**.

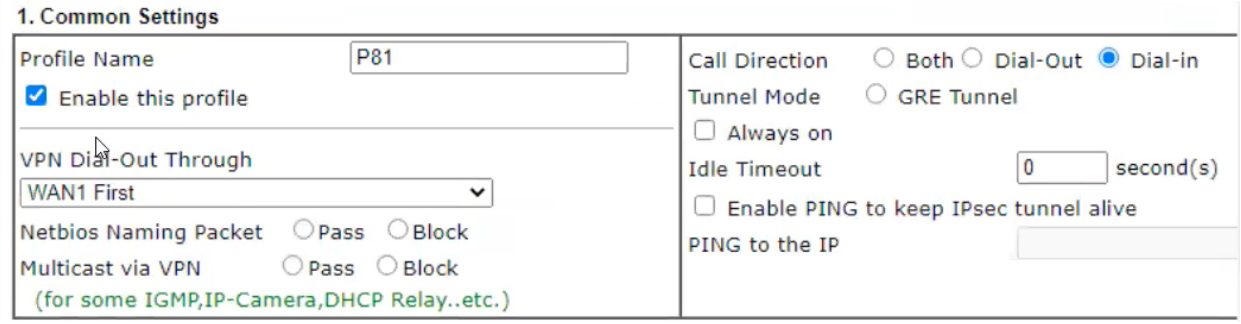
DrayTek Vigor2862 Router

To configure the tunnel in the DrayTek Vigor2862 Management Portal:

1. Log in to the DrayTek Vigor2862 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **LAN to LAN** and create a new profile.

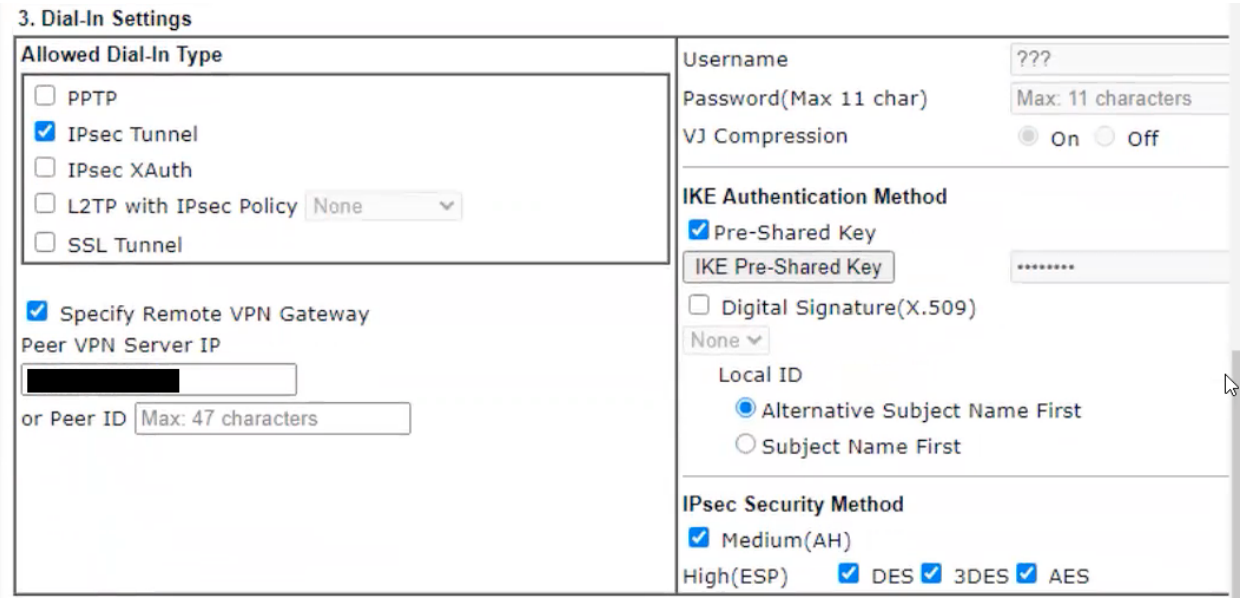


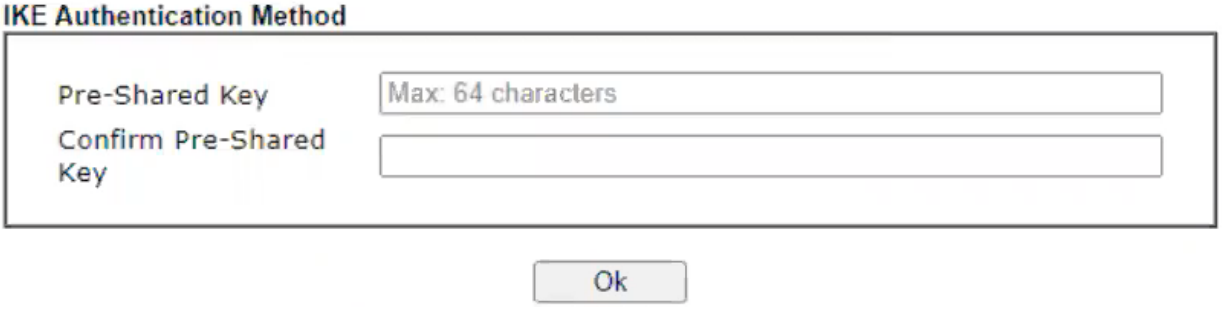
4. In the **Custom Settings** tab:



Field	Enter
Profile Name	Name for the profile. For example, Check Point SASE.
Enable this profile	Select
VPN Dial-Out Through	Your WAN interface.
Call Direction	Dial-in
Idle Timeout	0

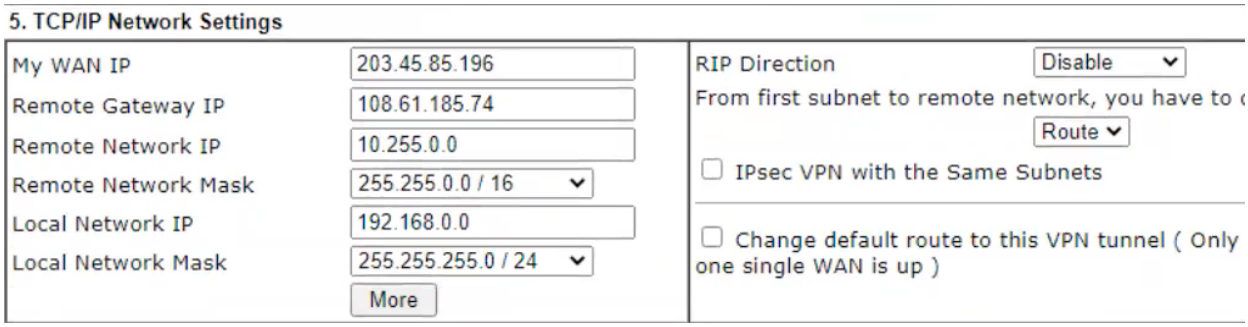
5. In the **Dial-In Settings**tab:





Field	Enter
Allowed Dial-In Type	IPsec Tunnel
Specify Remote VPN Gateway	Public IP address of the Check Point SASE gateway.
Pre-Shared Key	Select and click **IKE Pre-Shared Key** and enter the secret key specified in the Check Point SASE Administrator Portal.

6. In the **TCP/IP Network Settings** tab:

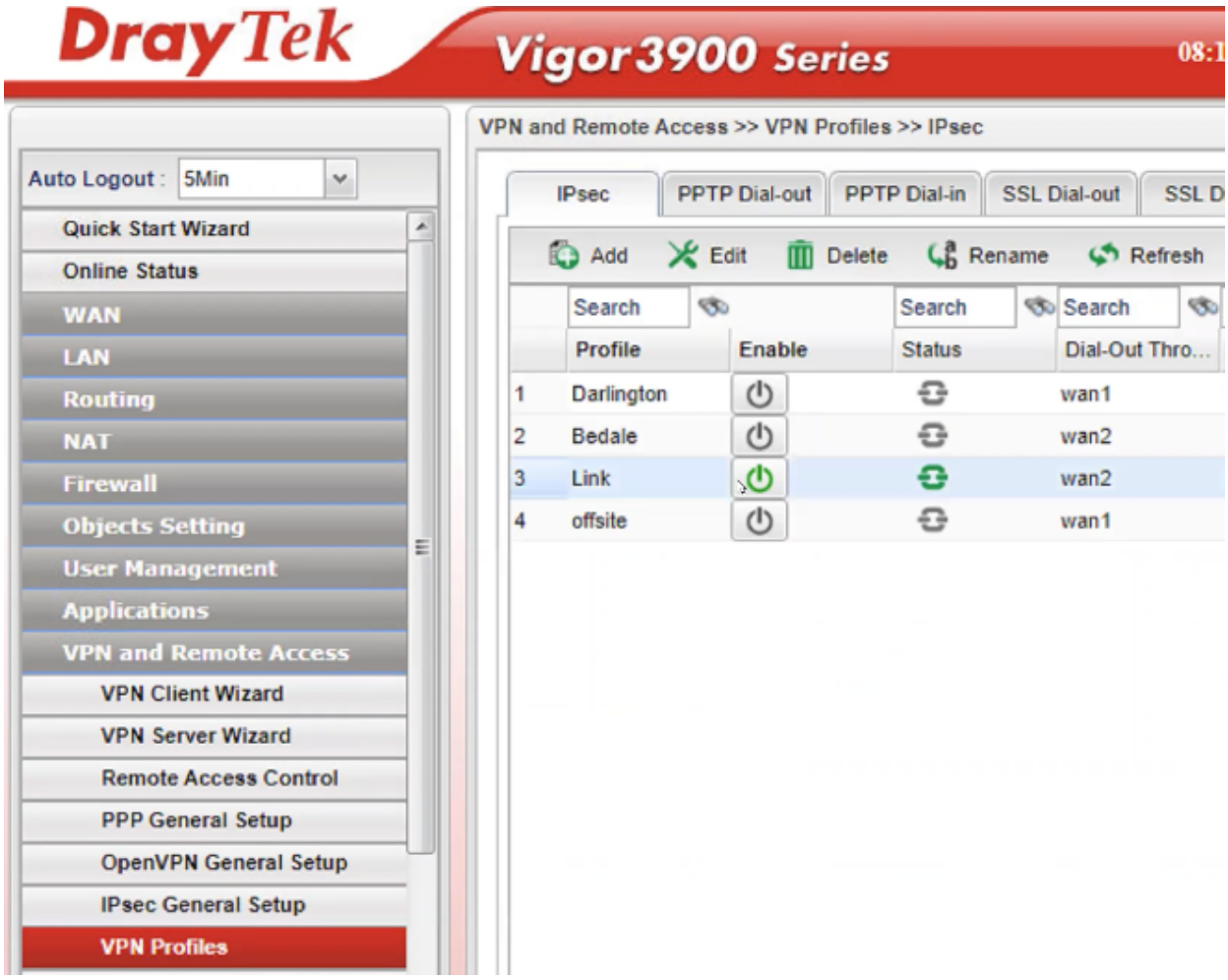


Field	Enter
My WAN IP	Your WAN interface's default IP address.
Remote Gateway IP	Public IP address of the Check Point SASE gateway.
Remote Network IP	Check Point SASE network subnet.
Local Network IP	Your LAN subnnet.

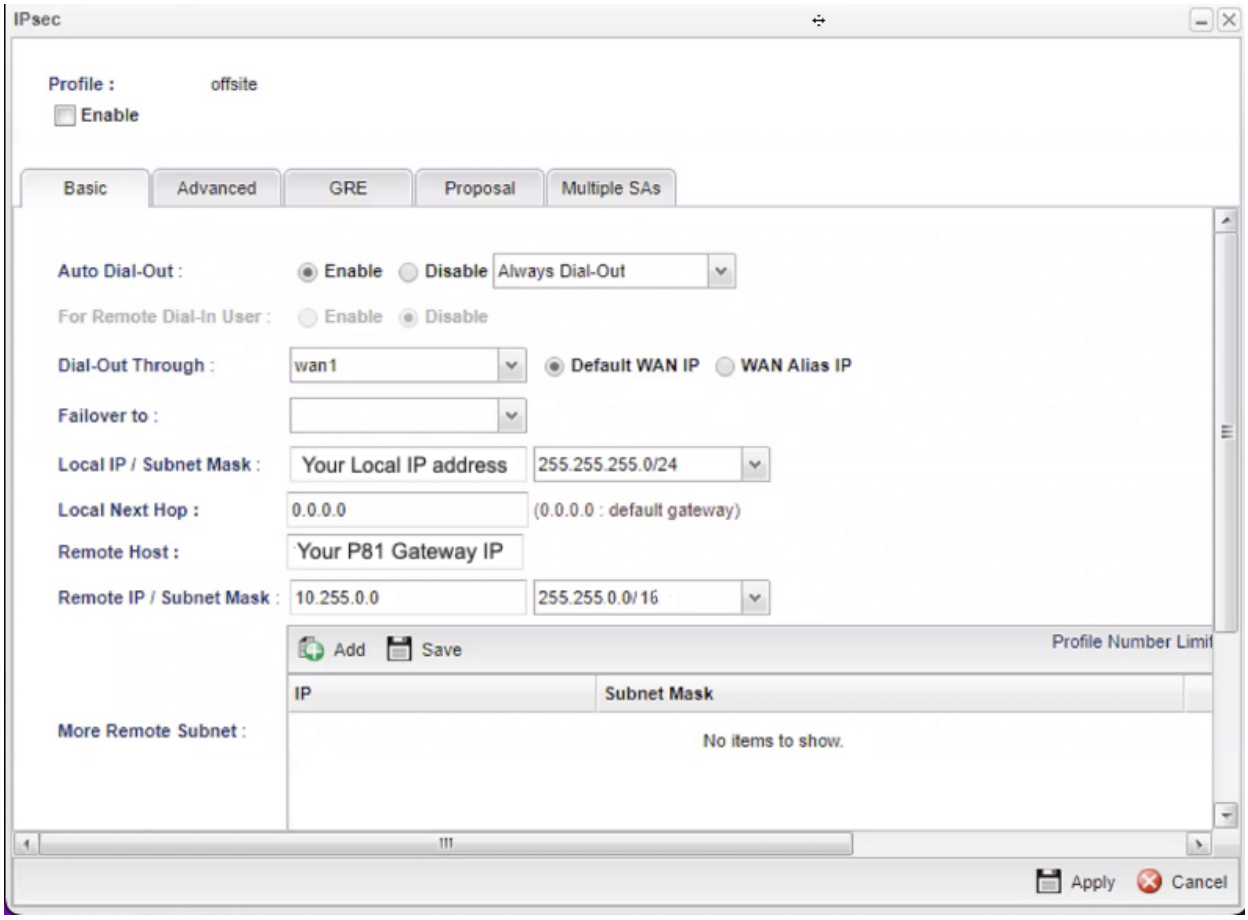
DrayTek Vigor3900 Router

To configure the tunnel in the DrayTek Vigor3900 Management Portal:

1. Log in to the DrayTek Vigor3900 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **VPN Profiles** and click **Add**.



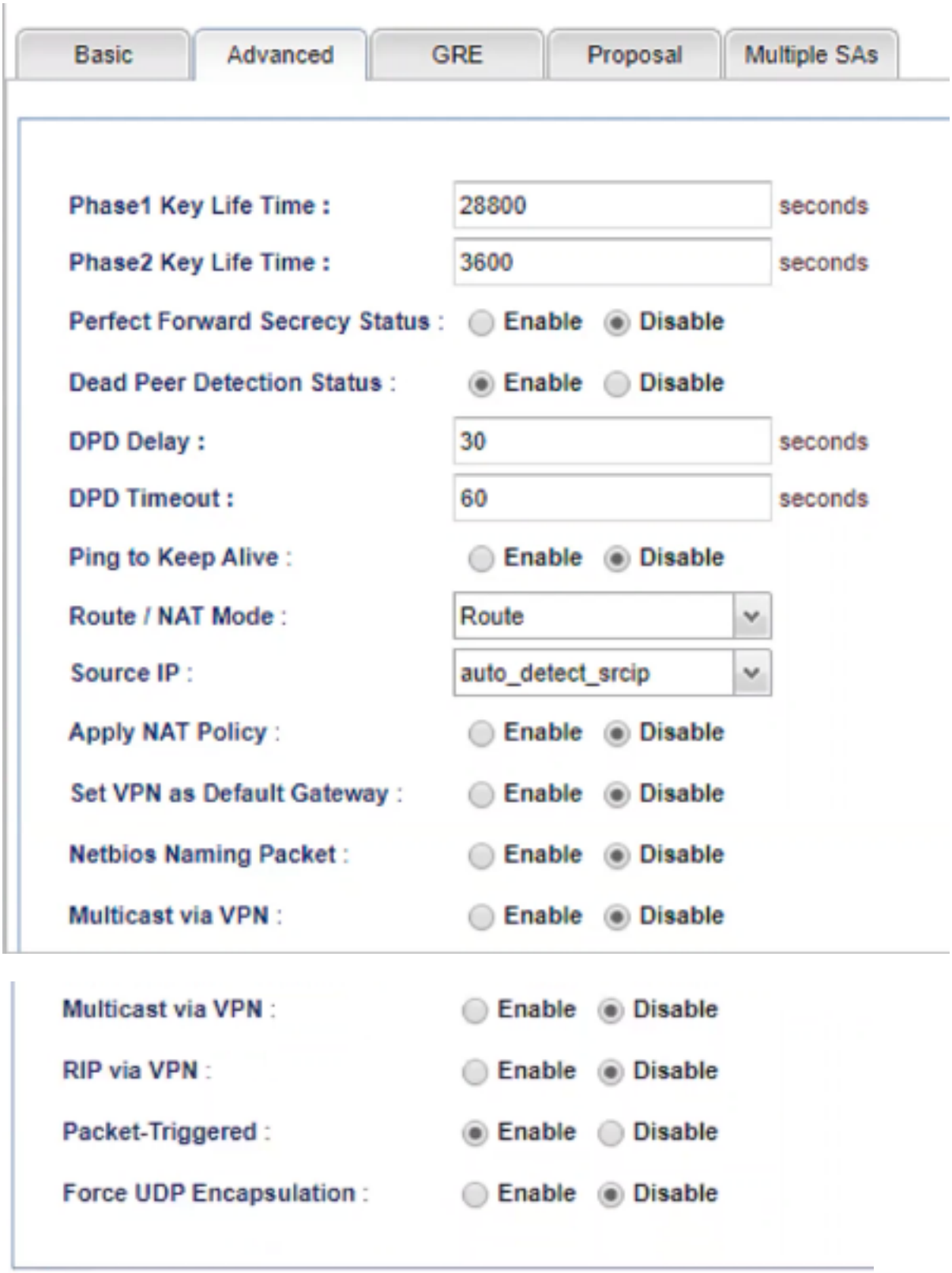
4. In the **Basic** tab:



Field	Enter
Auto Dial-Out	Enable; Always Dial-Out
Dial-Out Through	Your WAN interface; Default WAN IP
Failover	Blank
Local IP / Subnet Mask	Your router external IP address and subnets.
Remote Host	Public IP address of the Check Point SASE gateway.

Field	Enter
Remote IP / Subnet Mask	Default is 10.255.0.0 and 255.255.0.0/16. If you modified these in the Check Point SASE Administrator Portal, enter the modified values.
IKE Protocol	IKEv1
IKE Phase 1	Main Mode
Auth Type	PSK
Pre-shared Key	Secret key specified in the Check Point SASE Administrator Portal.
Security Protocol	ESP

5. In the **Advanced** tab:



Field	Enter
Phase 1 Key Lifetime	28800 seconds

Field	Enter
Phase 2 Key Lifetime	3600 seconds
Perfect Forward Secrecy Status	Enable
DPD Status	Enable
DPD Delay	30 seconds
DPD Timeout	60 seconds
Ping to Keep Alive	Disable
Route/NAT Mode	Route
Source IP	Auto-detect
Apply NAT Policy	Disable
Set VPN Default Gateway	Disable
Netbios Naming Packet	Disable
Multicast via VPN	Disable
RIP via Triggered	Enable
Packet Triggered	Enable
Force UDP Encapsulation	Disable

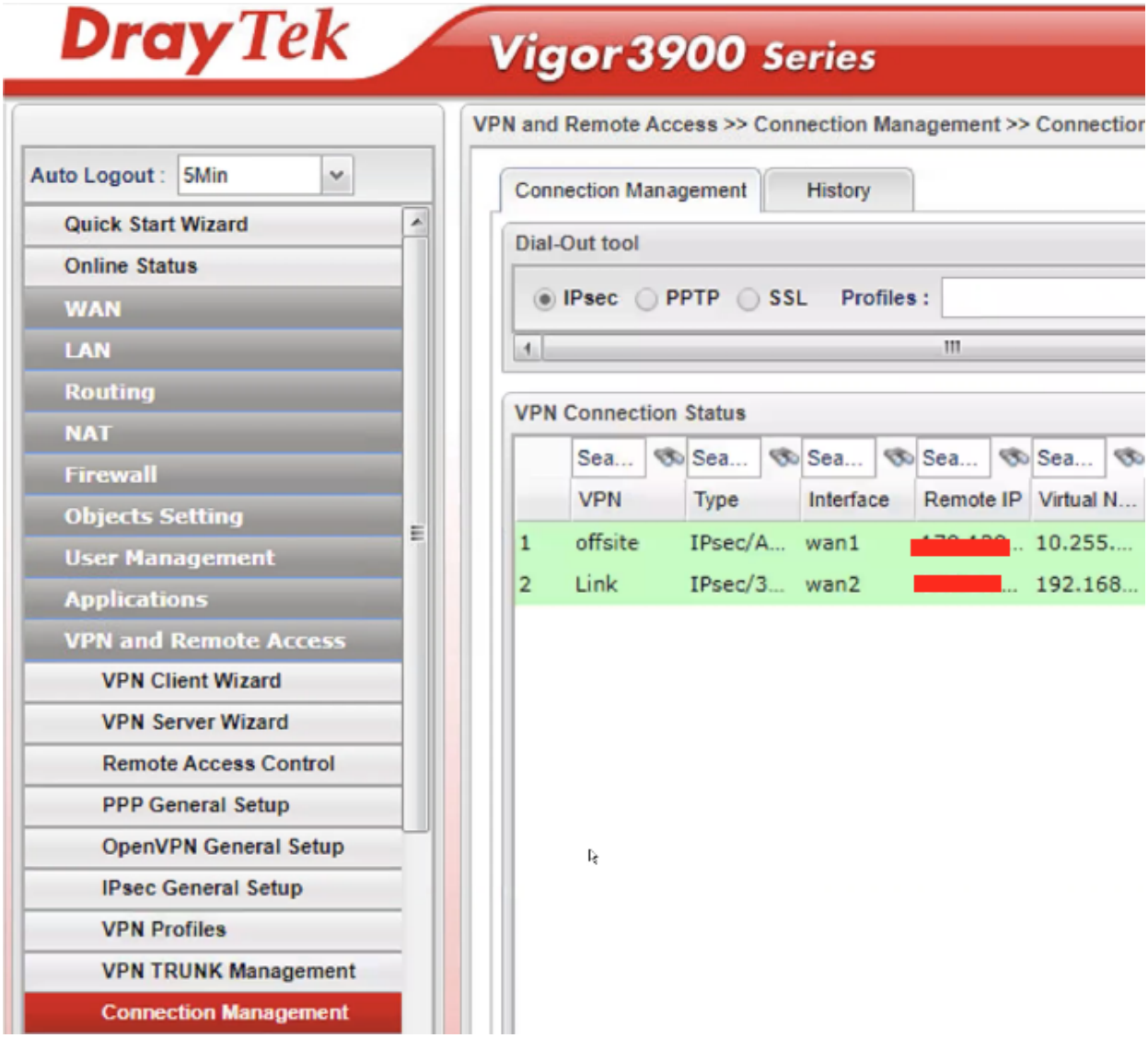
6. In the **GRE** tab:

Field	Enter
Enable GRE Function	Disable
Auto Generate GRE Key	Enable

7. In the **Proposal** tab:

Field	Enter
IKE Phase 1 Proposal	AES 256 G2
IKE Phase 1 Authentication	SHA1
IKE Phase 2 Proposal	AES 256 with auth
IKE Phase 2 Authentication	SHA1
Accepted Proposal	Accept

8. Click **Apply**.
9. To verify if the tunnel is up, from the left pane, click **Connection Management** and check if the profile is listed and highlighted in Green.



EdgeMax Router

To configure the tunnel in the EdgeMax Router through CLI:

1. Connect to the router through SSH and then enter the configuration mode. For example, using PuTTY.
2. Enable the **auto-firewall-nat-exclude** feature which automatically creates the IPsec firewall/NAT policies in the iptables firewall. Run:

```
set vpn ipsec auto-firewall-nat-exclude enable
```

3. Create IKE / Phase 1 (P1) Security Associations (SAs). Run:

```
set vpn ipsec ike-group FOO0 lifetime 28800
set vpn ipsec ike-group FOO0 proposal 1 dh-group 14
set vpn ipsec ike-group FOO0 proposal 1 encryption aes256
set vpn ipsec ike-group FOO0 proposal 1 hash sha1
set vpn ipsec ike-group FOO0 dead-peer-detection interval 15
set vpn ipsec ike-group FOO0 dead-peer-detection timeout 30
```

4. Create the ESP / Phase 2 (P2) SAs and enable Perfect Forward Secrecy (PFS). Run:

```
set vpn ipsec esp-group FOO0 lifetime 3600
set vpn ipsec esp-group FOO0 pfs enable
set vpn ipsec esp-group FOO0 proposal 1 encryption aes256
set vpn ipsec esp-group FOO0 proposal 1 hash sha1
```

5. Define the remote peering address. Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication mode pre-shared-secret
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication pre-shared-secret <secret key from Quantum SASE
Administrator Portal>
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
description ipsec
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
local-address <Your Edgerouter WAN IP>
```

6. Link the SAs created above to the remote peer and bind the VPN to a virtual tunnel interface (vti0). Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
ike-group FOO0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti bind vti0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti esp-group FOO0
```

7. Configure the virtual tunnel interface (vti0) and assign an internal IP address that is not used in any site. Run:

```
set interfaces vti vti0 address 192.168.20.20/32
```

8. Create a static route for the Check Point SASE subnet (the default is 10.255.0.0/16). Run:

```
set protocols static interface-route 10.255.0.0/16 next-hop-
interface vti0
```

9. Commit the changes and save the configuration. Run:

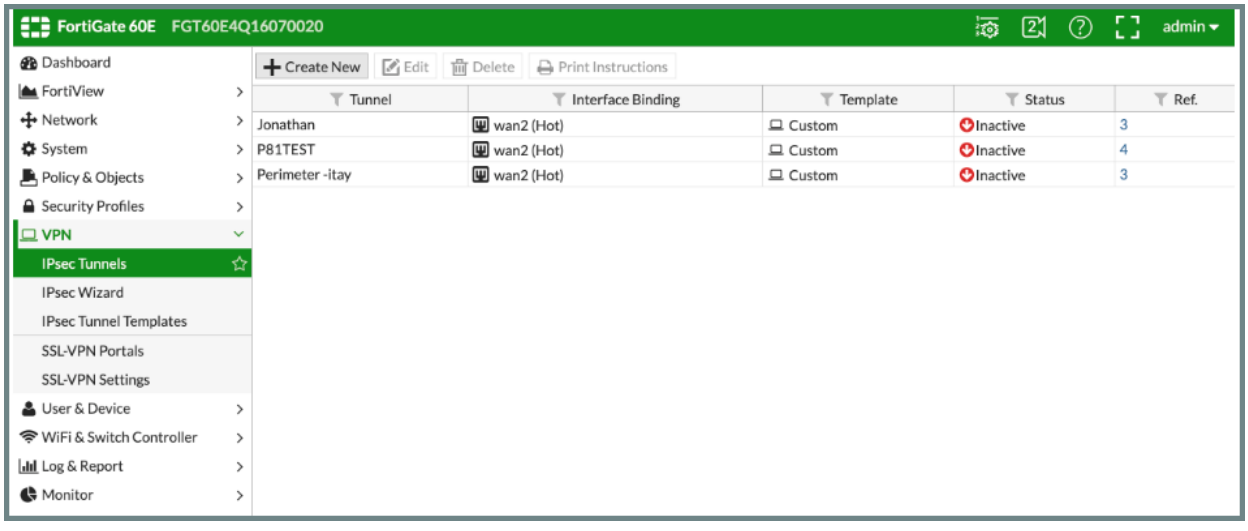
```
commit ; save
```

10. In the EdgeMax Management portal, go **VPN - site to site connection**.
11. Verify that the peer associated with the gateway IP address obtained from Check Point SASE has:
    - **Remote subnet**: 10.255.0.0/16 (or the local Check Point SASE gateway that you selected)
    - **Local subnet**: All the subnet range (CIDR) of your LAN devices

FortiGate Next Generation Firewall

To configure the tunnel in the FortiGate Next Generation Firewall Management Portal:

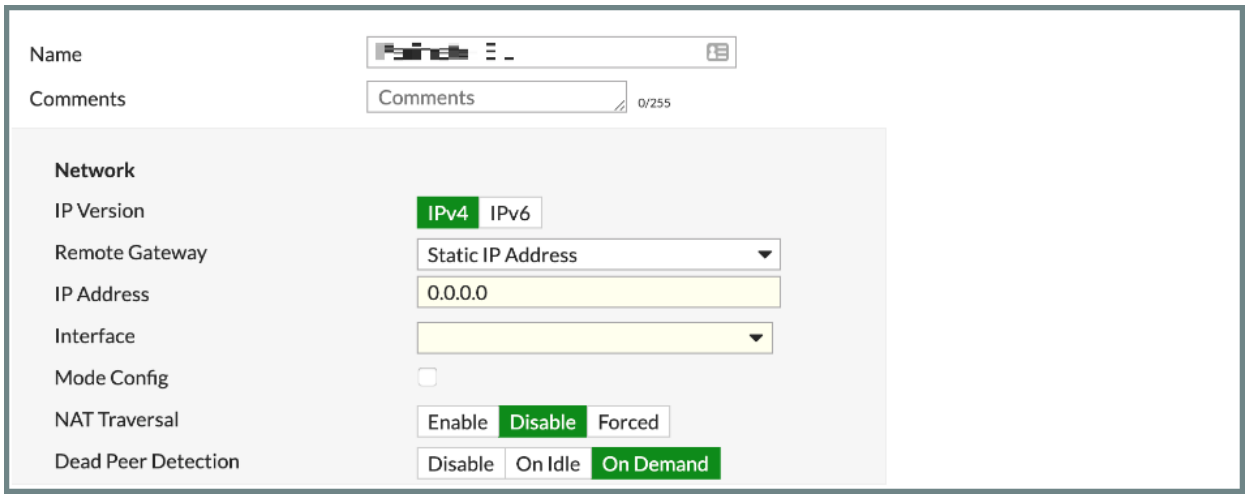
1. Log in to the FortiGate Next Generation Firewall Management Portal.
2. Go to **VPN > IPSec Tunnels**.



3. Click **Create New**.

   The **VPN Creation Wizard** window appears.

4. In the **Name** field, enter a name for the tunnel.
5. Set **Template Type** to **Custom**.
6. Click **Next**.



7. In the **Network** section:

Field	Enter
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	Public IP address of the location server.
Interface	Your WAN interface.
Mode Config	Clear
NAT Traversal	Disable
Dead Peer Detection	On-Demand

Important - For Enhanced Networks (CV4), set NAT Traversal to Enable. The tunnel does not connect when NAT Traversal is disabled.

Note - For Standard Networks (CV3), enable NAT Traversal only when the device sits behind NAT.

8. In the **Authentication** section:

Field	Enter
Method	Pre-shared key

Field	Enter
Pre-shared Key	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.
IKE Version	2
Mode	Main (ID Protection).

9. In the **Phase 1 Proposal** section:

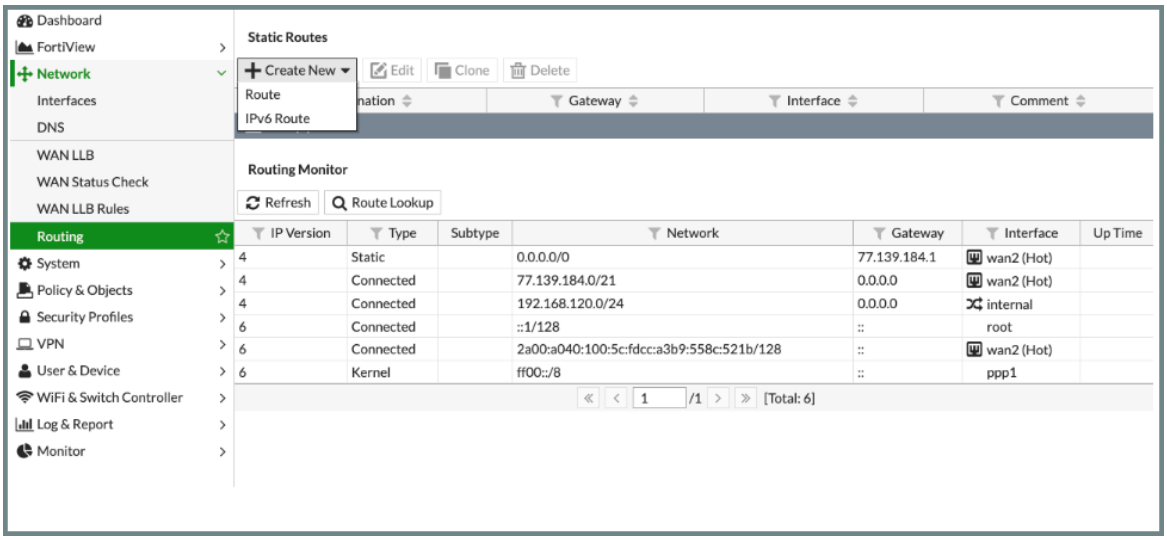
Field	Enter
Encryption	AES256
Authentication	SHA256
Diffie-Hellman Group	21
Key Lifetime (seconds)	28800
Local ID	Blank
XAUTH	Blank

10. In the **Phase 2 Selectors (+Advanced)** section:

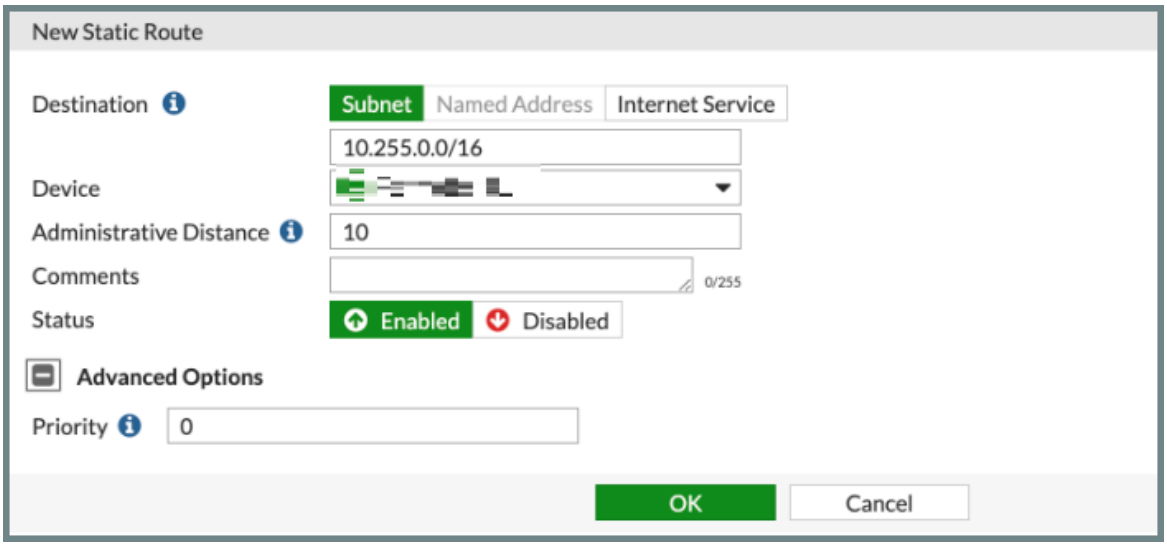
Field	Enter
Name	Check Point SASE
Local Address	Your local network subnet
Remote Address	Check Point SASE network subnet (10.255.0.0/255.255.0.0)
Enable Replay Detection	Unselect
Enable Perfect Forward Secrecy (PFS)	Select
Diffie-Gellman Group	21
Encryption	AES256

Field	Enter
Authentication	SHA256
Local Port	Select
remote Port	Select
Protocol	Select
Key Lifetime	Seconds
Seconds	3600

11. Add static routes from the Check Point SASE subnet (10.256.0.0/16) to the local network and vice versa through the VPN tunnel gateway:
    a. Click **Network > Routing**.
    b. Click **Create new** and select **Route**.
    c. In the **Destination** field, enter 10.255.0.0/16.
    d. From the **Device** list, select **Check Point SASE**.
    e. Click **OK**.
12. Add firewall rules to allow traffic from the Check Point SASE subnet (10.255.0.0/16) to your local network or services:
    a. Go to **Policy & Objects > IPv4 Policy**.



b. Click **Create New** and enter these:



Field	Enter
Name	Check Point SASE
Incoming Interface	Check Point SASE
Outgoing Interface	Your local network object.
Source	All
Destination	All
Schedule	Always
Service	All
NAT	Disabled

Leave the rest of the fields to default settings.

c. Click **OK**.

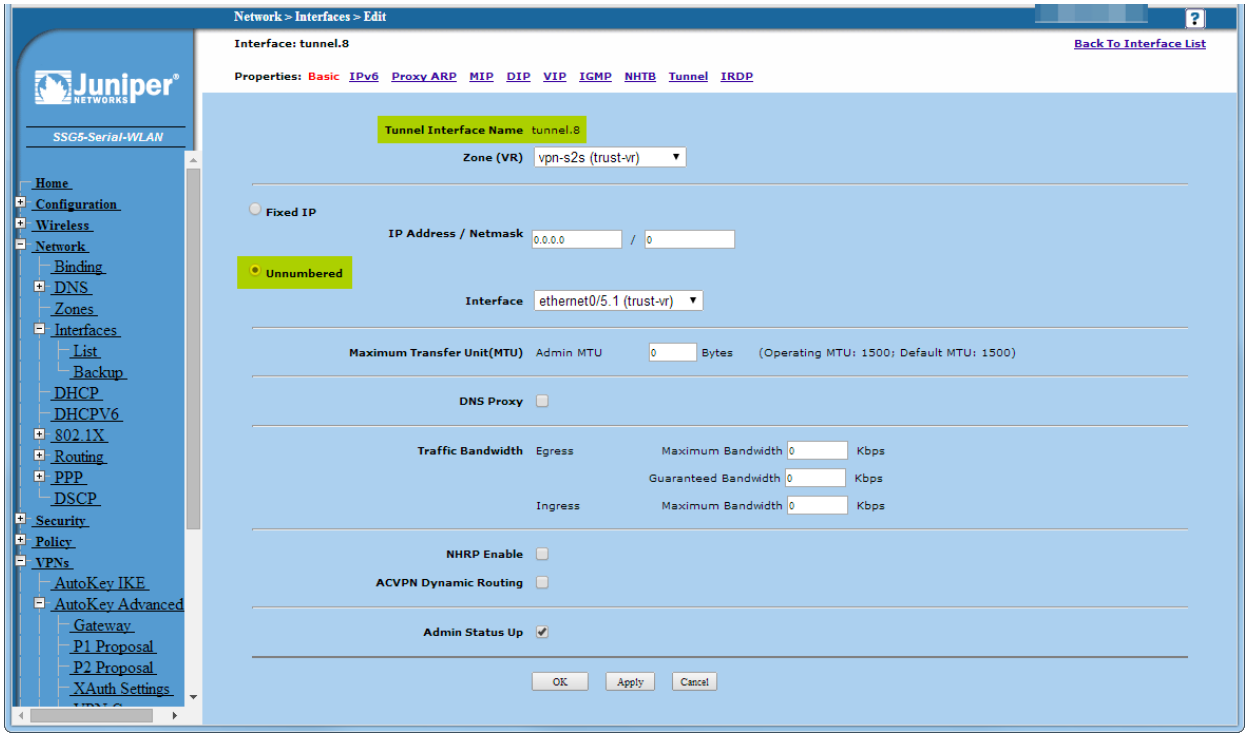
13. To verify that the tunnel is up, go to **VPN > IPSec Tunnels**. If the tunnel is listed in the table, then the tunnel is up.

Juniper Networks ScreenOS Firewall

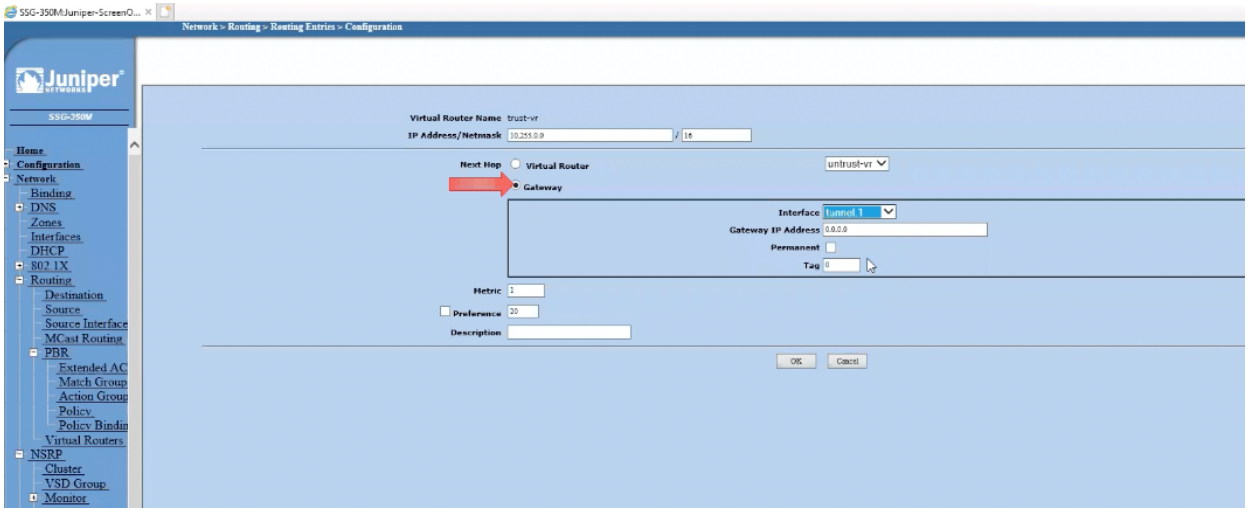
To configure the tunnel in the Juniper Networks ScreenOS Management Portal:

1. Log in to the Juniper Networks ScreenOS Management Portal with the Administrator account.

2. From the left pane. go to **Network > Interfaces**.
3. Create a new **Unnumbered** tunnel interface.



4. From the left pane, go to **Network > Routing > Source**:

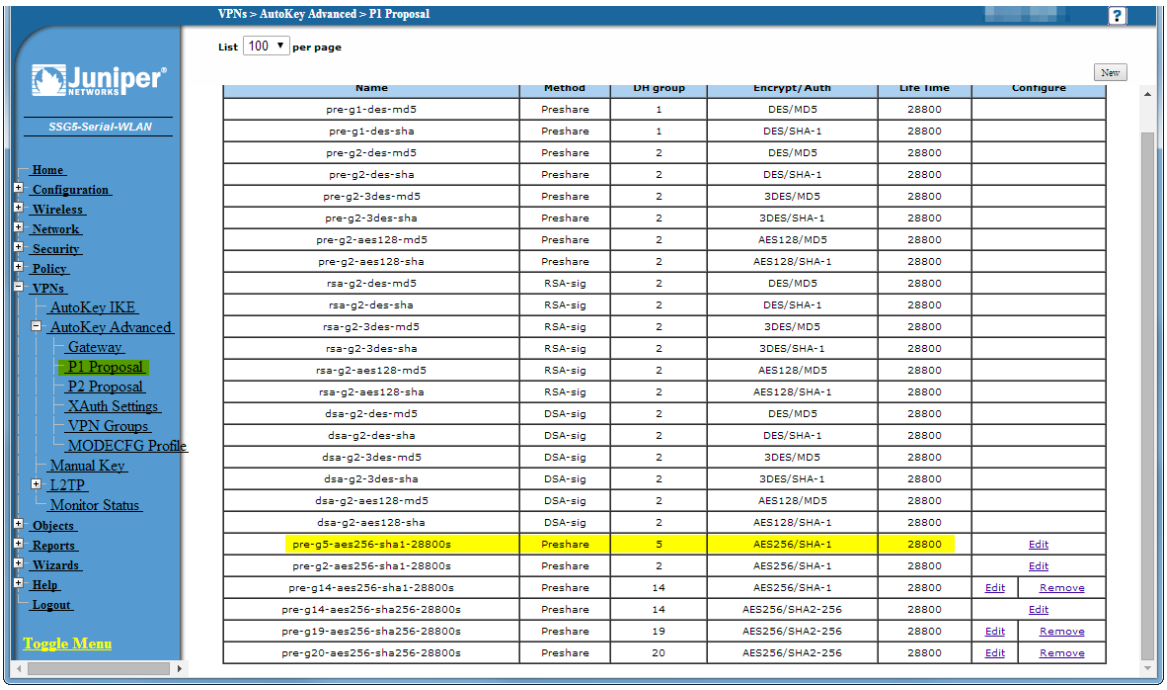


   a. Select an appropriate zone and click **New**.
   b. In the **IP Address/Netmask** field, enter the Check Point SASE network subnet.
   c. For **Next Hop**, select **gateway**.
   d. Click **OK**.

5. From the left pane, click **VPN**:

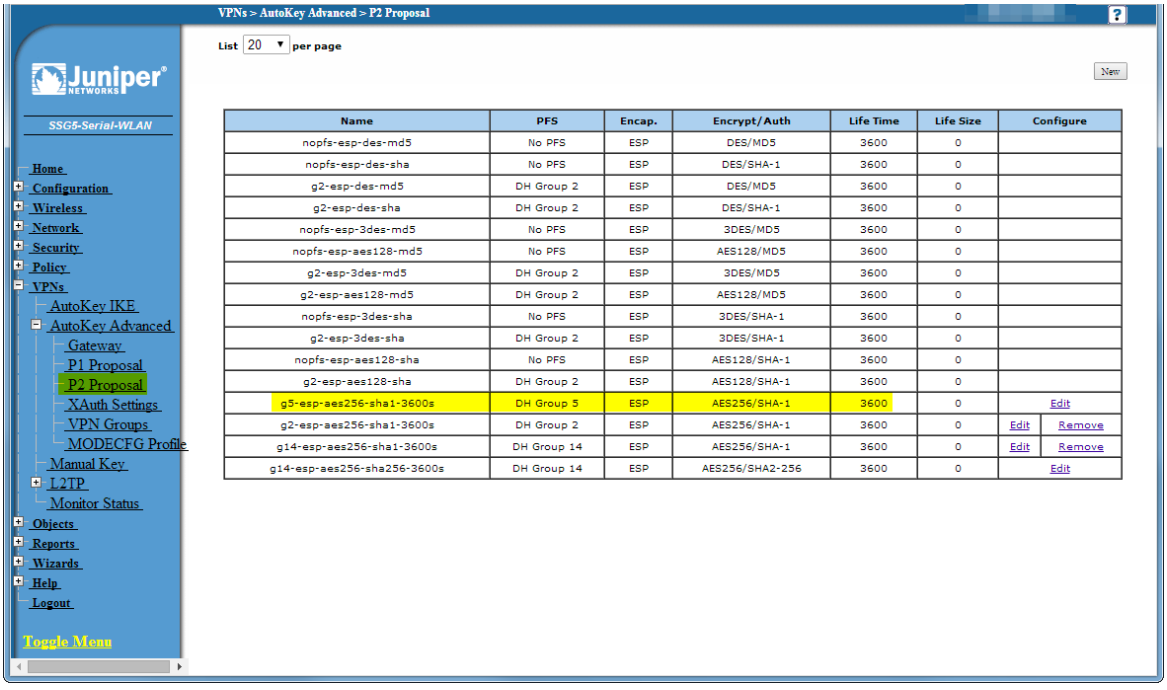
a. Select **AutoKey Advanced**.

b. Verify that the **P1 Proposal** is listed as shown in the following graphic.



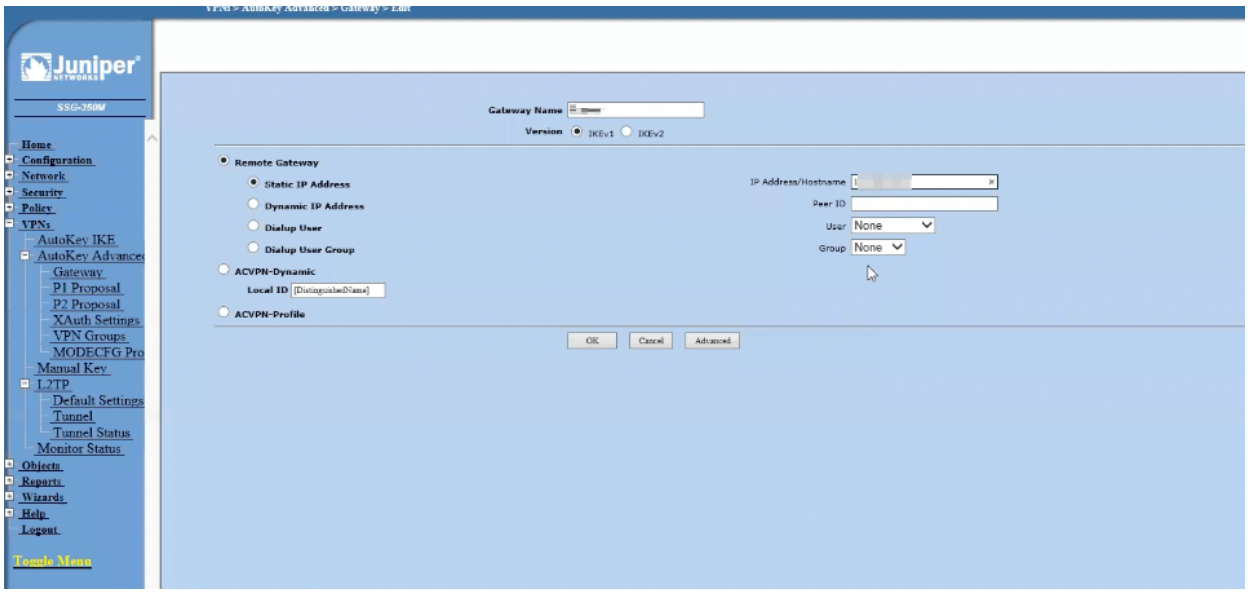
Name	Method	DH group	Encrypt/Auth	Life Time	Configure
pre-g1-des-md5	Preshare	1	DES/MD5	28800	
pre-g1-des-sha	Preshare	1	DES/SHA-1	28800	
pre-g2-des-md5	Preshare	2	DES/MD5	28800	
pre-g2-des-sha	Preshare	2	DES/SHA-1	28800	
pre-g2-3des-md5	Preshare	2	3DES/MD5	28800	
pre-g2-3des-sha	Preshare	2	3DES/SHA-1	28800	
pre-g2-aes128-md5	Preshare	2	AES128/MD5	28800	
pre-g2-aes128-sha	Preshare	2	AES128/SHA-1	28800	
rsa-g2-des-md5	RSA-sig	2	DES/MD5	28800	
rsa-g2-des-sha	RSA-sig	2	DES/SHA-1	28800	
rsa-g2-3des-md5	RSA-sig	2	3DES/MD5	28800	
rsa-g2-3des-sha	RSA-sig	2	3DES/SHA-1	28800	
rsa-g2-aes128-md5	RSA-sig	2	AES128/MD5	28800	
rsa-g2-aes128-sha	RSA-sig	2	AES128/SHA-1	28800	
dsa-g2-des-md5	DSA-sig	2	DES/MD5	28800	
dsa-g2-des-sha	DSA-sig	2	DES/SHA-1	28800	
dsa-g2-3des-md5	DSA-sig	2	3DES/MD5	28800	
dsa-g2-3des-sha	DSA-sig	2	3DES/SHA-1	28800	
dsa-g2-aes128-md5	DSA-sig	2	AES128/MD5	28800	
dsa-g2-aes128-sha	DSA-sig	2	AES128/SHA-1	28800	
pre-g5-aes256-sha1-28800s	Preshare	5	AES256/SHA-1	28800	Edit
pre-g2-aes256-sha1-28800s	Preshare	2	AES256/SHA-1	28800	Edit
pre-g14-aes256-sha1-28800s	Preshare	14	AES256/SHA-1	28800	Edit Remove
pre-g14-aes256-sha256-28800s	Preshare	14	AES256/SHA2-256	28800	Edit
pre-g19-aes256-sha256-28800s	Preshare	19	AES256/SHA2-256	28800	Edit Remove
pre-g20-aes256-sha256-28800s	Preshare	20	AES256/SHA2-256	28800	Edit Remove

c. Go to **P2 Proposal** and ensure the proposal is listed as shown in the following graphic.



Name	PFS	Encap.	Encrypt/Auth	Life Time	Life Size	Configure
nopfs-esp-des-md5	No PFS	ESP	DES/MD5	3600	0	
nopfs-esp-des-sha	No PFS	ESP	DES/SHA-1	3600	0	
g2-esp-des-md5	DH Group 2	ESP	DES/MD5	3600	0	
g2-esp-des-sha	DH Group 2	ESP	DES/SHA-1	3600	0	
nopfs-esp-3des-md5	No PFS	ESP	3DES/MD5	3600	0	
nopfs-esp-aes128-md5	No PFS	ESP	AES128/MD5	3600	0	
g2-esp-3des-md5	DH Group 2	ESP	3DES/MD5	3600	0	
g2-esp-aes128-md5	DH Group 2	ESP	AES128/MD5	3600	0	
nopfs-esp-3des-sha	No PFS	ESP	3DES/SHA-1	3600	0	
g2-esp-3des-sha	DH Group 2	ESP	3DES/SHA-1	3600	0	
nopfs-esp-aes128-sha	No PFS	ESP	AES128/SHA-1	3600	0	
g2-esp-aes128-sha	DH Group 2	ESP	AES128/SHA-1	3600	0	
g5-esp-aes256-sha1-3600s	DH Group 5	ESP	AES256/SHA-1	3600	0	Edit
g2-esp-aes256-sha1-3600s	DH Group 2	ESP	AES256/SHA-1	3600	0	Edit Remove
g14-esp-aes256-sha1-3600s	DH Group 14	ESP	AES256/SHA-1	3600	0	Edit Remove
g14-esp-aes256-sha256-3600s	DH Group 14	ESP	AES256/SHA2-256	3600	0	Edit

6. From the left pane, click **Gateway**:

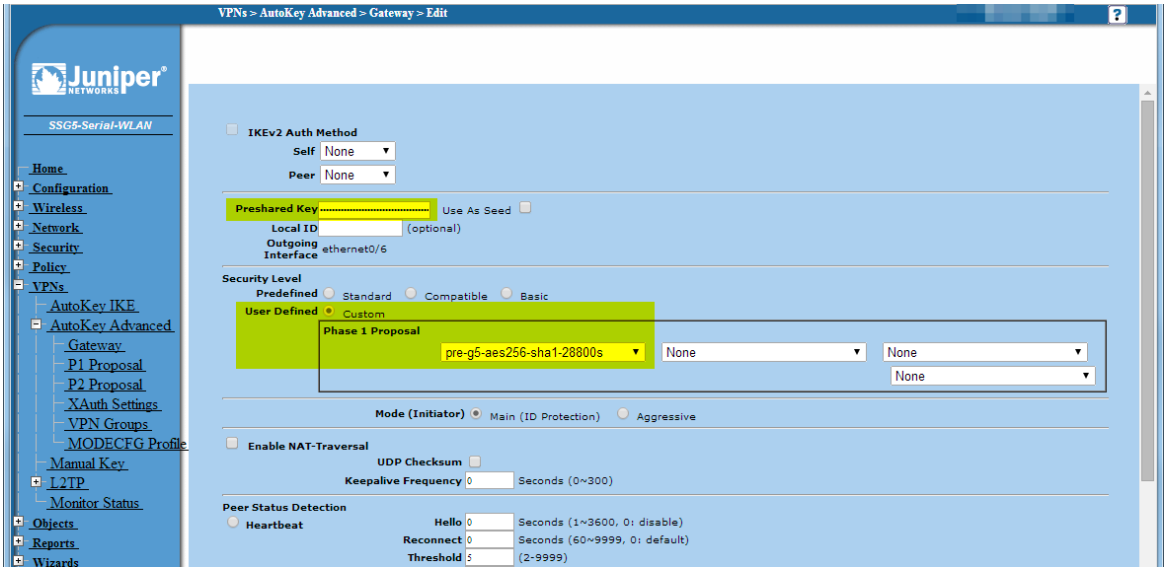


a. In the **Gateway Name** field, enter a name for the gateway.

b. Select **Remote Gateway** and then select **Static IP Address**.

c. In the **IP Address/Hostname** field, enter the public IP address of Check Point SASE gateway.

d. Click **Advanced**:

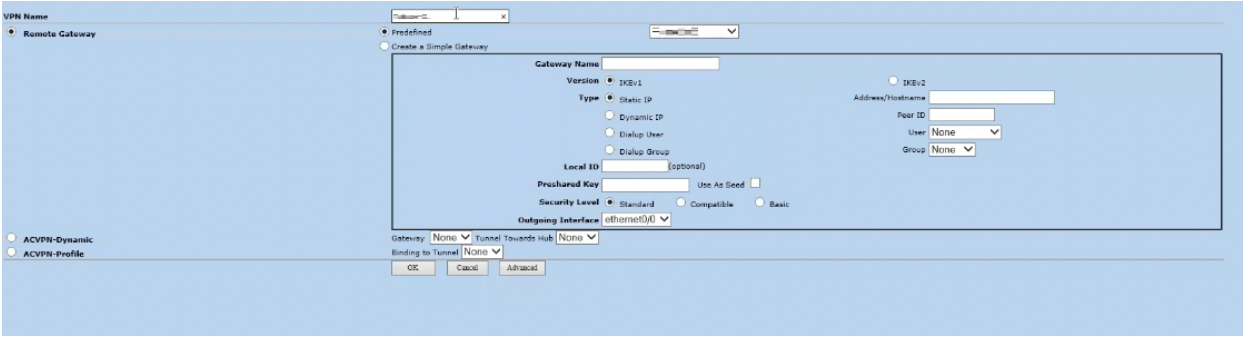


i. In the **Preshared Key** field, enter the secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.

ii. In the **Security Level** section, select **Custom** and from the **Phase 1 Proposal** list, select **pre-g5-aes256-sha1-28800s**.

iii. Enable **DPD** and set **DPD Interval** to **10s** and **DPD Retry** to **5s**.

7. From the left pane, click **VPN > Autokey IKE**:

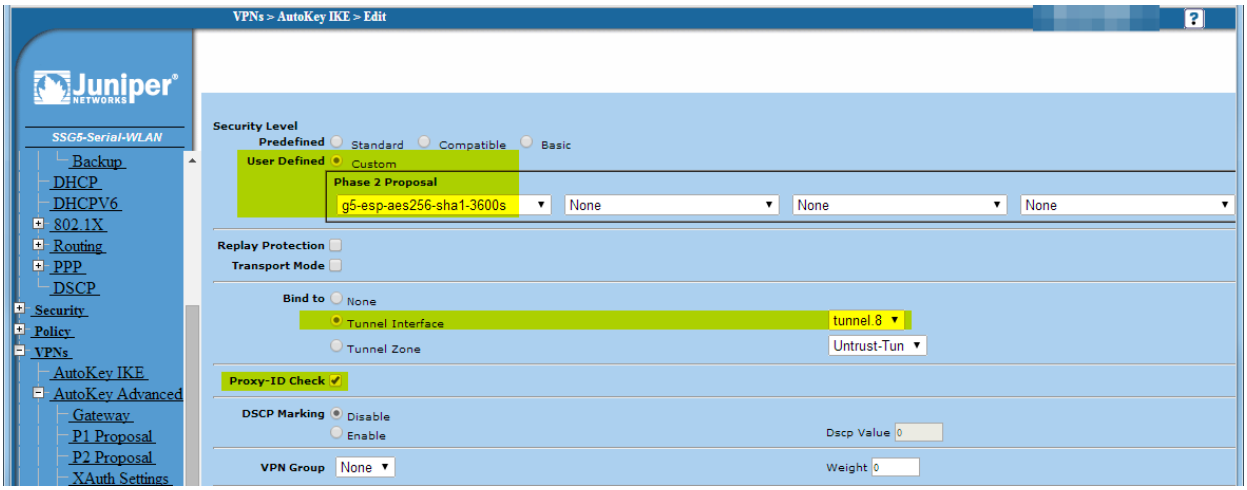


a. In the **VPN Name** field, enter a name for the VPN. For example, Check Point SASE.

b. Select **Remote Gateway** and then select **Predefined**.

c. Select the AutoKey Advanced Gateway that you created in the previous step.

8. From the left pane, click **VPN > Advanced**:

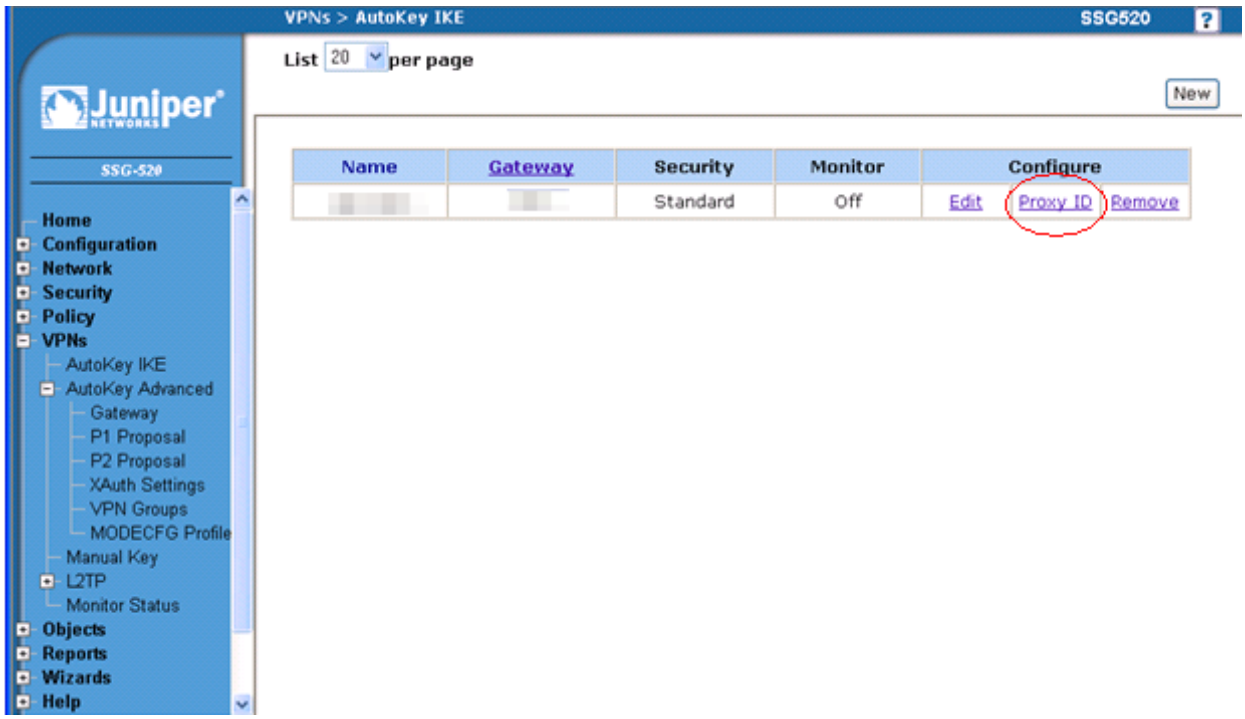


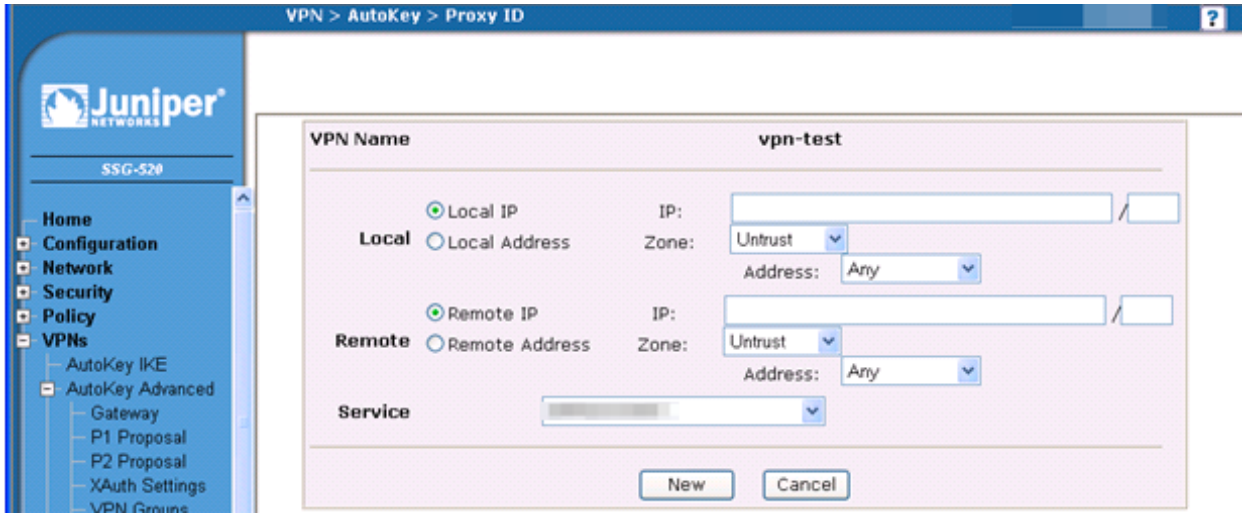
a. In the **Security Level** section, select **Custom** and from the **Phase 2 Proposal** list, select **g5-aes256-sha1-3600s**.

b. In the **Bind to** section, click **Tunnel Interface** and select the tunnel interface you created in step 3.

c. Select the **Proxy-ID Check** checkbox.

9. From the left pane, click **VPN > Autokey IKE**, configure **Proxy ID** with these details:





Field	Enter
Local proxy ID	Your local LAN subnet. For example, 192.168.120.0/24.
Remote Proxy ID	Check Point SASE network subnet. The default is 10.255.0.0./16.
Service	Any

Juniper (JunOS) SRX Firewall

To configure the tunnel with Juniper SRX firewall through CLI:

Note - To configure the tunnel in the Juniper SRX Management Portal, see Juniper VPN configuration generator.

1. Connect to the firewall through SSH. For example, using PuTTY.
2. Create a tunnel interface. Run:

   Note - Do not assign an IP address but make sure it's enabled for layer 3 communication.

   ```
   set interfaces st0 unit 0 family inet
   ```

3. Set up the IKE Proposal. Run:

   ```
   set security ike proposal QS description Perimeter81-SRXTunnel

   set security ike proposal QS authentication-method pre-shared-
   keys

   set security ike proposal QS dh-group group14

   set security ike proposal QS authentication-algorithm sha-256

   set security ike proposal QS encryption-algorithm aes-256-cbc

   set security ike proposal QS lifetime-seconds 28800
   ```

4. Set up the IKE policy configuration. Run:

   ```
   set security ike policy QS-policy proposals p81

   set security ike policy QS-policy pre-shared-key ascii-text
   <Secret_key_from_Quantum SASE Administrator Portal>
   ```

5. Set up the IKE gateway configuration. Run:

   ```
   set security ike gateway QS-ike-gateway ike-policy QS-policy
   ```

```
set security ike gateway QS-ike-gateway address <Public IP
address of Quantum SASE gatewy>

set security ike gateway QS-ike-gateway local-identity inet
<Locak IP address of the firewall>

set security ike gateway QS-ike-gateway external-interface ge-
0/0/0

set security ike gateway QS-ike-gateway version v1-only
```

6. Set up the IPSec proposal. Run:

```
set security ipsec proposal QS-proposal description Perimeter81

set security ipsec proposal QS-proposal protocol esp

set security ipsec proposal QS-proposal authentication-algorithm
hmac-sha-256-128

set security ipsec proposal QS-proposal encryption-algorithm aes-
256-cbc

set security ipsec proposal QS-proposal lifetime-seconds 3600
```

7. Set up the IPSec policy configuration. Run:

```
set security ipsec policy ipsec-QS-policy perfect-forward-secrecy
keys group14

set security ipsec policy ipsec-QS-policy proposals QS-proposal
```

8. Bind your tunnel interface and apply the configuration. Run:

```
set security ipsec vpn QS-ipsec bind-interface st0.0

set security ipsec vpn QS-ipsec ike gateway p81-ike-gateway

set security ipsec vpn QS-ipsec ike ipsec-policy ipsec-p81-policy
```

```
set security ipsec vpn QS-ipsec establish-tunnels on-traffic
immediately

set security address-book global address QS_internal
10.255.0.0/16
```

Note - To establish the tunnel only upon active traffic or set the firewall to the only to respond when the traffic is initiated from Check Point SASE (never initiate a tunnel), set firewall to the **Responder-Only** mode.

9. Set firewall security policies. Run:

   Note - If the tunnel interface is in a trusted zone or a zone that allows all the traffic, then skip this step. Otherwise, modify the parameters in the following commands according to your network topology.
   In the following example, all the traffic from **icmp** and **ssh** from zone **vpn** with a source address of 10.255.0.0/16 to any address in zone **trust** is allowed.

```
set security policies from-zone vpn to-zone trust policy vpn-
internal match source-address QS_internal

set security policies from-zone vpn to-zone trust policy vpn-
internal match destination-address any

set security policies from-zone vpn to-zone trust policy vpn-
internal match application junos-icmp-all

set security policies from-zone vpn to-zone trust policy vpn-
internal match application junos-ssh

set security policies from-zone vpn to-zone trust policy vpn-
internal then permit
```

10. Set host inbound services. Allow services to the firewall interfaces and your public facing interface. Run:

```
set security zones security-zone vpn interfaces st0.0 host-
inbound-traffic system-services ike

set security zones security-zone untrust interfaces ge-0/0/0.0
host-inbound-traffic system-services ike
```

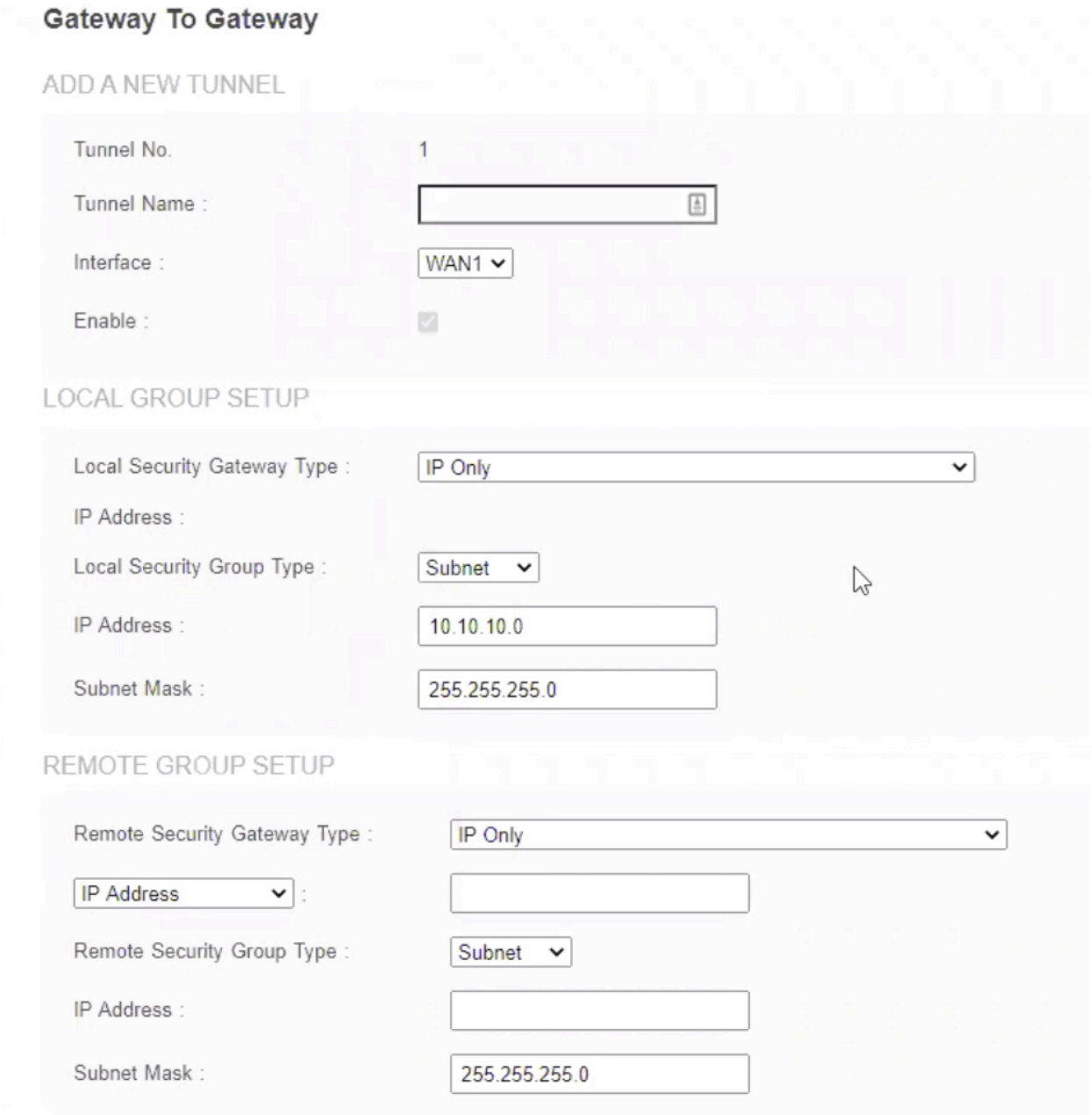
11. Define a static route to Check Point SASE network. Run:

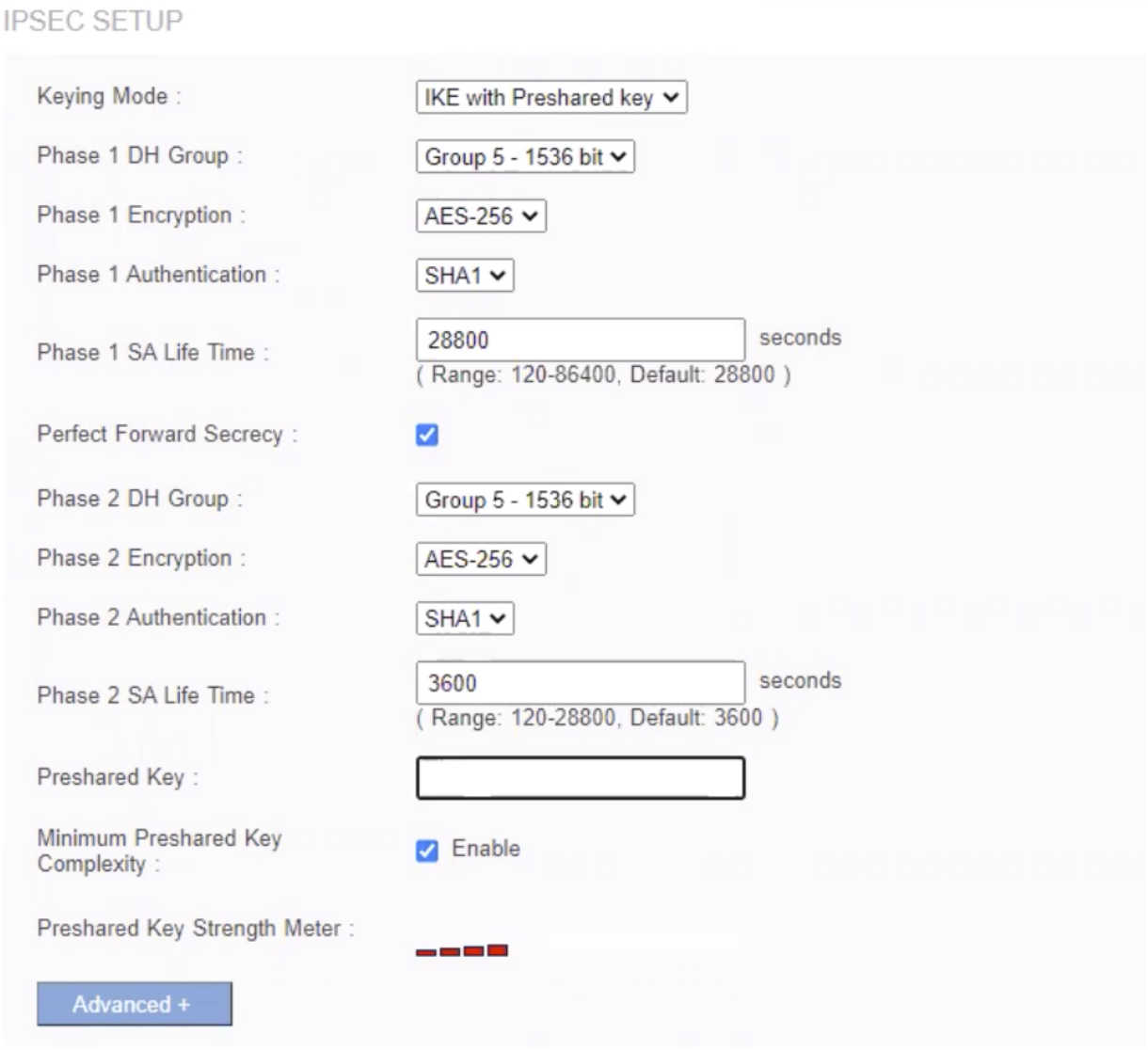
```
set routing-options static route 10.255.0.0/16 next-hop st0.0
```

Linksys Router

To configure the tunnel in the Linksys Management Portal:

1. Log in to the Linksys Management Portal with the Administrator account.
2. From the left panel, go to **VPN > Gateway to Gateway**.



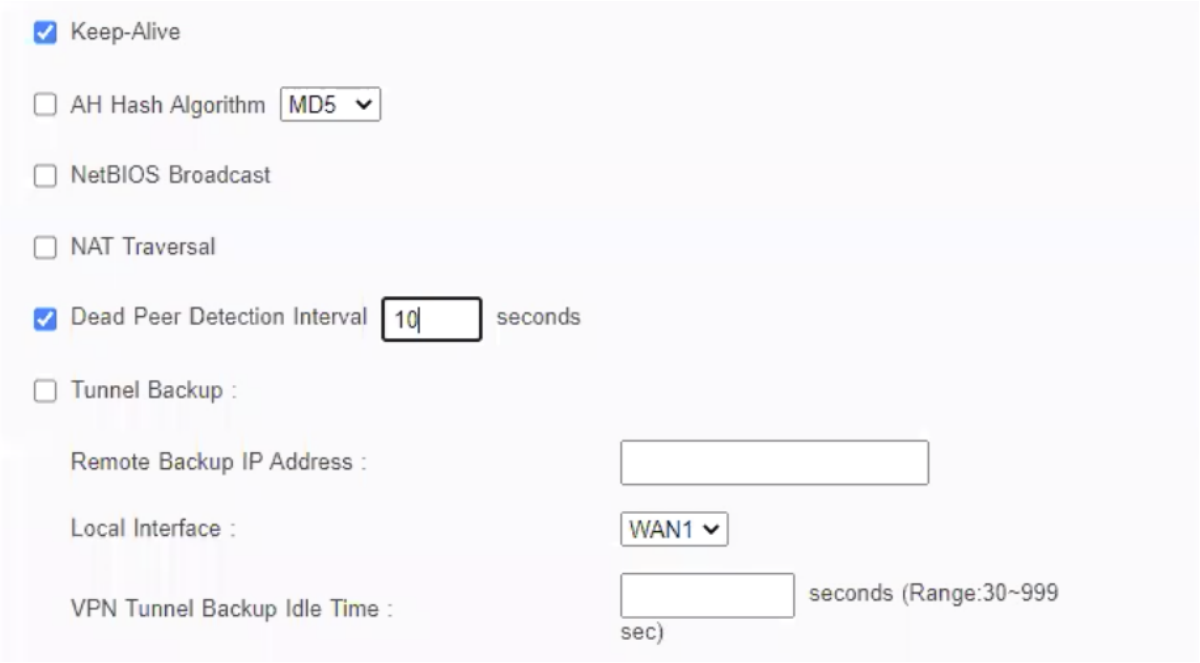


3. Enter these:

Field	Enter
Add a New Tunnel	
Tunnel Name	Name for the tunnel.
Interface	WAN1
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	Linksys external IP address.

Field	Enter
Local Security Group Type	Subnet
IP Address	Linksys local IP address.
Subnet Mask	Linksys subnet mask.
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	Public IP address of Check Point SASE gateway.
Remote Security group Type	Subnet
IP Address	10.255.0.0
Subnet Mask	255.255.0.0
IPSec Setup	
Keying Mode	IKE with PSK
Phase 1 DHG	Group 5
Phase 1 Encryption	aes256
Phase 1 Authentication	sha1
Phase 1 SA Lifetime	28800
Perfect Forward Secrecy	Selected
Phase 2 DHG	Group 5
Phase 1 Encryption	aes256
Phase 2 Authentication	sha1
Phase 2 SA Lifetime	3600
Preshared Key	Secret key specified in the Check Point SASE Administrator Portal.

4. Click **Advanced**:



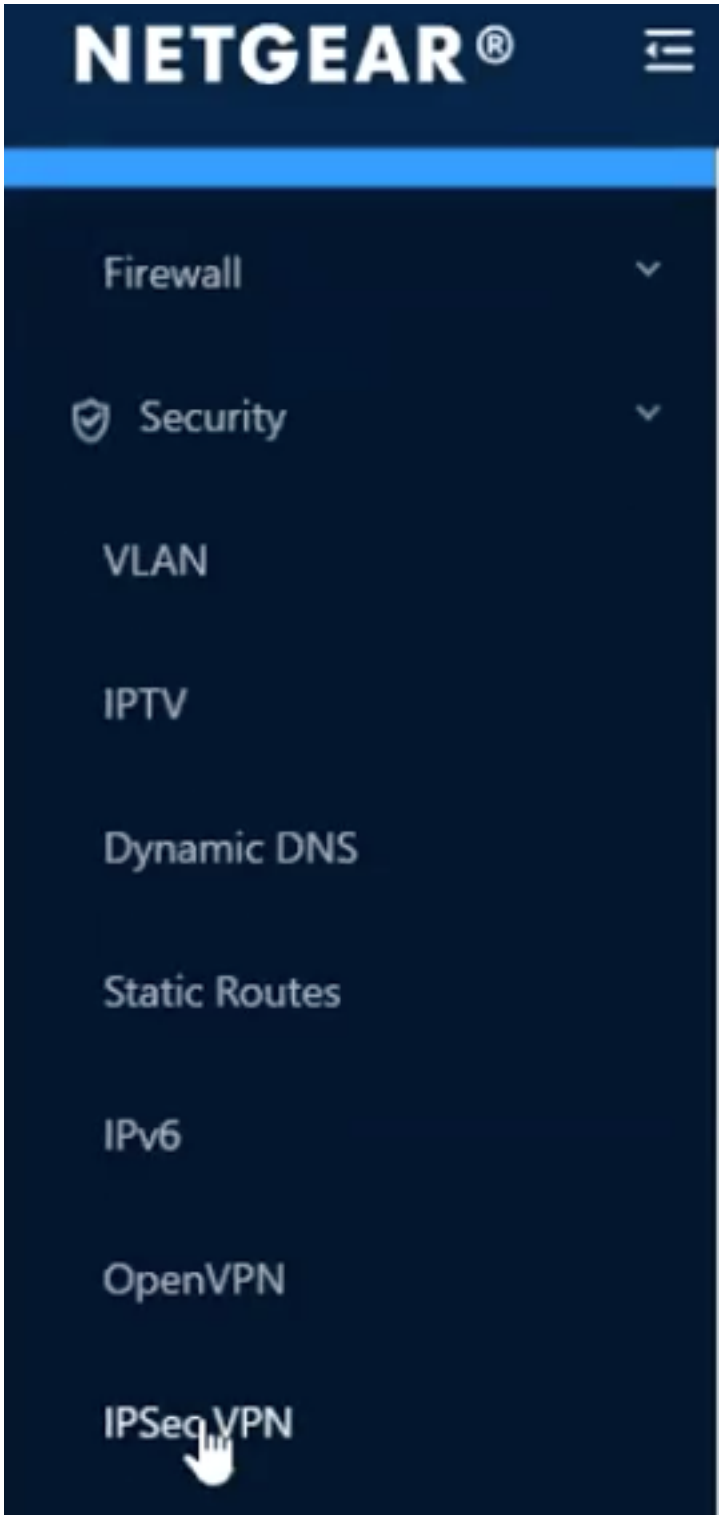
a. Select the **Keep-Alive** checkbox.

b. Select the **Dead Peer Detection Interval** checkbox and enter **10** seconds.

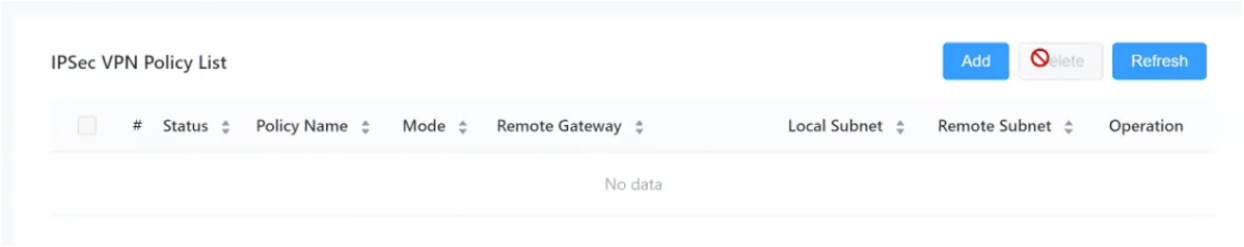
Netgear BR500 Router

To configure the tunnel in the Netgear BR500 Management Portal:

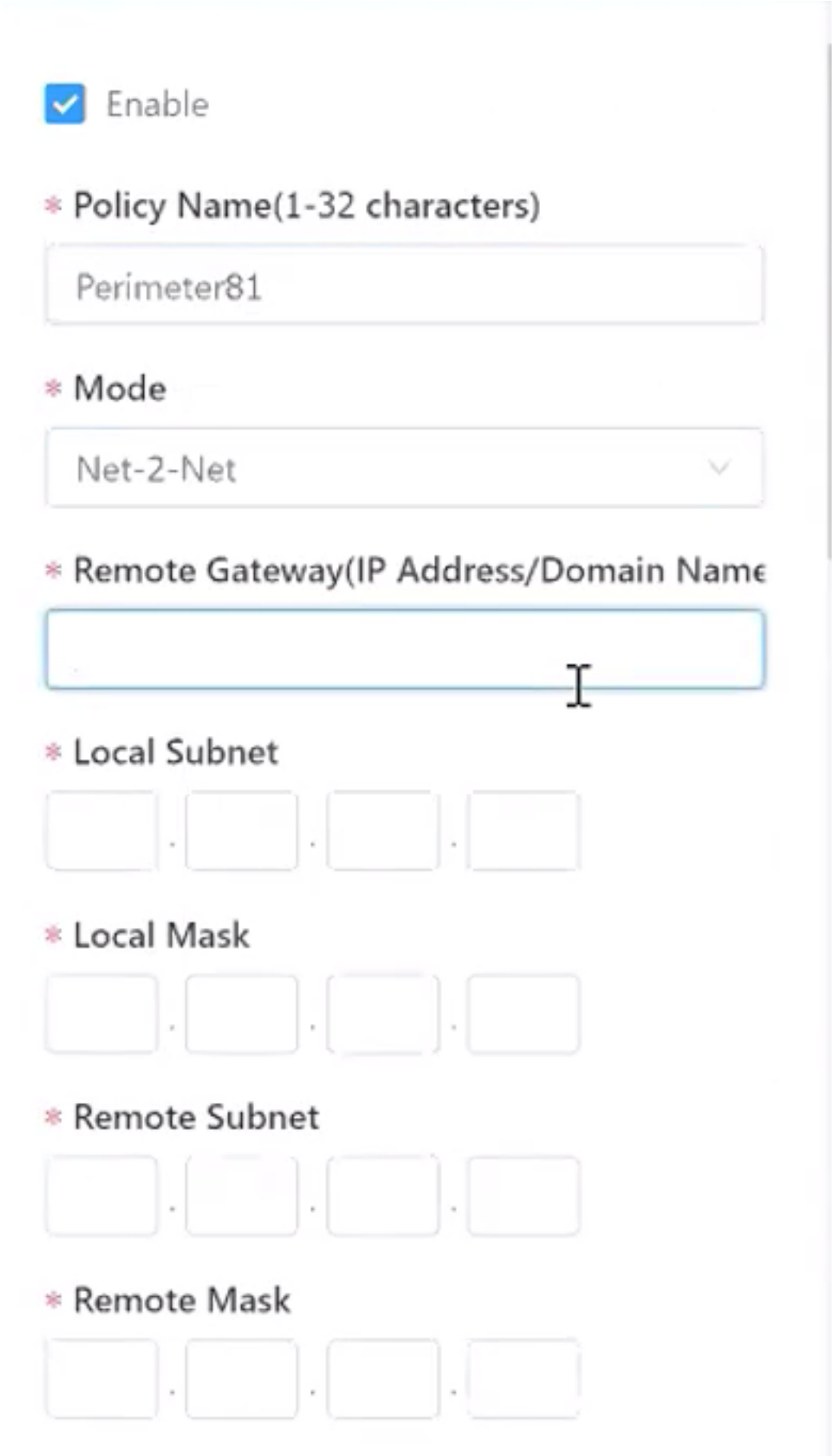
1. Log in to the Netgear BR500 Management Portal with the Administrator account.
2. From the left panel, go to **Security > IPSec VPN**.

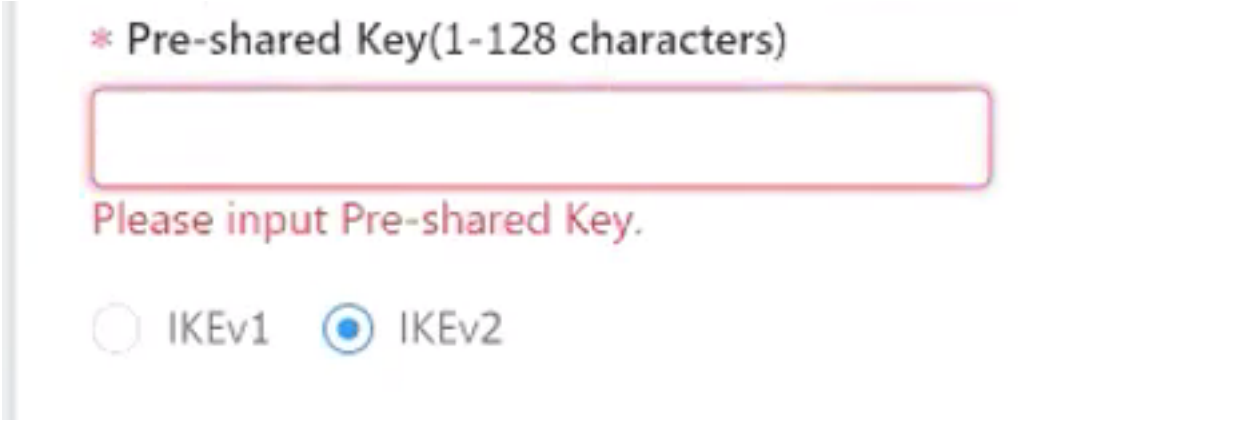

NETGEAR®
Firewall
Security
VLAN
IPTV
Dynamic DNS
Static Routes
IPv6
OpenVPN
IPSec VPN

3. Click **Add**.



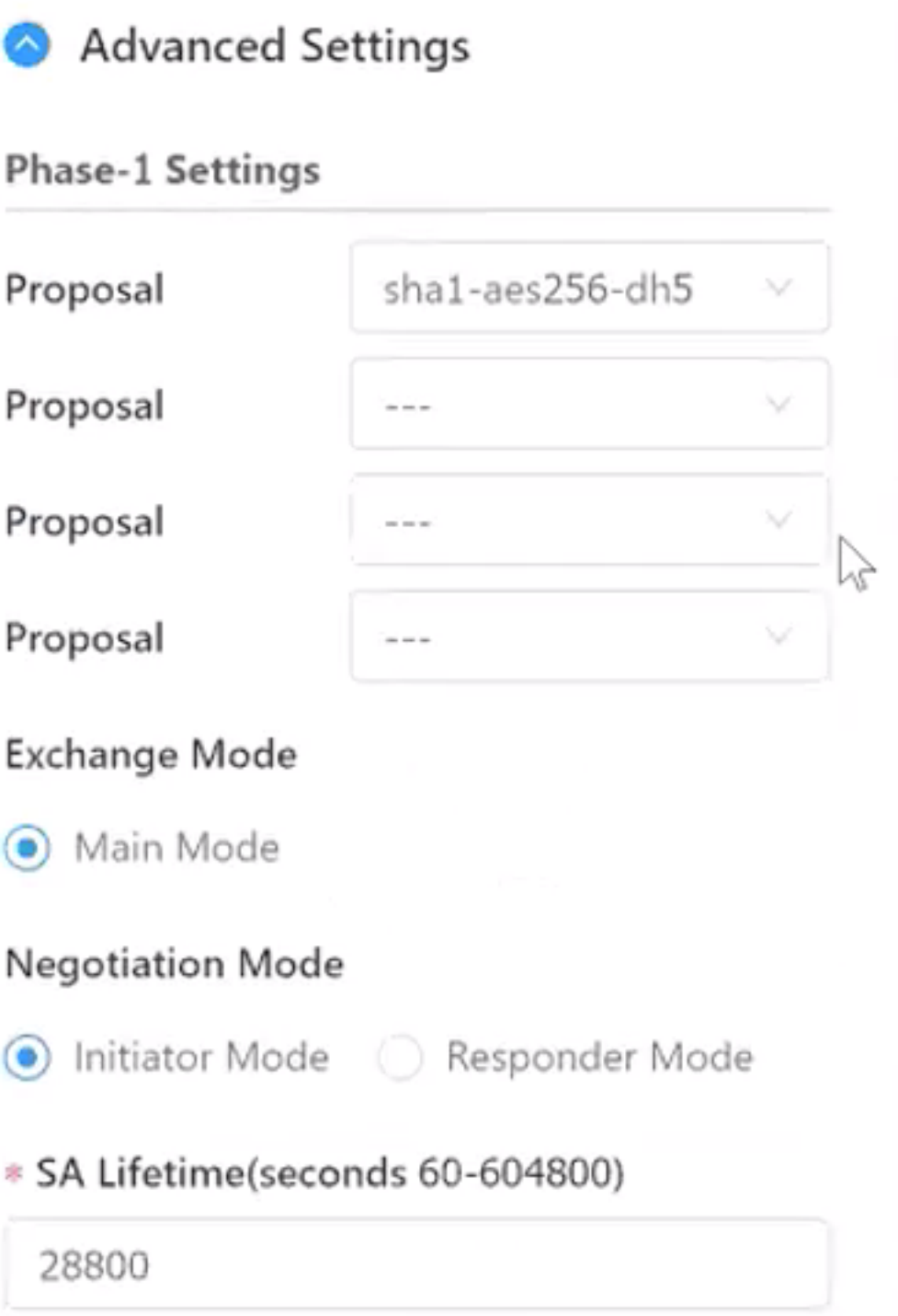
4. Enter these:


Enable
* Policy Name(1-32 characters)
Perimeter81
* Mode
Net-2-Net
* Remote Gateway(IP Address/Domain Name
* Local Subnet
* Local Mask
* Remote Subnet
* Remote Mask



Field	Enter
Policy Name	Name for the policy.
Mode	Net-2-Net
Remote Gateway IP	Public IP address of the Check Point SASE gateway.
Local Subnet and Local Mask	You LAN subnet and subnet mask.
Remote Subnet	Check Point SASE network subnets. Default is 10.255.0.0/16.
Remote Mask	255.255.0.0
Pre-shared Key (1-128 characters)	Secret key specified in the Check Point SASEAdministrator Portal and **IKEv2**.

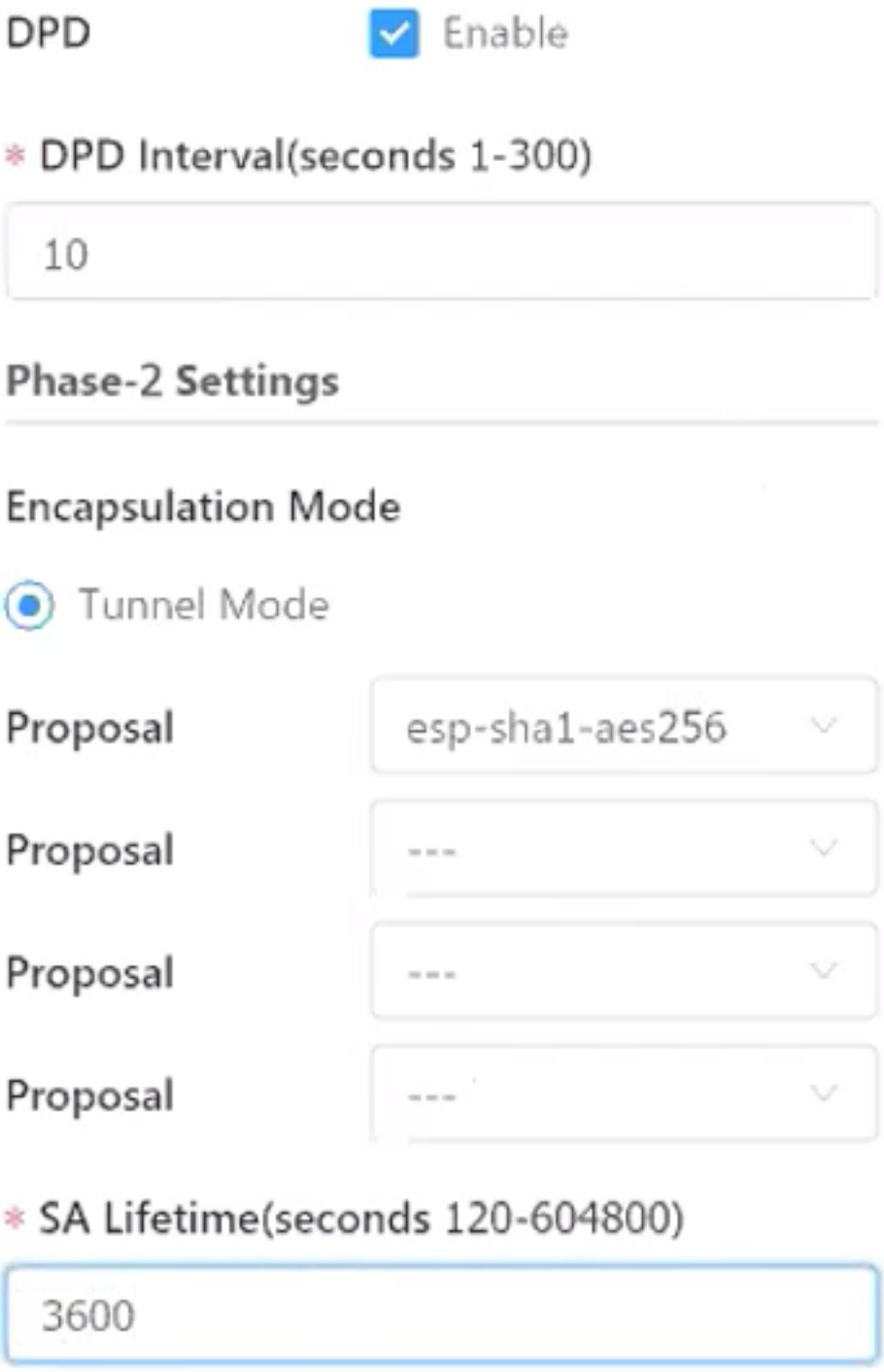
5. In the **Advanced Settings** section:


Advanced Settings
Phase-1 Settings
Proposal
sha1-aes256-dh5
Proposal

Proposal

Proposal

Exchange Mode
Main Mode
Negotiation Mode
Initiator Mode
Responder Mode
* SA Lifetime(seconds 60-604800)
28800



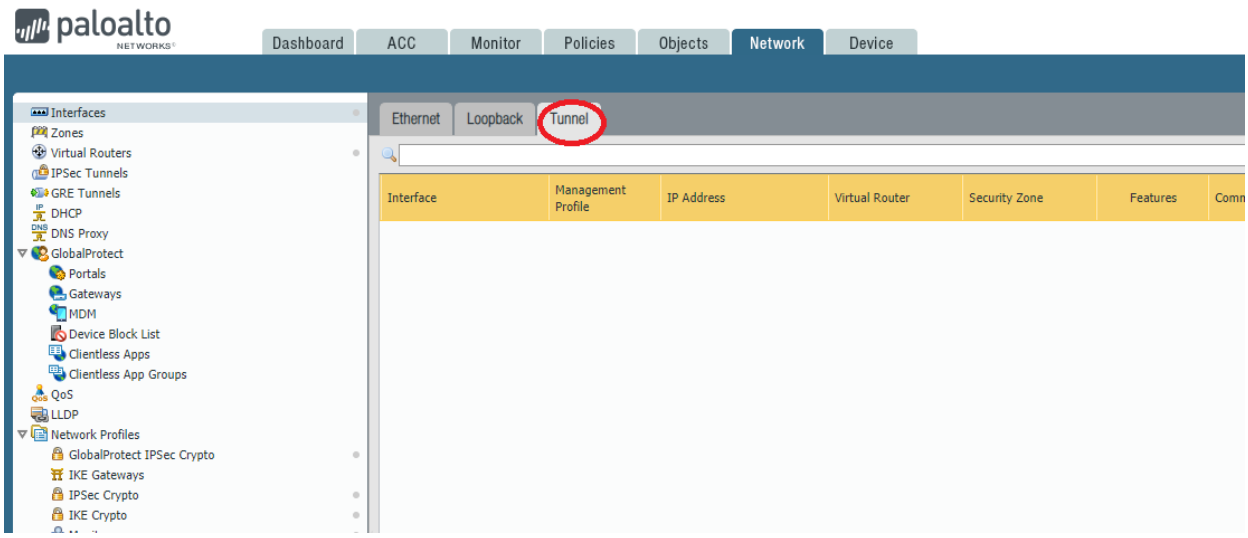
Field	Enter
Phase 1 Proposal	sha1-aes256-dh5
Exchange Mode	Main Mode
Negotiation Mode	Initiator Mode

Field	Enter
Phase I SA Lifetime seconds	28800
DPD	Enable
DPD Interval	10 seconds
Phase II Encapsulation Mode	Tunnel Mode
Phase II SA Lifetime seconds	3600

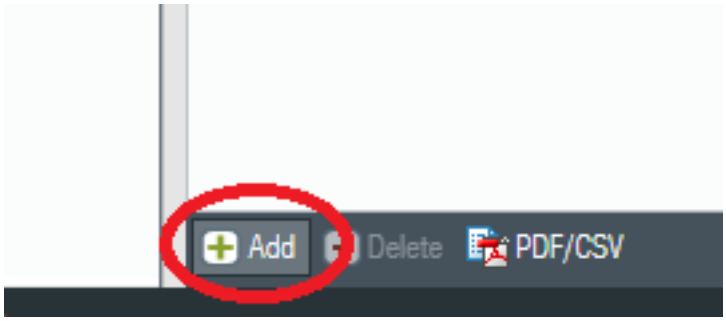
Palo Alto Firewall

To configure the tunnel in the Palo Alto Management Portal:

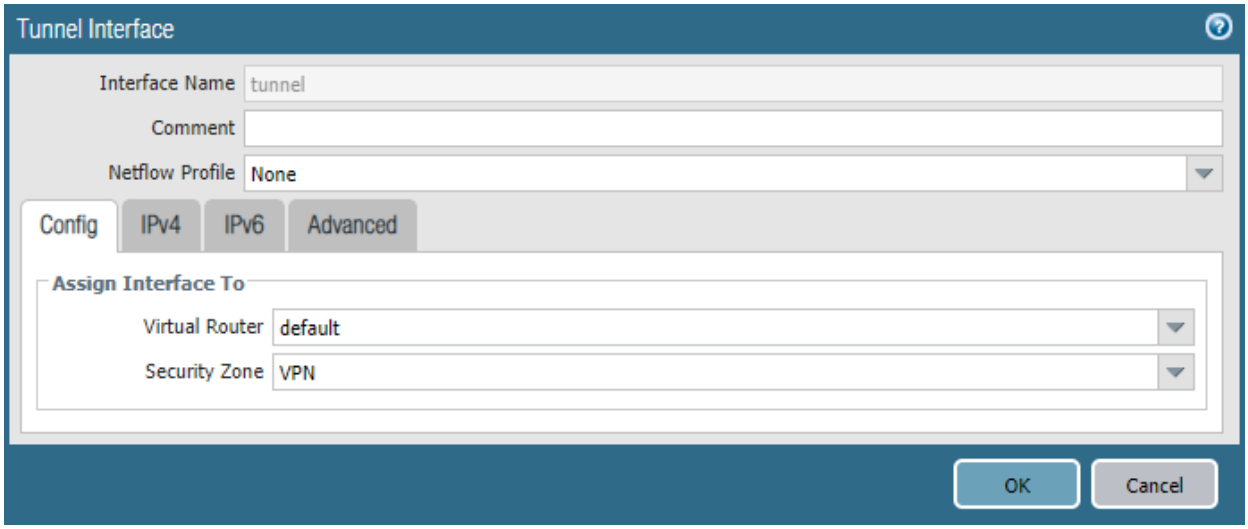
1. Log in to the Palo Alto Management Portal with the Administrator account.
2. Go to **Interfaces** and click the **Tunnel** tab.



3. Click **Add**.



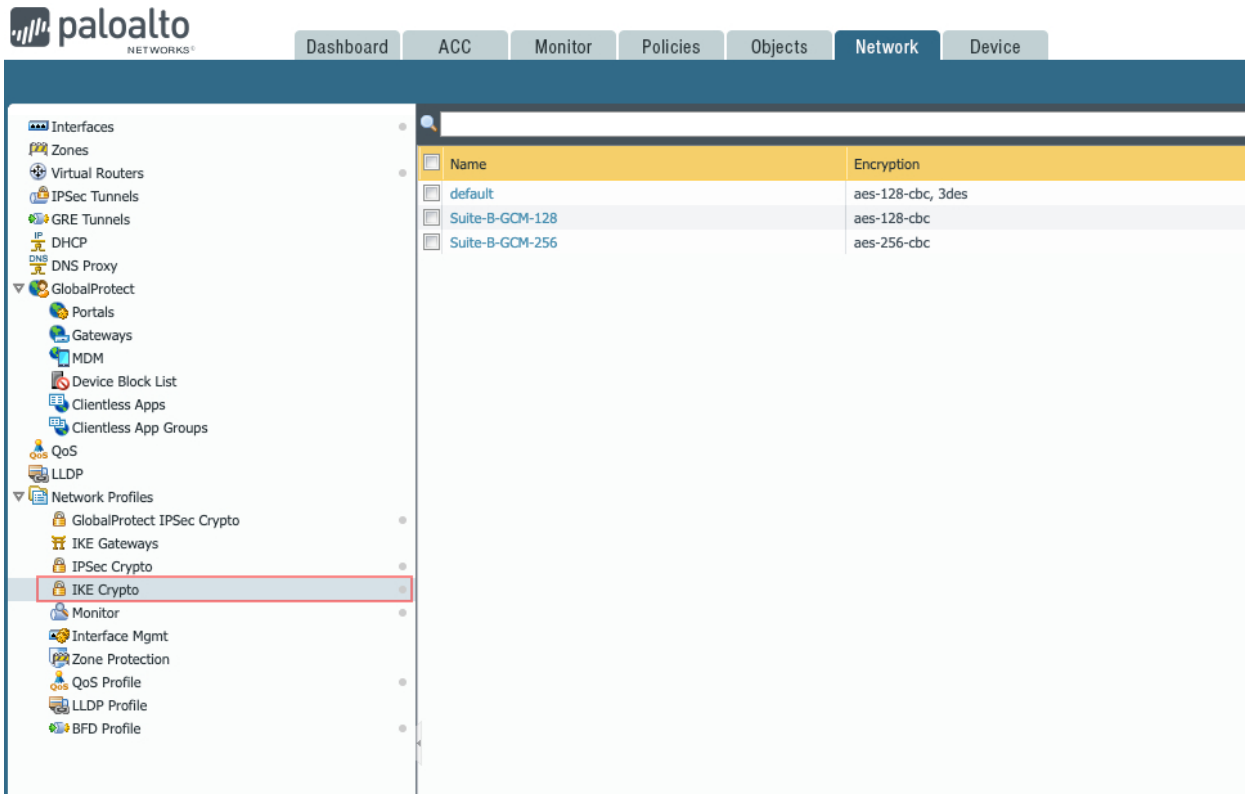
The **Tunnel Interface** window appears.



4. From the **Virtual Router** list, select the virtual router for the tunnel interface.
5. From the **Security Zone** list, select a zone for the tunnel interface

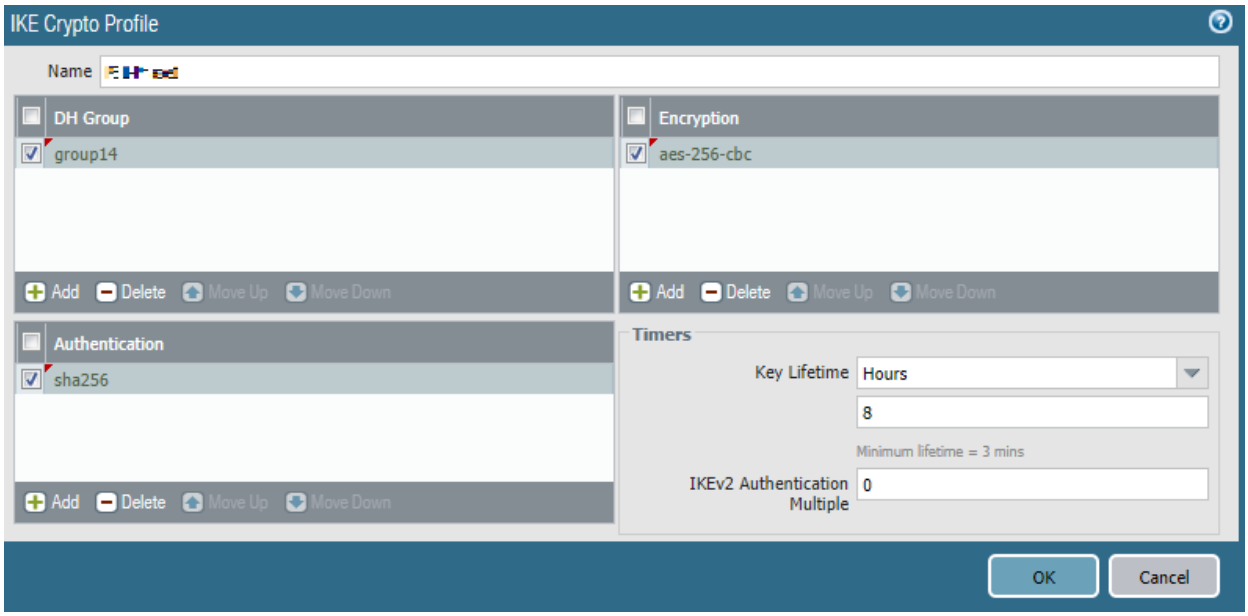
   Note - Configure a new zone for the tunnel interface for granular control of traffic ingress and egress through the tunnel. If the tunnel interface zone is different from the zone where the traffic originates or departs, then configure a policy to allow the traffic from the source zone to the tunnel interface zone.

6. Click **OK**.
7. Go to **Network Profiles > IKE Crypto**.



8. In the **Networks** tab, click **Add**.

The **IKE Crypto Profile** window appears.

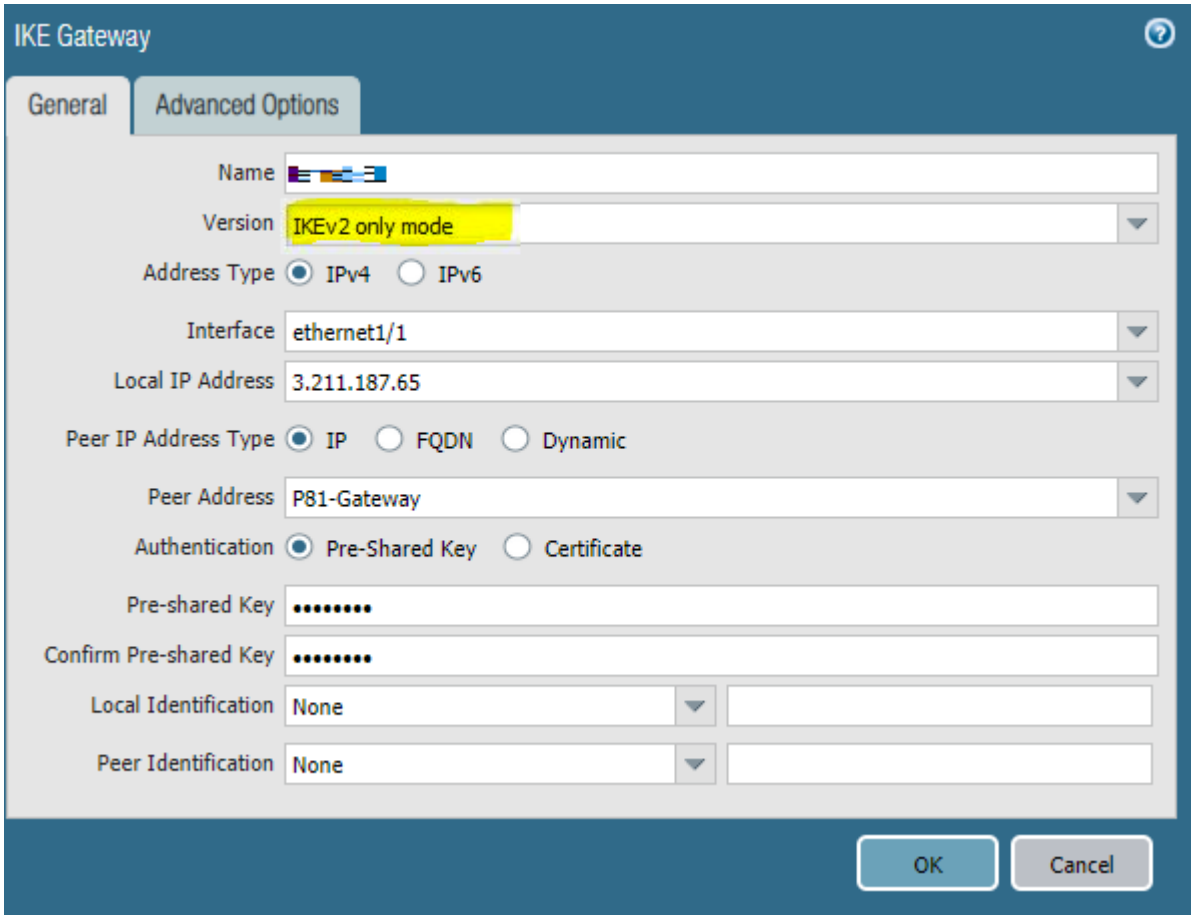


9. Enter these:

Field	Enter
Name	Name for the profile.
DH Group	14
Encryption	aes-256-cbc
Authentication	sha256
Key Lifetime	8 Hours
IKEv2 Authentication Multiple	0

10. Go to **Network Profiles > IKE Gateways**.
11. In the **Networks** tab, click **Add**.

    The **IKE Gateway** window appears.



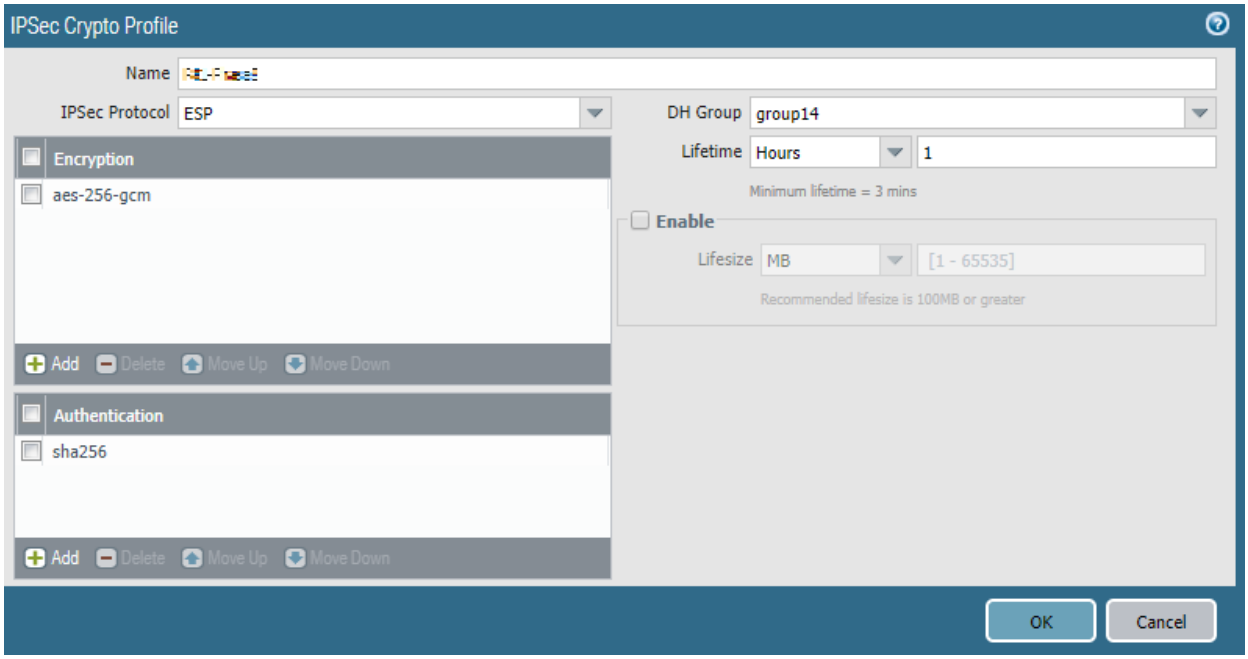
12. In the **General** tab:

Field	Enter
Name	Name for the gateway.
Version	IKEv2 only mode. If the firewall does not support IKEv2 , select IKEv1.
Address	IPv4
Interface	External interface connected to the internet.
Local IP Address	External IP address.
Peer IP Address Type	IP
Peer Address	Public IP address of the Check Point SASE gateway.
Authentication	Pre-Shared Key
Pre-shared Key	An alphanumeric string. Make a note of the key.

Field	Enter
Local Identification	None
Peer Identification	None

13. Click **OK**.
14. Go to **Network Profiles > IPSec Crypto**.
15. In the **Networks** tab, click **Add**.

    The **IPSec Crypto Profile** window appears.



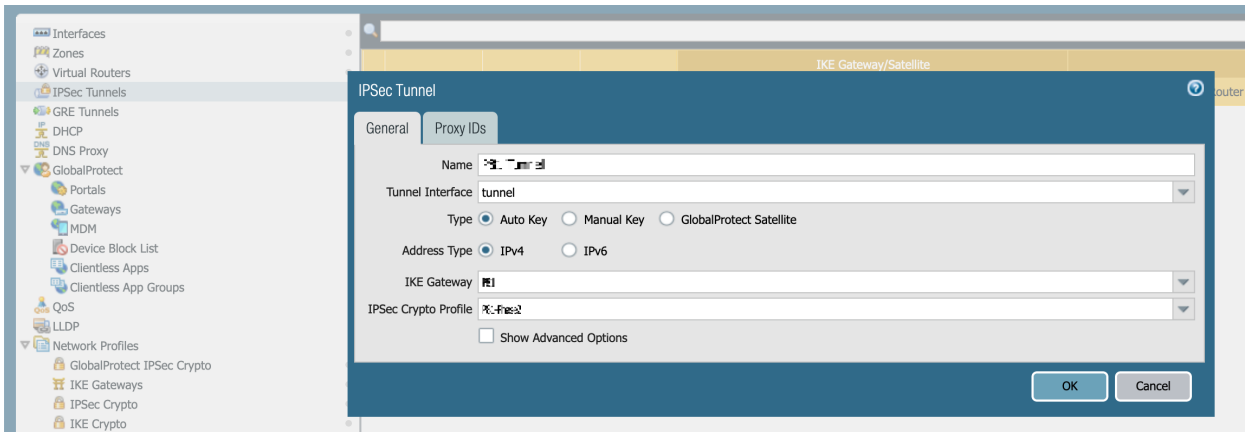
16. Enter these:

Field	Enter
Name	Name for the profile.
IPSec Protocol	ESP
DH Group	14
Encryption	aes-256-cbc
Lifetime	1 hour
Authentication	sha256

17. Click **OK**.

18. Click **IPSec Tunnels**.
19. In the **Networks** tab, click **Add**.

    The **IPSec Tunnel** window appears.

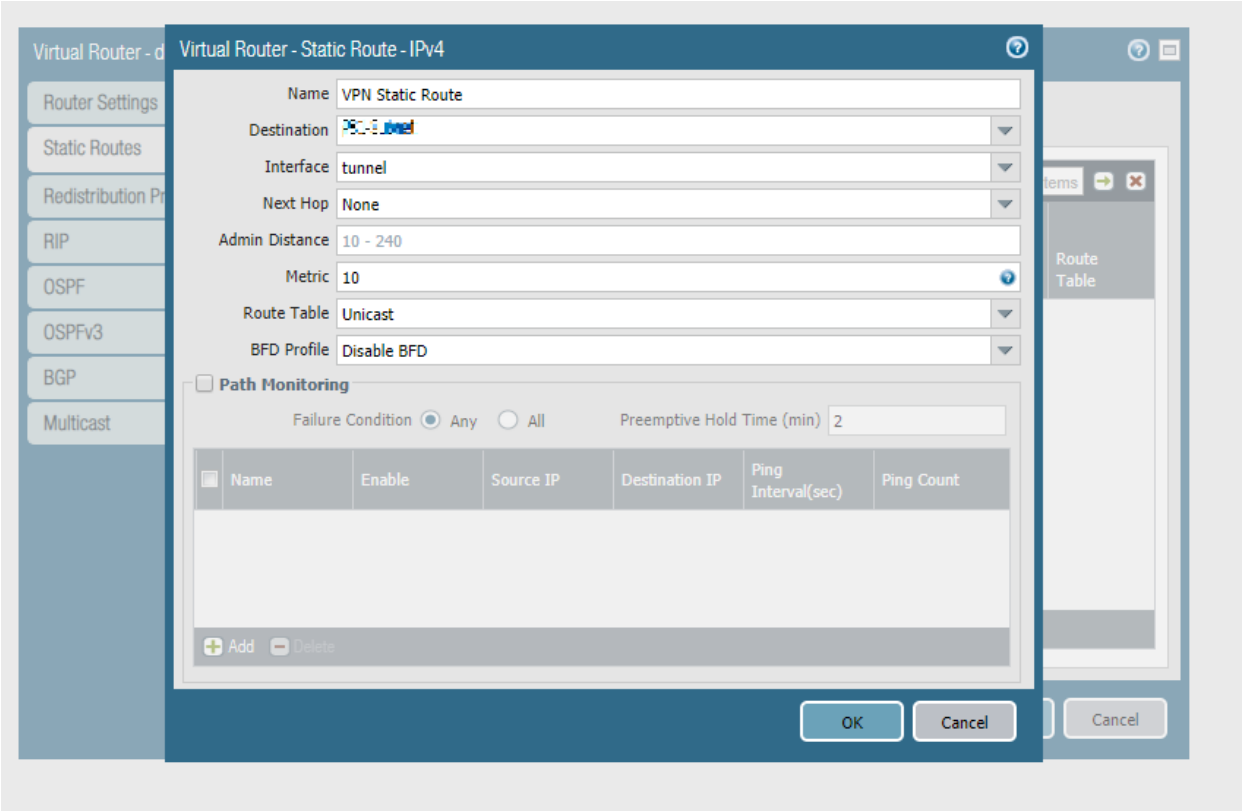


20. Enter these:

Field	Enter
Name	Name for the tunnel.
Tunnel Interface	An appropriate interface.
Type	Auto Key
Address	IPv4
IKE Gateway	Gateway that was defined previously.
IPSec Crypto Profile	Profile that was defined previously.

21. Click **Virtual Routers**.
22. Click **Static Routes** and click **Add**.

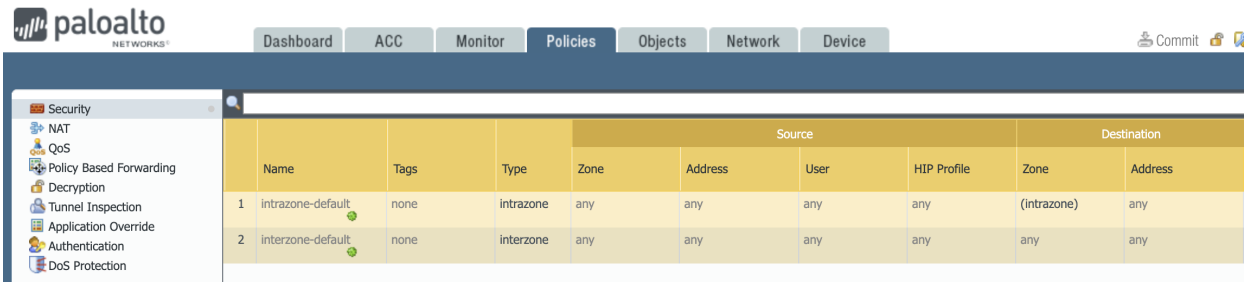
    The **Virtual Router - Static Route - IPv4** window appears.



23. Enter these:

Field	Enter
Name	Name for the static route.
Destination	Check Point SASE subnet.
Interface	An appropriate interface.
Next Hop	None
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

24. Go to **Network Profiles > IKE Crypto**.
25. Click the **Policies** tab. By default, IKE negotiation and IPSec/ESP packets are allowed. If they are not, create an appropriate rule.



Palo Alto Redundant Tunnel

This guide explains how to configure a Site-to-Site High Availability (HA) redundant VPN tunnel between your SASE network and a Palo Alto Firewall, including both firewall and SASE console configuration.

Pre-requisites

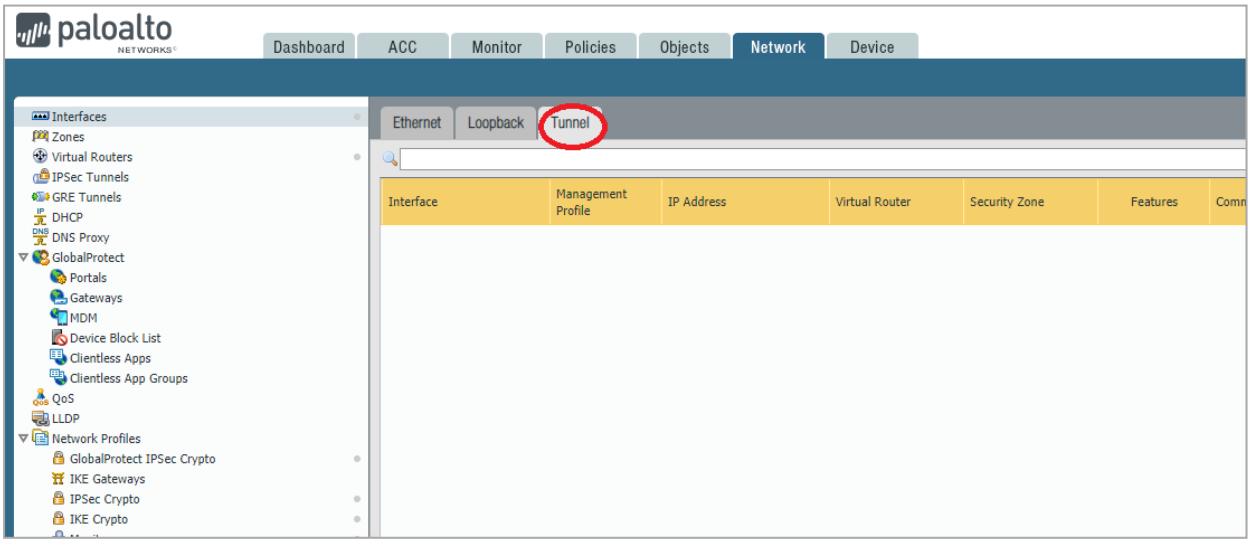
Before you begin, ensure that you have:

- An active SASE account and a functioning network.
- The SASE application installed on your devices.
- An active Palo Alto Firewall account with administrative permissions.

Configuration in Palo Alto WebGUI

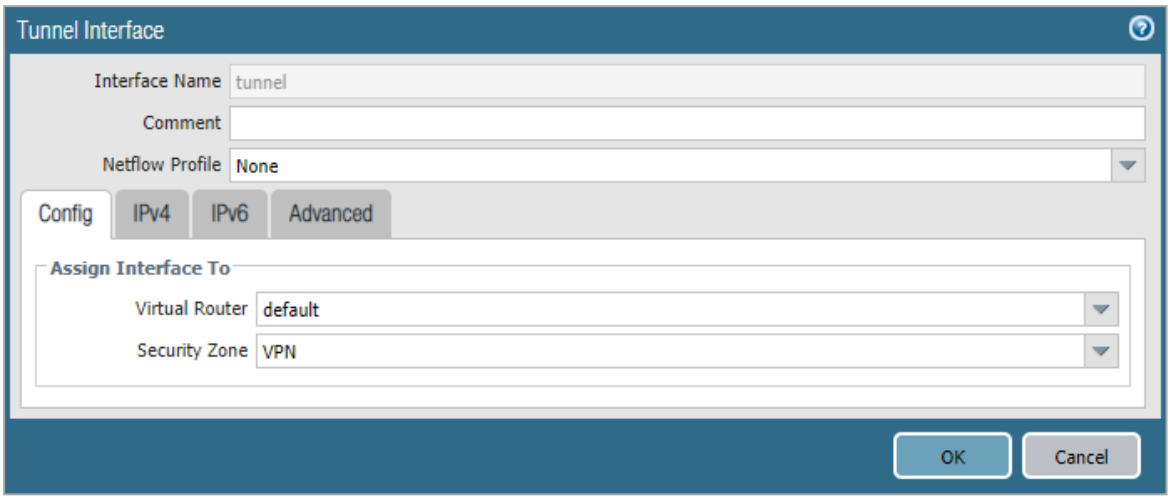
Step 1: Configure Tunnel Interfaces

1. Open the **Palo Alto WebGUI** and go to **Network**.
2. Select **Interfaces** and go to **Tunnel**.

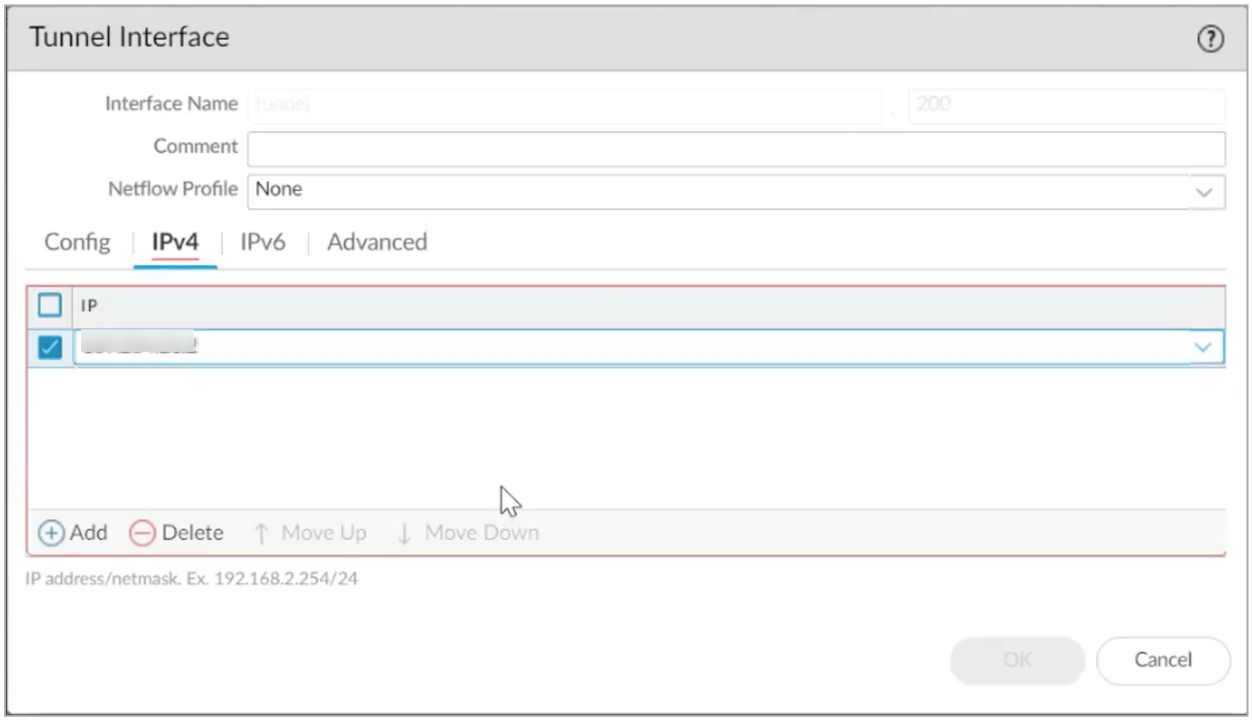


3. Click **Add**.
4. Configure these parameters:

- **Virtual Router**: Select the virtual router for the tunnel interface.
- **Security Zone**: Create a dedicated zone for tunnel traffic. If the tunnel interface is in a different zone than the source or destination, create a security policy to allow the traffic.



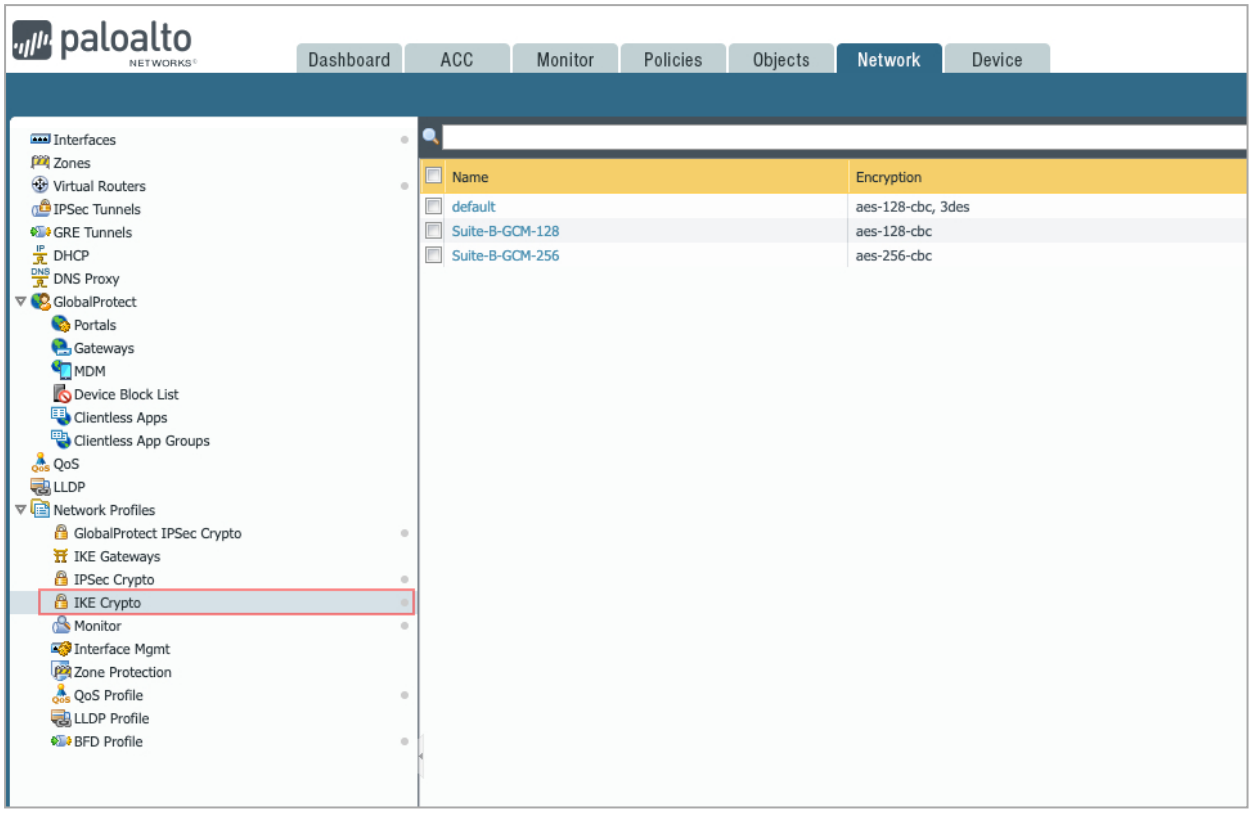
5. Click the **IPv4** tab and click **Add**. Enter the internal address for the first tunnel (use the 169.254.x.x range).



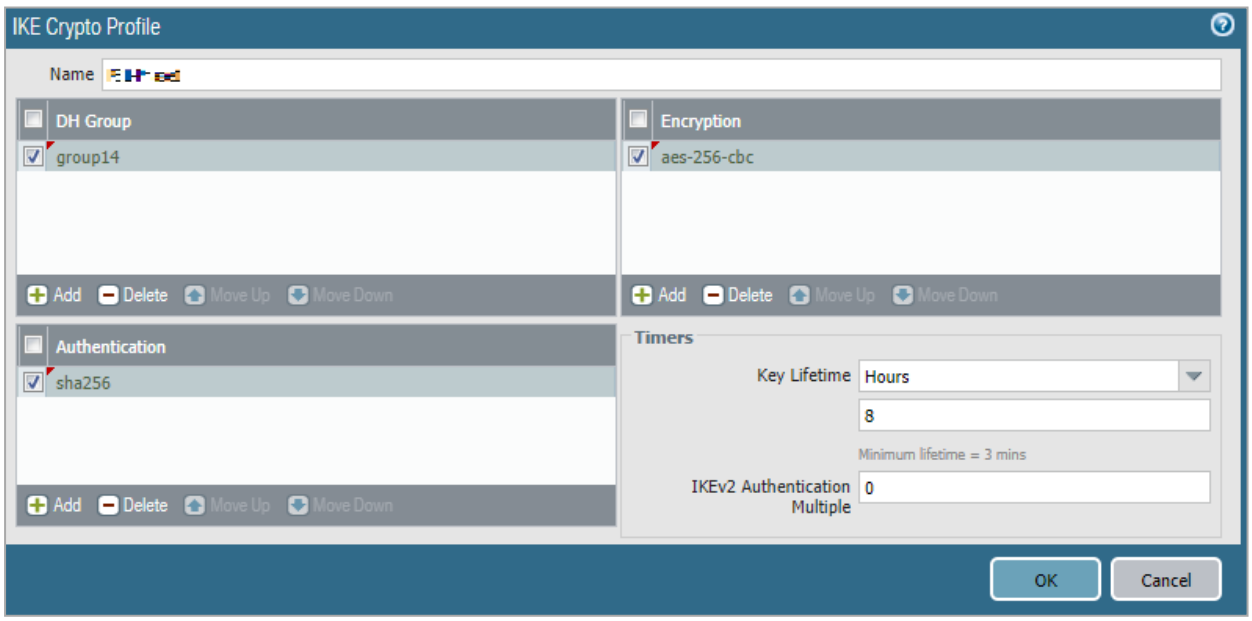
6. Click **OK**.
7. Repeat the steps to create the second tunnel interface.

Step 2: Configure IKE Crypto Profile

1. Go to **Network Profiles** > **IKE Crypto**.



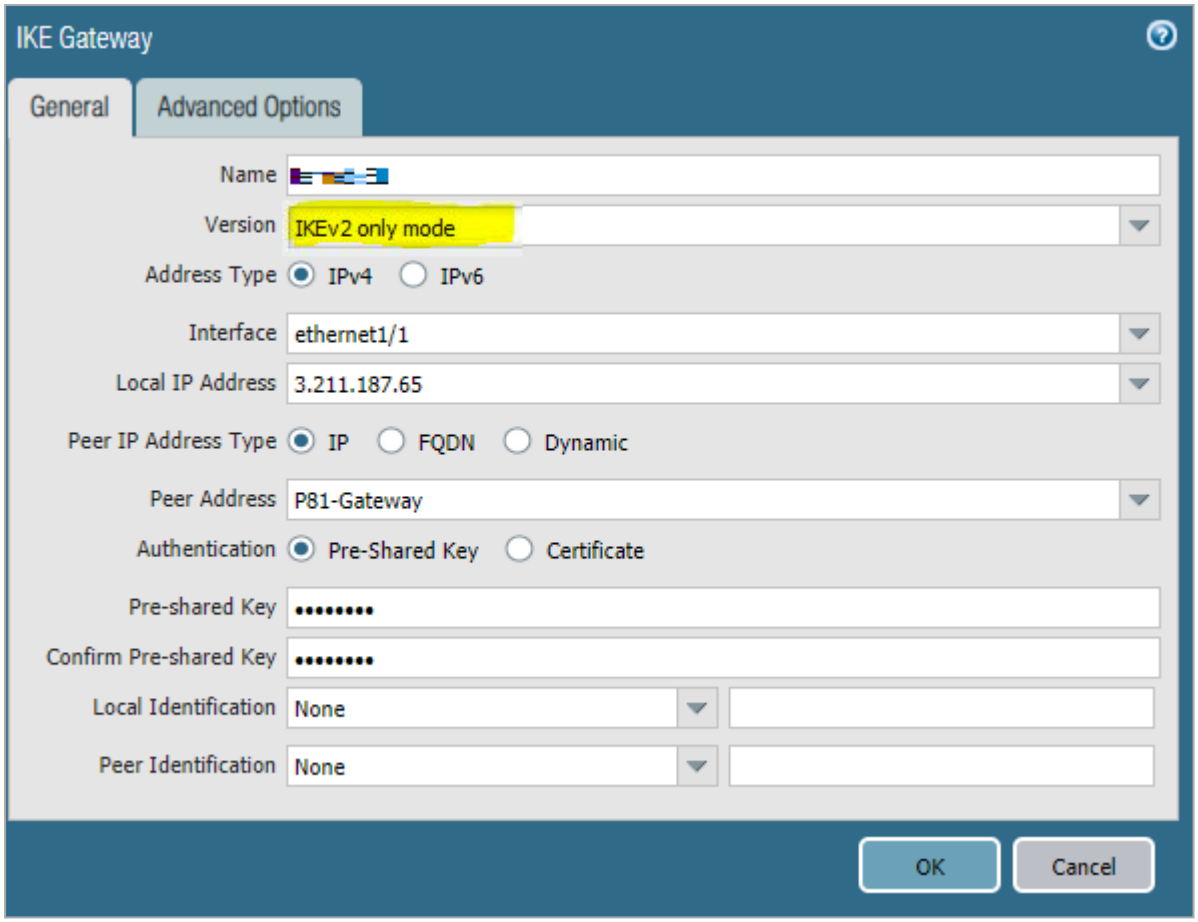
2. Click **Add** and define the IKE Crypto profile (IKEv1 Phase 1) parameters:



Field	Enter
Name	Enter a descriptive name
DH Group	14
Encryption	aes-256-cbc
Authentication	sha256
Key Lifetime	8 Hours
IKEv2 Authentication Multiple	0

Step 3: Configure IKE Gateway

1. Go to **Network Profiles** > **IKE Gateway**.
2. Click **Add** and fill these details:

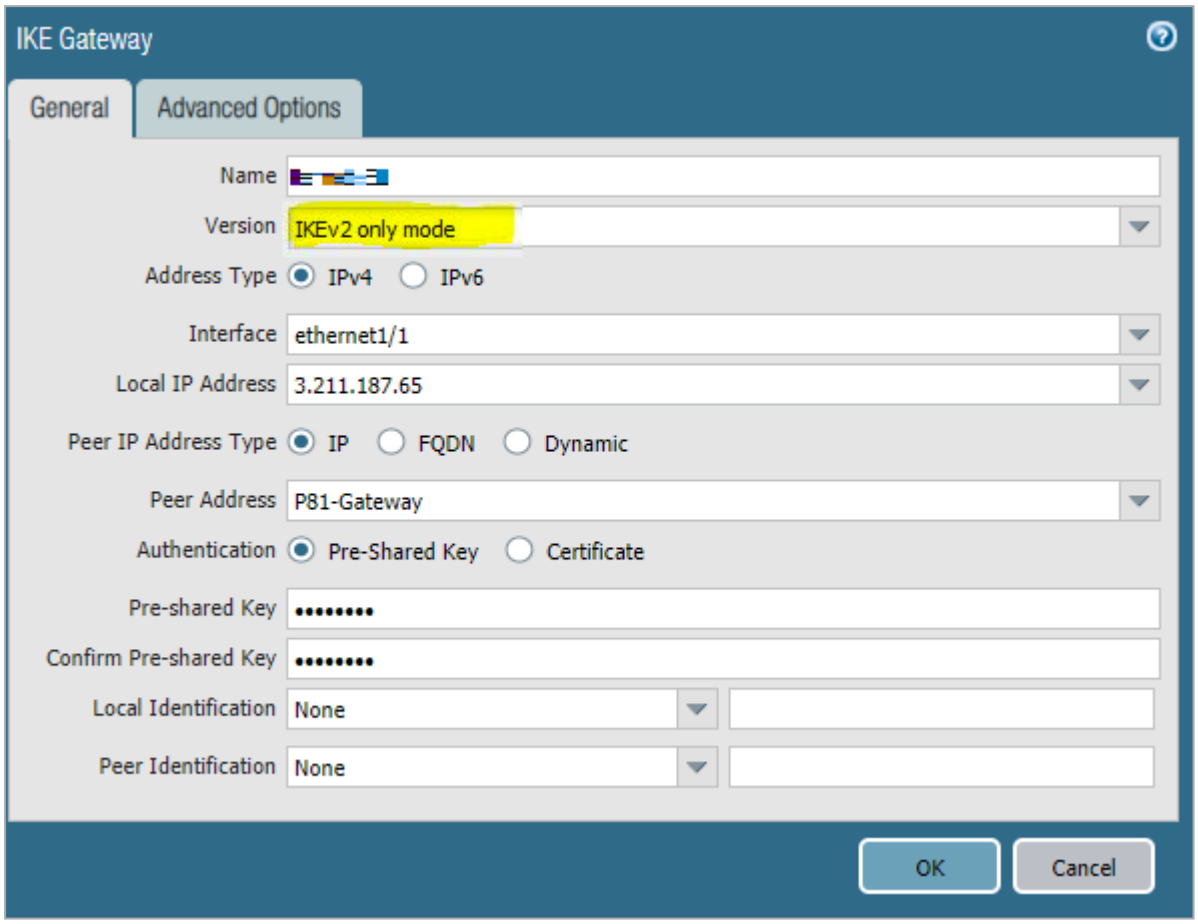


Field	Enter
Name	Name for the gateway.
Version	Select IKEv2 (or IKEv1 if unsupported)
Address	IPv4
Interface	External interface connected to the internet.
Local IP Address	External IP address.
Peer IP Address Type	IP
Peer Address	Public IP address of the Check Point SASE gateway.
Authentication	Pre-Shared Key
Pre-shared Key	Enter a strong key (mix of uppercase, lowercase, and numbers). Make a note of the key.

3. Repeat the steps for the second SASE gateway.

Step 4: Configure IPsec Crypto Profile

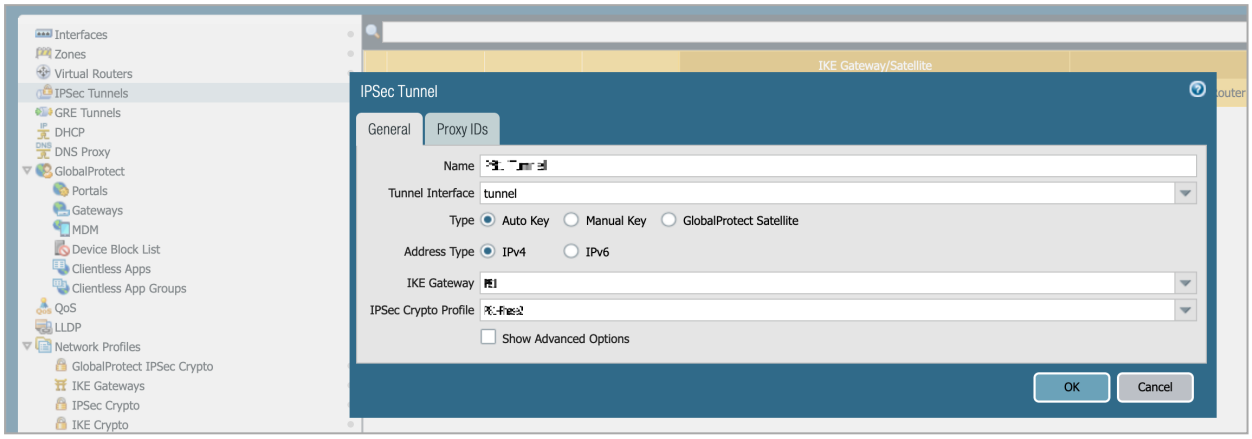
1. Go to **Network Profiles** > **IPsec Crypto**.
2. Click **Add** and enter these details:



Field	Enter
Name	P81-Phase2
IPsec Protocol	ESP
DH Group	14
Encryption	aes-256-cbc
Lifetime	1 hour
Authentication	sha256

Step 5: Configure IPsec Tunnels

1. Go to **Network Profiles** > **IPsec Tunnels**.
2. Click **Add** and enter these details:

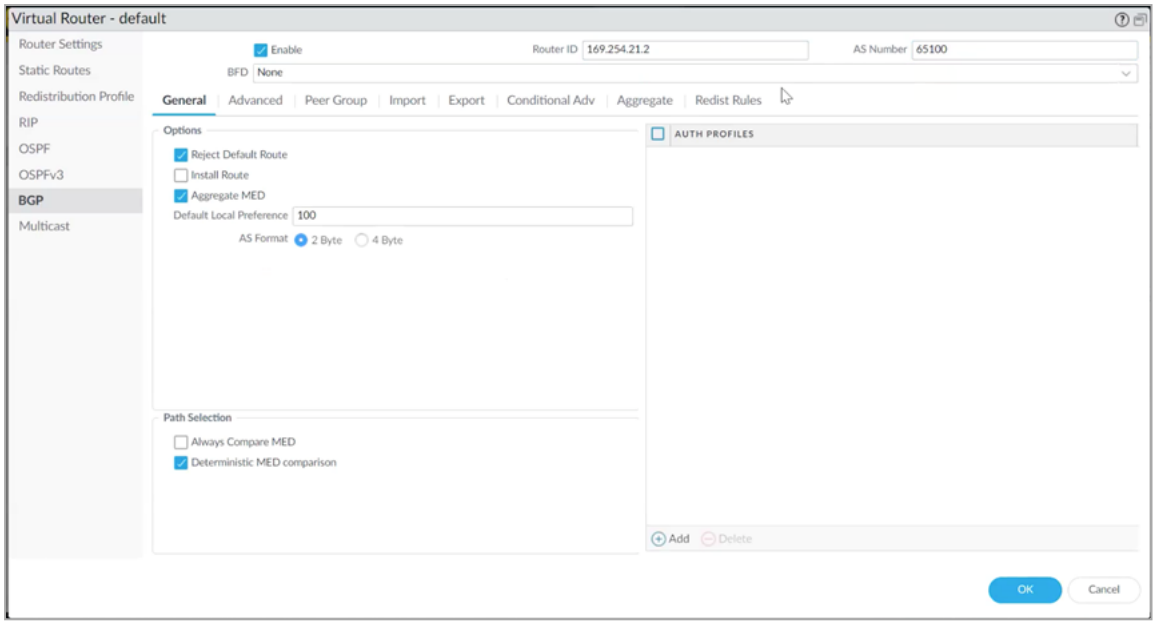


Field	Enter
Name	Name for the tunnel.
Tunnel Interface	An appropriate interface.
Type	Auto Key
Address	IPv4
IKE Gateway	Select the previously defined gateway.
IPsec Crypto Profile	Select the previously defined profile.

3. Repeat the steps for the second IPsec tunnel.

Step 6: Configure BGP

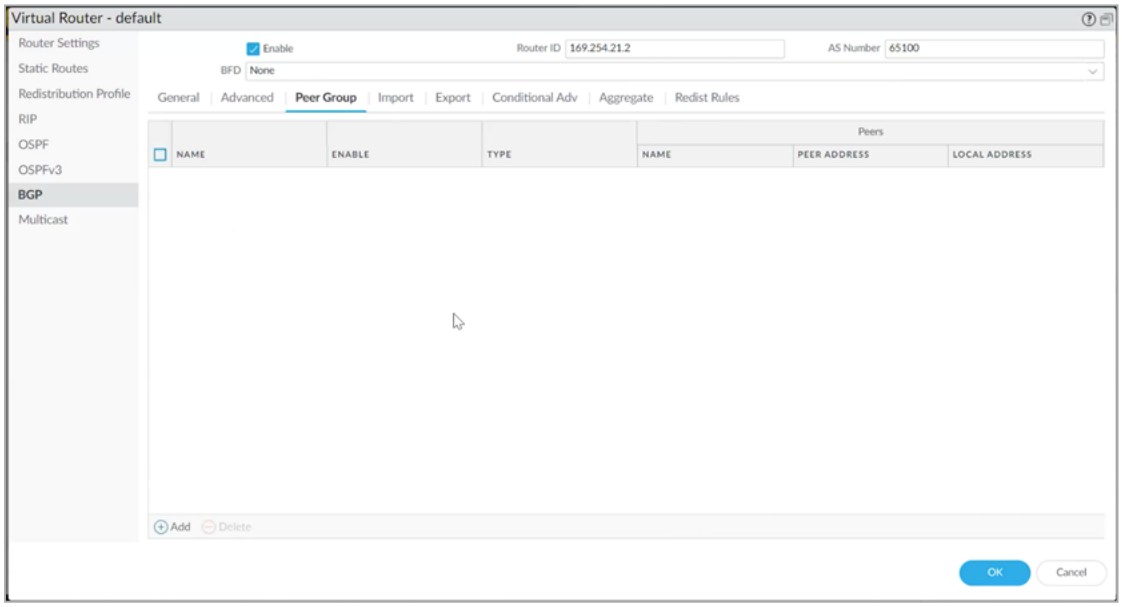
1. Go to **Network Profile** > **Virtual Routers**.
2. Click **BGP** and enter these details:



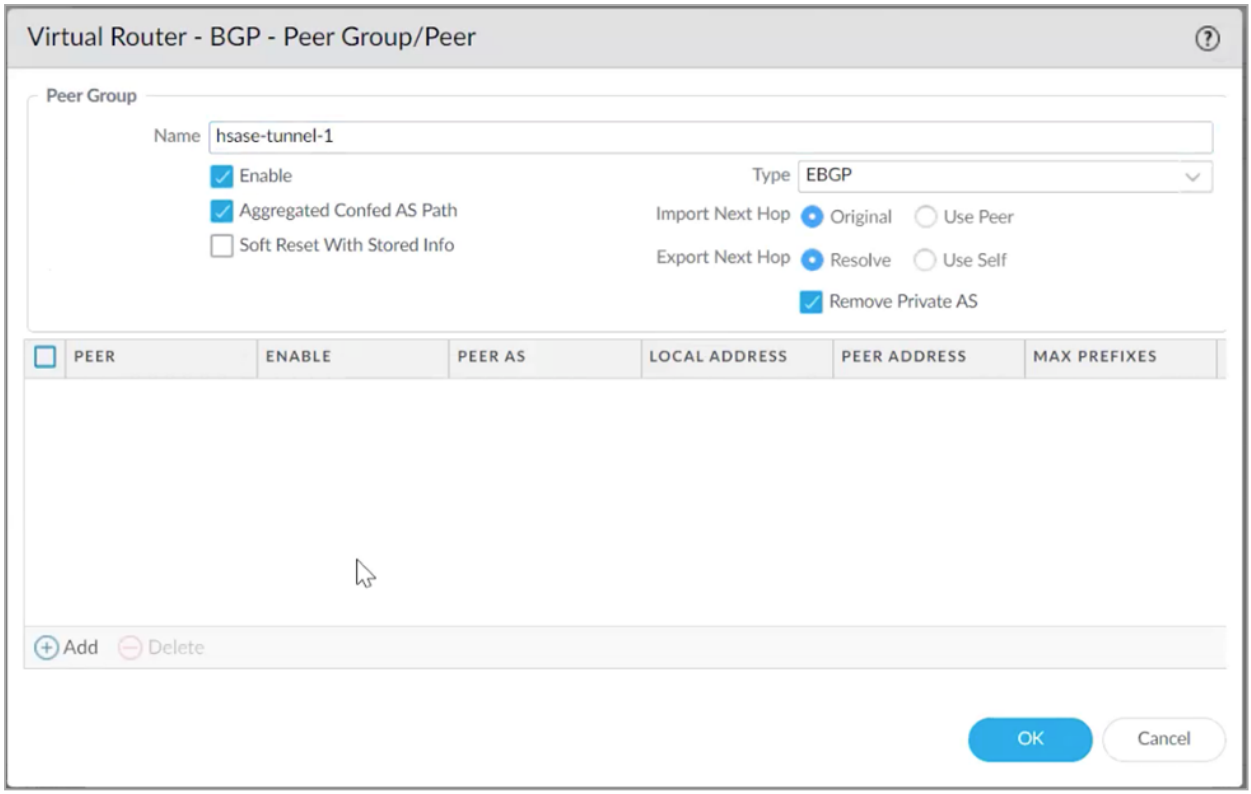
- **Router ID**: Internal address for the first tunnel (from Step 1).
- **AS Number**: AS number for the Palo Alto Firewall.

Add BGP Peer Group and Peers (for redundancy)

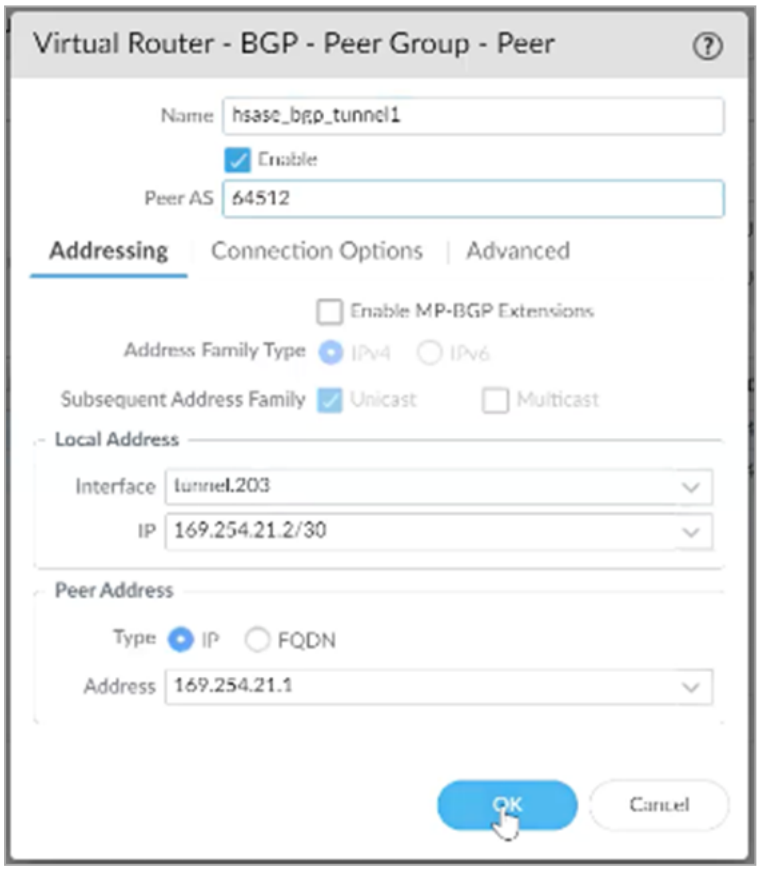
1. Under **Peer Group**, click **Add** and enter a name for the Peer Group.



2. Under **Peer**, click **Add**.



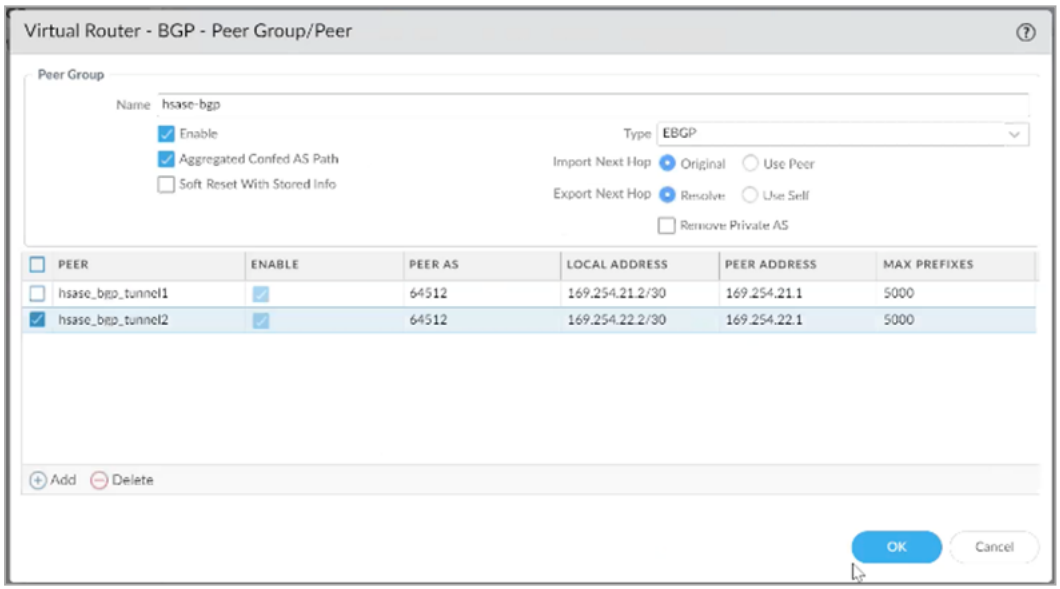
In the Peer window, configure these details:



Field	Enter
Name	Enter a descriptive name.
Peer AS	SASE AS number (default: 65000).
Local Address	▪ **Interface**: Select the first tunnel interface created in Step 1. ▪ **IP**: Select the internal address assigned to the first tunnel.
Peer Address	Internal (BGP) address for the first SASE gateway.

3. Go to **Connection Options**, set **Multi Hop** to **3**.
4. Repeat for the second tunnel interface.

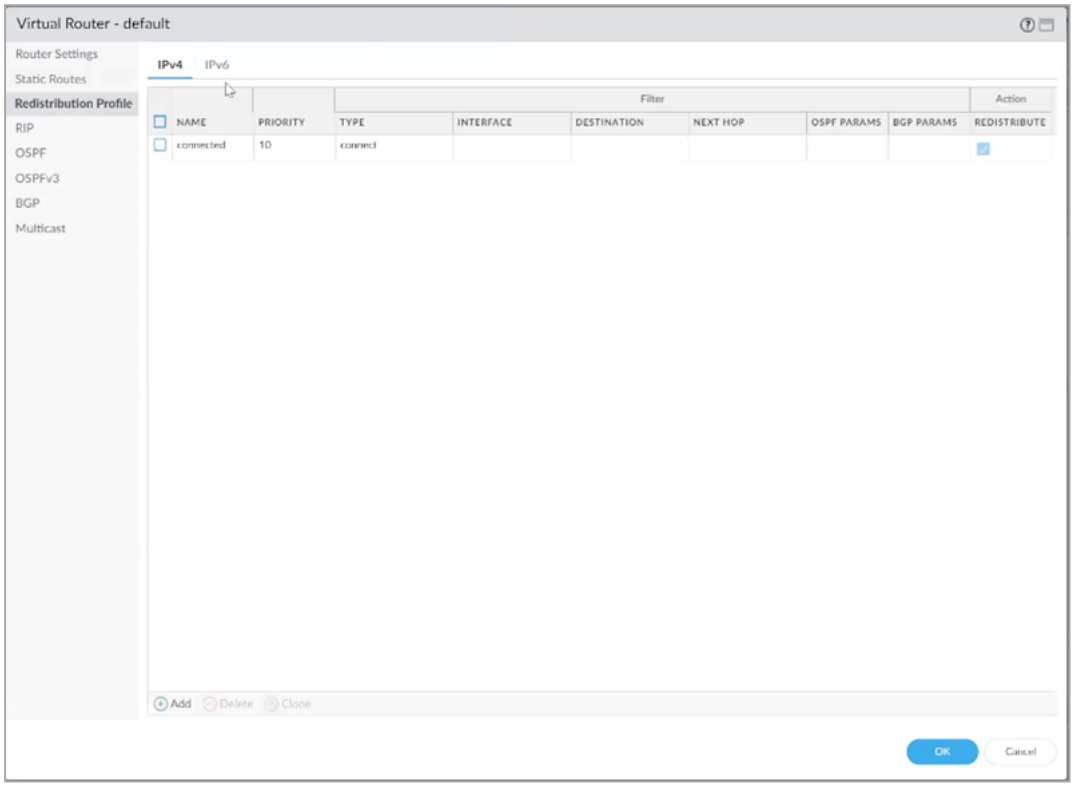
   The Peer Group configuration should resemble the example shown below.



Step 7: Configure Redistribution Profile and BGP Import Rules

Redistribution Profile

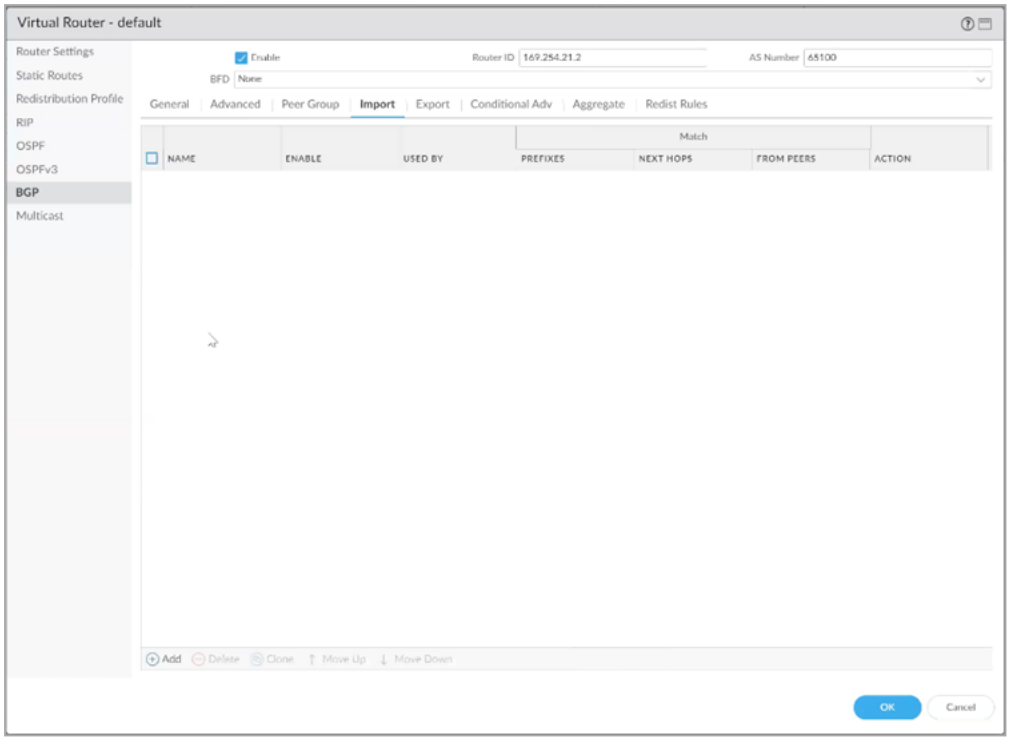
1. Go to **Virtual Router** > **Redistribution Profile** > **Add**.



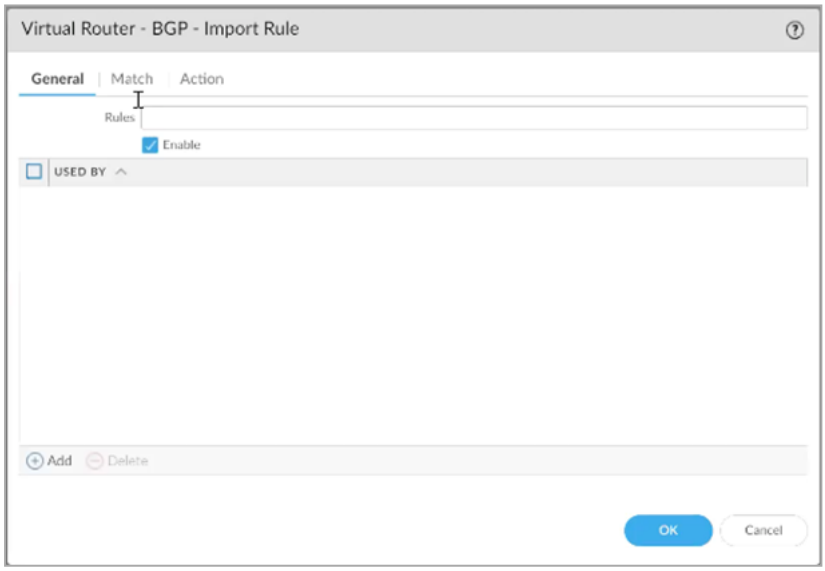
2. Configure:
   - **Name** and **Priority**
   - Enable **Redist**
   - Under **General Filter**, check **Static**
3. Click **OK**.

BGP Import Rules

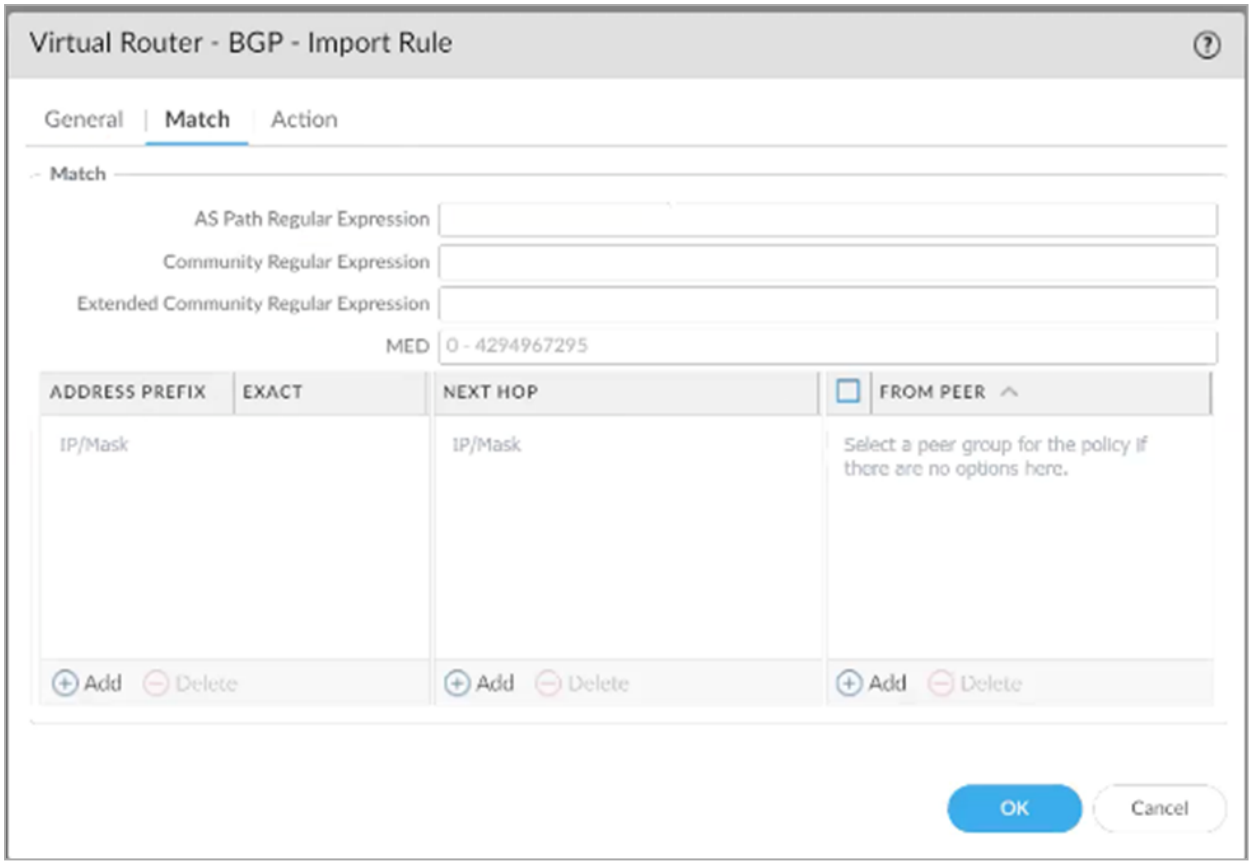
1. Go to **BGP** > **Import** > **Add**.



2. Enter a **Name** for the rule.

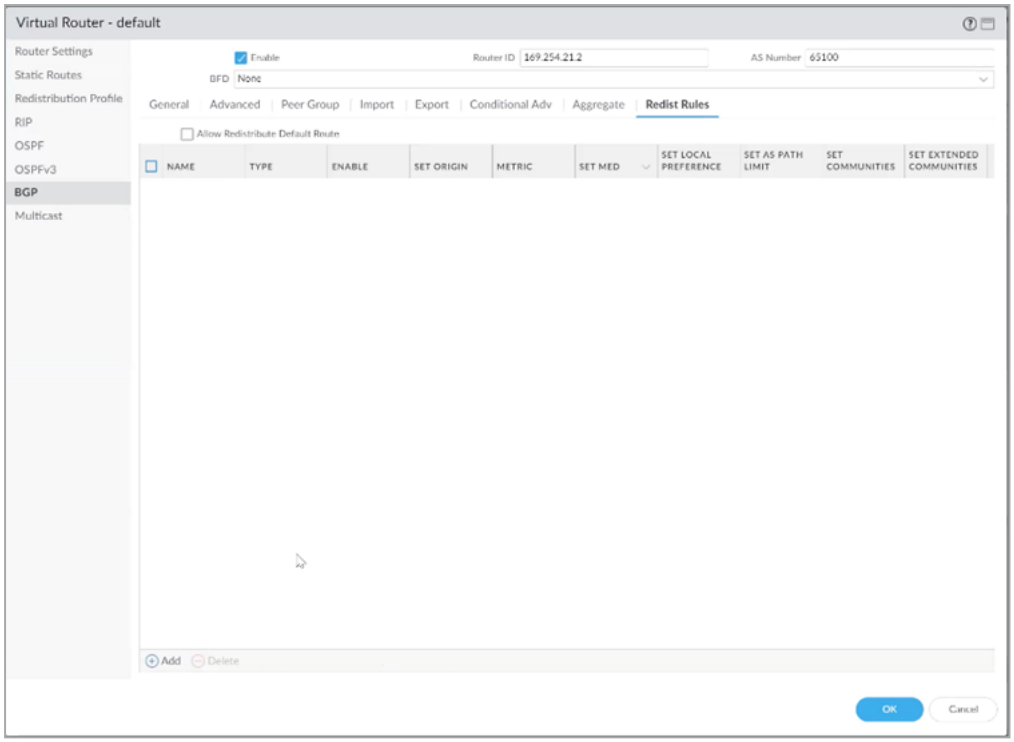


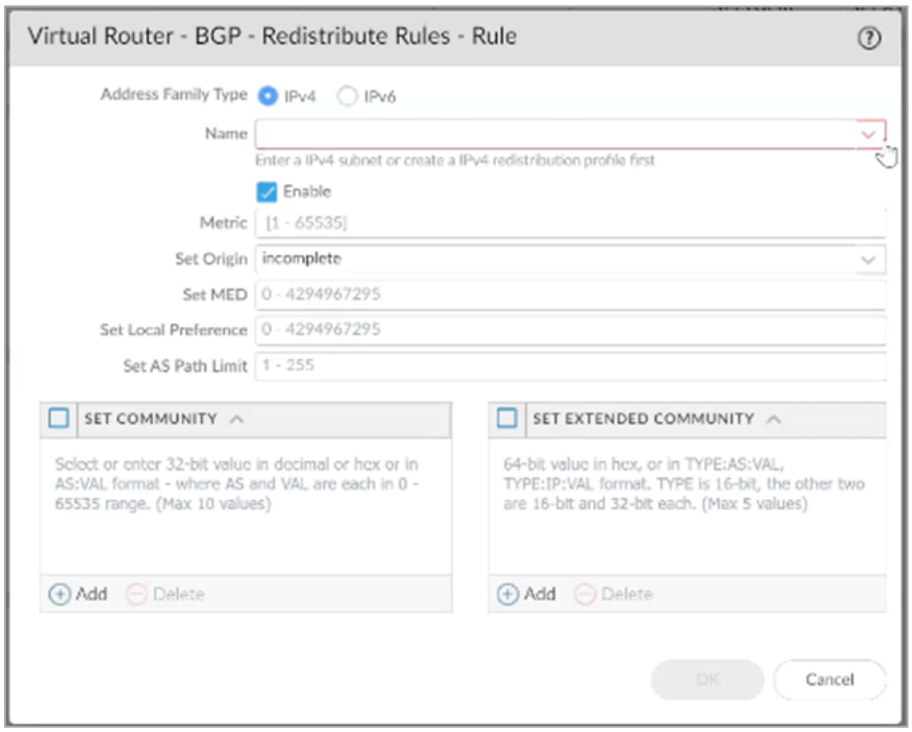
3. Click **Add** and select the created peer group.
4. Under Match, configure:



- **AS Path Regular Expression**: _<SASE AS>$ (replace with the actual SASE AS)
- **FROM PEER**: Select the two tunnel interfaces created previously.

5. Under **Action**, choose **Allow**.
6. Under **Redist Rules**, click **Add** and select the redistribution profile created earlier.

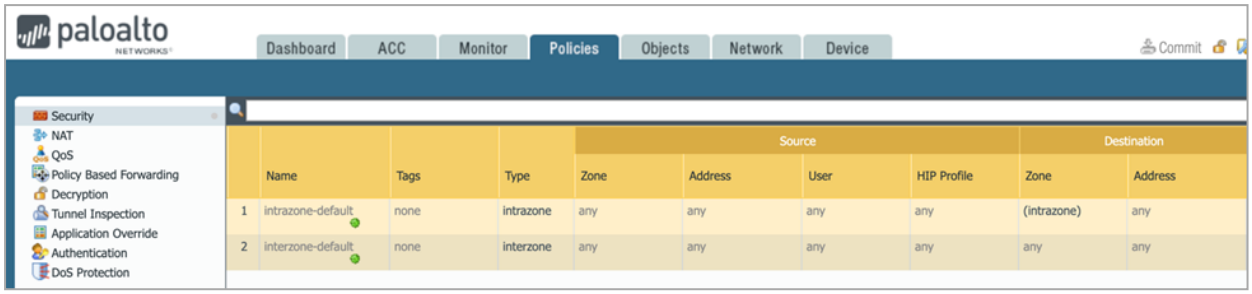

Virtual Router - default
Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP
Multicast
Enable
Router ID 169.254.21.2
AS Number 65100
BFD None
General
Advanced
Peer Group
Import
Export
Conditional Adv
Aggregate
Redist Rules
Allow Redistribute Default Route
NAME
TYPE
ENABLE
SET ORIGIN
METRIC
SET MED
SET LOCAL PREFERENCE
SET AS PATH LIMIT
SET COMMUNITIES
SET EXTENDED COMMUNITIES
Add
Delete
OK
Cancel


Virtual Router - BGP - Redistribute Rules - Rule
Address Family Type IPv4 IPv6
Name
Enter a IPv4 subnet or create a IPv4 redistribution profile first
Enable
Metric [1 - 65535]
Set Origin incomplete
Set MED 0 - 4294967295
Set Local Preference 0 - 4294967295
Set AS Path Limit 1 - 255
SET COMMUNITY
Select or enter 32-bit value in decimal or hex or in AS:VAL format - where AS and VAL are each in 0 - 65535 range. (Max 10 values)
Add
Delete
SET EXTENDED COMMUNITY
64-bit value in hex, or in TYPE:AS:VAL, TYPE:IP:VAL format. TYPE is 16-bit, the other two are 16-bit and 32-bit each. (Max 5 values)
Add
Delete
OK
Cancel

7. Click **OK**.

Step 8: Configure Security Policies

1. Open the **Policies** tab and select **Security**.

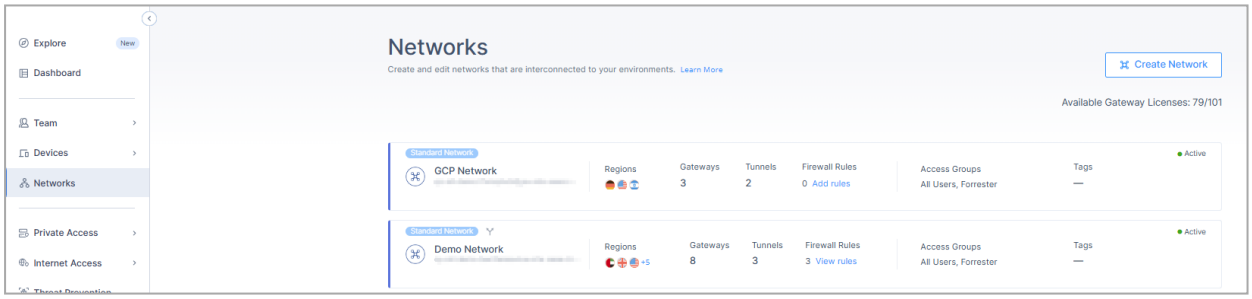


2. By default, IKE negotiation and IPsec/ESP packets are permitted.
3. If behavior differs or if you require more granular traffic control, click **Add** and create an appropriate Security policy rule.
4. Click **Commit** to apply the configuration changes.

Configuring the tunnel in the Management Platform

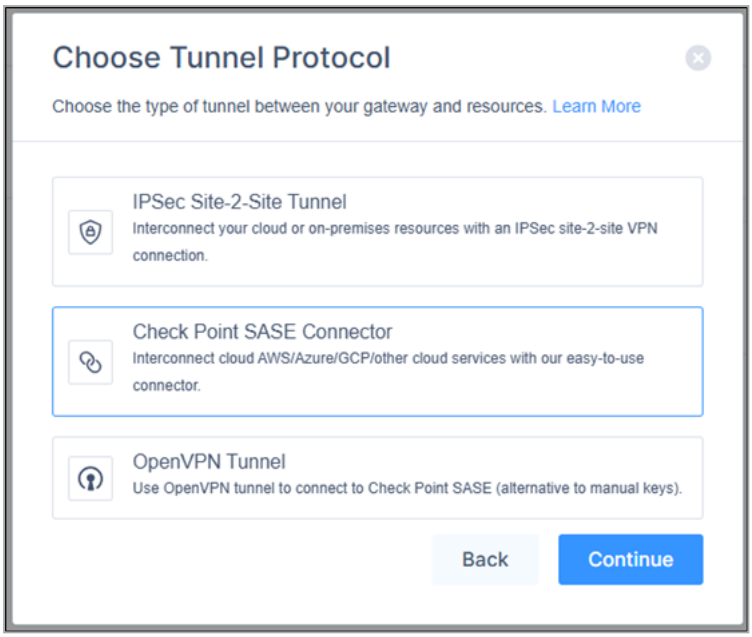
Step 1 : Configuring Tunnel and Routes Table

1. Access the SASE Administrator Portal and click **Networks**.

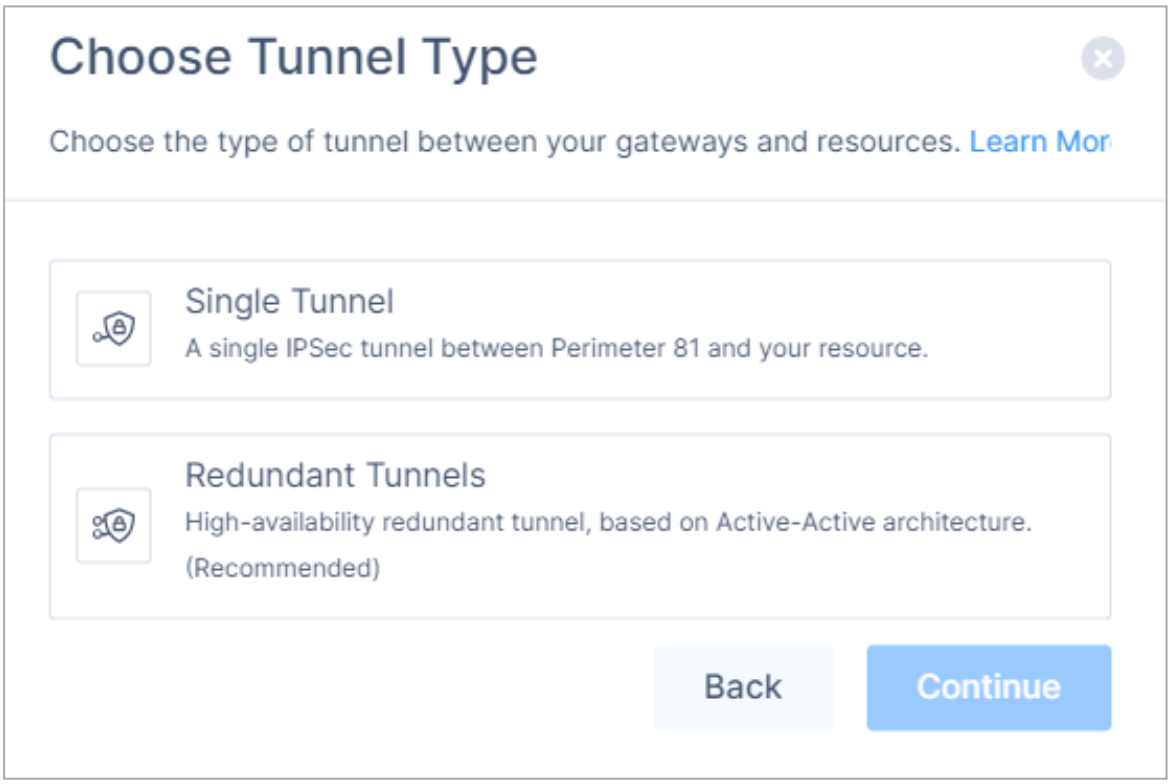


2. Select the network.
3. Click ... .
4. Select **Add Tunnel** for the gateway from which you want to add the IPsec Site-to-Site VPN tunnel.

a. Click **IPsec Site-2-Site Tunnel** and click **Continue**.



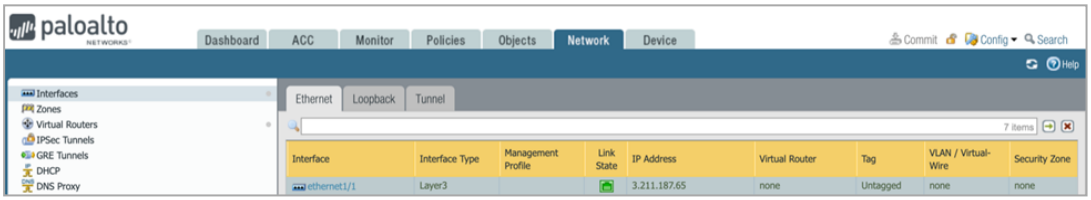
b. Click **Redundant Tunnels** and click **Continue**.



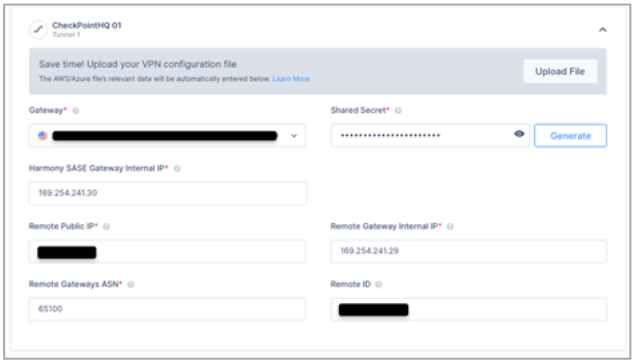
c. In the **Tunnel name** field, enter a logical name.

d. Expand **Tunnel 1** and specify these:

- **Shared Secret** – The value previously set on the first IKE Gateway.
- **SASE Gateway Internal IP** - The SASE internal IP address as you configured in the first PEER Group.
- **Remote Public IP** - Enter the firewalls external Interface IP. This can be found in Palo Alto WebGUI under Network /Interfaces /Ethernet.

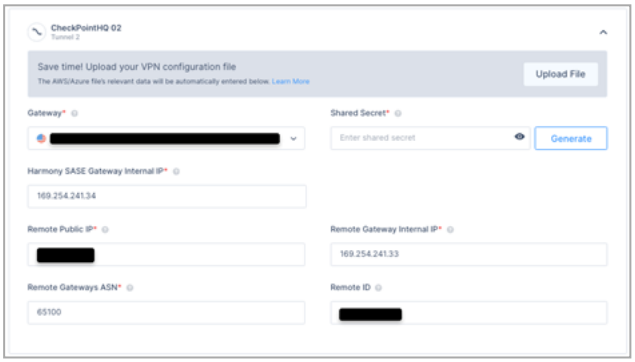


- **Remote Gateway Internal IP** - The firewall internal IP address as you configured in the first **PEER Group**.
- **Remote Gateway ASN** - The ASN of the Palo Alto Firewall.
- **Remote ID** - Enter the same value as per **Public IP**. If behind NAT, enter the internal LAN IP of the Palo Alto Device (example 192.168.1.1).



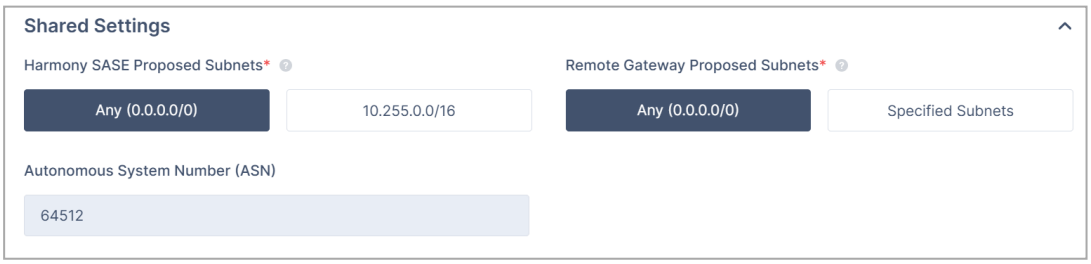
e. Expand **Tunnel 2** and specify these:

- **Gateway** - Select the second SASE Gateway for the tunnel.
- **Shared Secret** - The value previously set on the second IKE Gateway.
- **SASE Gateway Internal IP** - The SASE internal IP address as you configured in the second PEER Group.
- **Remote Public IP** - Enter the firewalls external Interface IP.
- **Remote Gateway Internal IP** - The firewall internal IP address as you configured in the second PEER Group.
- **Remote Gateways ASN** - The ASN of the Palo Alto Firewall.
- **Remote ID** - Enter the same value as you did **Public IP**. If behind NAT, enter the internal LAN IP of the Palo Alto Device (example 192.168.1.1).

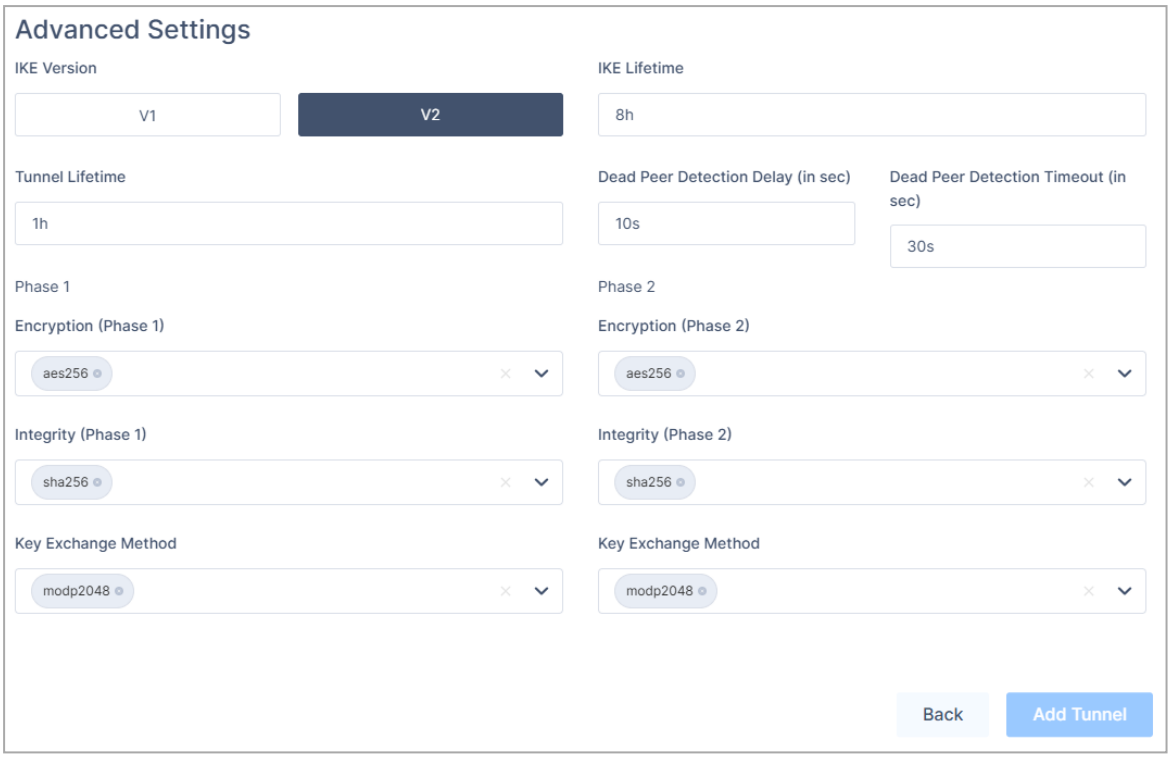


f. Expand Shared Settings and specify these:

- **SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Autonomous System Number (ASN)** - Default value is **64512**, if not set, enter the AS Number for the SASE network.



g. In the **Advanced Settings** section, specify these:



Field	Enter
IKE Version	V2
IKE Lifetime	8h
Tunnel Lifetime	1h
Dead Peer Detection Delay	10s
Dead Peer Detection Timeout	30s
Phase 1	▪ **Encryption (Phase 1)**: aes256 ▪ **Integrity (Phase 1)**: sha256 ▪ **Key Exchange Method**: modp2048
Phase 2	▪ **Encryption (Phase 2)**: aes256 ▪ **Integrity (Phase 2)**: sha256 ▪ **Key Exchange Method**: modp2048

h. Click **Add Tunnel**.

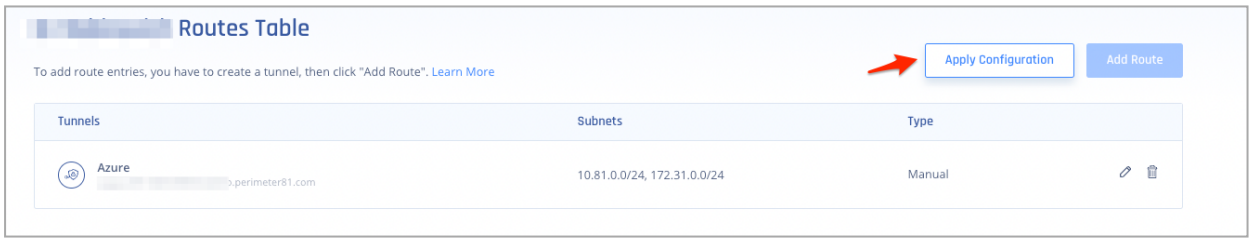
5. Select **Routes Table**:
   a. Click **Add Route**.

   The **Add Route** window appears.

   b. Enter all the Subnets on the remote side of the tunnel and then click **Add Route**.

   Note - Make sure that in the Tunnel list, you have selected the previously entered Tunnel name.

6. Click **Apply Configuration**.



Step 2: Verifying the Setup

Once you complete the above steps, the tunnel becomes active.

1. Verify the setup in the SASE Administrator Portal:
   a. Click **Networks**.
   b. Locate the tunnel you created, and check the tunnel status.

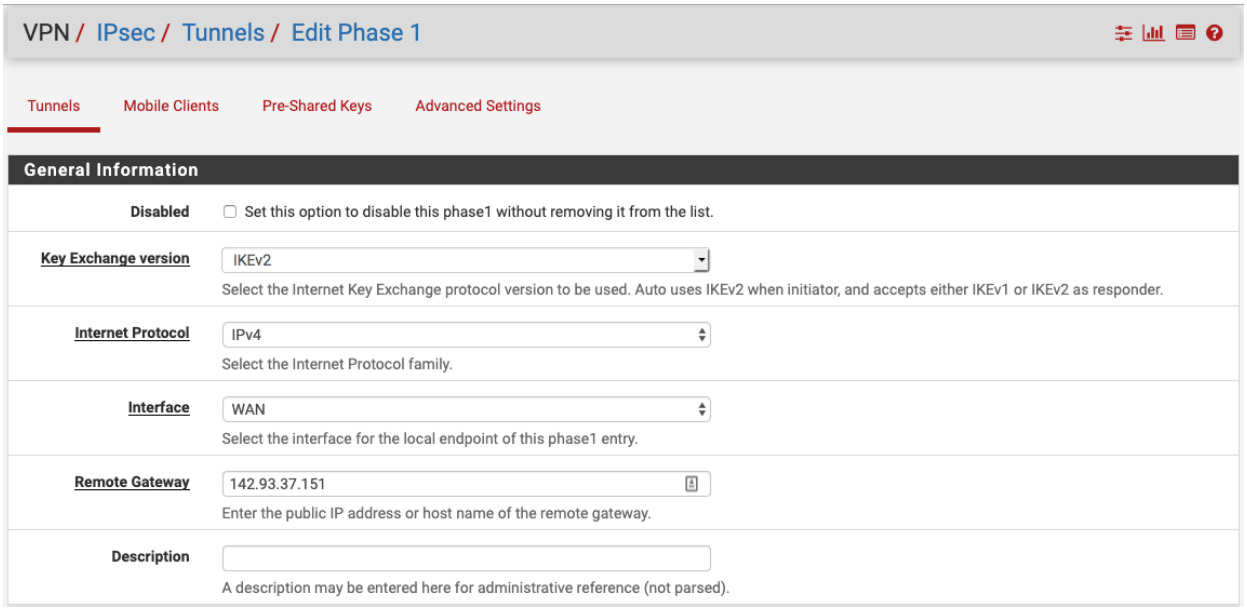
   It should indicate that the tunnel is **Up**, signifying a successful connection.

2. Verify the setup in the SASE Agent:
   a. Connect to your network using the SASE Agent.
   b. Access one of the resources in your environment.

pfSense Firewall

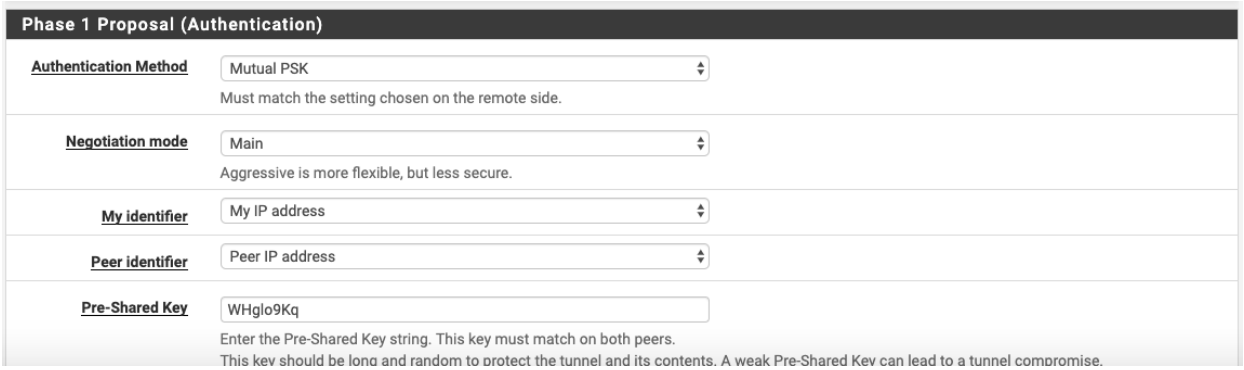
To configure the tunnel in the pfSense Management Portal:

1. Log in to the pfSense Management Portal with the Administrator account.
2. Go to **VPN > IPsec**.
3. Click **+Add P1**.
4. In the **General Information** section:



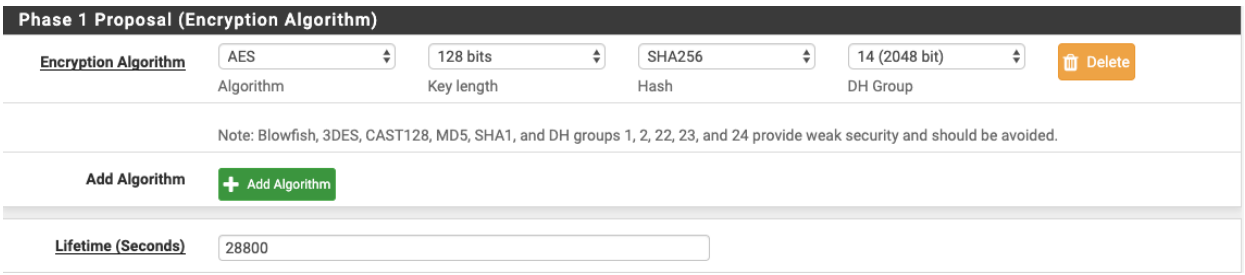
Field	Enter
Key Exchange version	IKEv2 if supported. Otherwise IKEv1.
Internet Protocol	IPv4
Interface	WAN
Remote Gateway	Public IP address of the Check Point SASE gateway.

5. In the **Phase 1 Proposal (Authentication)** section:



Field	Enter
Authentication Method	Mutual PSK
Negotiation Mode	Main
My Identifier	My IP Address **Note** - For Dynamic-IP Tunnel, select **Distinguished Name** and enter the predefined Remote ID.
Peer Identifier	Peer IP Address
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247* .

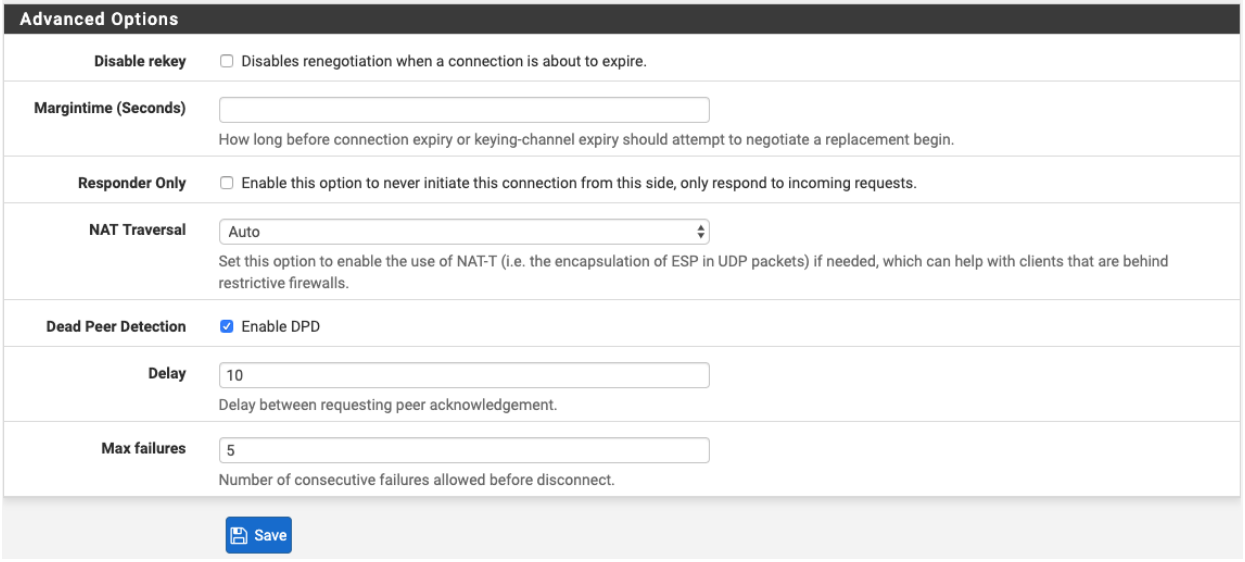
6. In the **Phase 1 Proposal (Encryption Algorithm)** section:



Field	Enter
Algorithm	AES
Key Length	256 bits
HASH	SHA256
DH Group	14

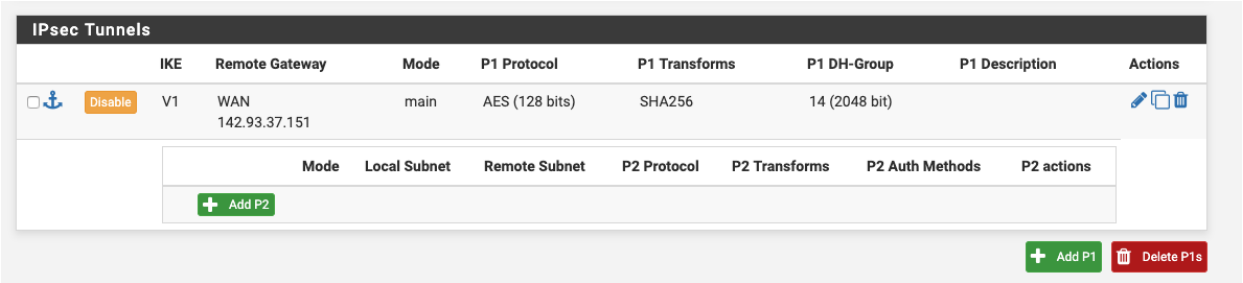
Field	Enter
Lifetime (Seconds)	28800

7. In the **Advanced Options** section:

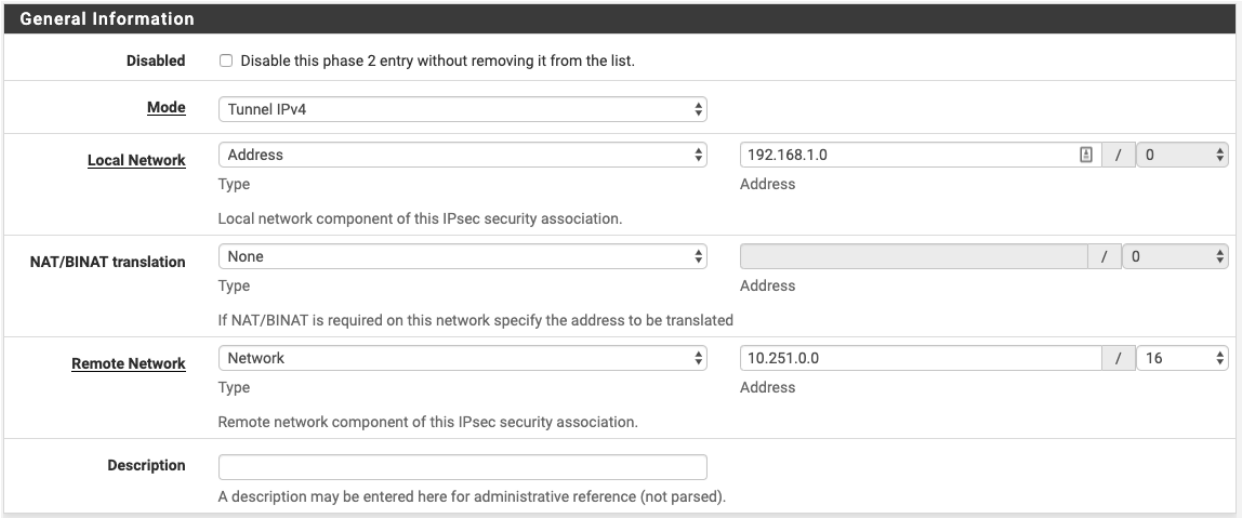


Field	Enter
Disable rekey	Clear
Margintime (Seconds)	Blank
Responder Only	Clear
NAT Traversal	Auto
Dead Peer Detection	Select
Delay	10
Max failures	5

8. Click **Save**.
9. Click **+Add P2**.

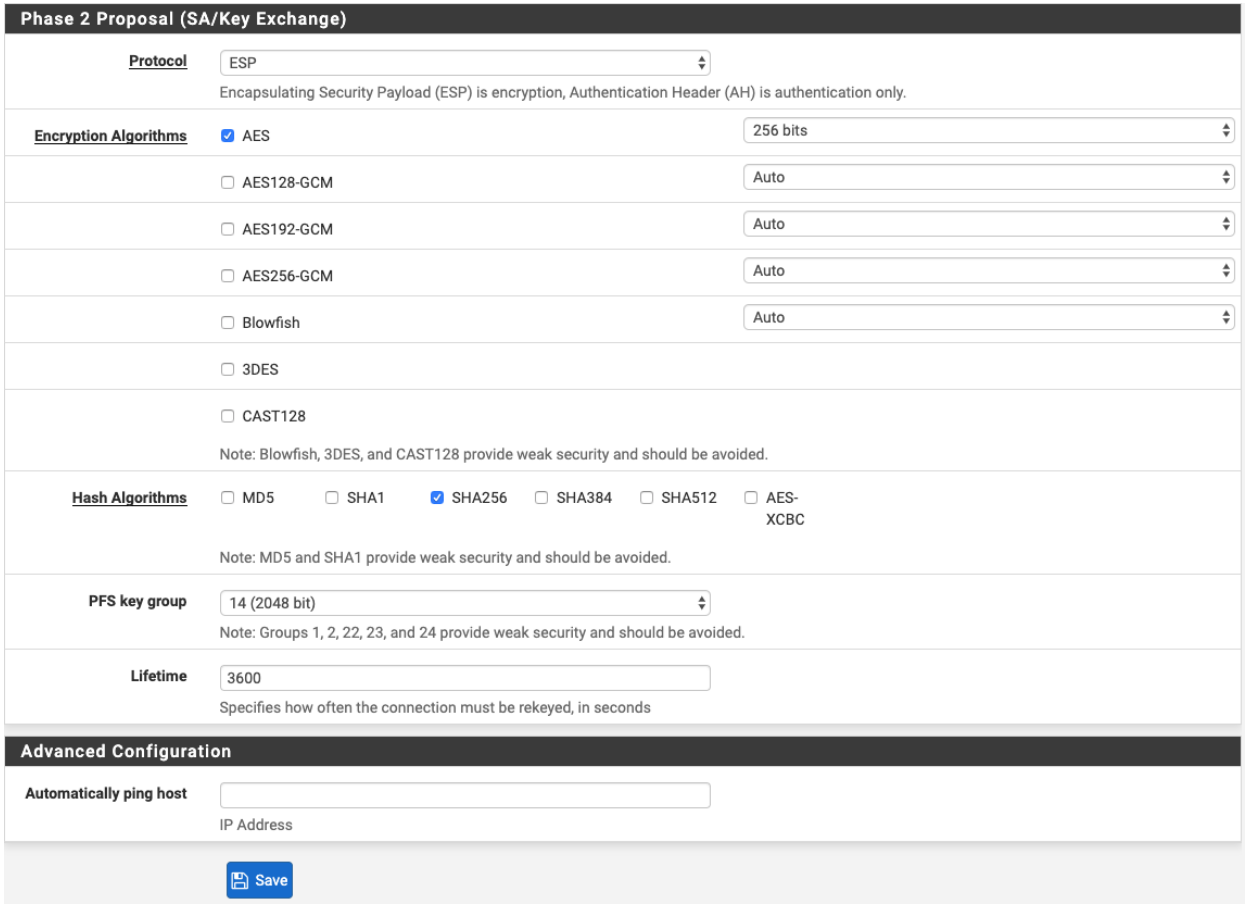


10. In the **General Information** section:



Field	Enter
Mode	Tunnel IPv4
Local Network Type	Network
Local Network Address	Your local LAN network subnet.
Remote Network Type	Network
Remote Network Address	Check Point SASE remote network subnet.

11. In the **Phase 2 Proposal (SA/Key Exchange)** section:

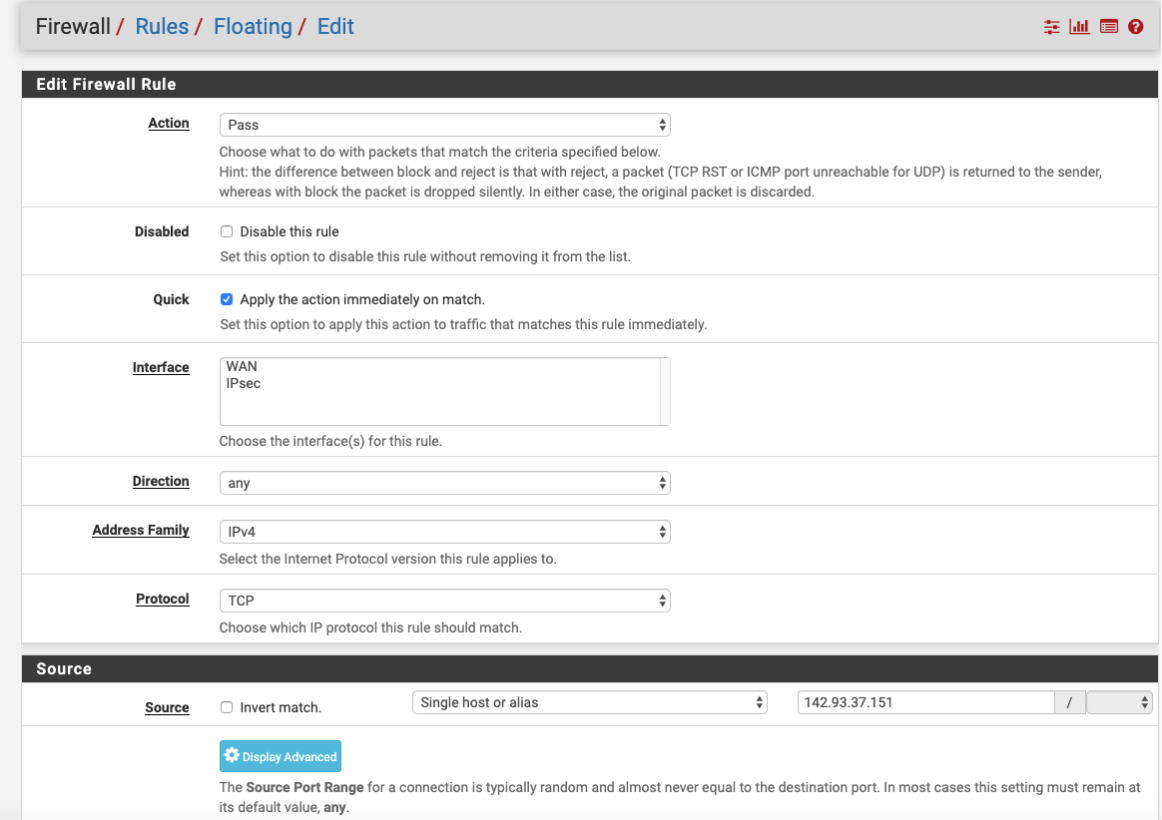


Field	Enter
Protocol	ESP
Encryption Algorithm	AES 256 bits
Hash Algorithm	SHA256
PFS Key Group	14

12. Click **Save**.
13. (Optional) Configure firewall rules:

a. Go to **Firewall > Rules**.

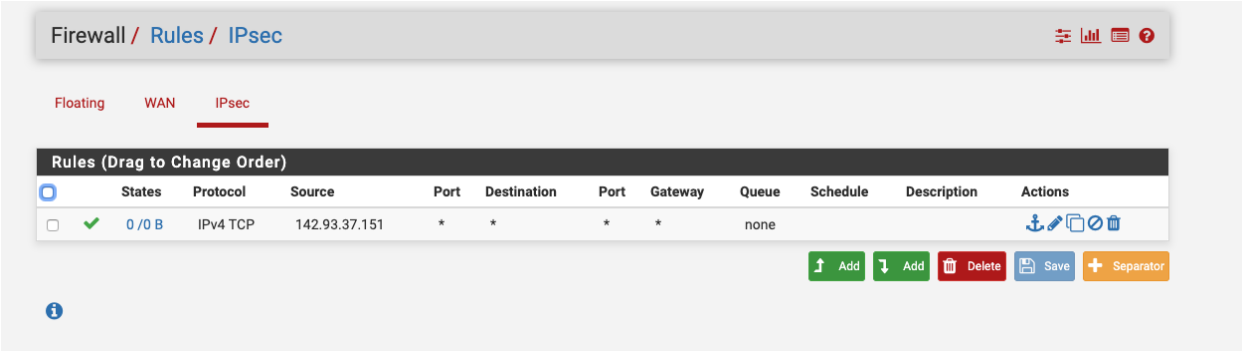
b. Under **IPSEC**, add a new rule:



Field	Enter
Action	Pass
Quick	Mark v
Interface	WAN and IPSEC
Source	Public IP address of Check Point SASE gateway
Destination	Any or an external IP address.

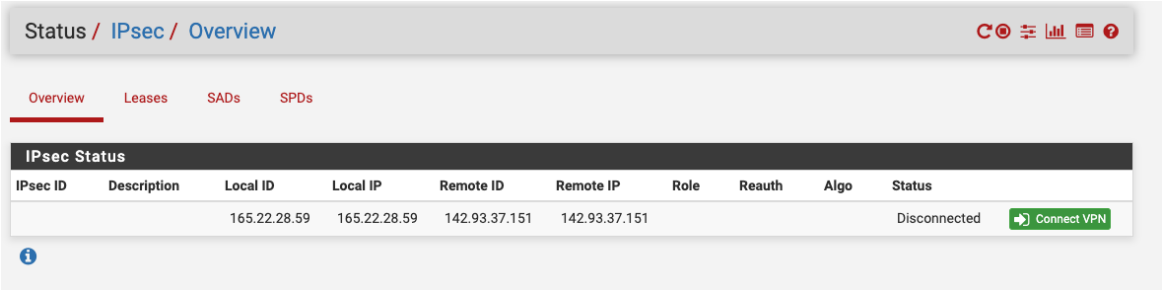
c. Click **Save**.

14. Under **IPSEC**, add a new rule:



Field	Enter
Action	Pass
Source	Public IP address of Check Point SASE gateway
Destination	Any or an external IP address.

15. Click **Save**.
16. Click **Apply Changes**.
17. Activate the tunnel:
    a. From the **Menu Bar**, click **Status > IPsec**.

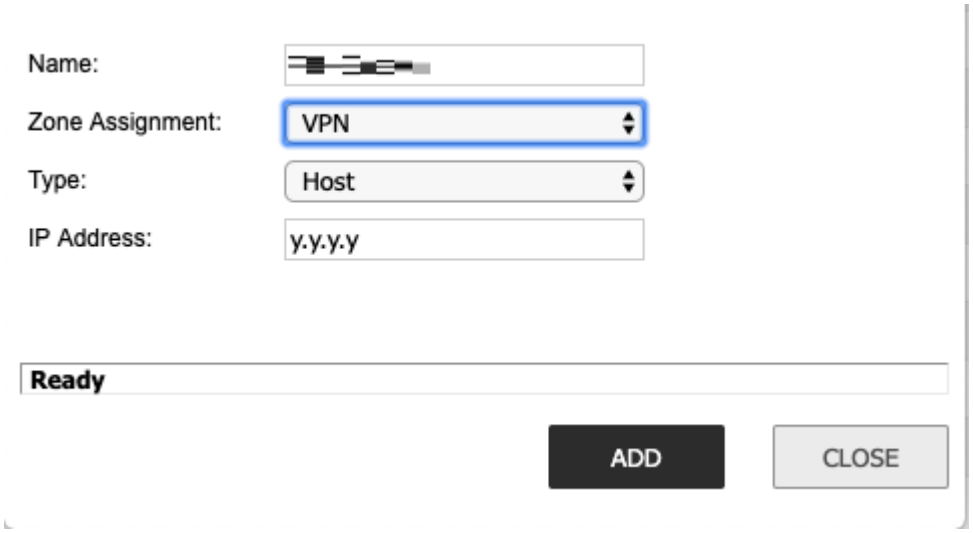


    b. Click **Connect VPN** for the tunnel to Check Point SASE gateway.

SonicWall Firewall

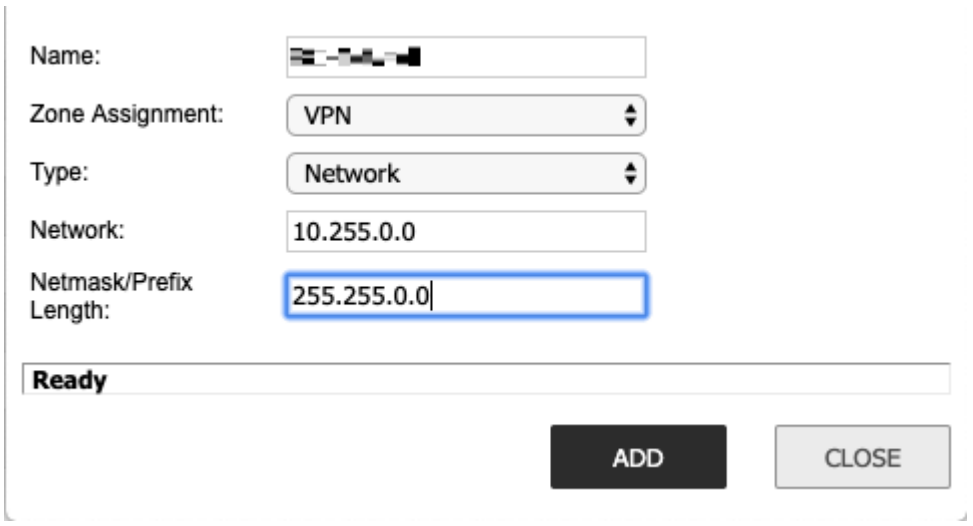
To configure the tunnel in the SonicWall Management Portal:

1. Log in to the SonicWall Management Portal with the Administrator account.
2. Go to **Objects > Address Objects**.
3. Add a gateway object:



Field	Enter
Name	Name for the gateway object.
Zone Assignment	VPN
Type	Host
IP Address	Public IP address of Check Point SASE gateway.

4. Click **Add**.
5. Add a network object:



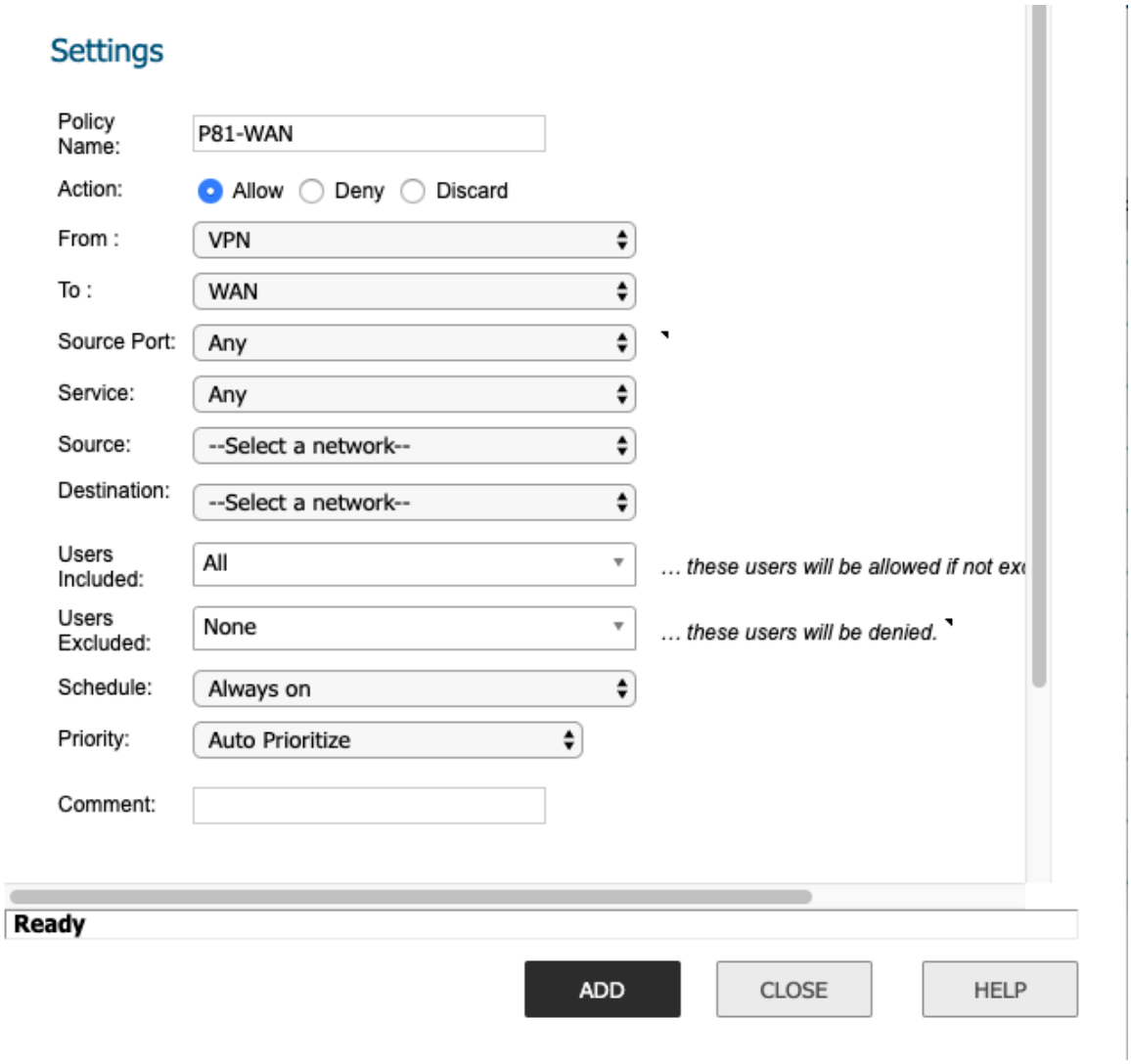
Field	Enter
Name	Name for the network object.
Zone Assignment	VPN
Type	Host
Network	Public IP address of Check Point SASE gateway.
Netmask/Prefix length	Check Point SASE subnet mask (255.255.255.0)

6. Click **Add**.
7. Configure firewall policies from VPN to WAN:

a. Go to **Policy > Rules**.

b. Click **Add**.

The **Settings** window appears.



c. Enter these:

Field	Enter
Policy Name	Name for the firewall policy.
Action	Allow
From	VPN
To	WAN
Source Port	Any
Service	Any
Source	Check Point SASE gateway object.
Destination	Your external internet interface object.

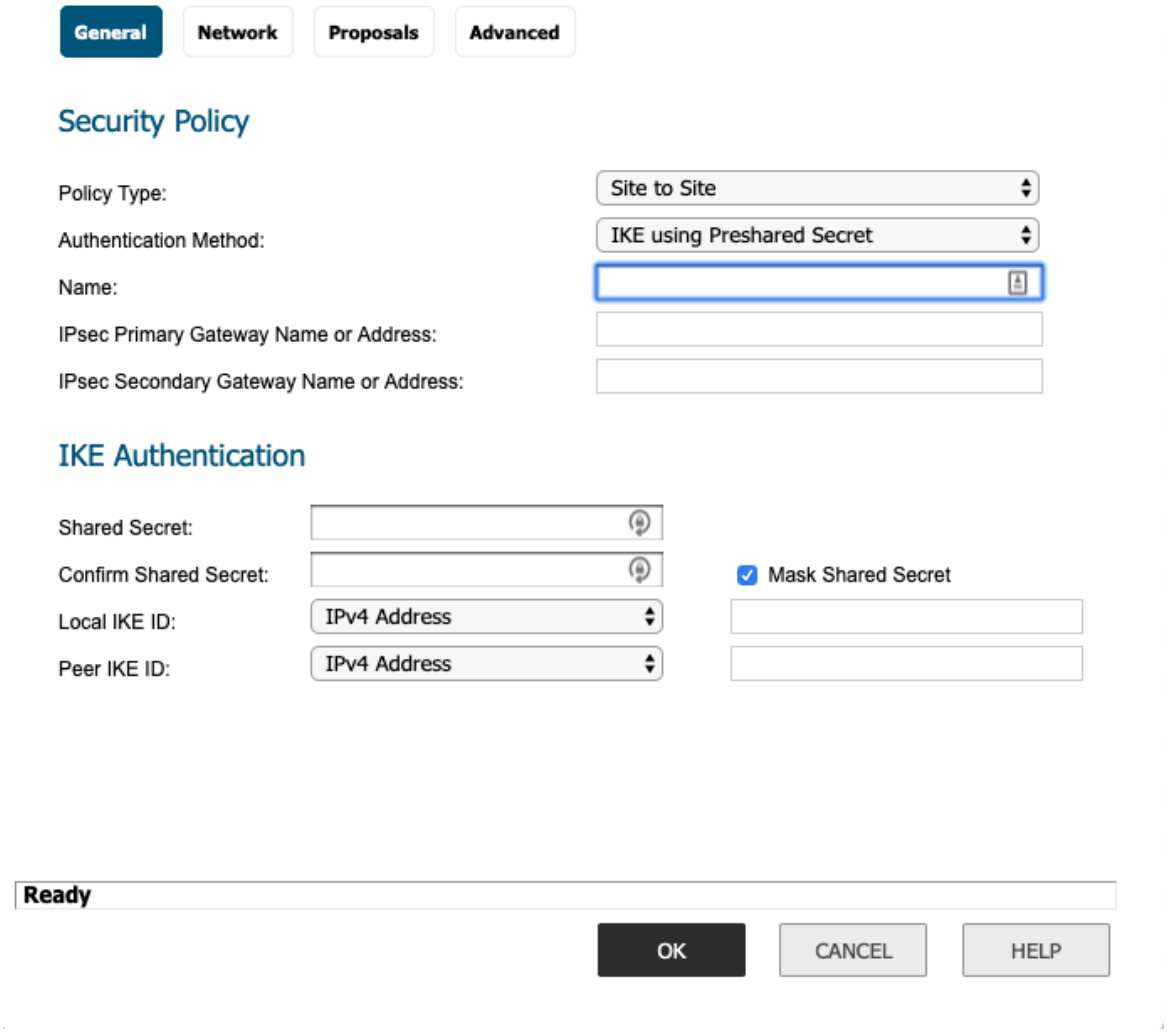
d. Click **Add**.

8. Create a site-to-site connection:

a. Click **VPN**.

b. In the **Base Settings** section, click **VPN Policy**.

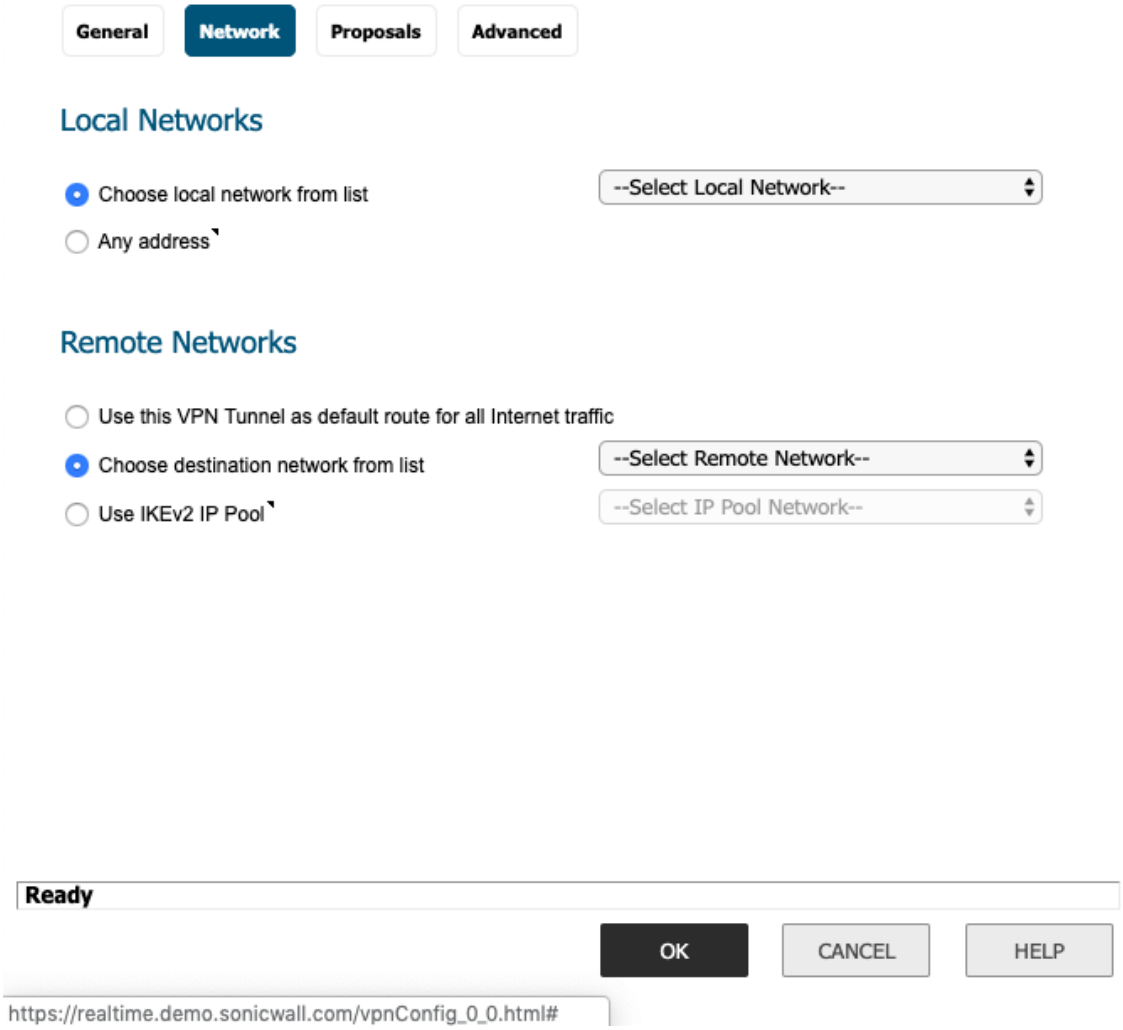
c. In the **General** tab, enter these:



Field	Enter
Security Policy	
Policy Type	Site to Site
Authentication Method	IKE using Preshared Secret
Name	Name for the site-to-site connection.
IPsec primary Gateway Name or Address	Public IP address of Check Point SASE gateway.

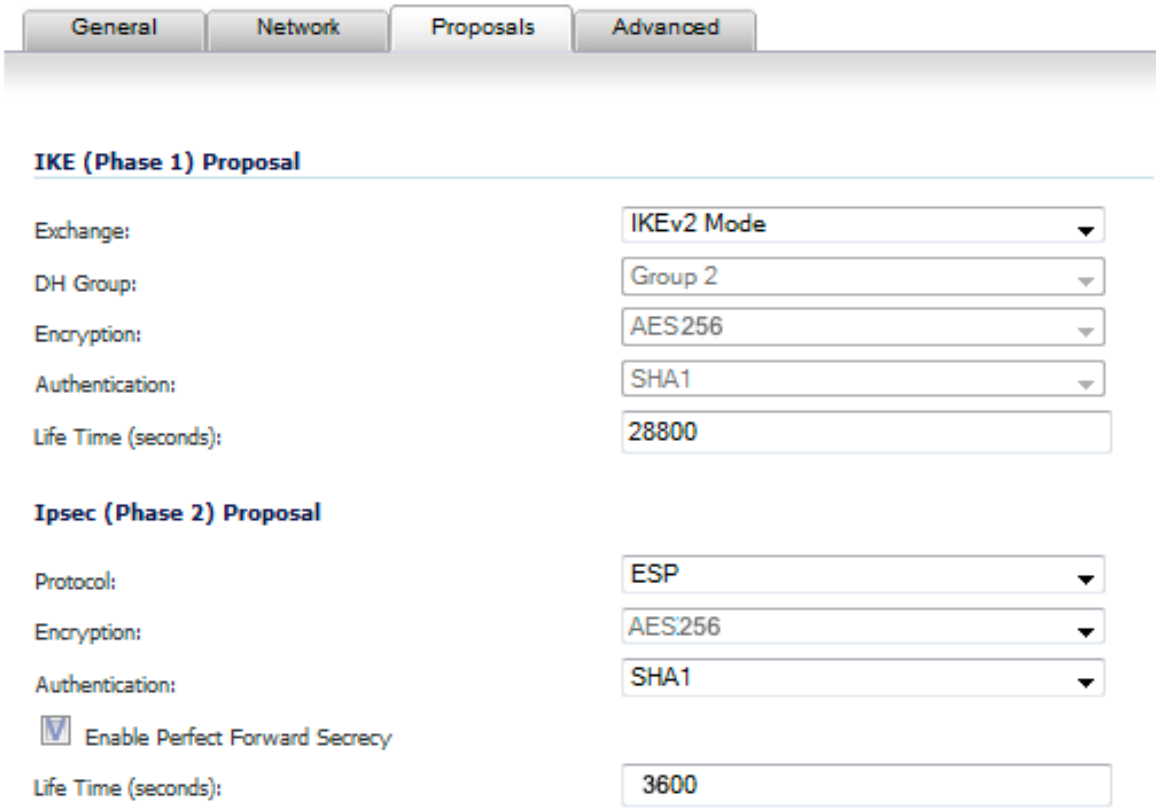
Field	Enter
IPsec Secondary Gateway Name or Address	Blank
Service	Any
Source	Check Point SASE gateway object.
Destination	Your external internet interface object.
IKE Authentication	
Shared Secret	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.
Confirm Secret	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.
Local IKE ID	IPv4 Address and your local external internet address.
Peer IKE ID	IPv4 Address and the public IP address of Check Point SASE gateway.

d. In the **Network** tab, enter these:



Field	Enter
Local Networks	
Choose a local network from the list	Your local LAN network.
IKE Authentication	
Choose destination network from the list	Check Point SASE network object.

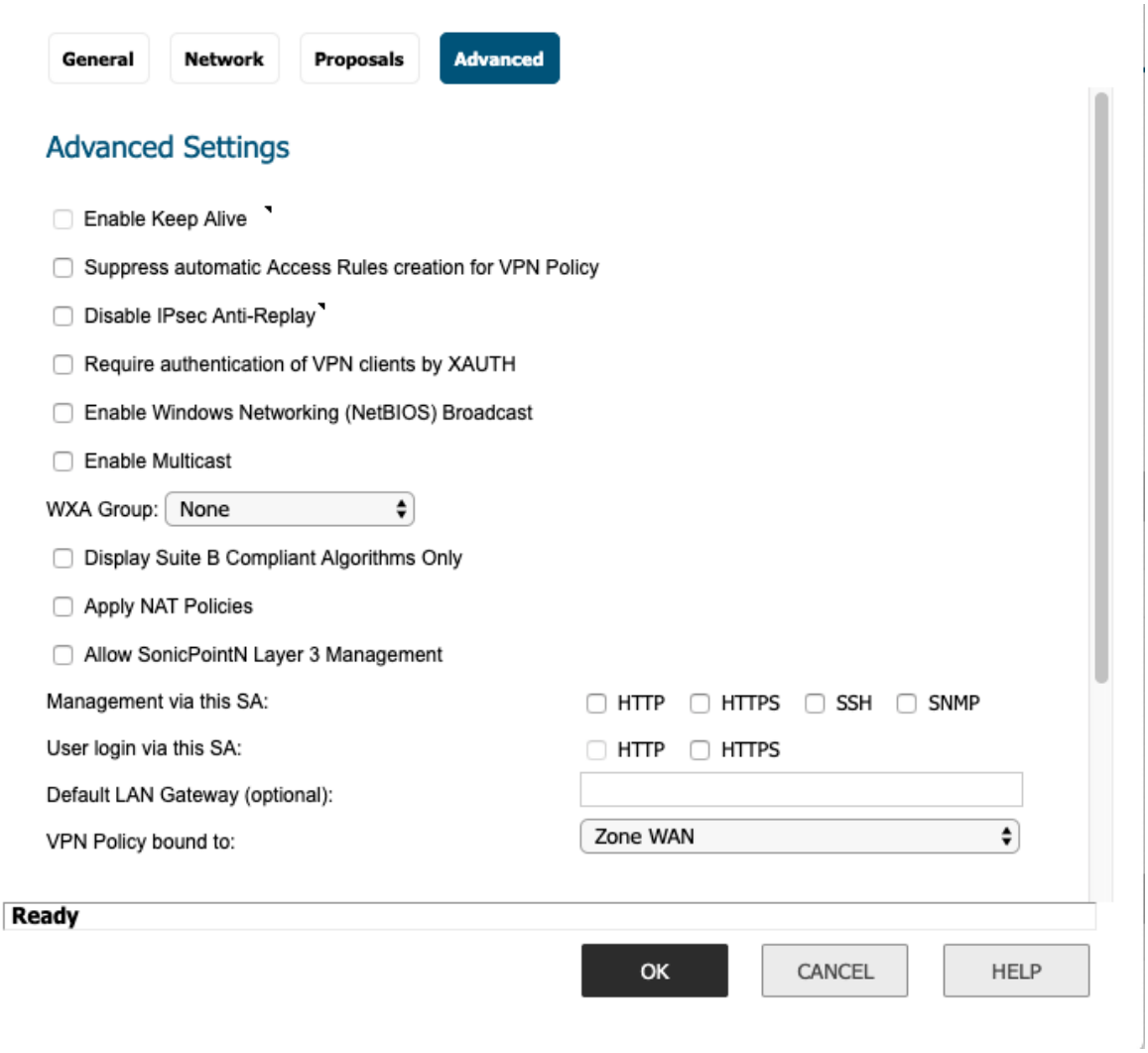
e. In the **Proposals** tab, enter these:



Field	Enter
IKE (Phase 1) Proposal	
Exchange	IKEv2 Mode
DH Group	Group 2
Encryption	AES-256
Authentication	SHA1
Life Time (seconds)	28800
IKE (Phase 2) Proposal	
Protocol	ESP
Encryption	AES-256
Authentication	SHA1

Field	Enter
Enable Perfect Forward Security	Select
DH Group	Group 2
Life Time (seconds)	3600

f. In the **Advanced Settings** tab, select the **Enable Keep Alive** checkbox.



g. Click **OK**.

h. Make sure the change is committed to SonicWall. In the **VPN Policies** screen, make sure that the new VPN policy is enabled.

You can select the **Play** (►) button to the right of the **Currently Active VPN Tunnels** to view whether the tunnel is up or not.

If the tunnel is not up, navigate to the **Event Logs** and check the logs for errors in the new VPN policy.

Sophos XG Firewall

To configure the tunnel in the Sophos XG Management Portal:

1. Log in to the Sophos XG Management Portal with the Administrator account.
2. Add a local and remote LAN object:
   a. Go to **Hosts and Services > IP Host**, click **Add** and enter these:

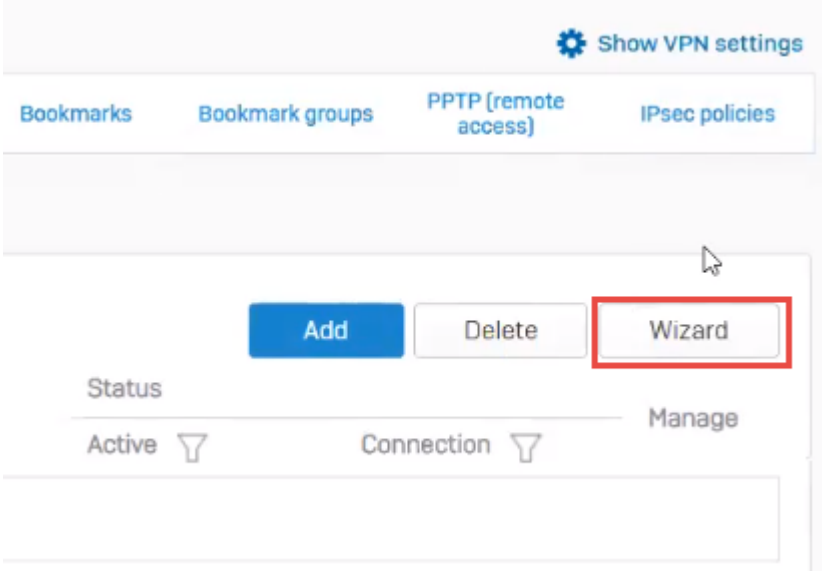
Field	Enter
Name	Name for the object.
IP Family	IPv4
Type	Network
IP Address	Your local network and subnet.

   b. Repeat step a to add a remote LAN object:

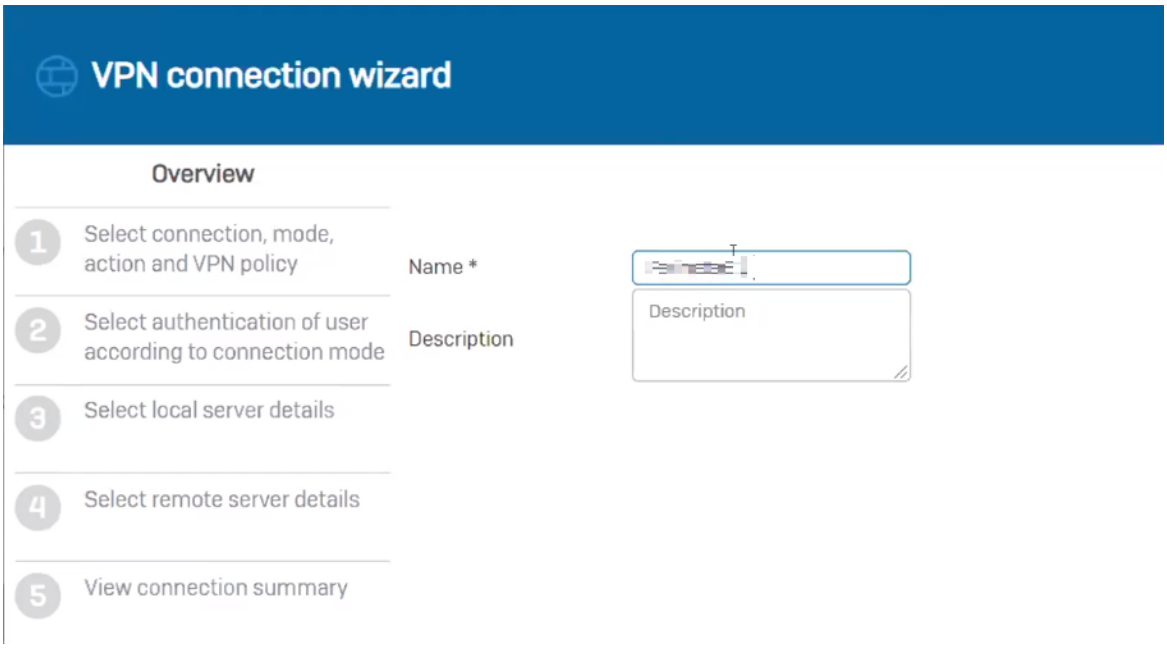
Field	Enter
Name	Name for the object.
IP Family	IPv4
Type	Network
IP Address	Your remote network and subnet.

3. Create an IPsec VPN connection:

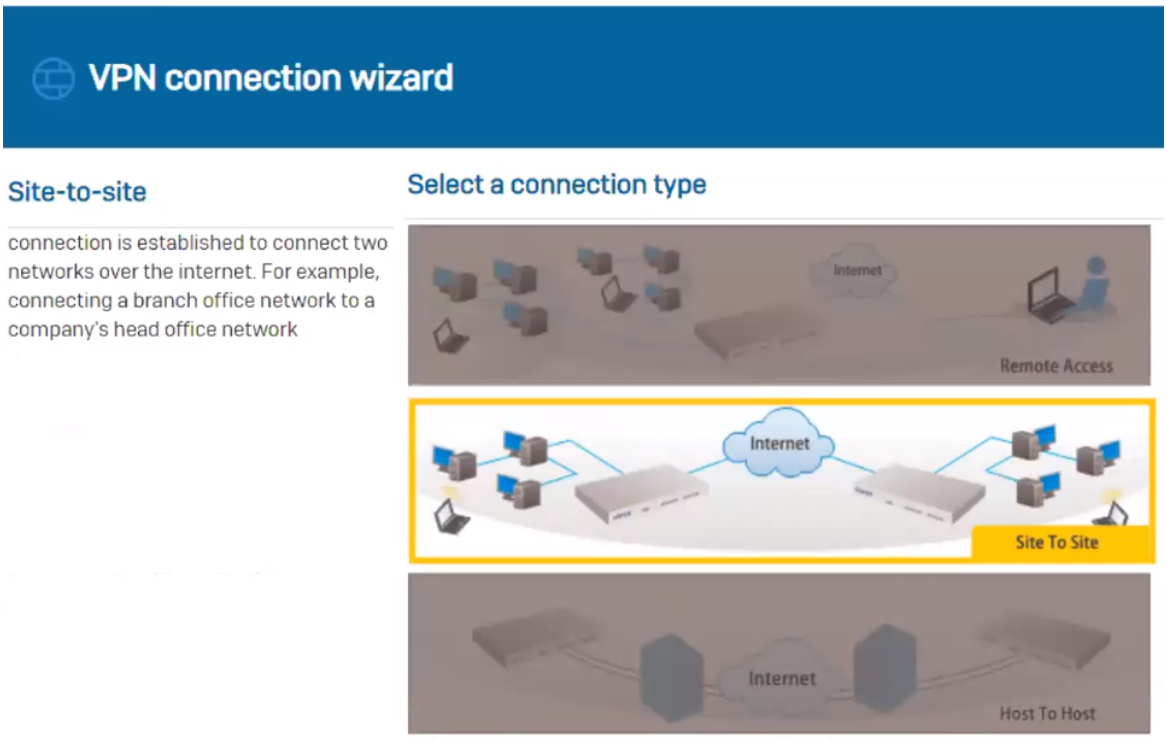
a. Go to **VPN > IPsec Connections** and select **Wizard**.



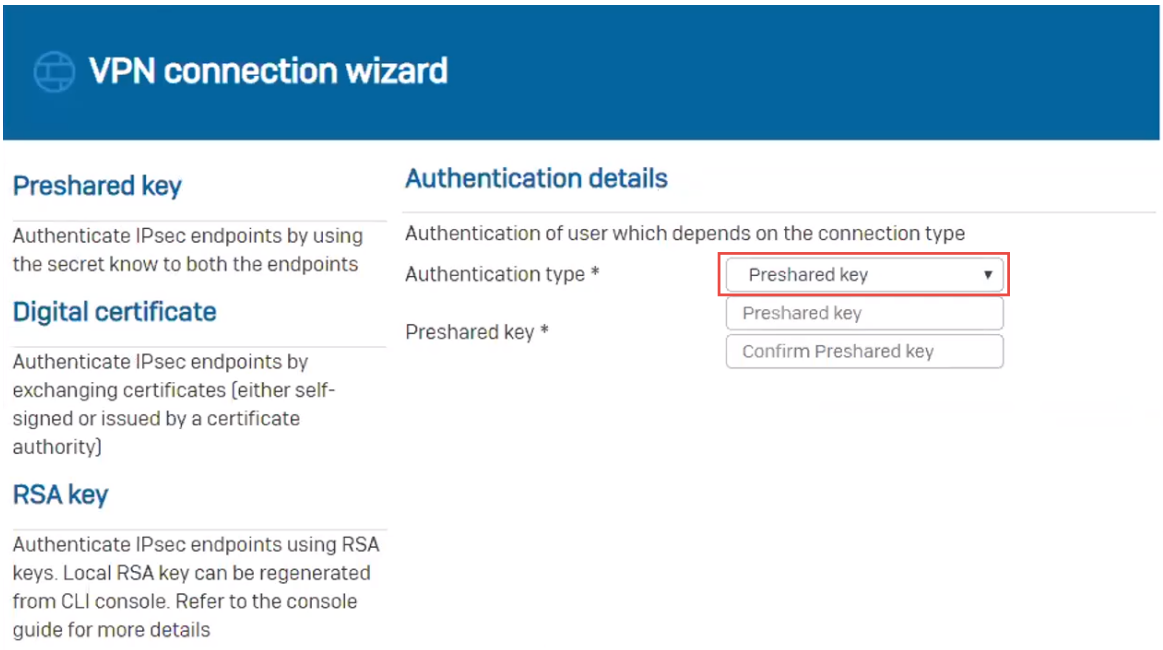
b. In the **Name** field, enter a name for the connection, and click **Start**.



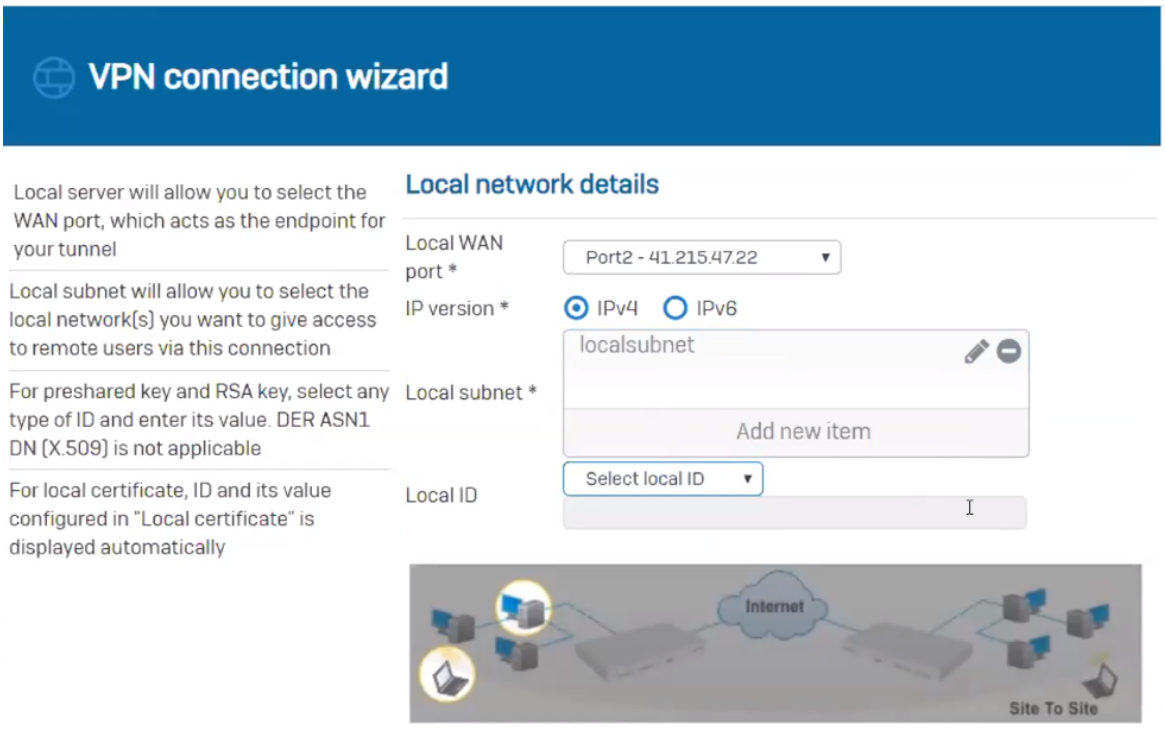
c. For **Select a connection type**, select **Site To Site** and select **Head Office**.



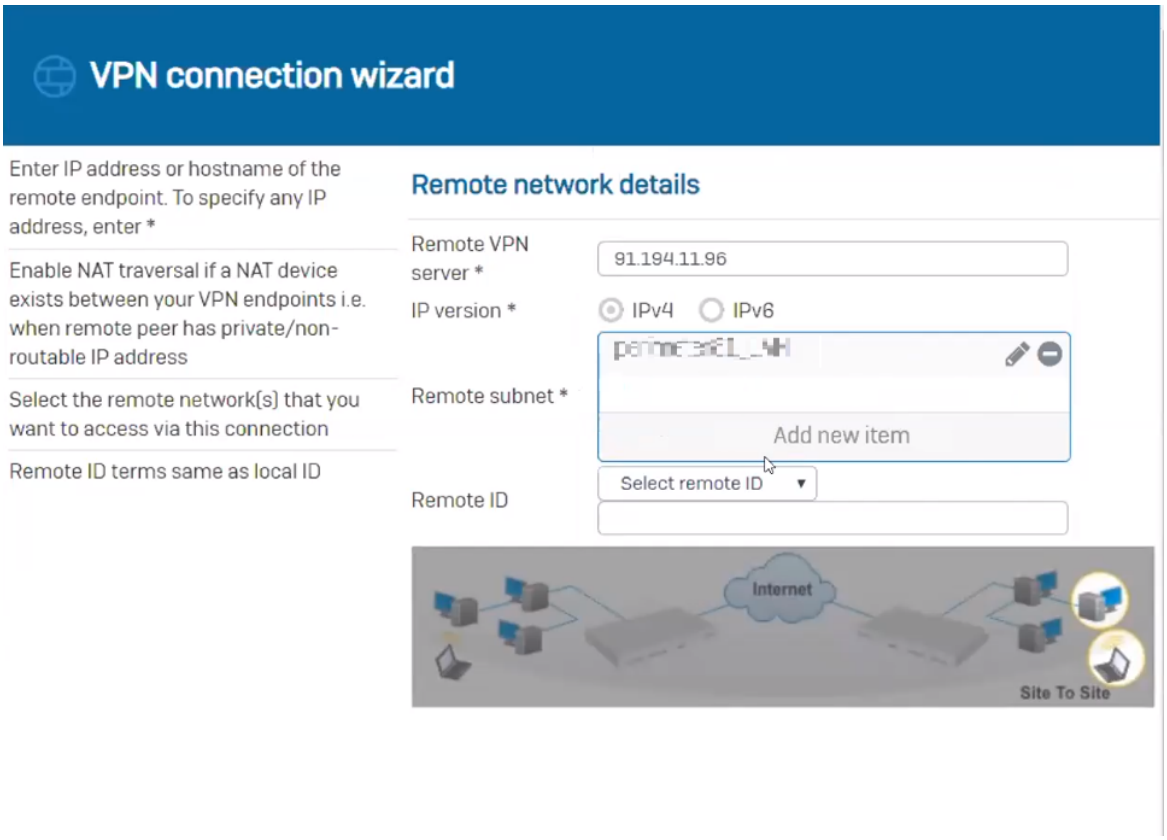
d. From the **Authentication type** list, select **Preshared key**.



e. In the **Local subnet** field, enter the local LAN created earlier in the procedure.



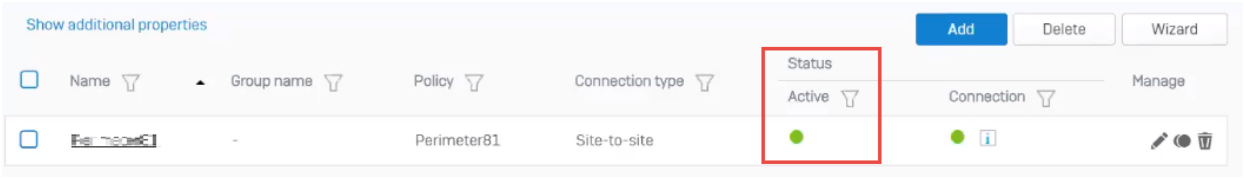
f. In the **Remote subnet** field, enter the remote LAN created earlier in the procedure.



g. From the **User Authentication** list, select **Disabled**.

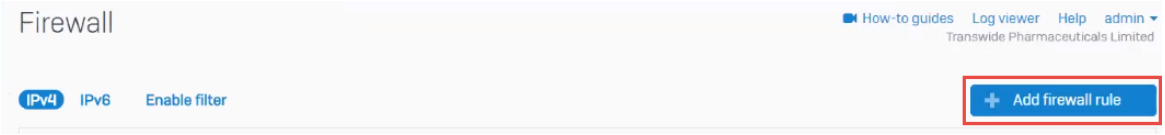
h. Review the IPSec connection summary and click **Finish**.

4. Set **Status** to **Active**.

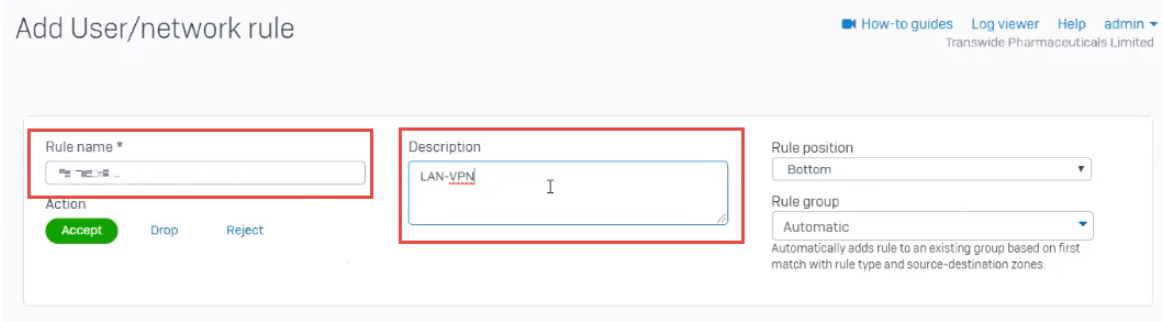


5. Add two firewall rules to allow the VPN traffic:

a. Click **Firewall** and click **Add Firewall Rule**.

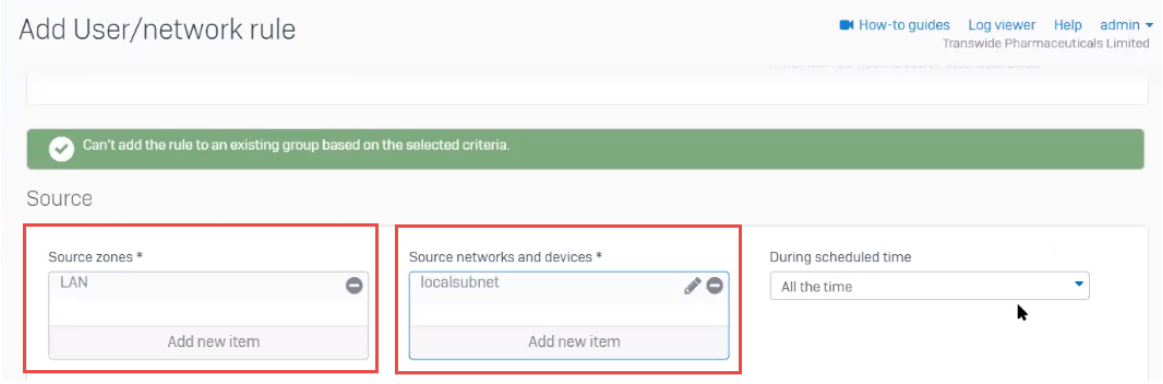


b. In the **Name** field, enter a name for the rule.



c. In the **Description** field, enter **LAN-VPN**.

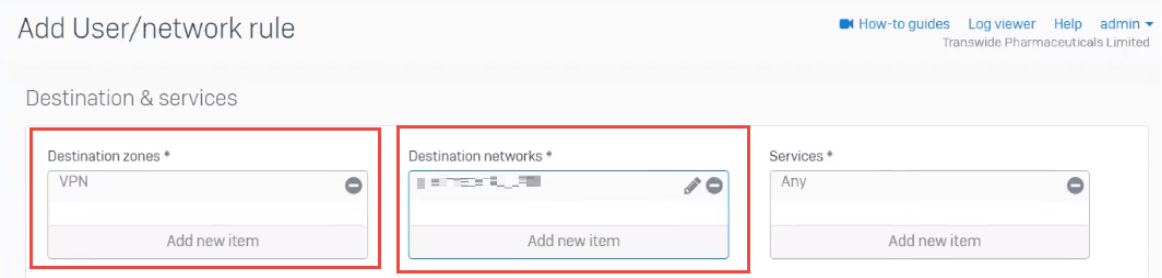
d. In the **Source** section:



i. In the **Source zones** field, enter **LAN**.

ii. In the **Source network and devices** field, enter **local subnet**.

e. In the **Destination &services** section:



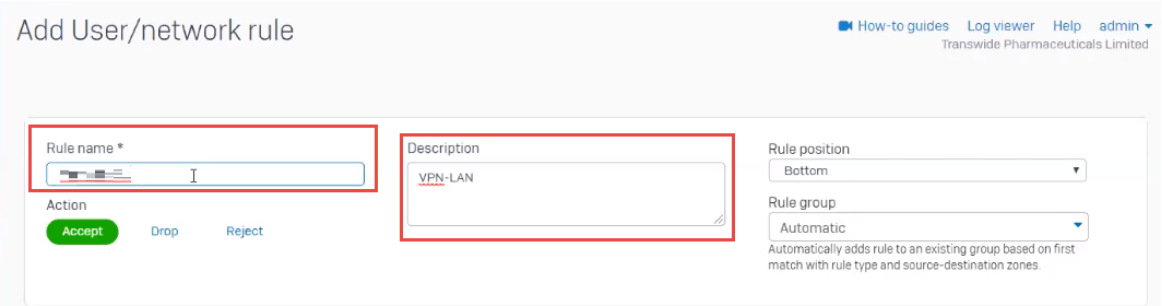
i. In the **Destination zones** field, enter **VPN**.

ii. In the **Destination networks** field, enter **Check Point SASE_LAN**.

f. Click **Save**.

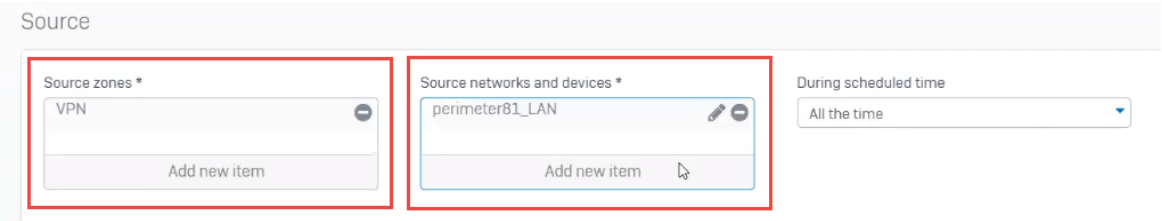
g. Add the second firewall, click **Firewall** and click **Add Firewall Rule**.

h. In the **Name** field, enter a name for the rule.



i. In the **Description** field, enter **VPN-LAN**.

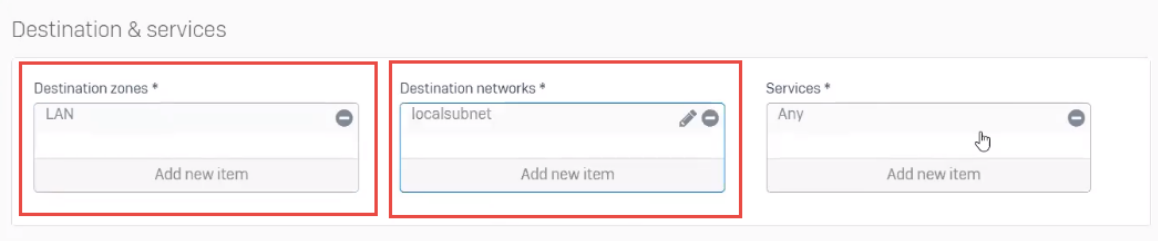
j. In the **Source** section:



i. In the **Source zones** field, enter **VPN**.

ii. In the **Source network and devices** field, enter **Check Point SASE_LAN**.

k. In the **Destination &services** section:



i. In the **Destination zones** field, enter **LAN**.

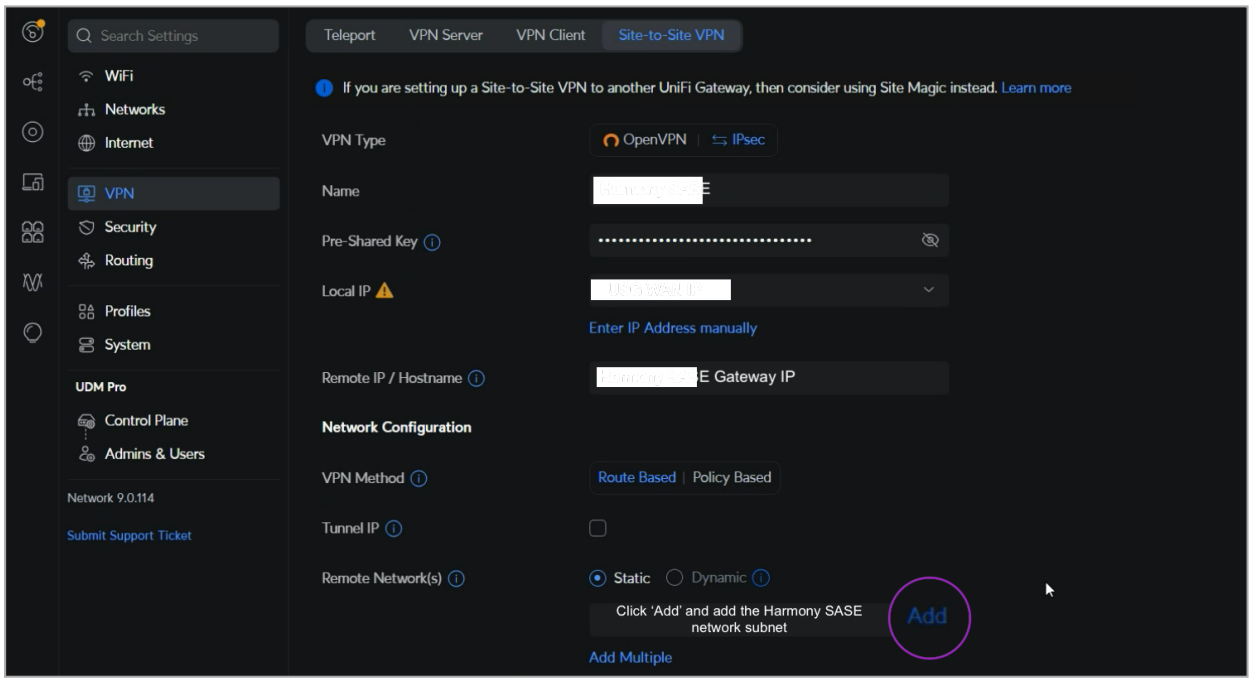
ii. In the **Destination networks** field, enter **local subnet**.

l. Click **Save**.

UniFi USG Firewall

To configure the tunnel in the UniFi USG Management Portal:

1. Log in to the UniFi USG Management Portal with the Administrator account.
2. Click **VPN**, and then click the **Site-to-Site VPN** tab.

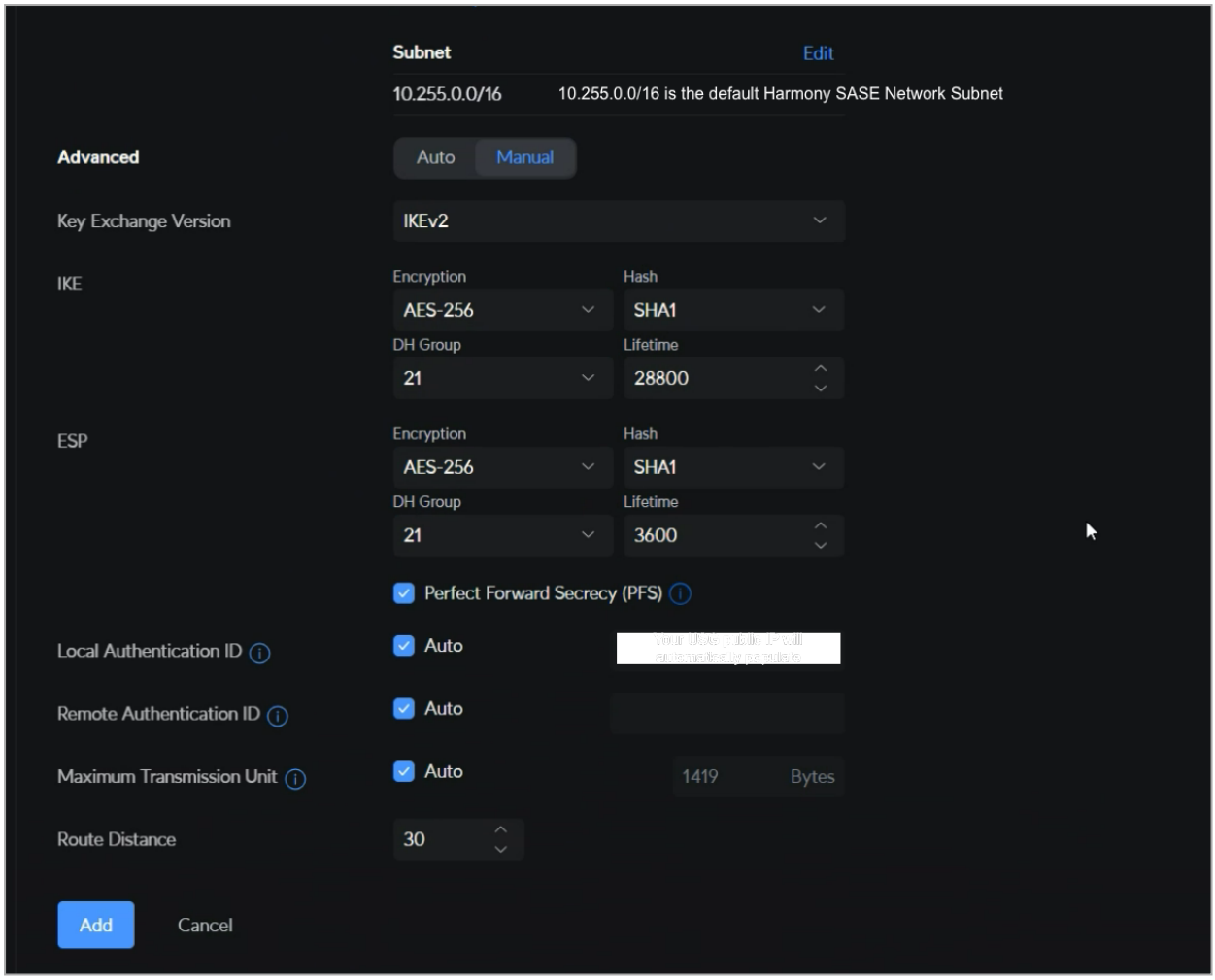


3. Specify these:

Field	Enter
VPN Type	IPsec

Field	Enter
Name	Name for the network.
Pre-shared key	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.
Local IP	Public IP address of the UniFi USG firewall.
Remote IP / Hostname	Check Point SASE gateway IP.
VPN Method	Route Based
Remote Network(s)	Static

4. Click **Add**.
5. In the **Subnet** field, click **Edit** to enter the Check Point SASE network subnet. The default value is `10.255.0.0/16`.
6. In the **Advanced** section, select **Manual** and specify these:



Field	Enter
Key Exchange version	IKEv2
IKE	
Encryption	AES-256
Hash	SHA1
DH Group	21
Lifetime	28800
ESP	
Encryption	AES-256

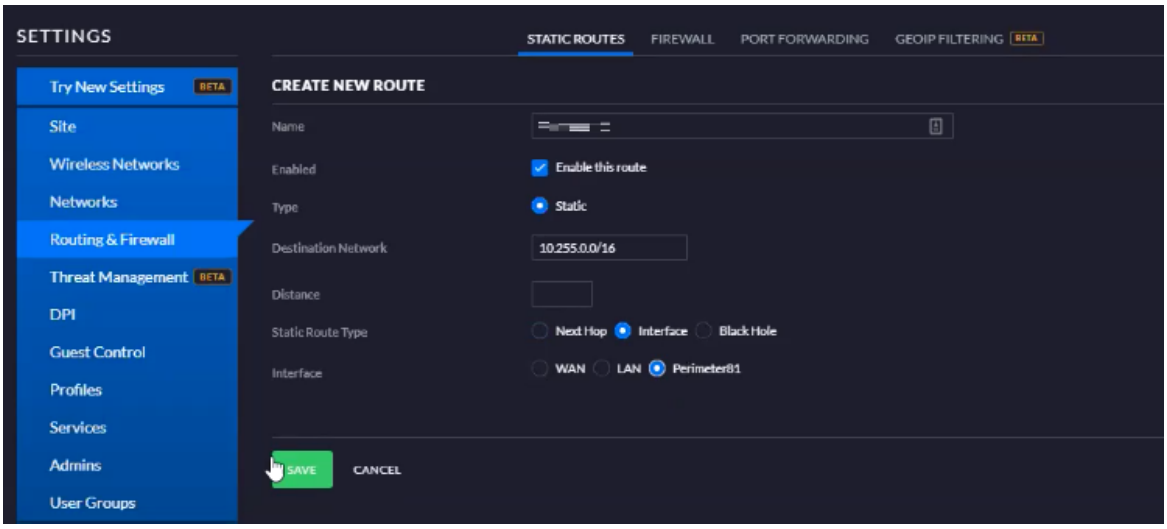
Field	Enter
Hash	SHA1
DH Group	21
Lifetime	3600
Perfect Forward Secrecy (PFS)	Enable
Local Authentication ID	Select Auto
Remote Authentication ID	Select Auto
Maximum Transmission Unit	Select Auto
Route Distance	Set a distance

7. Click **Add**.

   To create a Route-Based IPSEC Site-to-Site connection between Check Point SASE and your Ubiquiti network:
   a. Set **Dynamic Routing** to **Enable** .
   b. Add any other subnet specified in **Remote Subnets** and make sure that a reverse traffic route is created under **Static Routes** in the UniFi USG firewall for each connected subnet to route through the Check Point SASE Interface.
   c. In the Check Point SASEAdministrator Portal, change **Check Point SASE Gateway Proposal Subnets** and **Remote Gateway Proposal Subnets** to **Any (0.0.0.0/0)**.
   d. Create separate static routing in Check Point SASE.

8. Add static routes from Check Point SASE subnet (10.255.0.0/16) to the local network and vice versa through the VPN gateway:

a. Go to **Routing & Firewall > Static Routes > Create New Route**.

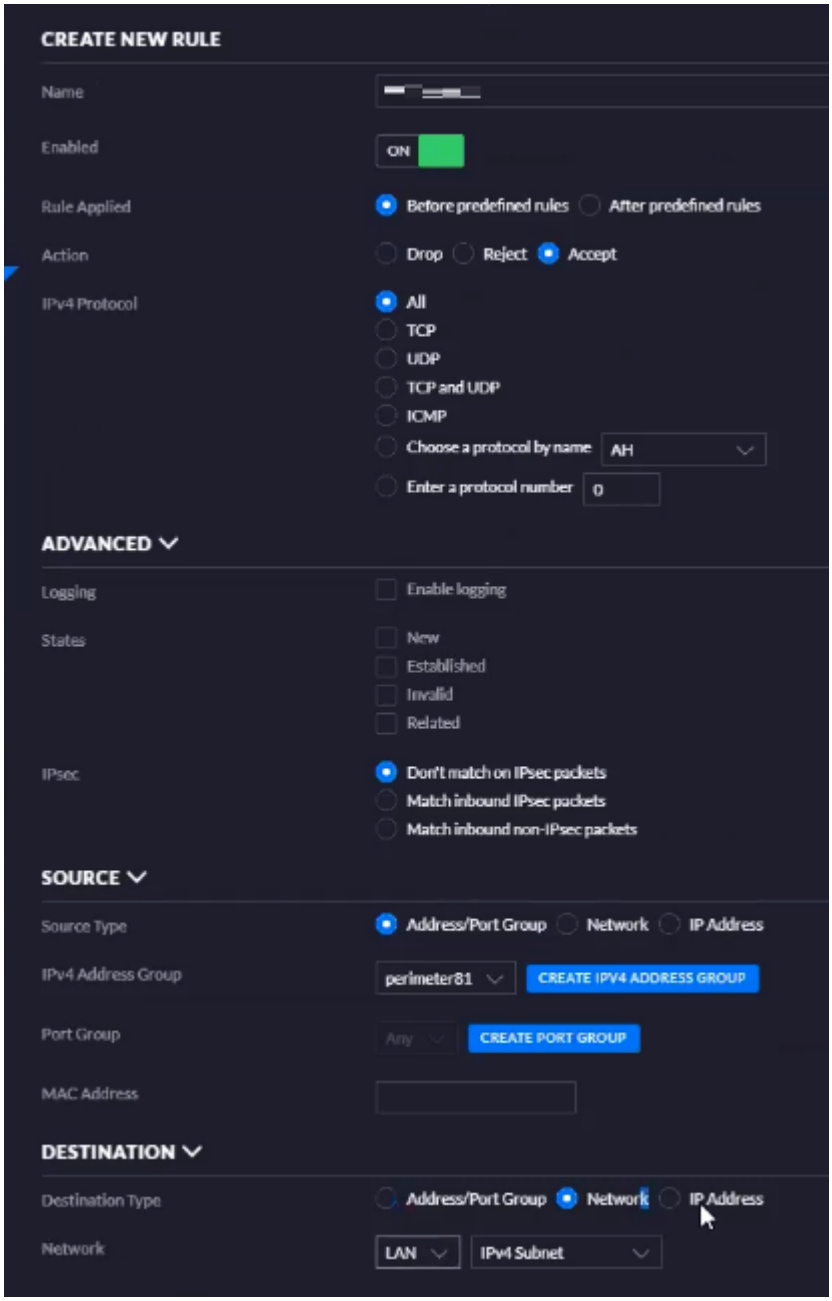


b. Enter these:

Field	Enter
Name	Name for the static route.
Enabled	Select the Enable this route checkbox.
Type	Static
Destination Network	Check Point SASE subnet. The default is 10.255.0.0/16.
Static Route Type	Interface
Interface	Select the interface created in the previous procedure.

c. Click **Save**.

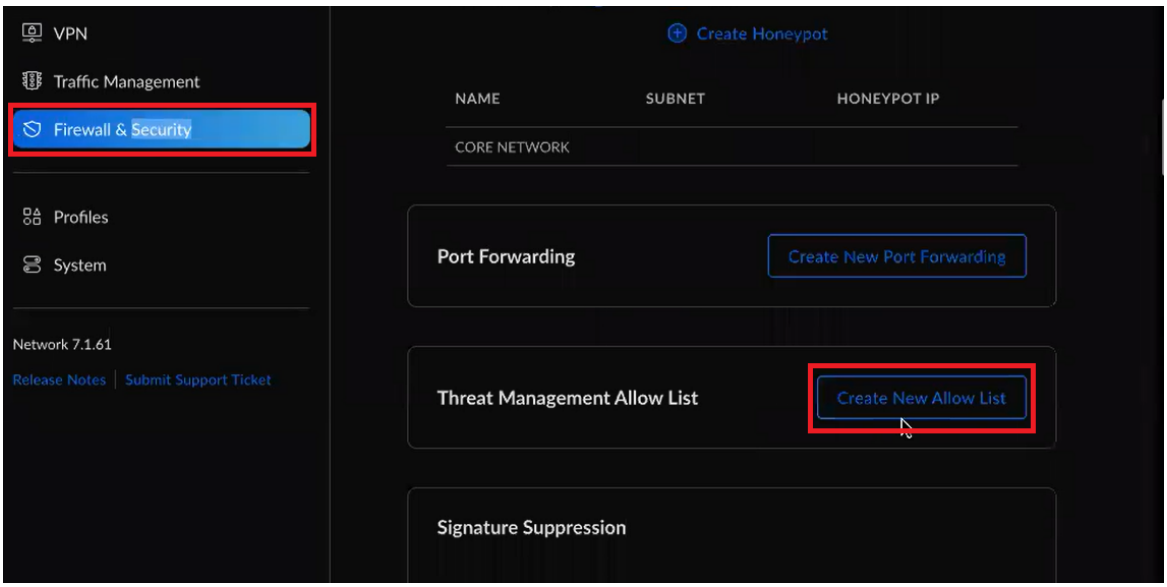
9. Create a firewall rule to allow traffic from Check Point SASE subnet to the LAN network.



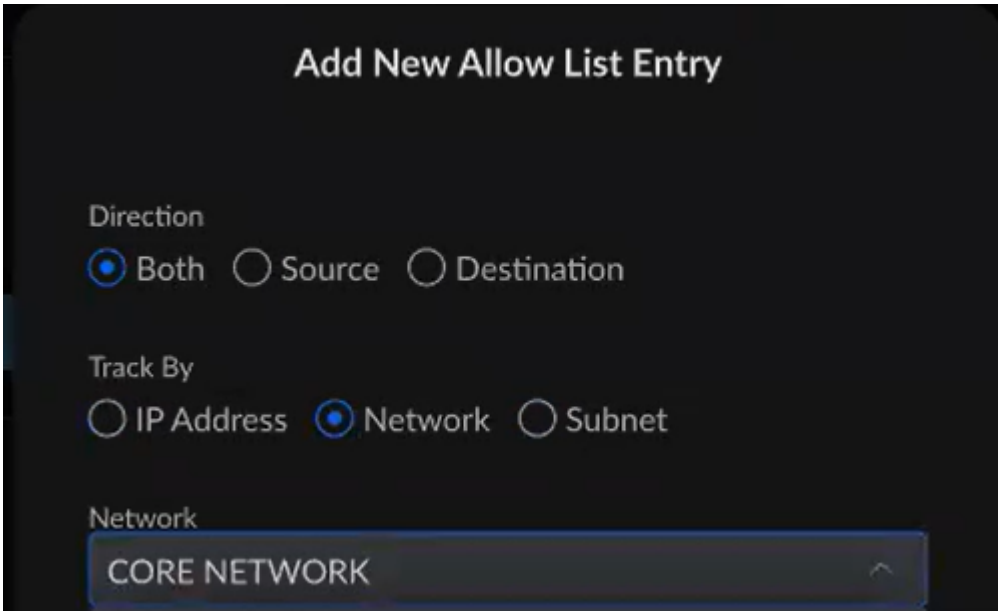
10. If you have enabled IPS/IDS on the UniFi USG firewall, then to establish a tunnel between the Check Point SASE network and UniFi USG firewall version 7 and later, create an exception in your Threat detection system:

a. Click the **Firewall & Security** tab.

b. Click **Create New Allow List**.



c. Select the site-to-site network that you created for this setup.

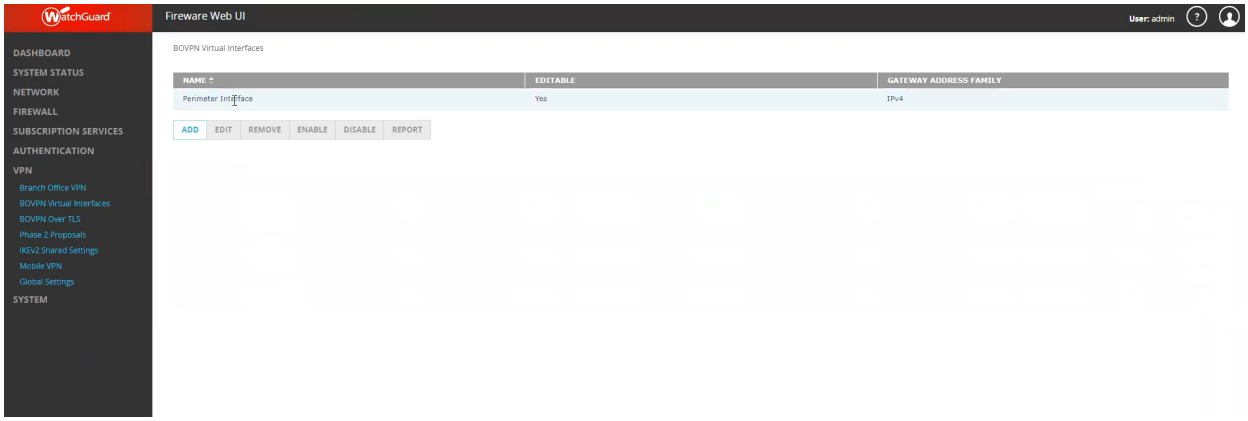


d. Save your changes.

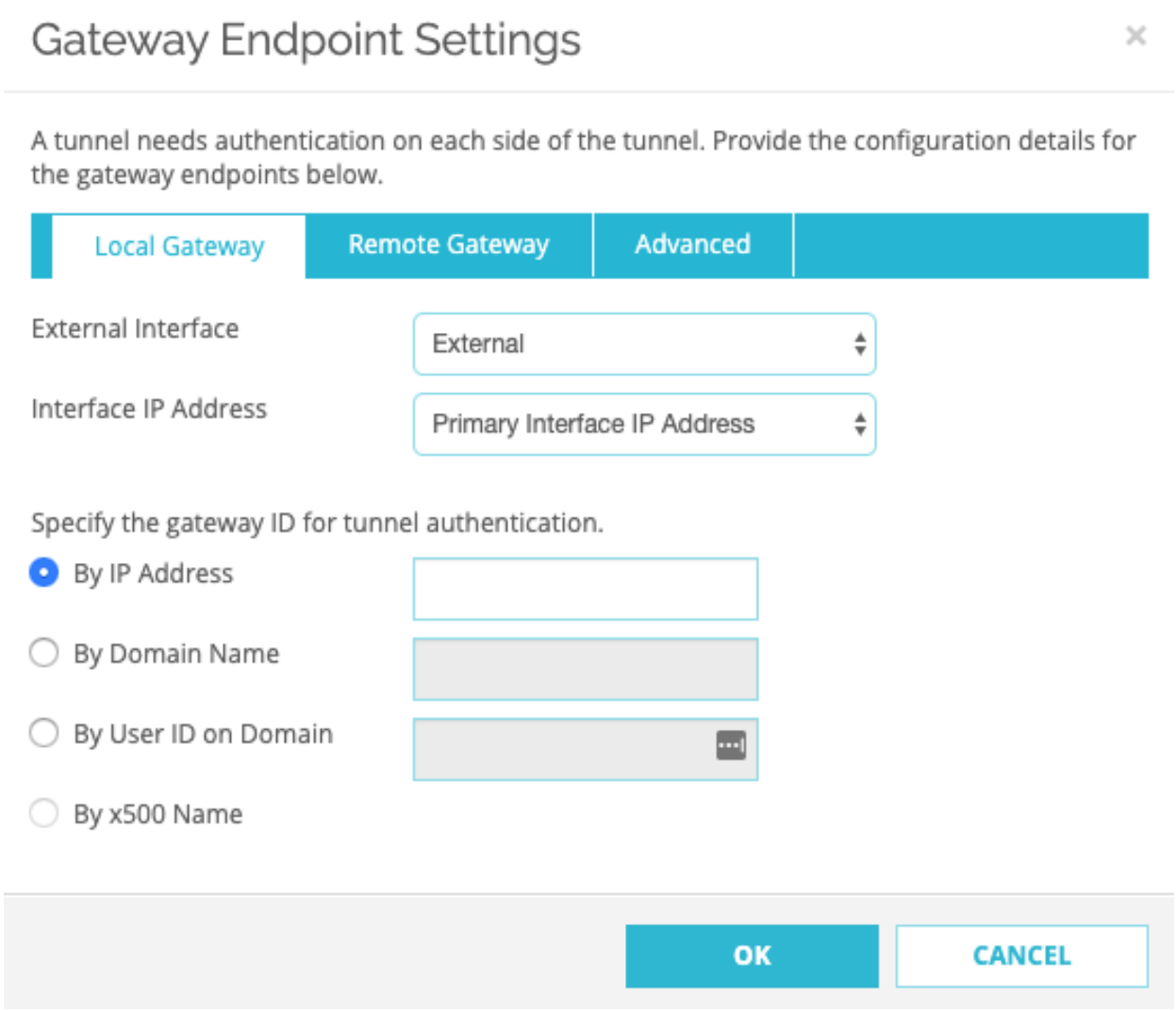
WatchGuard Firewall

To configure the tunnel in the WatchGuard Management Portal:

1. Log in to the WatchGuard Management Portal with the Administrator account.
2. From the left pane, click **VPN > BOVPN Virtual Interfaces**.
3. Click **Add**.



4. In the **Remote Endpoint Type** section, select **Cloud VPN or Third-Party Gateway**.
5. In the **Gateway Address Family** section, select **IPv4 Addresses**.
6. In the **Gateway Settings** section, enter the secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.
7. In the **Local Gateway** tab:

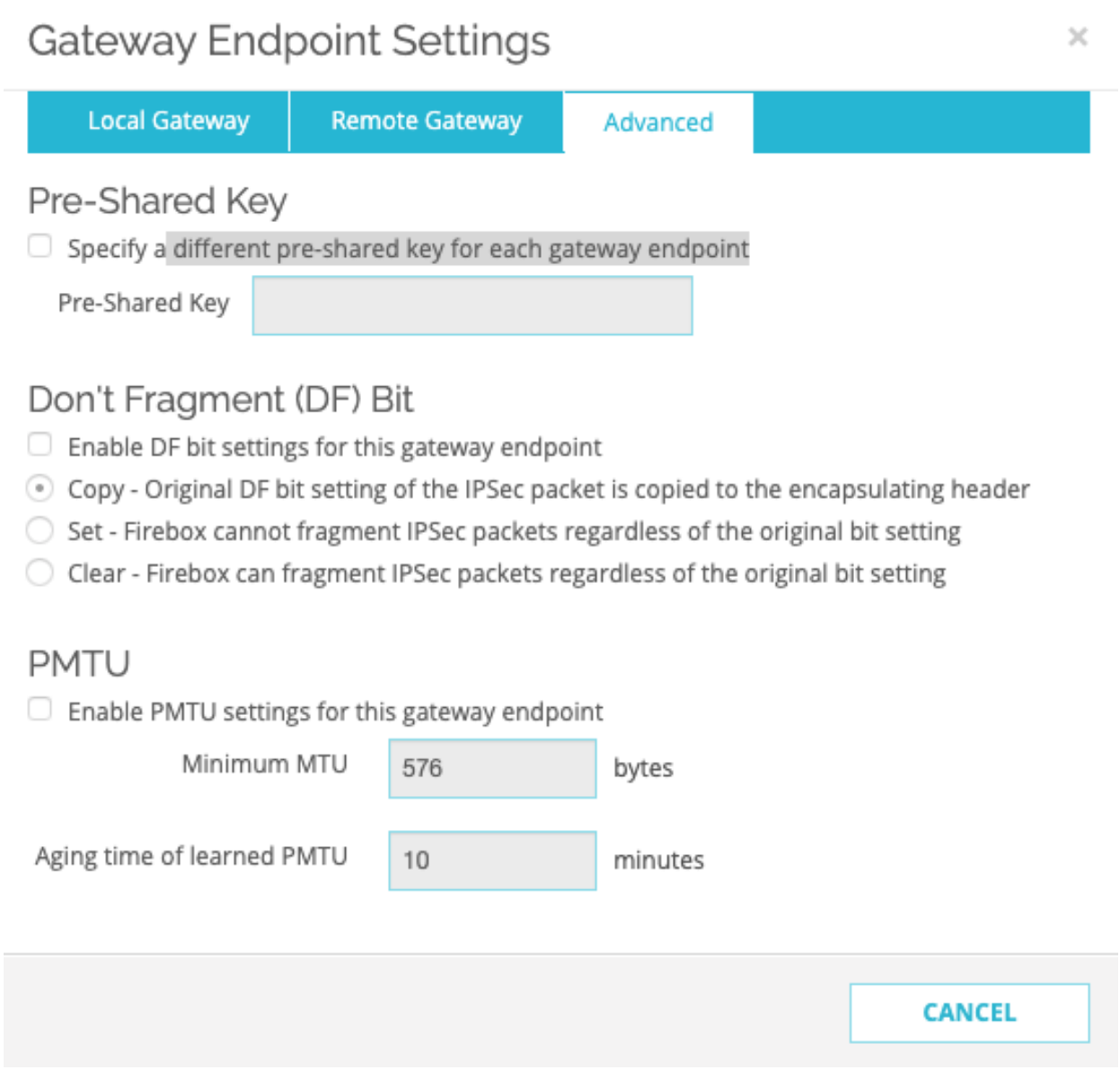


Field	Enter
External Interface	External
Interface IP Address	Primary Interface IP Address
Specify the gateway ID for tunnel authentication	
By IP Address	WatchGuard firewall local IP address.

8. In the **Remote Gateway** tab:

Field	Enter
Static IP Address	WatchGuard firewall IP address.
By IP Address	WatchGuard firewall IP address.

9. In the **Advanced** tab:



Field	Enter
Pre-Shared Key	
Specify a different pre-shared key for each gateway endpoint	Select the checkbox.
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.

Leave rest of the fields with the default values.

10. In the **Phase 1 Settings** tab:

Field	Enter
Version	IKEV2
Mode	Main
NAT Traversal	Select
Keep-alive interval	Select
IKE Keep-alive	30 seconds
Message Interval	30 seconds
Max failures	5
Dead Peer Detection (RFC3706)	Select
Traffic idle timeout	20 seconds
Max retries	5

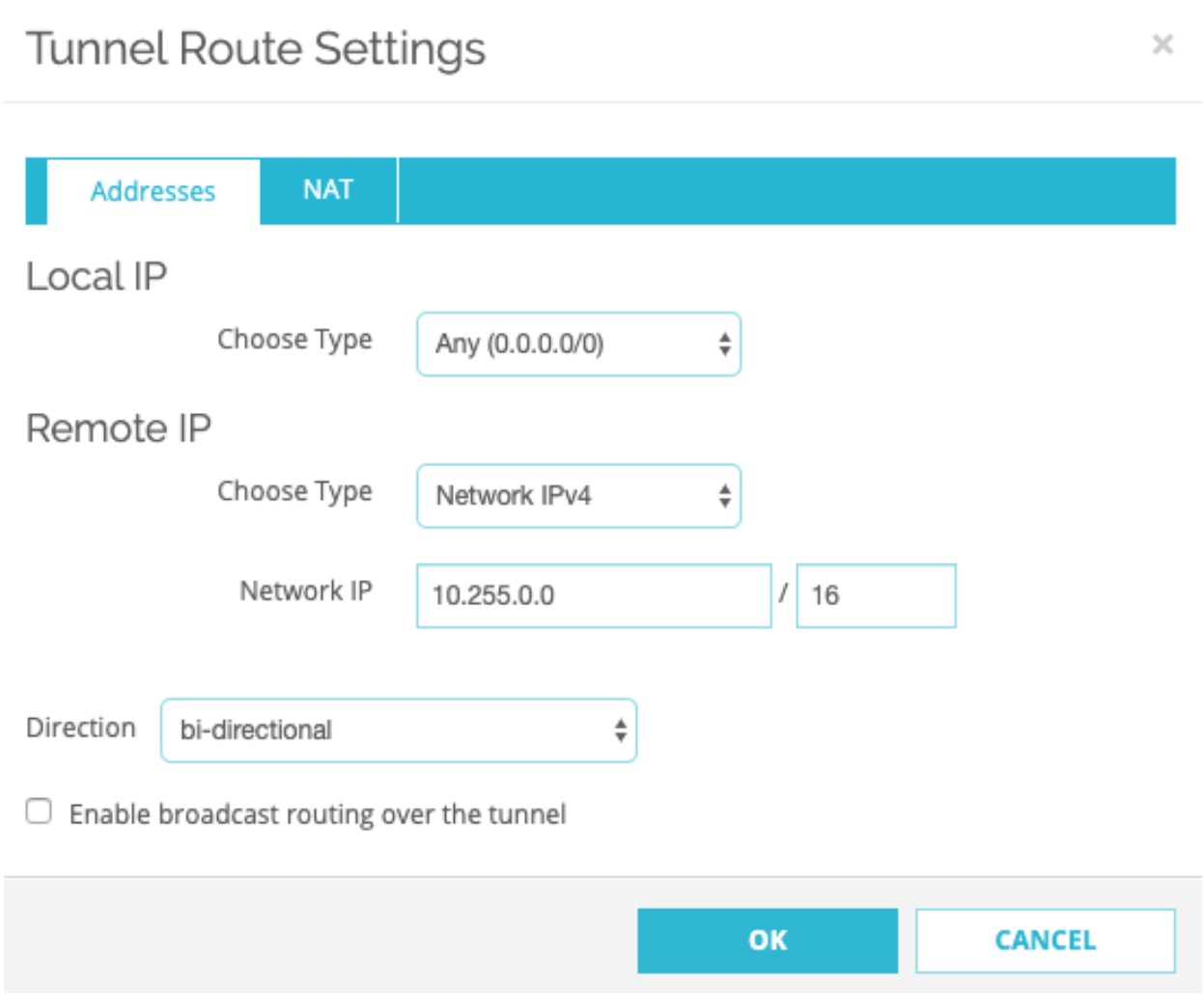
11. Click **OK**.
12. Go to **Transform Settings**, click **Add** and enter these:

Field	Enter
Authentication	SHA2-256
Encryption	AES(256-bit)
SA Life	8 hours
Key Group	Diffie-Hellman Group 14

13. In the **BOVPN Virtual Interfaces** page, in the **Tunnel** section, click **Add** and enter these:

Field	Enter
Name	Name for the tunnel.
Gateway	Firewall that you created for this setup.

14. Go to tab **Addresses** tab, click **Add** and enter these:



Field	Enter
Local IP	ANY (0.0.0.0/0)
Remote IP	Check Point SASE network remote IP address. The default is 10.255.0.0./16.
Direction	bi-directional
Key Group	Diffie-Hellman Group 14

Leave rest of the fields with the default values.

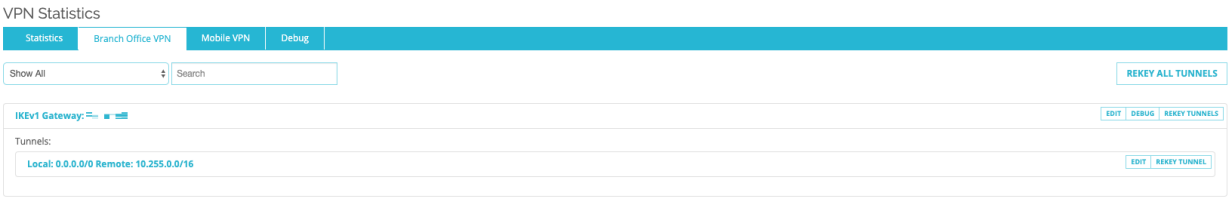
15. Go to **Phase 2 Settings**:
    a. Select the checkbox next to **Enable Perfect Forward Secrecy** next to and select **Diffie-Hellman Group 14**.

b. In the **IPSec Proposals** section, select **ESP-AES256-SHA256** and click **Add**.

   Leave rest of the fields with the default values.

c. Click **Save**.

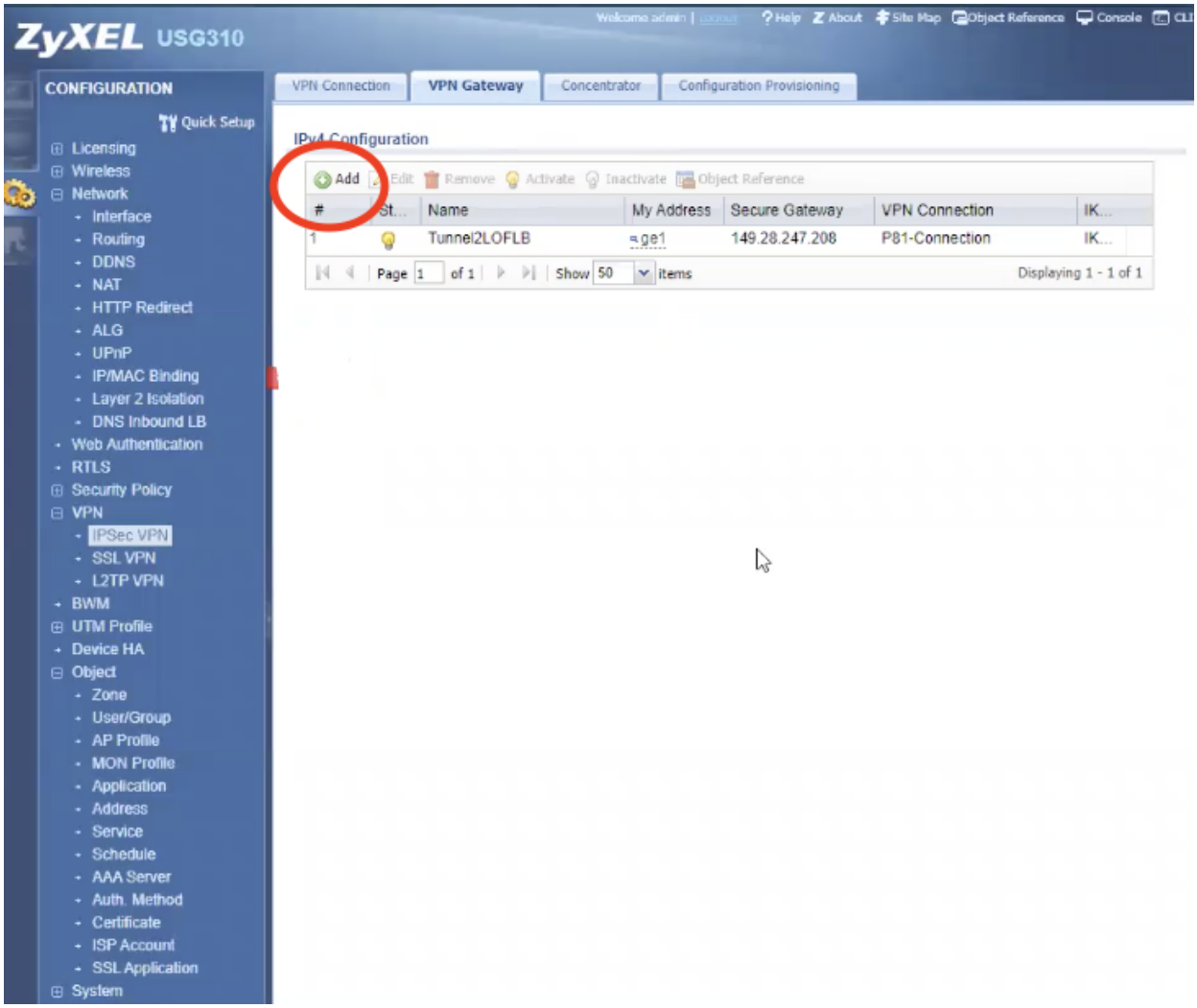
16. To verify whether the tunnel is up, go to **System Status > VPN Statistics > Branch Office VPN**. If the tunnel is up, the tunnel is listed under **Tunnels**.



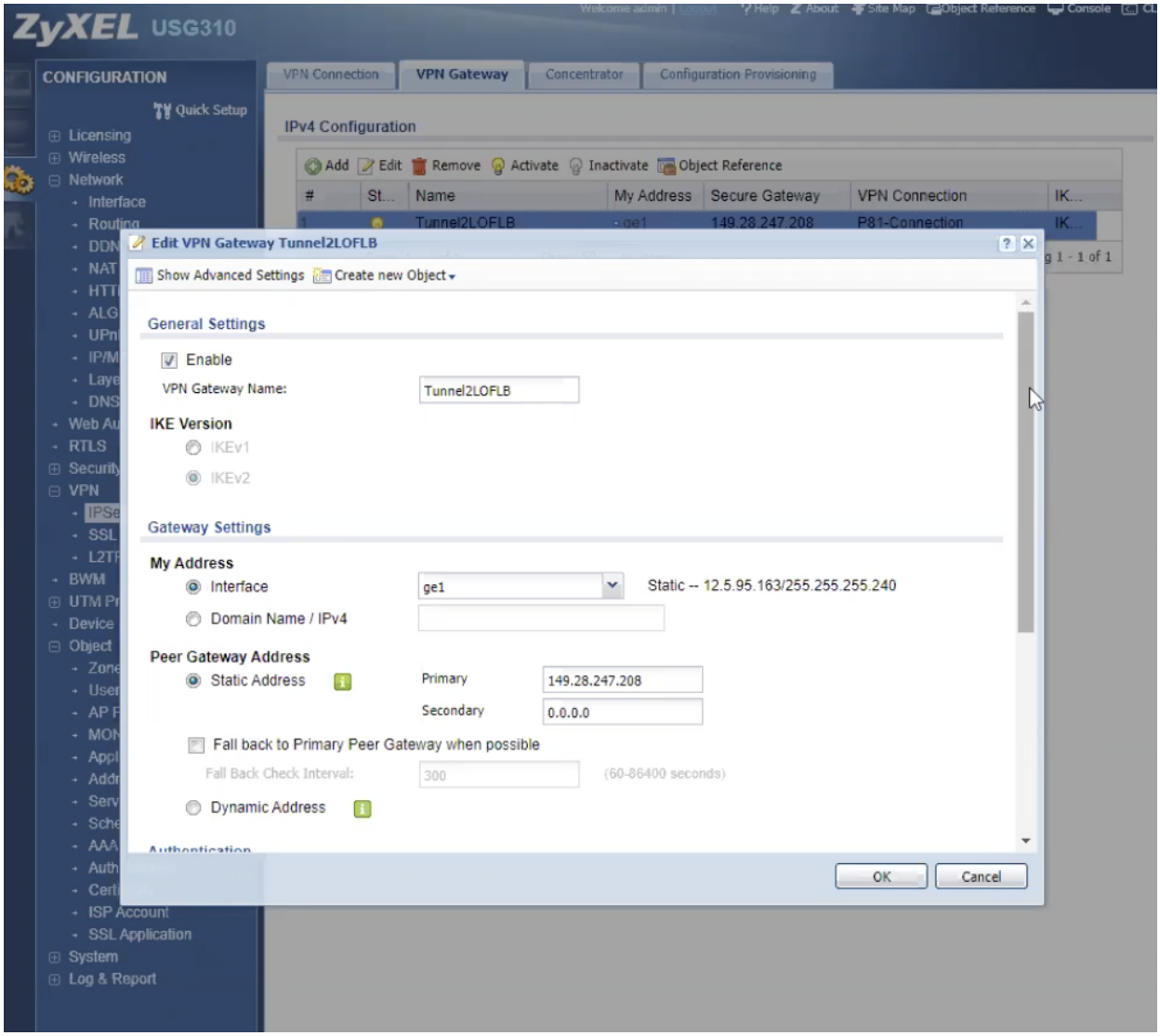
Zyxel USG Firewall

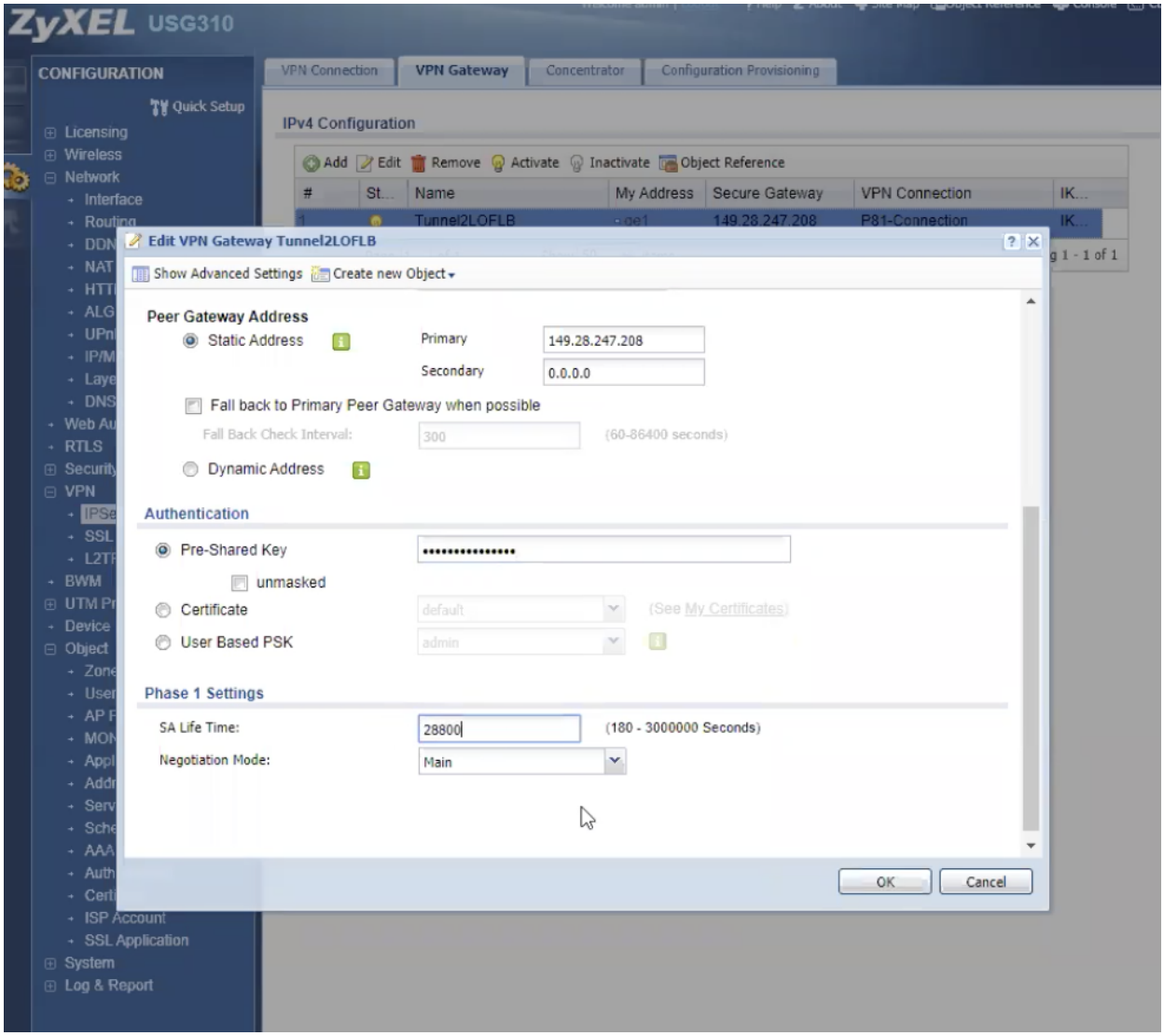
To configure the tunnel in the Zyxel USG Management Portal:

1. Log in to the Zyxel USG Management Portal.
2. Go to **Configuration > VPN > IPSec VPN**.



3. In the **VPN Gateway** tab, click **Add**.
4. In the **General settings** section:
    a. Select the **Enable** checkbox.
    b. In the **VPN Gateway Name** field, enter a name for the gateway.
5. In the **Gateway Settings** section:

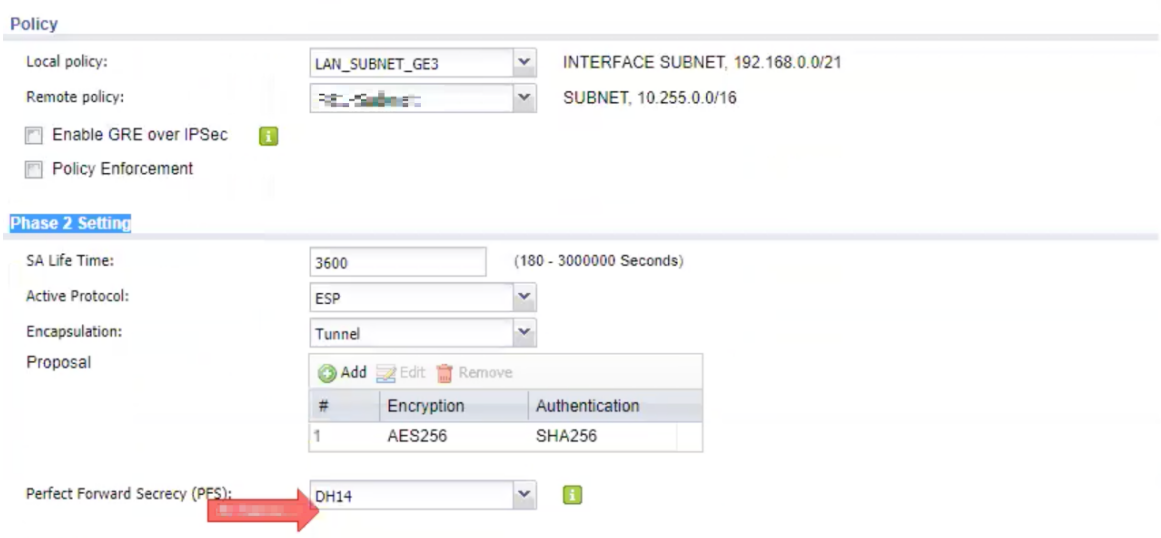

ZyXEL USG310
CONFIGURATION
Quick Setup
Licensing
Wireless
Network
Interface
VPN
SSL
ISP Account
SSL Application
System
Log & Report
VPN Connection
VPN Gateway
Concentrator
Configuration Provisioning
IPv4 Configuration
Add
Edit
Remove
Activate
Inactivate
Object Reference
St... Name My Address Secure Gateway VPN Connection IK...
Tunnel2LOFLB ge1 149.28.247.208 P81-Connection
Edit VPN Gateway Tunnel2LOFLB
Show Advanced Settings
Create new Object
General Settings
Enable
VPN Gateway Name:
Tunnel2LOFLB
IKE Version
IKEv1
IKEv2
Gateway Settings
My Address
Interface
ge1
Static -- 12.5.95.163/255.255.255.240
Domain Name / IPv4
Peer Gateway Address
Static Address
Primary
149.28.247.208
Secondary
0.0.0.0
Fall back to Primary Peer Gateway when possible
Fall Back Check Interval:
300
(60-86400 seconds)
Dynamic Address
OK
Cancel



Field	Enter
My Address	
Interface	You WAN interface.
Peer gateway Address	
Static Address Primary	Public IP address of Check Point SASE gateway.
Static Address Secondary	0.0.0.0
Authentication	
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Check Point SASE Administrator Portal" on page 247*.

Field	Enter
Phase 1 Settings	
SA Life Time	28800
Negotiation Mode	Main

6. Click **OK**.
7. Add a VPN tunnel:
   a. Go to **Configuration > VPN > IPSec VPN**.
   b. In the **VPN Connection** tab, click **Add**.
   c. Enable and enter a rule name.
   d. Select **Site-to-Site** and select the created VPN gateway.
   e. Set the local policy to your LAN subnet and the remote policy to your Check Point SASE subnet.



   f. Select **Create new Object** and choose **IPv4 Address**.

> **Note** - Check if the IP address of the remote subnet does not already exist on the local subnet to avoid a double IP address configuration. The remote subnet must match the local subnet to reach the local network.

   g. Select **Show Advanced Settings** and make sure that the **Encryption** and **Authentication** in **Phase 2 Setting** are the same as the **Phase 1 Setting**.

On-premises Router - Configuring the Tunnel in the Management Portal

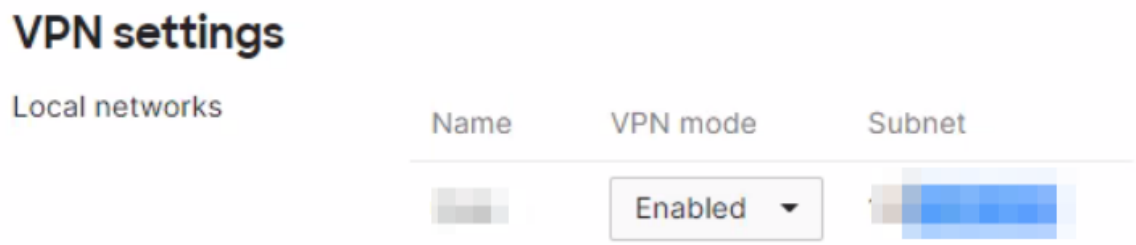
Check Point SASE supports these on-premises router devices for the IPSec Site-2-Site VPN tunnel connection with the Check Point SASE gateway:

- *"Cisco Meraki Router" on page 506*
- *"D-Link DSR Series Router" on page 509*
- *"DrayTek Vigor2862 Router" on page 516*
- *"DrayTek Vigor3900 Router" on page 519*
- *"EdgeMax Router" on page 526*
- *"Linksys Router" on page 528*
- *"Netgear BR500 Router" on page 532*

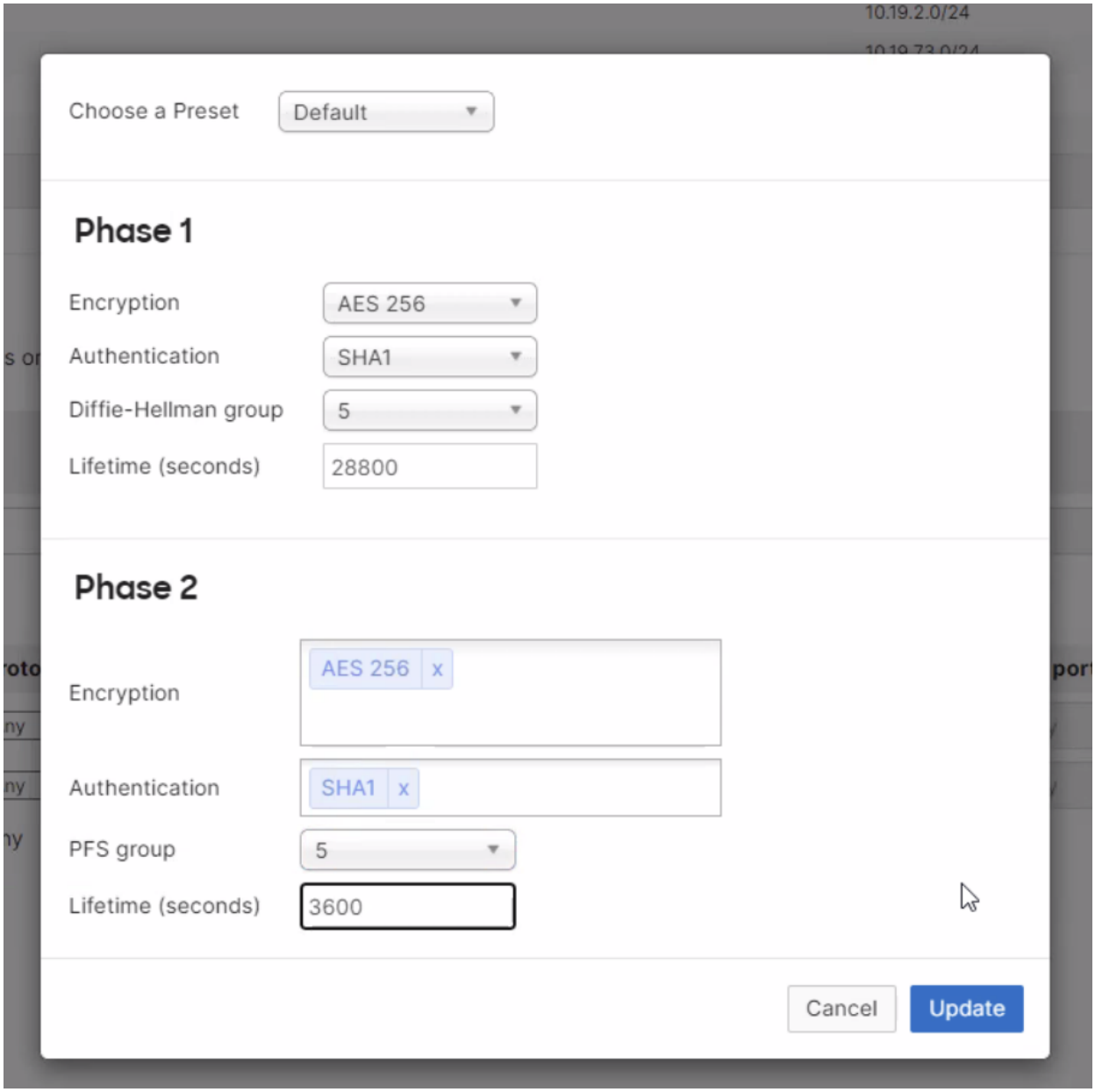
Cisco Meraki Router

To configure the tunnel in the Cisco Meraki Management Portal:

1. Log in to the Cisco Meraki Management Portal with the Administrator account.
2. Go to **Security Appliance > Configure > Site-to-site VPN**.
3. Make sure that the local LAN you want t connect from the Check Point SASE network is participating in the VPN.



4. Scroll down to the **Non-Meraki VPN peers** section.
5. Click **Add a peer**:



Field	Enter
Name	Name for the remote device or VPN.
IKE Version	IKEv1
Public Ip	Public IP address of the Check Point SASE gateway.
Remote ID	Public IP address of the Check Point SASE gateway.
Private subnets	Check Point SASE network subnets. Default is 10.255.0.0/16.
Preshared secret key	Secret key specified in the Check Point SASE Administrator Portal.

Field	Enter
IPsec Policy to use	Custom
Phase 1	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	28800
Phase 2	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	3600

6. Click **Update**.
7. Edit the router rules to allow the traffic through the Check Point SASE tunnel. These rules apply to inbound and/or outbound VPN traffic from all MX appliances in the organization that participate in site-to-site VPN.

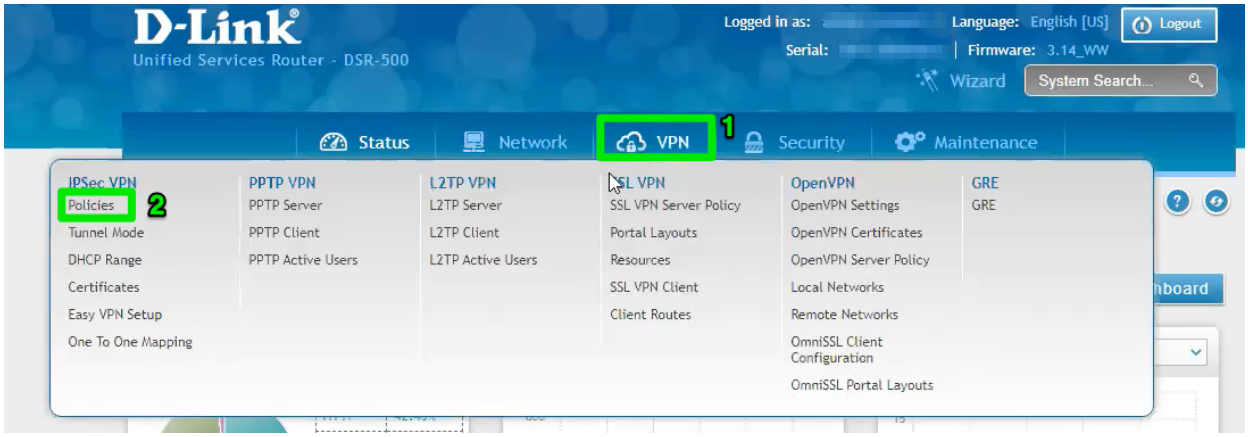
   To create a rule, got to **Security Appliance > Configure > Site-to-site VPN**, in the **Site-to-site firewall** section, select **Add a rule**.

   For reference, see the Layer 3 firewall rules.

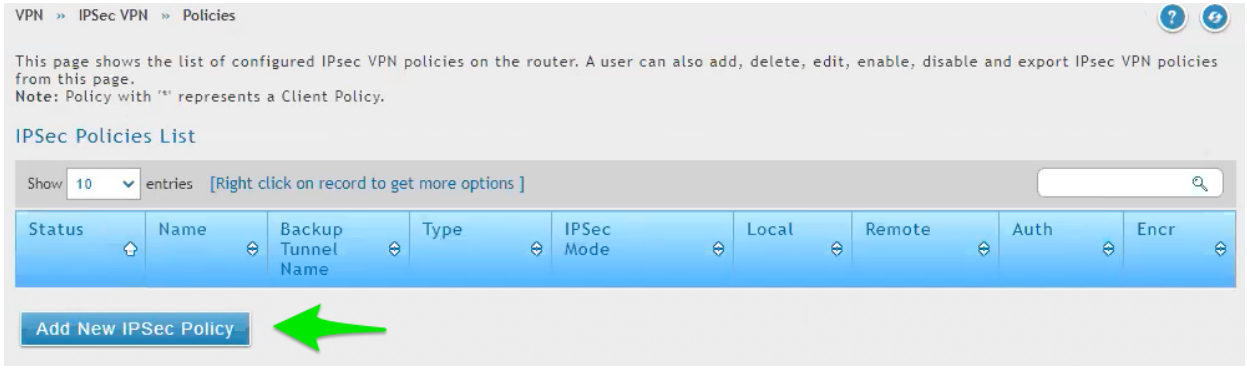
D-Link DSR Series Router

To configure the tunnel in the D-Link DSR Series Router Management Portal:

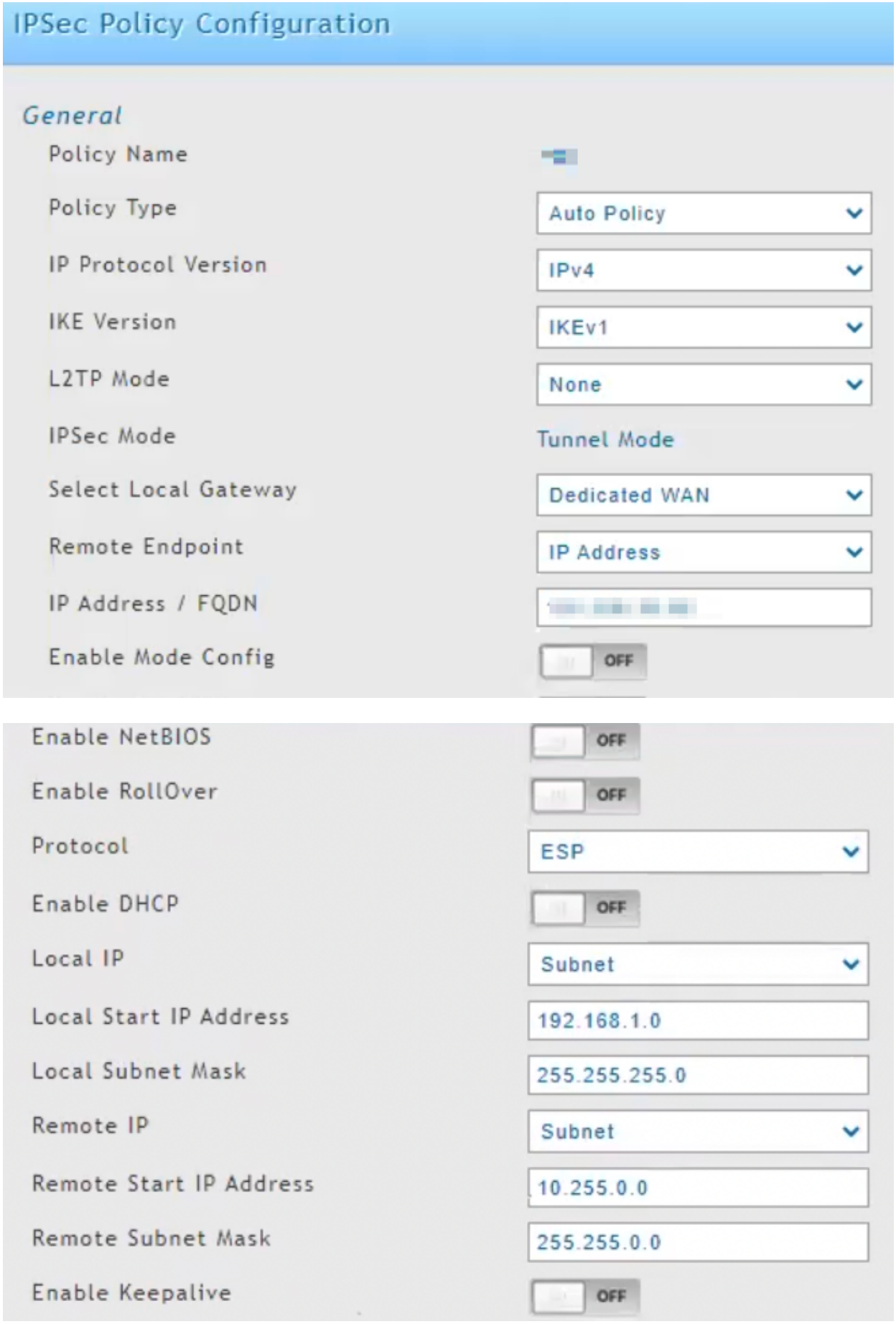
1. Log in to the D-Link DSR Series Router Management Portal with the Administrator.
2. Click **VPN**.



3. Click **IPSec VPN > Policies**.
4. Click **Add New IPSec Policy**.



5. In the **General** section:


IPSec Policy Configuration
General
Policy Name
Policy Type
Auto Policy
IP Protocol Version
IPv4
IKE Version
IKEv1
L2TP Mode
None
IPSec Mode
Tunnel Mode
Select Local Gateway
Dedicated WAN
Remote Endpoint
IP Address
IP Address / FQDN
Enable Mode Config
OFF
Enable NetBIOS
OFF
Enable RollOver
OFF
Protocol
ESP
Enable DHCP
OFF
Local IP
Subnet
Local Start IP Address
192.168.1.0
Local Subnet Mask
255.255.255.0
Remote IP
Subnet
Remote Start IP Address
10.255.0.0
Remote Subnet Mask
255.255.0.0
Enable Keepalive
OFF

Field	Enter
Policy Name	Name for the policy.
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address/FQDN	Public IP address of the Check Point SASE gateway.
Enable Config Mode	Off
Enable NetBIOS	Off
Enable RollOver	Off
Protocol	ESP
Enable DHCP	Off
Local IP	Subnet
Local Start IP Address	Your local subnet
Local Subnet Mask	Matching subnet mask
Remote IP	Subnet
Remote Start IP Address	10.255.0.0
Remote Subnet Mask	255.255.0.0
Enable Keepalive	Off

6. In the **Phase1 (IKE SA Parameters)** section:

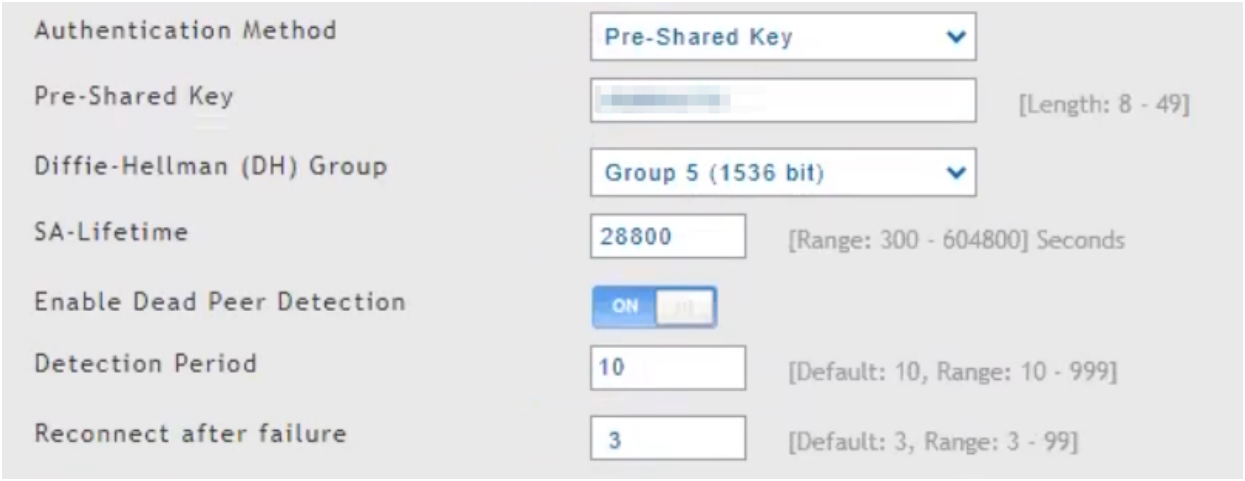
Field	Enter
Exchange Mode	Main
Direction/Type	Responder
NAT Traversal	Off
Local Identifier Type	Local Wan IP
Remote Identifier Type	Remote Wan IP

7. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
AES-128	Off
AES-256	On
Blowfish	Off

Field	Enter
3DES	Off
AES-192	Off

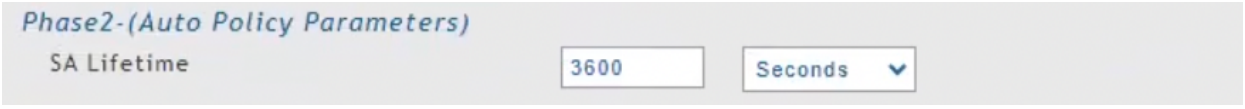
8. In the **Authentication Algorithm** section:



Field	Enter
MD5	Off
SHA2-256	Off
SHA2-512	On
Authentication Method	Pre-Shared Key
Pre-Shared Key	Secret key specified in the Check Point SASE Administrator Portal.
Diffie-Hellman (DH) Group	Group 5
SA-Lifetime	28800

Field	Enter
Enable dead Peer Detection	On
Detection Period	10
Reconnect after failure	3

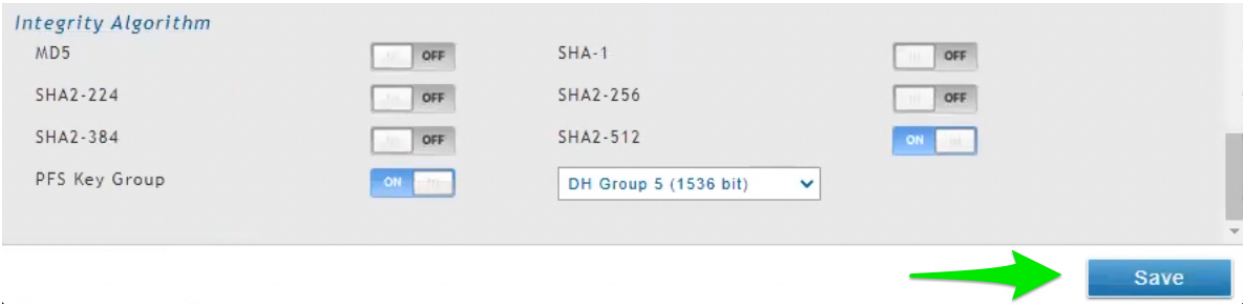
9. In the **Phase2 - (Auto Policy Parameters)** section, in the **SA Lifetime** field, enter **3600 seconds**.



10. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
3DES	Off
AES-192	Off
None	Off
AES-128	Off
AES-256	On

11. In the **Integrity Algorithm** section:



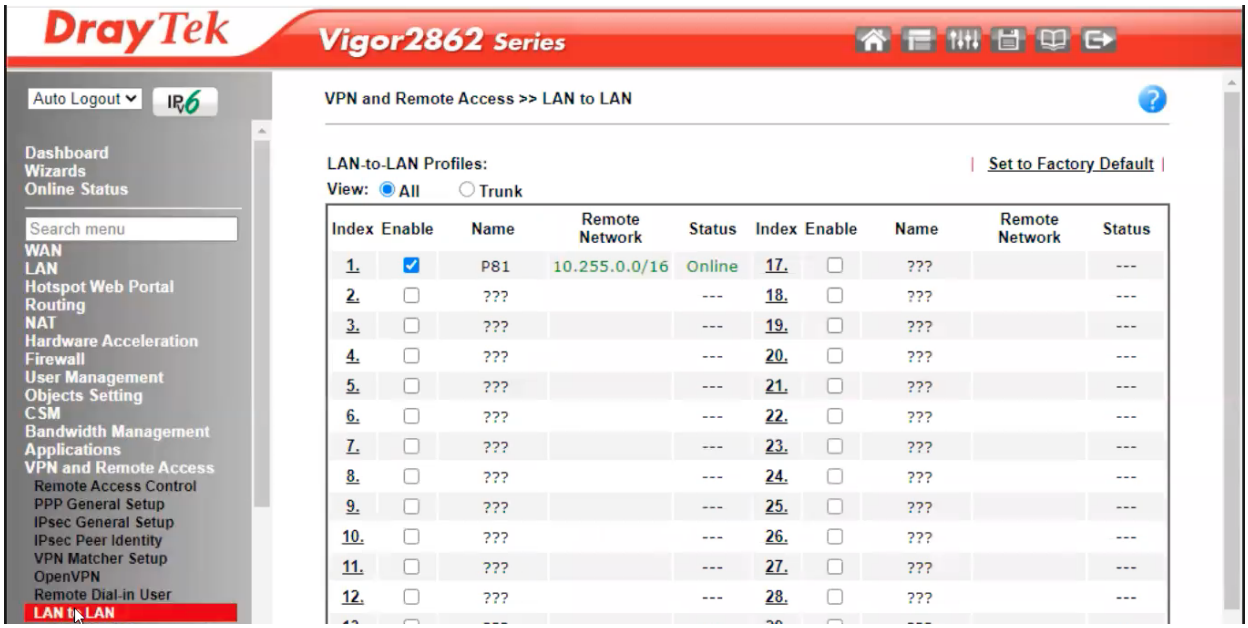
Field	Enter
MD5	Off
SHA-224	Off
SHA2-384	Off
PFS Key Group	On
SHA-1	Off
SHA2-256	Off
SHA2-512	On

12. Click **Save**.

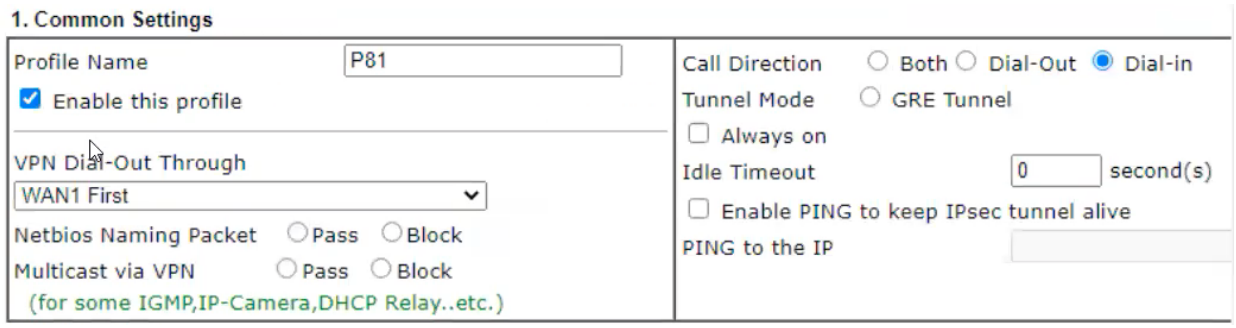
DrayTek Vigor2862 Router

To configure the tunnel in the DrayTek Vigor2862 Management Portal:

1. Log in to the DrayTek Vigor2862 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **LAN to LAN** and create a new profile.



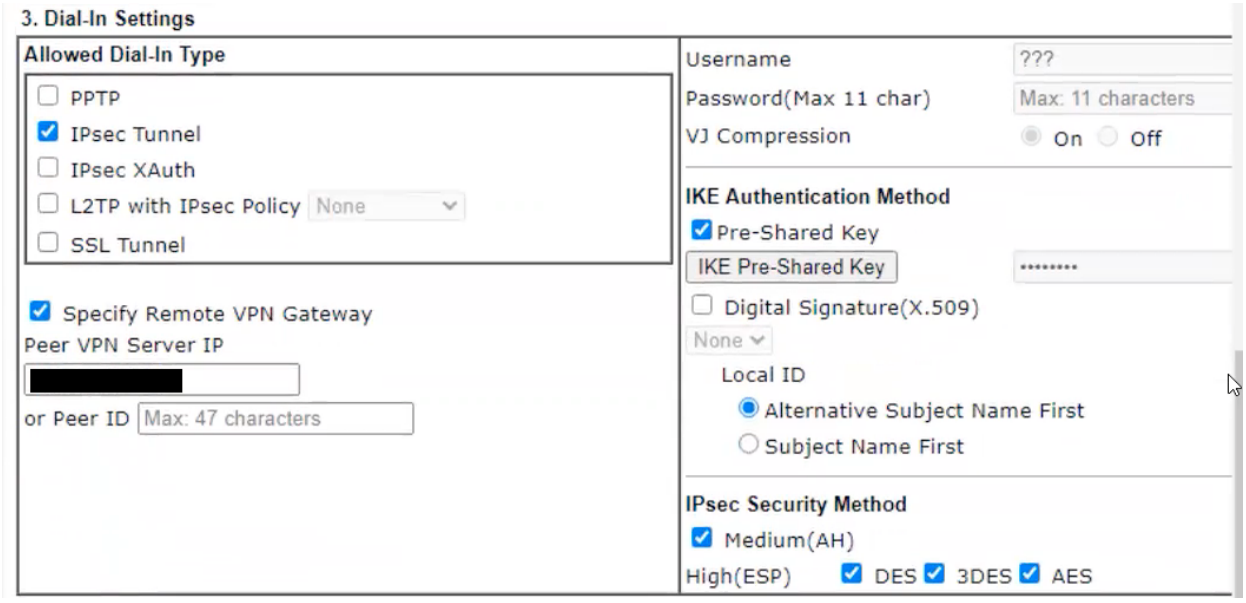
4. In the **Custom Settings** tab:

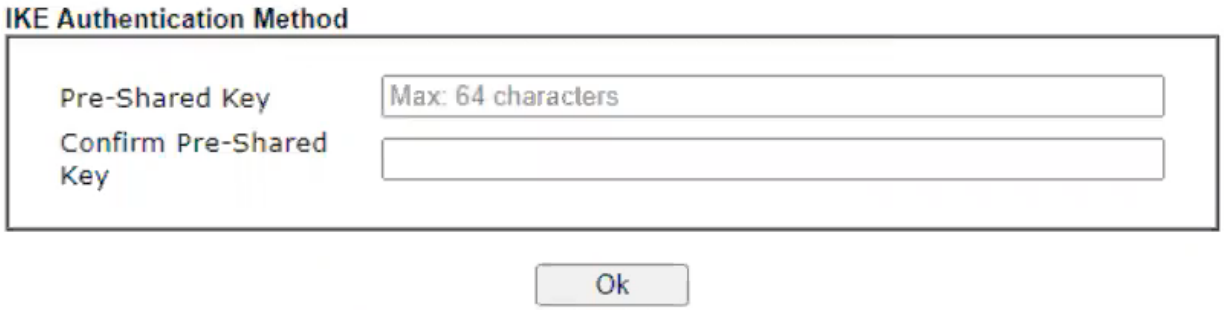


Field	Enter
Profile Name	Name for the profile. For example, Check Point SASE.
Enable this profile	Select
VPN Dial-Out Through	Your WAN interface.
Call Direction	Dial-in

Field	Enter
Idle Timeout	0

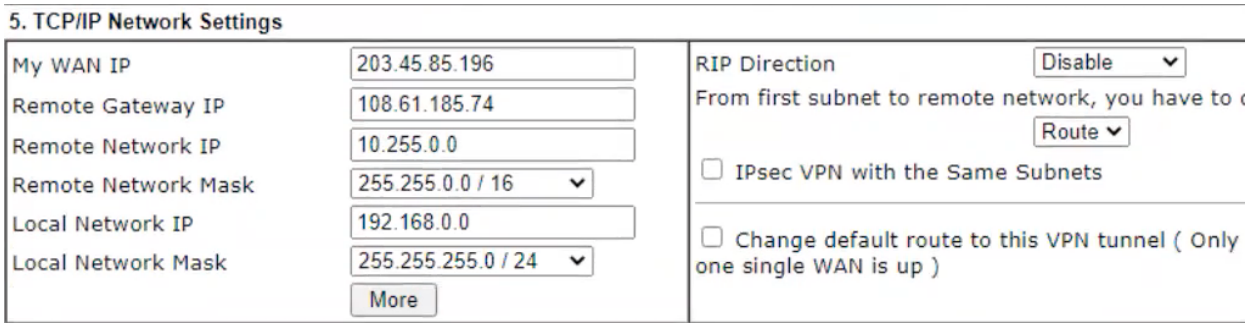
5. In the **Dial-In Settings**tab:





Field	Enter
Allowed Dial-In Type	IPsec Tunnel
Specify Remote VPN Gateway	Public IP address of the Check Point SASE gateway.
Pre-Shared Key	Select and click **IKE Pre-Shared Key** and enter the secret key specified in the Check Point SASE Administrator Portal.

6. In the **TCP/IP Network Settings** tab:

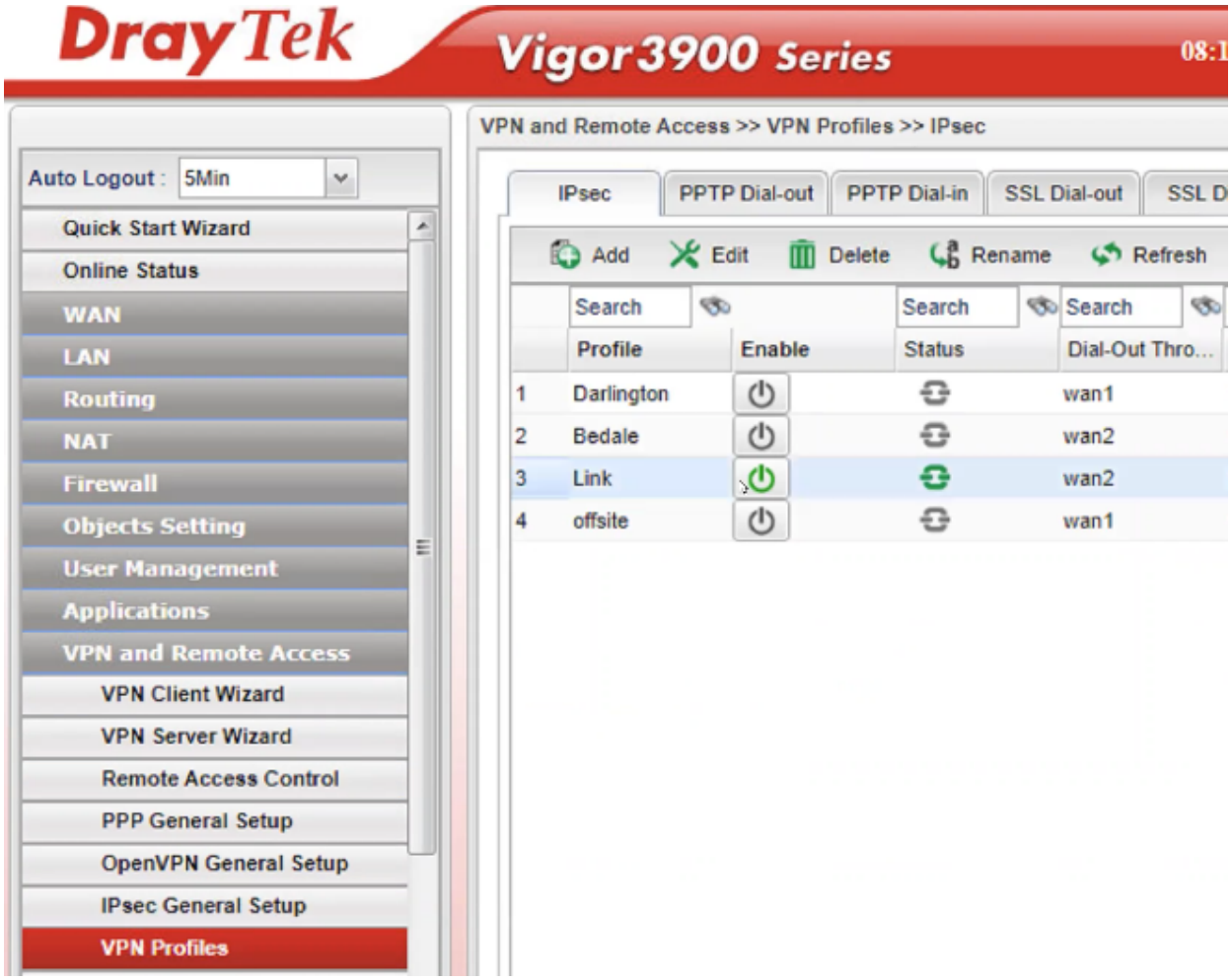


Field	Enter
My WAN IP	Your WAN interface's default IP address.
Remote Gateway IP	Public IP address of the Check Point SASE gateway.
Remote Network IP	Check Point SASE network subnet.
Local Network IP	Your LAN subnnet.

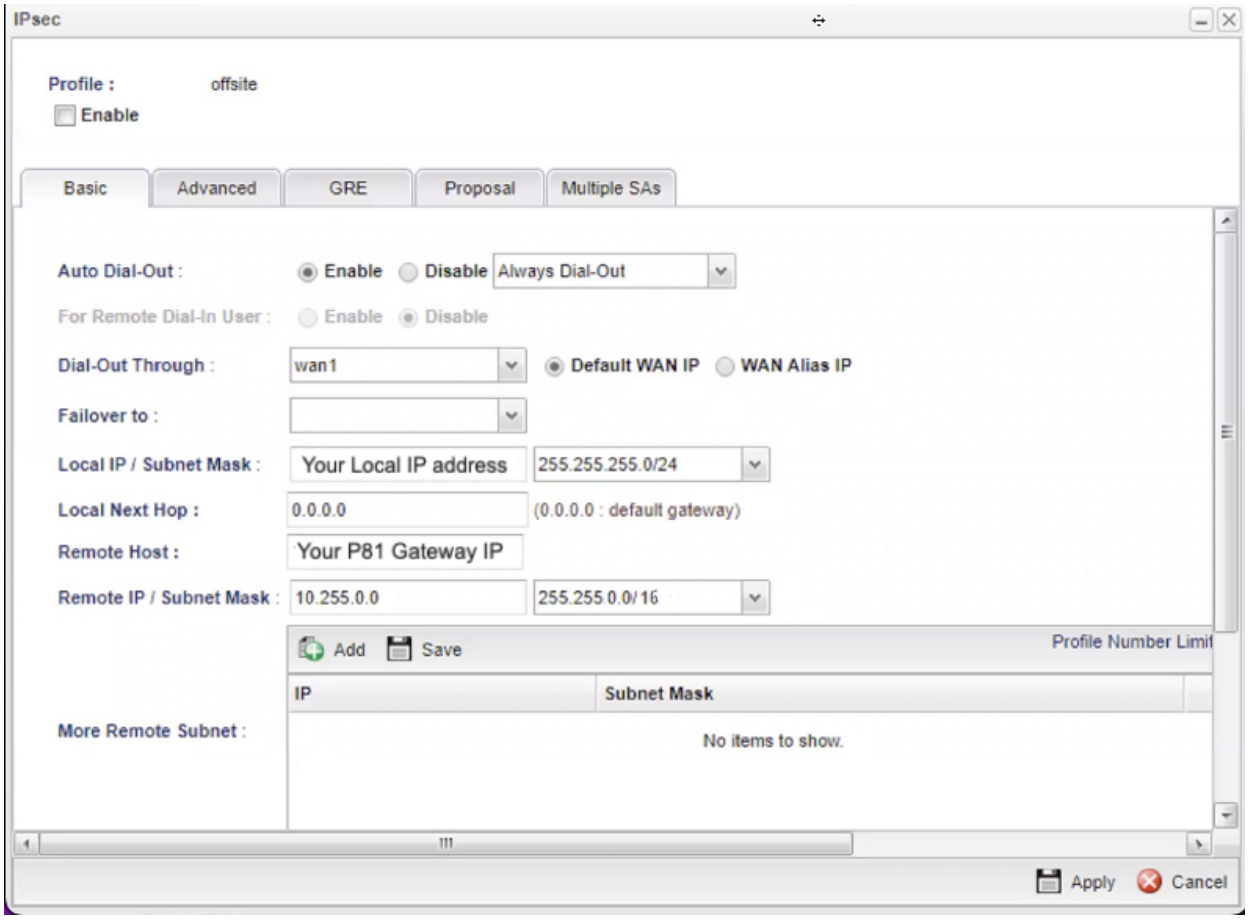
DrayTek Vigor3900 Router

To configure the tunnel in the DrayTek Vigor3900 Management Portal:

1. Log in to the DrayTek Vigor3900 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **VPN Profiles** and click **Add**.



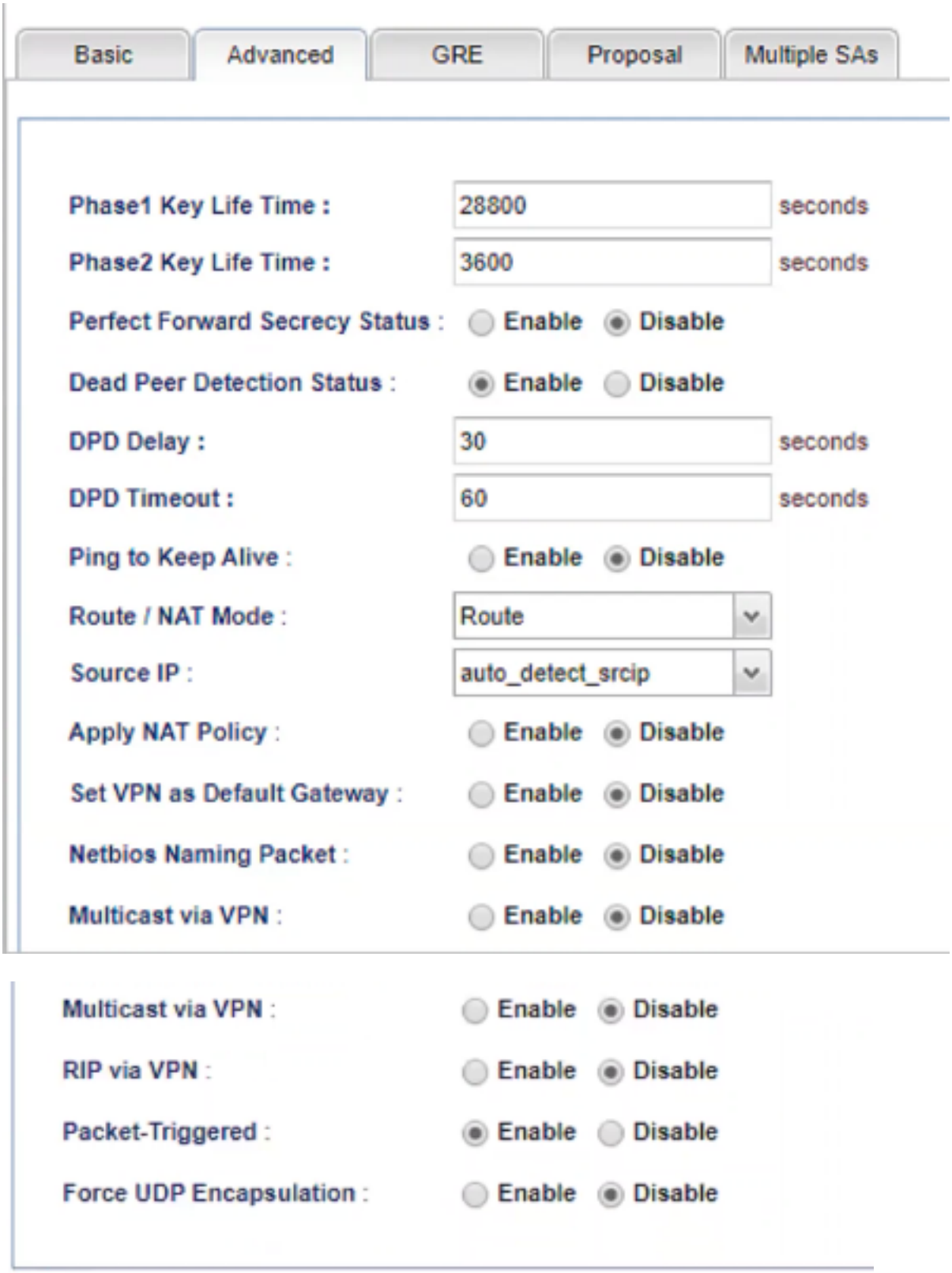
4. In the **Basic** tab:



Field	Enter
Auto Dial-Out	Enable; Always Dial-Out
Dial-Out Through	Your WAN interface; Default WAN IP
Failover	Blank
Local IP / Subnet Mask	Your router external IP address and subnets.
Remote Host	Public IP address of the Check Point SASE gateway.

Field	Enter
Remote IP / Subnet Mask	Default is 10.255.0.0 and 255.255.0.0/16. If you modified these in the Check Point SASE Administrator Portal, enter the modified values.
IKE Protocol	IKEv1
IKE Phase 1	Main Mode
Auth Type	PSK
Pre-shared Key	Secret key specified in the Check Point SASE Administrator Portal.
Security Protocol	ESP

5. In the **Advanced** tab:



Field	Enter
Phase 1 Key Lifetime	28800 seconds

Field	Enter
Phase 2 Key Lifetime	3600 seconds
Perfect Forward Secrecy Status	Enable
DPD Status	Enable
DPD Delay	30 seconds
DPD Timeout	60 seconds
Ping to Keep Alive	Disable
Route/NAT Mode	Route
Source IP	Auto-detect
Apply NAT Policy	Disable
Set VPN Default Gateway	Disable
Netbios Naming Packet	Disable
Multicast via VPN	Disable
RIP via Triggered	Enable
Packet Triggered	Enable
Force UDP Encapsulation	Disable

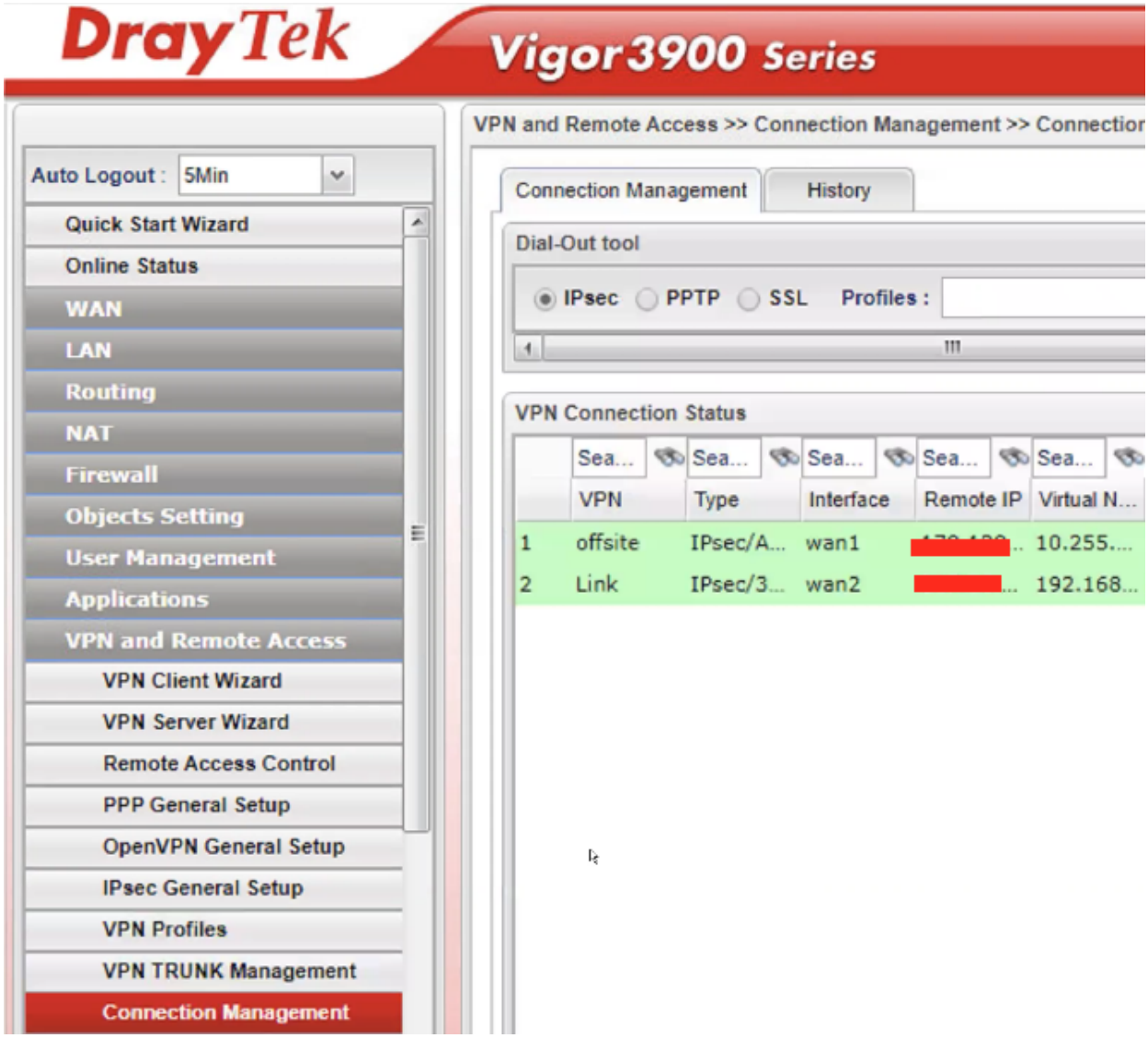
6. In the **GRE** tab:

Field	Enter
Enable GRE Function	Disable
Auto Generate GRE Key	Enable

7. In the **Proposal** tab:

Field	Enter
IKE Phase 1 Proposal	AES 256 G2
IKE Phase 1 Authentication	SHA1
IKE Phase 2 Proposal	AES 256 with auth
IKE Phase 2 Authentication	SHA1
Accepted Proposal	Accept

8. Click **Apply**.
9. To verify if the tunnel is up, from the left pane, click **Connection Management** and check if the profile is listed and highlighted in Green.


DrayTek
Vigor3900 Series
Auto Logout : 5Min
Quick Start Wizard
Online Status
WAN
LAN
Routing
NAT
Firewall
Objects Setting
User Management
Applications
VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
OpenVPN General Setup
IPsec General Setup
VPN Profiles
VPN TRUNK Management
Connection Management
VPN and Remote Access >> Connection Management >> Connectior
Connection Management
History
Dial-Out tool
IPsec
PPTP
SSL
Profiles :
VPN Connection Status
VPN
Type
Interface
Remote IP
Virtual N...
1
offsite
IPsec/A...
wan1
10.255....
2
Link
IPsec/3...
wan2
192.168...

EdgeMax Router

To configure the tunnel in the EdgeMax Router through CLI:

1. Connect to the router through SSH and then enter the configuration mode. For example, using PuTTY.
2. Enable the **auto-firewall-nat-exclude** feature which automatically creates the IPsec firewall/NAT policies in the iptables firewall. Run:

```
set vpn ipsec auto-firewall-nat-exclude enable
```

3. Create IKE / Phase 1 (P1) Security Associations (SAs). Run:

```
set vpn ipsec ike-group FOO0 lifetime 28800
set vpn ipsec ike-group FOO0 proposal 1 dh-group 14
set vpn ipsec ike-group FOO0 proposal 1 encryption aes256
set vpn ipsec ike-group FOO0 proposal 1 hash sha1
set vpn ipsec ike-group FOO0 dead-peer-detection interval 15
set vpn ipsec ike-group FOO0 dead-peer-detection timeout 30
```

4. Create the ESP / Phase 2 (P2) SAs and enable Perfect Forward Secrecy (PFS). Run:

```
set vpn ipsec esp-group FOO0 lifetime 3600
set vpn ipsec esp-group FOO0 pfs enable
set vpn ipsec esp-group FOO0 proposal 1 encryption aes256
set vpn ipsec esp-group FOO0 proposal 1 hash sha1
```

5. Define the remote peering address. Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication mode pre-shared-secret
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication pre-shared-secret <secret key from Quantum SASE
Administrator Portal>
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
description ipsec
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
local-address <Your Edgerouter WAN IP>
```

6. Link the SAs created above to the remote peer and bind the VPN to a virtual tunnel interface (vti0). Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
ike-group FOO0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti bind vti0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti esp-group FOO0
```

7. Configure the virtual tunnel interface (vti0) and assign an internal IP address that is not used in any site. Run:

```
set interfaces vti vti0 address 192.168.20.20/32
```

8. Create a static route for the Check Point SASE subnet (the default is 10.255.0.0/16). Run:

```
set protocols static interface-route 10.255.0.0/16 next-hop-
interface vti0
```

9. Commit the changes and save the configuration. Run:

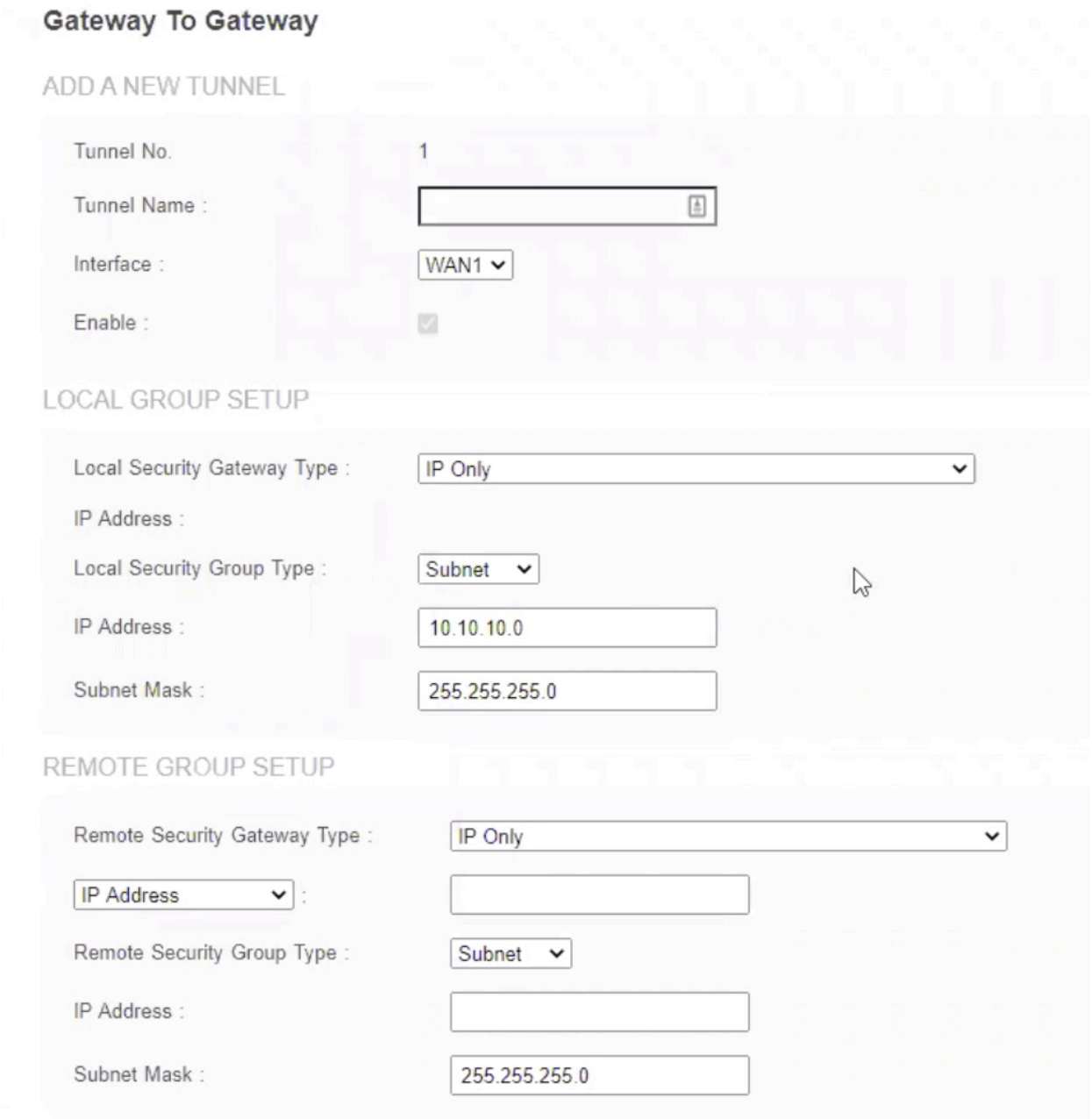
```
commit ; save
```

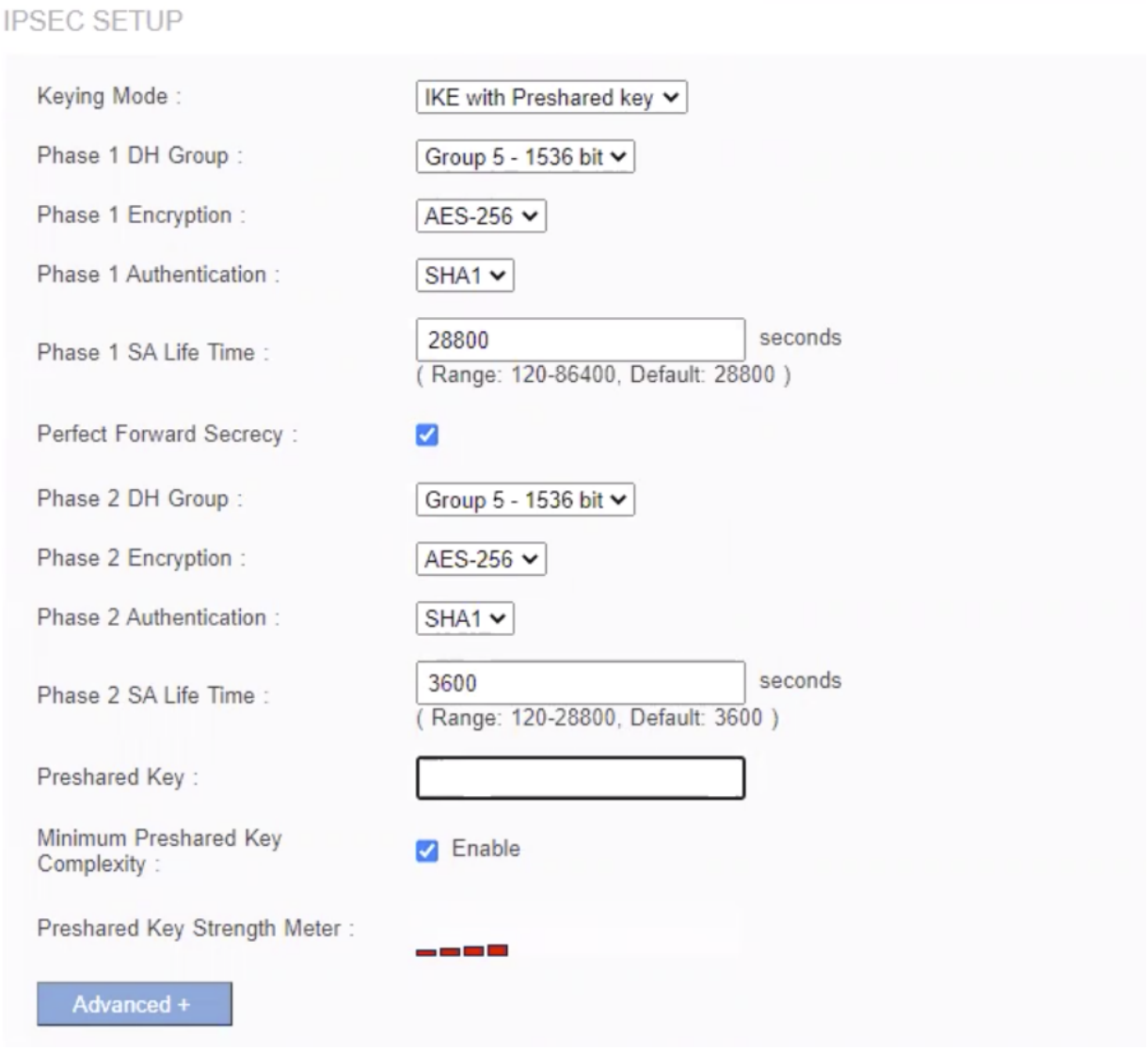
10. In the EdgeMax Management portal, go **VPN - site to site connection**.
11. Verify that the peer associated with the gateway IP address obtained from Check Point SASE has:
    - **Remote subnet**: 10.255.0.0/16 (or the local Check Point SASE gateway that you selected)
    - **Local subnet**: All the subnet range (CIDR) of your LAN devices

Linksys Router

To configure the tunnel in the Linksys Management Portal:

1. Log in to the Linksys Management Portal with the Administrator account.
2. From the left panel, go to **VPN > Gateway to Gateway**.



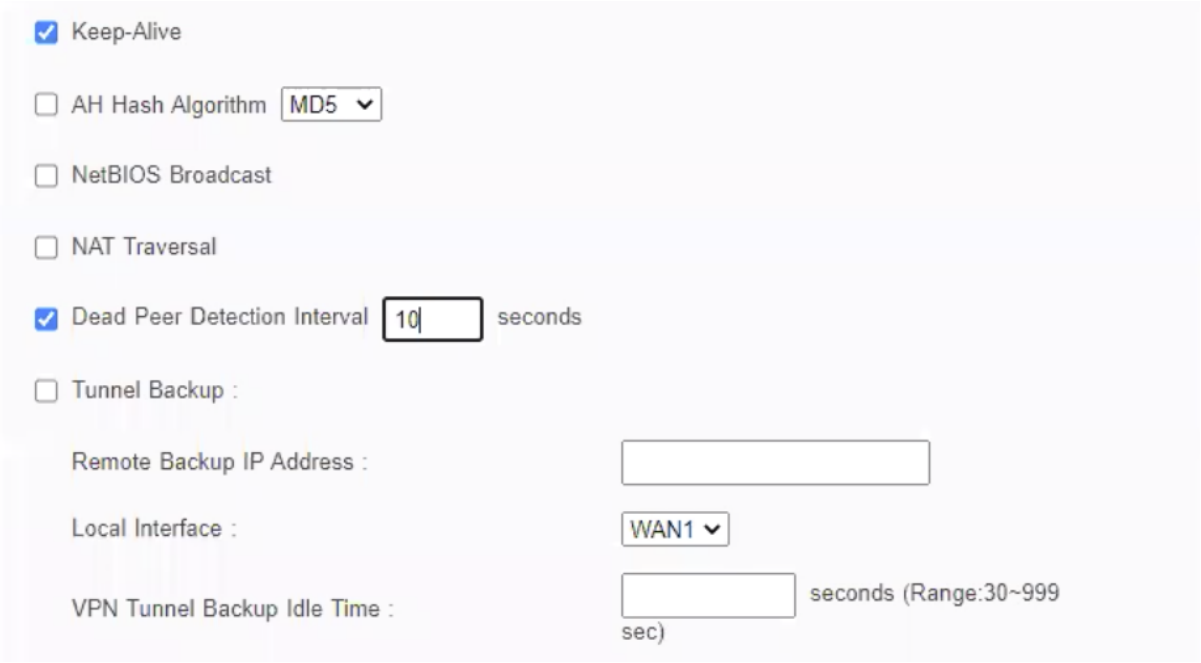


3. Enter these:

Field	Enter
Add a New Tunnel	
Tunnel Name	Name for the tunnel.
Interface	WAN1
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	Linksys external IP address.

Field	Enter
Local Security Group Type	Subnet
IP Address	Linksys local IP address.
Subnet Mask	Linksys subnet mask.
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	Public IP address of Check Point SASE gateway.
Remote Security group Type	Subnet
IP Address	10.255.0.0
Subnet Mask	255.255.0.0
IPSec Setup	
Keying Mode	IKE with PSK
Phase 1 DHG	Group 5
Phase 1 Encryption	aes256
Phase 1 Authentication	sha1
Phase 1 SA Lifetime	28800
Perfect Forward Secrecy	Selected
Phase 2 DHG	Group 5
Phase 1 Encryption	aes256
Phase 2 Authentication	sha1
Phase 2 SA Lifetime	3600
Preshared Key	Secret key specified in the Check Point SASE Administrator Portal.

4. Click **Advanced**:



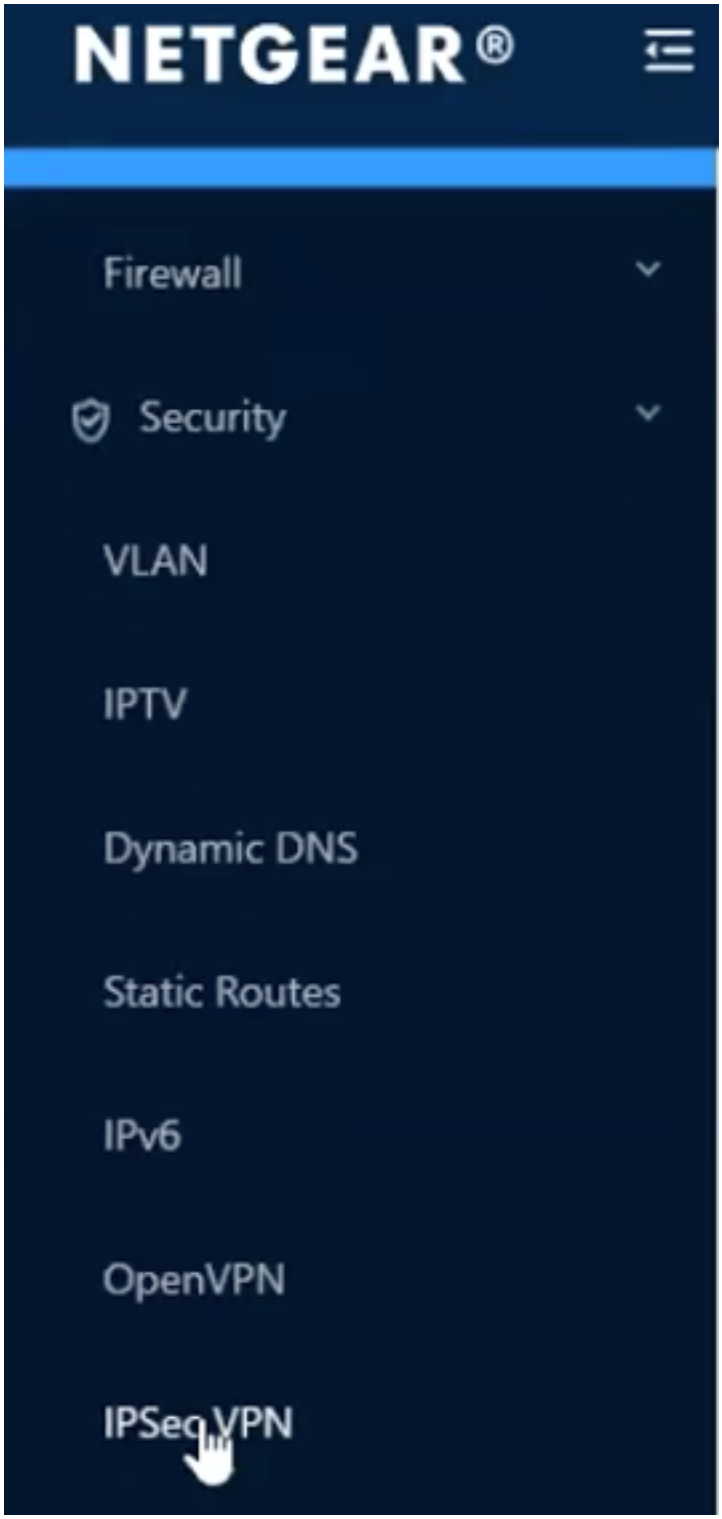
a. Select the **Keep-Alive** checkbox.

b. Select the **Dead Peer Detection Interval** checkbox and enter **10** seconds.

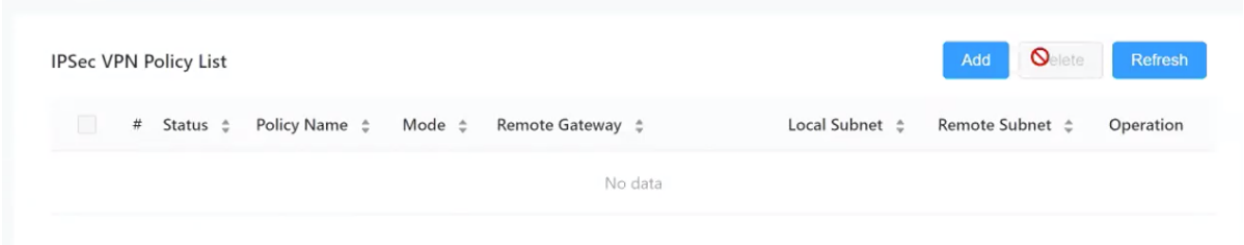
Netgear BR500 Router

To configure the tunnel in the Netgear BR500 Management Portal:

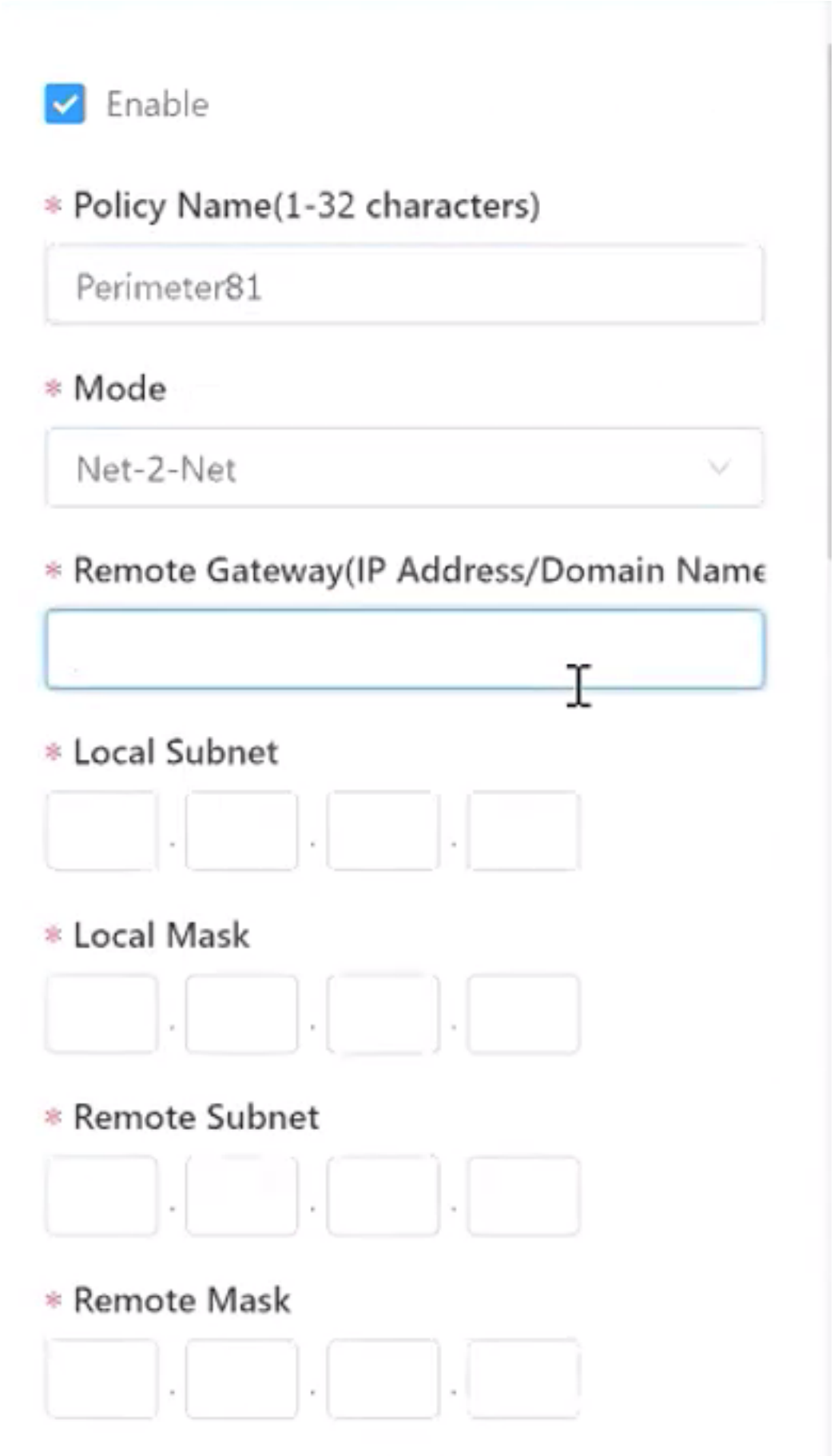
1. Log in to the Netgear BR500 Management Portal with the Administrator account.
2. From the left panel, go to **Security > IPSec VPN**.

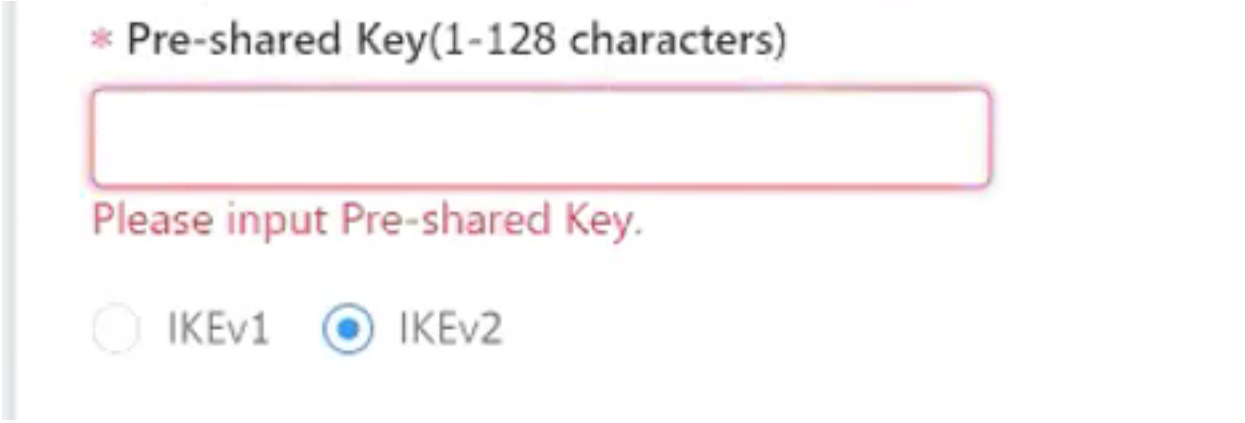


3. Click **Add**.



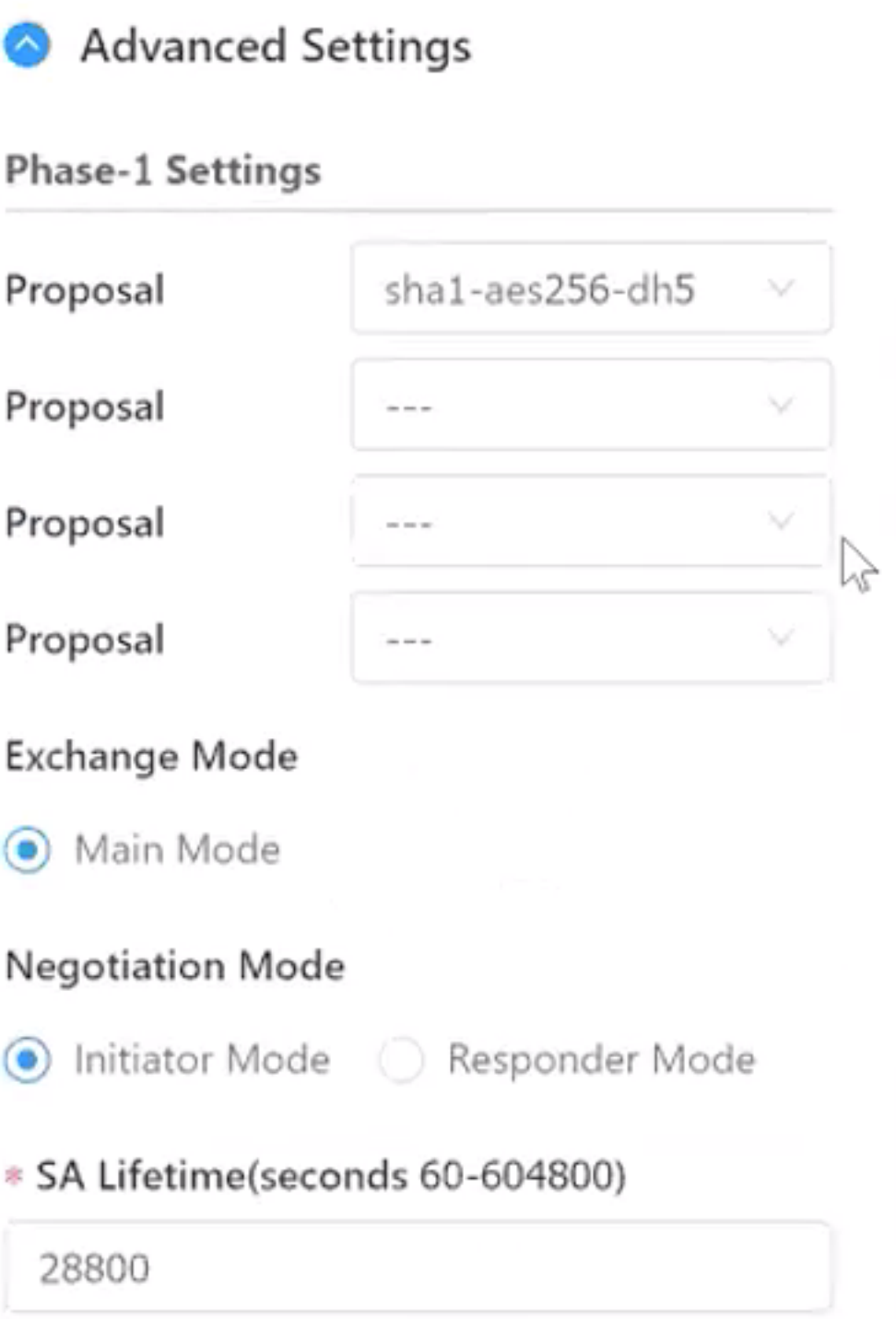
4. Enter these:


Enable
* Policy Name(1-32 characters)
Perimeter81
* Mode
Net-2-Net
* Remote Gateway(IP Address/Domain Name
* Local Subnet
* Local Mask
* Remote Subnet
* Remote Mask



Field	Enter
Policy Name	Name for the policy.
Mode	Net-2-Net
Remote Gateway IP	Public IP address of the Check Point SASE gateway.
Local Subnet and Local Mask	You LAN subnet and subnet mask.
Remote Subnet	Check Point SASE network subnets. Default is 10.255.0.0/16.
Remote Mask	255.255.0.0
Pre-shared Key (1-128 characters)	Secret key specified in the Check Point SASEAdministrator Portal and **IKEv2**.

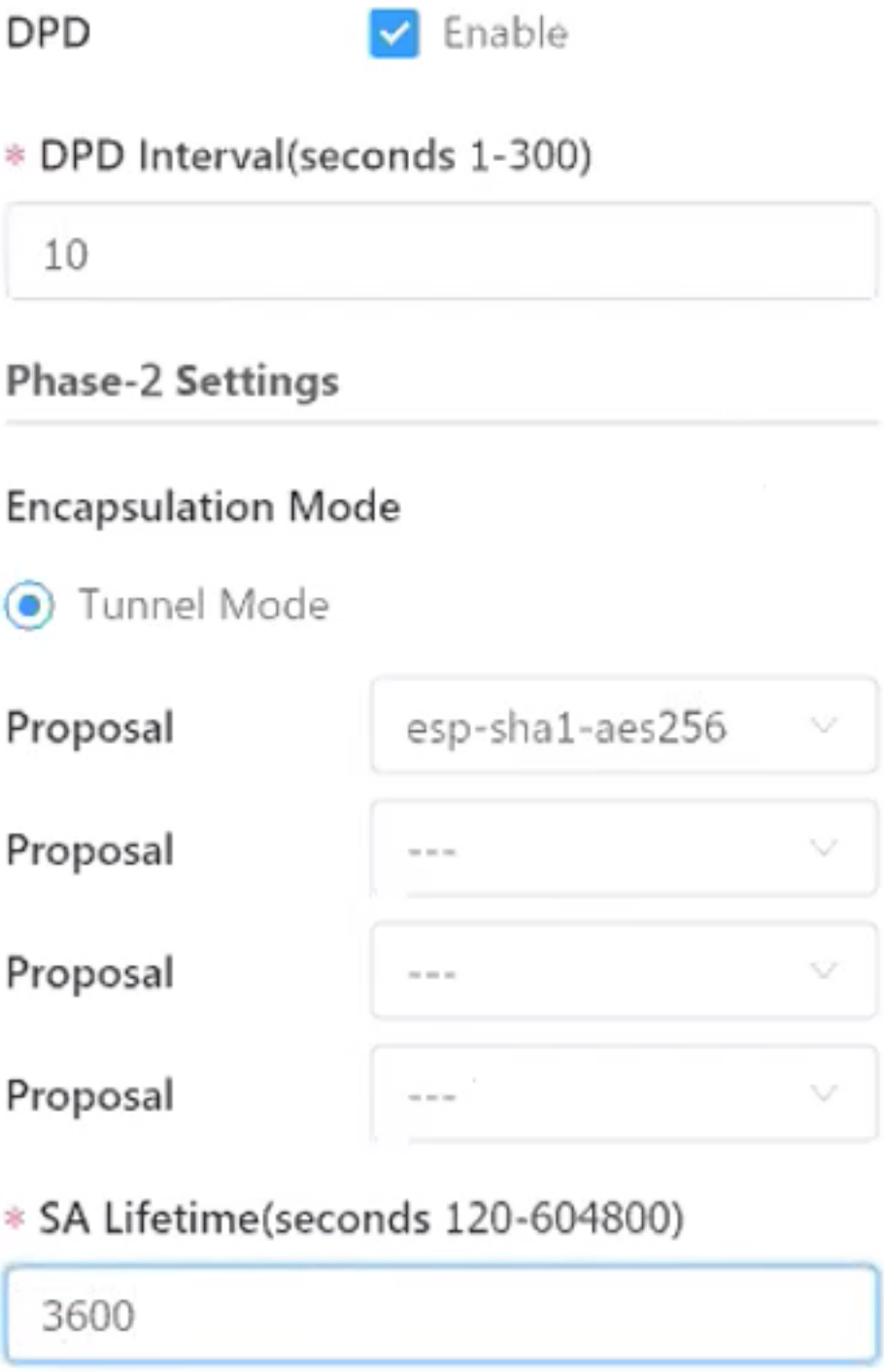
5. In the **Advanced Settings** section:


Advanced Settings
Phase-1 Settings
Proposal
sha1-aes256-dh5
Proposal

Proposal

Proposal

Exchange Mode
Main Mode
Negotiation Mode
Initiator Mode
Responder Mode
* SA Lifetime(seconds 60-604800)
28800



Field	Enter
Phase 1 Proposal	sha1-aes256-dh5
Exchange Mode	Main Mode
Negotiation Mode	Initiator Mode

Field	Enter
Phase I SA Lifetime seconds	28800
DPD	Enable
DPD Interval	10 seconds
Phase II Encapsulation Mode	Tunnel Mode
Phase II SA Lifetime seconds	3600

Configuring the Cloud-based Resources

High-Level Procedure

1. *"Prerequisites" on page 247*
2. For a cloud-based resource, configure any of these:

   Single Tunnel
   - *"AWS Virtual Gateway" on page 555*
   - *"AWS Transit Gateway" on page 575*
   - *"Google Cloud Platform" on page 687*
   - *"Azure Virtual Network Gateway" on page 623*

   Redundant Tunnels
   - *"AWS Redundant Tunnels - Virtual Private Gateway" on page 592*
   - *"AWS Redundant Tunnels - Transit Gateway" on page 606*
   - *"Google Cloud Platform (GCP) Redundant Tunnels" on page 700*
   - *"Azure Virtual Network Gateway Redundant Tunnels" on page 649*
   - *"Azure Virtual WAN Redundant Tunnels" on page 667*

   Other Cloud Options
   - *"Alibaba Cloud" on page 546*
   - *"Heroku Enterprise" on page 722*
   - *"IBM Cloud" on page 723*

3. *"Verifying the Setup" on page 735*.

Using the Configuration File for Tunnel Configuration

You can upload a configuration file generated from the cloud-based resource management portal containing the configuration settings into the Check Point SASE Administrator Portal. This eliminates the manual configuration in the Check Point SASE Administrator Portal.

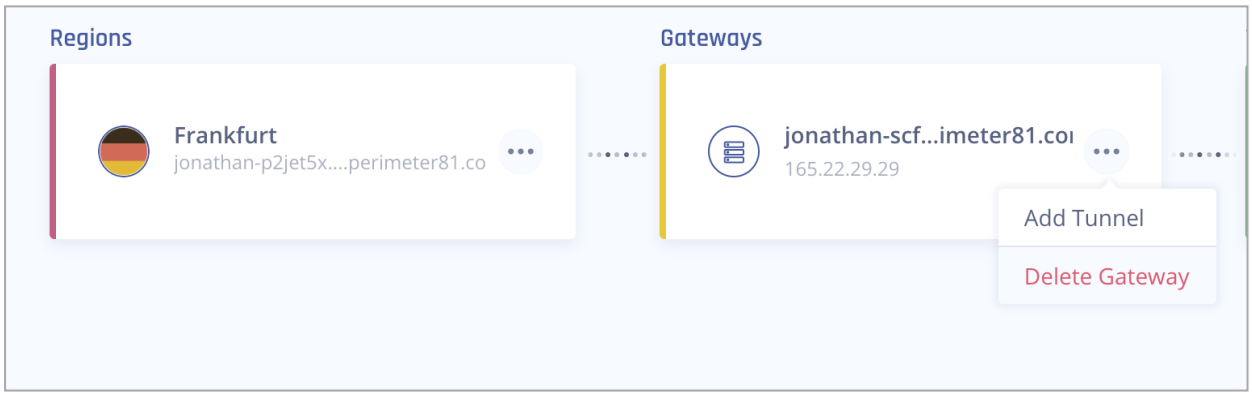
The cloud-based resources that support a configuration file are:

- *"AWS Transit Gateway" on page 575*
- *"AWS Virtual Gateway" on page 555*
- *"AWS Redundant Tunnels - Transit Gateway" on page 606*
- *"AWS Redundant Tunnels - Virtual Private Gateway" on page 592*
- *"Azure Virtual Network Gateway" on page 623*

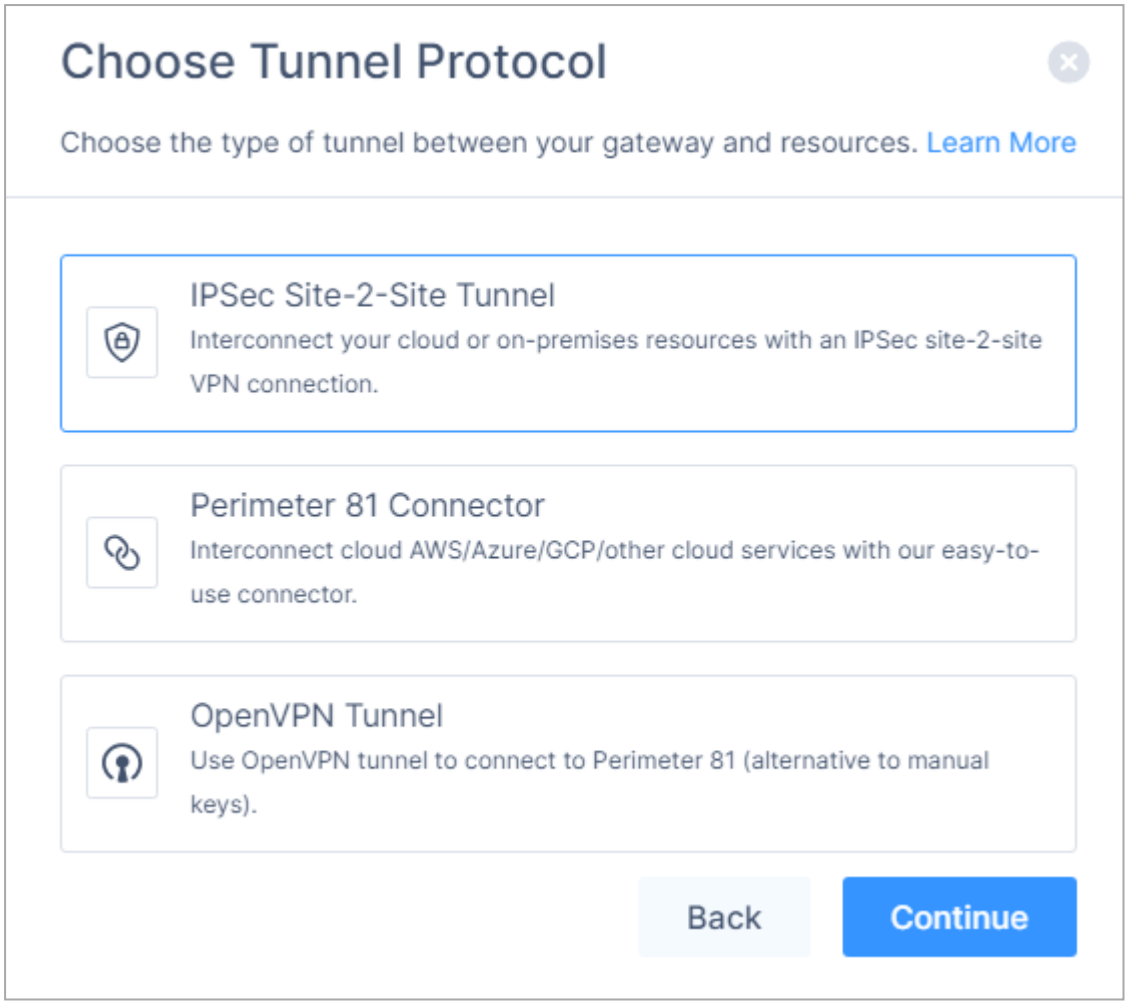
Uploading the Configuration File in the Check Point SASE Administrator Portal

After you download the configuration file from the cloud-based resource management portal, upload the file in the Check Point SASE Administrator Portal.

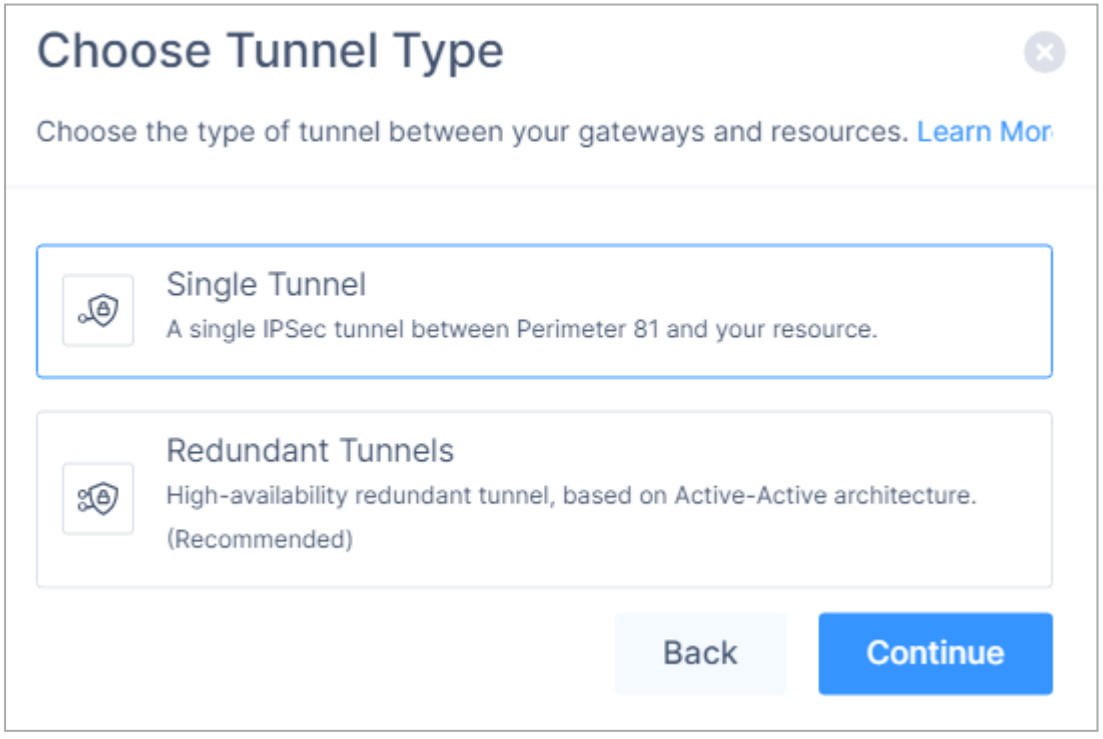
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



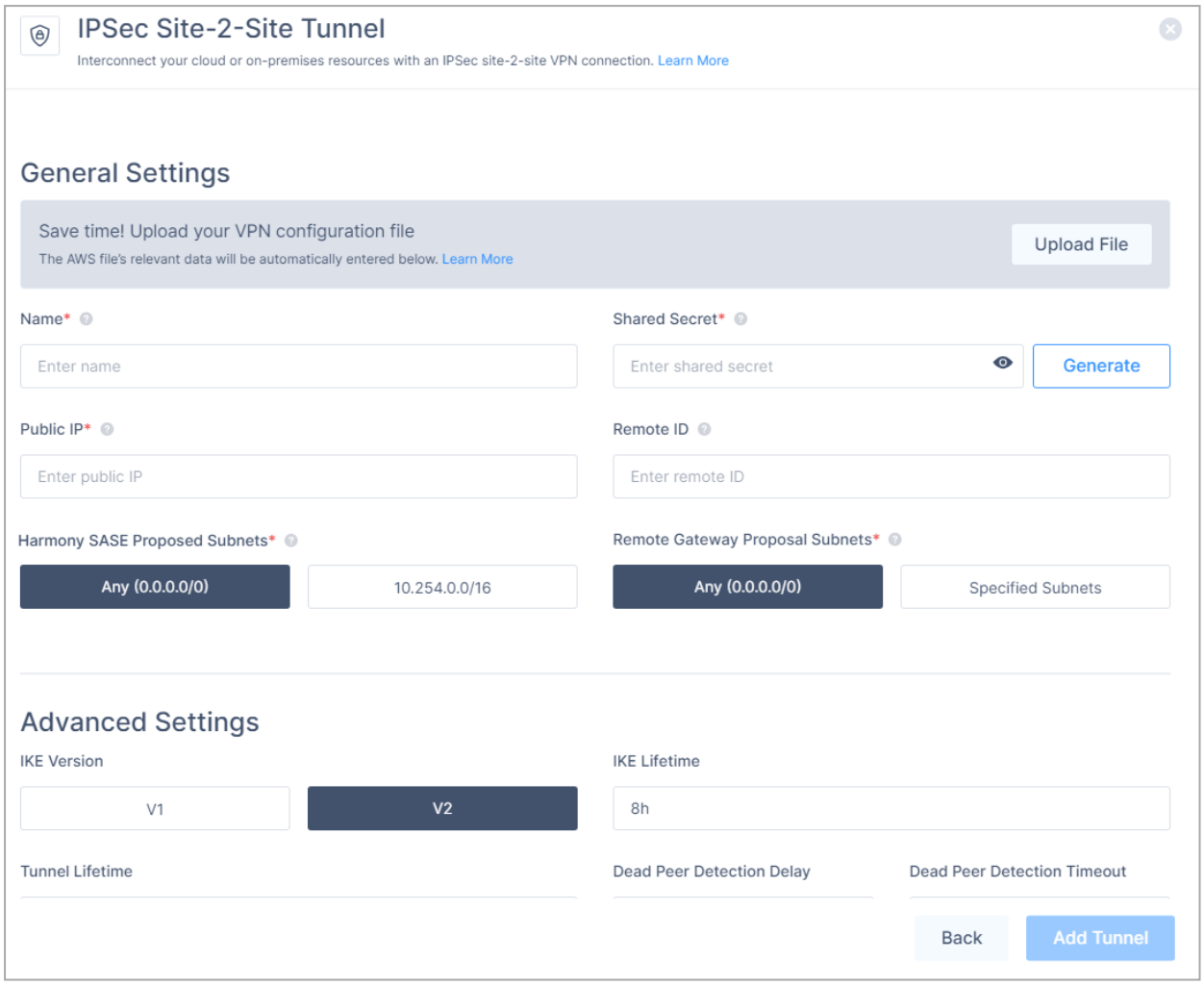
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



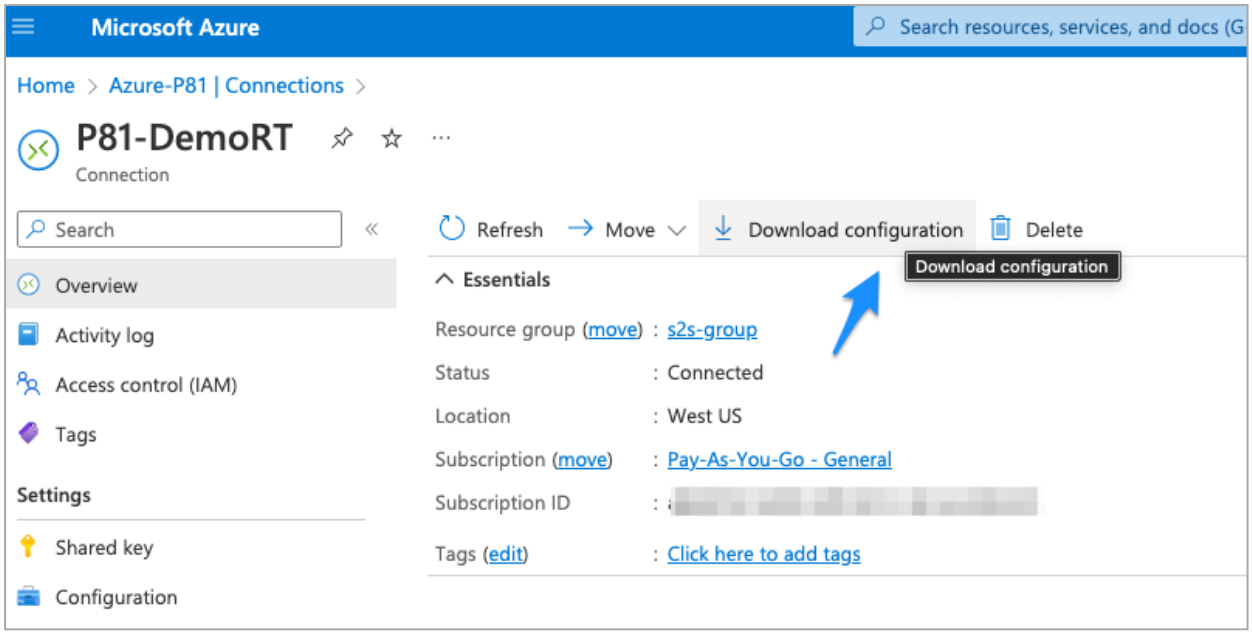
The **IPSec Site-2-Site Tunnel** window appears.



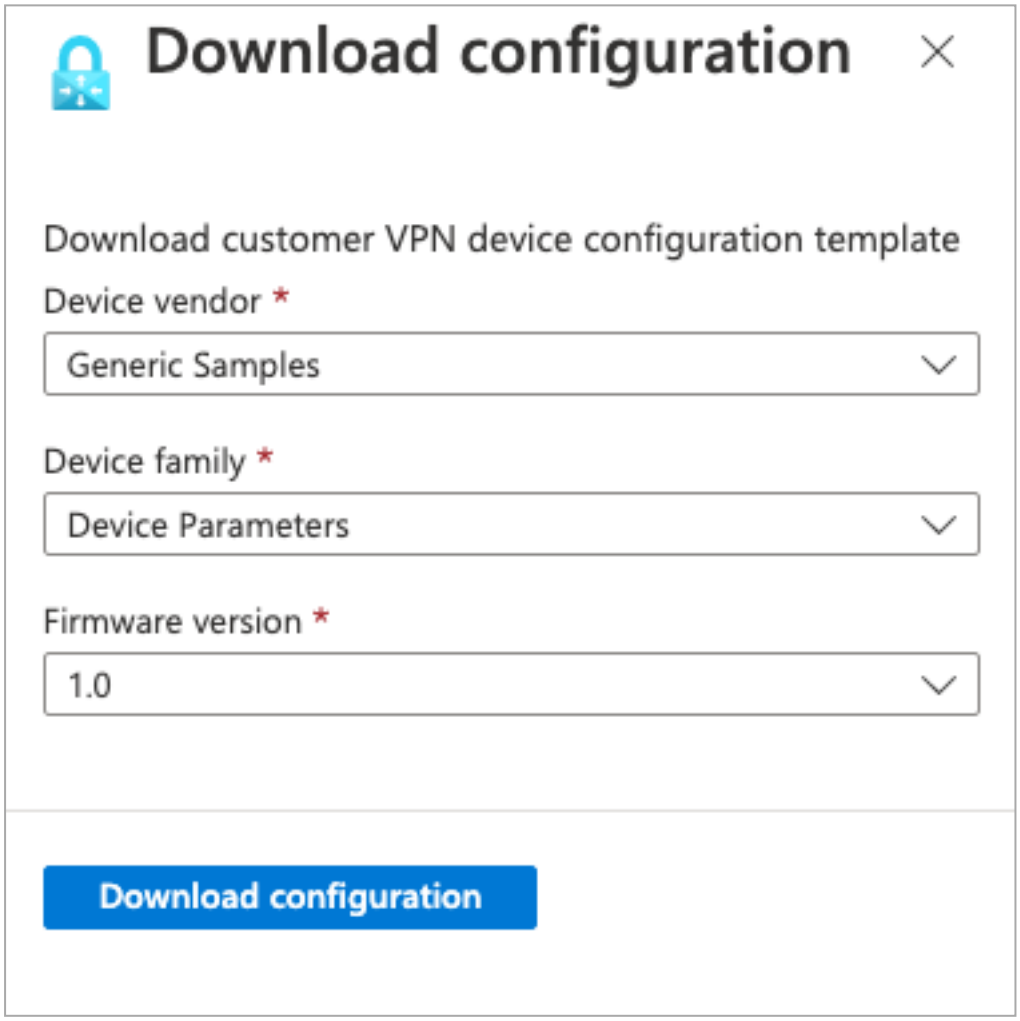
6. In the **General Settings** section, click **Upload File**.

Microsoft Azure

1. Access the Azure Management Portal and set up your Site-to-Site tunnel. For instructions, see *"Azure Virtual Network Gateway" on page 623*.
2. Go to your Virtual network gateway, click **Connections** and select your Check Point SASE connection.
3. Go to **Overview** and click **Download configuration**.



The **Download configuration** window appears.



4. Enter these:

a. **Device vendor** - Generic Samples.

b. **Device family** - Device Parameters.

c. **Firmware version** - 1.0.

5. Click **Download Configuration**.

   The system downloads the configuration file.

Tunnel Values

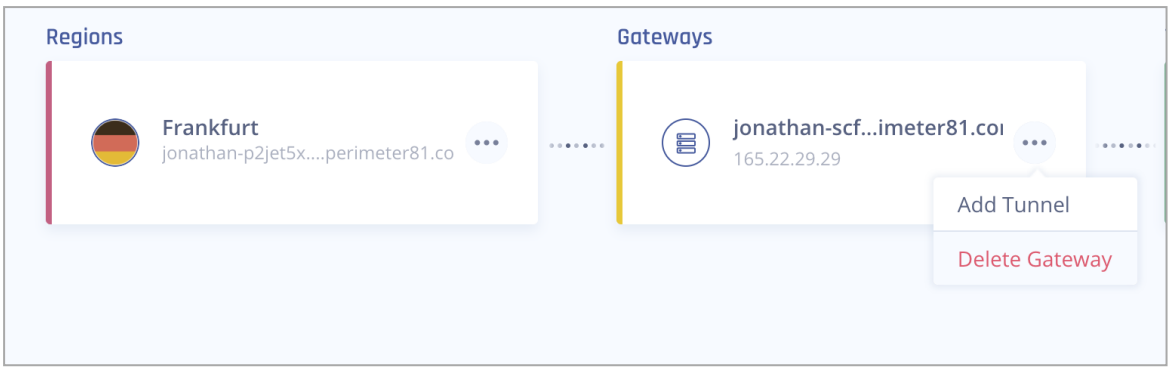
The tunnel values extracted from the configuration file are:

- **General Settings**:
  - Shared Secret (Pre-Shared Key)
  - SASE Gateway internal IP
  - Remote Public IP
  - Remote ID
  - Remote Gateway internal IP
  - Remote Gateway ASN (for redundant tunnels)
- **Advanced Settings**:
  - IKE Version
  - IKE Lifetime
  - Tunnel Lifetime
  - Dead Peer Detection Delay
  - Dead Peer Detection Timeout
  - Cipher Suites (Azure Only)

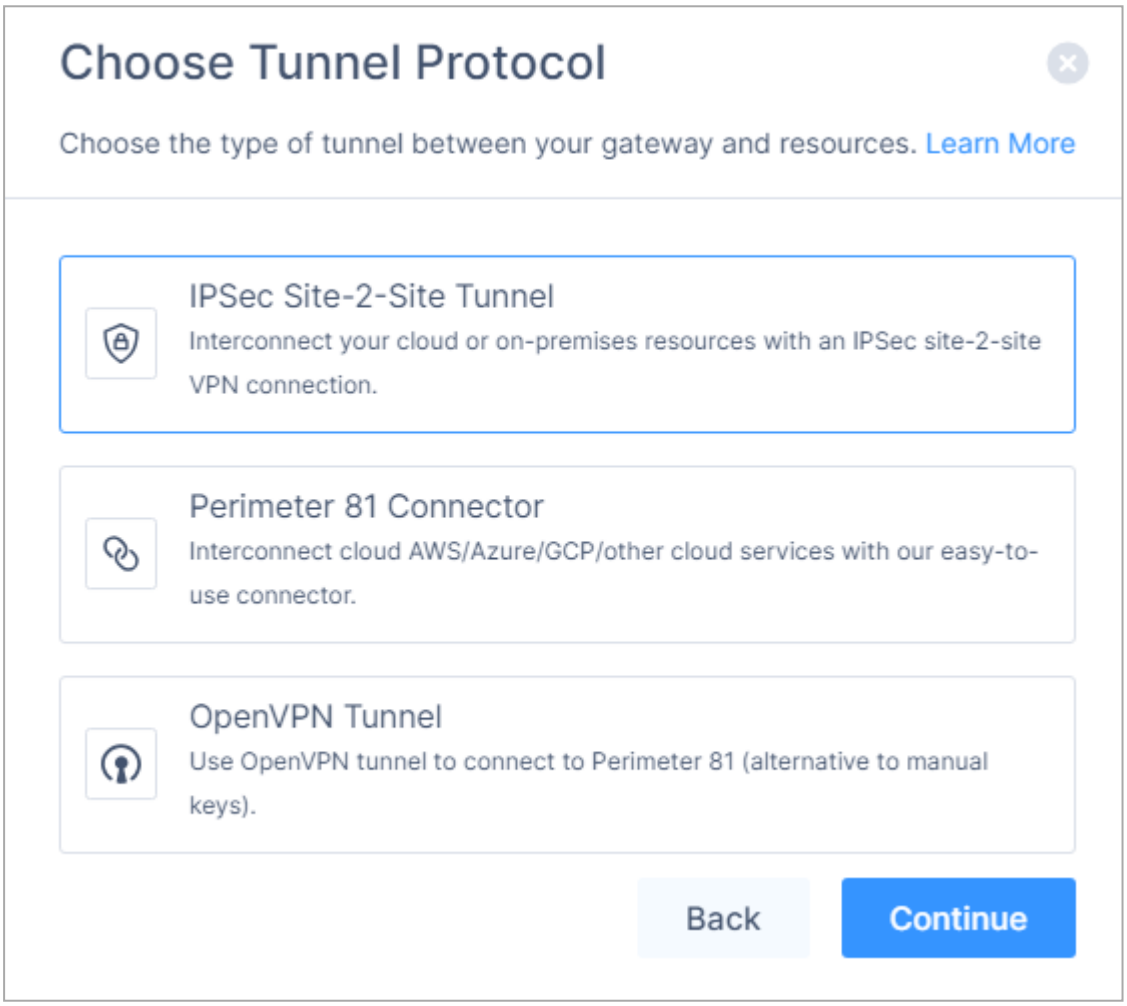
Uploading the Configuration File in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.

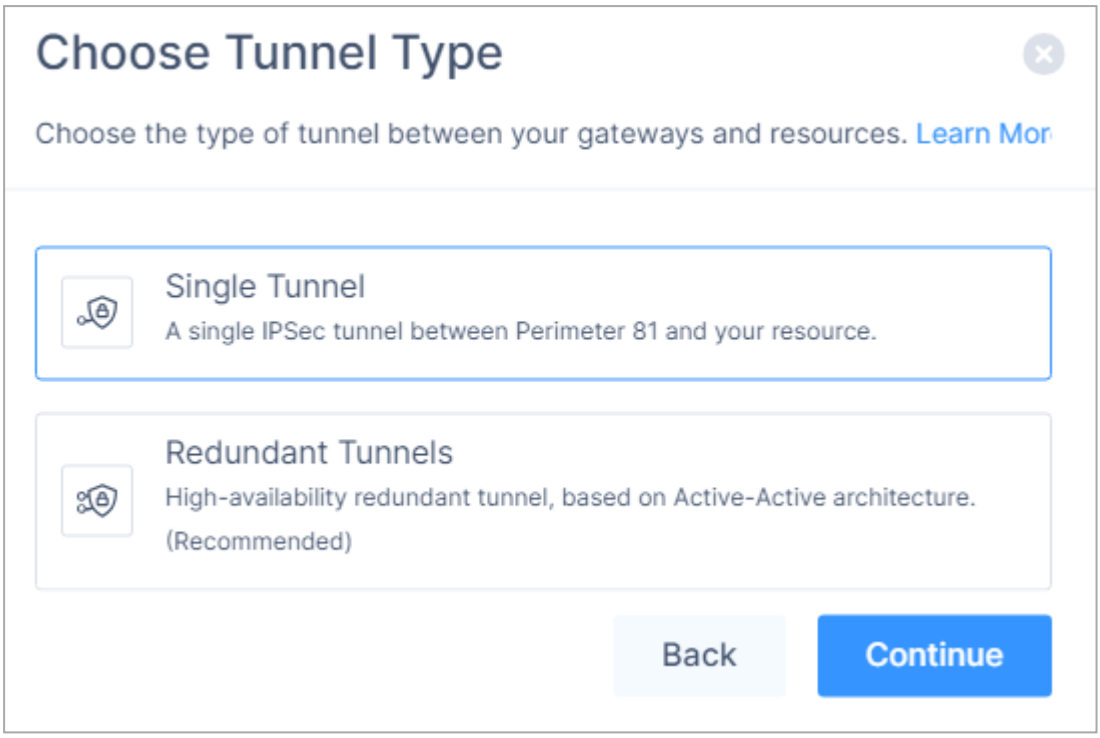
3. In the required gateway, click ··· > **Add Tunnel**.



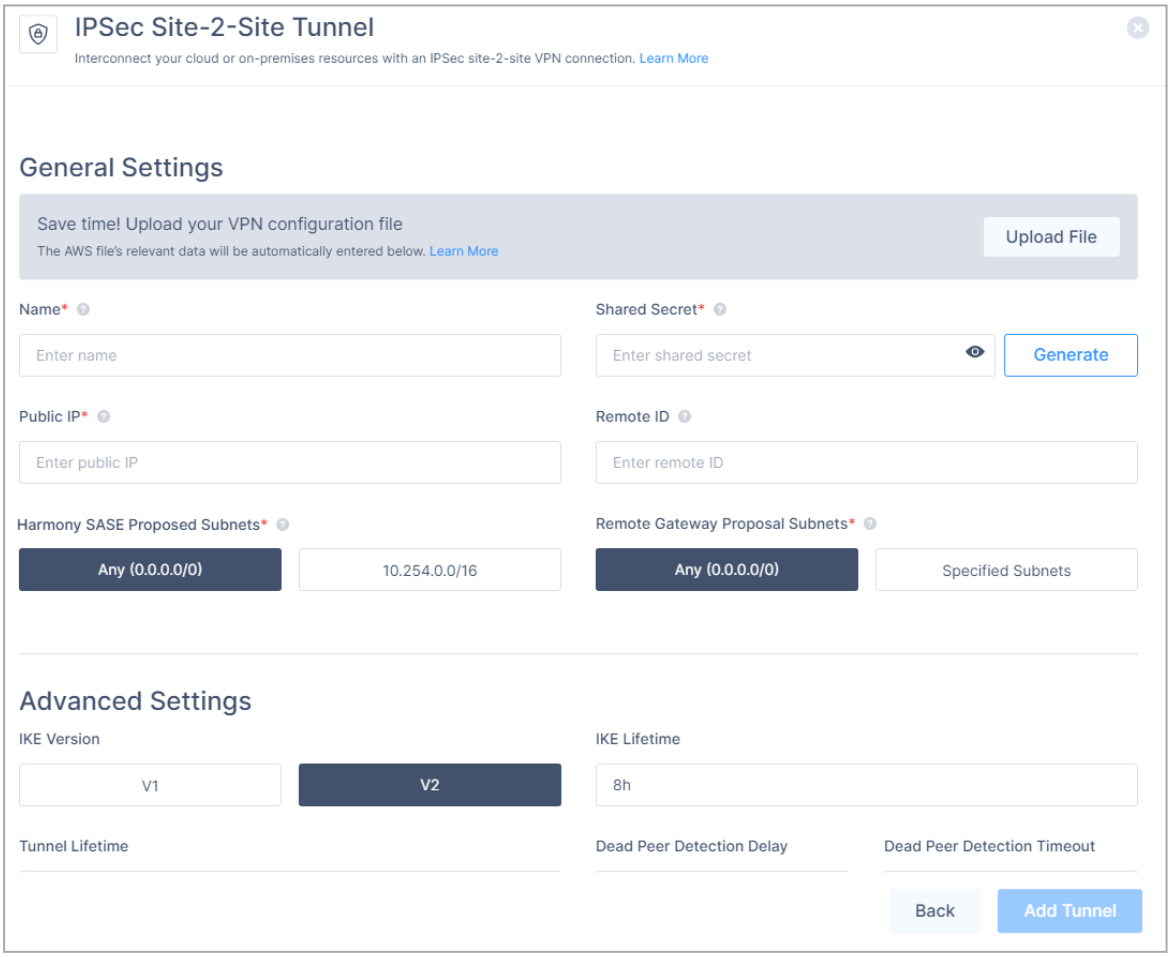
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, click **Upload File**.

Alibaba Cloud

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Step 1 - Configurations in Alibaba Cloud

Setting Up a Tunnel

1. Access the VPC console.
2. In the **Management Platform** on the left side, click **VPN** > **IPsec Connections**.
3. Select a region.
4. In the **IPsec Connections** page, click **Create IPsec Connection**.
5. In the **Create IPsec Connection** page, configure the IPsec-VPN connection with the following information:
    a. **Name** - Name of the IPsec-VPN connection.
    b. **VPN Gateway** - Select the VPN Gateway to connect. If there are no gateways, create a new gateway.
    c. **Customer Gateway** - Select the customer gateway to connect. If none exists, create a new one for the Check Point SASE gateway public IP address.
    d. **Local Network** - CIDR block of the VPC to be connected with the on-premises data center. This parameter is used for phase two negotiation.
    e. **Remote Network** - CIDR block of the on-premises data center to be connected with the VPC. This parameter is used for phase two negotiation (if you do not select a specific subnet).

    Check Point SASE default value is **10.255.0.0/16**.
    f. **Effective Immediately** - Yes.

g. **Advanced Configuration** - IKE Configurations

   i. **Pre-Shared Key** - Pre-shared key used for the authentication between the VPN Gateway and the customer gateway. By default, it is an automatically generated value. However, you can also specify a pre-shared key. This key should be used also in the Check Point SASE side.

   ii. **Version** - IKEv1

   iii. **Negotiation Mode** - Main mode

   iv. **Encryption Algorithm** - aes256

   v. **Encryption Algorithm** - sha1

   vi. **DH Group** - group2

   vii. **SA Life Cycle (seconds)** - SA lifecycle for phase one negotiation. The default value is 86,400 seconds.

   viii. **LocalId** - Local VPN Gateway public IP address

   ix. **RemoteId** - Check Point SASE gateway public IP address

h. **Advanced Configuration**: **IPSec Configurations**

   - **Encryption Algorithm** - aes256
   - **Authentication Algorithm** - sha1
   - **DH Group** - group2
   - **SA Life Cycle (seconds)** - SA lifecycle for phase two negotiation. The default value is 86,400 seconds.

i. **Health Check** - Optional

6. Click **OK**.

Setting Access Rules in Alibaba Security Groups

1. Access the VPC console and go to your security group associated with your server.
2. Add Allow rule with 10.255.0.0/16 object to the desired ports.

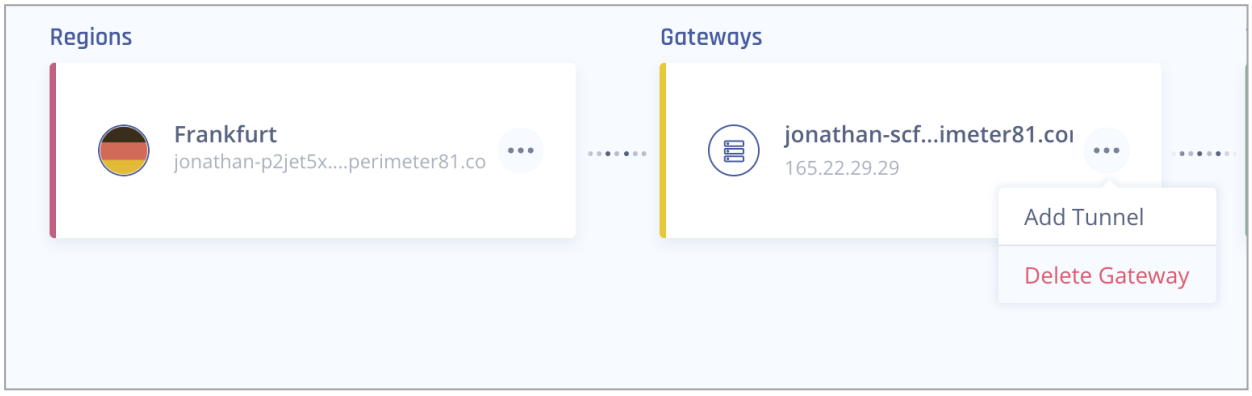
Setting Routes in Alibaba Cloud

1. Access the VPC console and go to your VPN.
2. Click **Route Tables**.
3. Add this route under the System route table or on your custom route table:

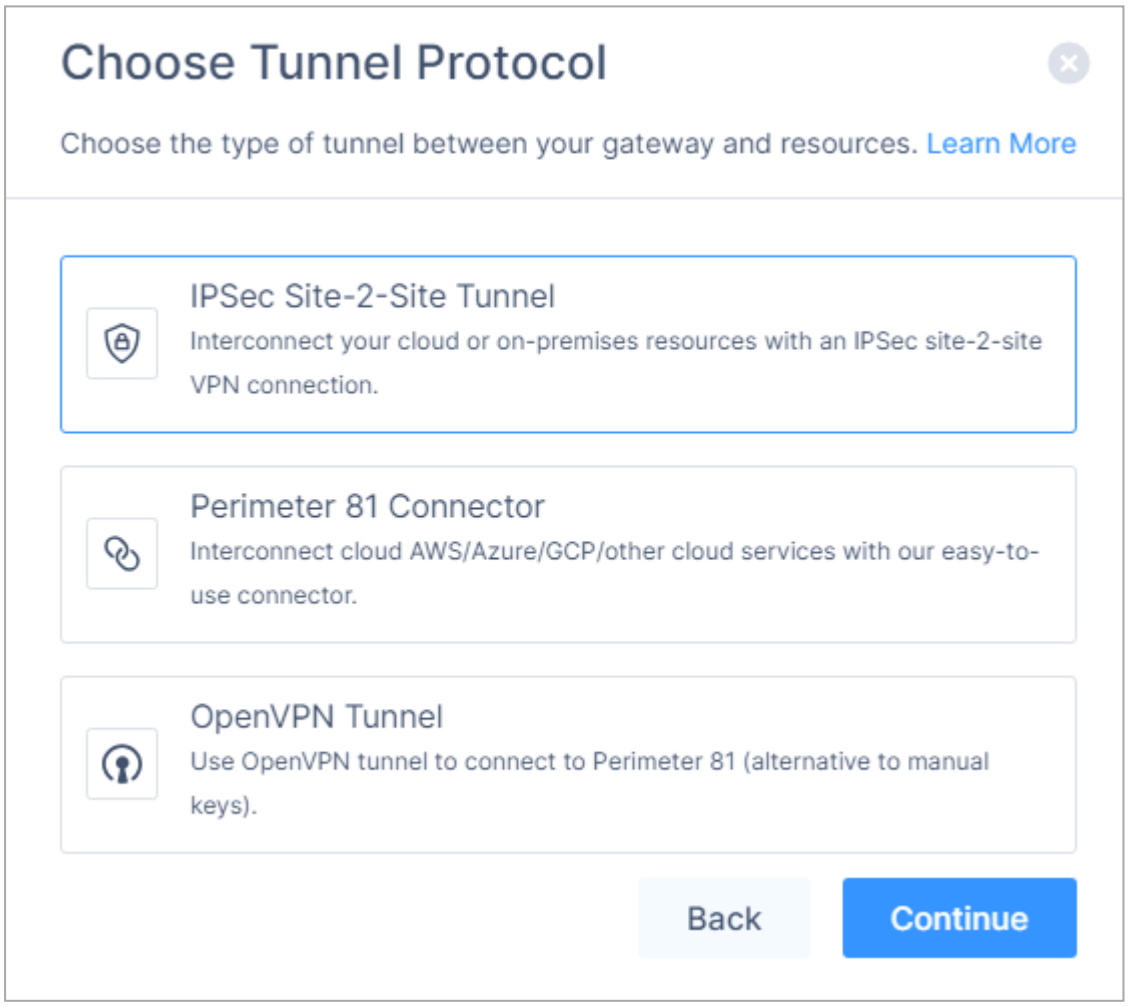
   10.255.0.0/16.

Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

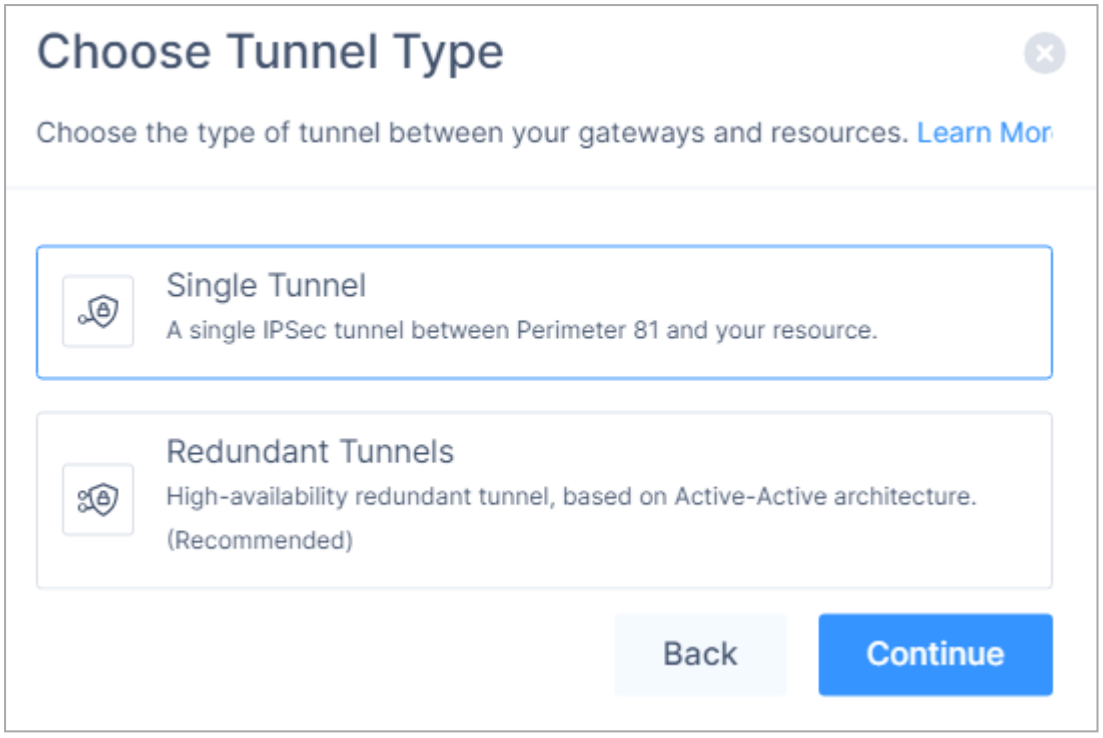
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



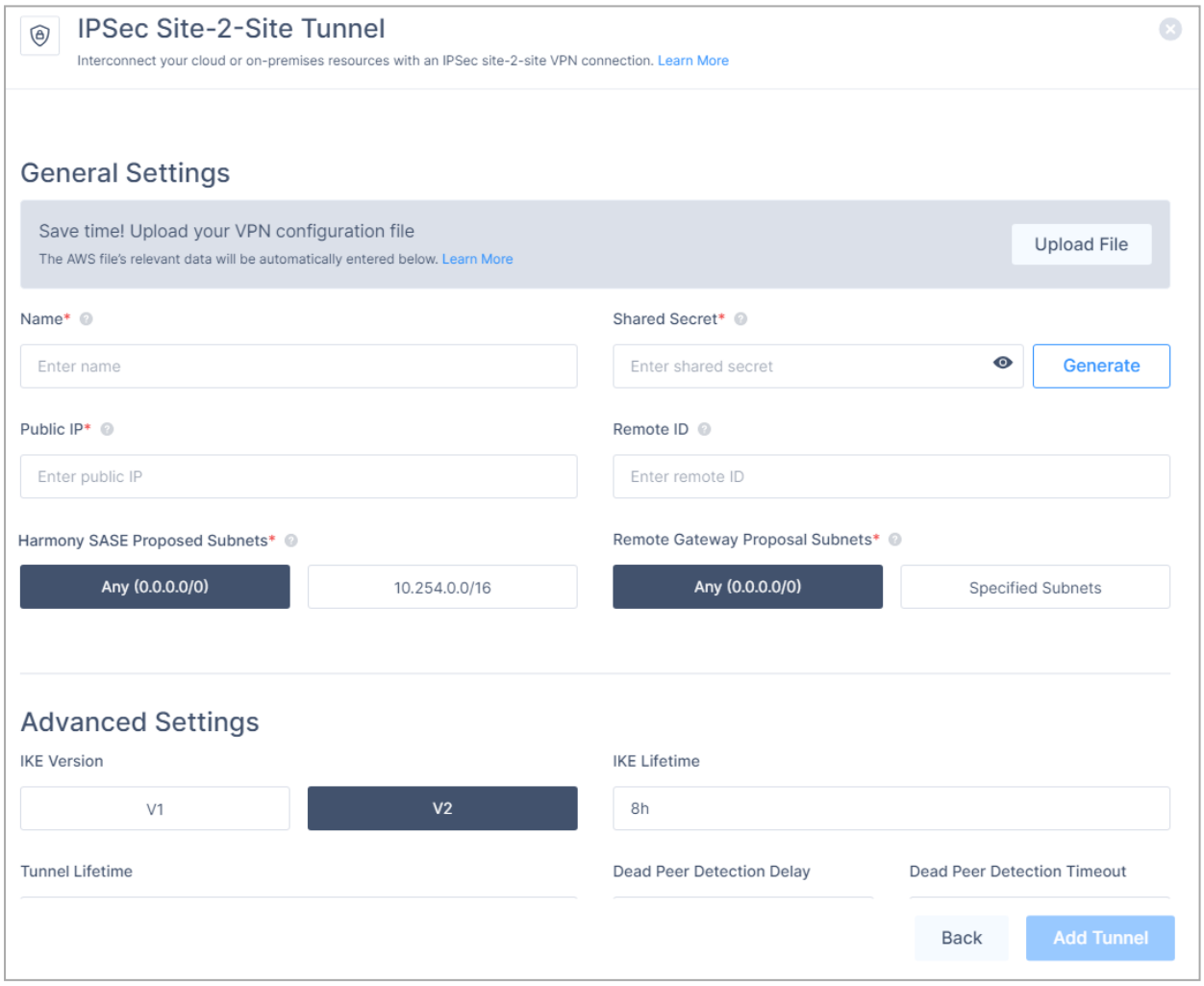
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
    a. **Name** - Name of the tunnel.
    b. **Shared Secret** - Shared secret you set in VPC console.
    c. **Public IP** and **Remote ID**: Enter Alibaba VPN Gateway Public IP address.
    d. In **Perimeter 81 Gateway Proposal Subnets**, select **Any** or **Specific Subnet**.

e. In **Remote Gateway Proposal Subnets**, enter your VPC console subnet/s.

f. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha512	sha512	ecp 521	ecp 521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha512	sha512	ecp 521	ecp 521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha512	sha512	ecp 521	ecp 521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha512	sha512	ecp 521	ecp 521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes 256	aes 256	sha512	sha512	ecp 521	ecp 521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes 256	aes 256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes 256	aes 256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes 256	aes 256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

7. Click **Add Tunnel**.

AWS Virtual Gateway

This chapter describes the process to establish a Site-to-Site IPsec tunnel between your Check Point SASE network and your AWS environment.

Use this configuration if your connection is intended for a single Virtual Private Cloud (VPC).

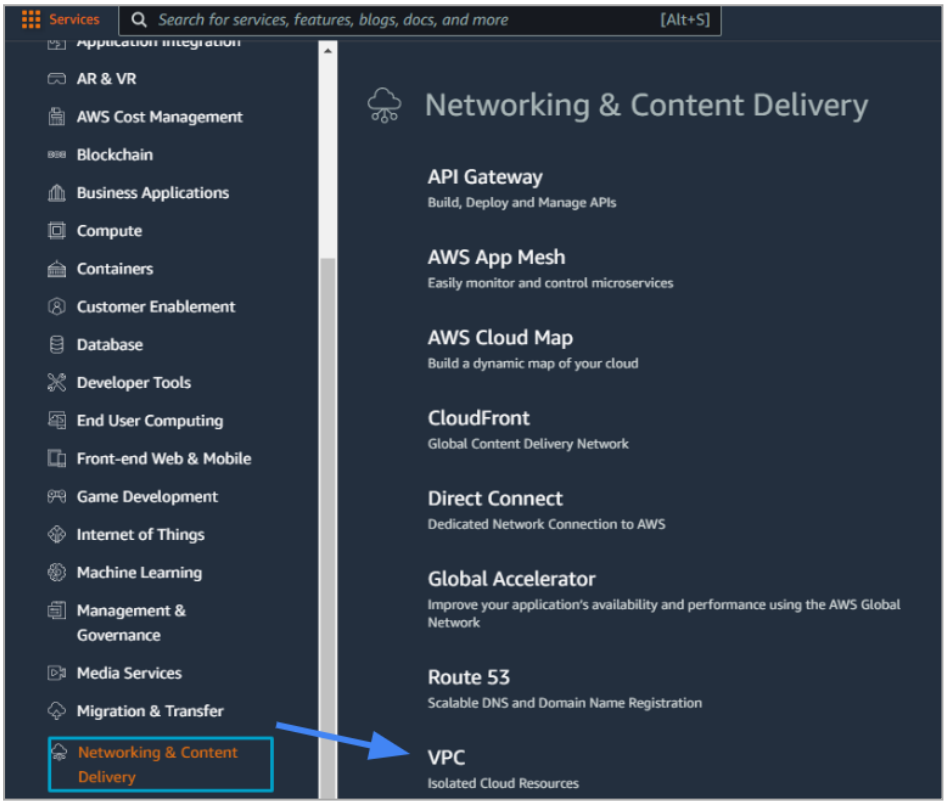
If you have multiple VPCs, see *"AWS Transit Gateway" on page 575*.

Prerequisites

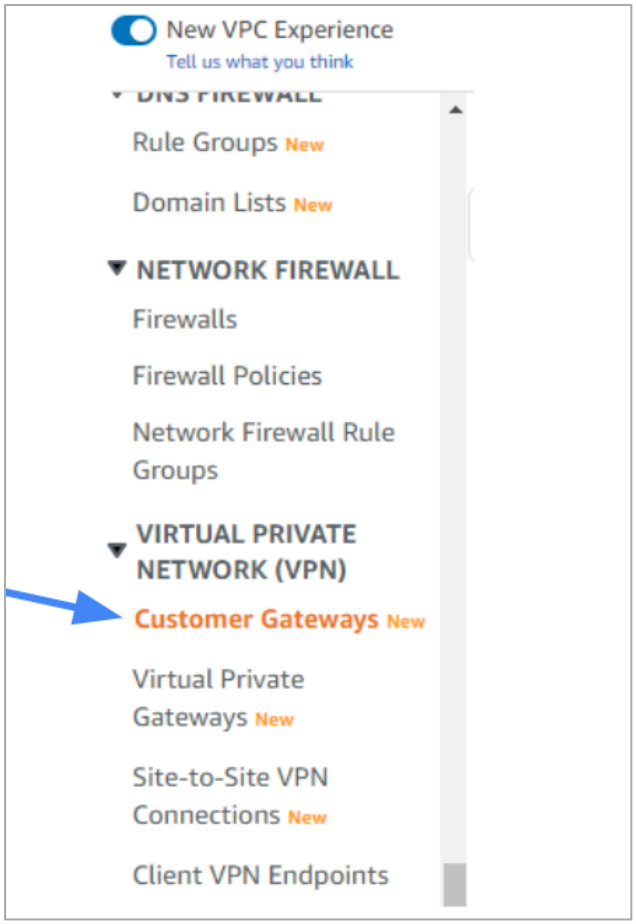
- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Step 1 - Configuring the Tunnel in the AWS Management Console

1. Access the AWS Management console and go to the **VPC** section.
2. In the **Services** section, scroll down to **Networking & Content Delivery** and select **VPC**.



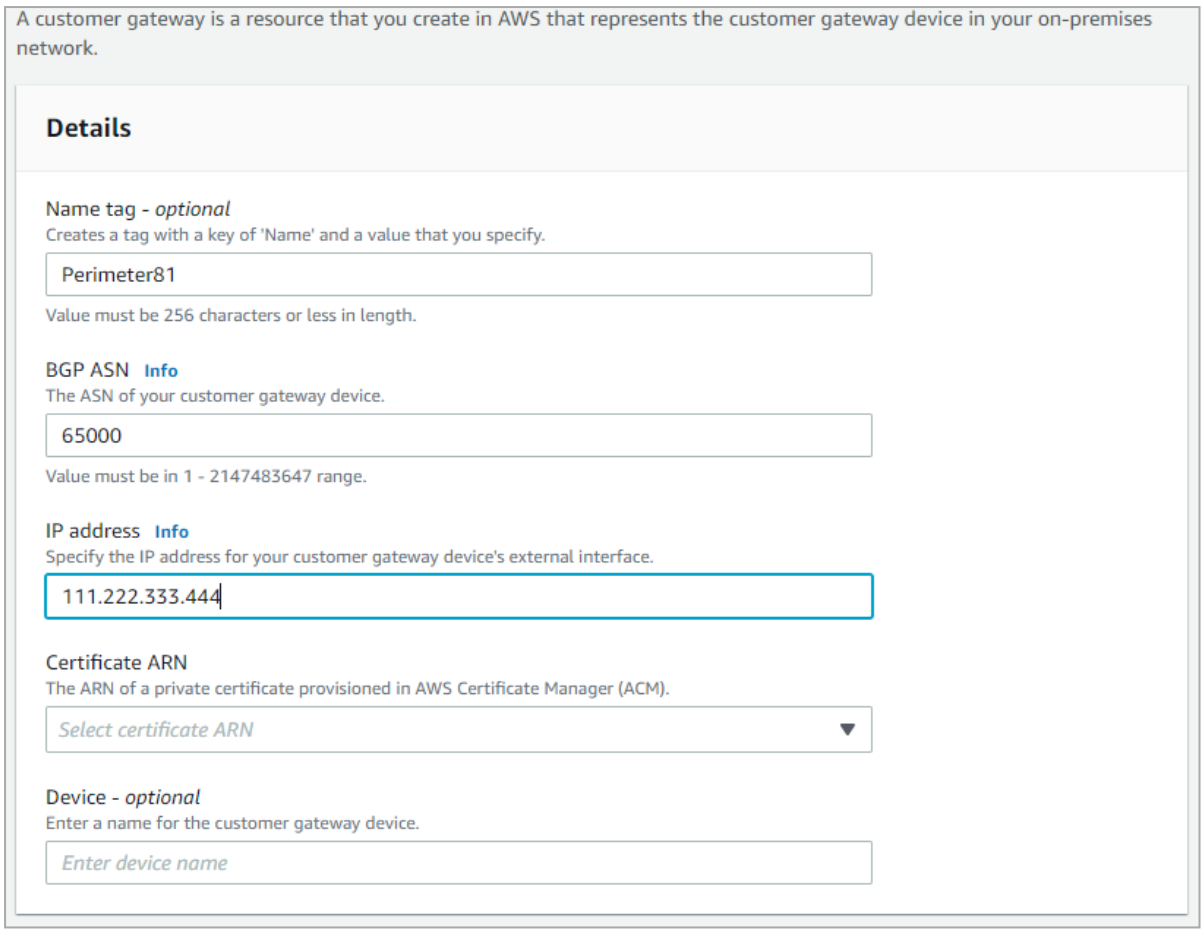
3. In the left menu **Virtual Private Network (VPN)** section, click **Customer Gateways**.



4. Click **Create Customer Gateway**.
5. Click **static** routing.
6. Enter the IP Address of the Check Point SASE Gateway. To get the IP Address, go to the Check Point SASE Administrator Portal and see the **Networks** page.

7. Select **Create Customer Gateway**.

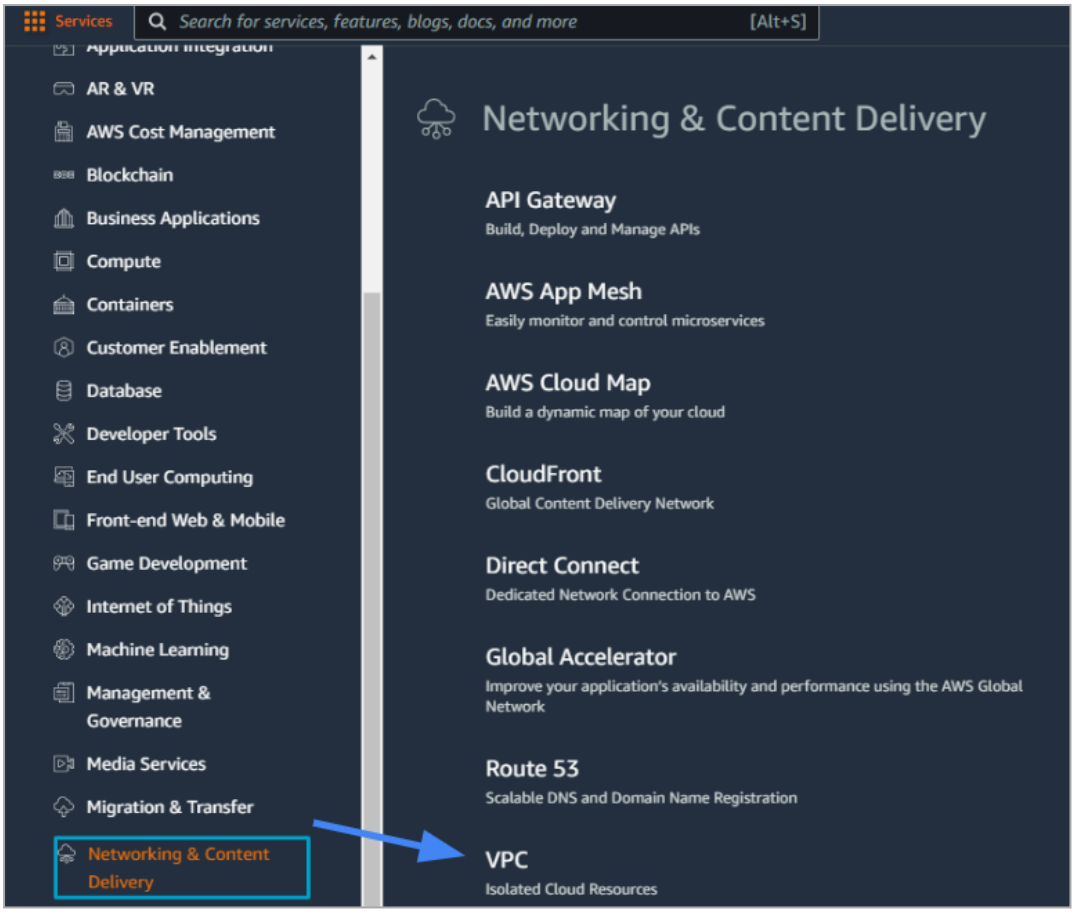
   A message displays to indicate that the gateway was created successfully.



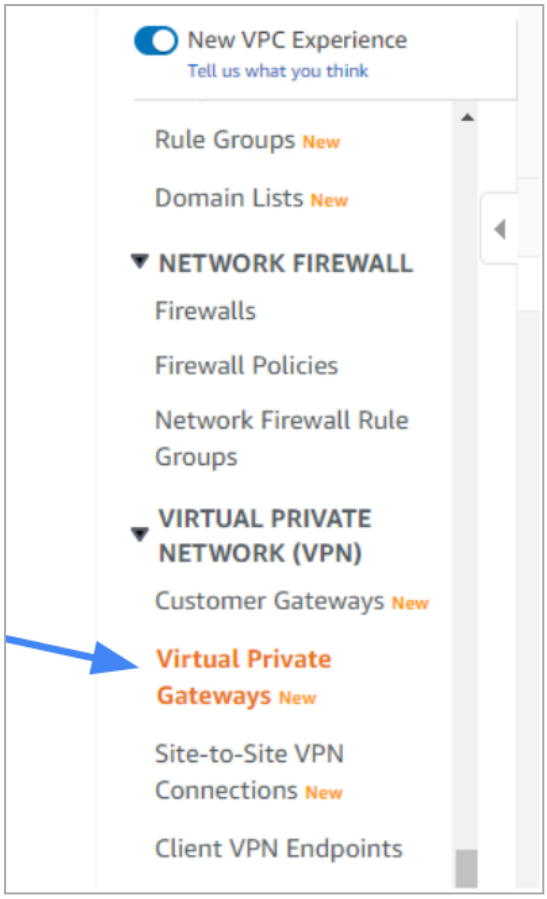
Configuring a Virtual Private Gateway

Important - If you already have a virtual private gateway attached to your VPC, skip this section and continue with *"Creating a Virtual Private Network Connection" on page 563*.

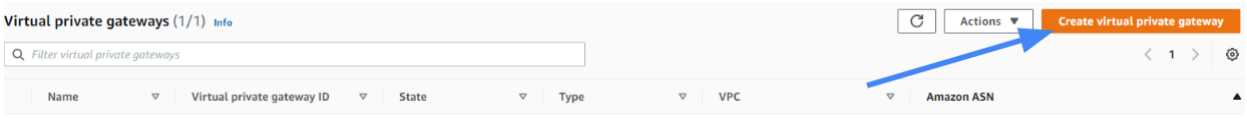
1. Access the AWS Management console and go to **Services**, scroll down to **Networking & Content Delivery** and click **VPC**.



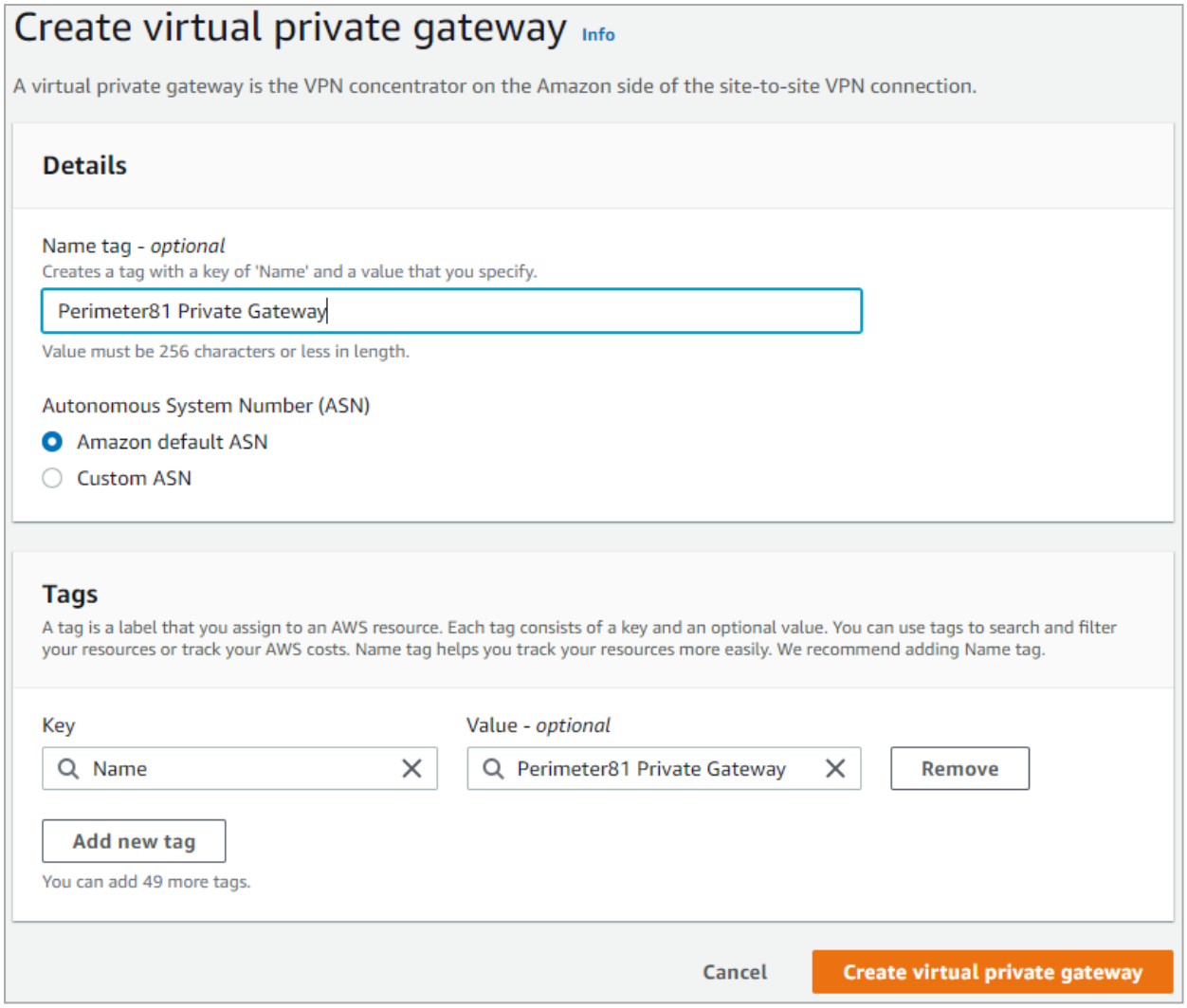
2. On the left menu, go to **Virtual Private Network (VPN)** > **Virtual Private Gateways**.



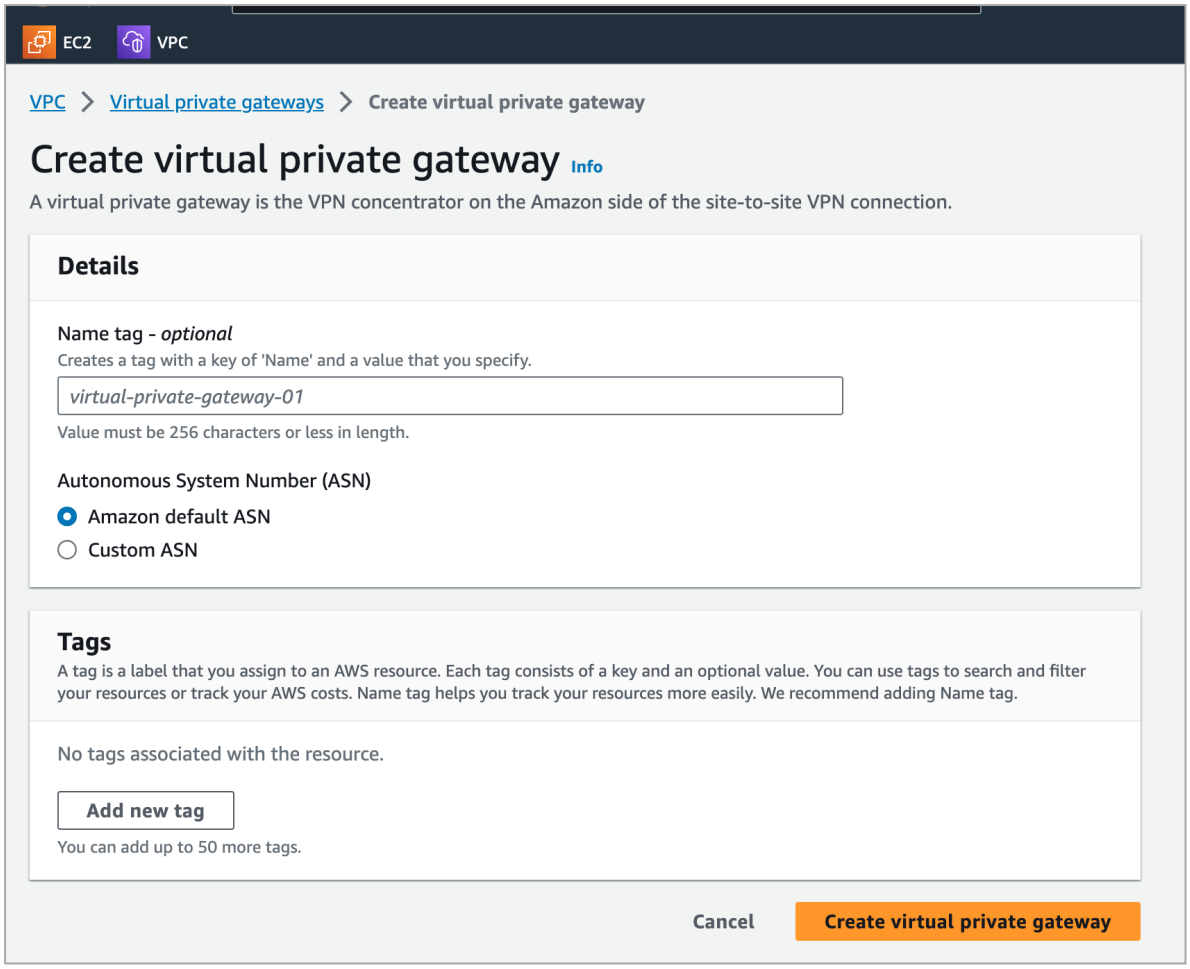
3. Click **Create Virtual Private Gateway**.



The **Create virtual private gateway** window appears.

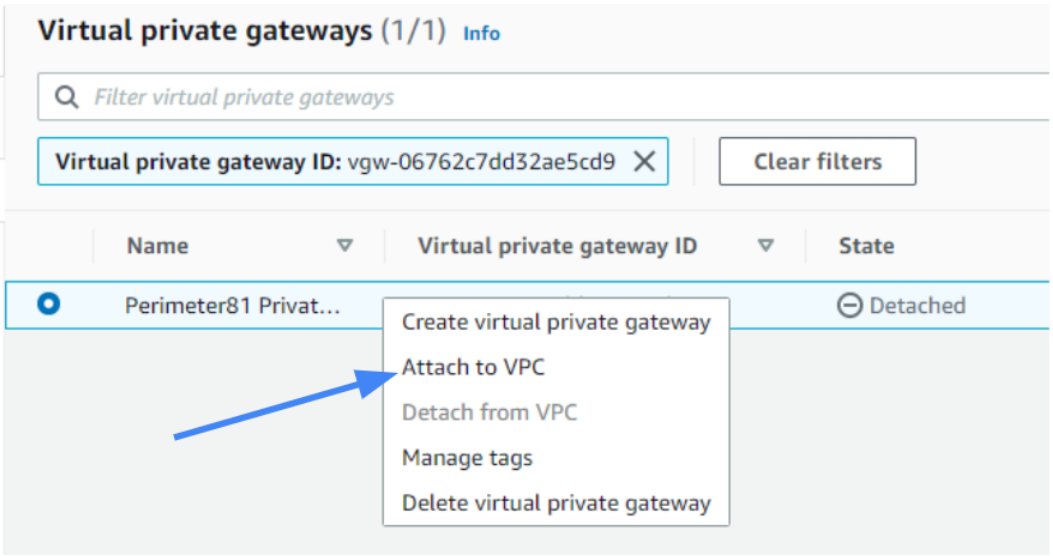


4. In the **Name** field, enter the name of the gateway, for example US_HQ.
5. In the **ASN** field, click **Amazon default ASN**.
6. Click **Create virtual private gateway**.



The systems displays a message that the virtual Private Gateway was created successfully.

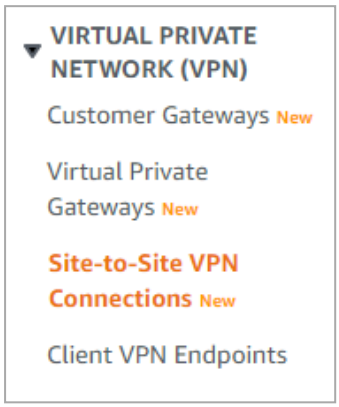
7. Select the newly created gateway and click **Actions**. On the context menu, select **Attach to VPC**.



8. From the drop-down menu, select the VPC and select **Yes, Attach**.

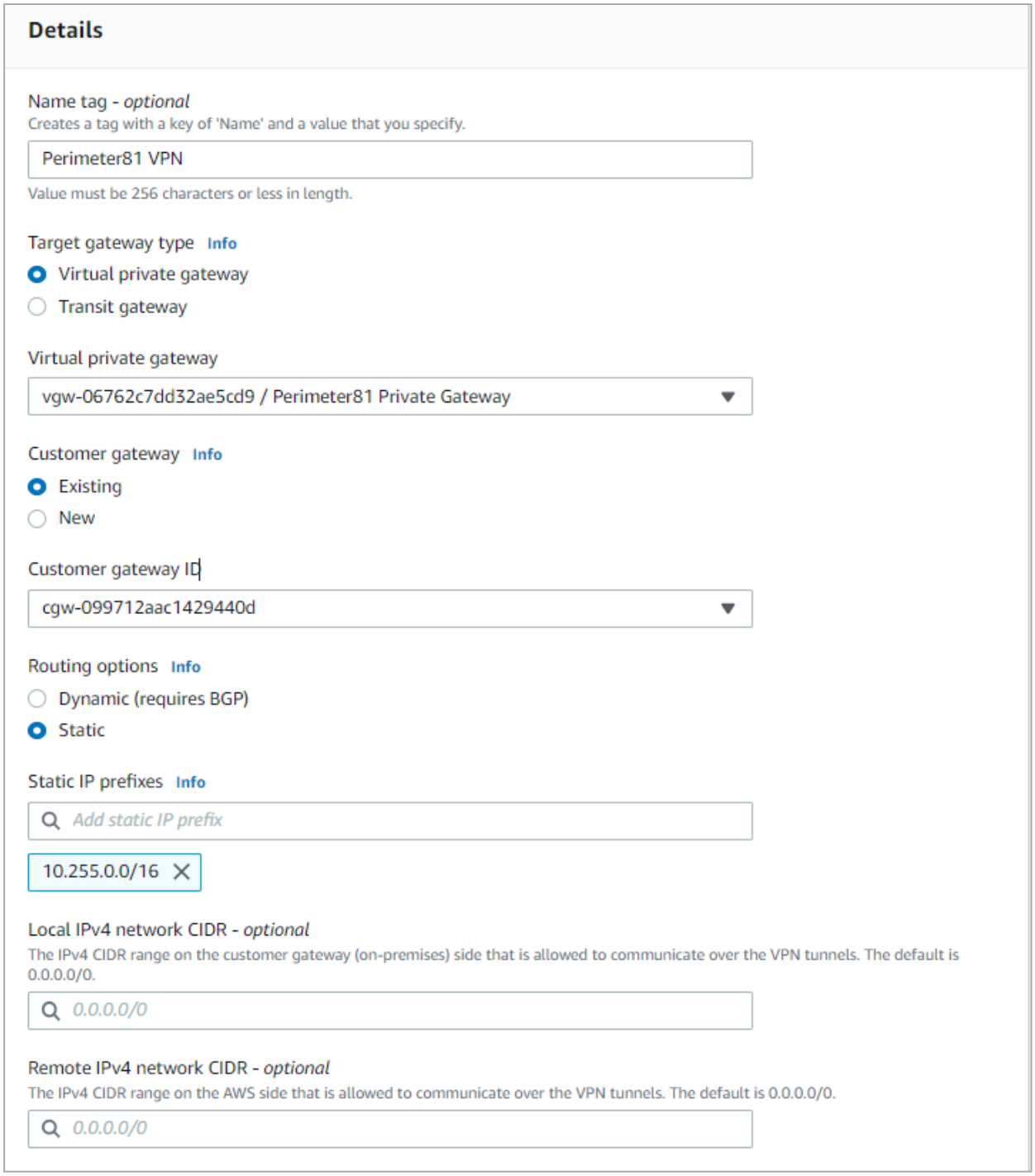
Creating a Virtual Private Network Connection

1. Access the AWS Management console and go to **Services**, scroll down to **Networking & Content Delivery** and click **VPC**.
2. On the left menu, go to **Virtual Private Network** > **Site-to-SiteVPN Connections**.



3. Click **Create VPN Connection**.

The **Create VPN Connection** window appears.



4. In the **Name** field, enter the name tag (for example, US_HQ).
5. In the **Target gateway type** field, click **Virtual private gateway**.
6. In the **Customer gateway** field, click **Existing**.
7. From the **Customer gateway ID** list, select the **Customer Gateway** that you have created.
8. In the **Routing Options** field, select **Static**.

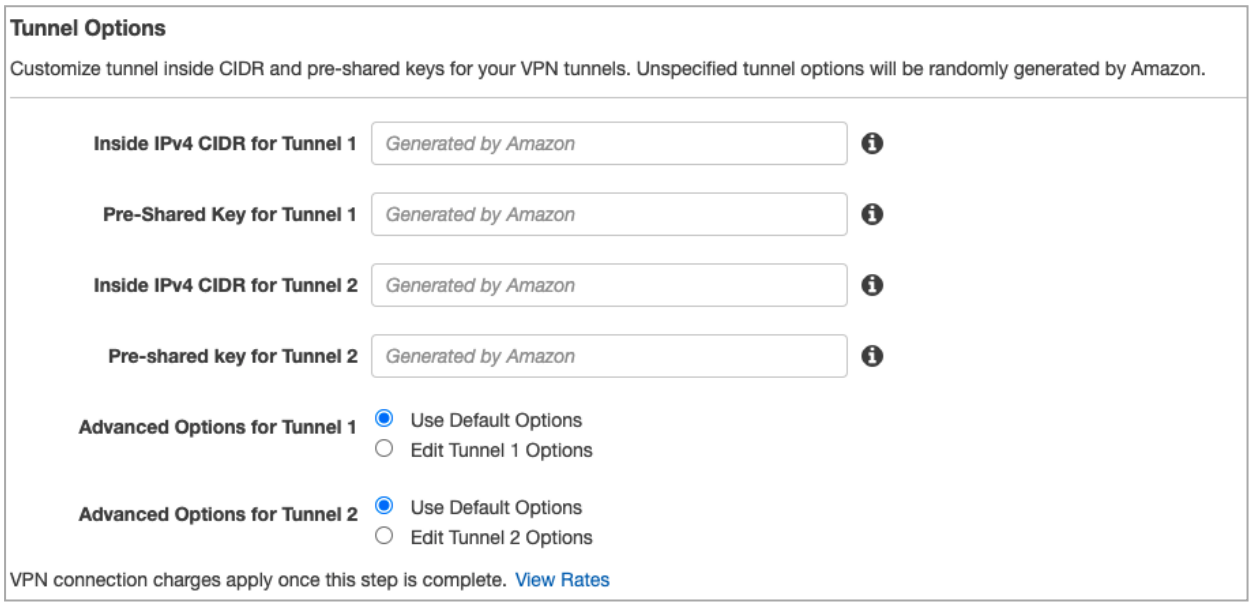
9. In the **Static IP prefixes** field, enter your Check Point SASE network subnet (Usually 10.255.0.0/16).

   Important - This address might differ if you have not chosen the default subnet mask for your tunnel.

10. In **Tunnel Options** section:

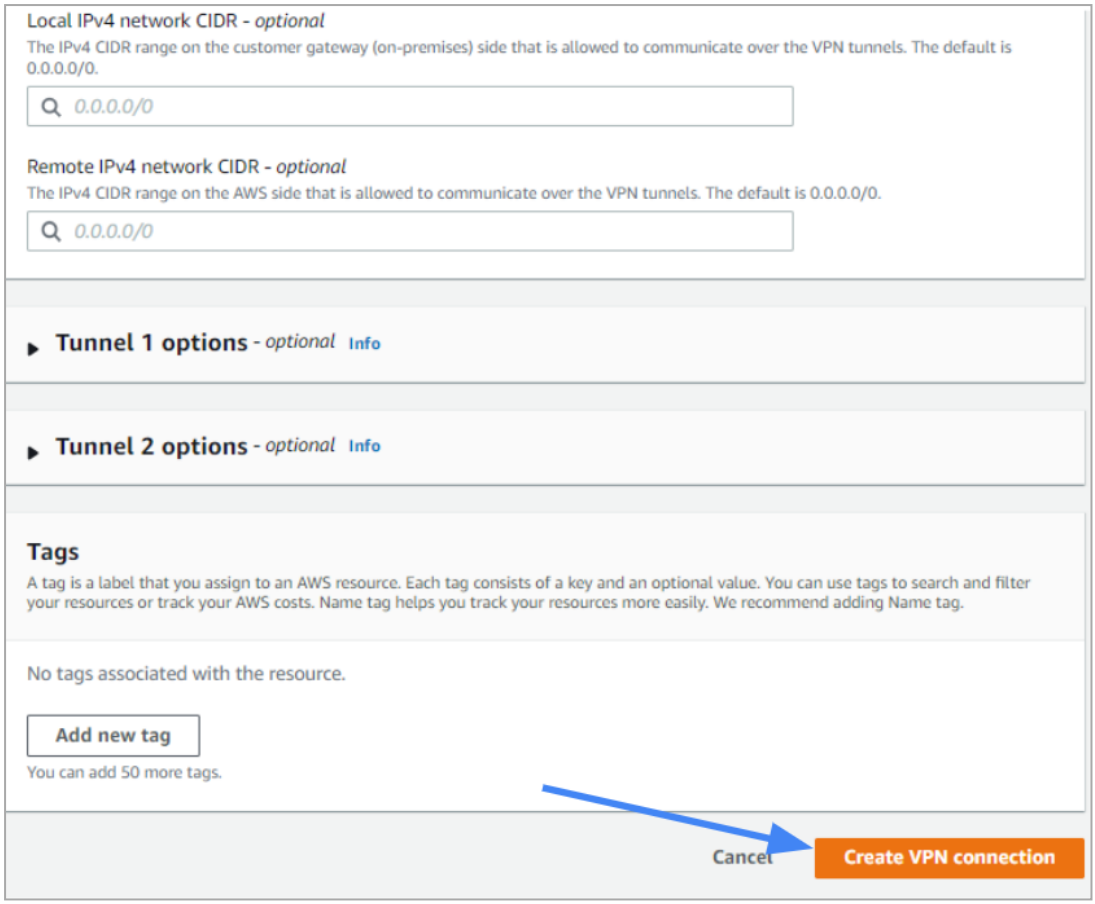
    a. In **Advanced Options**, select **Edit Tunnel Options**.

    b. In **DPD timeout**, set the value to **60**.



Note - AWS supports various types of encryption and hash formats for both the tunnels. If the tunnel options are set to default (as shown below) it accepts any encryption suite you want for the handshake with Check Point SASE. In this screen, you can also select the inside subnets you want to connect through the tunnel.

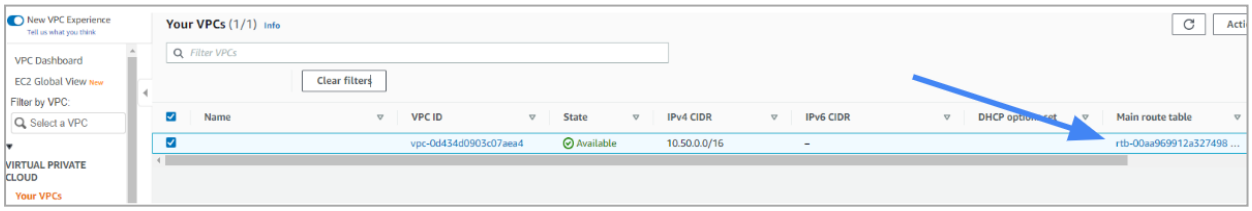
11. Click **Create VPN connection**.



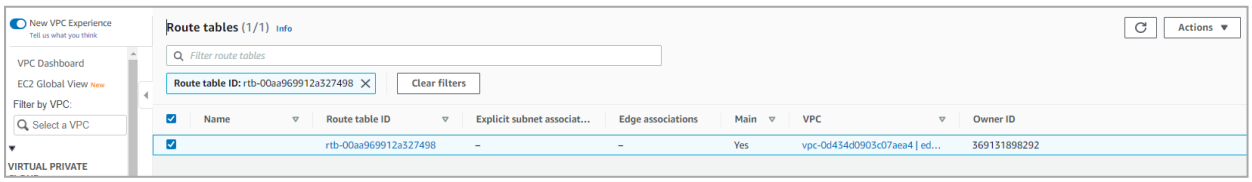
The system displays a message that a VPN Connection Request was created successfully.

Configuring the Routing Rules to the Default Gateway

1. Access the AWS Management console and go to the **VPC** section.
2. Enter the Route table associated with your VPC.

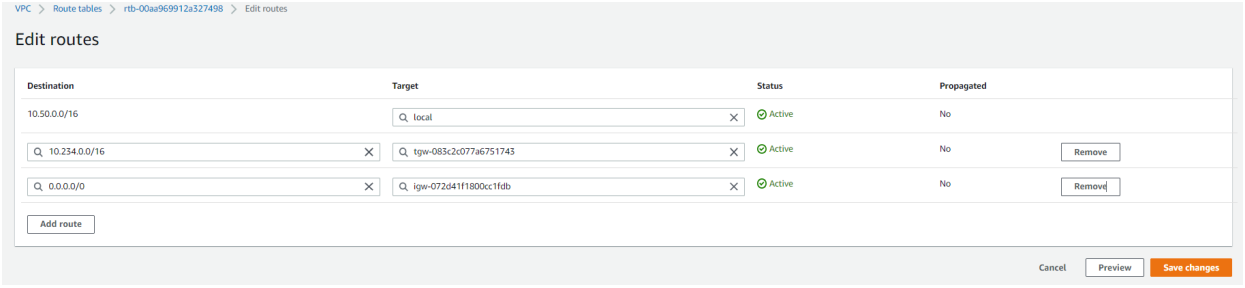


3. In the **Route Tables** menu option, select the routing table associated with the VPC you have created for the tunnel.



4. Click **Edit**.

The **Edit routes** window appears.



5. Add the new static routes for these subnets:

   a. In the **Destination** field, enter your Check Point SASE network subnet listed in the Check Point SASE Administrator Portal (**Networks** > **Gateway** > **Settings**)

   Usually 10.255.0.0/16

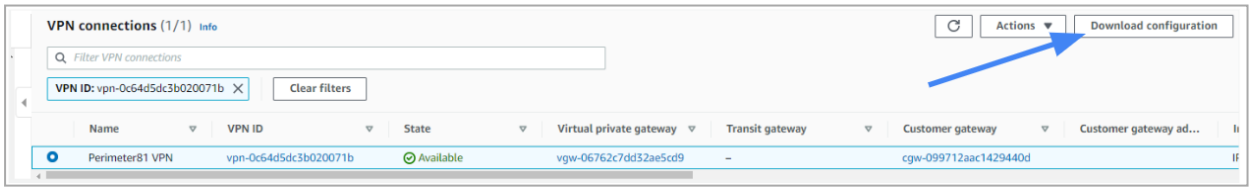
   b. In the **Target** field, enter your new VPN Gateway ID as the target (it appears under the subcategory Virtual Private Gateway).

6. Click **Save changes**.

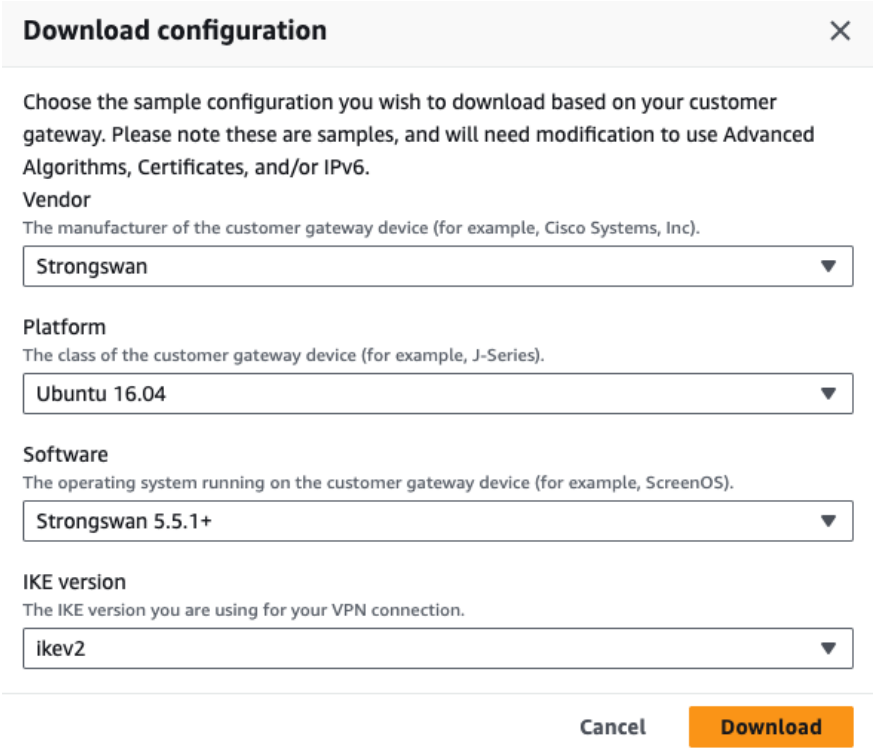
Note - If you have a customized security group associated with your VPC, configure your AWS security groups to allow all traffic from Check Point SASE subnets (usually 10.255.0.0/16) or allow only particular traffic using the port and IP restrictions.

Configuring the Tunnel

1. Access the AWS Management console and go to **Site-to-Site VPN Connections** and click **Download configuration**.

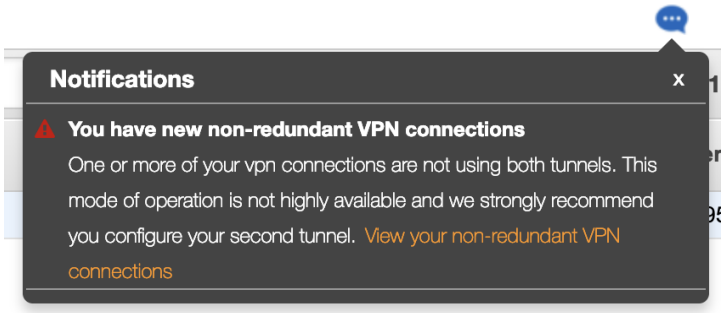


The **Download configuration** window appears.



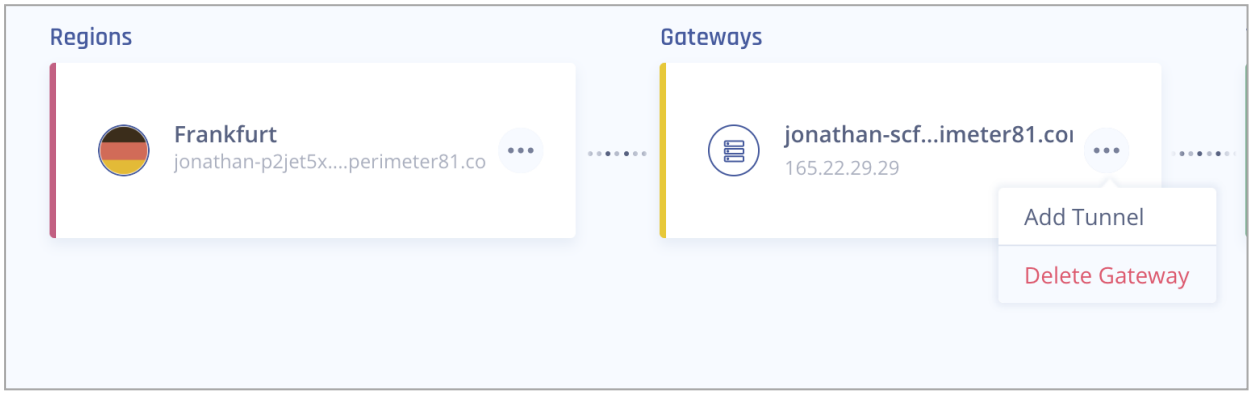
2. Enter these:
    a. **Vendor** - Strongswan
    b. **Platform** - Ubuntu 16.04
    c. **Software** - Strongswan version.
    d. **Ike version** - Ikev2
3. Click **Download**.

Important - When you examine the configuration file, you may notice that AWS has created two separate tunnels for the same VPN connection, however Check Point SASE utilizes only one of them.
We recommend you to use the one that appears first in the file.

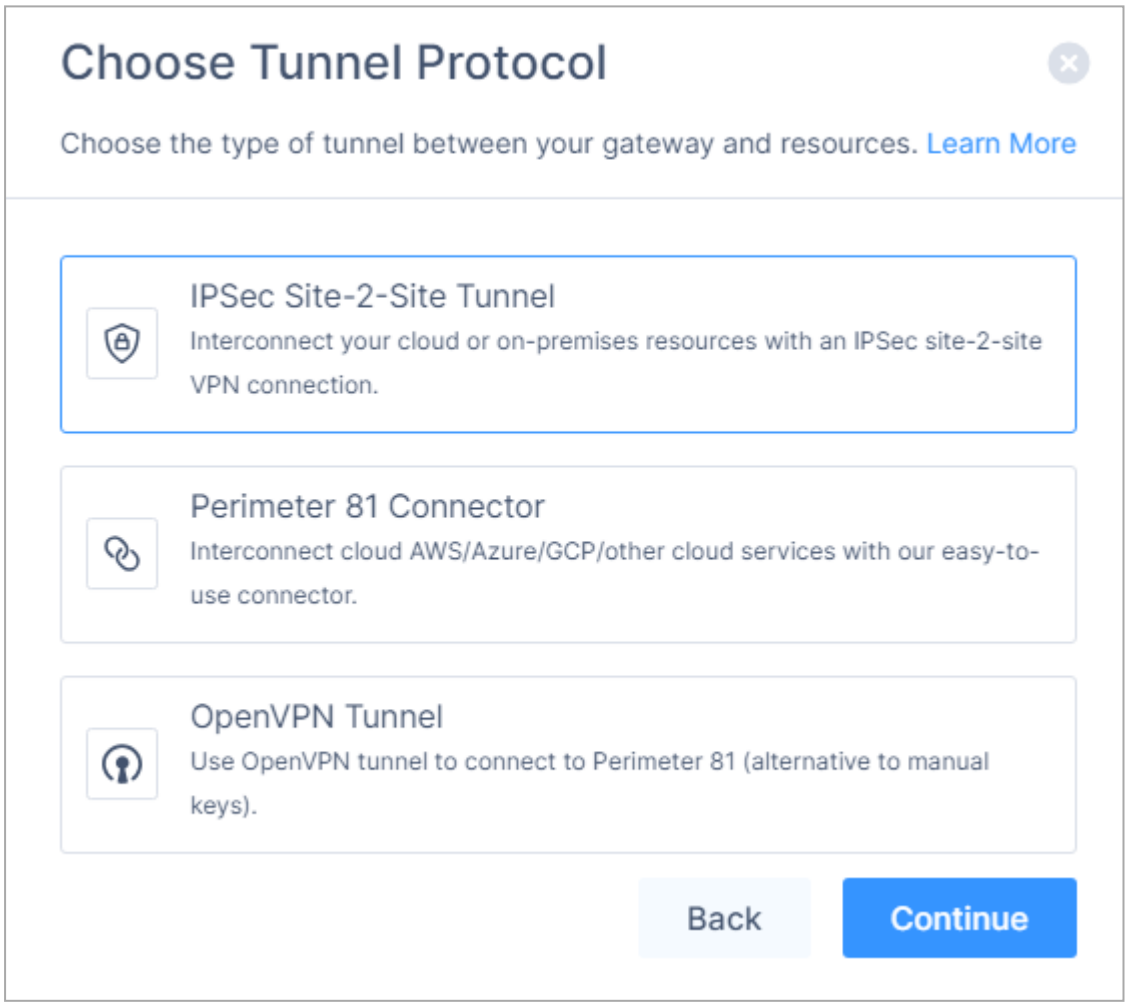


Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

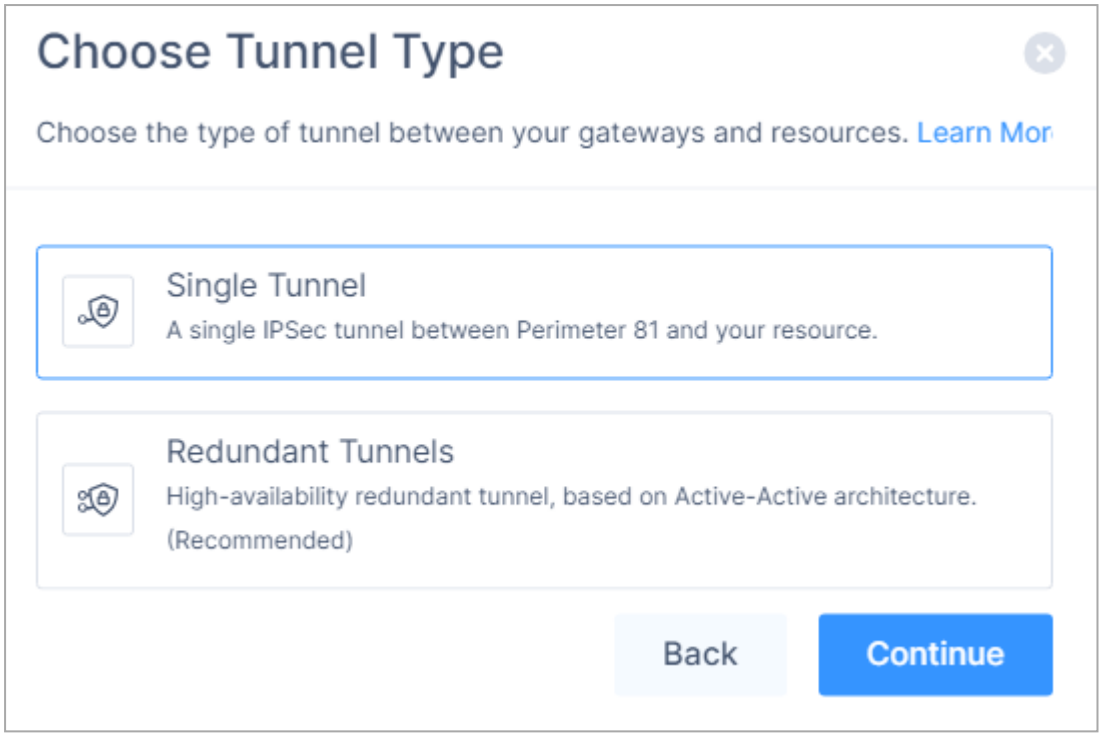
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



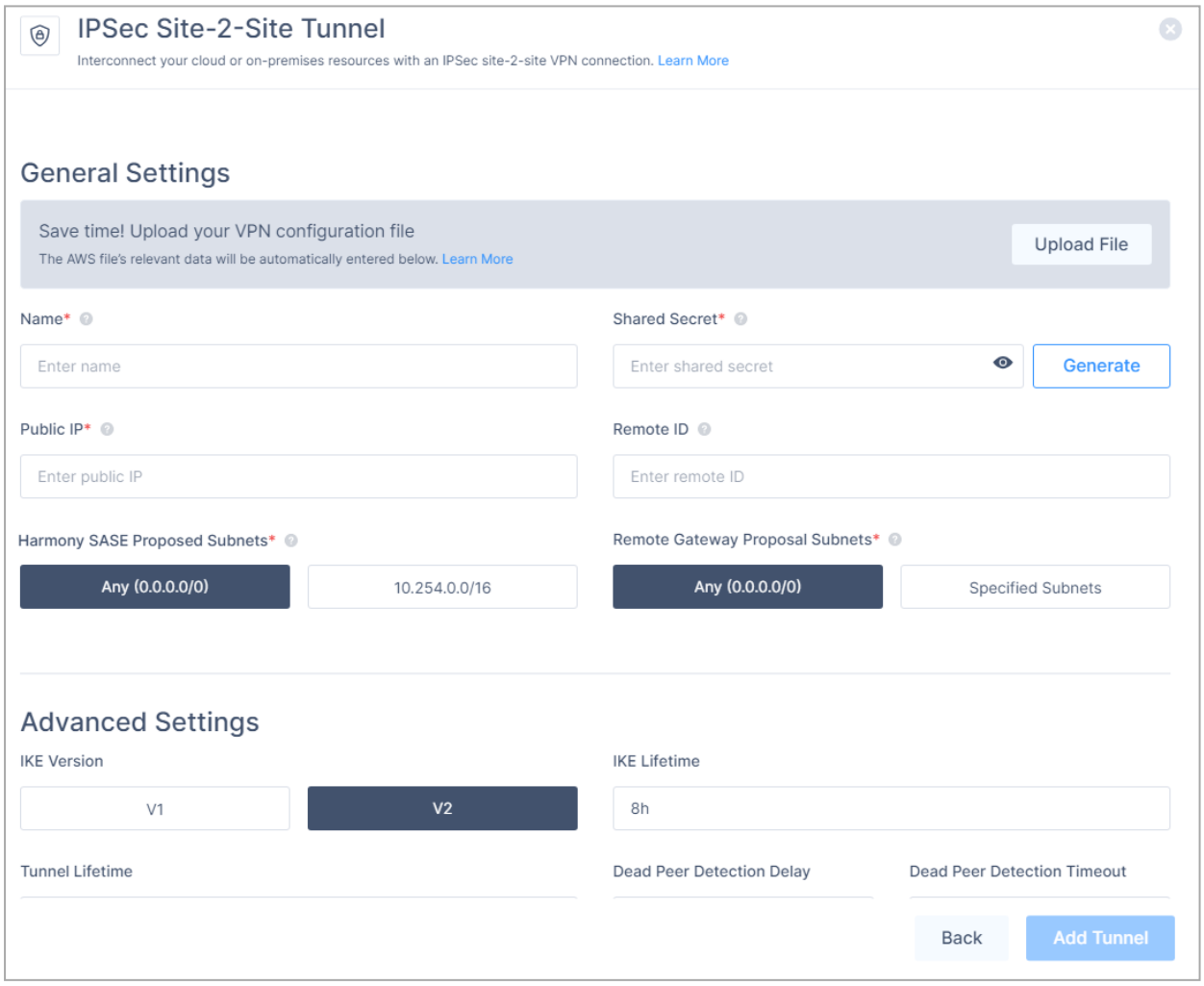
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.

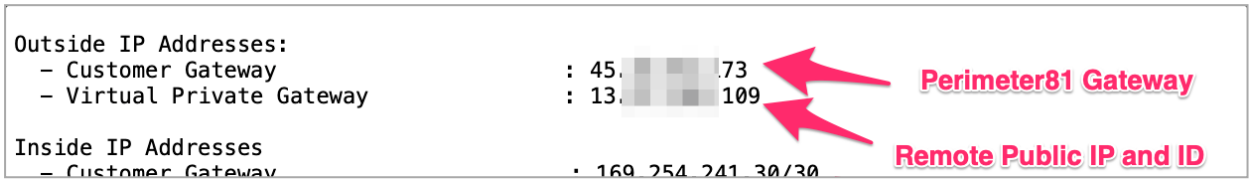


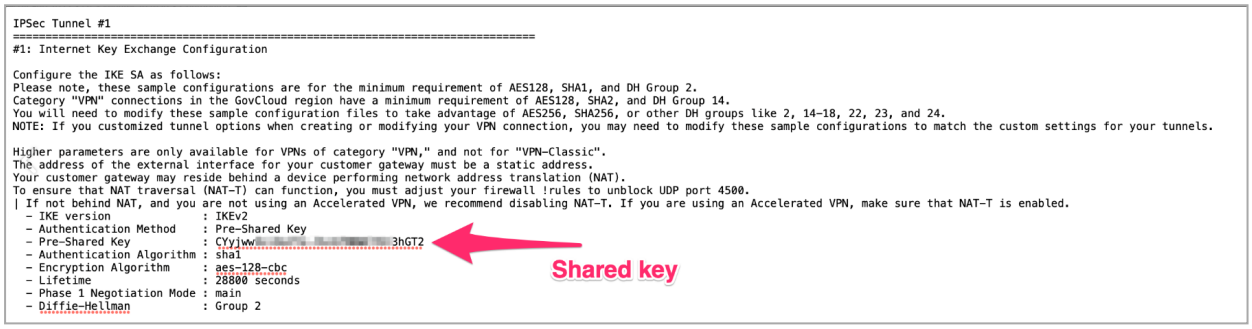
The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the AWS Management console.

7. For manual configuration, open the configuration file you downloaded and copy the below values and paste it for **Public IP**, **Remote ID** (both identical), and **Shared Secret**.



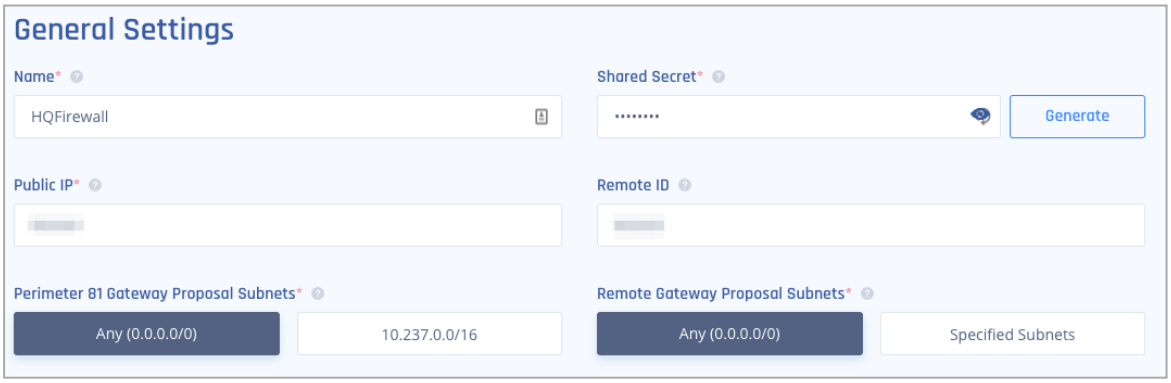


8. In the **General Settings** section, enter these:

   a. **Name** - Name of the tunnel.

   b. **Perimeter 81 Gateway Proposal Subnets** - **Any (0.0.0.0/0)**.

   c. **Remote Gateway Proposal Subnets** - **Any (0.0.0.0/0)**.



9. In the **Advanced Settings** section, enter the information for your tunnel type:

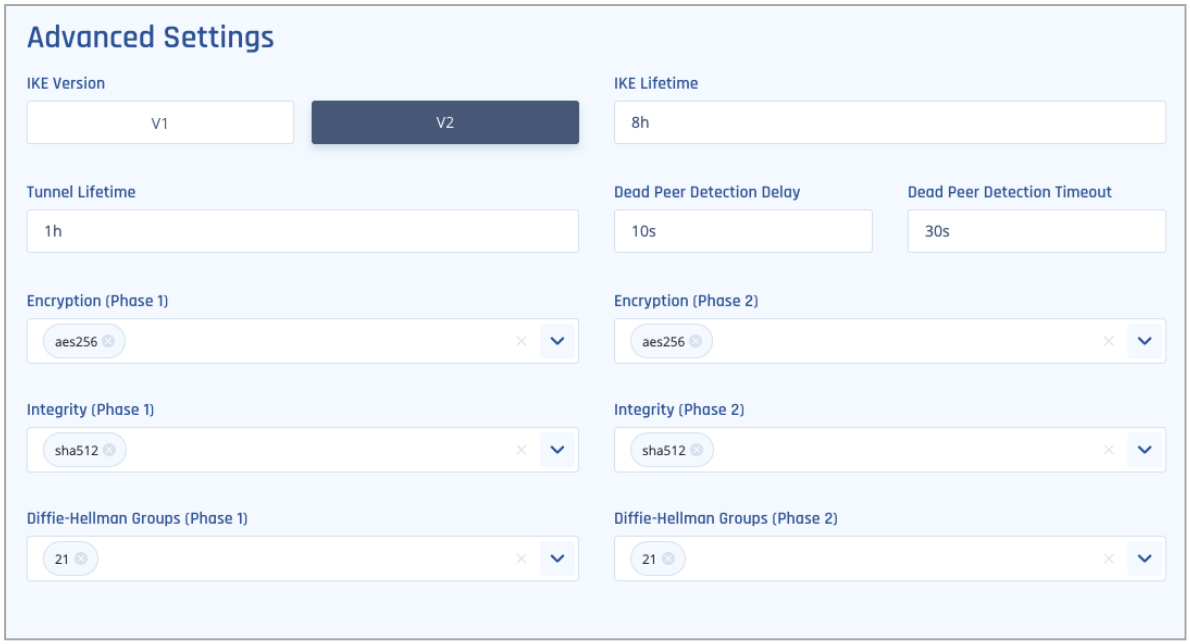
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

Make sure to verify the tunnel settings under section 3 in the configuration.



10. Click **Add Tunnel**.

AWS Transit Gateway

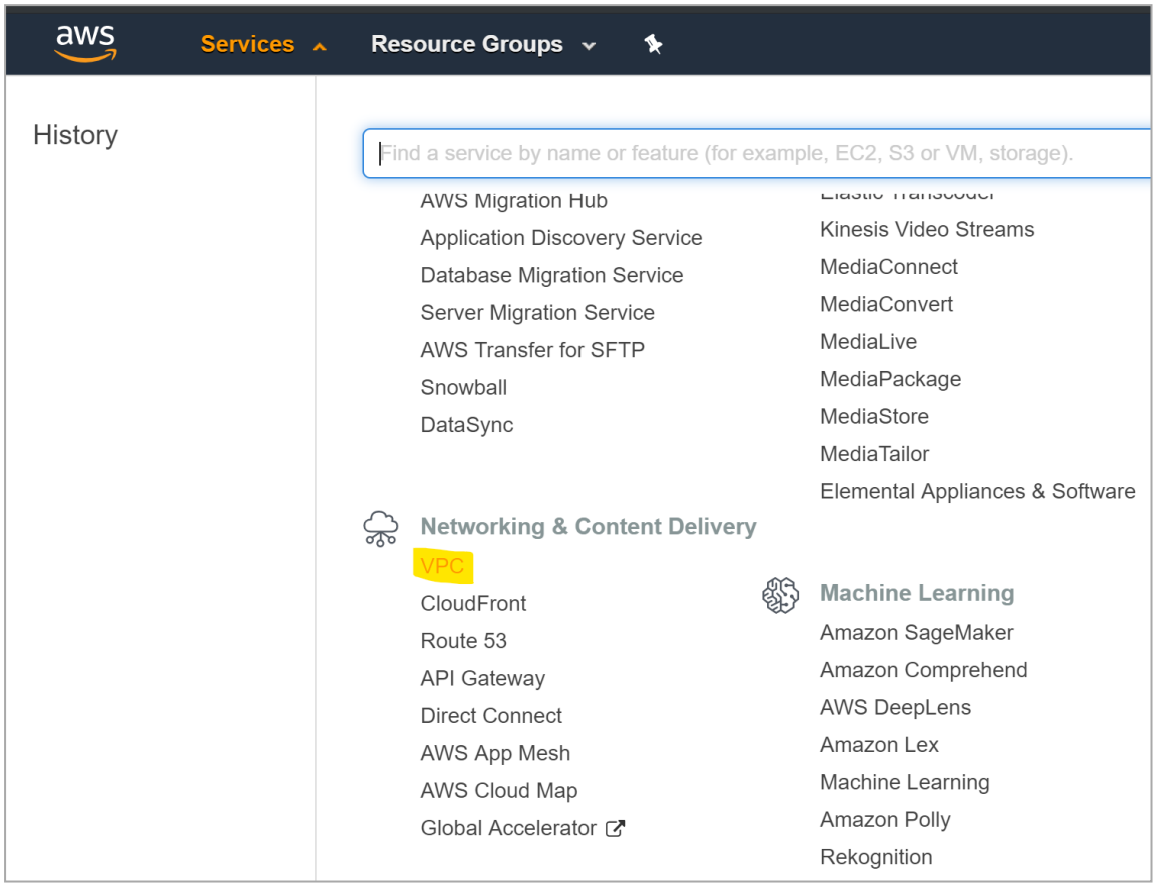
Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

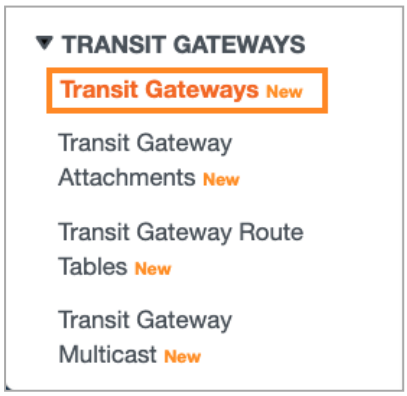
Step 1 - Configurations in the AWS Management Console

Creating the Transit Gateway and Transit Gateway Attachments

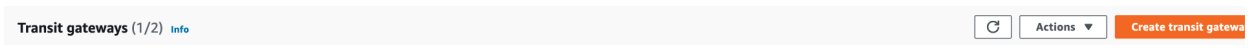
1. Access the AWS Management console and go to the **VPC** section.



2. On the left pane, click **Transit Gateways**.



3. On the top pane, click **Create transit gateway**.



The **Create transit gateway attachment** page appears.

4. In the **Name tag** field, enter a name of the Transit Gateway.

   Keep the default values for rest of the fields.

5. Click **Create transit gateway**.

Creating the Transit Gateway Attachments

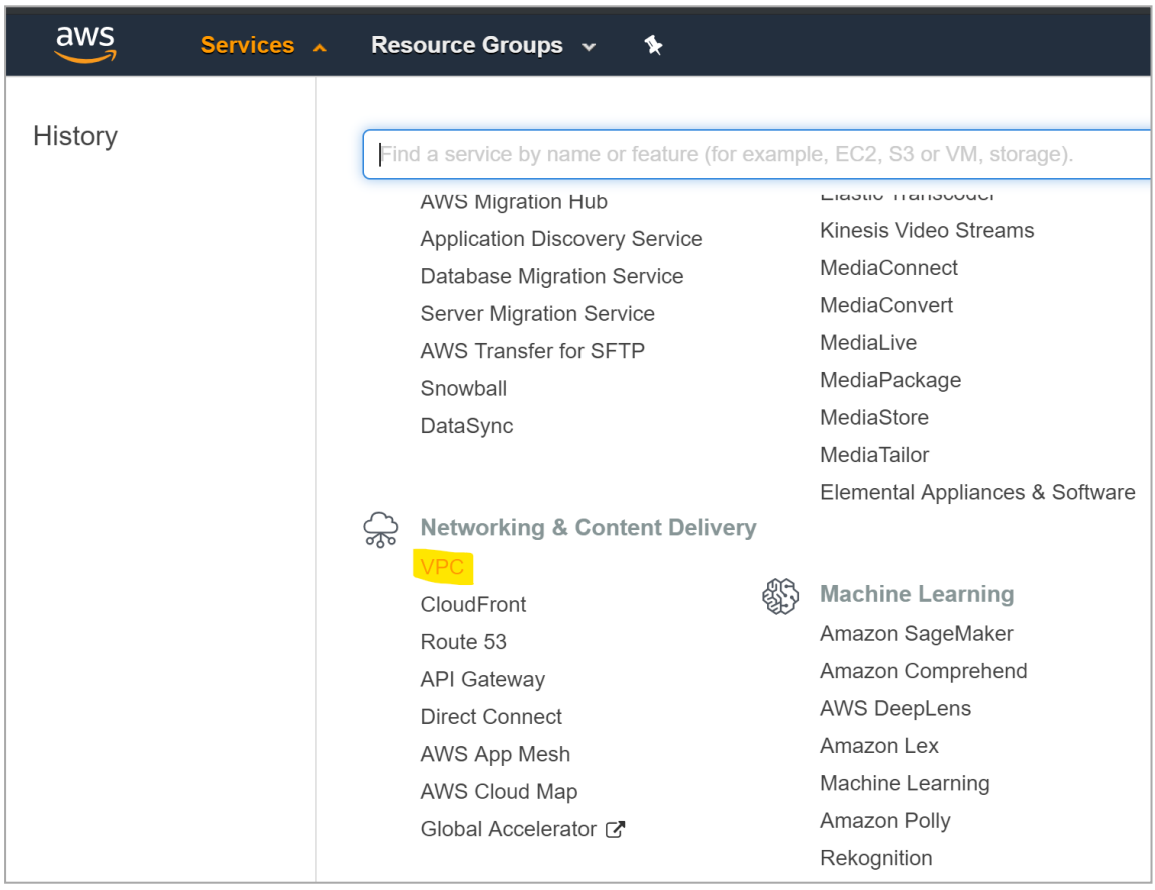
You can create an attachment for VPCs, other VPNs, and other Peered Transit Gateways located on another AWS region. All connected attachments can communicate with each other as defined in the Transit Gateway's routes.

A single VPC attachment connects one VPC to the Transit Gateway. You may connect multiple VPC attachments to a single Transit Gateway.

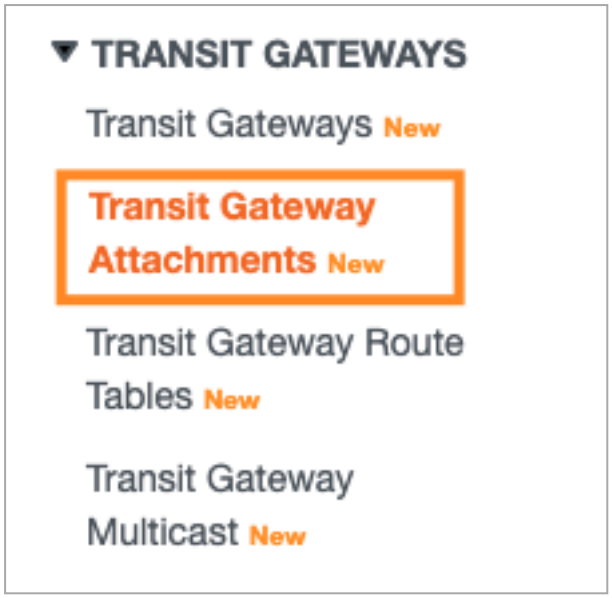
Creating the Transit Gateway VPC Attachments

Note - If you already have a Transit Gateway Attachment to your VPC, skip this procedure and go to *"Creating the Transit Gateway VPN Attachment" on page 581*.

1. Access the AWS Management console and go to the **VPC** section.

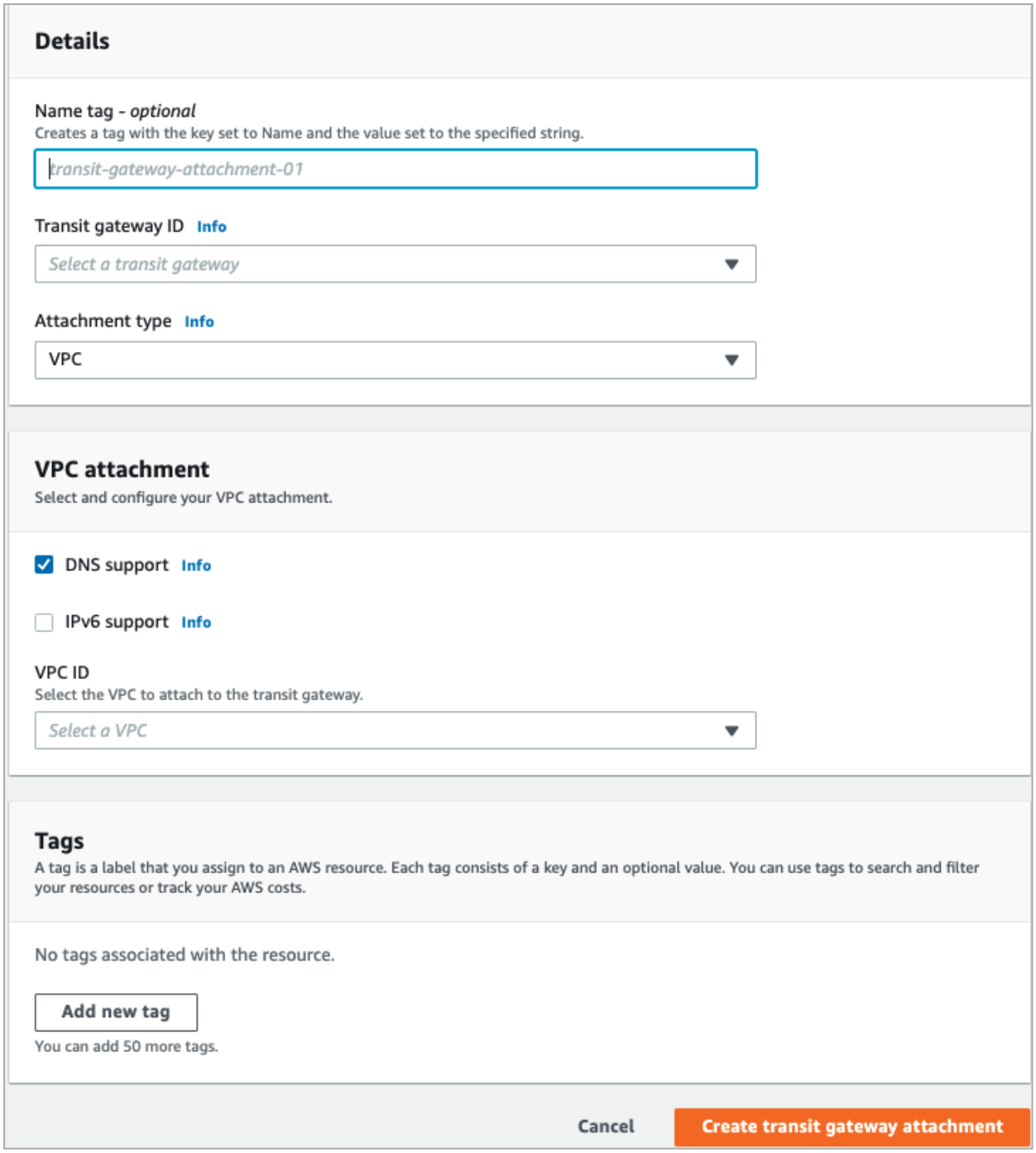


2. On the left pane, click **Transit Gateway Attachments**.



3. On the top pane, click **Create transit gateway attachment**.

The **Create transit gateway attachment** page appears.



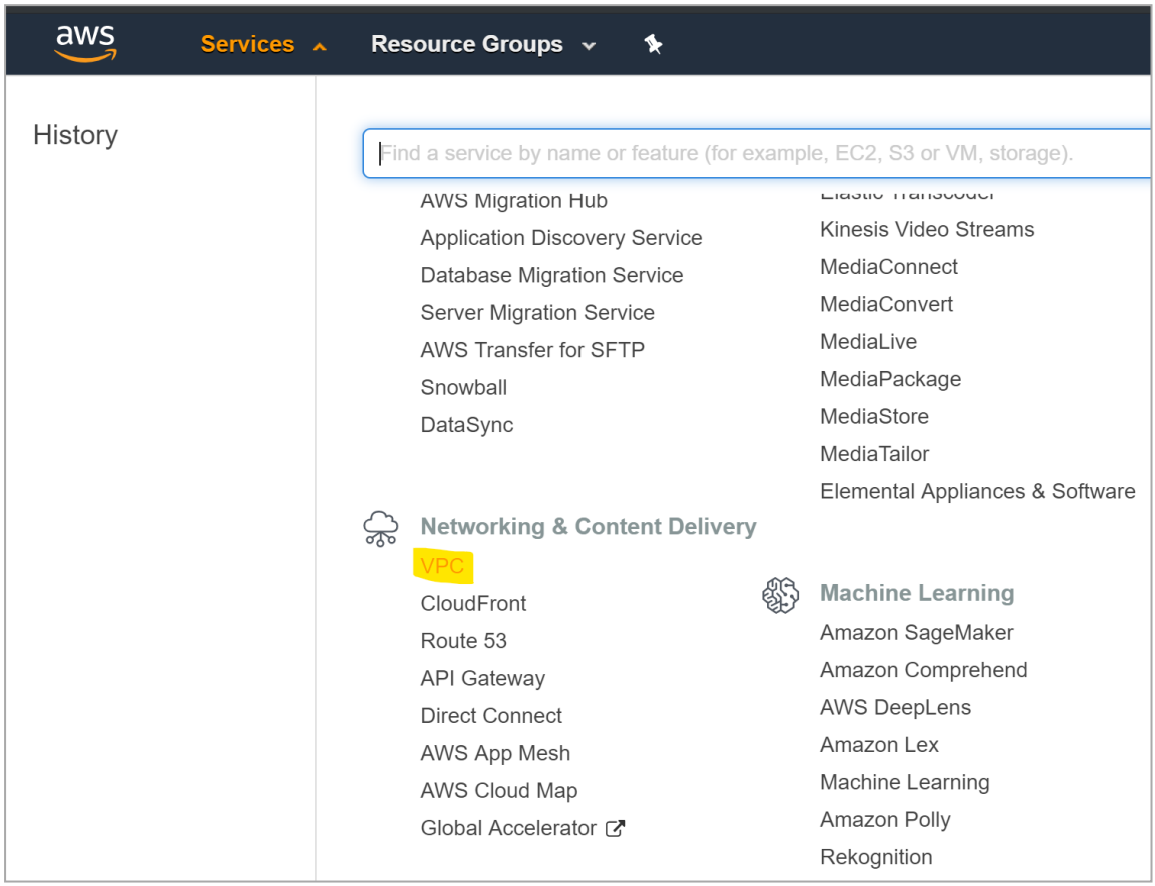
4. Enter these:
   a. **Name Tag** - Name of the Transit Gateway Attachment.
   b. **Transit gateway ID** - Select the newly created Transit gateway.
   c. **Attachment Type** - VPC
   d. **VPC ID** - Select the relevant VPC.

      Keep the default values for rest of the fields.
5. Click **Create transit gateway attachment**.

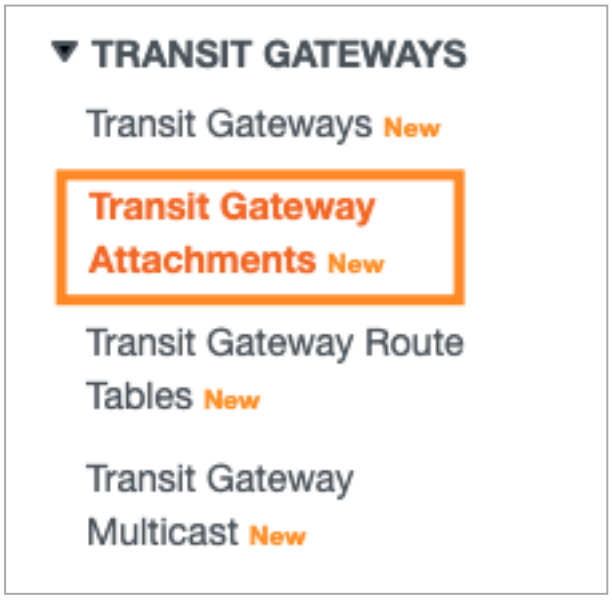
Note - Repeat the above procedure for each of the VPCs that you want to access to.

Creating the Transit Gateway VPN Attachment

1. Access the AWS Management console and go to the **VPC** section.

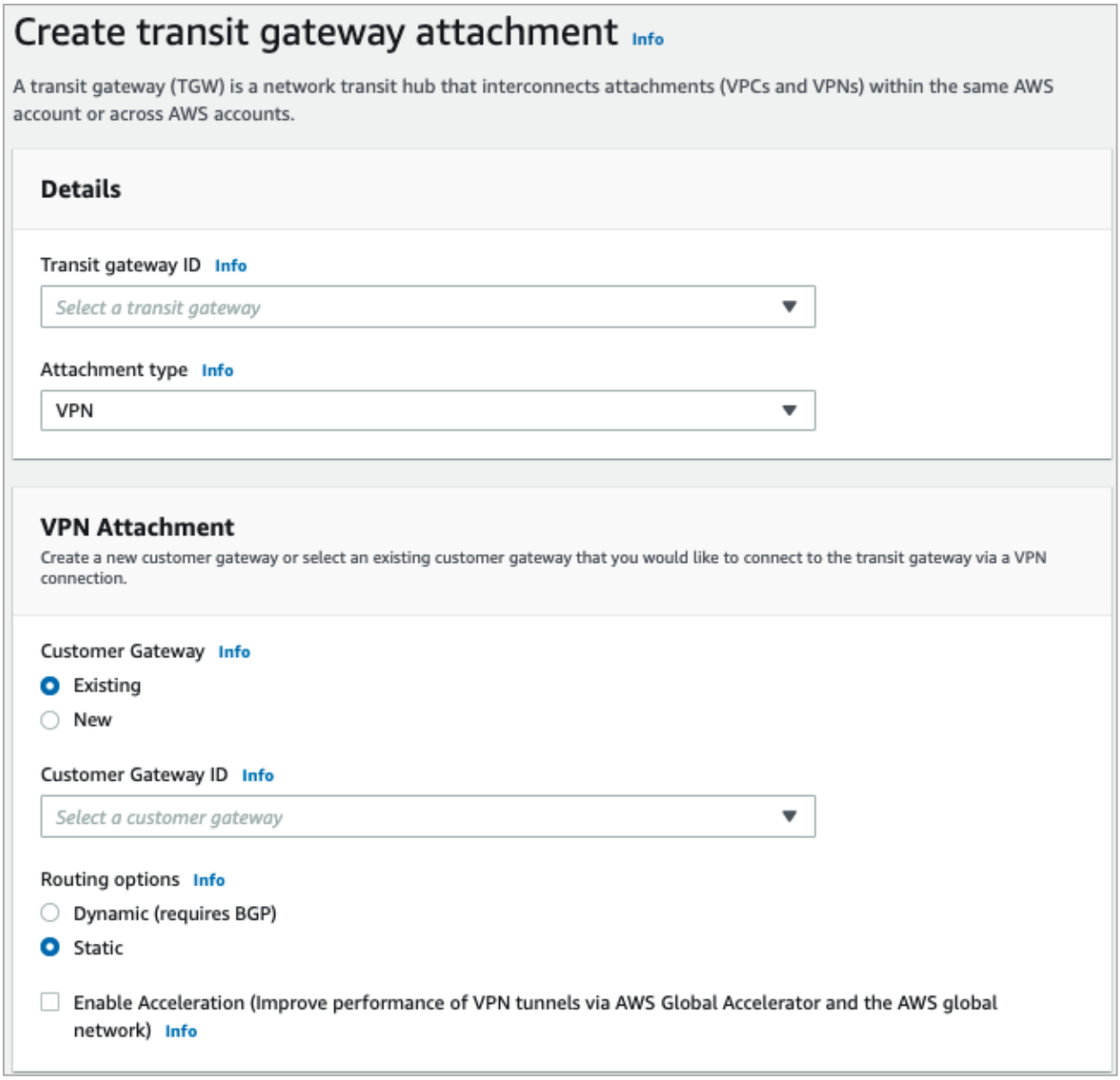


2. On the left pane, click **Transit Gateway Attachments**.



3. On the top pane, click **Create transit gateway attachment**.

The **Create transit gateway attachment** page appears.



4. Enter these:
   a. **Transit gateway ID** - Select the newly created Transit gateway.
   b. **Attachment Type** - VPN
   c. **Customer Gateway** - New

d. **IP address** - IP address of the relevant Gateway in the Check Point SASE Administrator Portal.

e. **BGP ASN** - Keep the default value.

f. **Routing Options** - Static

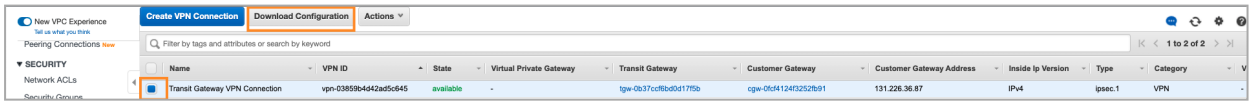
Keep the default values for rest of the fields.

5. Click **Create transit gateway attachment**.

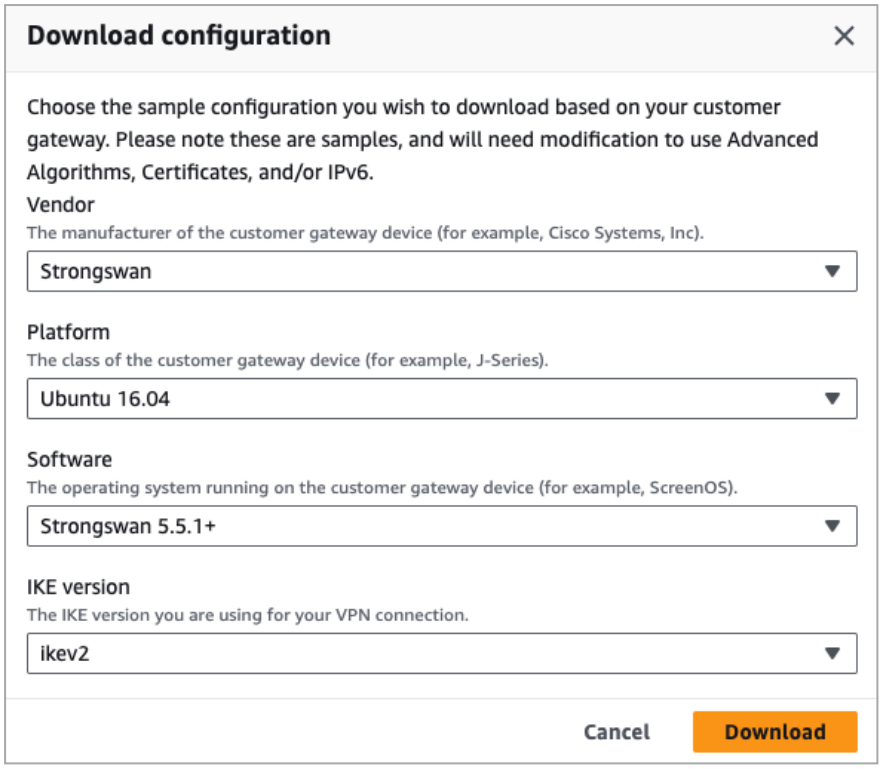
Configuring the Tunnel

1. Access the AWS Management console and on the left pane, in the **Virtual Private Network (VPN)** section, click **Site-to-Site VPN Connections**.

2. Select the newly created Transit Gateway VPN connection record.
3. On the top pane, click **Download Configuration**.



The **Download configuration** window appears.



4. Enter these:
    a. **Vendor** - Strongswan
    b. **Platform** - Ubuntu version
    c. **Software** - Strongswan version
    d. **Ike version** - Ikev2
5. Click **Download**.

Configuring the Routing

1. Access the AWS Management console and go to the **VPC** section.
2. In the **Transit Gateways** section, select **Transit Gateway Route Tables**.

3. Select the relevant Transit Gateway Route Table.
4. If your routes do not propagate automatically:

a. At the bottom, click **Propagations**.

b. Verify that all of the Transit Gateway Attachments are included.

> **Note** - If any of the Transit Gateway Attachments is missing a route, click **Create propagation** and add the missing route.

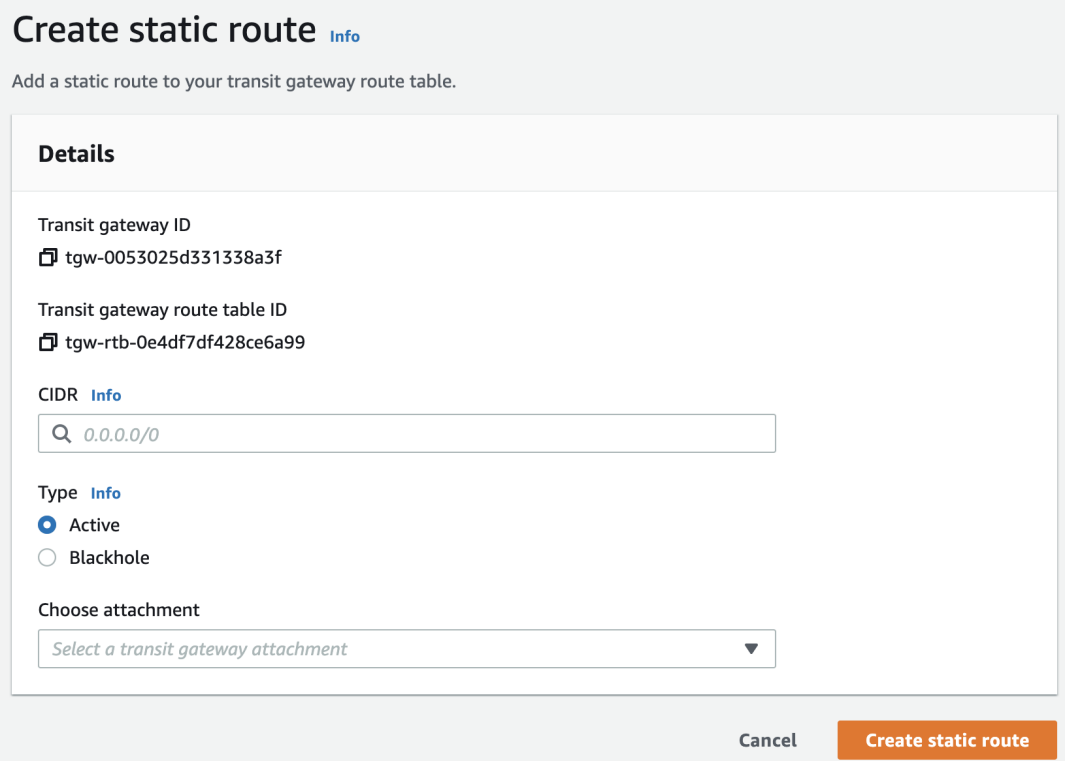
c. At the bottom, click **Associations**.

d. Verify that all of the Transit Gateway Attachments are included (same as the previous step).

> **Note** - If any of the Transit Gateway Attachments is missing a route, click **Create propagation** and add the missing route.

e. At the bottom, click **Routes**.

The **Create static route** window appears.



f. In the **CIDR** field, enter your Check Point SASE subnet. To find your Check Point SASE network subnet:

i. Go to the Check Point SASE Administrator Portal > **Networks** page.

ii. In your network, click ··· next to your network.

iii. Click **Edit Network**.

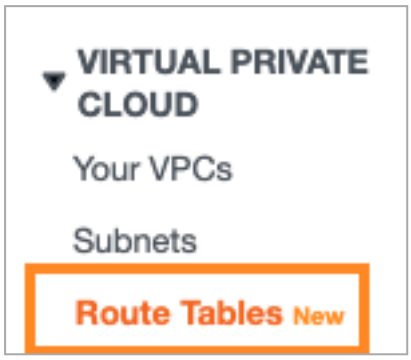
iv. Copy the **Subnet** value.

g. Select **Type** as **Active**.

h. From the **Choose attachment** list, select the VPN attachment.

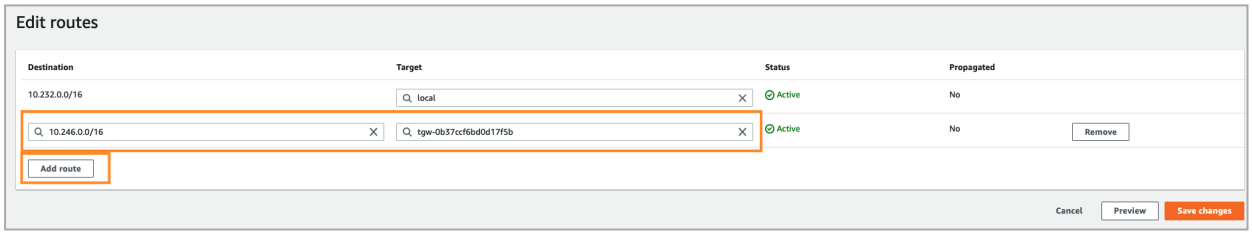
i. Click **Create static route**.

5. In the left pane, in the **Virtual Private Cloud** section, click **Route Tables**.



6. Select the Route Table for one of the attached VPCs.
7. At the bottom, click **Routes**.
8. Click **Edit Routes**.

   The **Edit routes** window appears.



9. Click **Add route**.
10. Enter these:

    a. **Destination** - Your Check Point SASE subnet. To find your Check Point SASE network subnet, see step 4f above.

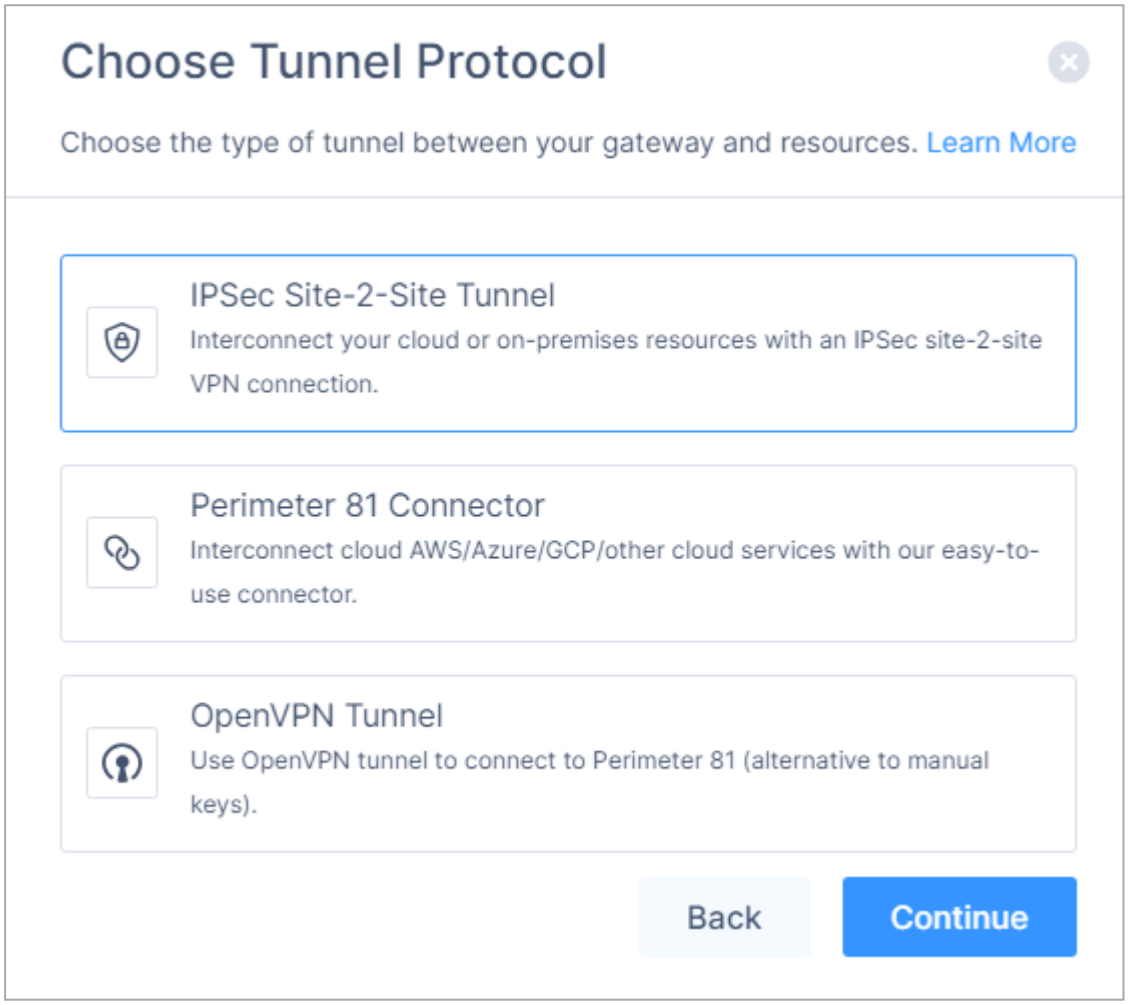
    b. **Target** - Select Transit Gateway and pick the relevant Transit Gateway.

11. Click **Save changes**.

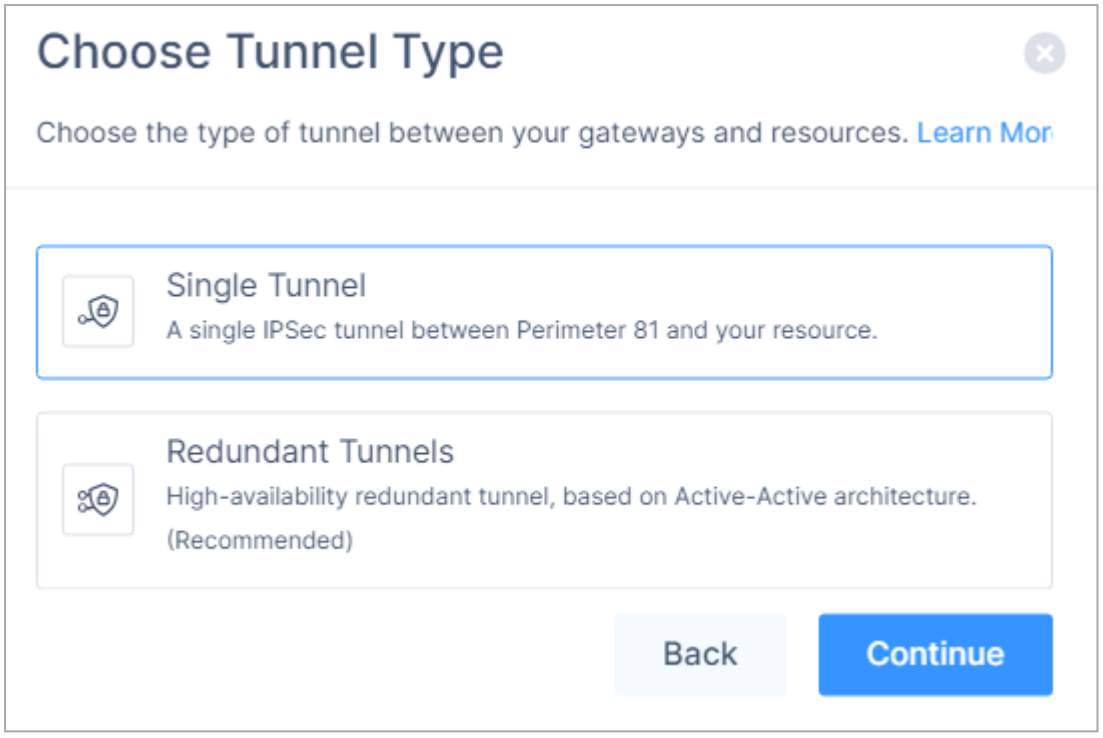
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

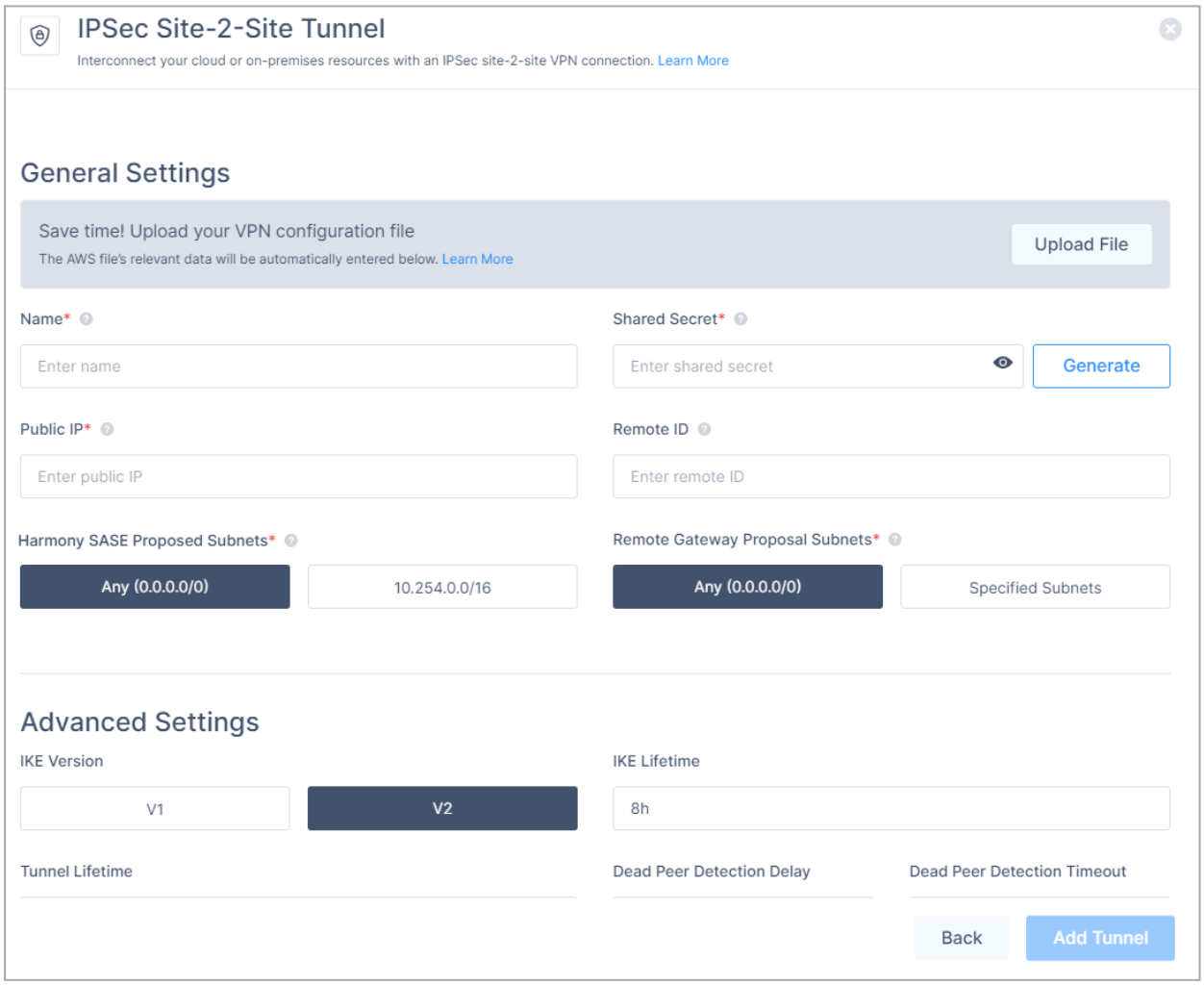
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



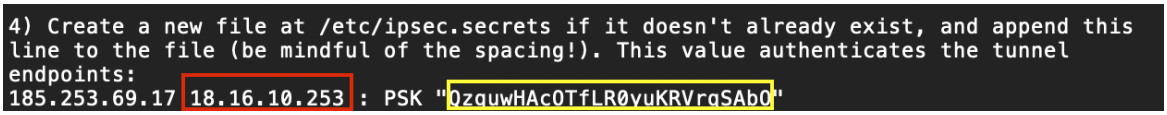
5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the AWS Management console.
7. For manual configuration, open the configuration file you downloaded and copy and paste these attributes.
   a. **Shared Secret** - Paste the value marked in yellow. Omit the quotation marks.
   b. **Public IP & Remote ID** - Paste the IP address marked in red. This is your AWS external IP address.



   c. **Perimeter 81 Gateway Proposal Subnets** - 0.0.0.0/0.
   d. **Remote Gateway Proposal Subnets** - 0.0.0.0/0.
8. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

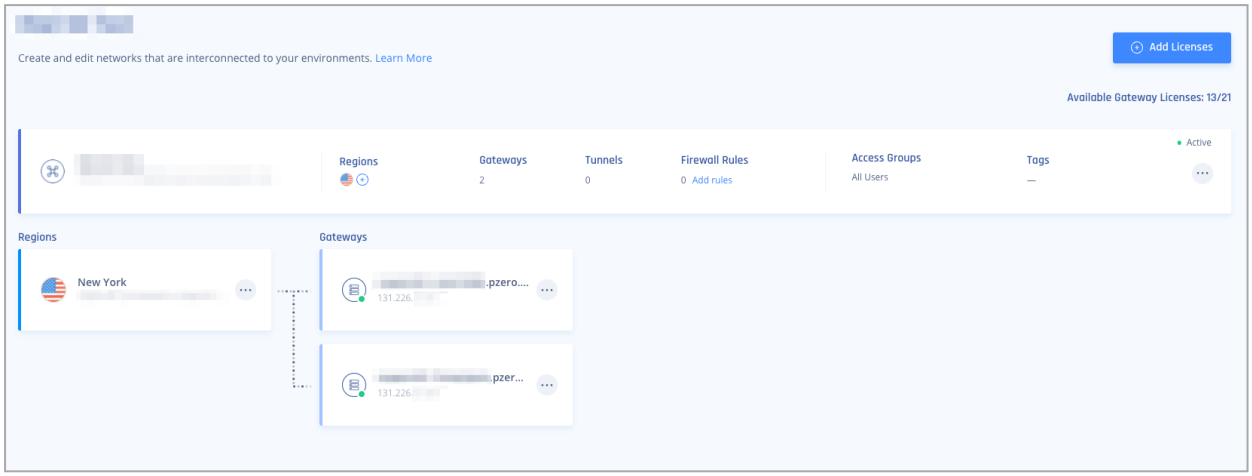
9. Click **Add Tunnel**.

AWS Redundant Tunnels - Virtual Private Gateway

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Check Point SASE network must have at least two different gateways in the same network.



Notes -

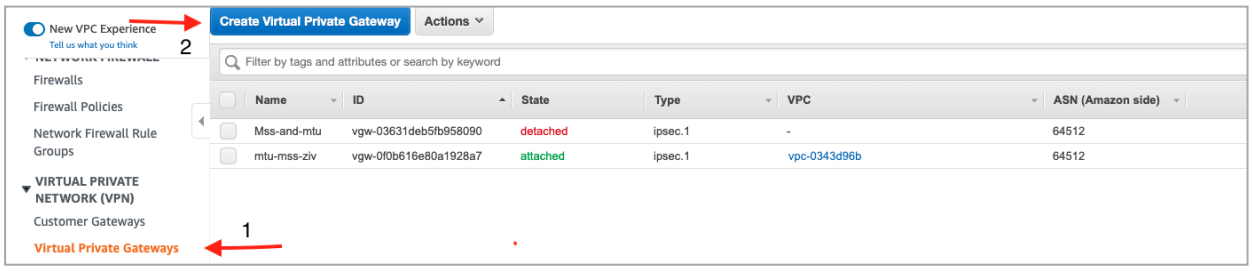
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the AWS Management Console

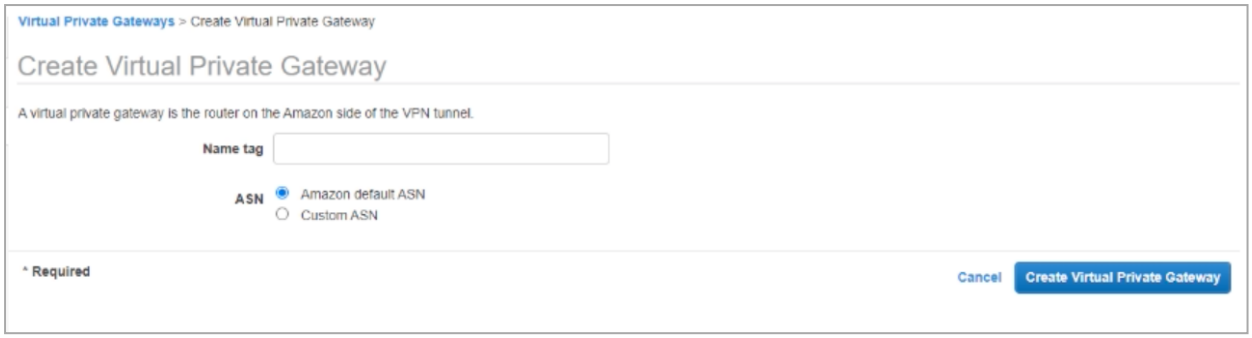
Creating a Virtual Private Gateway

Note - If you already have a Virtual Private Gateway in your AWS region, skip this procedure.

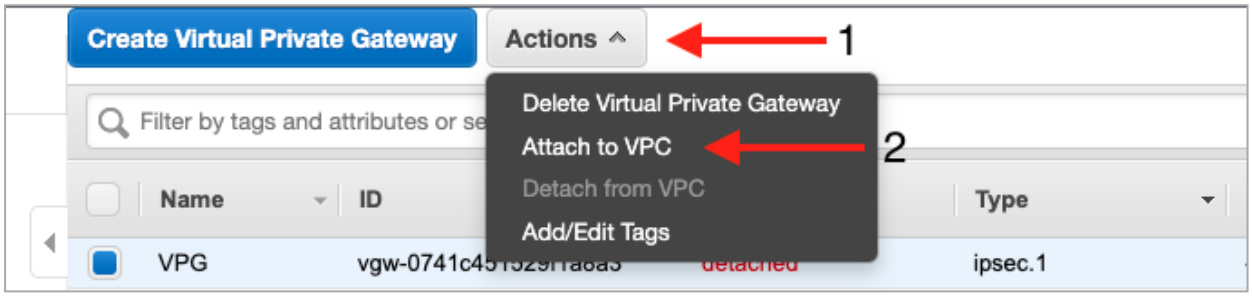
1. Access the AWS Management Console and go to the **VIRTUAL PRIVATE NETWORK (VPN)** section.
2. Click **Virtual Private Gateways** > **Create Virtual Private Gateway**.



3. Create the Virtual Private Gateway with the default settings.



4. Select the newly created Virtual Private Gateway and on the top, click **Actions** > **Attach to VPC**.



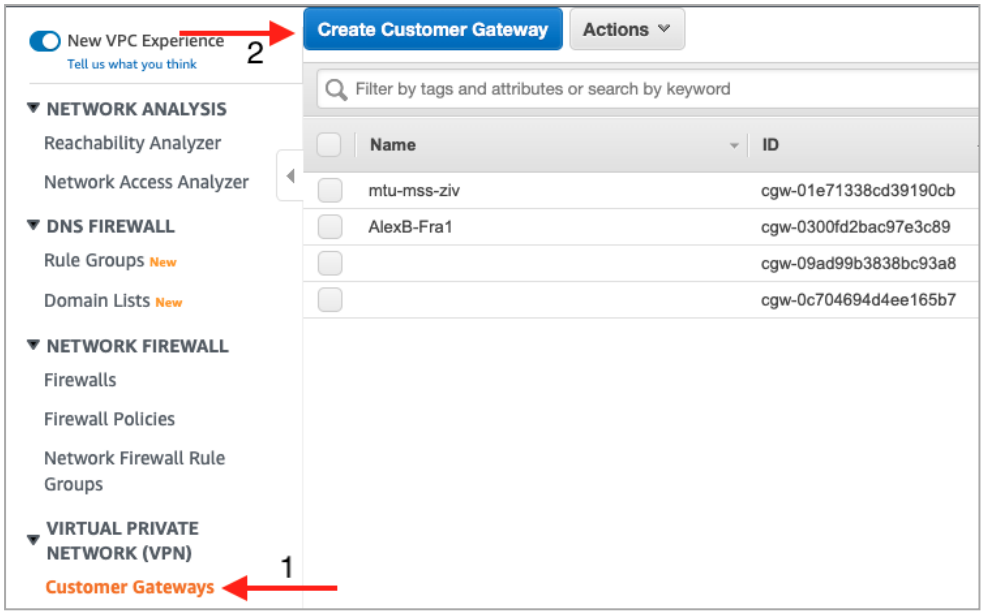
The **Attach to VPC** window appears.

5. From the **VPC** drop-down list, select the relevant VPC.

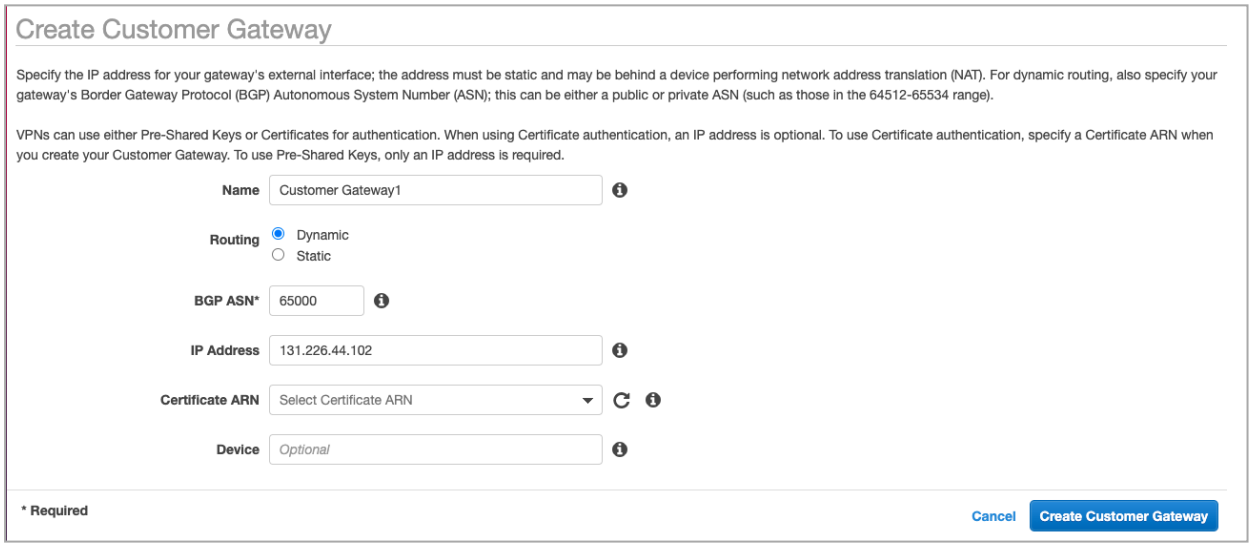
6. Click **Yes, Attach**.

Creating Two Customer Gateways

1. Access the AWS Management Console and go to the **VIRTUAL PRIVATE NETWORK (VPN)** section.
2. Click **Customer Gateway** > **Create Customer Gateway**.



The **Create Customer Gateway** window appears.



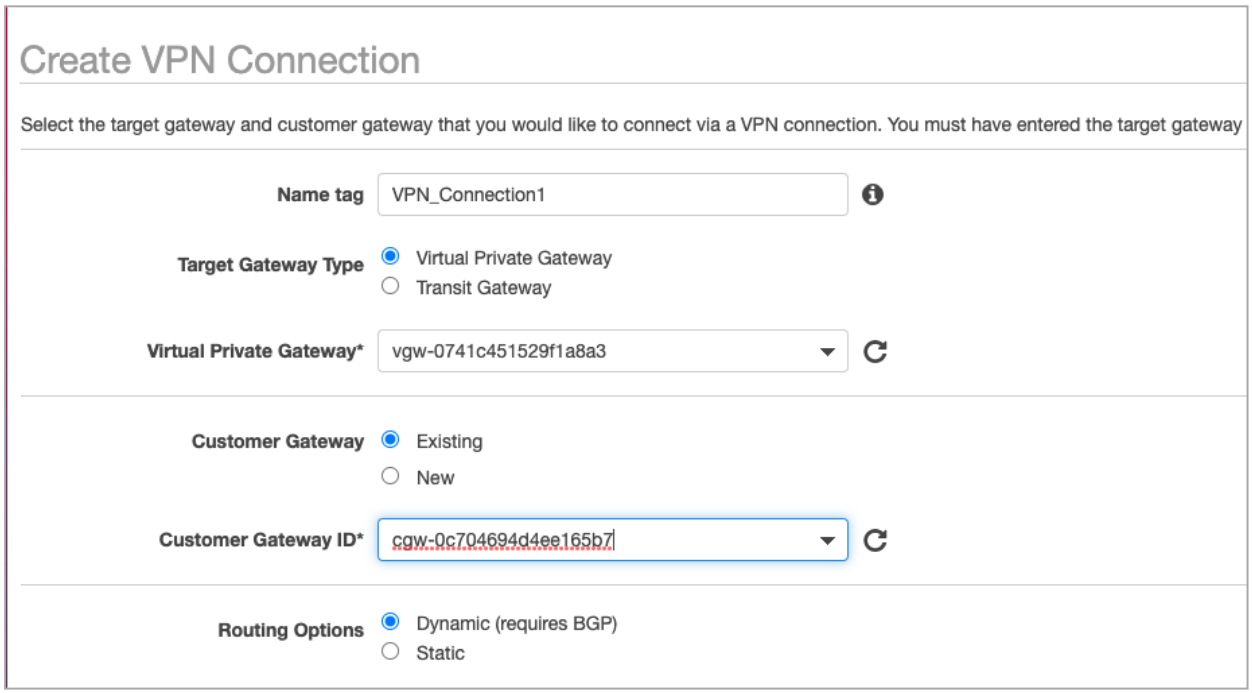
3. Enter these:
   a. **Name** - Name of the gateway.
   b. **Routing** - Dynamic.
   c. **IP Address** - IP address of the first Check Point SASE gateway.
   d. **BGP ASN** - ASN for the Check Point SASE gateway. Keep it as 64512.
4. Click **Create Customer Gateway**.
5. To create the second customer gateway, repeat steps 1- 4.

   In the **IP Address** field, enter the IP address of the second Check Point SASE gateway.

Creating Two Site-to-Site VPN Connections

1. Access the AWS Management Console.
2. In your AWS VPC, in the **VIRTUAL PRIVATE NETWORK(VPN)** section, click **Site-to-Site VPN Connections** > **Create VPN Connection**.

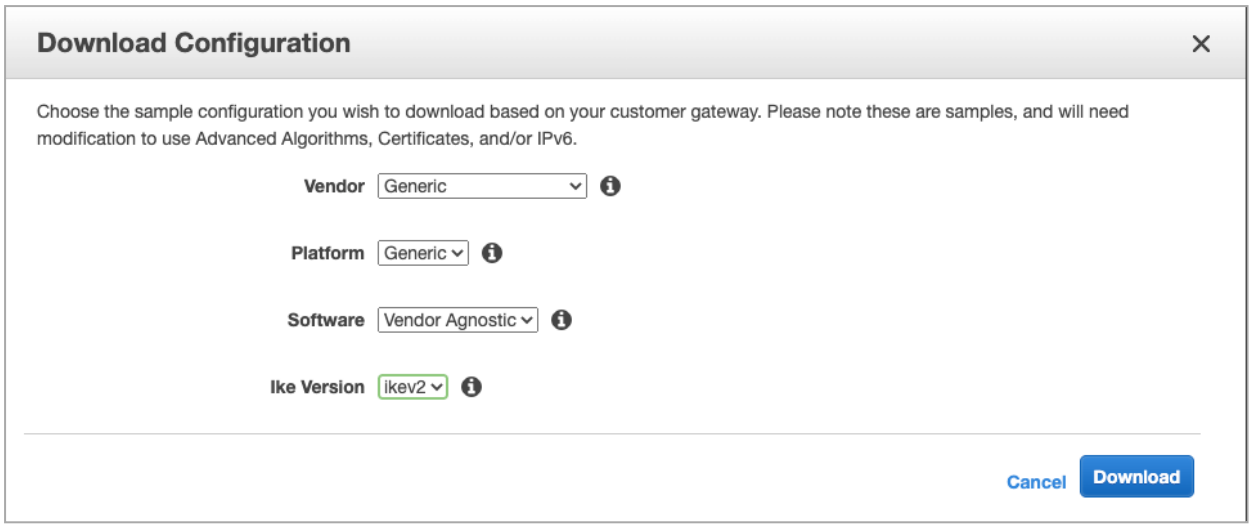
The **Create VPN Connection** window appears.



3. Enter these:
   a. **Target Gateway Type** - Virtual Private Gateway.
   b. **Virtual Private Gateway** - Select the first Virtual Private Gateway created.
   c. **Customer Gateway** - Existing.
   d. **Customer Gateway ID** - Select the first Customer Gateway created.
   e. **Routing Options** - Dynamic (requires BGP).

   Keep the other options to default.
4. Click **Download Configuration**.

The **Download configuration** window appears.

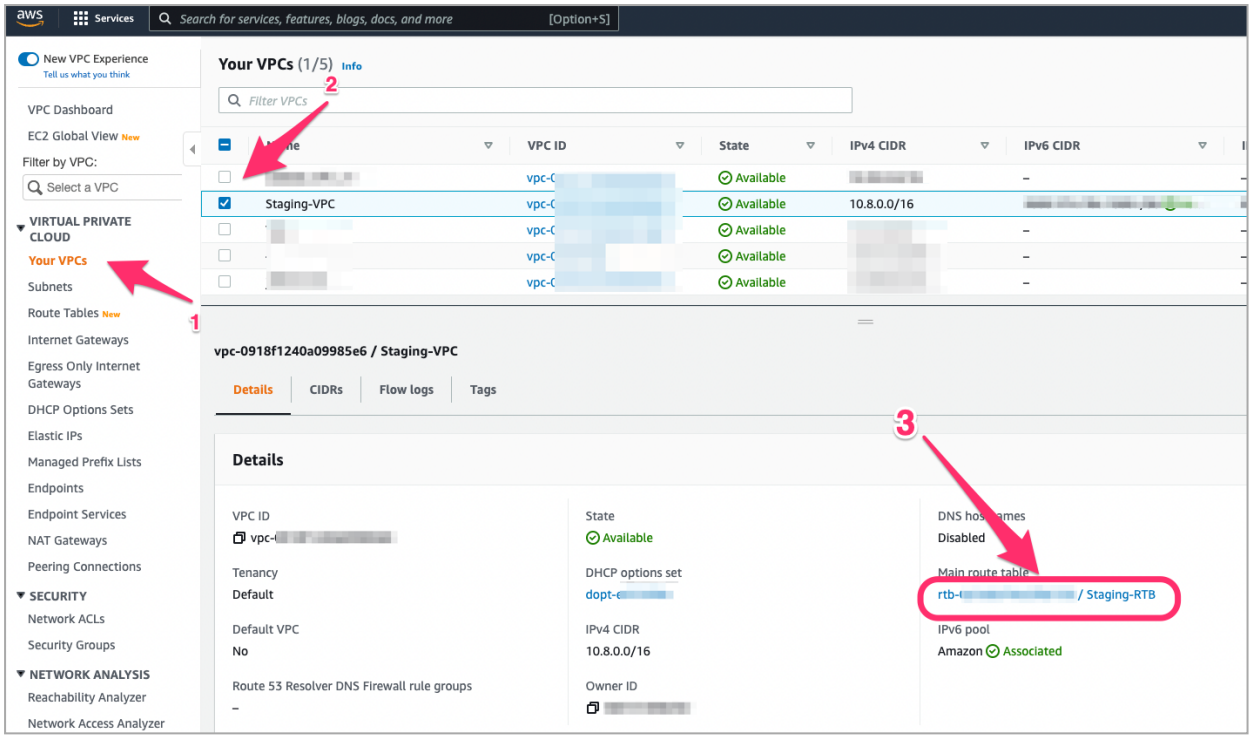


5. Enter these:
   a. **Vendor** - Generic
   b. **Platform** - Generic
   c. **Software** - Vendor Agnostic
   d. **Ike version** - Ikev2
6. Click **Download**.

   The system downloads the file. Rename the file as *Tunnel1.txt*.
7. Repeat steps 1-6 for the second Customer Gateway.
8. Rename the second downloaded file as *Tunnel2.txt*.

Creating Static Routes

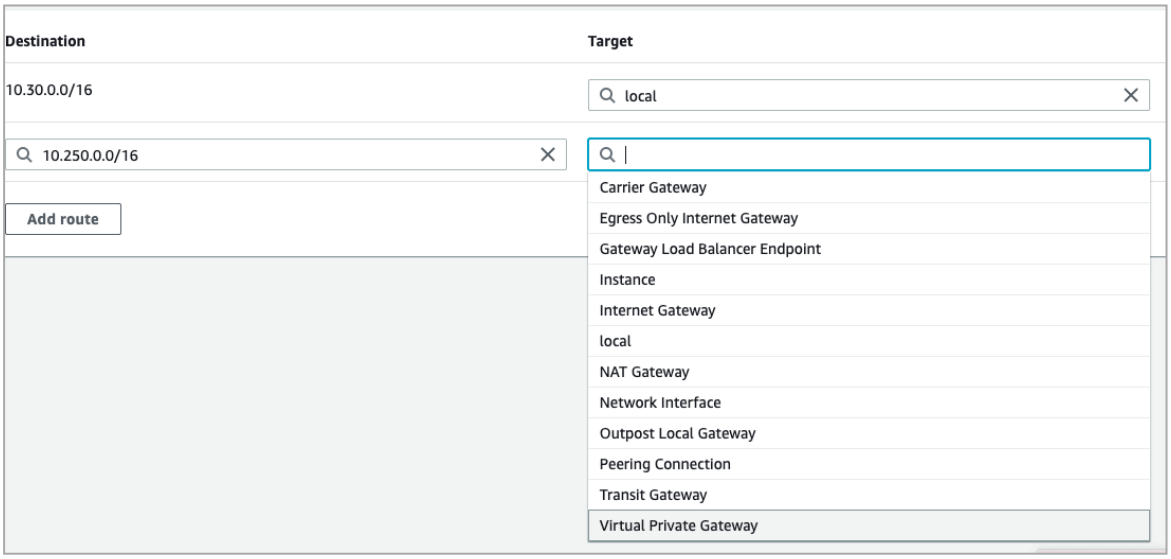
1. Access the AWS Management Console and Go to **VPC**.
2. Select the corresponding VPC attached to the Virtual Private Gateway and then select the **Main Route Table** for the VPC.



3. Edit the main Route Table for the VPC:

   a. In the **Destination** column, add the subnet mask of your Check Point SASE network.

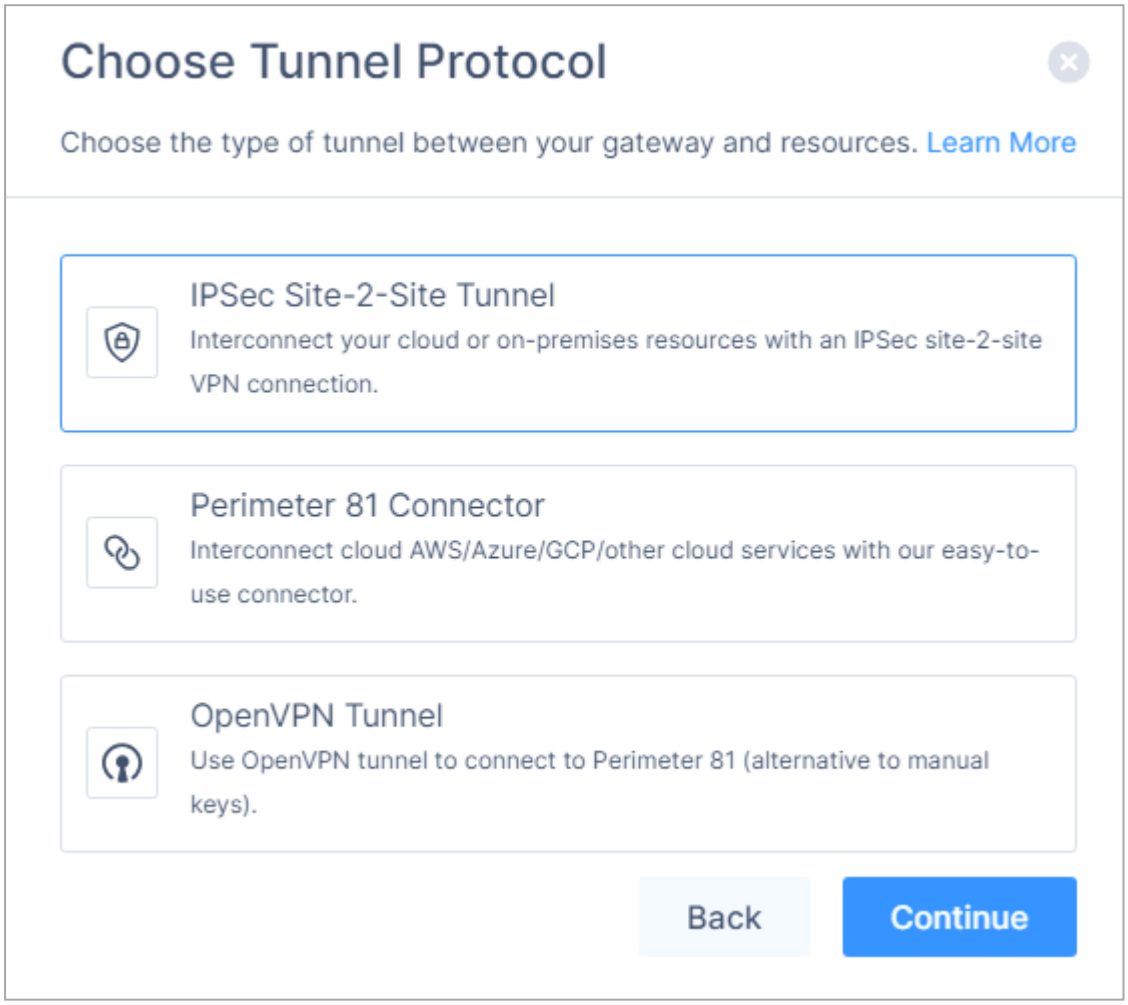
   b. In the **Target** column, select **Virtual Private Gateway** (Route for reverse traffic).



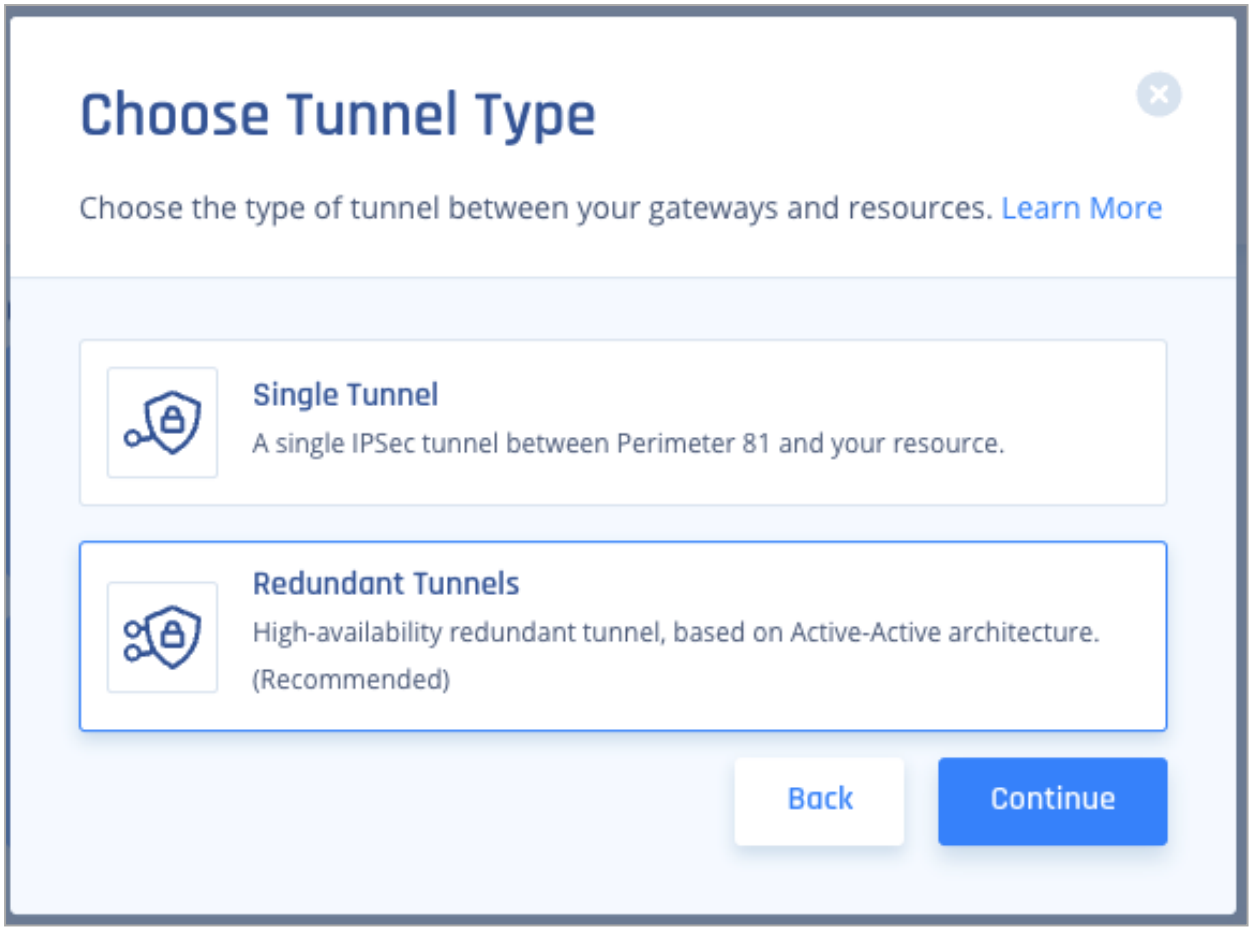
Note - If this is not the Main Route Table for the VPC, locate each subnet associated with the VPC and add the reverse route for the Check Point SASE internal subnet range.

Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal

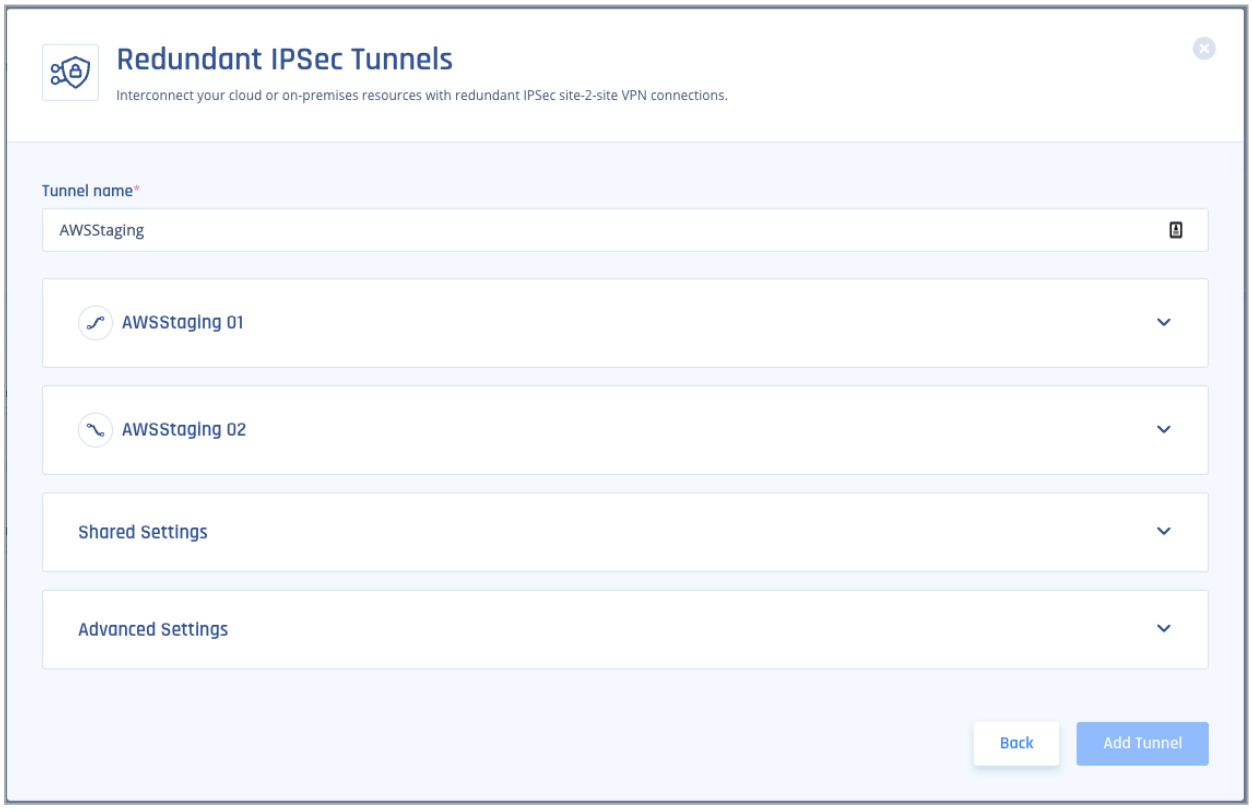
1. Access the Check Point SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.



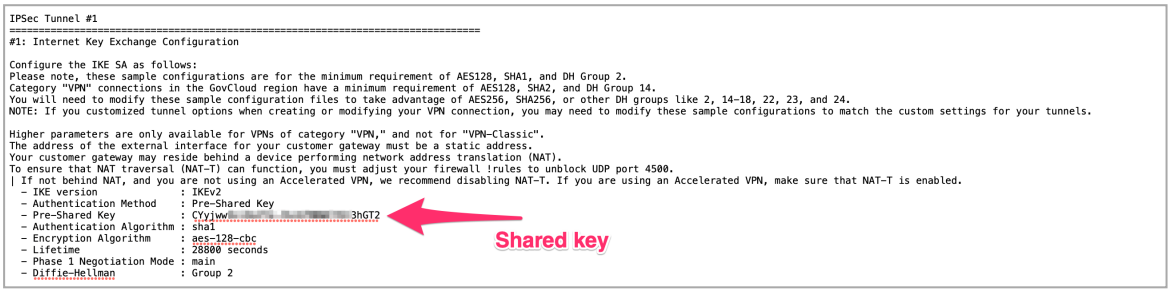
6. For the first tunnel:

   a. Expand the **Tunnel 01** drop-down.

   b. To automatically populate the tunnel configuration values, click **Upload File** and upload Tunnel_1.txt file.

   c. For manual configuration, copy the values from Tunnel_1.txt file as shown below.

   a. **Shared Secret** - Pre-Shared Key

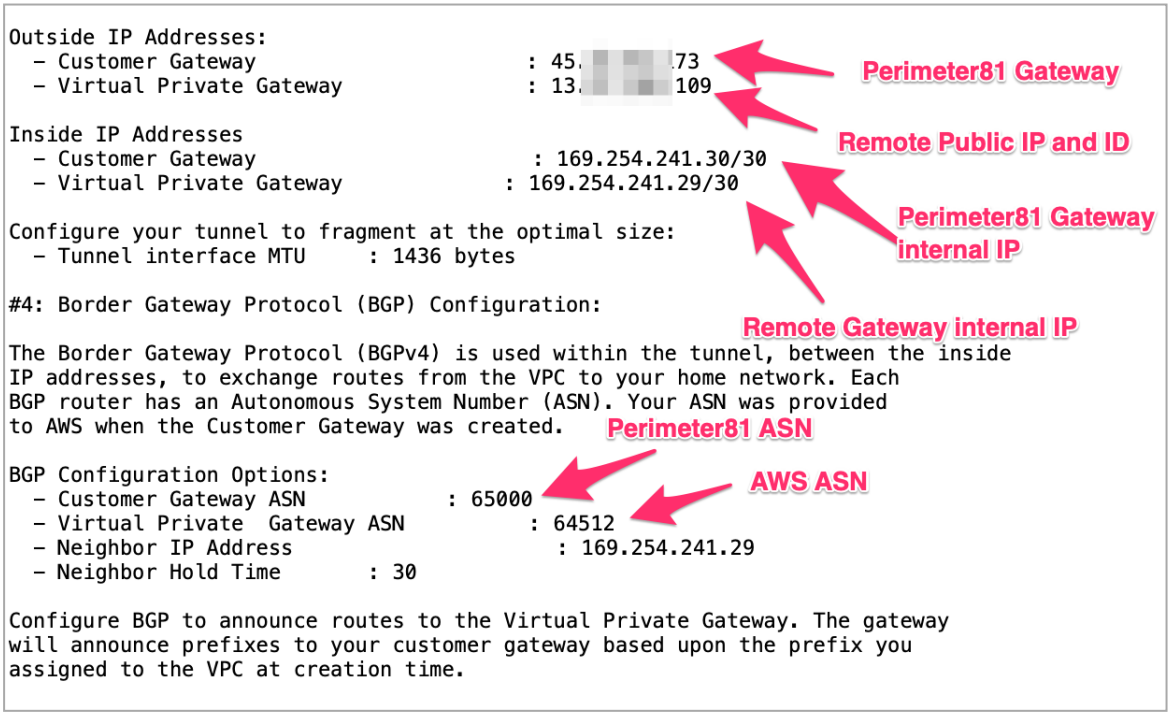


   b. **Check Point SASE gateway Internal IP** - Inside IP Addresses of Customer Gateway.

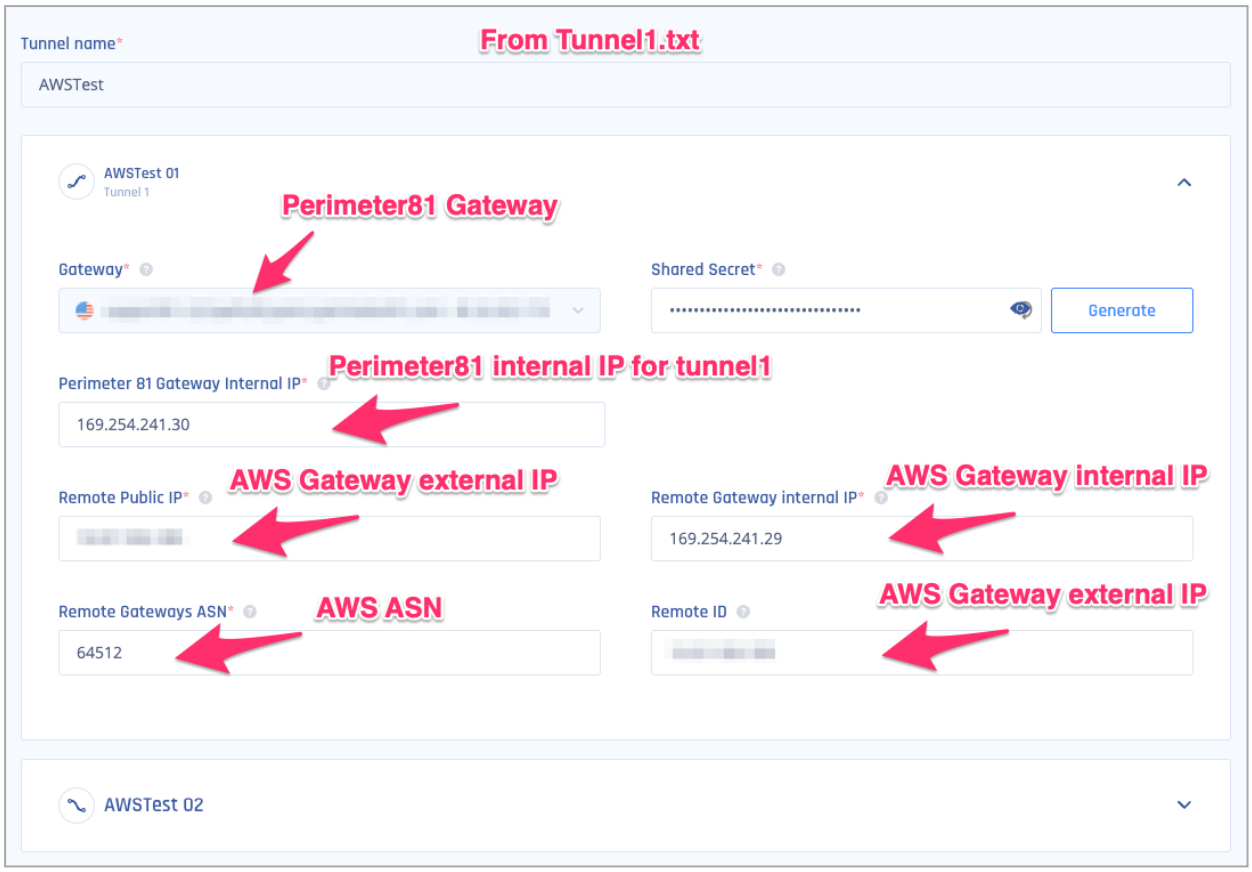
   c. **Remote Public IP & Remote ID** - Outside IP Addresses of Virtual Private Gateway.

   d. **Remote Gateway internal IP** - Inside IP Addresses of Virtual Private Gateway. The IP on the AWS side has a subnet (/30), discard it when pasting.

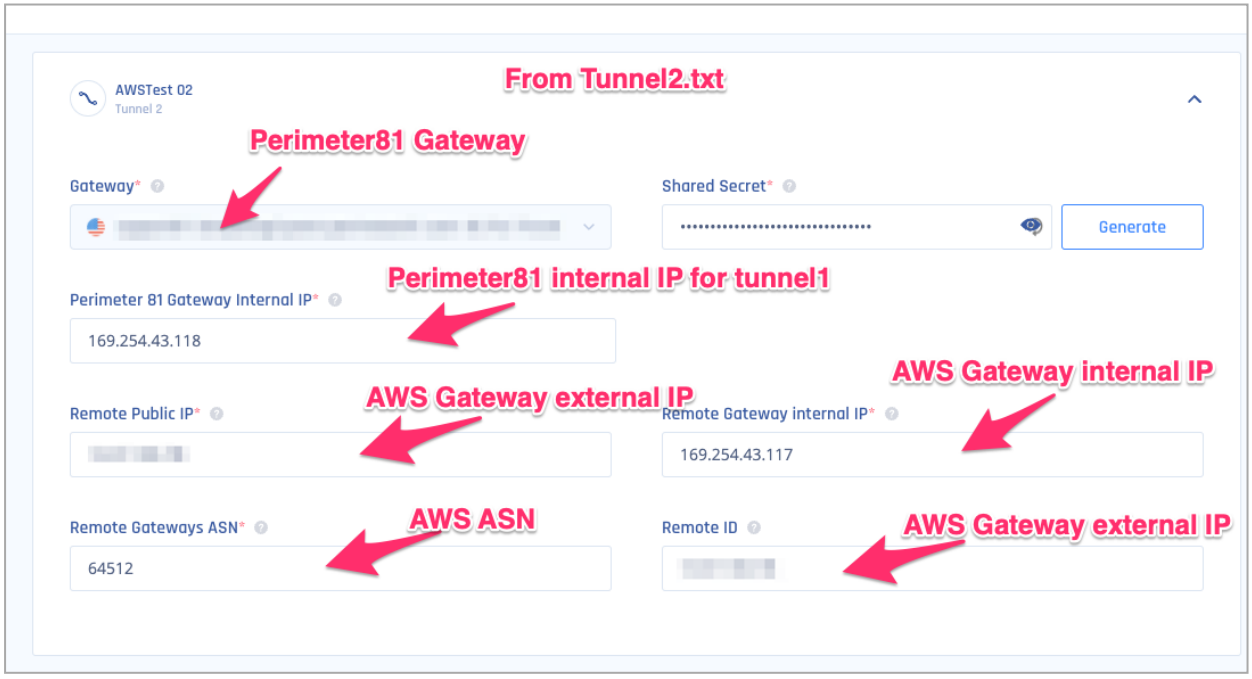
   e. **Remote Gateway ASN** - BGP Configuration Options of Virtual Private Gateway ASN from the file.



7. Enter the above copied values:



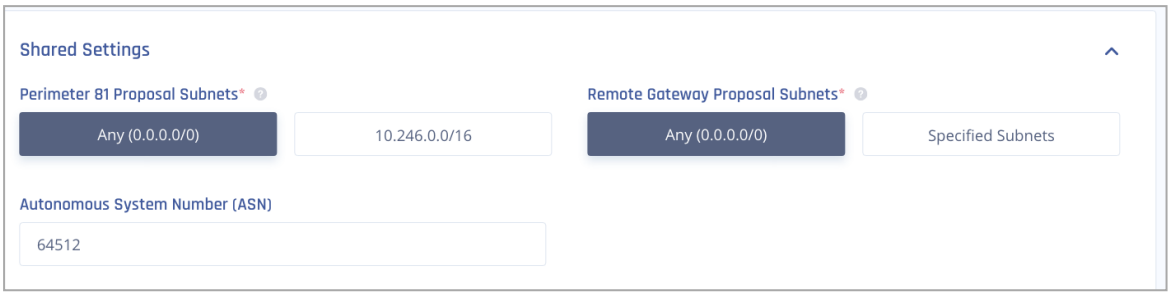
8. For the second tunnel, expand the **Tunnel 02** drop-down and repeat step 6 with the values from *Tunnel_2.txt* file.



9. In the **Shared Settings** section:

a. In the **Proposal Subnets** field, select **Any(0.0.0.0/0)** for both sides.

b. The **ASN** number should be the same as the Customer Gateway ASN you configured on the AWS Management console.



10. In the **Advanced Settings** section, enter the information for your tunnel type:

Field Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

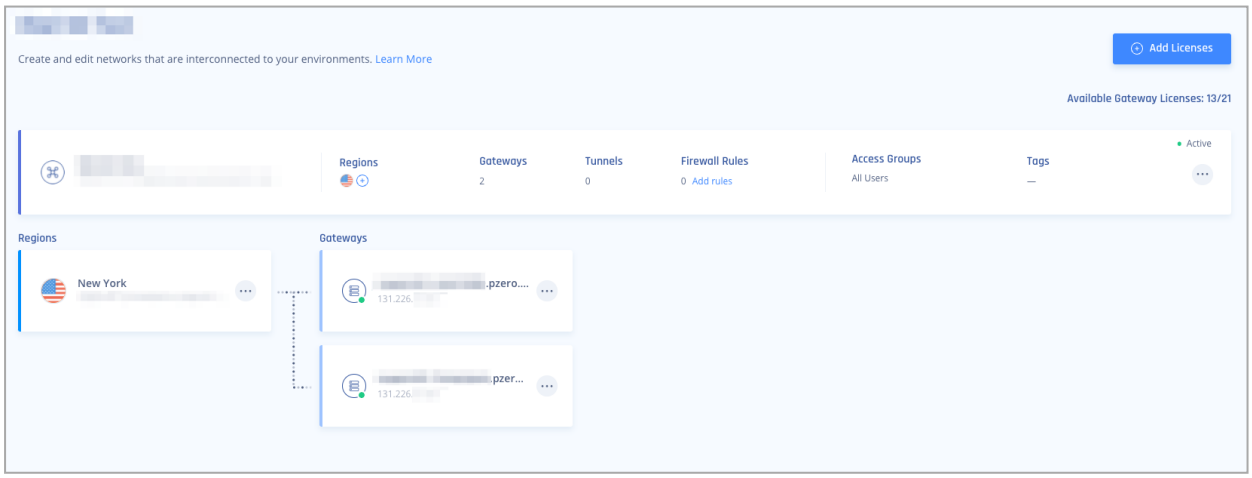
[1] Suggested values. For other supported ciphers, see this Google article.

11. Click **Add Tunnel**.

AWS Redundant Tunnels - Transit Gateway

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.
- Your Check Point SASE network must have at least two different gateways in the same network.



Notes -

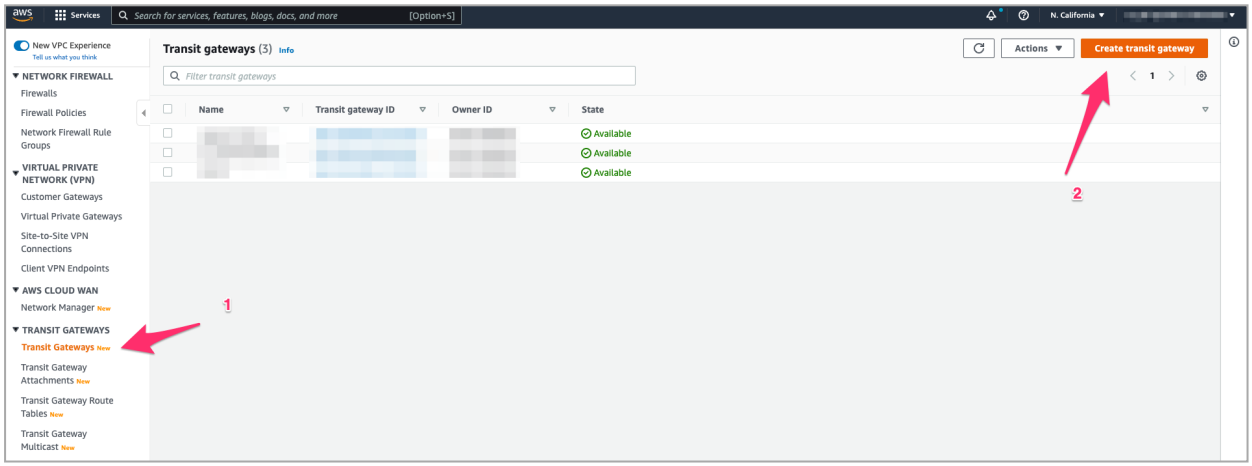
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the AWS Management Console

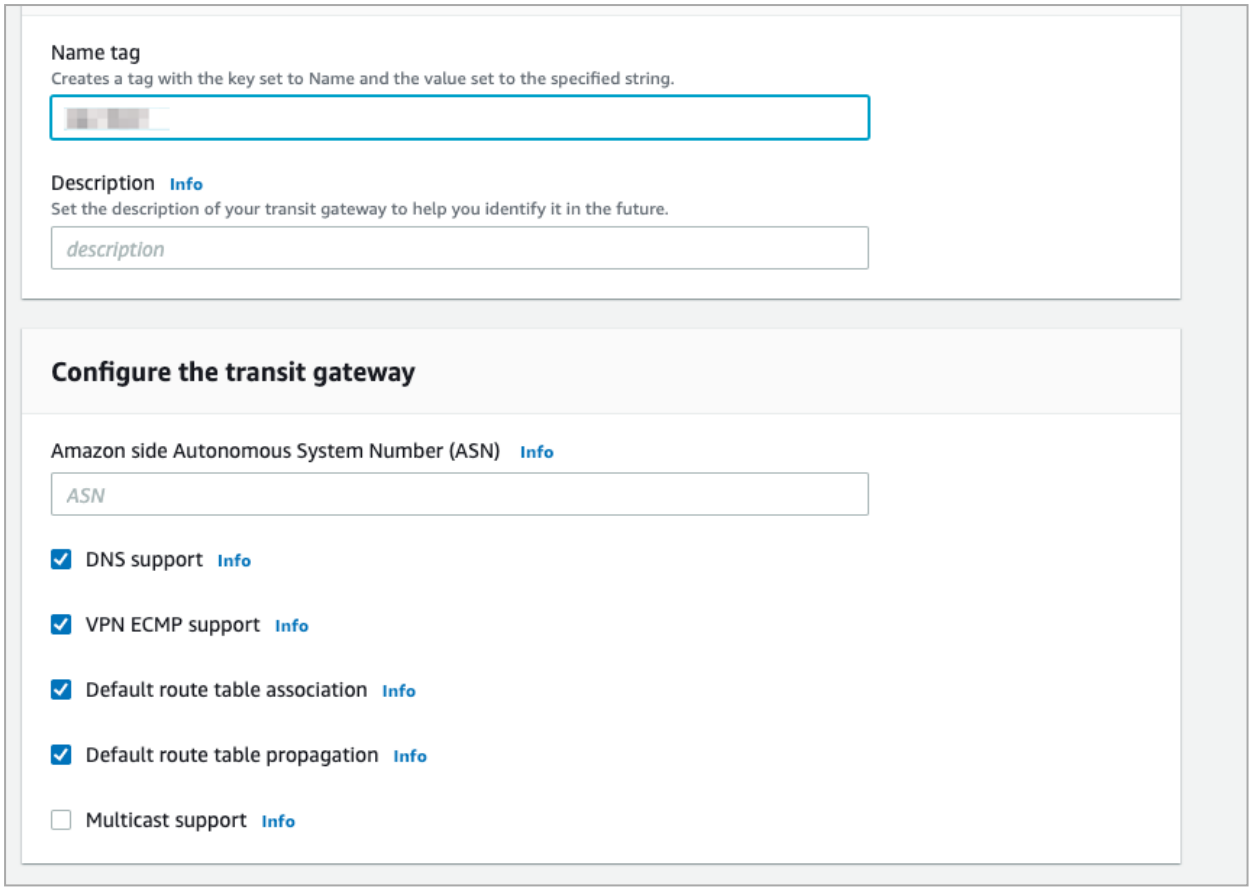
Creating a Transit Gateway

Note - If you already have a Transit Gateway in your AWS region, skip this procedure.

1. Access the AWS Management Console and go to the **TRANSIT GATEWAYS** section.
2. Click **Transit Gateway** > **Create transit Gateway**.



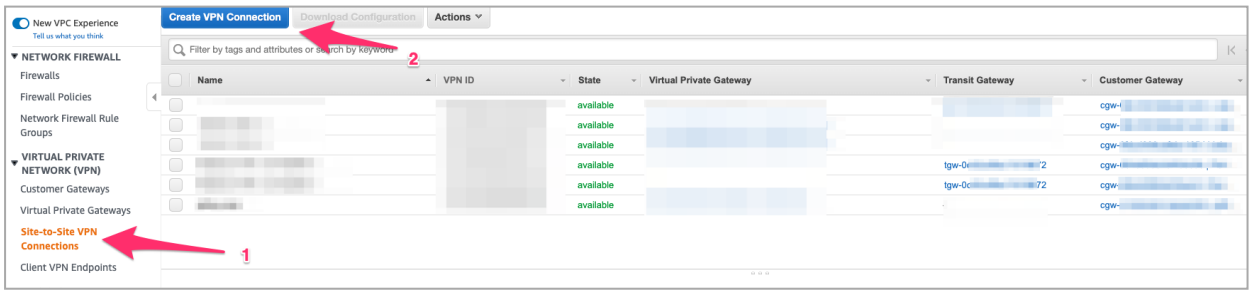
3. Create the Transit Gateway with the default settings.



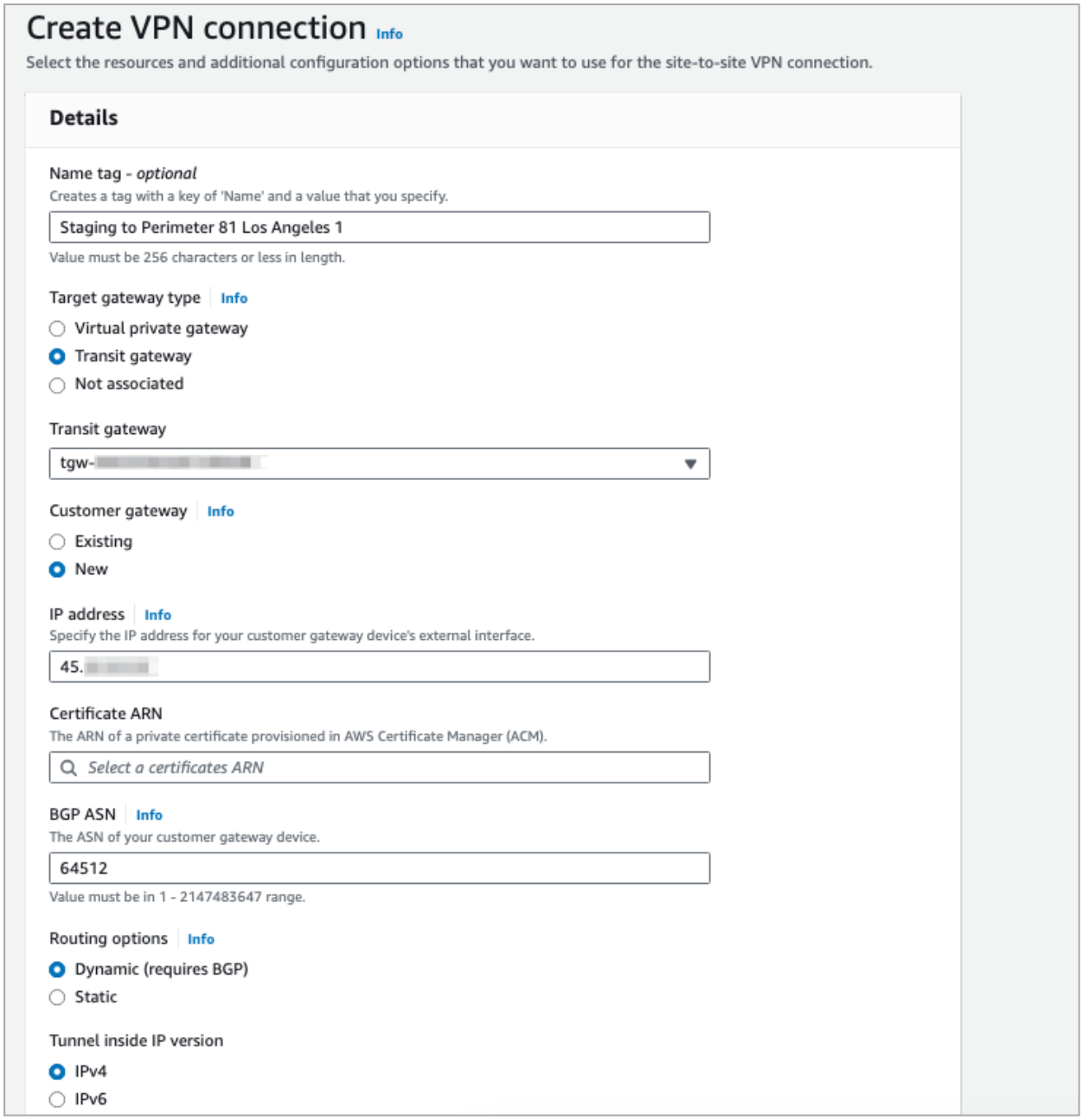
4. In the **VPC** section, go to **Transit Gateway Attachments** and create a Transit Gateway Attachment for your VPC.

Creating Two Site-to-Site VPN Connections

1. Access the AWS Management Console and go to your **AWS VPC** > **VIRTUAL PRIVATE NETWORK(VPN)** section.
2. Click **Site-to-Site VPN Connections** > **Create VPN Connection**.



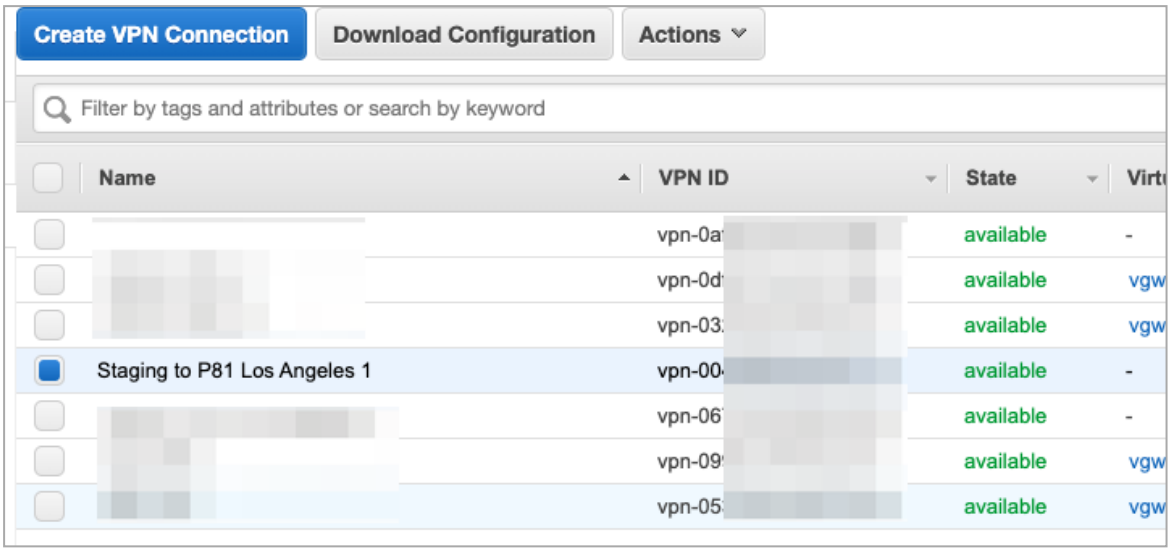
The **Create VPN connection** window appears.



3. Enter these:
    a. **Transit Gateway** - Transit gateway you created.
    b. **Customer gateway** - New.
    c. **IP address** - IP address of the first Check Point SASE gateway.
    d. **BGP ASN** - ASN you plan to use for the Check Point SASE network. The default is 64512.

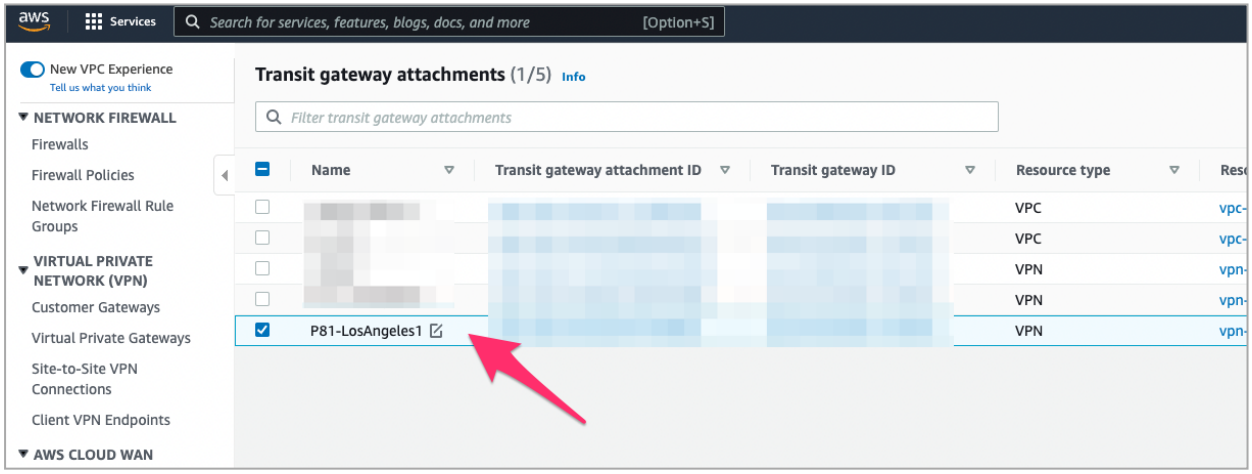
e. **Routing options** - Dynamic (requires BGP).

(Recommended) Use suitable naming conventions so that you can locate and distinguish between the connections later.

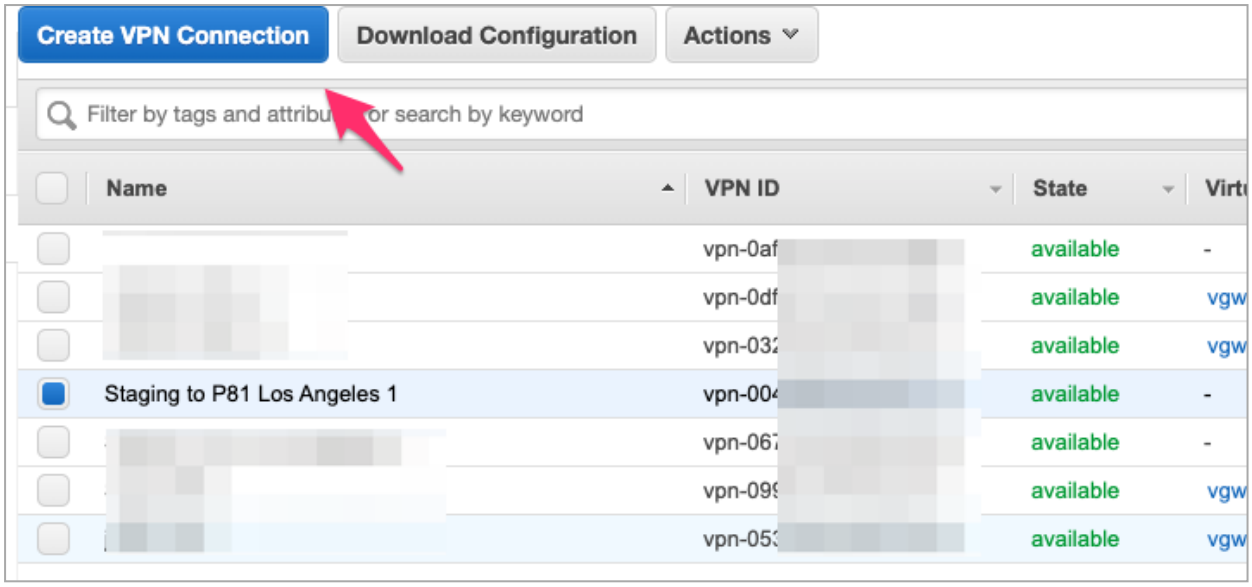


4. In the **TRANSIT GATEWAYS** section, go to **Transit Gateway attachments** and find the Transit Gateway Attachment you created.

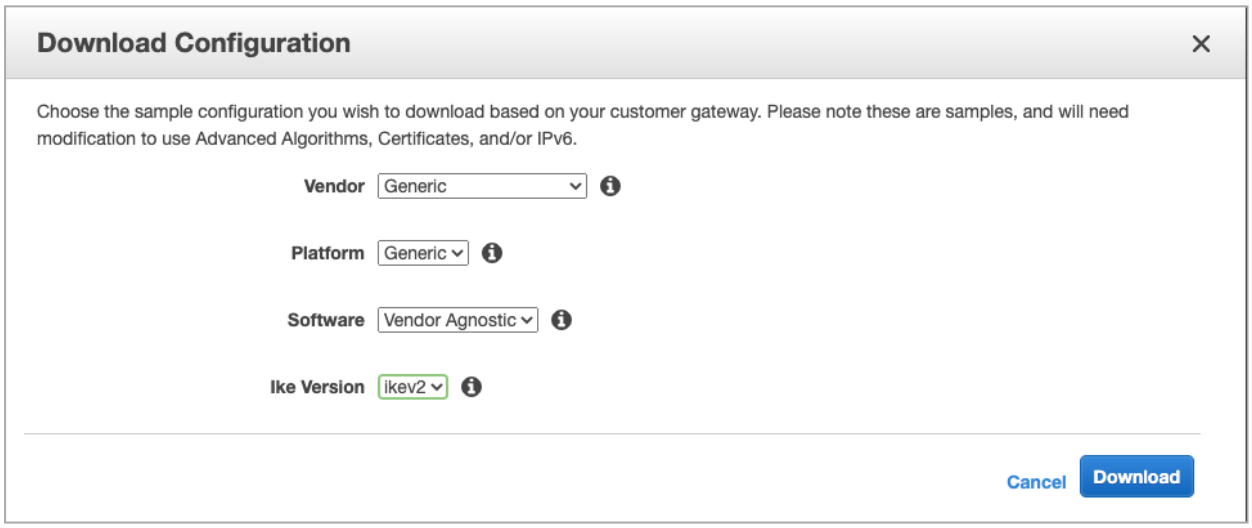
Rename it with a meaningful name.



5. Go back to **Site-to-Site VPN Connections**, select the VPN connection you created, and then click **Download Configuration**.

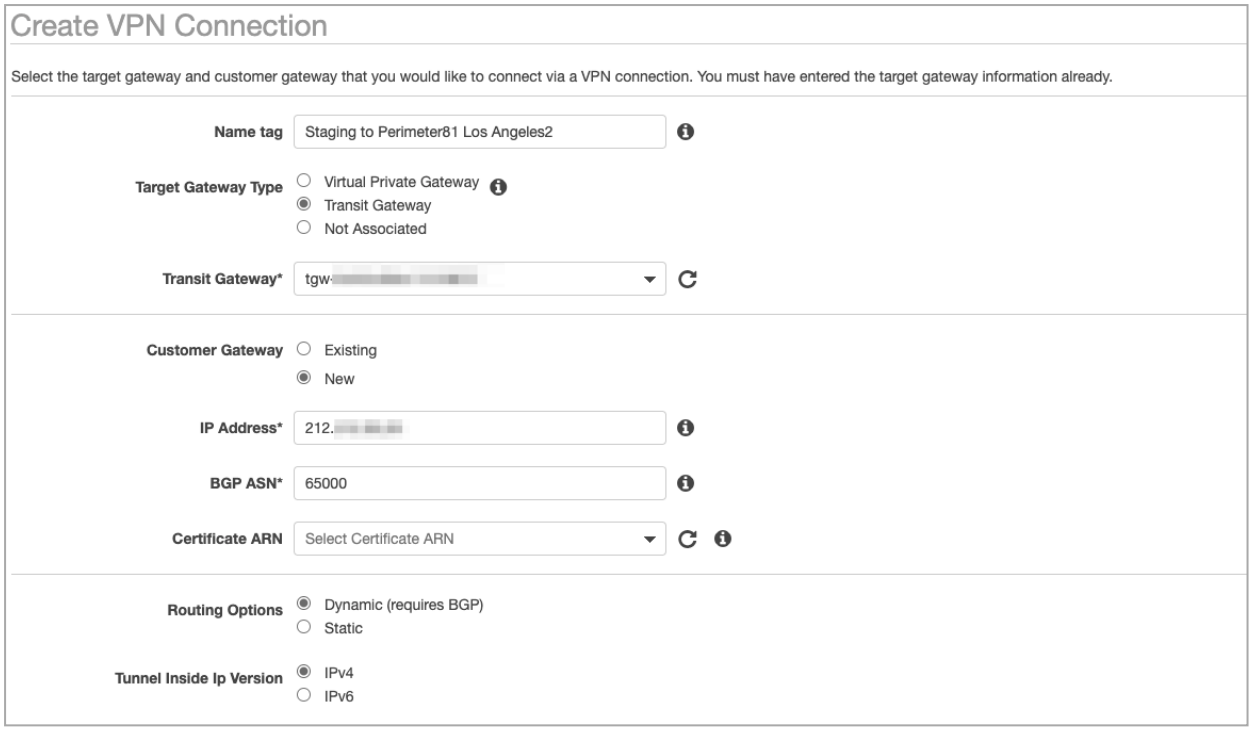


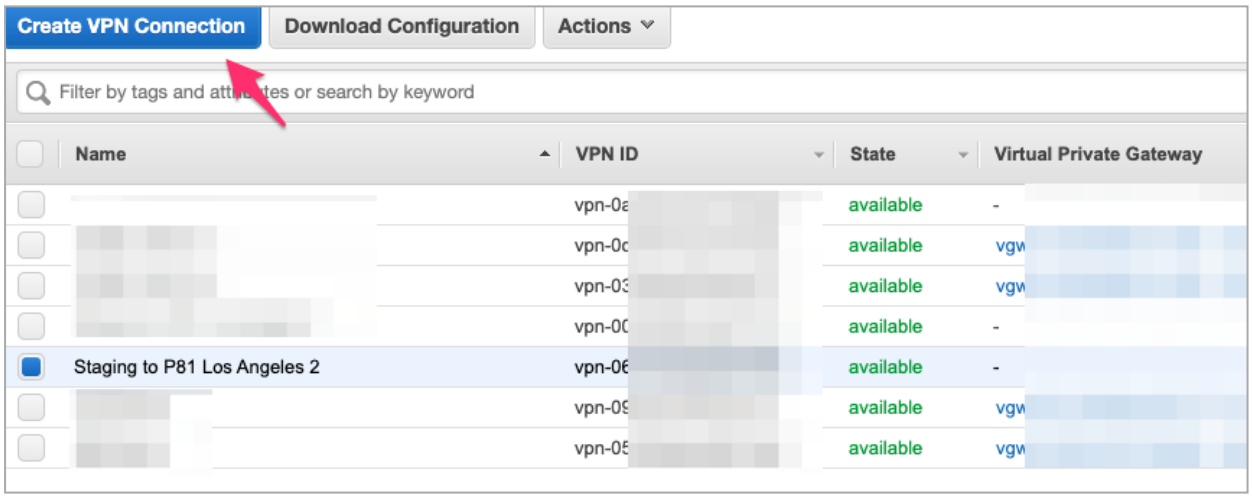
The **Download configuration** window appears.



6. Enter these:
   a. **Vendor** - Generic
   b. **Platform** - Generic
   c. **Software** - Vendor Agnostic
   d. **Ike version** - Ikev2
7. Click **Download**.

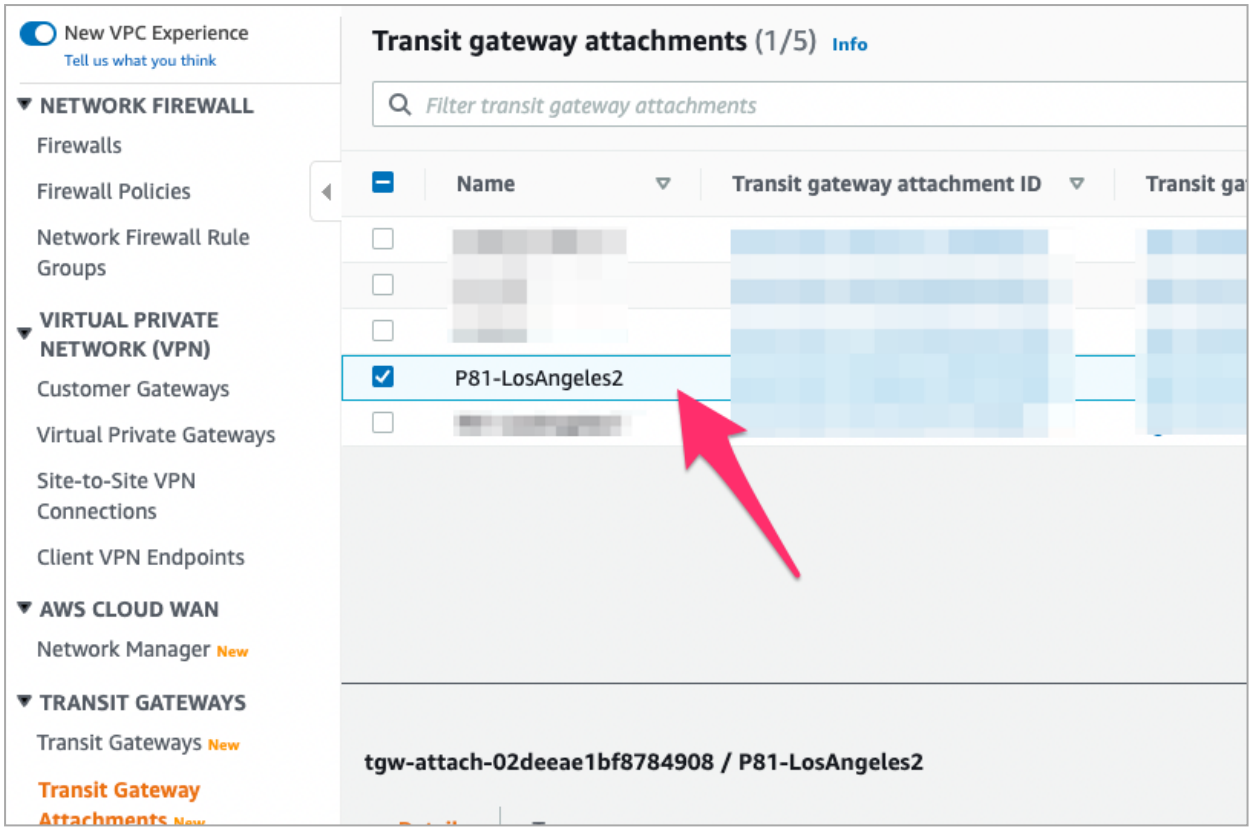
   The system downloads the file. Rename the file as *Tunnel1.txt*.
8. Repeat steps 1-7 for the other Site-to-Site Tunnel with the IP address of the second Check Point SASE gateway.



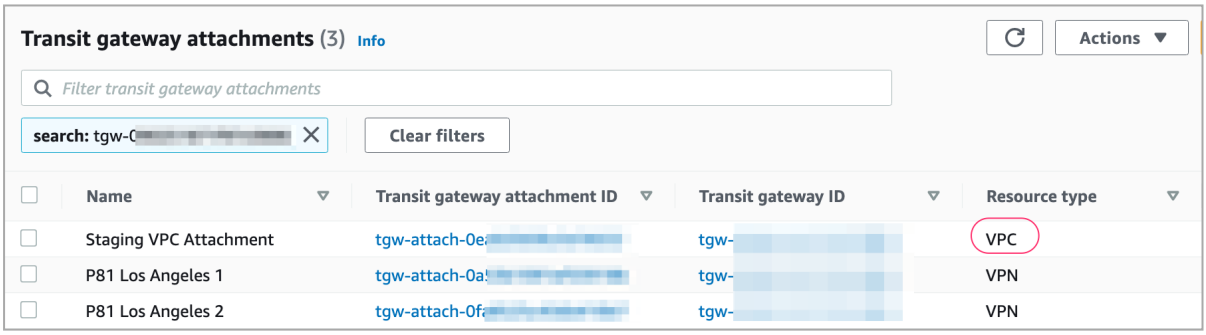


9. Rename the second downloaded file as *Tunnel2.txt*.
10. In the **TRANSIT GATEWAYS** section, go to **Transit Gateway attachments** and find the Transit Gateway Attachment you created.

    Rename it with a meaningful name.

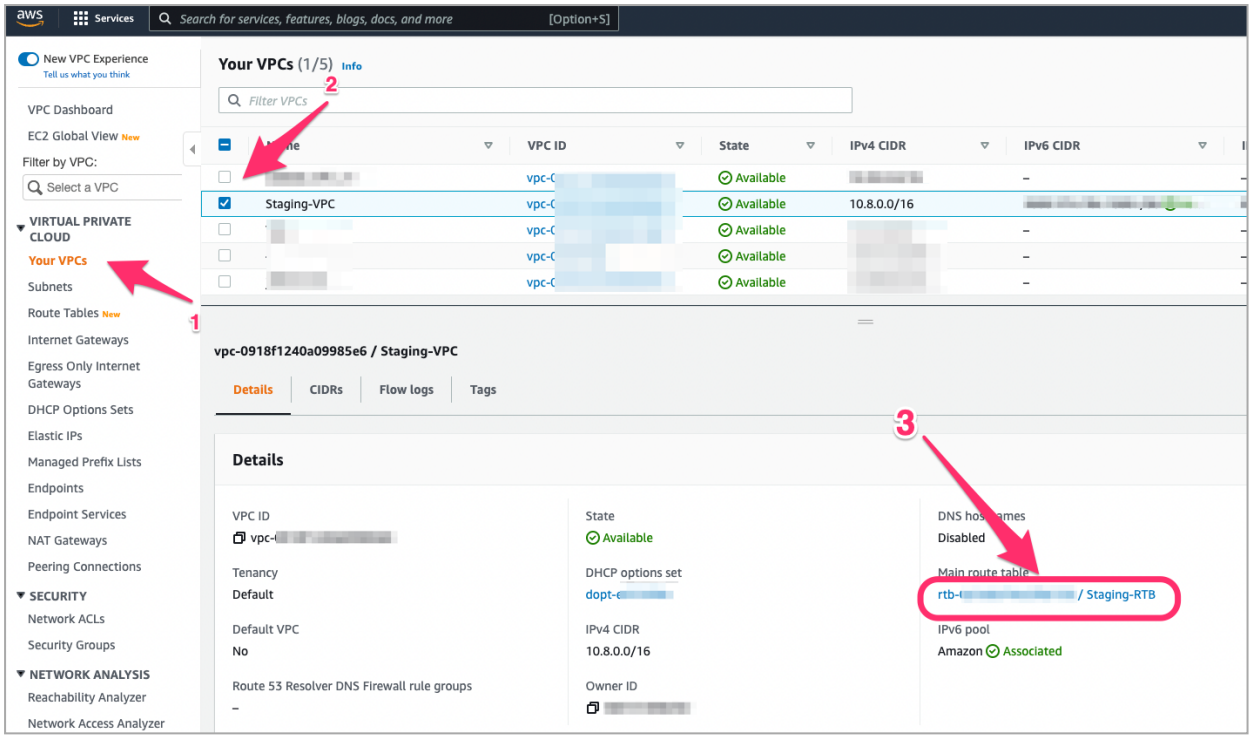


Note - To access your VPC through the redundant connection, you must have a VPC Attachment connected to the Transit gateway.



Creating Static Routes

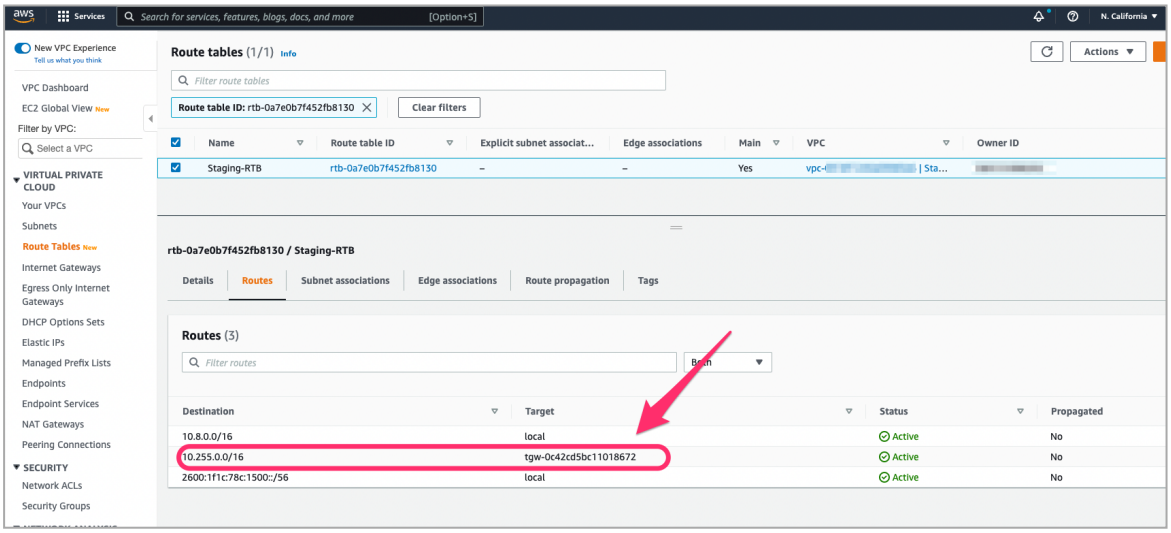
1. Access the AWS Management Console and go to **VPC**.
2. Select the corresponding VPC attached to the Transit Gateway and then select the **Main Route Table** for the VPC.



3. Edit the main Route Table for the VPC:

   a. In the **Destination** column, add the subnet mask of your Check Point SASE network.

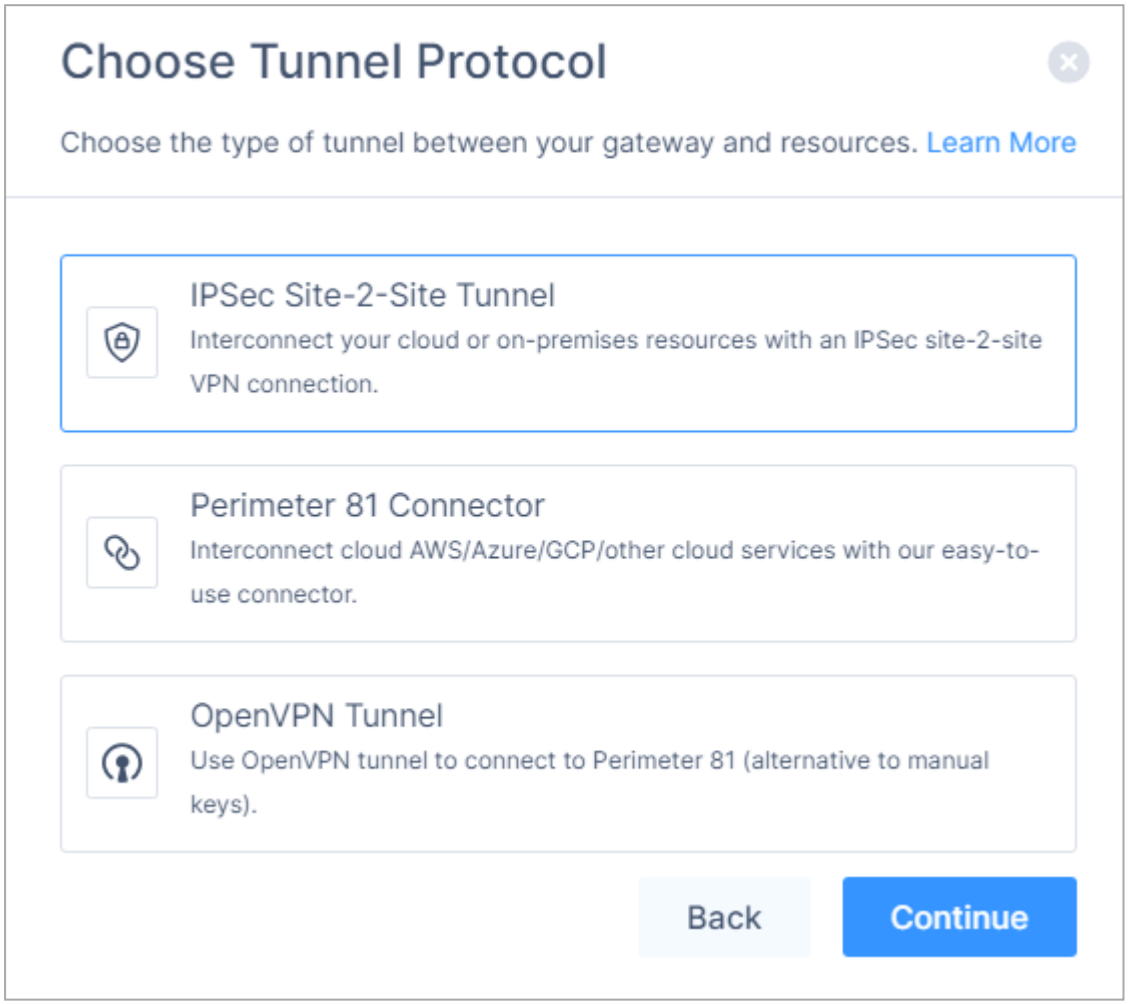
   b. In the **Target** column, select **Transit Gateway** (Route for reverse traffic).



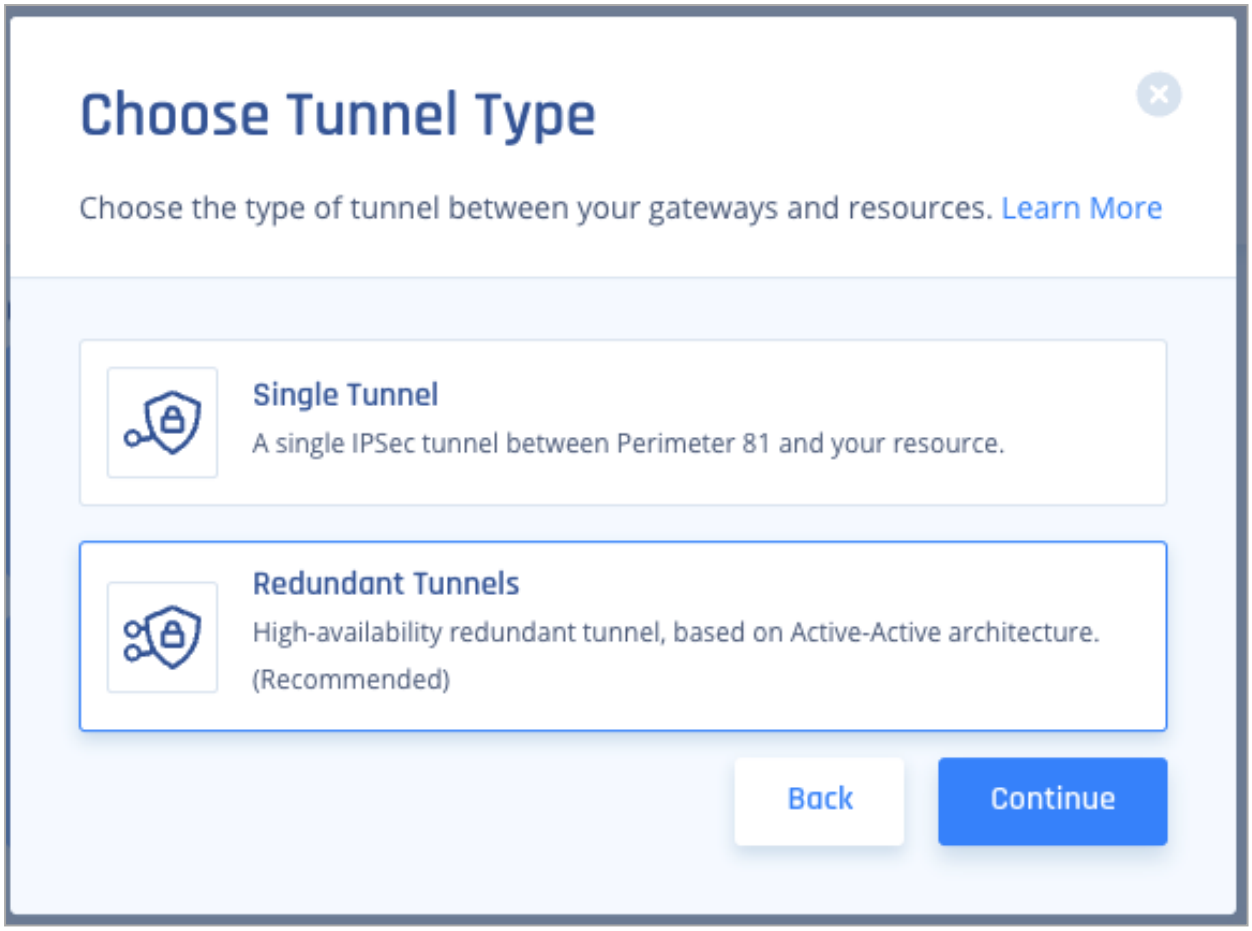
Note - If this is not the Main Route Table for the VPC, locate each subnet associated with the VPC and add the reverse route for the Check Point SASE internal subnet range.

Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal

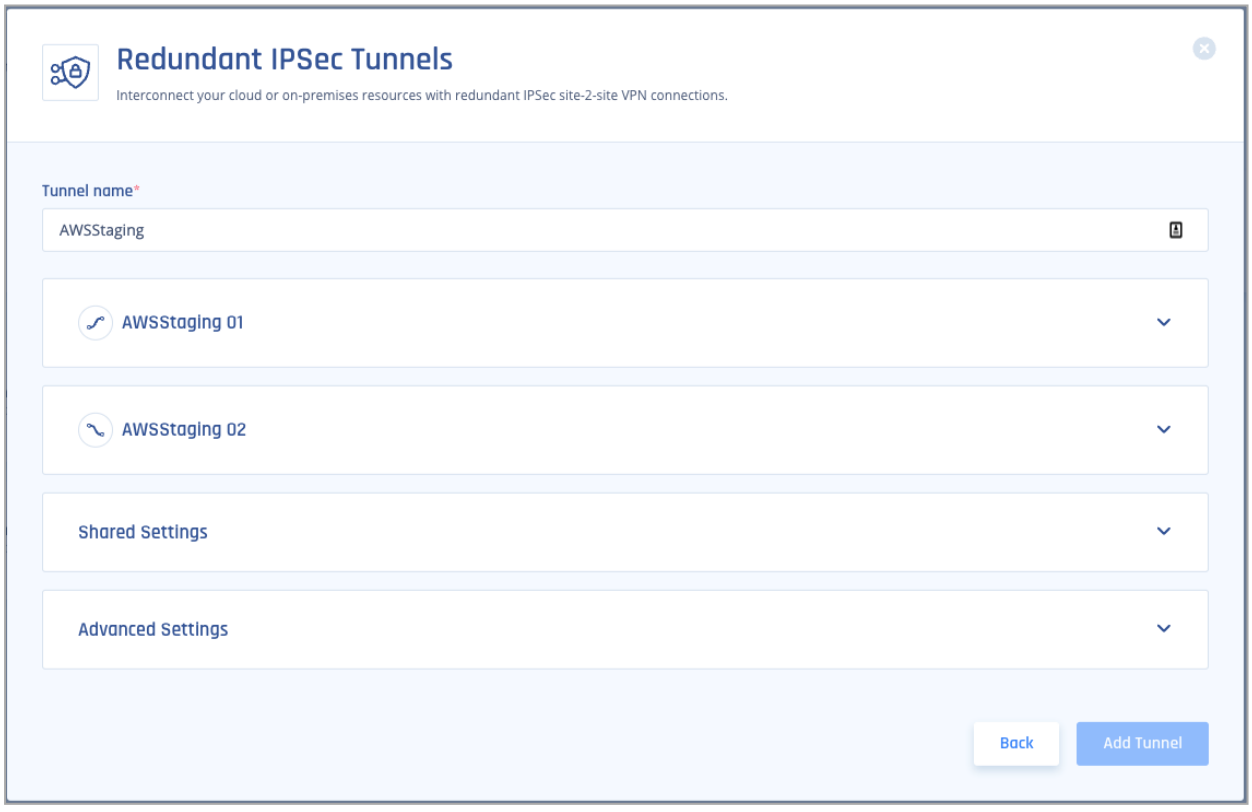
1. Access the Check Point SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



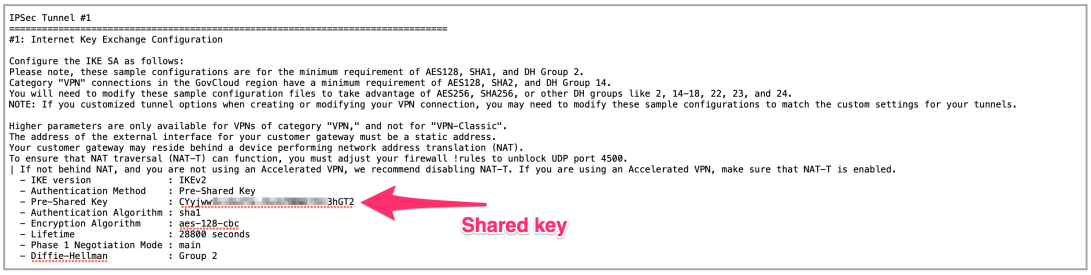
The **Redundant IPSec Tunnels** window appears.



6. For the first tunnel:
    a. Expand the **Tunnel 01** drop-down.
    b. To automatically populate the tunnel configuration values, click **Upload File** and upload Tunnel_1.txt file.

c. For manual configuration, copy the values from Tunnel_1.txt file as shown below.

i. **Shared Secret** - Pre-Shared Key

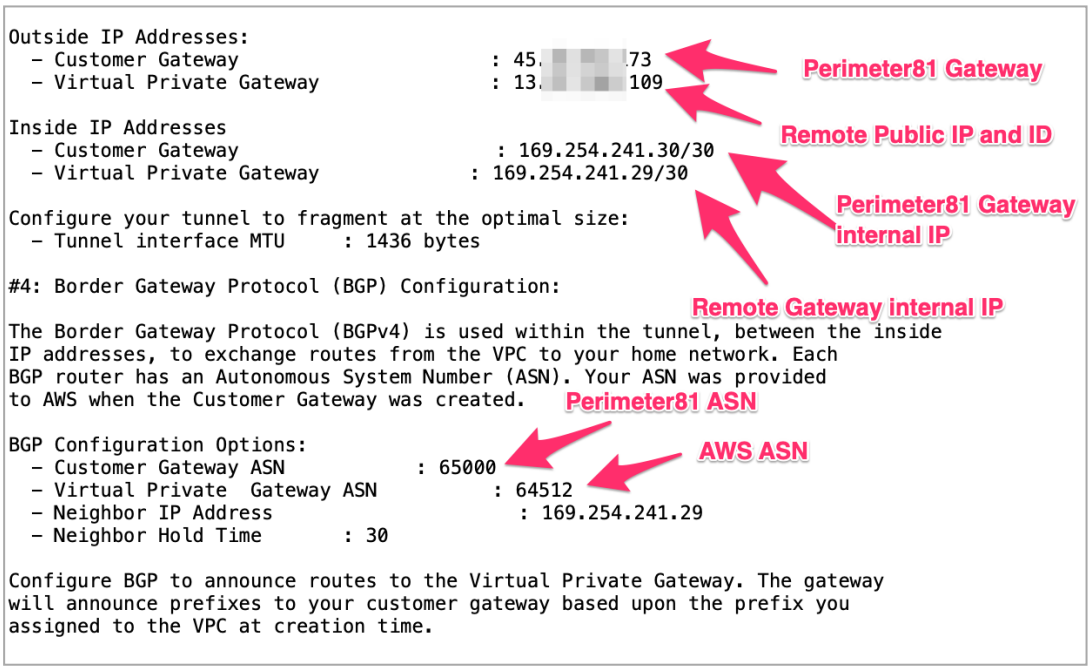


ii. **Check Point SASE gateway Internal IP** - Inside IP Addresses of Customer Gateway.

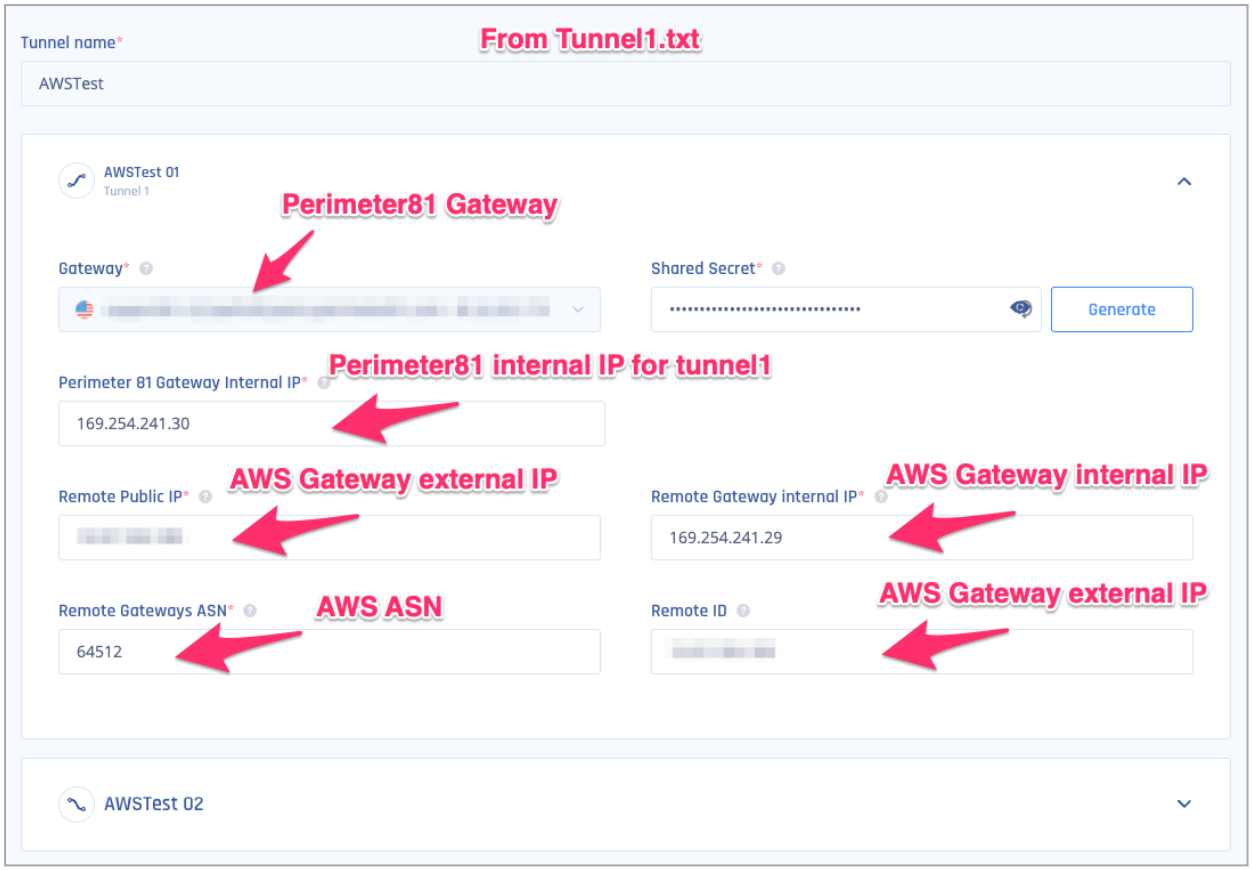
iii. **Remote Public IP & Remote ID** - Outside IP Addresses of Virtual Private Gateway.

iv. **Remote Gateway internal IP** - Inside IP Addresses of Virtual Private Gateway. The IP on the AWS side has a subnet (/30), discard it when pasting.

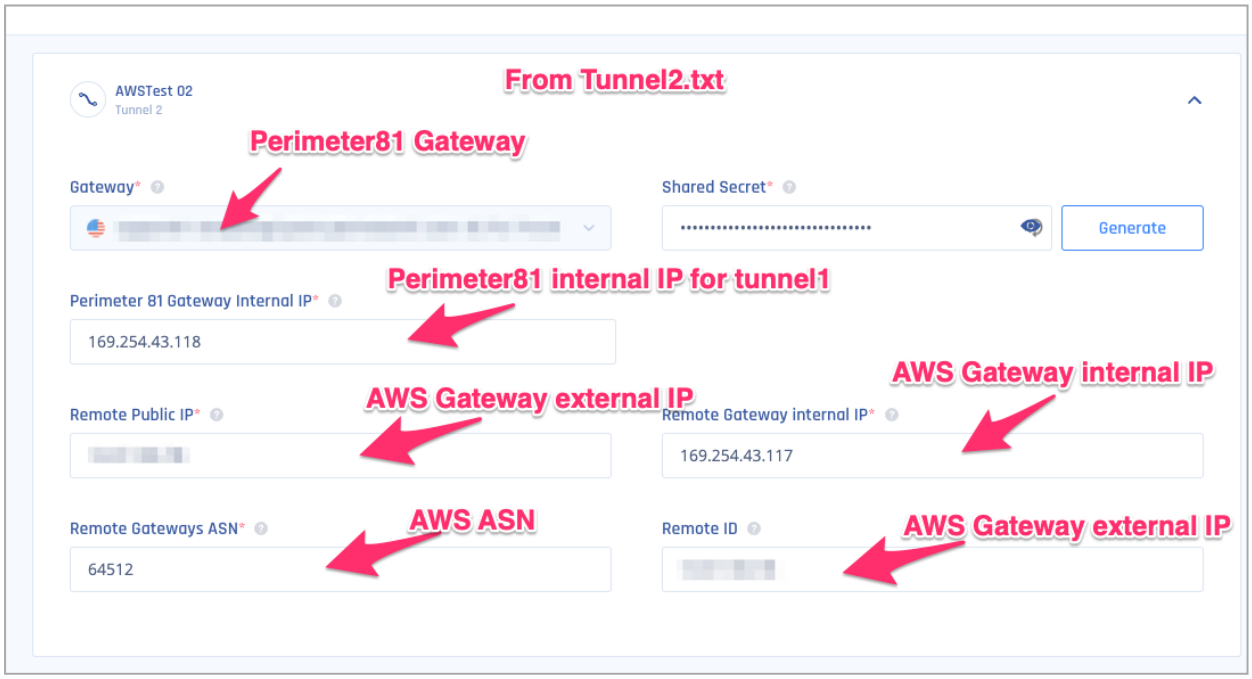
v. **Remote Gateway ASN** - BGP Configuration Options of Virtual Private Gateway ASN from the file.



7. Enter the above copied values.



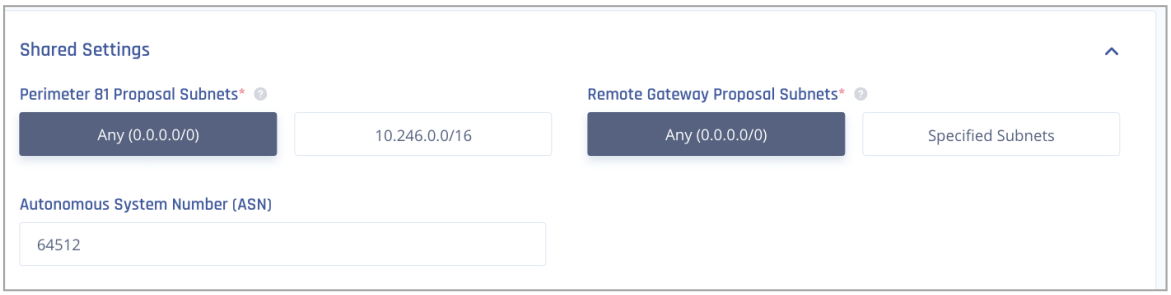
8. For the second tunnel, expand the **Tunnel 02** drop-down and repeat step 6 with the values from *Tunnel_2.txt* file.



9. In the **Shared Settings** section:

a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.

b. The **ASN** number should be the same as the Customer Gateway ASN you configured on the AWS Management console.



10. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

11. Click **Add Tunnel**.

Azure Virtual Network Gateway

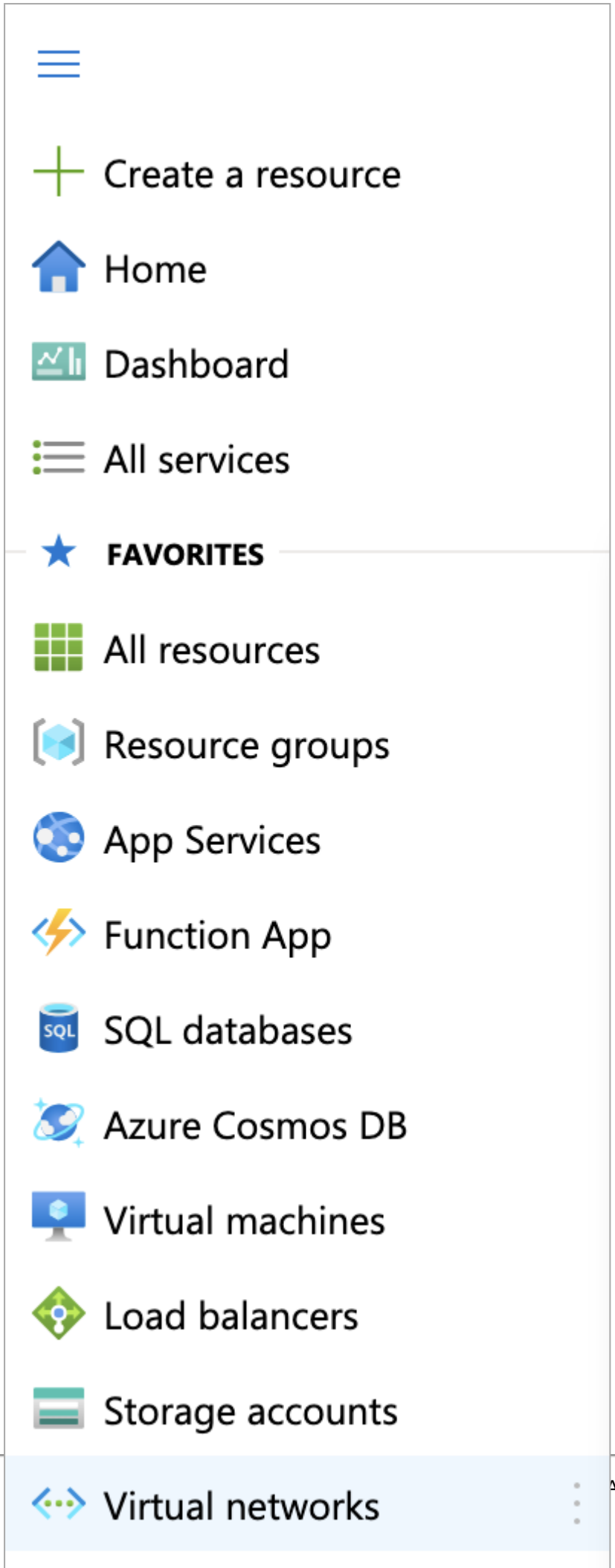
Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

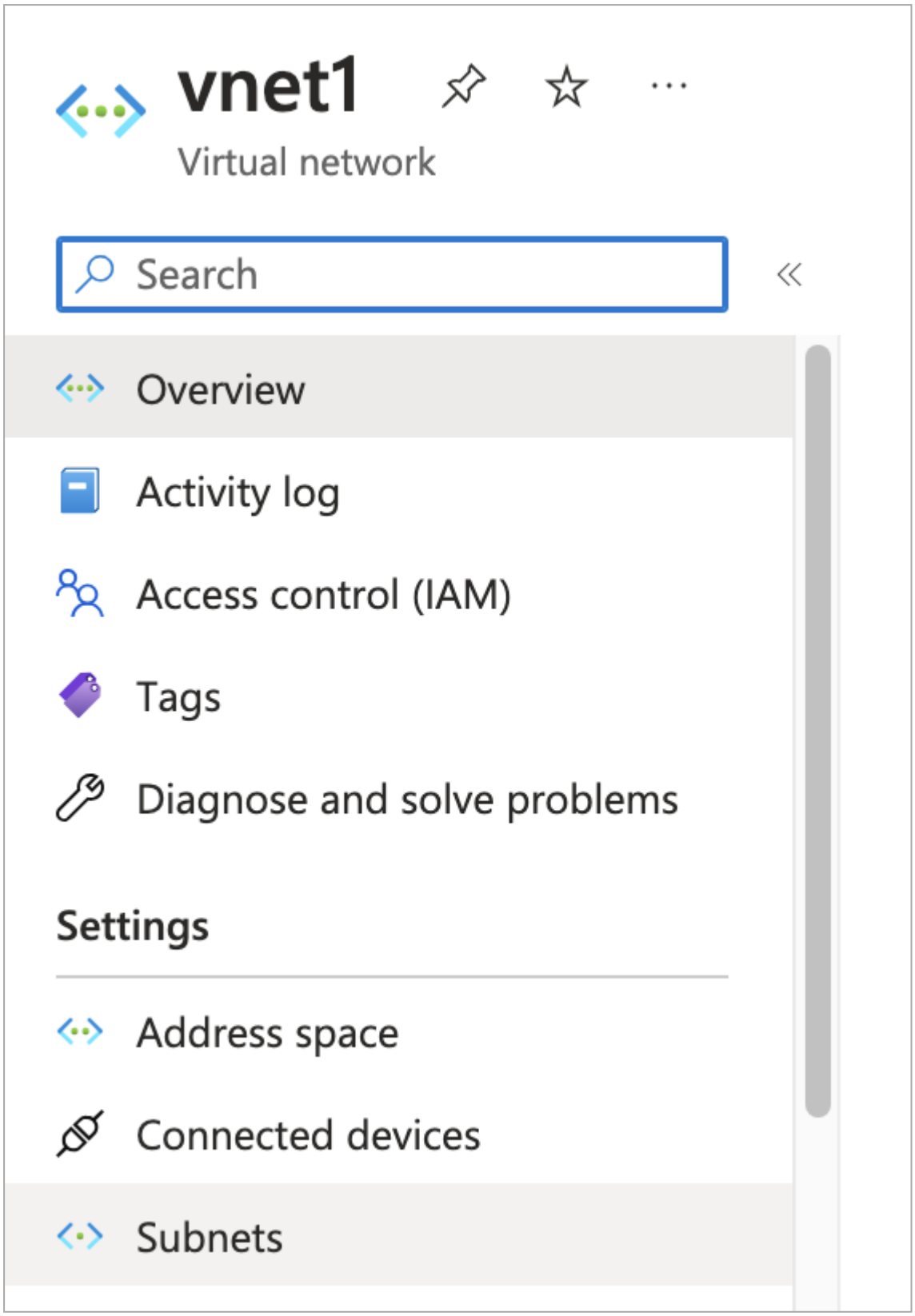
Step 1 - Configurations in the Azure Management Portal

Creating a Gateway Subnet

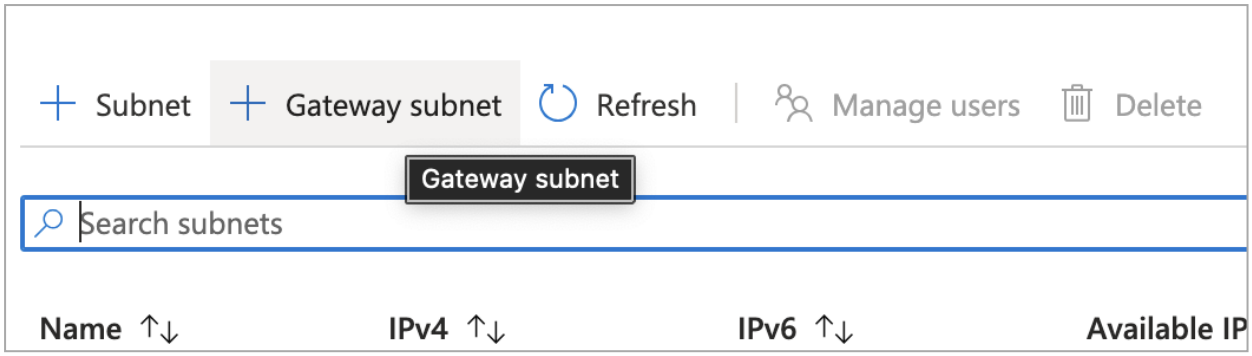
1. Access the Azure Management Portal and go to **Virtual networks**.


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks

2. Click the virtual network to which you wan to create the gateway and click **Subnets**.



3. Click **+ Gateway subnet**. The system populates the subnet name as **Gateway subnet** by default.



4. (Optional) Adjust the auto-filled Address range values. This subnet is used for the Virtual Gateway only.

   If this range is not auto-filled:

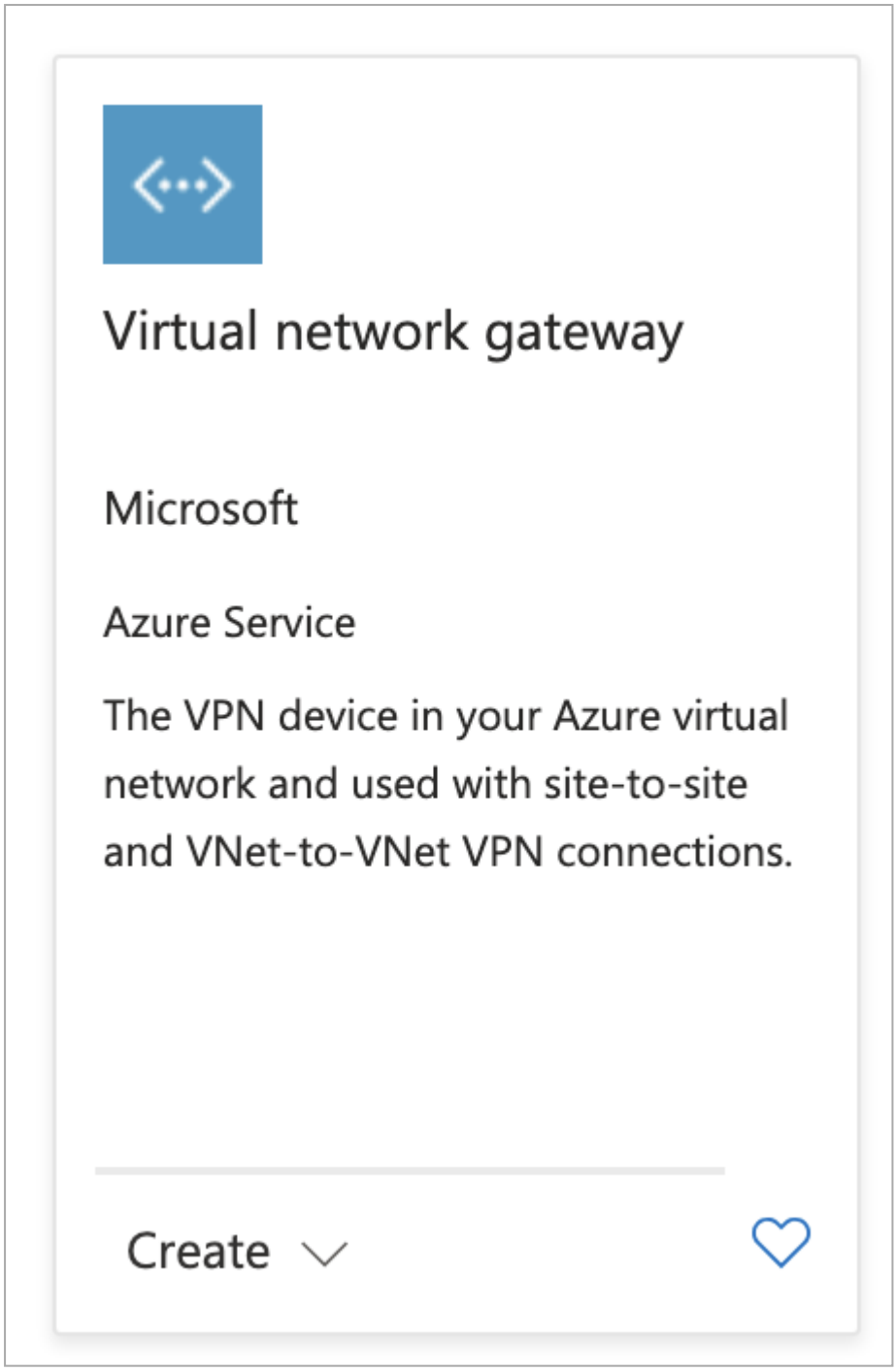
   a. Go to address space and click **+Add**.

   b. Select a random /27 bit mask subnet space. For example, 10.1.255.0/27.

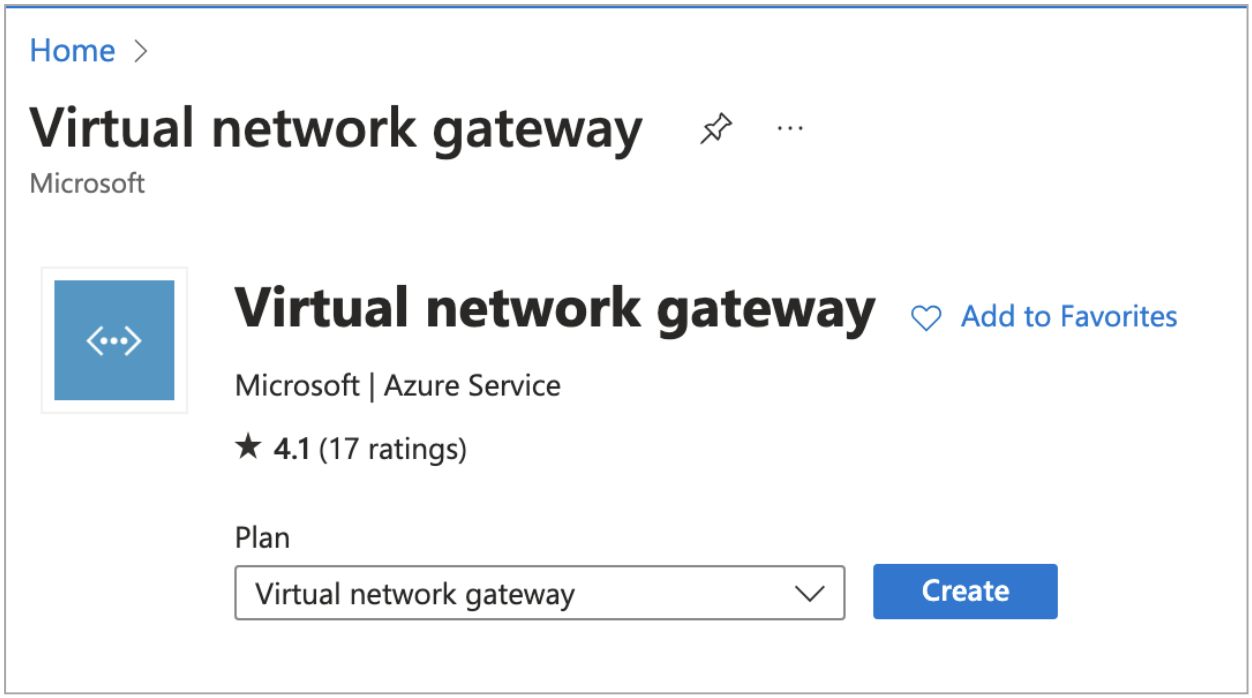
Creating a Virtual Network Gateway

1. Access the Azure Management Portal and click **+Create a resource**.

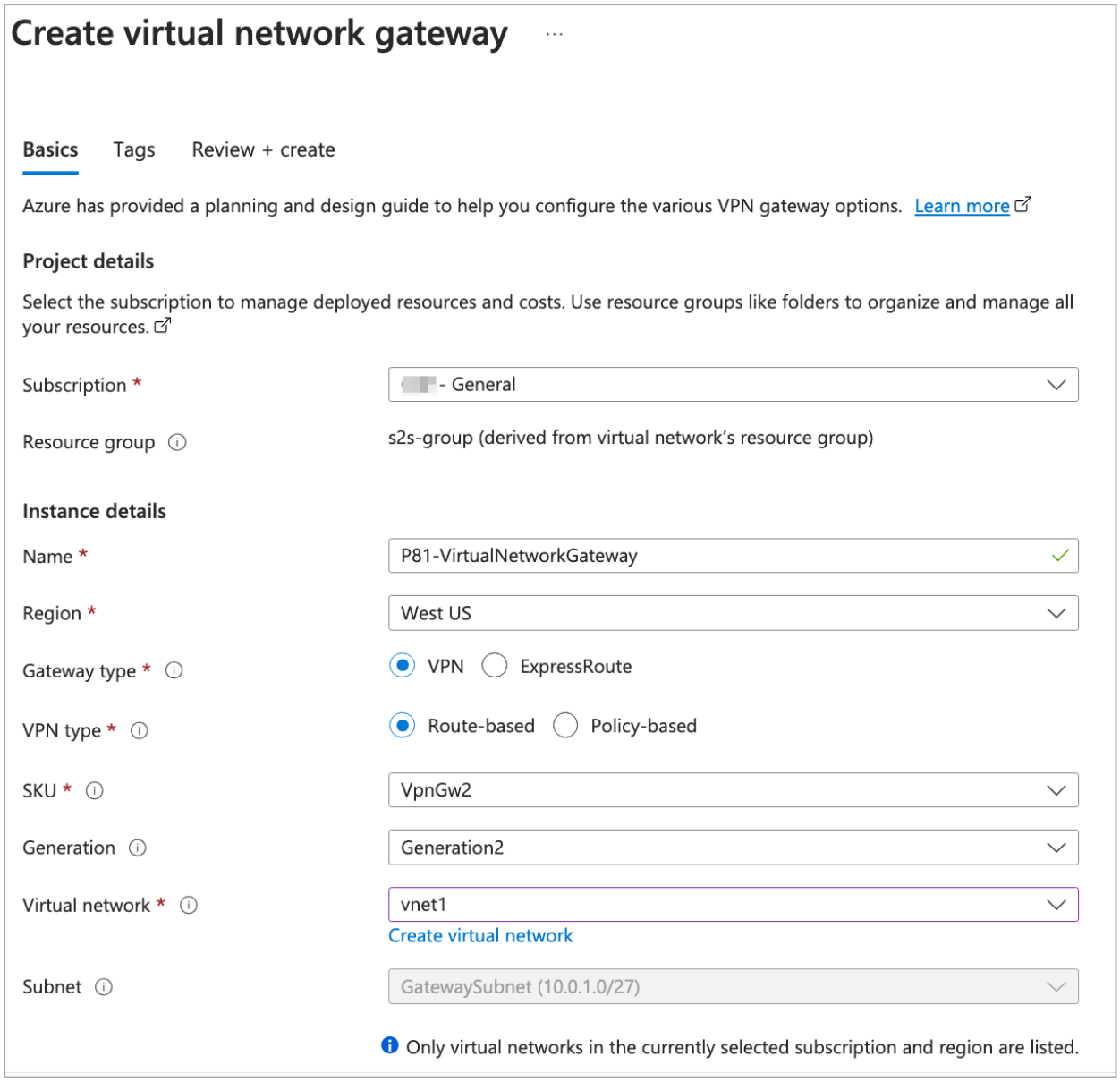
2. Search for **Virtual Network Gateway** and click it in the search results.



3. Click **Create**.



4. The **Create virtual network gateway** window appears.



5. Enter these:
   a. **Name** - Name of the gateway.
   b. **Region** - Region where your resources are located.
   c. **Gateway type** - VPN.
   d. **SKU** - Select the gateway SKU from the list. The SKUs listed depends on the selected VPN.

e. **Virtual network** - The Virtual network that contains the resources you want to reach through the tunnel.

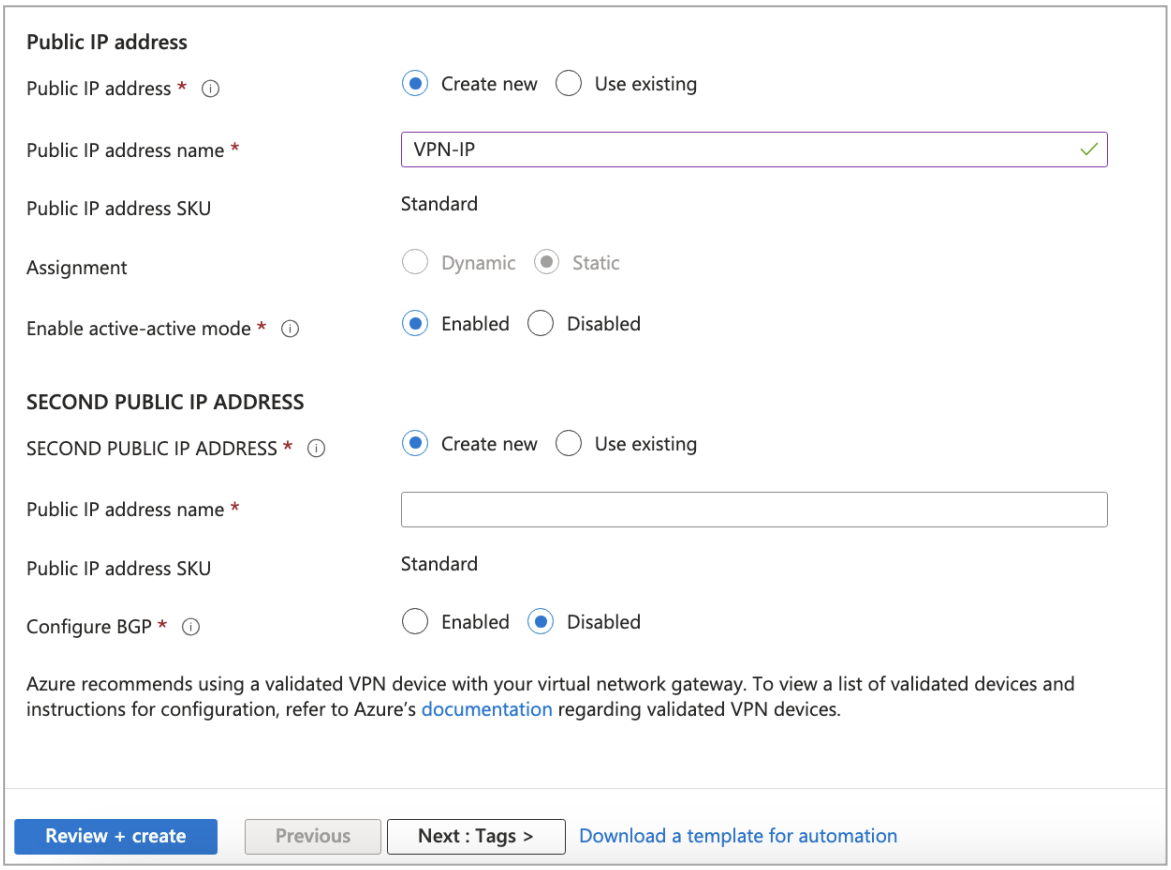
   The **Choose a virtual network** page appears.

   Note - If you do not see your VNet, make sure your virtual network is located in the selected **Region**.

f. **Subnet** - Subnet range for your virtual network.

   This setting appears only when you create a gateway subnet for your virtual network for the first time.

g. **Public IP address** - Click **Create New** or choose an existing IP used by your organization.



h. **Enable active-active mode** - Disabled.

i. **Configure BGP** - Disabled.

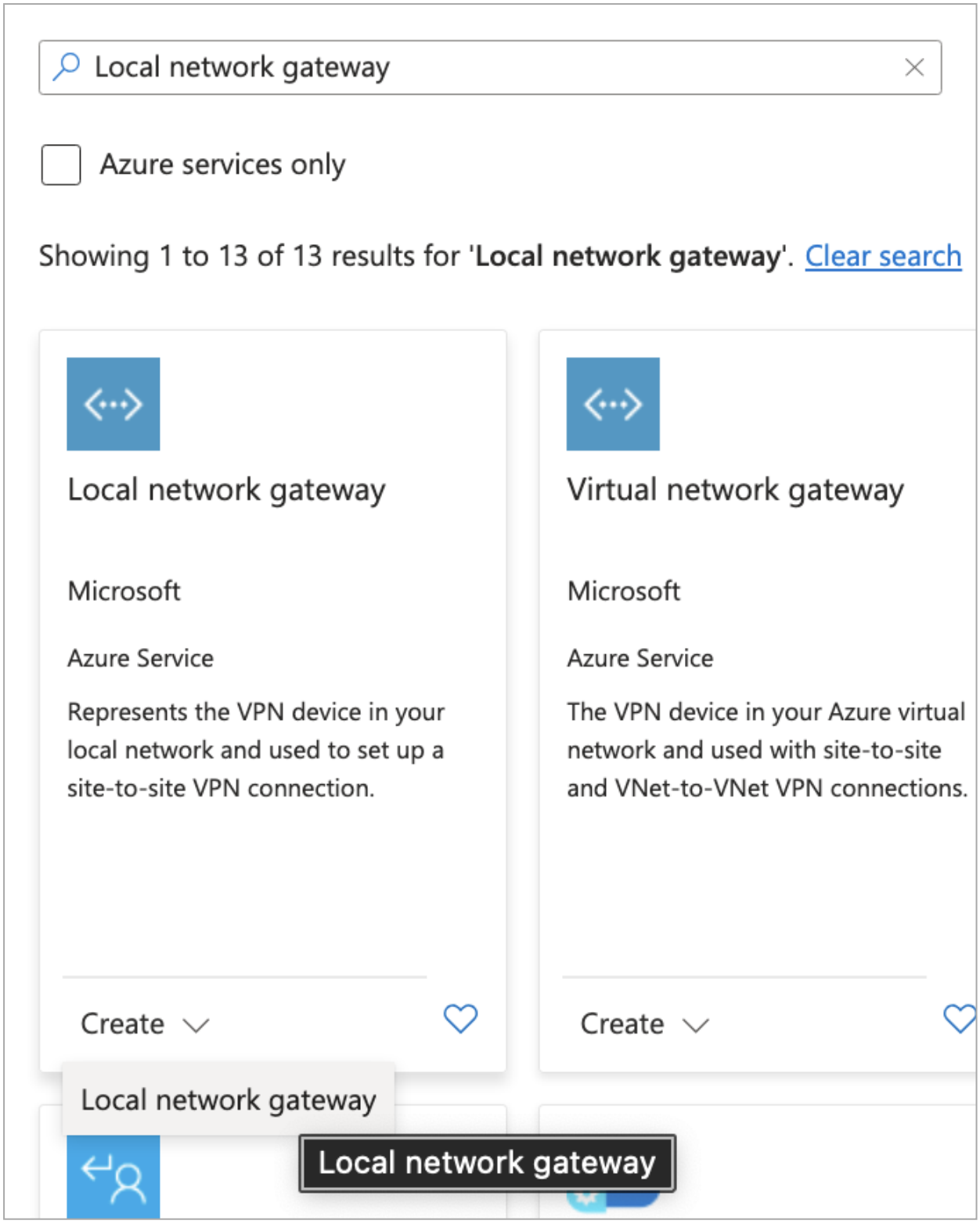
j. Click **Review+create**.

   The system starts to create the VPN gateway and it may take up to 45 minutes to complete.

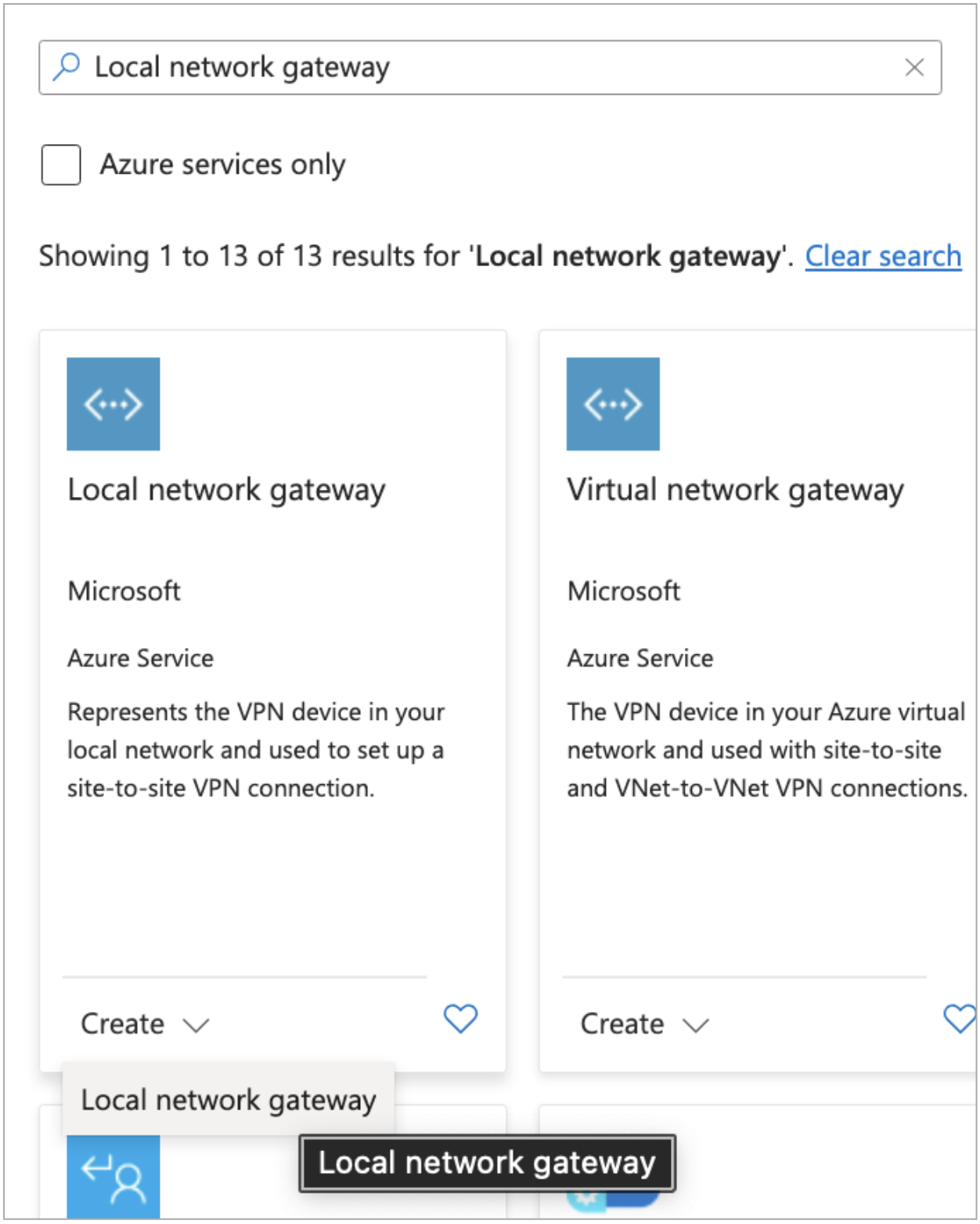
Creating a Local Network Gateway

1. Access the Azure Management Portal and click **+Create a resource**.

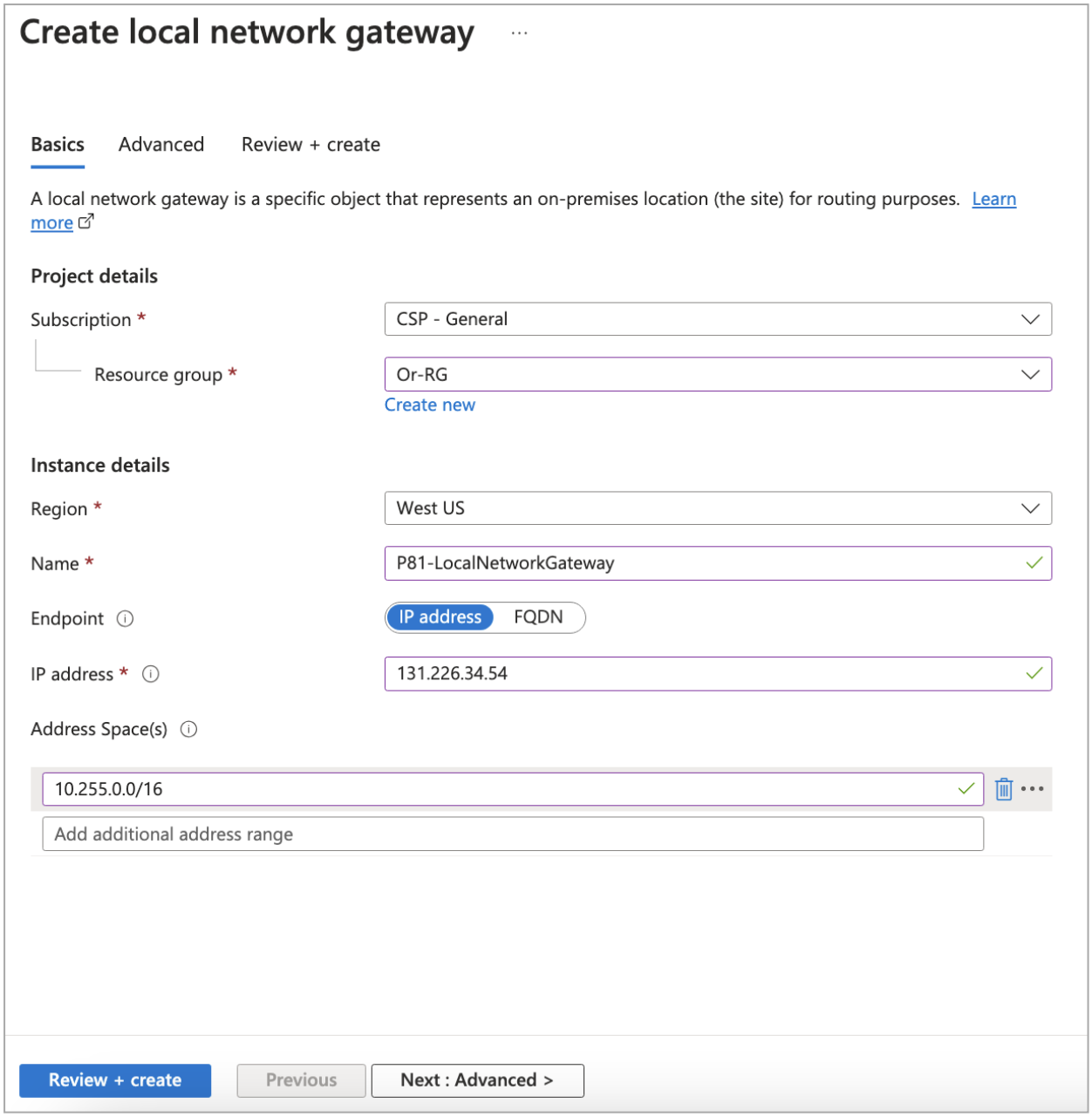
2. Search for **Local network gateway** and click it in the search results.



3. Click **Create**.



The **Create local network gateway** page appears.



4. Enter these:
   a. **Name** - Name of your gateway.
   b. **IP address** - IP address of your Check Point SASE gateway.

c. **Address Space** - Check Point SASE subnet.

   Make sure that these ranges do not overlap with other networks' ranges that you want to connect to.

d. **Subscription** - Verify that the value is correct.

e. **Resource Group** - Select the resource group that you want to use. Create a new resource group or select one that you have already created.

f. **Location** - Select the location where this object is created.

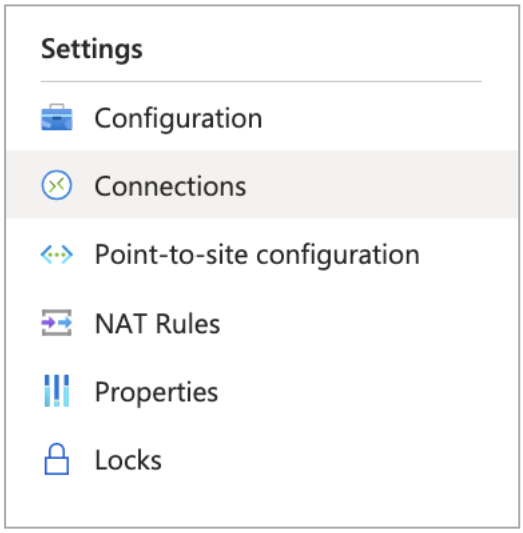
   (Optional) Select the location in which your Virtual Network resides.

g. **SKU** - Select the gateway SKU from the list. The SKUs listed depends on the selected VPN.

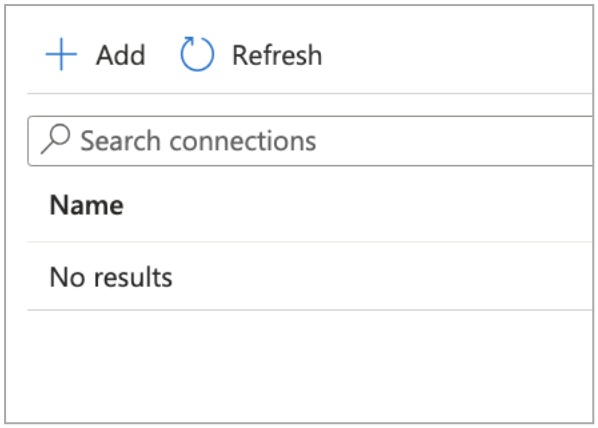
5. Click **Create**.

Creating the IPSecTunnel Connection

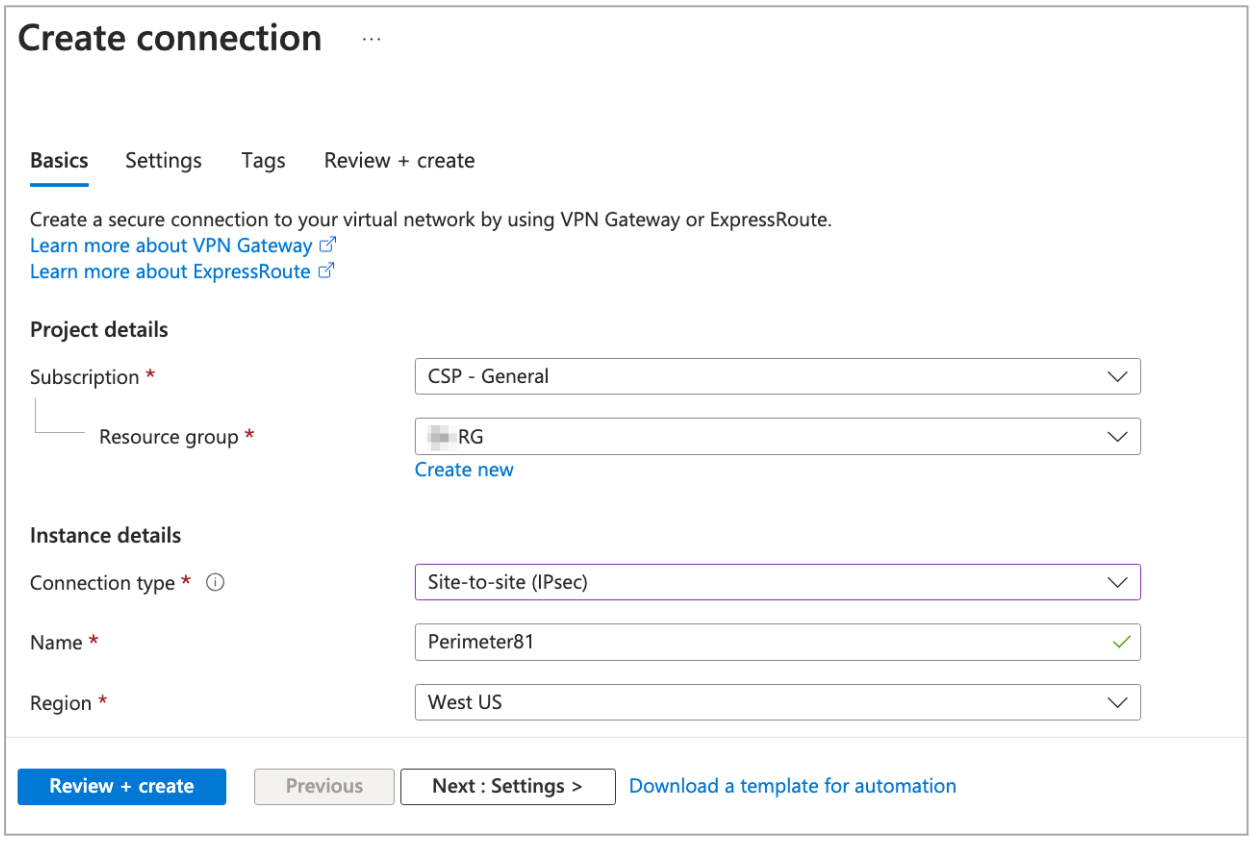
1. Access the Azure Management Portal and go to your **Virtual Network Gateway** page.
2. Go to **Settings** and click **Connections**.



3. Click **+Add**.

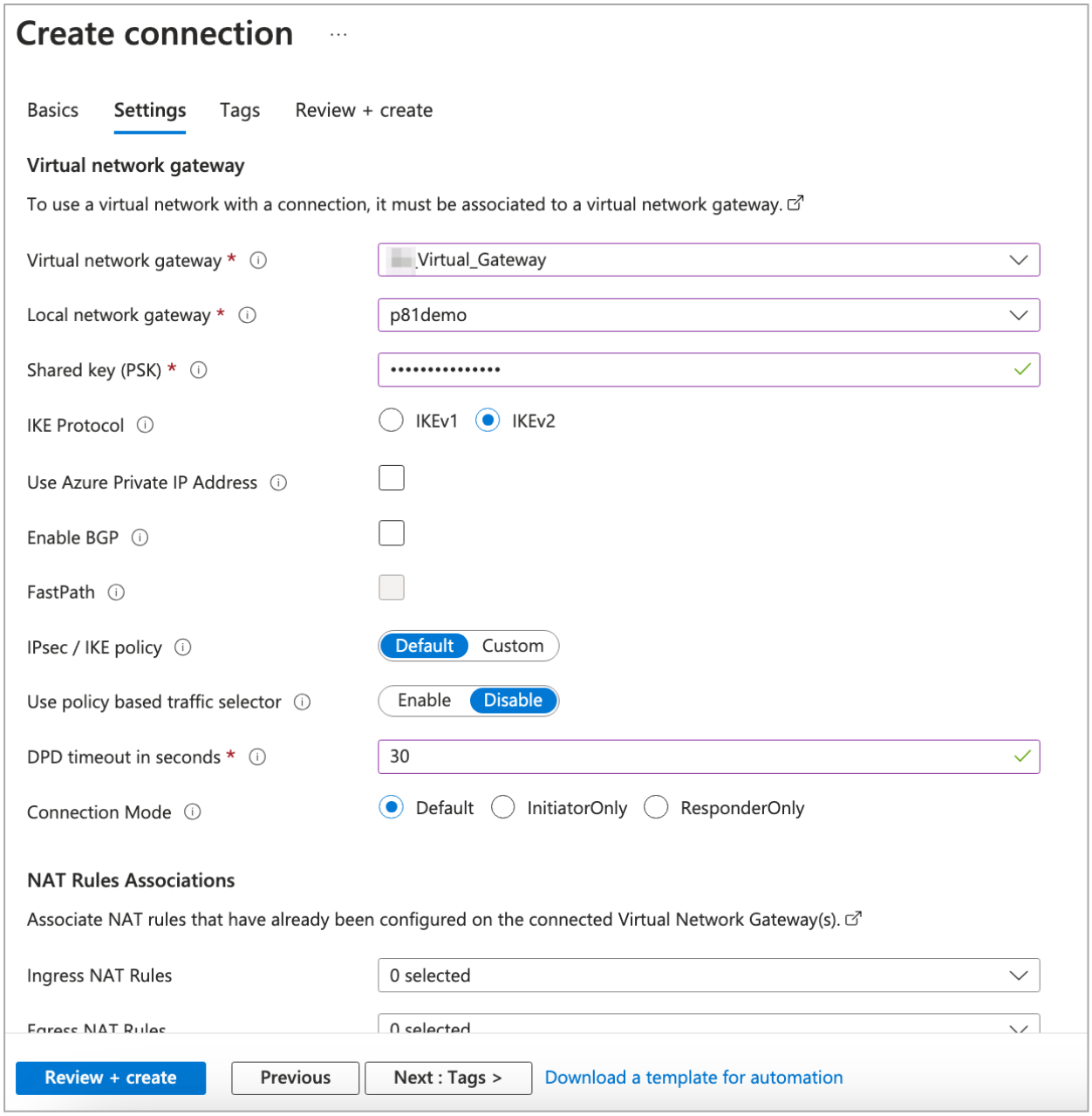


The **Create connection** window appears.



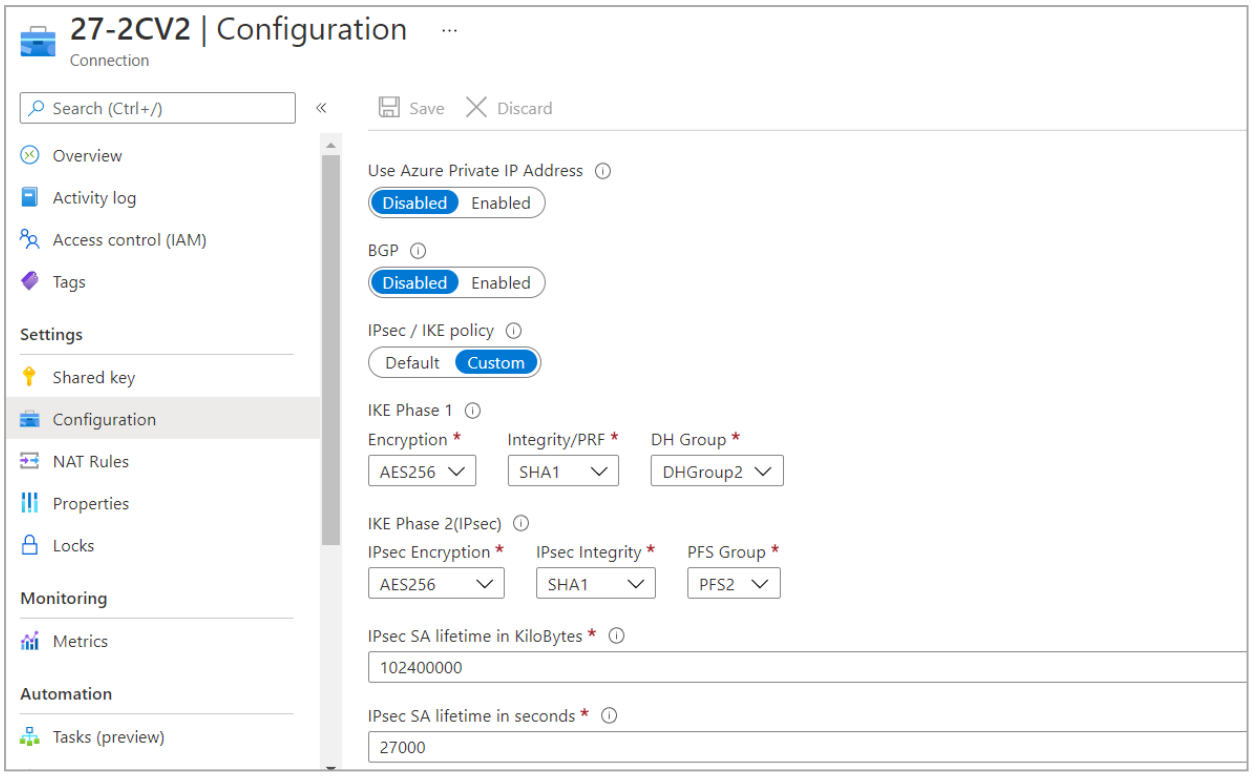
4. In the **Basics** tab, enter these:
   a. **Connection type** - Site-to-site (IPSec).
   b. **Name** - Name of the connection.
5. Click **Next: Settings >**.

   The **Settings** tab appears.

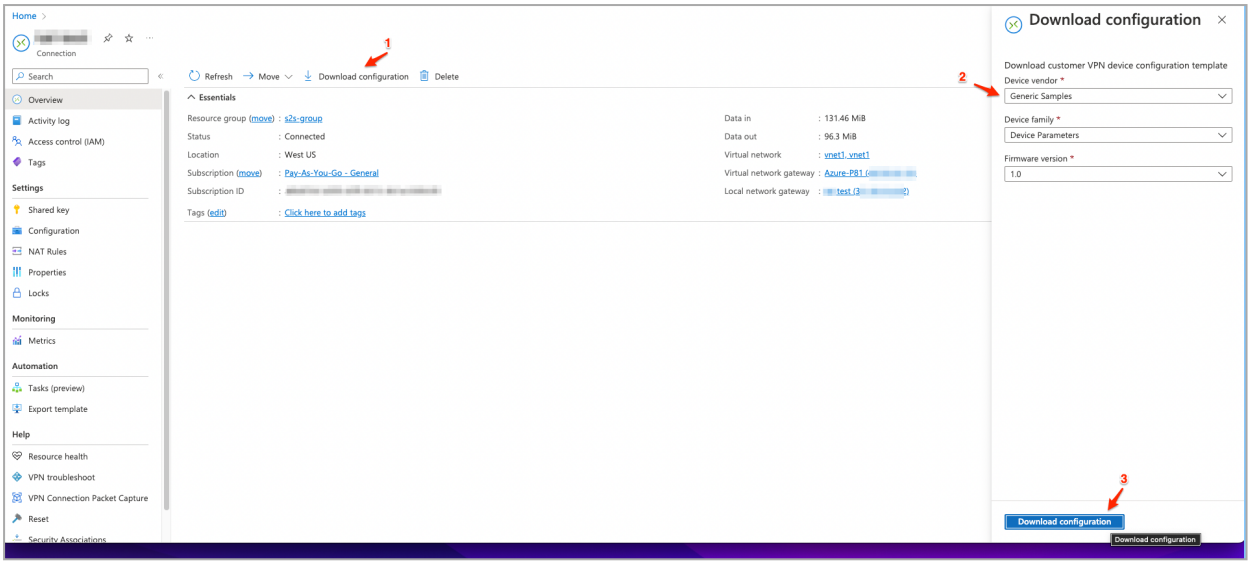


6. Enter these:
   a. **Virtual network gateway** - IP address you receive from Azure. The value is static.
   b. **Local network gateway** - Local network gateway (your Check Point SASE network address) which you have created. The value is static.
   c. **Shared Key (PSK)** - Create a unique key value. This must match with the key value used for the Check Point SASE tunnel.
   d. **IKE Protocol** - IKev2.
   e. **DPD timeout in seconds** - 30
7. Click **Review + Create** to create your connection.
8. Select the connection you just created and click **configuration**.

The **Configuration** window appears.



9. Enter these:
    a. **IPsec / IKE policy** - Select **Custom** and use these values to align with the values set in Check Point SASE tunnel settings.
        i. **Encryption** - AES256
        ii. **Integrity/PRF** - SHA1
        iii. **DH Group** - DHGroup2
        iv. **IPsec Encryption** - AES256
        v. **IPsec Integrity** - SHA1
        vi. **PFS Group** - PFS2
        vii. **IPsec SA lifetime in KiloBytes** - 102400000
        viii. **IPsec SA lifetime in seconds** - 27000
10. Go to **Overview** > **Download configuration**.

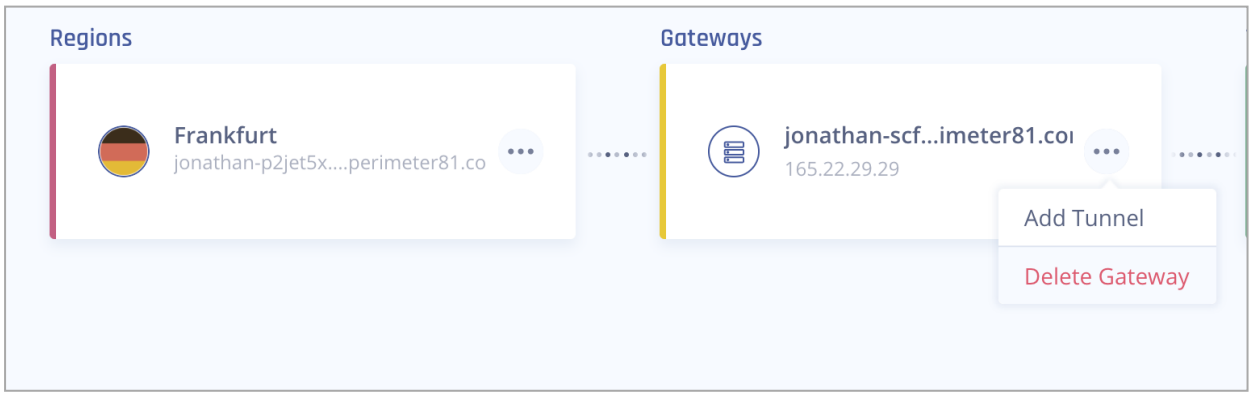


11. Enter these:
    a. **Device vendor** - Generic Samples
    b. **Device family** - Device Parameters
    c. **Firmware version** - 1.0
12. Click **Download Configuration**.

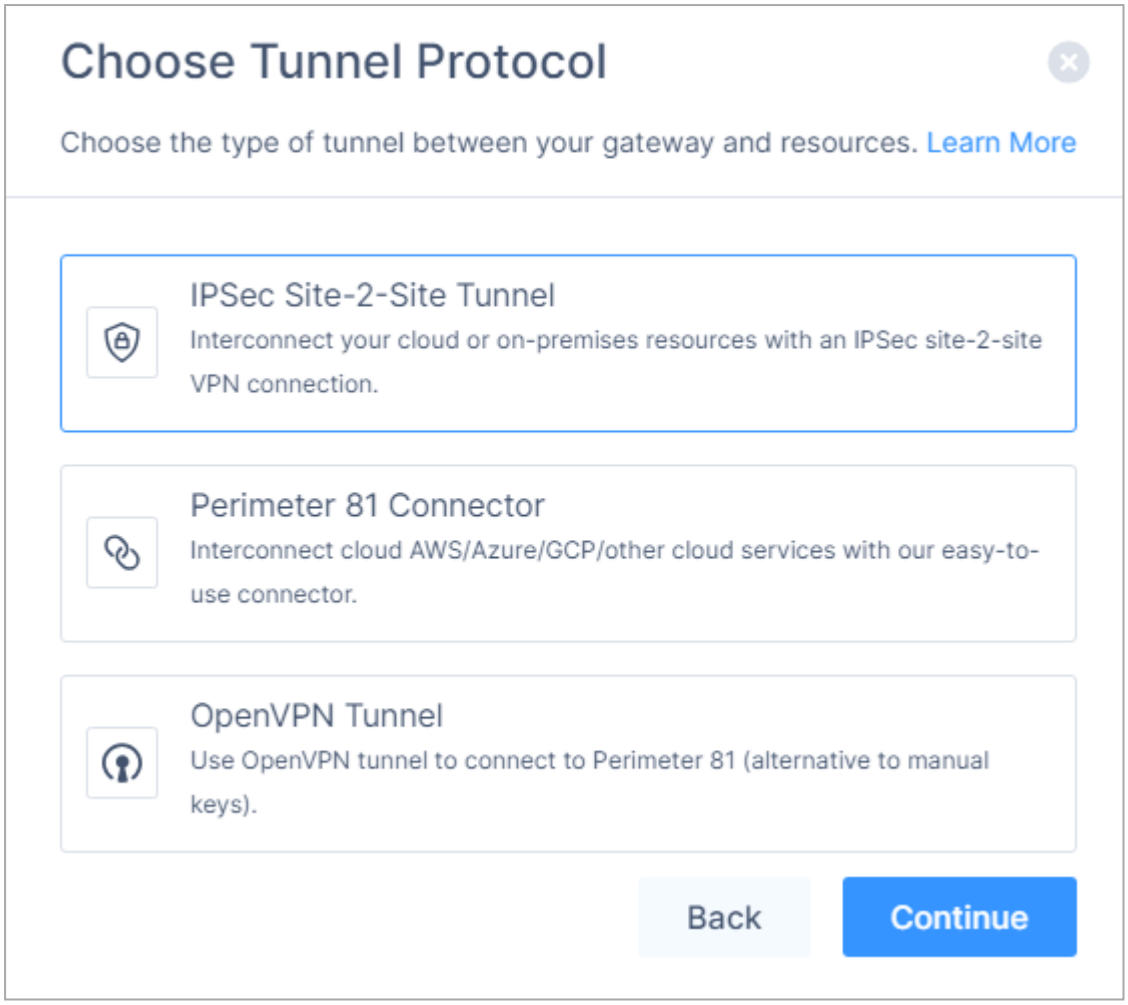
    The system downloads the configuration file.

Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

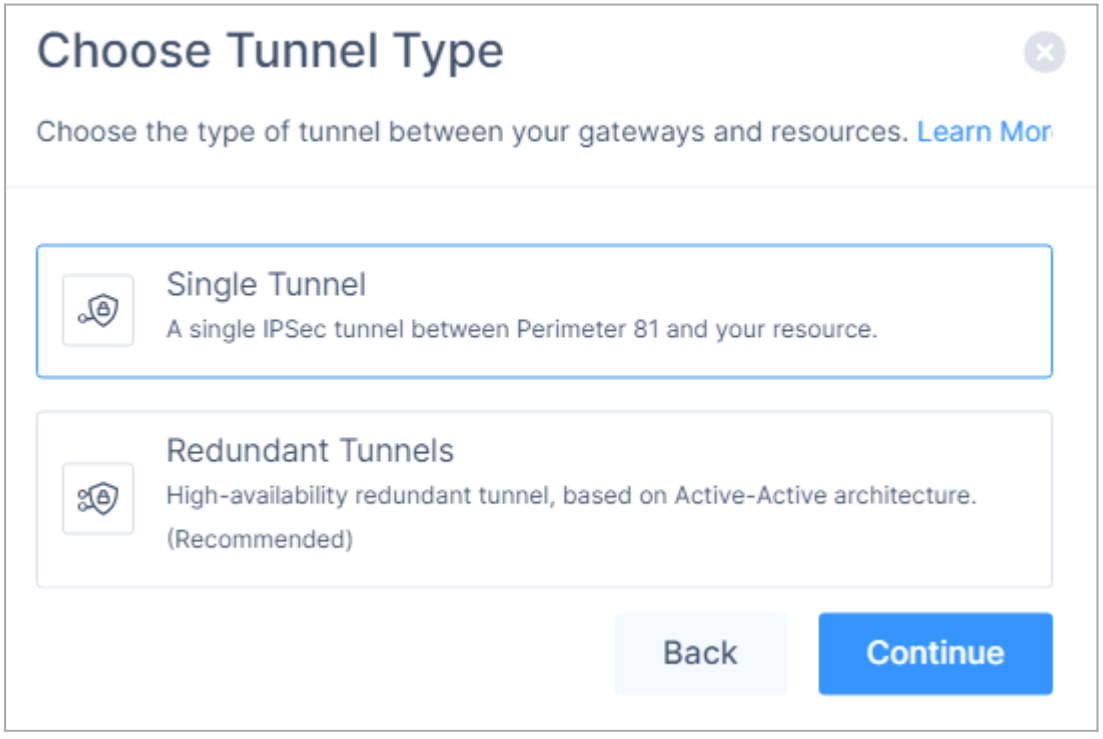
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



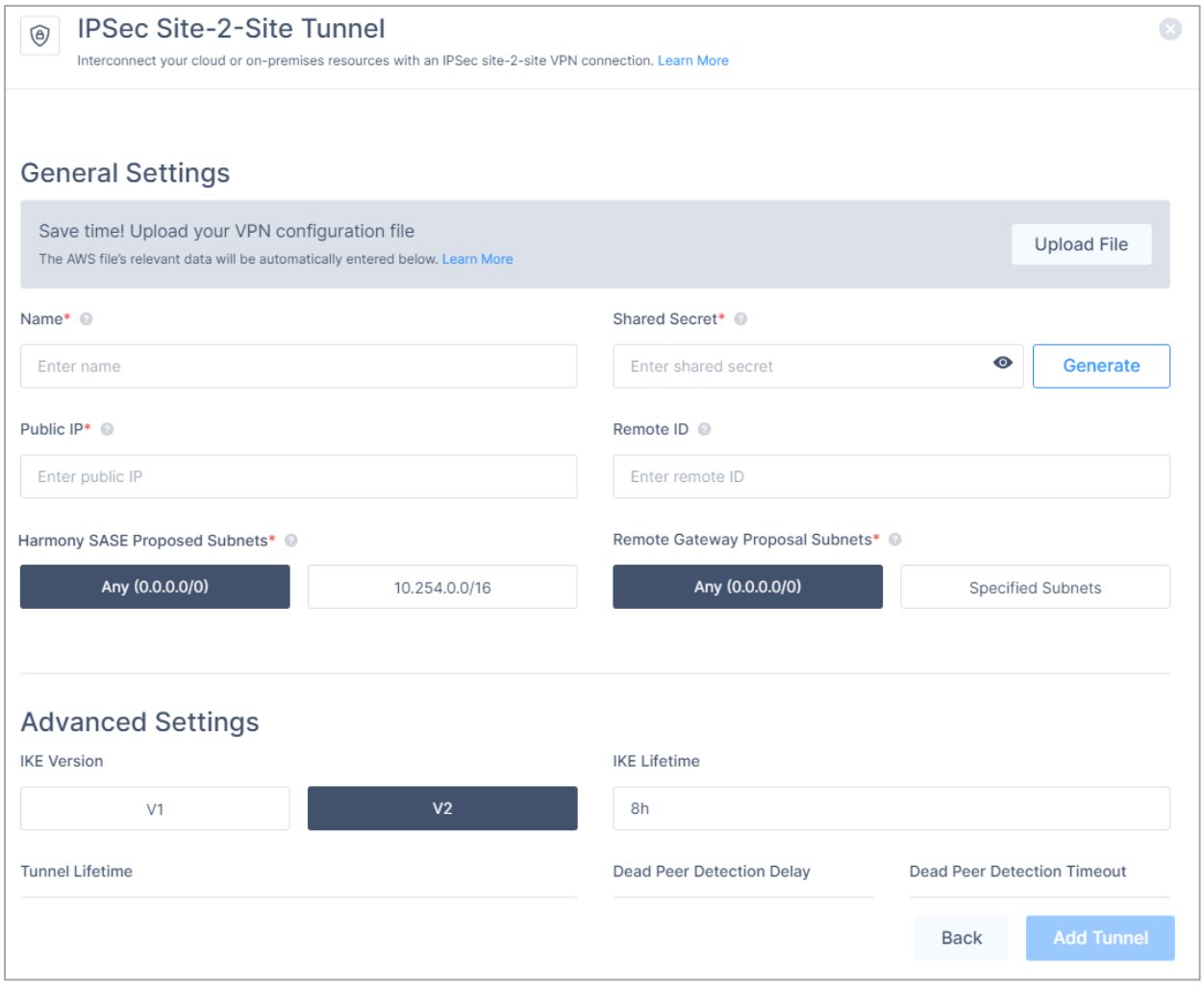
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the Azure Management Portal.
7. For manual configuration, in the **General Settings** section, enter these:
    a. **Name** - Name of the tunnel.
    b. **Shared Secret** - Shared secret you set in the Azure Management Portal.
    c. **Public IP** - Public IP address of the Azure Virtual network gateway.
    d. **Remote ID** - Remote ID of Azure Virtual network gateway.
    e. **Perimeter 81 Gateway Proposal Subnets** - Any (0.0.0.0/0).
    f. **Remote Gateway Proposal Subnets** - Any (0.0.0.0/).
8. To enter the details in **Advanced Settings** section, open the configuration file downloaded from the Azure Management Portal and refer the

    [2] IPsec/IKE parameters.

```
[2] IPsec/IKE parameters

> IKE version:          IKEv2
  + Encryption algorithm: aes-cbc-256
  + Integrity algorithm:  sha1
  + Diffie-Hellman group: 2
  + SA lifetime (seconds): 27000
  + Pre-shared key:       MyKeyIsGr8!
  + UsePolicyBasedTS:     False

> IPsec
  + Encryption algorithm: esp-gcm 256
  + Integrity algorithm:  sha1
  + PFS Group:            2
  + SA lifetime (seconds): 3600
```

9. Enter the information for your tunnel type:

Field Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

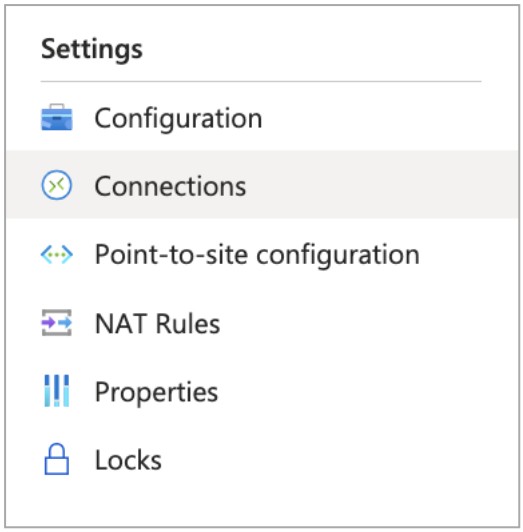
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

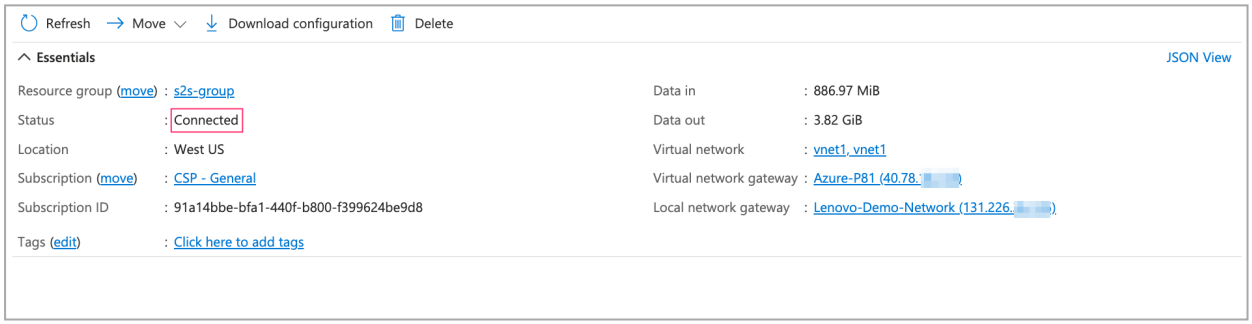
Verifying the VPN Connection in the Azure Management Portal

1. Access the Azure Management Portal and go to your **Virtual Network Gateway** page.
2. Go to **Settings** and click **Connections**.



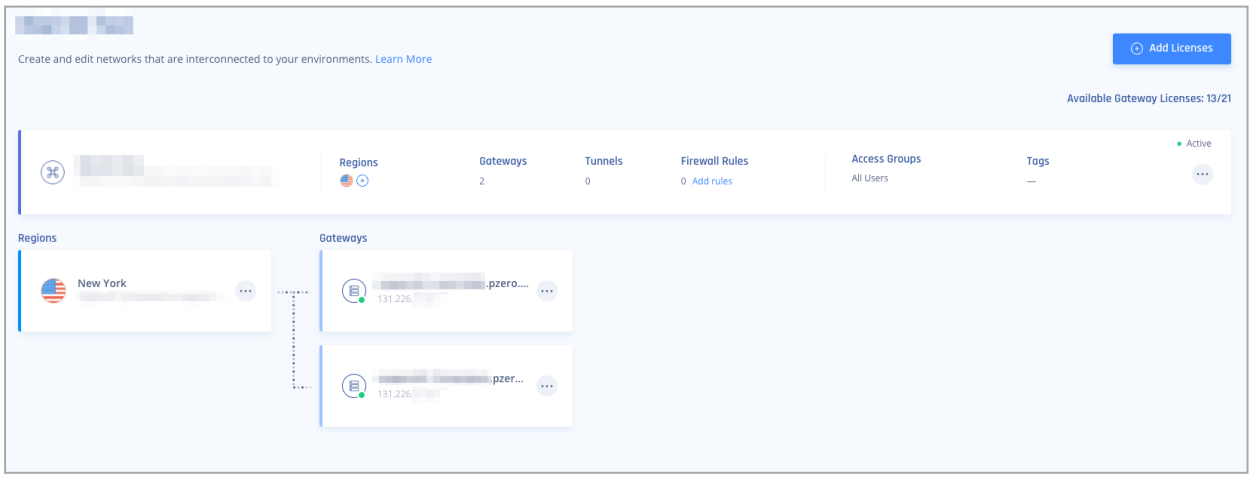
3. In the connection you created, click the **Overview** tab.

   Make sure that the **Status** is **Connected** and that there is data coming in (**Data in**) and going out (**Data out**).



Azure Virtual Network Gateway Redundant Tunnels

- Your Check Point SASE network must have at least two different gateways in the same network.



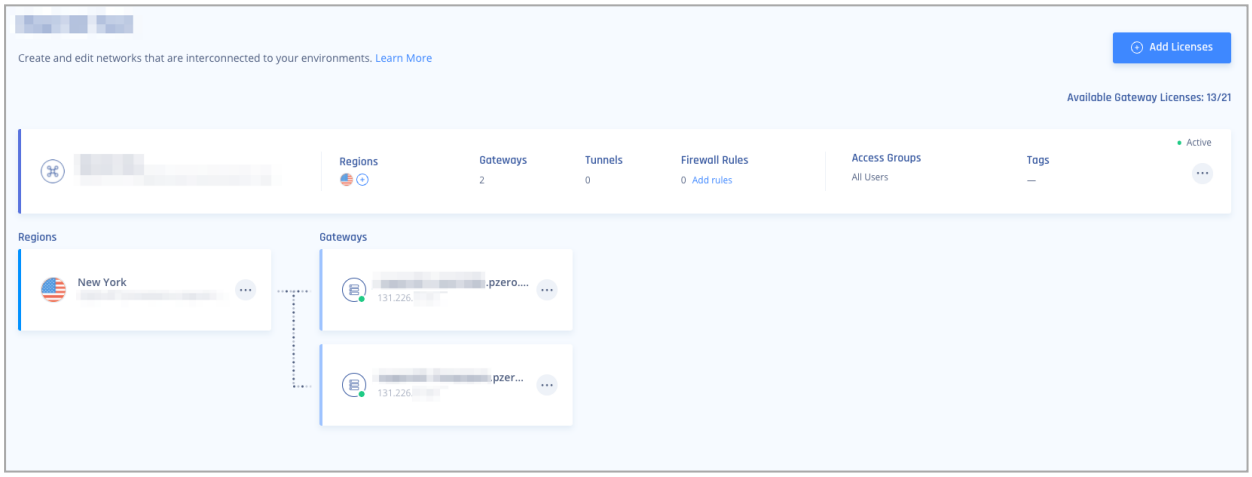
Notes -

- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Azure Redundant Tunnels - Virtual Network Gateway

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.
- Your Check Point SASE network must have at least two different gateways in the same network.

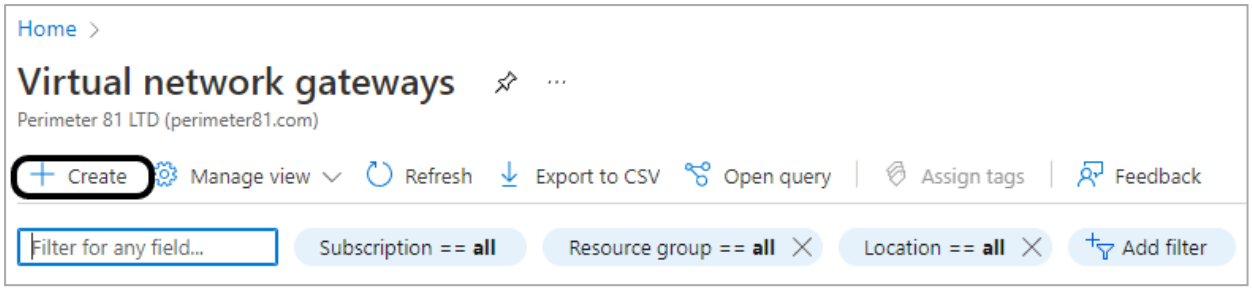


Notes -

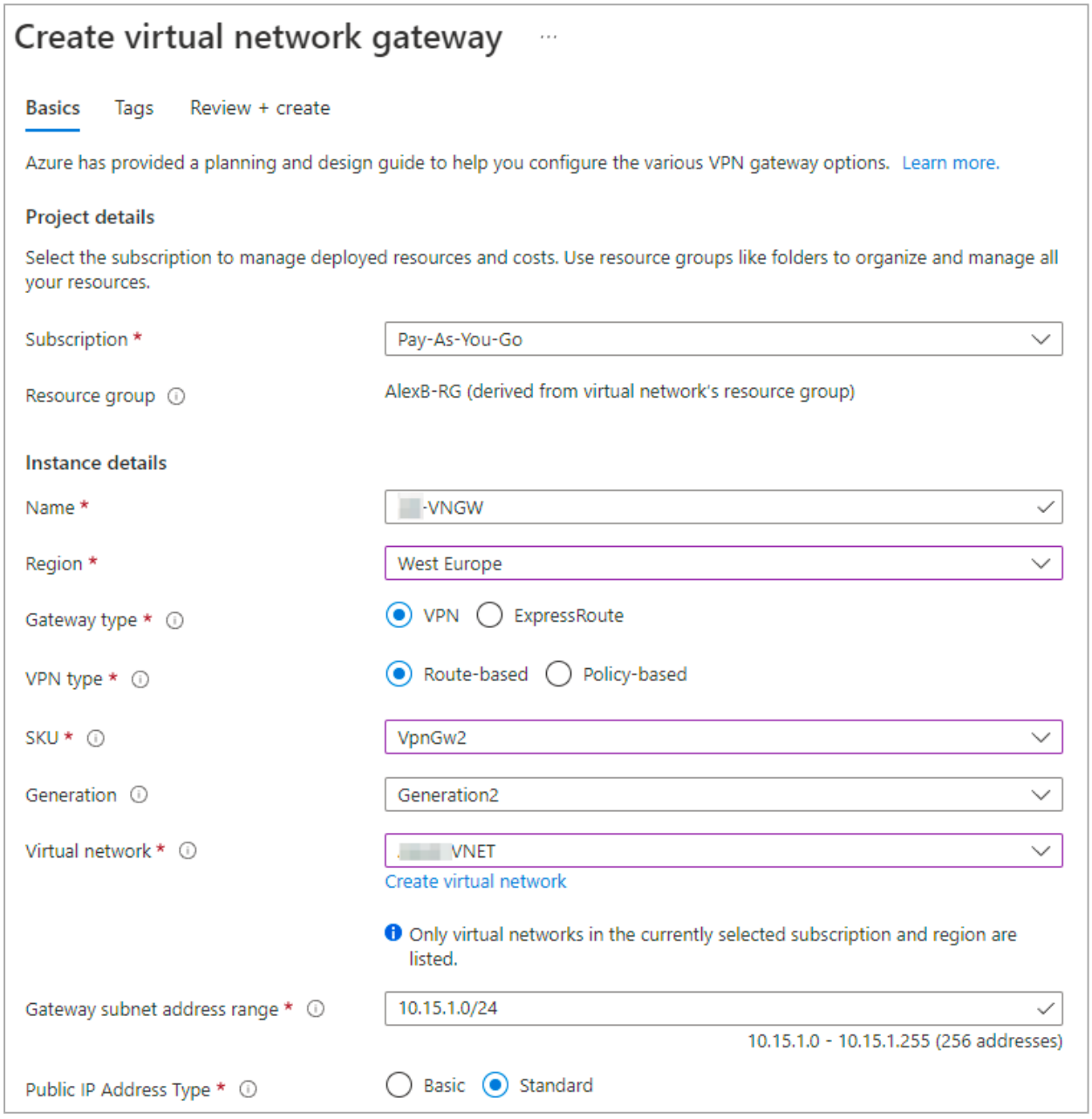
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the Azure Management Portal

1. Access the Azure Management Portal and go to **Virtual network gateways**.
2. Click **+Create**.



The **Create virtual network gateway** window appears.



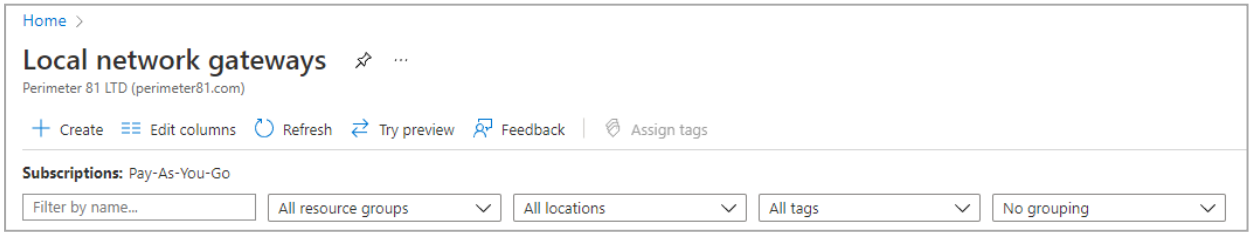
3. Enter these:

Item	Value
Name	Name of the gateway.
Region	Region where your resources are located.
Gateway type	VPN
VPN type	Route-Based
SKU	Select based on your preference and requirements.
Virtual network	Select the relevant VNET.
Gateway subnet address range	(If not filled automatically) Address range reserved for your Azure gateway.
Public IP address	Create new or select existing.
Enable active-active mode	Enabled
Second Public IP Address	Create new or select existing.
Configure BGP	Enabled
ASN	Leave default or configure based on your preference.
Custom Azure APIPA BGP IP address	Leave as empty.

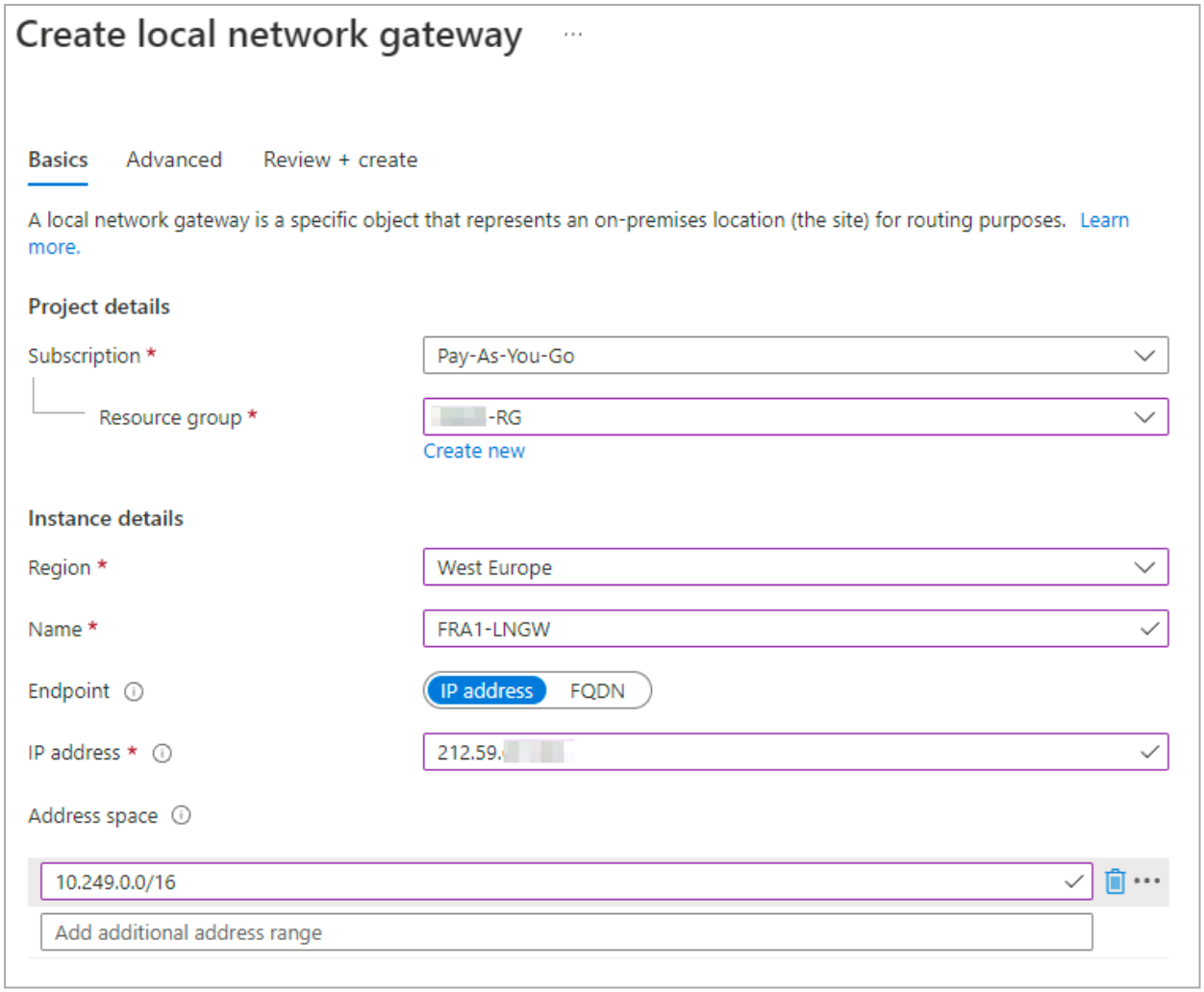
Creating Local Network Gateways

You must create two local network gateways, one for each of your SASE gateways.

1. Access the Azure Management Portal and go to **Local network gateways**.
2. Click **+Create**.



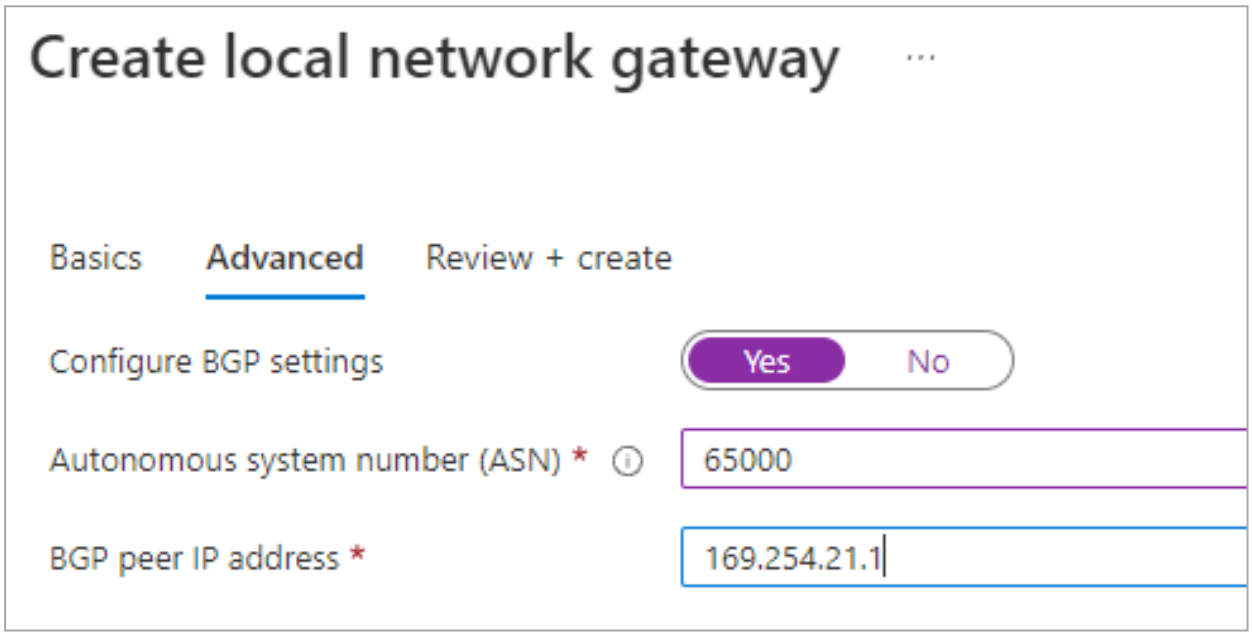
The **Create local network gateway** window appears.



3. Enter these:

Item	Value
Basics tab	
Resource group	Select the relevant resource group.
Region	Region where your resources are located.
Name	Name of the gateway.
Endpoint	IP address
IP address	Public IP address of the gateway in the Check Point SASE Administrator Portal.
Address Space	Subnet value of the network in the Check Point SASE Administrator Portal.

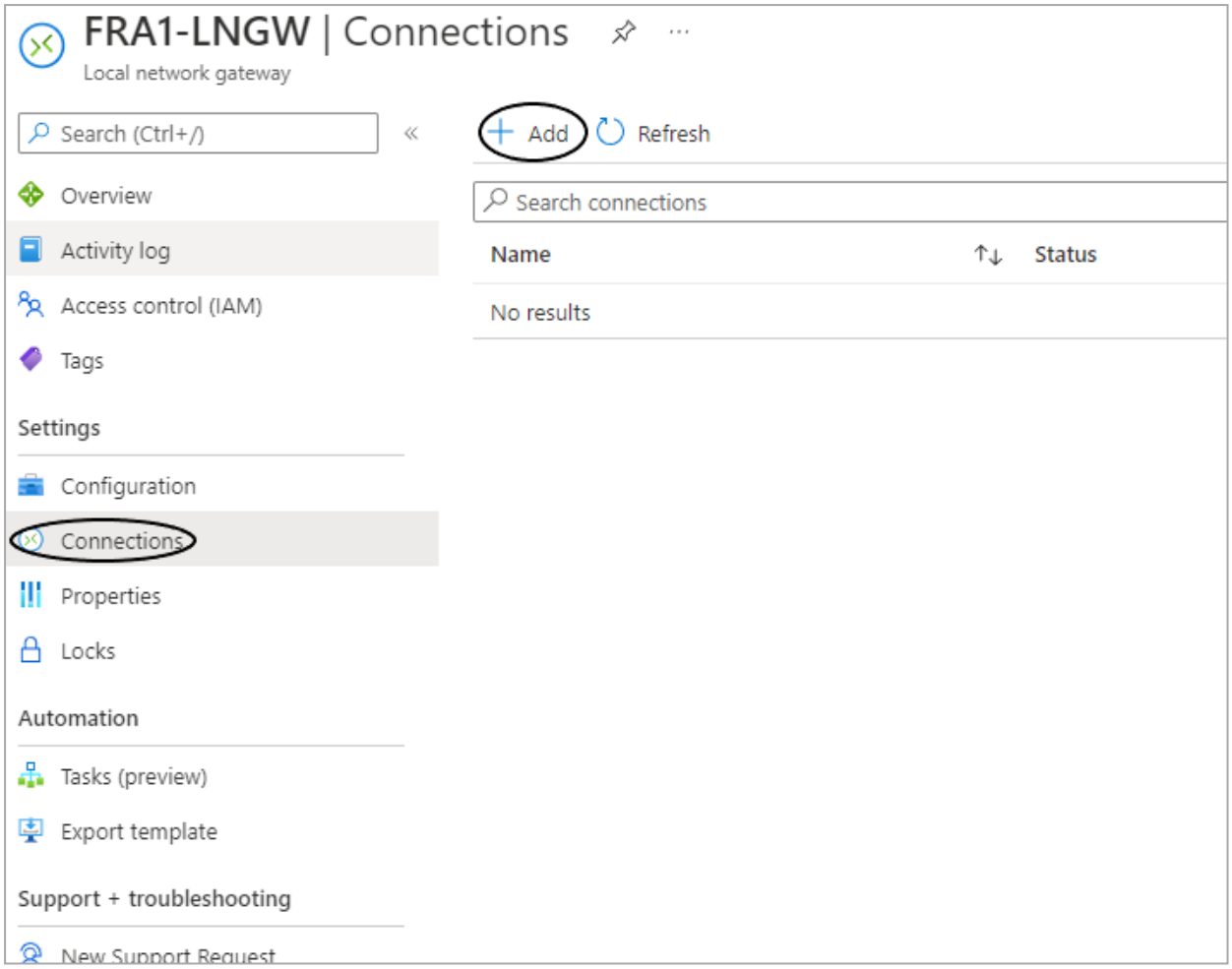
Item	Value
Advanced tab	
Configure BGP settings	Yes
ASN	Leave default or select a value from the permitted range.
BGP peer IP address	Any address from the permitted range.



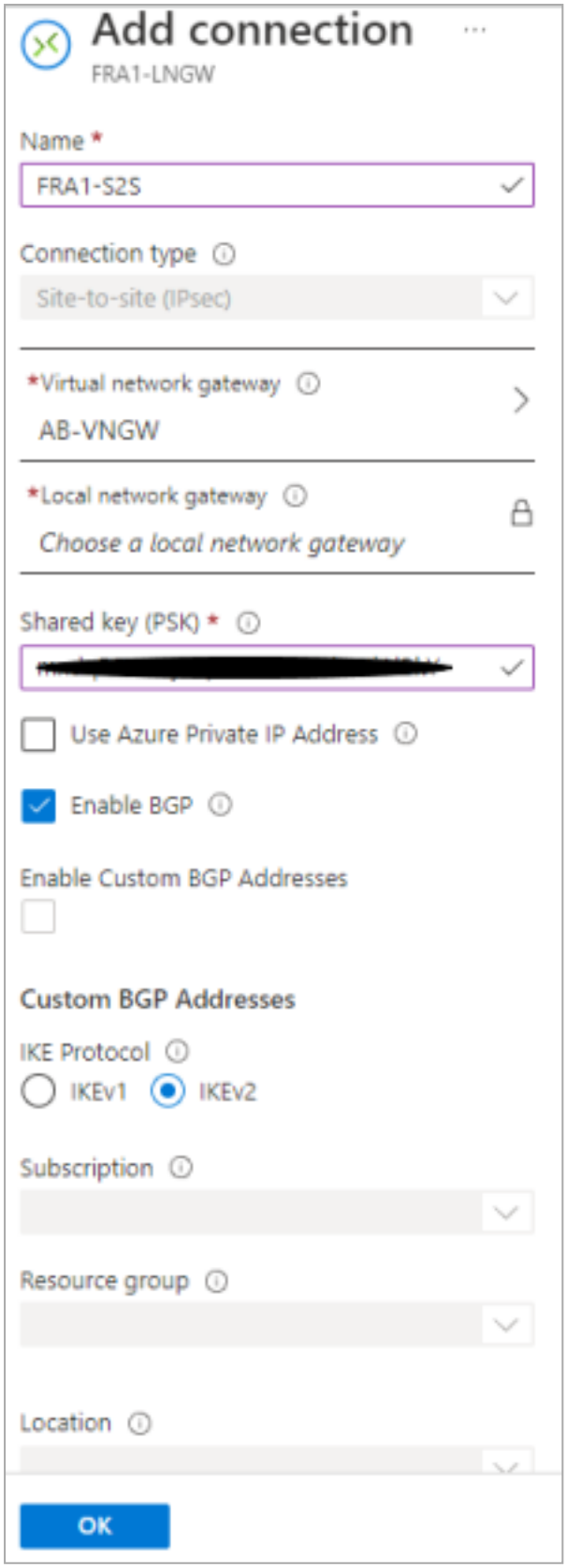
4. Repeat the above steps to create the second local network gateway.

Creating a Connection

1. Access the Azure Management Portal and go to your local network gateway and click **Connections**.
2. Click **+Add**.



The **Add connection** window appears.

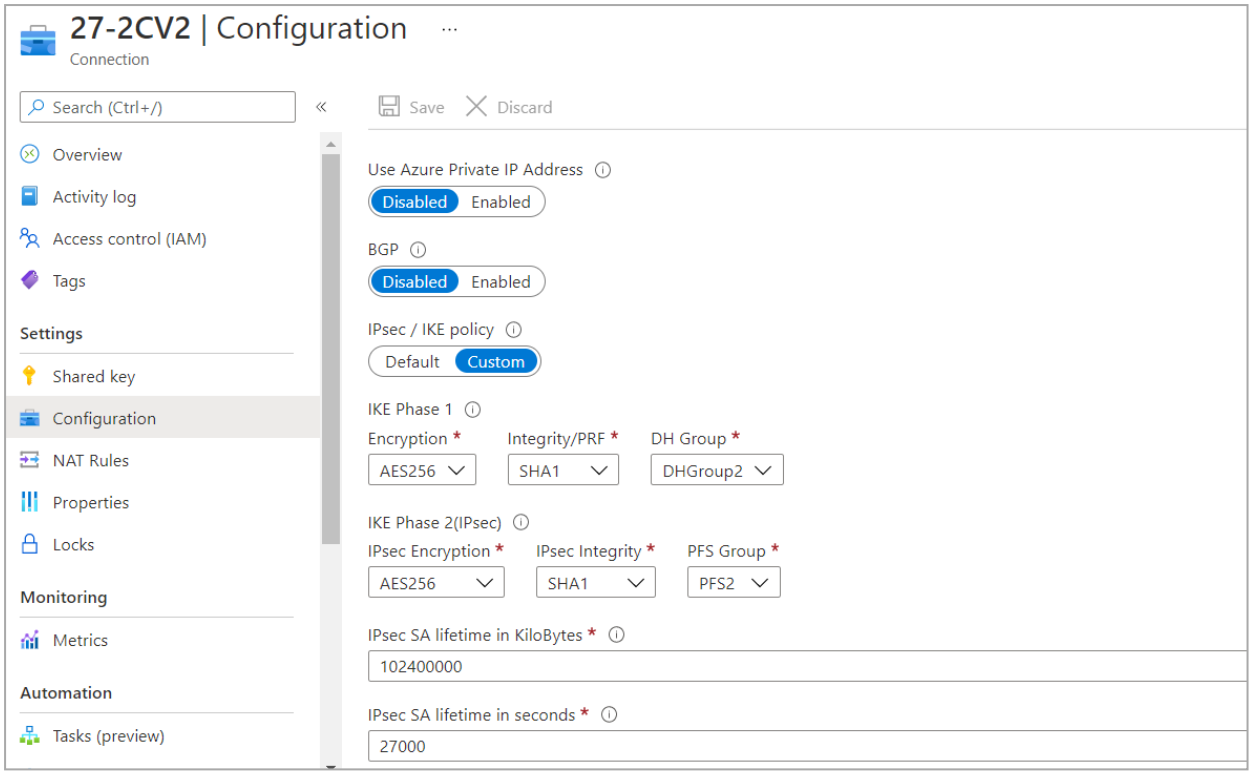


3. Enter these:

Item	Value
Name	Name of the connection.
Virtual Private Gateway	Select the first Virtual Private Gateway you created.
Local network gateway	Field is locked for editing.
Shared key (PSK)	Generate a key on the Check Point SASE side, or on a different PSK generating application. The key must only contain numbers, letters, underscore (_) and period (.).
Use Azure Private IP Address	Leave as cleared.
Enable BGP	Select the checkbox.
IKE Protocol	IKEv2

4. Click **OK**.
5. Open the connection you just created and click **Configuration**.

   The **Configuration** window appears.

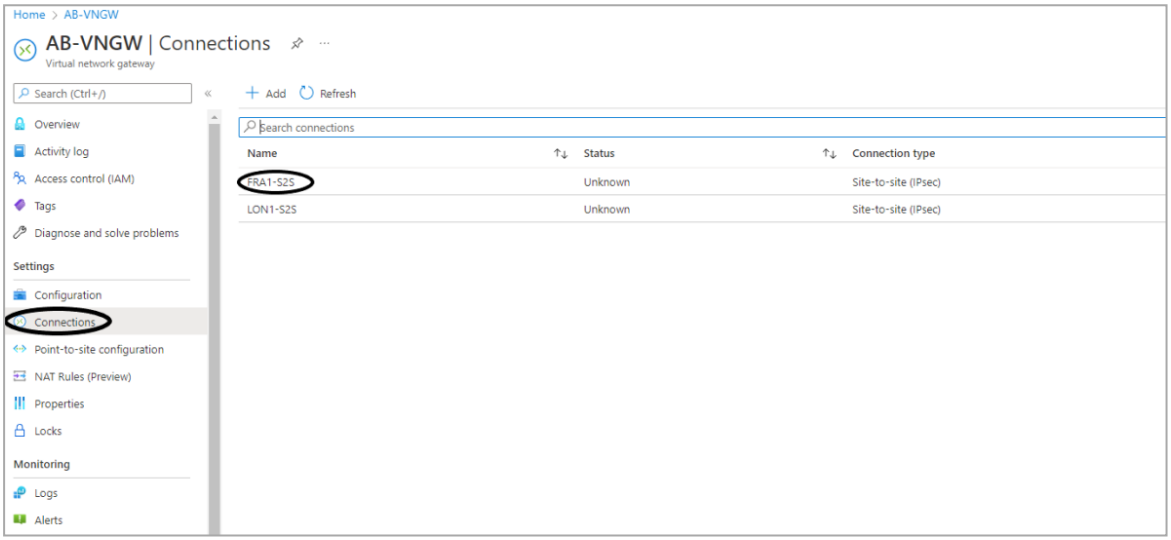


6. In the **IPsec / IKE policy** field, select **Custom** and enter these (same values are set for the tunnel in the Check Point SASE Administrator Portal:

Item	Value
Encryption	AES256
Integrity/ PRF	SHA1
DH Group	DHGroup2
IPsec Encryption	AES256
IPsec Integrity	SHA1
PFS Group	PFS2
IPsec SA lifetime in KiloBytes	102400000

Item	Value
IPsec SA lifetime in seconds	27000

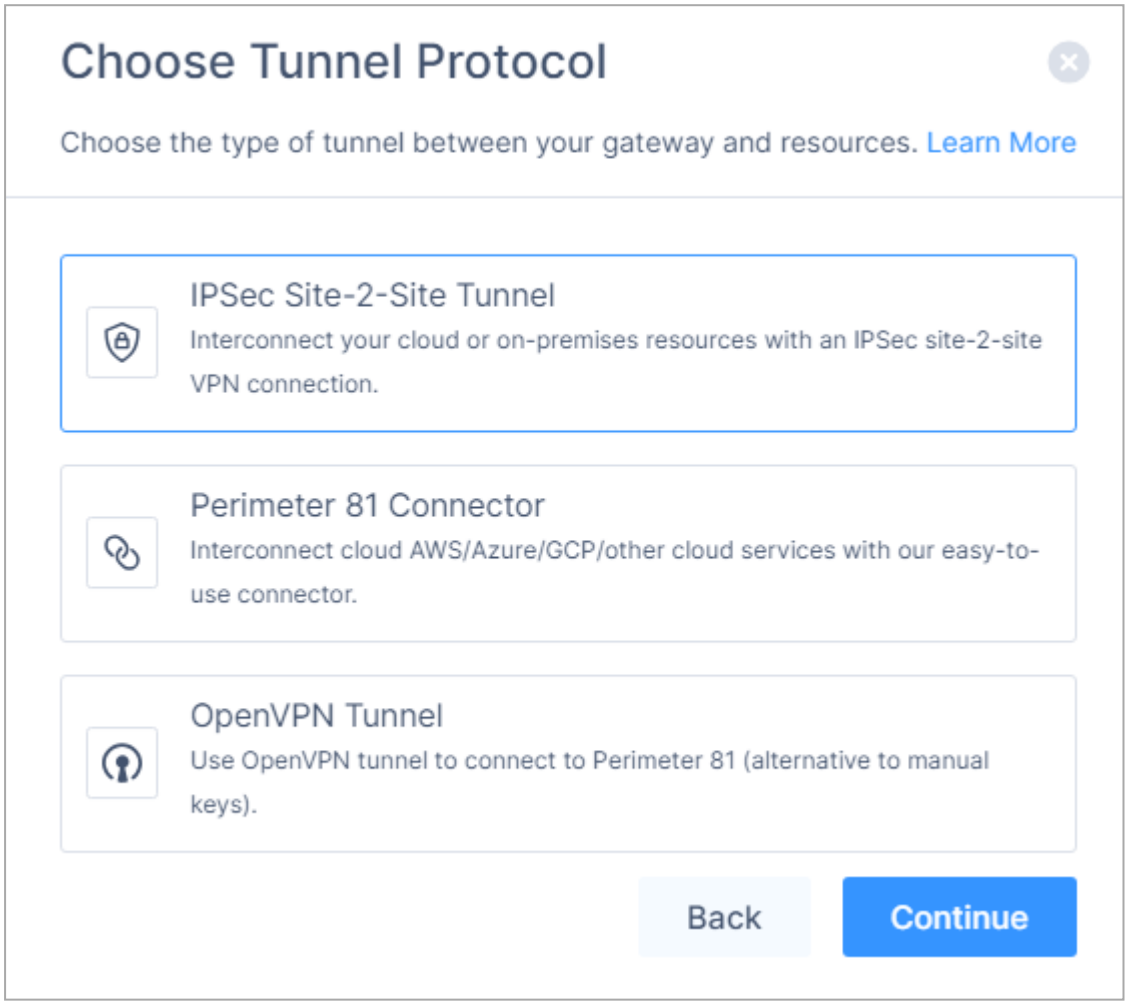
7. Repeat the above steps to create a connection for the second local network gateway.
8. Download the tunnel configuration for the first connection:
   a. Go to your **Virtual network gateway** > **Settings** > **Connections** and click on your first connection.



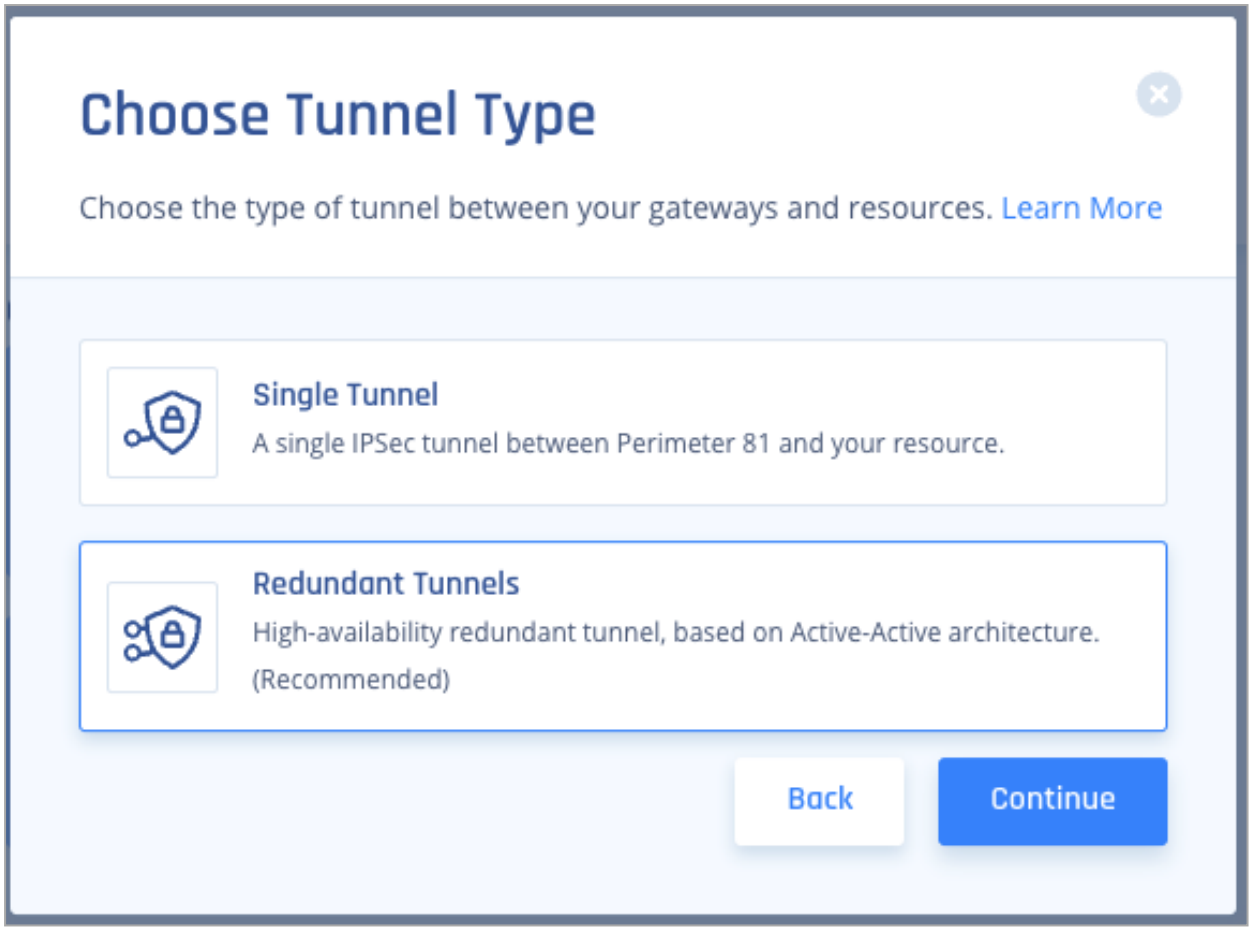
   b. Click **Download configurations**.
   c. Enter these:
      i. **Device vendor** - Generic Samples
      ii. **Device family** - Device Parameters
      iii. **Firmware version** - 1.0
   d. Click **Download configuration**.

Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal

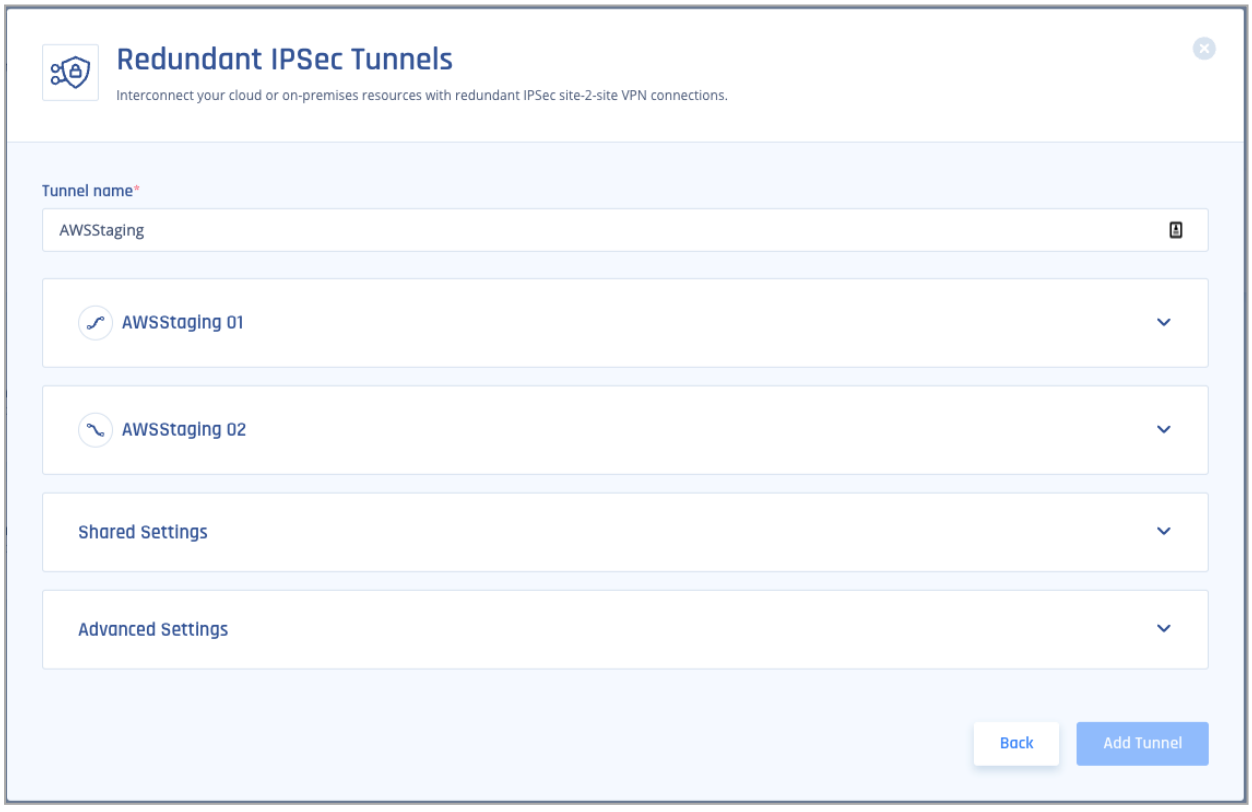
1. Access the Check Point SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



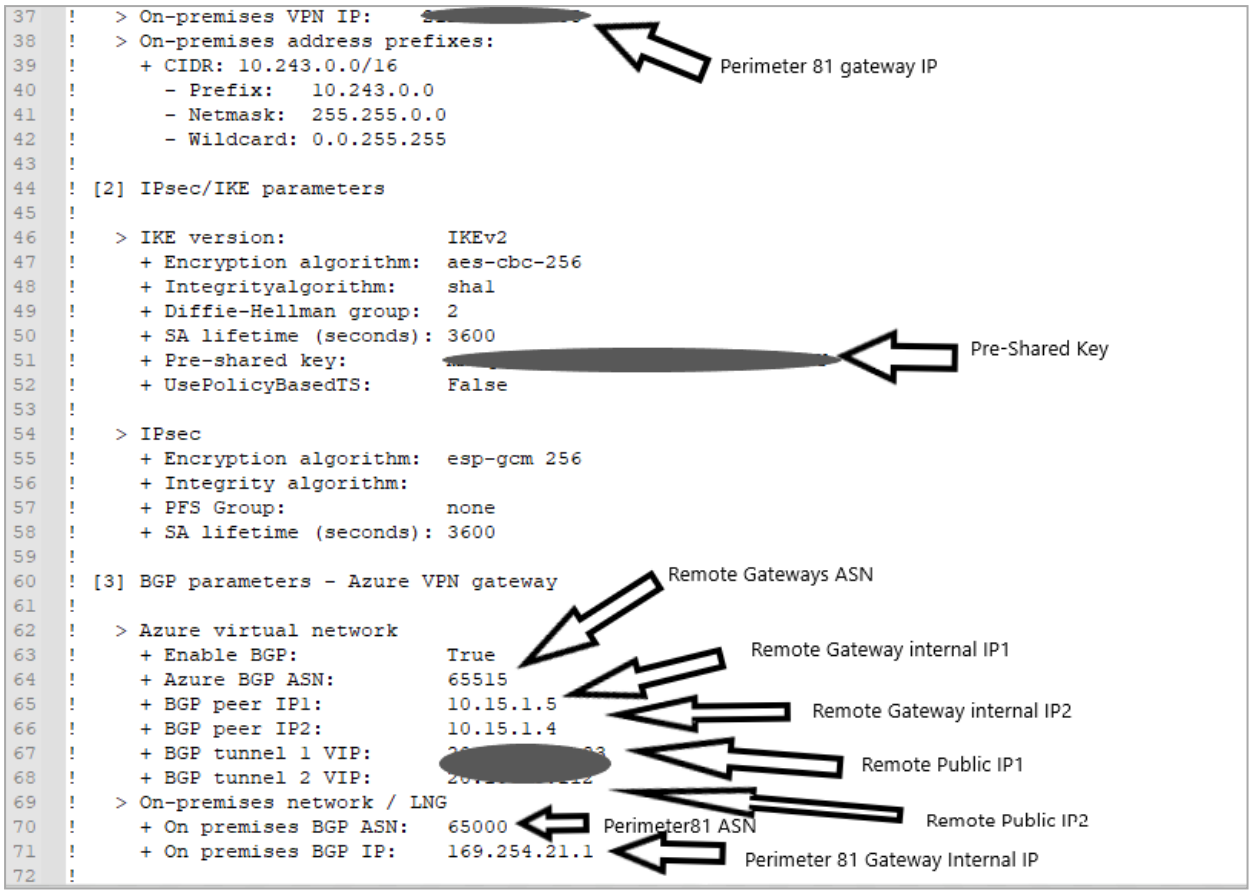
5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.

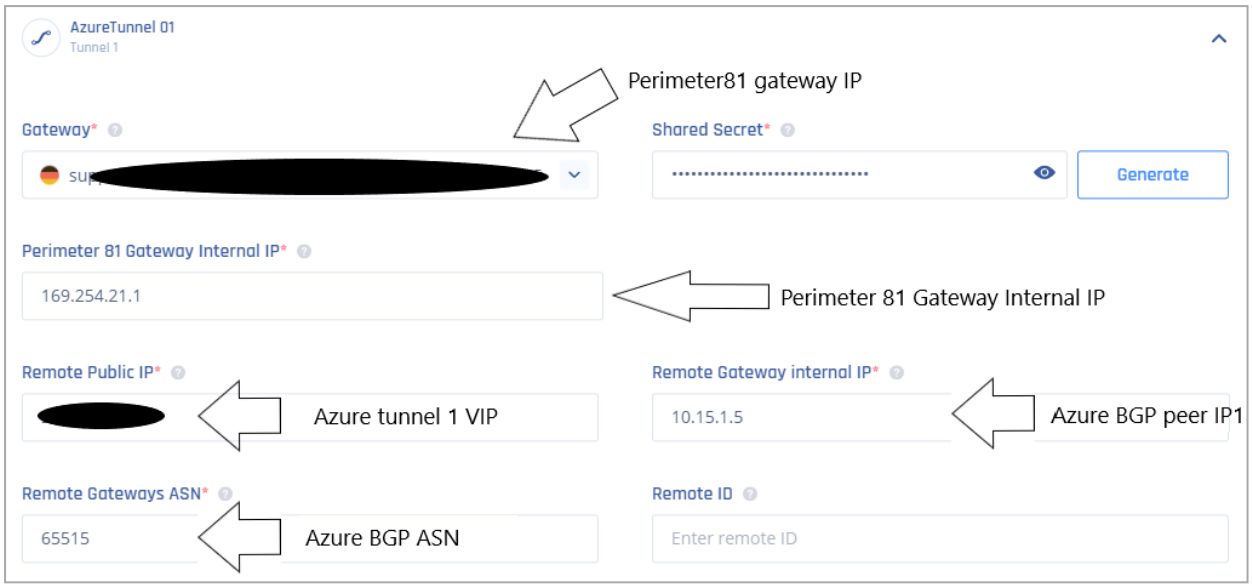


6. Copy the values for the first tunnel from the downloaded configuration file:

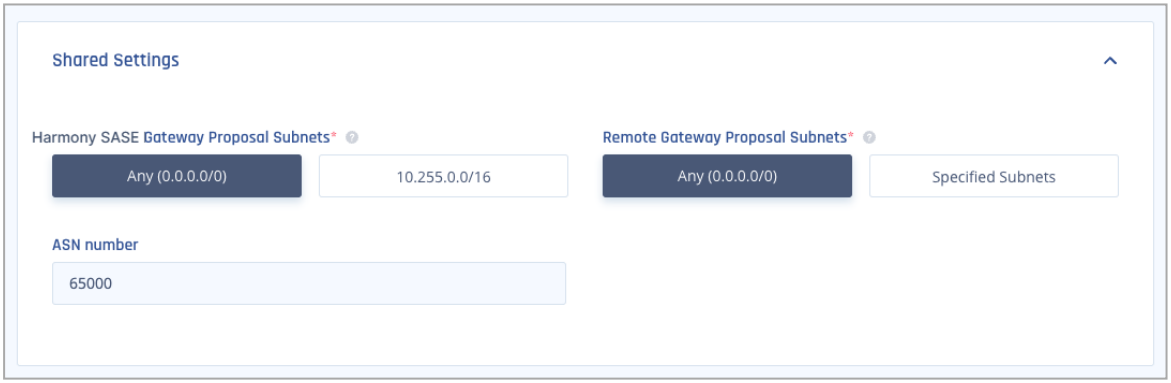


Item	Value
Shared Secret	Pre-Shared Key
Check Point SASE gateway Internal IP	Inside IP Addresses of Customer Gateway
Remote Public IP & Remote ID	Outside IP Addresses of Virtual Private Gateway
Remote Gateway internal IP	Inside IP Addresses of Virtual Private Gateway
Remote Gateway ASN	BGP Configuration Options of Virtual Private Gateway ASN

In the Check Point SASE Administrator Portal, enter the values for Tunnel 1 as:



7. Repeat step 6 for the second tunnel.
8. In the **Shared Settings** section:
   a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.
   b. **ASN** number must be the same for the Check Point SASE side.



9. In the **Advanced Settings** section, enter the information for your tunnel type (unless you have configured customer settings on the Azure side):

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

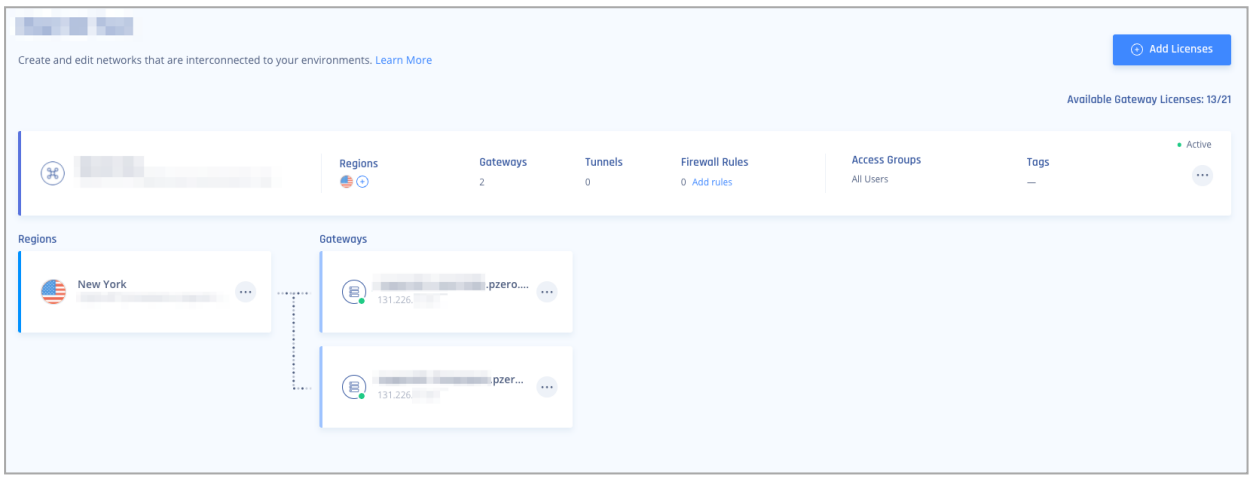
[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

Azure Virtual WAN Redundant Tunnels

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.
- Your Check Point SASE network must have at least two different gateways in the same network.



Notes -

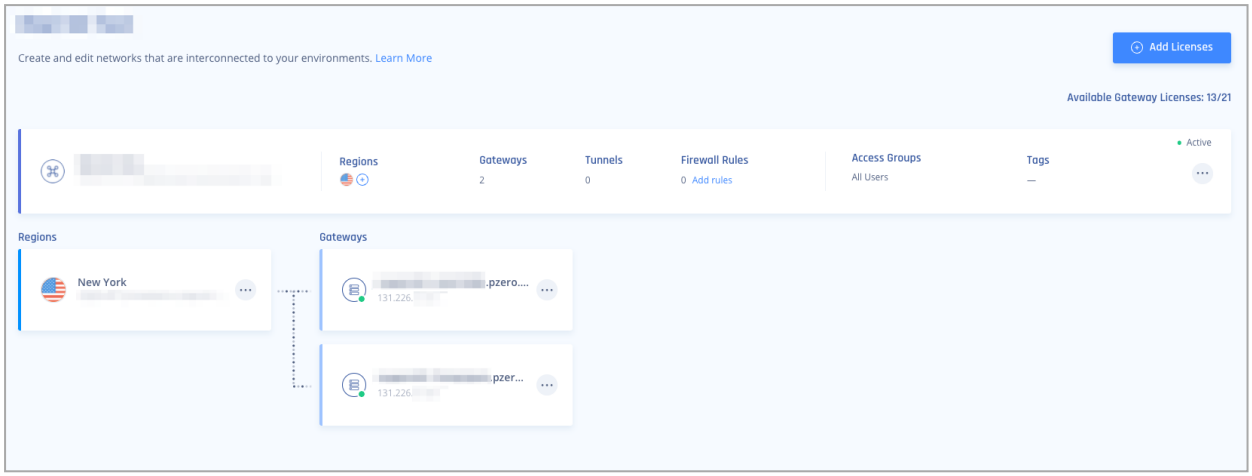
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Azure Redundant Tunnels - Virtual WAN

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Check Point SASE network must have at least two different gateways in the same network.

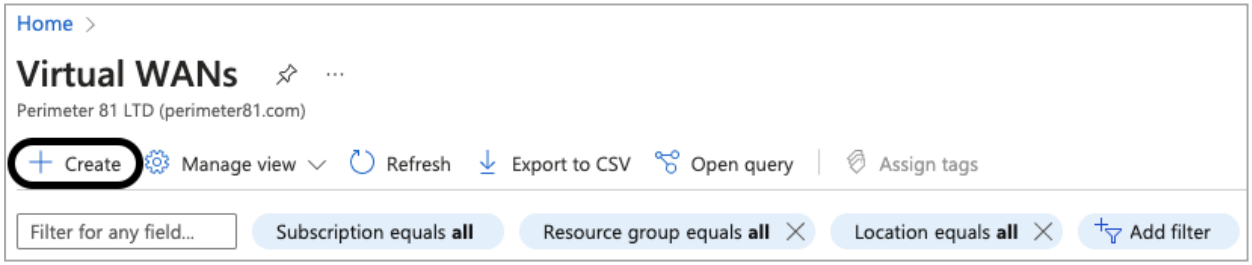


Notes -

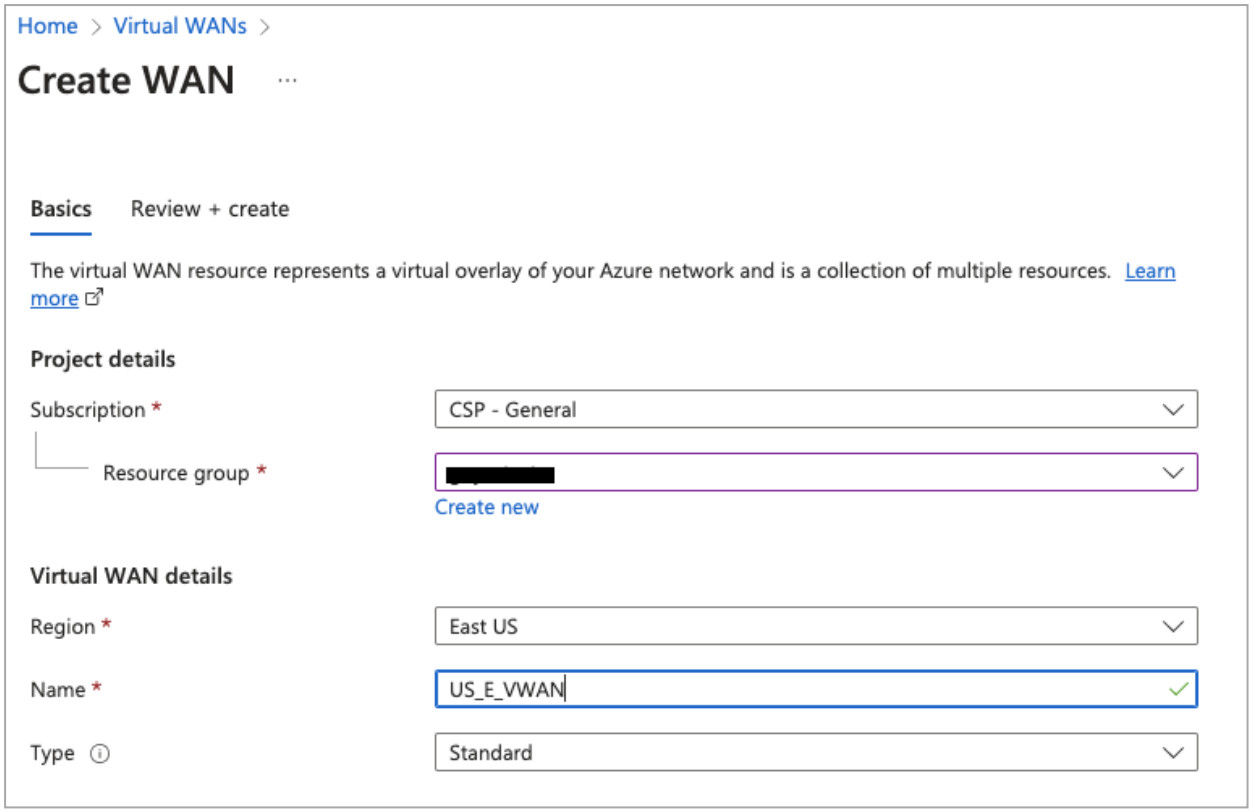
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the Azure Management Portal

1. Access the Azure Management Portal and go to **Virtual WANs** and click **+Create**.



The **Create WAN** window appears.



2. In the **Basics** tab, enter these:

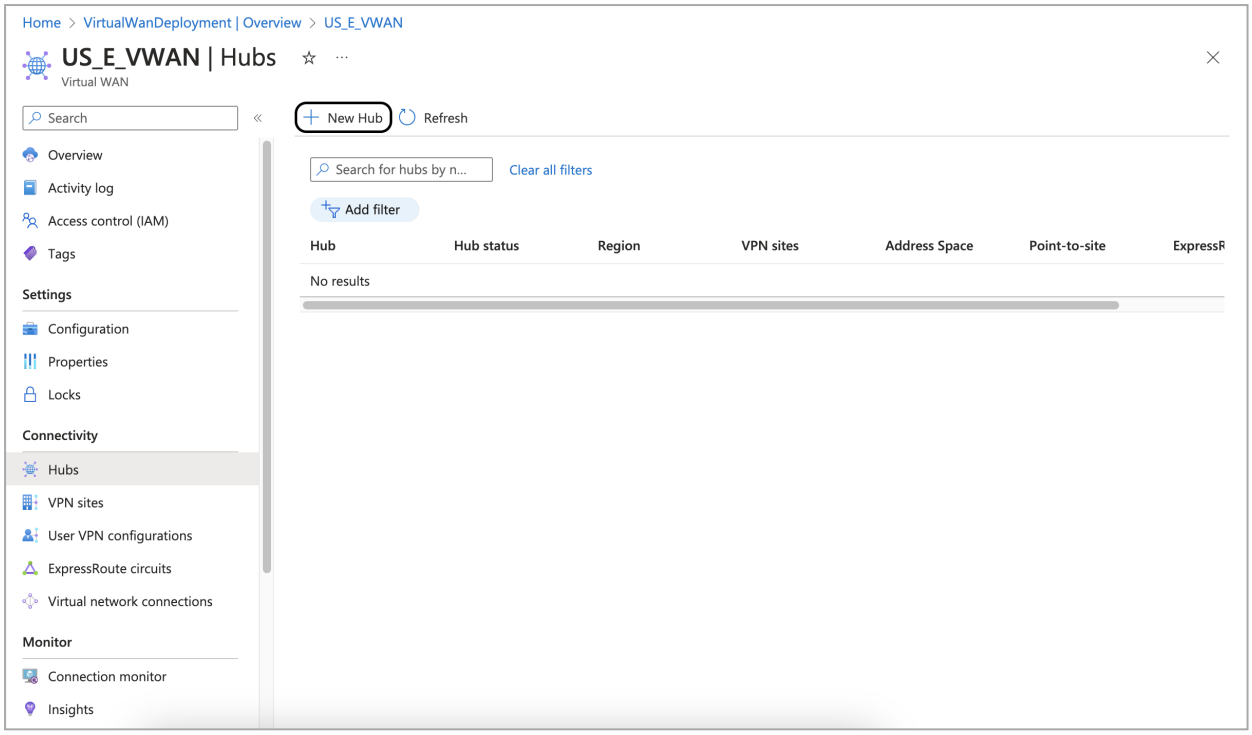
Item	Value
Subscription	Select the relevant subscription and resource group.
Region	Region where your resources are located.
Name	Name of the virtual WAN.
Type	Standard

3. Click **Review+create**.
4. Click **Create**.

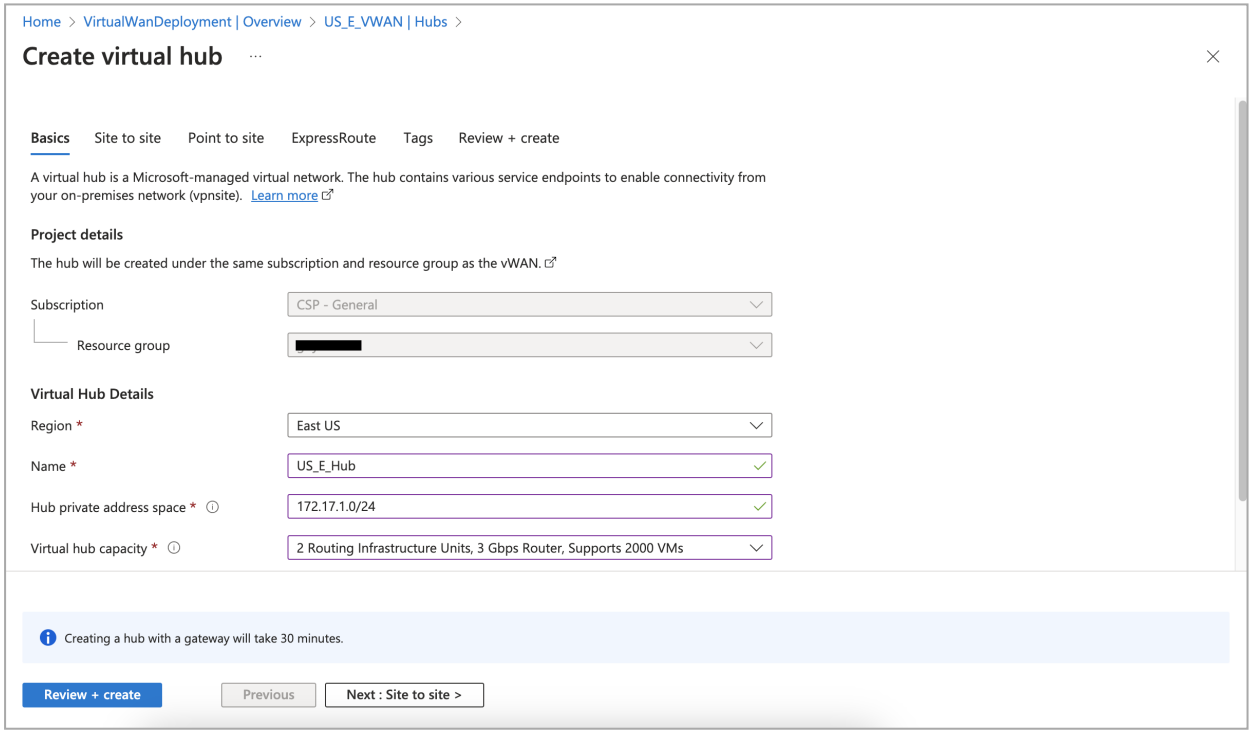
Creating a Virtual Hub

Note - If you already have a virtual hub in your Azure region, skip this step.

1. Access the Azure Management Portal and go to the Virtual WAN you created and from the left pane, click **Hubs** > **+New Hub**.



The **Create virtual hub** window appears.



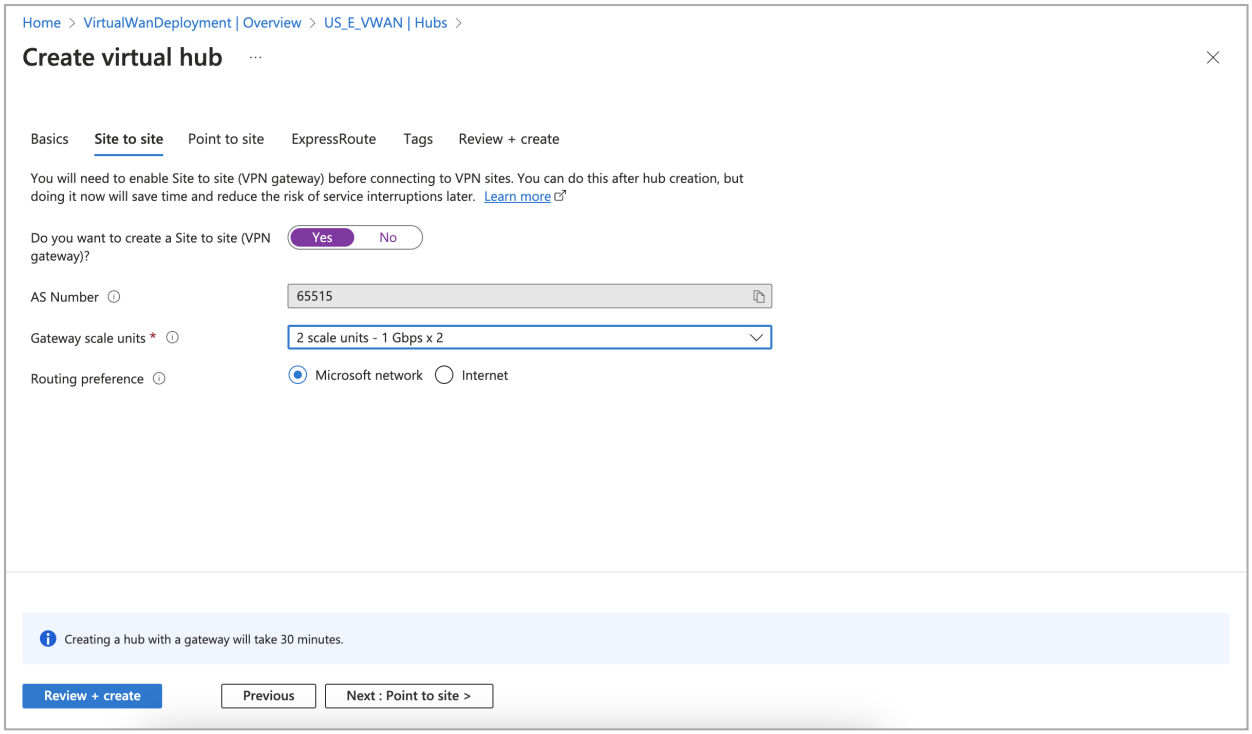
2. In the **Basics** tab, enter these:

Item	Value
Region	Region where your resources are located.

Item	Value
Name	Name of the virtual hub.
Endpoint	IP Address
Hub private address space	Select a CIDR range that does not overlap with any existing CIDR (/24 range is the minimal one).
Address Space	Subnet value of the network in the Check Point SASEAdministrator Portal.
Virtual hub capacity	Select a value according to the maximum number of VMs to be connected through this hub.

3. In the **Site to site** tab, enter these:

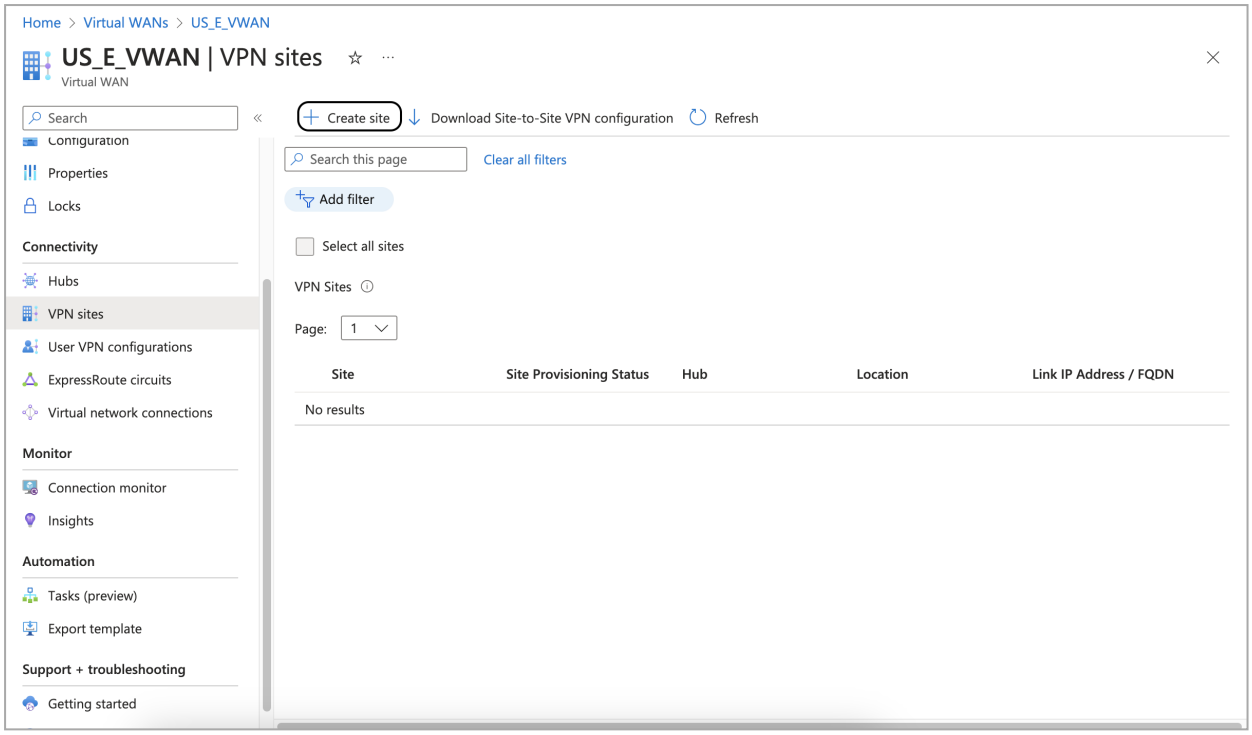
Item	Value
Create a Site to site (VPN gateway)	Yes
Gateway scale units	Select the required value from the list.
Routing preference	Microsoft network



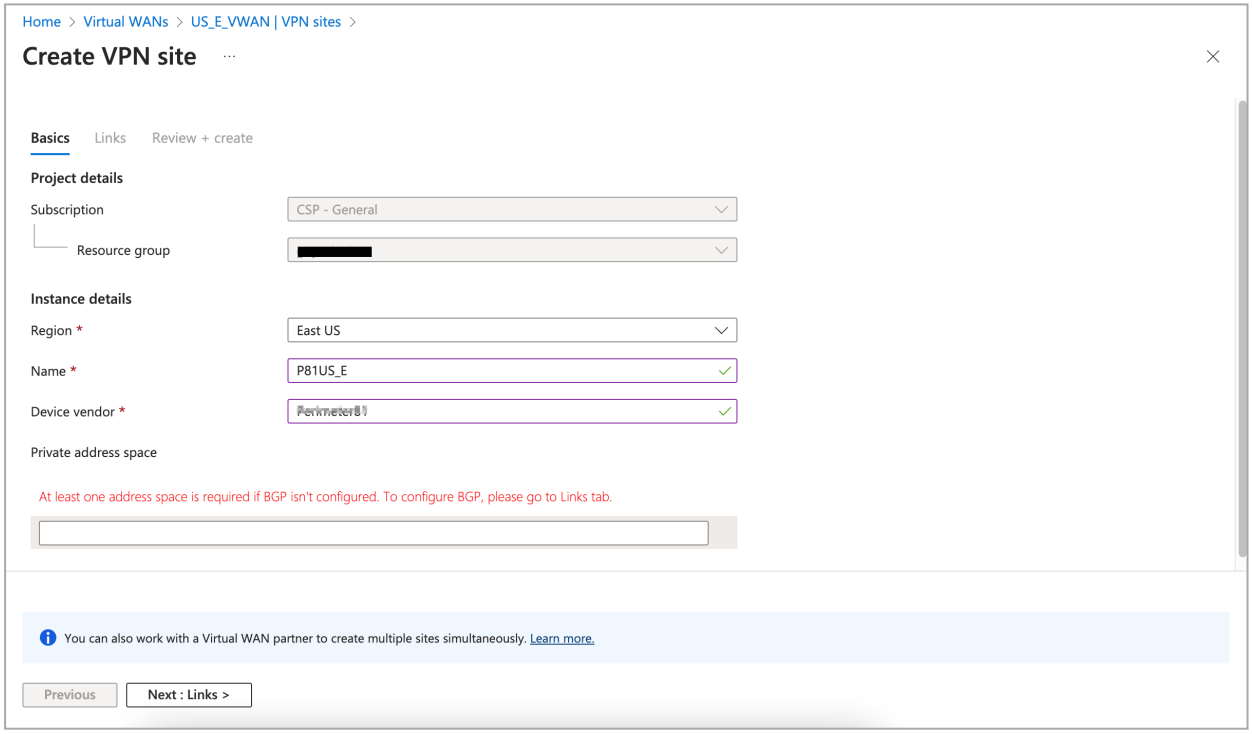
4. Click **Review+create**.
5. Click **Create**.

Creating a Site

1. Access the Azure Management Portal and go to the Virtual WAN you created, and from the left pane, select **VPN sites**.
2. Click **+Create site**.



The **Create VPN site** window appears.



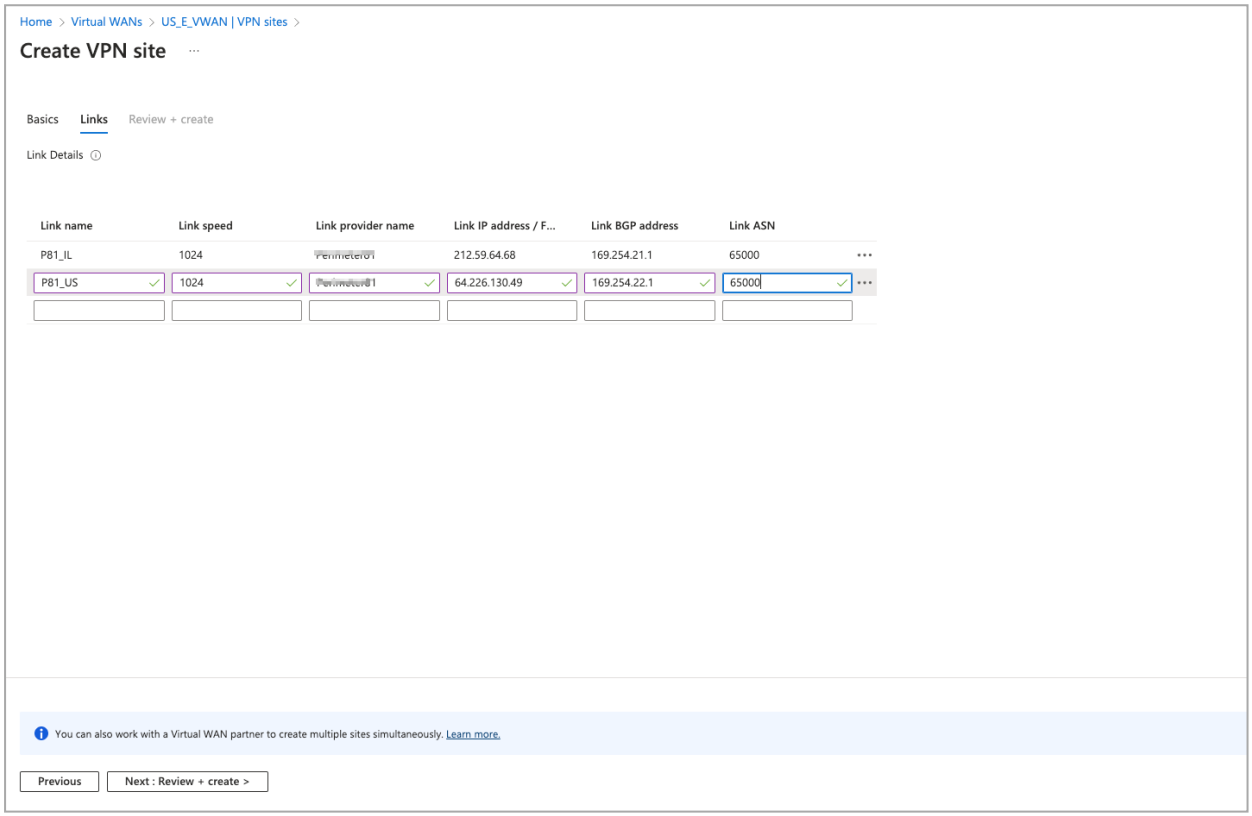
3. In the **Basics** tab, enter these:

Item	Value
Region	Region where your resources are located.

Item	Value
Name	Name of the VPN site.
Device vendor	Check Point SASE
Private address space	Leave as empty.

4. Click **Next:Links**.

   The **Links** tab appears.

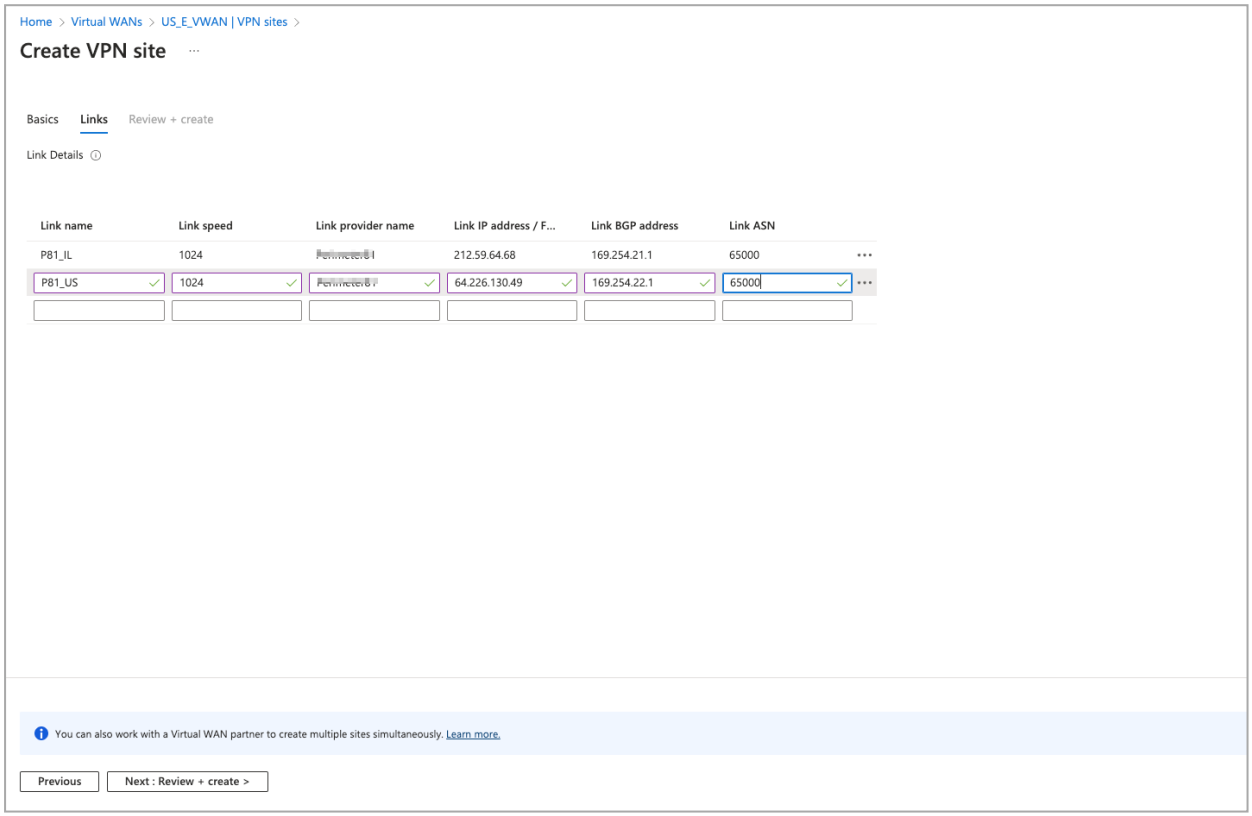


5. Enter these:

Item	Value
Link name	Name of the link that connects to the first Check Point SASE gateway.
Link speed	1024
Link provider name	Check Point SASE
Link IP address	IP address of the first Check Point SASE gateway.

Item	Value
Link BGP address	Any address in the permitted range.
Link ASN	ASN for your Check Point SASE network.

6. Repeat the above step to link the second Check Point SASE gateway.

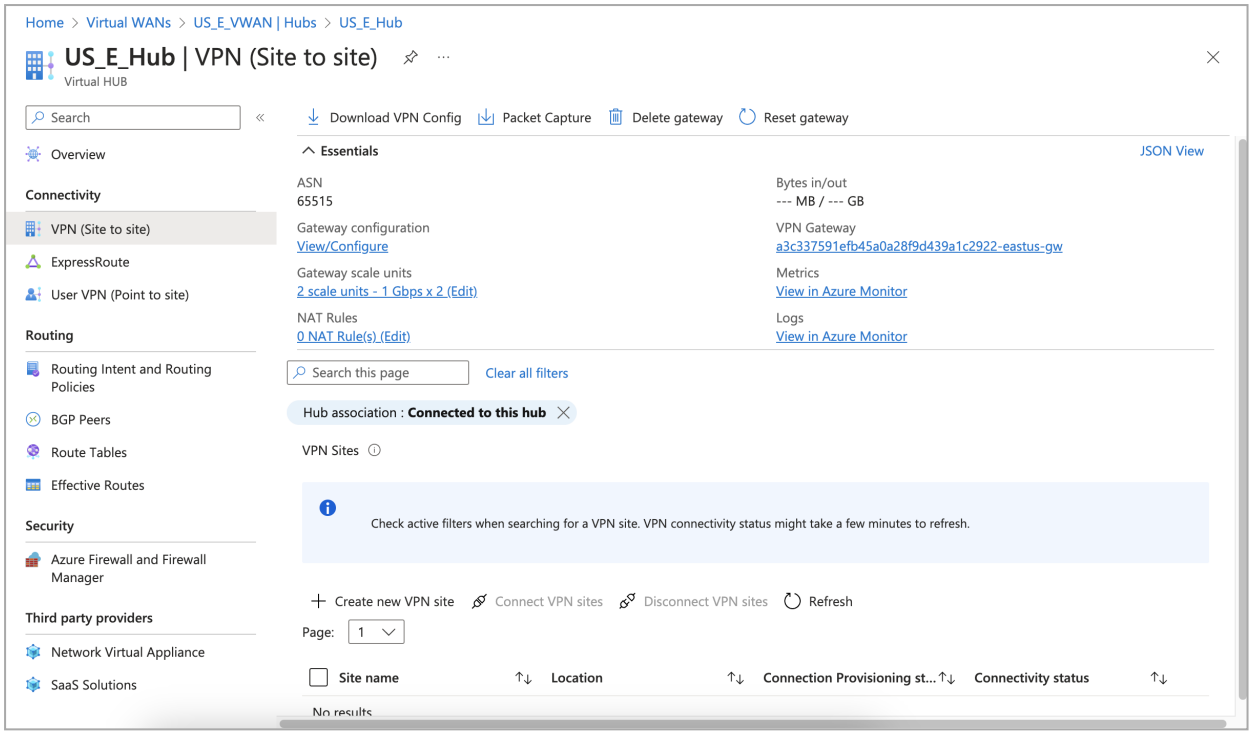


7. Click **Review+create**.
8. Click **Create**.

Connecting the Site to your Virtual Hub

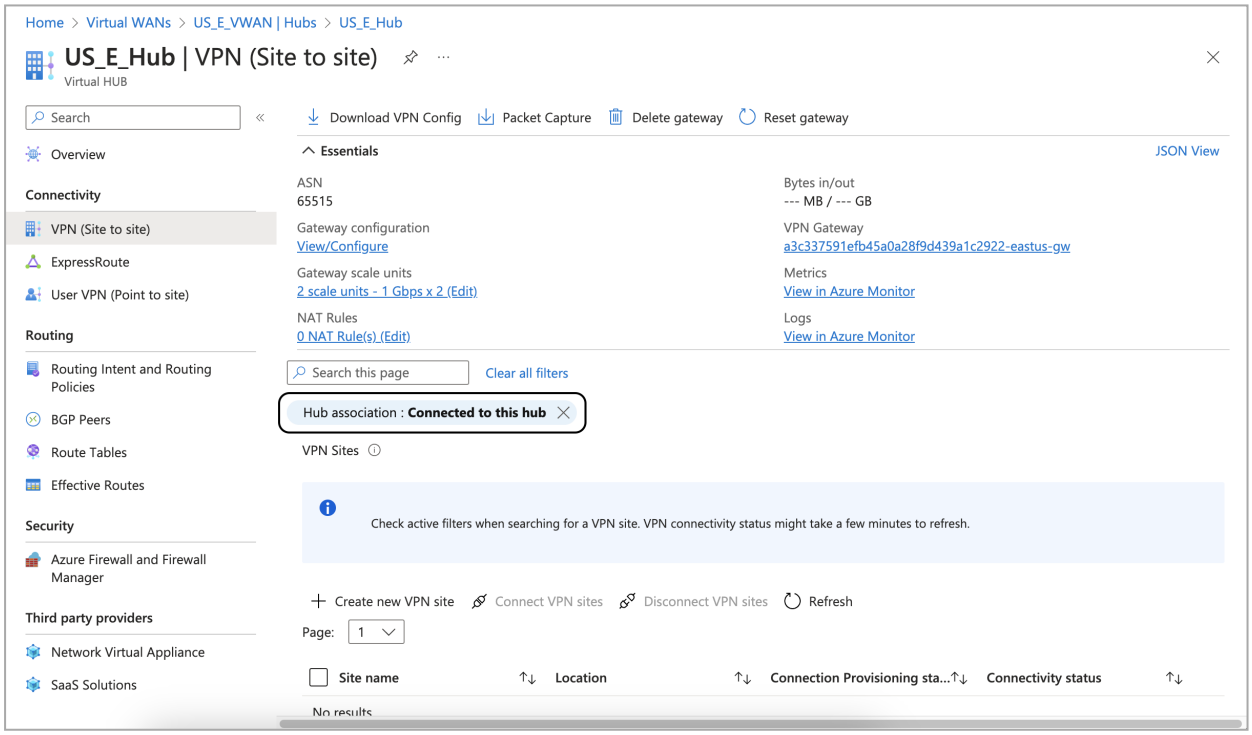
1. Access the Azure Management Portal and go to the Virtual WAN you created, and from the left pane, click **Hubs**.
2. Click the virtual hub you created.

   The **Hub** page appears.
3. From the left pane, in the **Connectivity** section, click **VPN (Site to site)**.

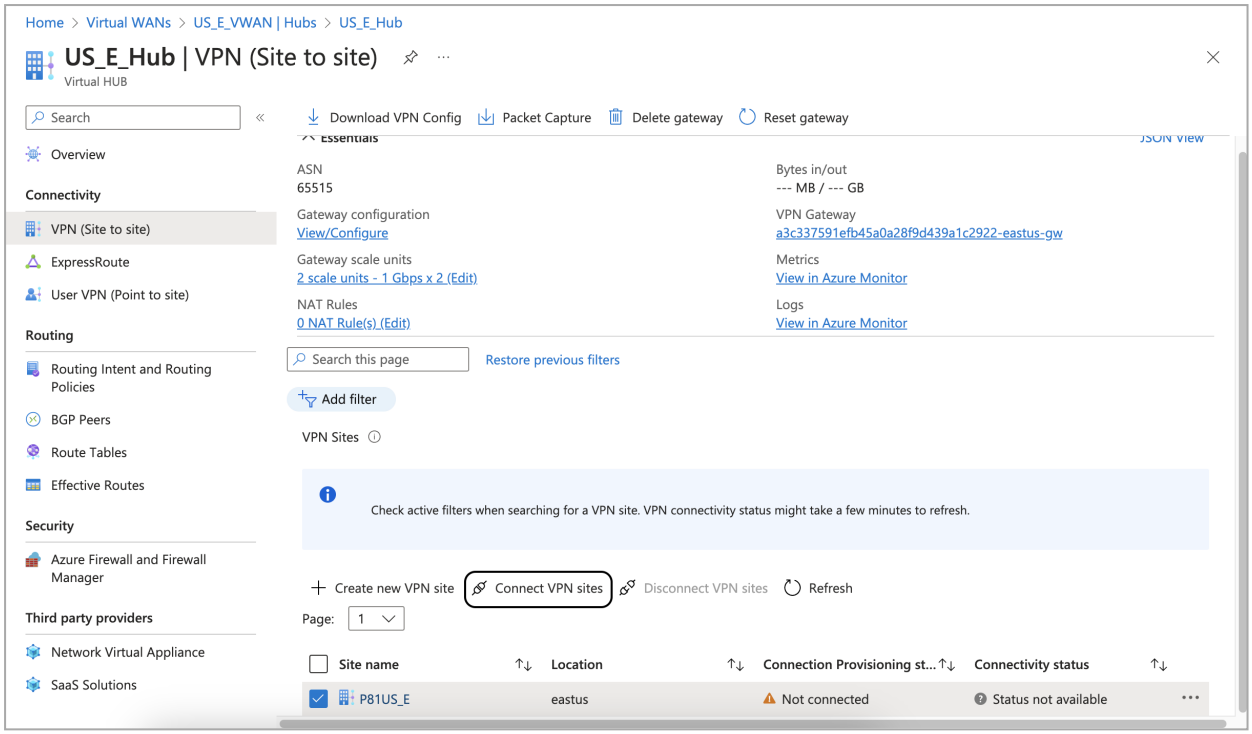


The **VPN (Site to site)** page appears.

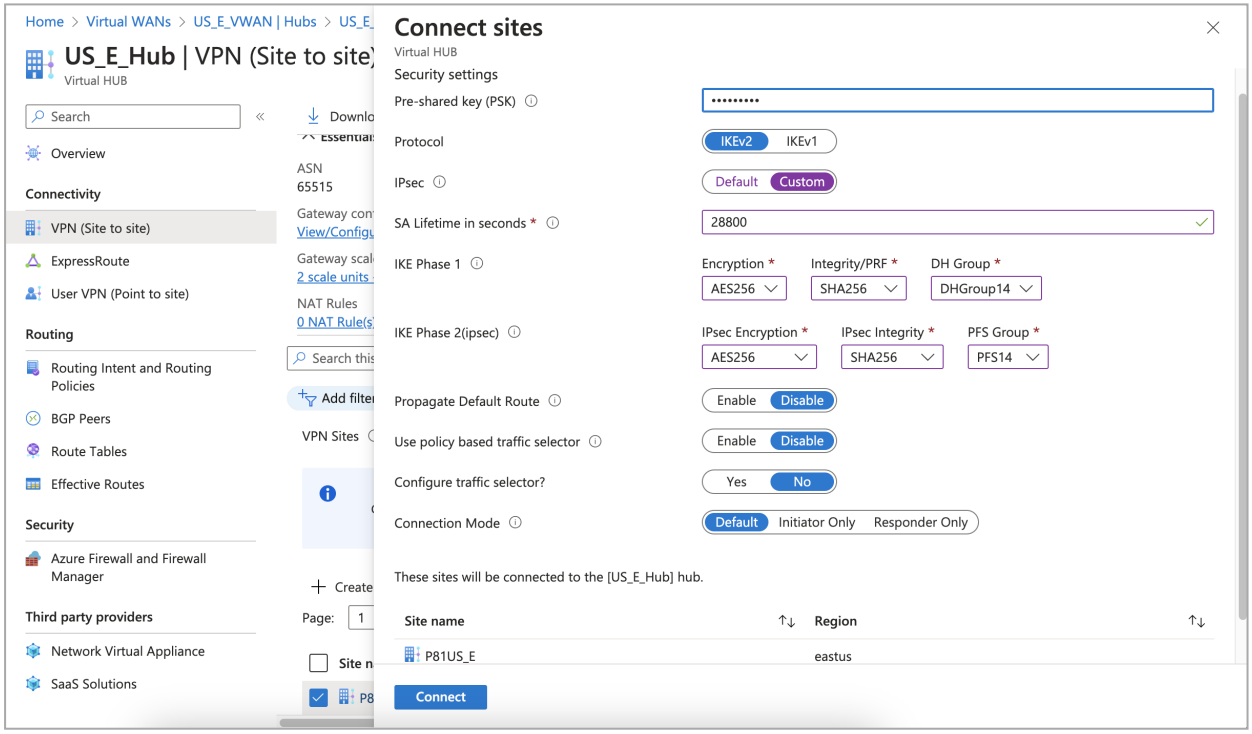
4. Clear the filter to view your site in the list.



5. Select the checkbox next to the created site and click **Connect VPN Sites**.



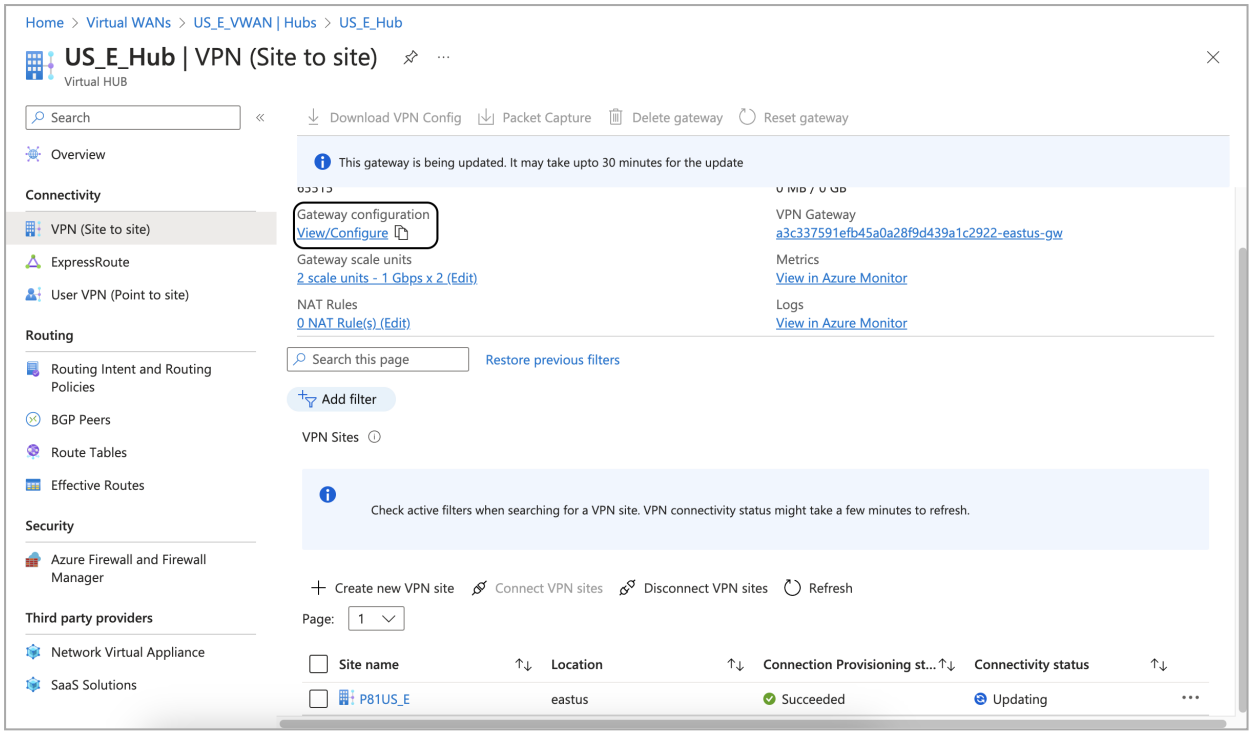
The **Connect sites** window appears.



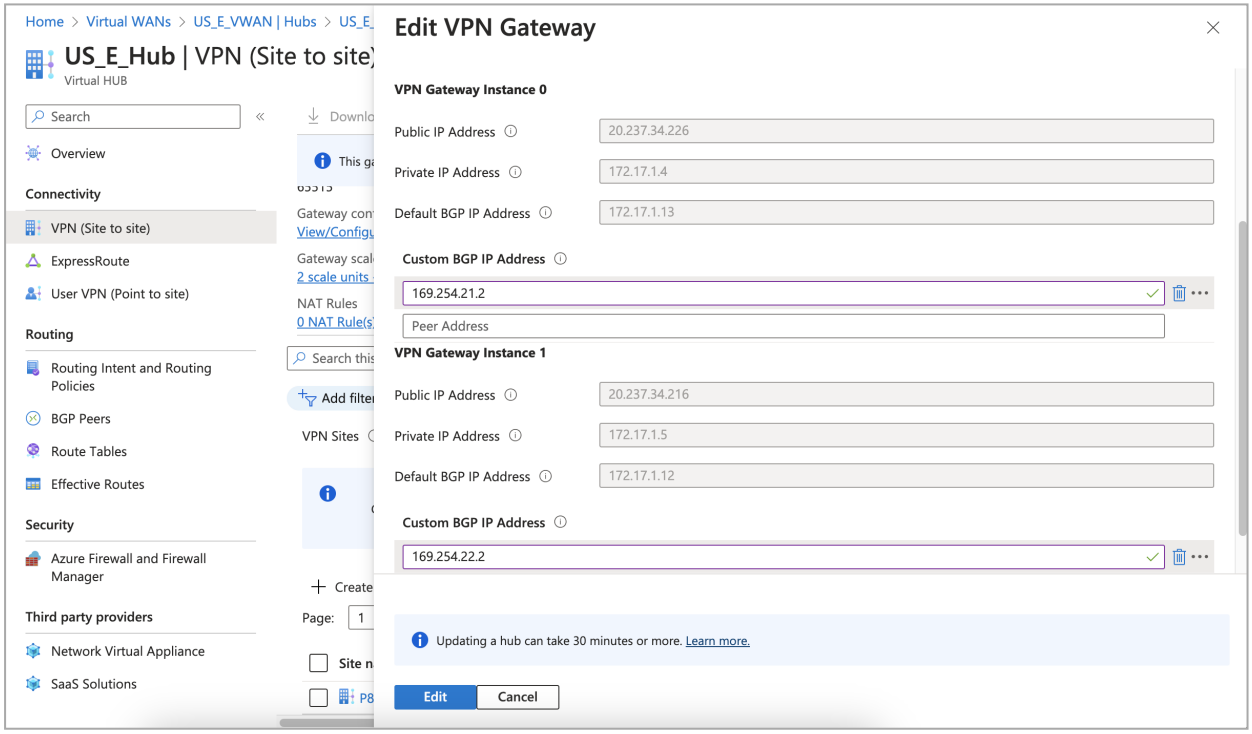
6. Enter these:

Item	Value
Pre-shared key (PSK)	Pre-shared key for this connection.
Protocol	IKEv2
IPsec	Custom
SA Lifetime in seconds	28800
IKE Phase 1	
Encryption	AES256
Integrity/PRF	SHA256
DH Group	DHGroup14
IKE Phase 2(ipsec)	
IPsecEncryption	AES256
IPsec Integrity	SHA256
PFS Group	PFS14
Propagate Default Route	Disable
Use policy based traffic selector	Disable
Configure traffic selector	No
Connection Mode	Default

7. Go to the **VPN (Site to site)** window and click **View/Configure** to configure the gateway.

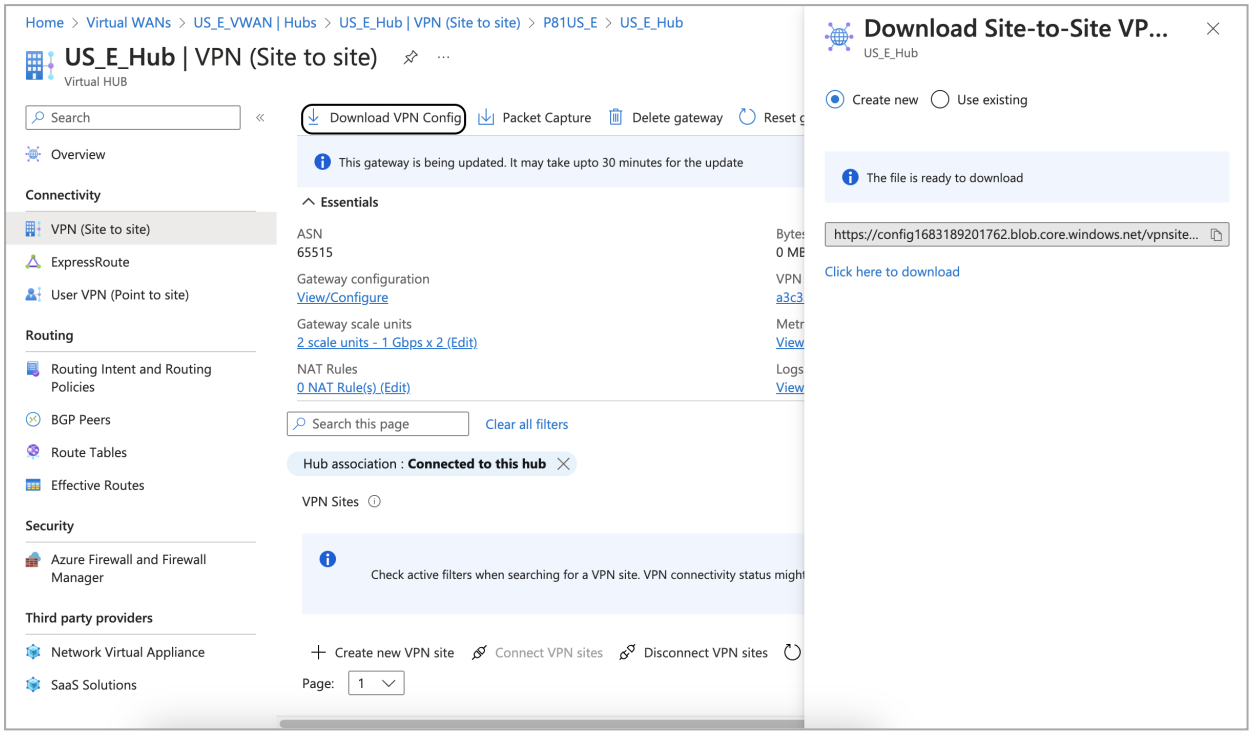


The **Edit VPN Gateway** window appears.



8. In the **VPN Gateway Instance 0** section, set the **Custom BGP IP Address** to the same network range as the BGP address for the first link.
9. In the **VPN Gateway Instance 1** section, set the **Custom BGP IP Address** to the same network range as the BGP address for the second link.
10. Click **Edit** and then **Confirm**.

11. Go to the **VPN (Site to site)** window and click **Download VPN Config** to download the configuration.

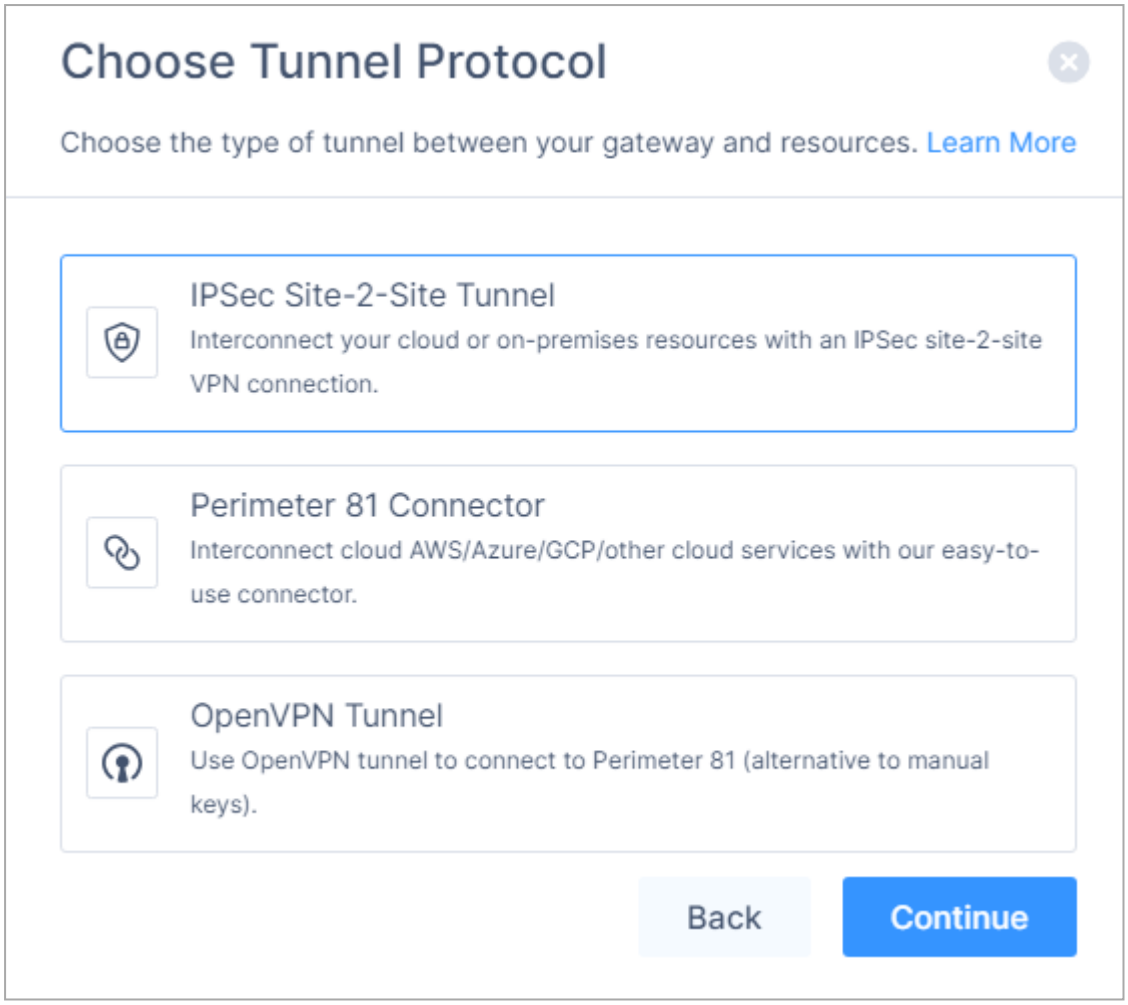


12. Click the download link.

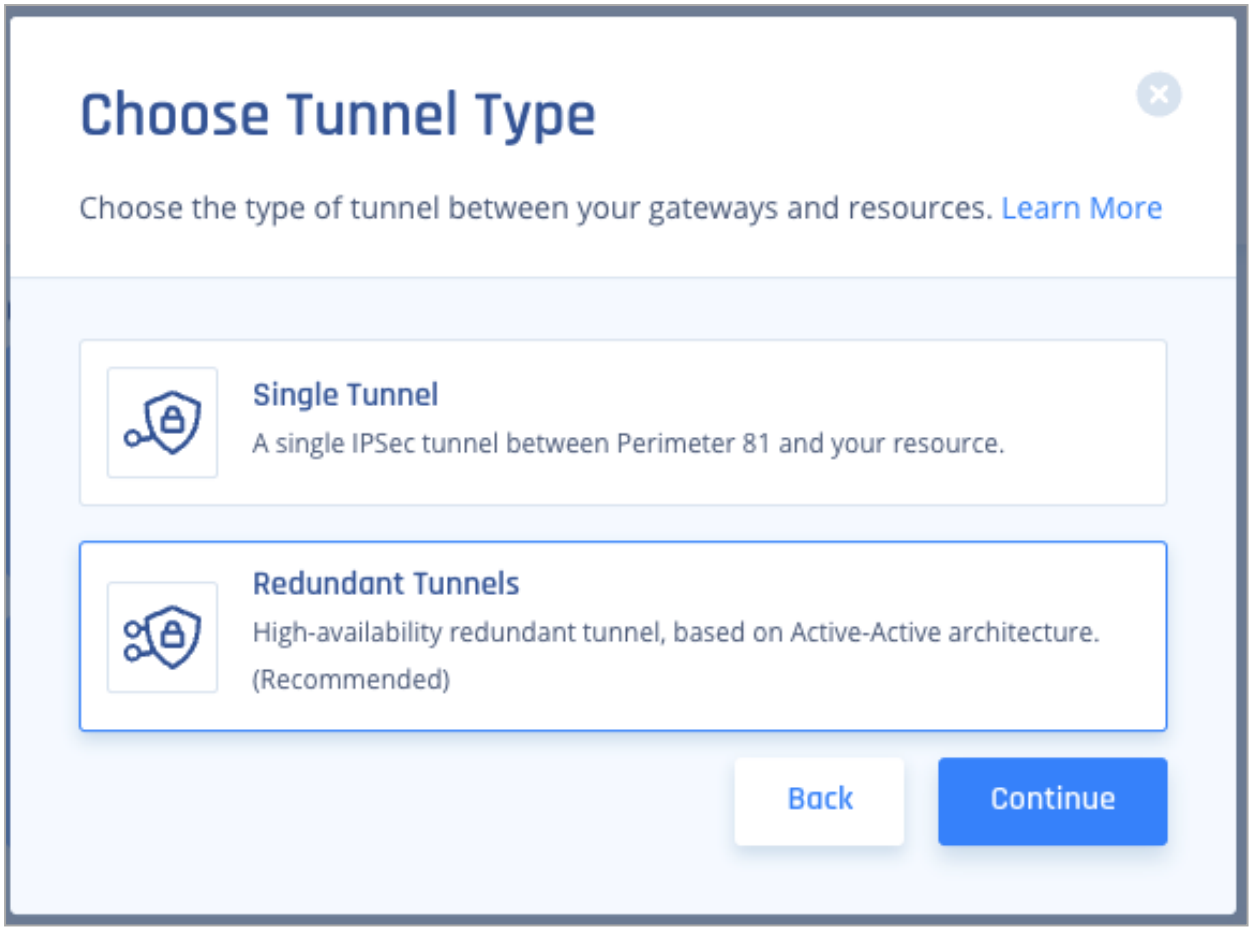
    The system downloads the configuration file.

Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal

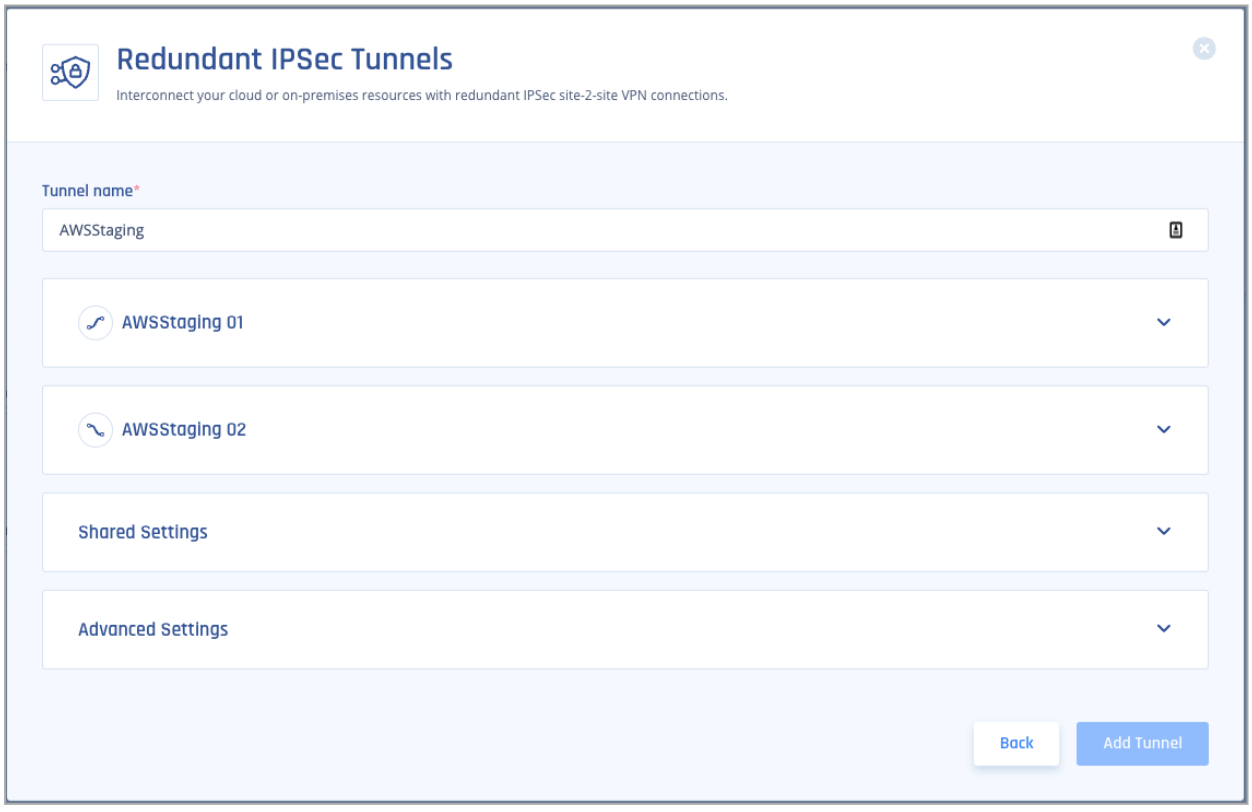
1. Access the Check Point SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



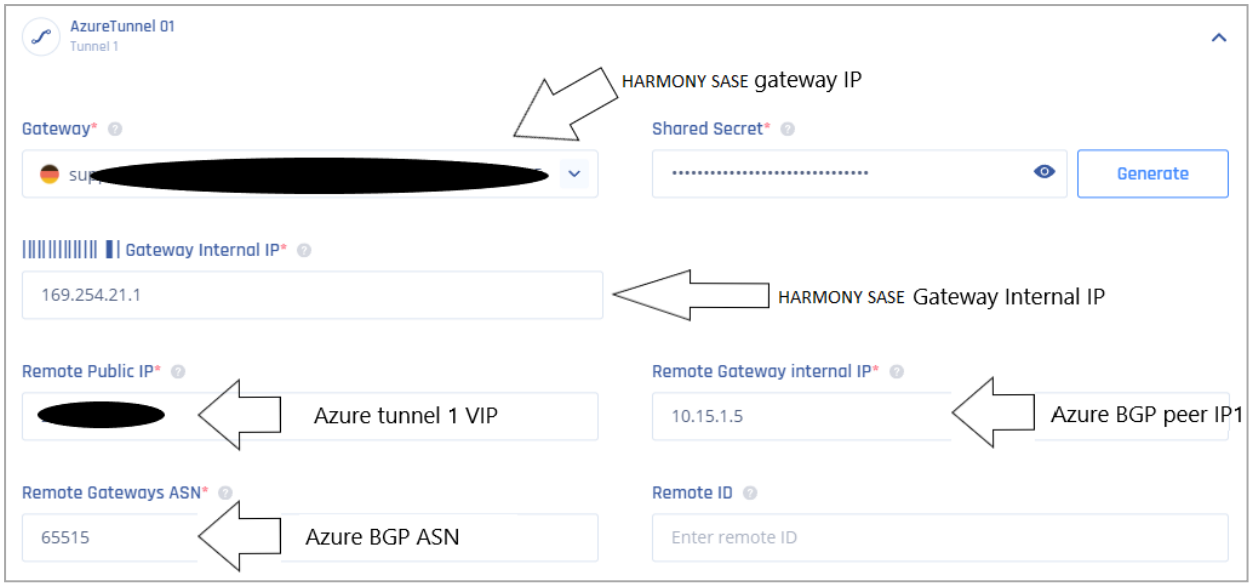
The **Redundant IPSec Tunnels** window appears.



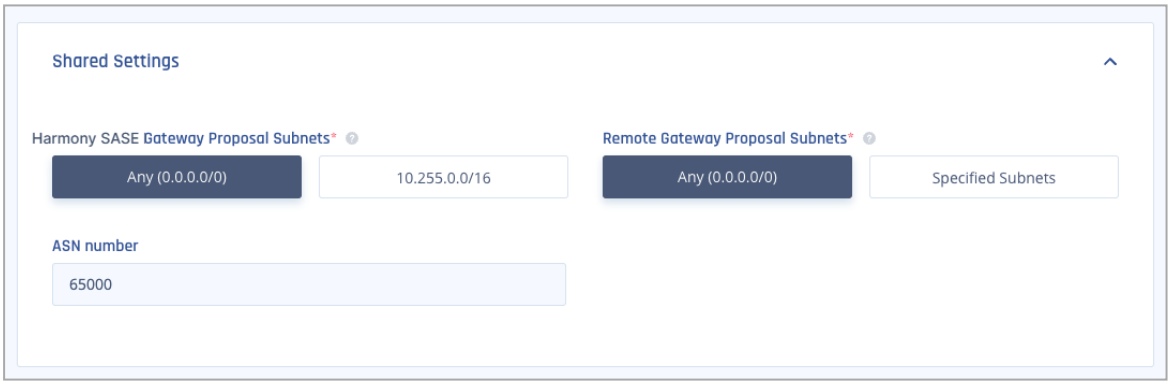
6. Copy the values for the first tunnel from the downloaded configuration file:

Item	Value
Shared Secret	PSK
Check Point SASE gateway Internal IP	Inside IP Addresses of Customer Gateway
Remote Public IP & Remote ID	Public IP Addresses of **VPN Gateway Instance 0**.
Remote Gateway internal IP	BGPPeeringAddress of **VPN Gateway Instance 0**
Remote Gateway ASN	Azure ASN

In the Check Point SASE Administrator Portal, enter the values for Tunnel 1 as:



7. Repeat step 6 for the second tunnel.
8. In the **Shared Settings** section:
   a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.
   b. **ASN** number must be the same for the Check Point SASE side.



9. In the **Advanced Settings** section, enter the information for your tunnel type (unless you have configured customer settings on the Azure side):

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

Google Cloud Platform

This chapter describes the procedure to establish a Site-to-Site IPsec tunnel between your Check Point SASE network and Google Cloud Platform (GCP).

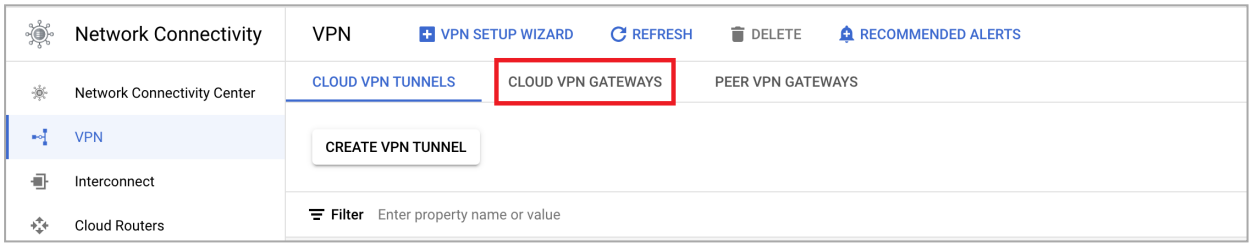
Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

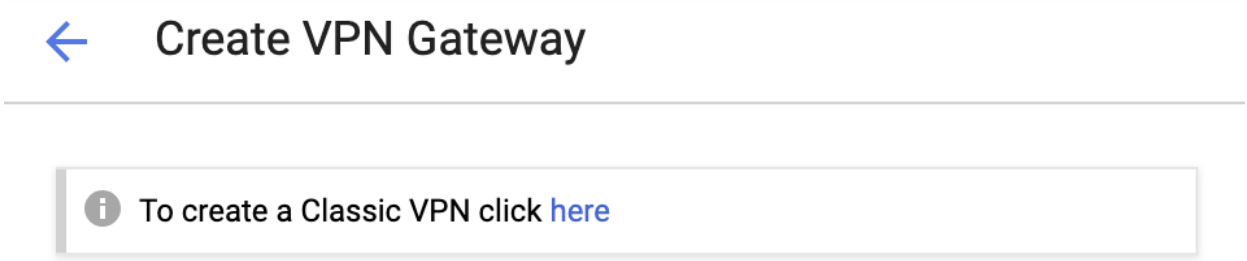
Step 1 - Configurations in the GCP Console

Creating a Virtual Private Gateway

1. Access the GCP console and go to **Network Connectivity**.
2. In the left menu, click **VPN**.
3. Click **Cloud VPN Gateways** > **Create VPN gateway**.



4. Click the link to create Classic VPN.



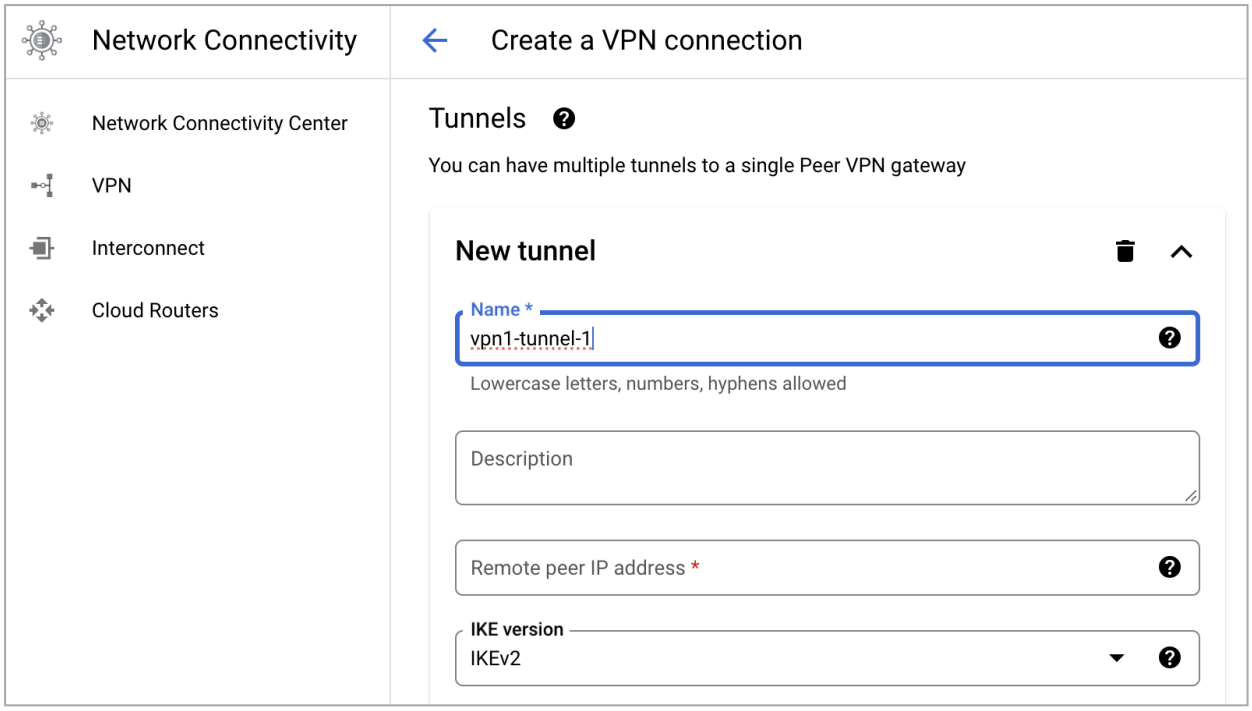
5. Enter these:
   i. **Name** - Name of the gateway.
   ii. **Network** - Select **default** or a specific VPC.

iii. **Region** - Select the region where your resources are located.

iv. **IP address** - Create an IP address to connect your gateway and click **Reserve**.

Creating a Tunnel

1. Access the GCP console and go to **Network Connectivity**.
2. In the left menu, click **VPN**.
3. Click **Cloud VPN Tunnels** > **Create VPN tunnel**.
4. Enter these:



i. **Name** - Name of the tunnel.

ii. **Remote peer IP address** - IP address of your Check Point SASE Gateway.

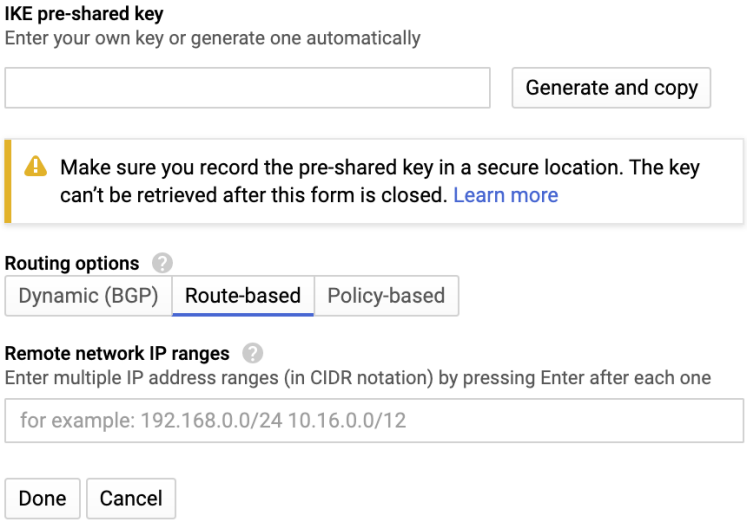
To obtain this, go to the Check Point SASEAdministrator Portal > **Networks** and select the network that contains the gateway to which you wan to create a tunnel.

iii. **IKE Version** - IKEv2

iv. **IKE pre-shared key** - Click **Generate and copy** or select a key of your own and note it down.

v. **Routing options** - Route-based

vi. **Remote network IP ranges** - 10.255.0.0/16 (unless customized)



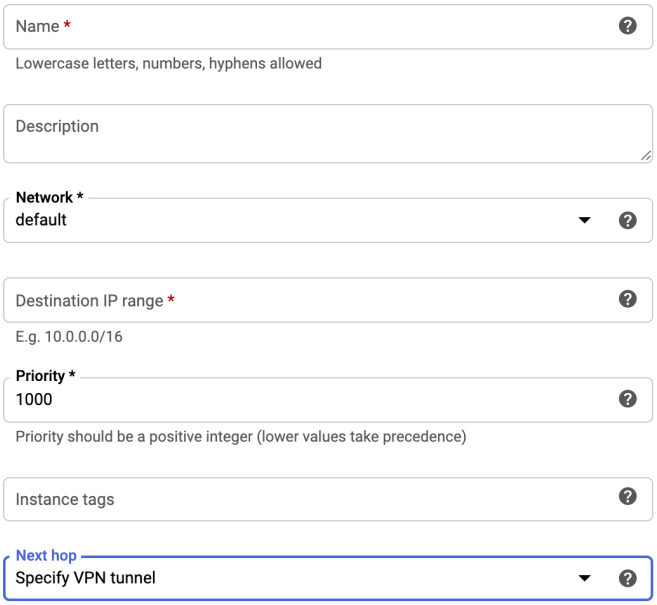
5. Click **Done** and then **Create**.

Configuring the Routing Rules to the VPC Network

1. Access the GCP console and go to the **VPC Network** section.
2. In the left menu, click **Routes**.

3. Click **Create Route Rule**.
4. Enter these:
   a. **Name** - Name of the VPN gateway.
   b. **Network** - Select the VPC network that contains the instances served by the VPN gateway. This must be the same network selected in the previous steps.
   c. **Destination IP range** - 10.255.0.0/16 (or customized)
   d. **Priority** - 1000
   e. **Next hop** - Select **Specify VPN Tunnel**.

f. **Next hop VPN tunnel** - Select the VPN tunnel you created in the previous steps.

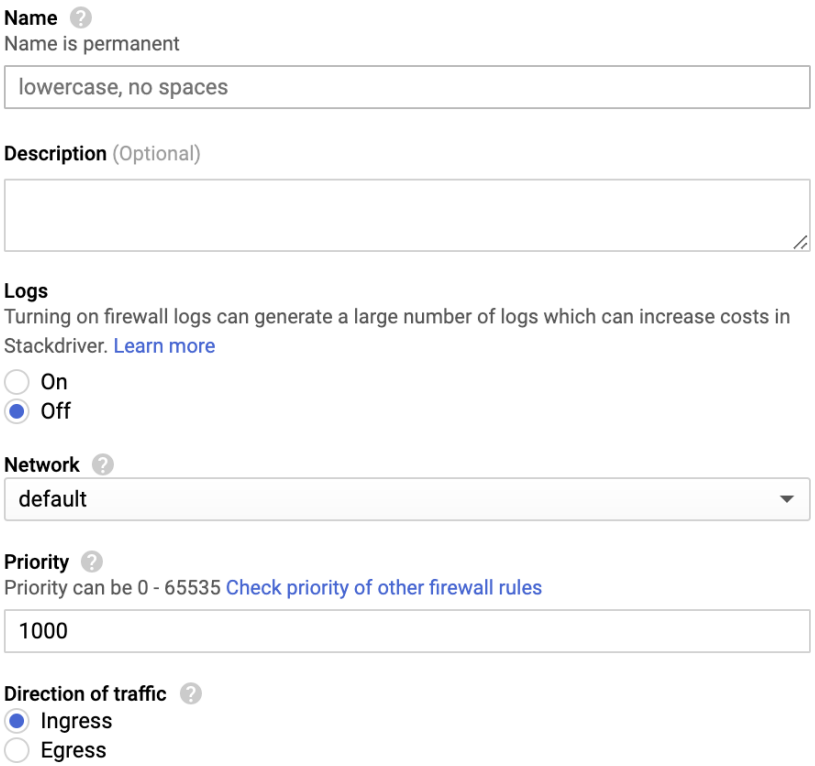


5. Click **Create**.

Allowing Incoming Connections from Check Point SASE Local Network Using Firewall Rules

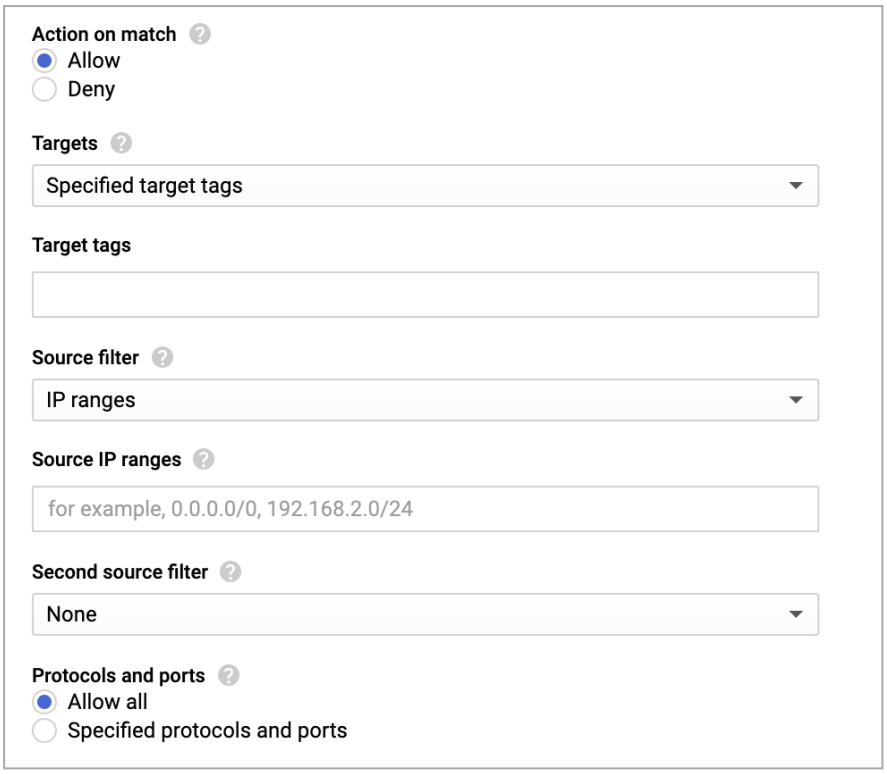
1. Access the GCP console and go to the **VPC Network** section.
2. In the left menu, click **Firewall rules**.

3. Click **Create Firewall Rule**.



4. Enter these:
   a. **Name** - Name of the rule.
   b. **Logs** - Off
   c. **Network** - Select the VPC network that contains the instances served by the VPN gateway. This must be the same network selected in the previous steps.
   d. **Priority** - 1000
   e. **Direction of traffic** - Ingress.

f. **Action on match** - Allow



g. (Optional) **Target tags**

h. **Source filter** - IP ranges

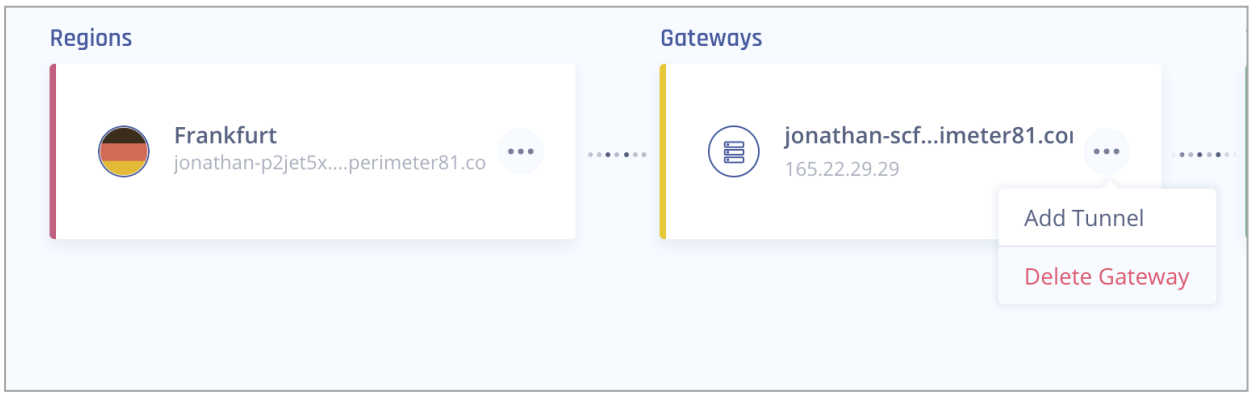
i. **Source IP ranges** - 10.255.0.0/16 (unless customized)

j. **Second source filter** - None

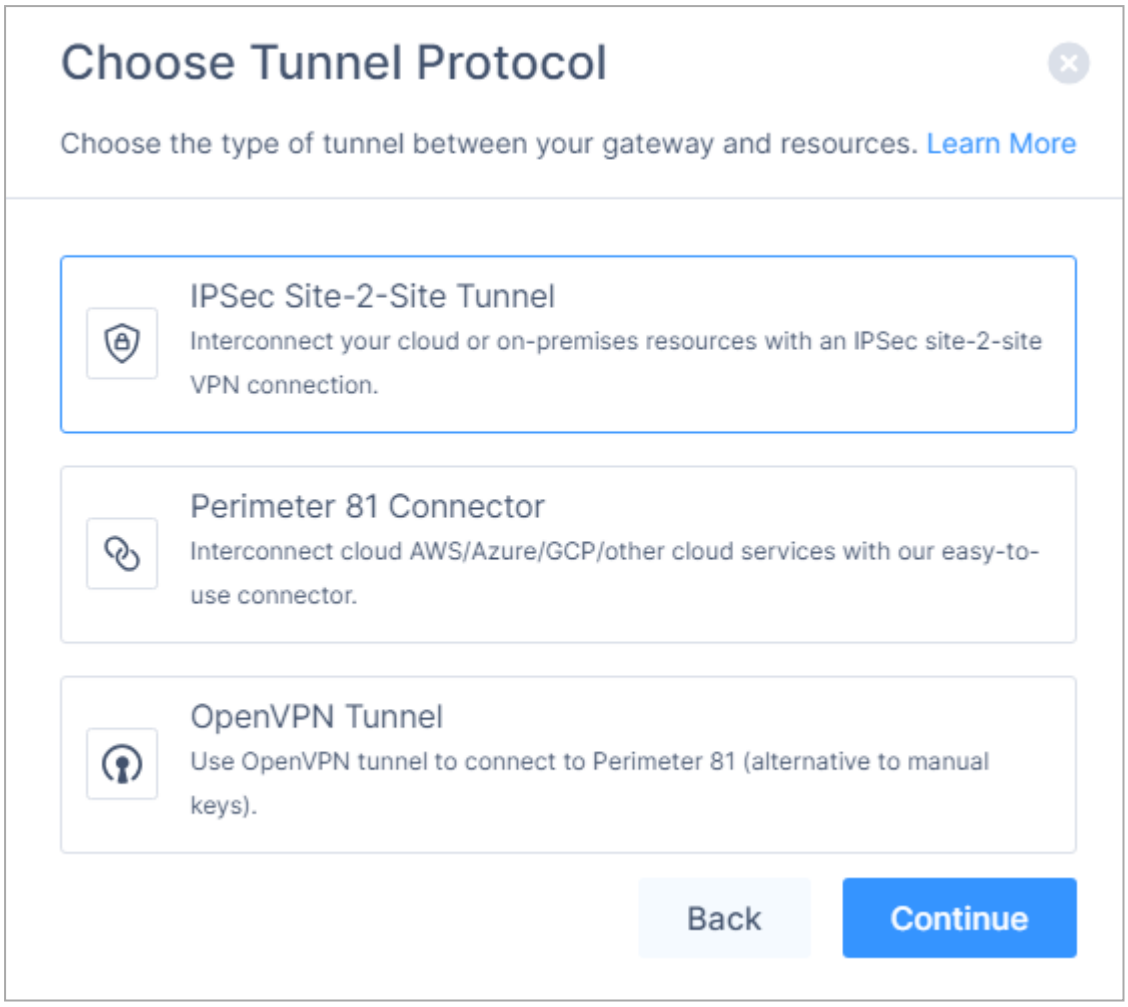
k. **Protocols and ports** - Allow all

Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

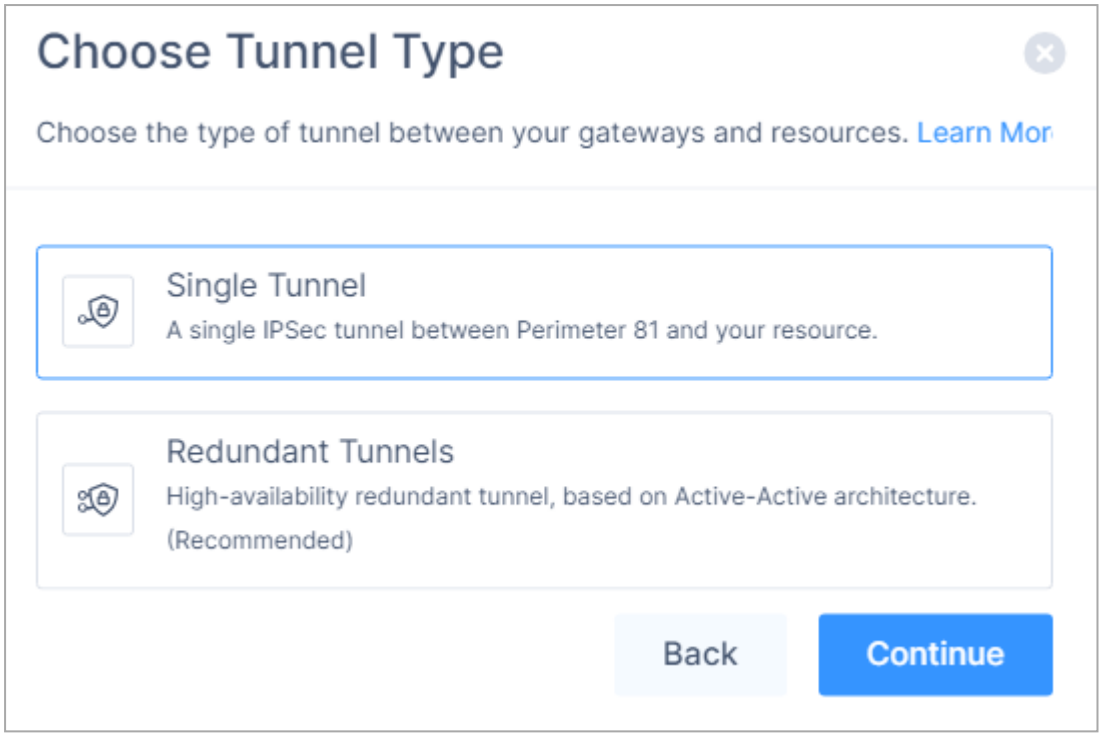
1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



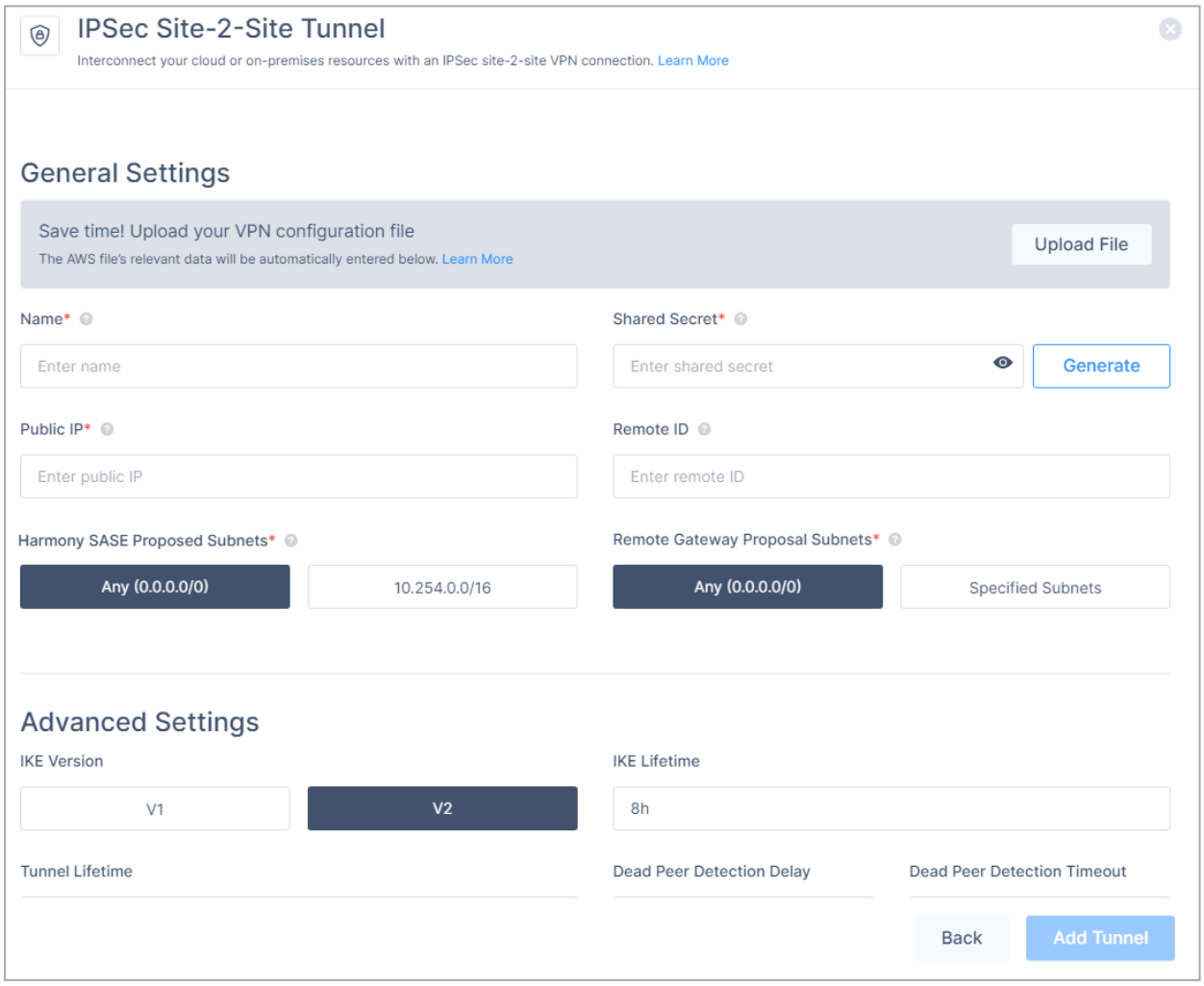
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



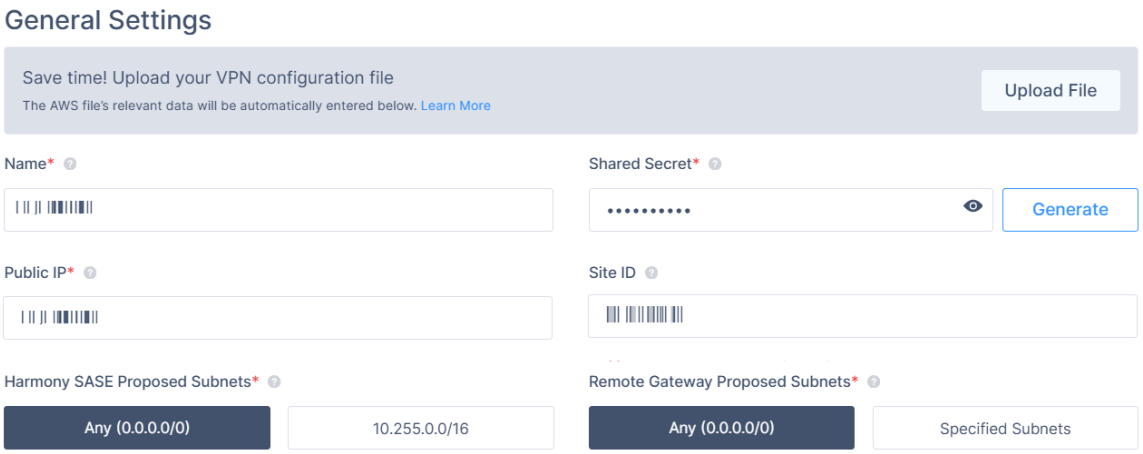
5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
   a. **Name** - Name of the tunnel.
   b. **Check Point SASE Gateway Proposal Subnets** - Any (0.0.0.0/0)
   c. **Remote Gateway Proposal Subnets** - Any (0.0.0.0/0)



7. In the **Advanced Settings** section, enter the information for your tunnel type:

Field Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

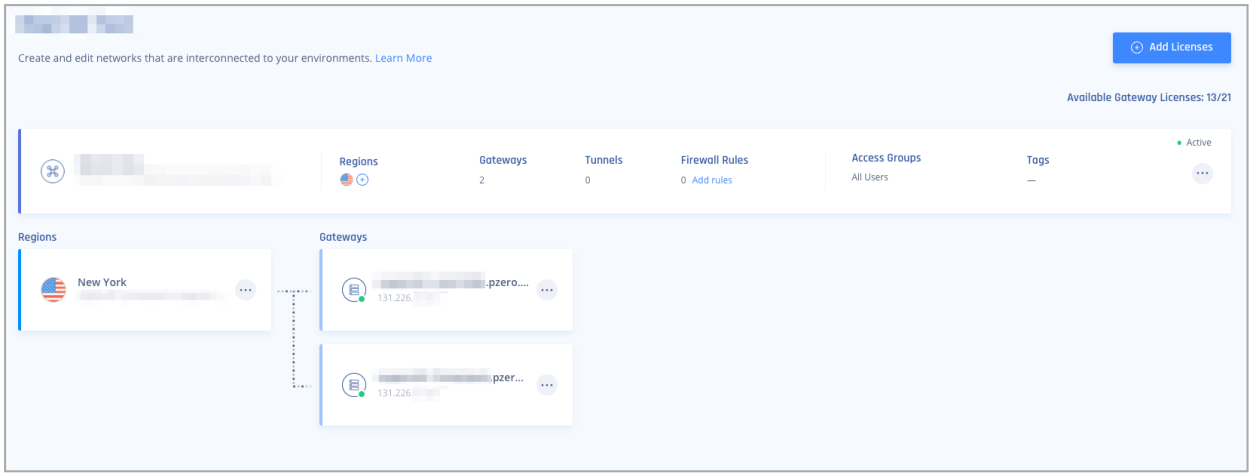
8. Click **Add Tunnel**.

Google Cloud Platform (GCP) Redundant Tunnels

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Check Point SASE network must have at least two different gateways in the same network.



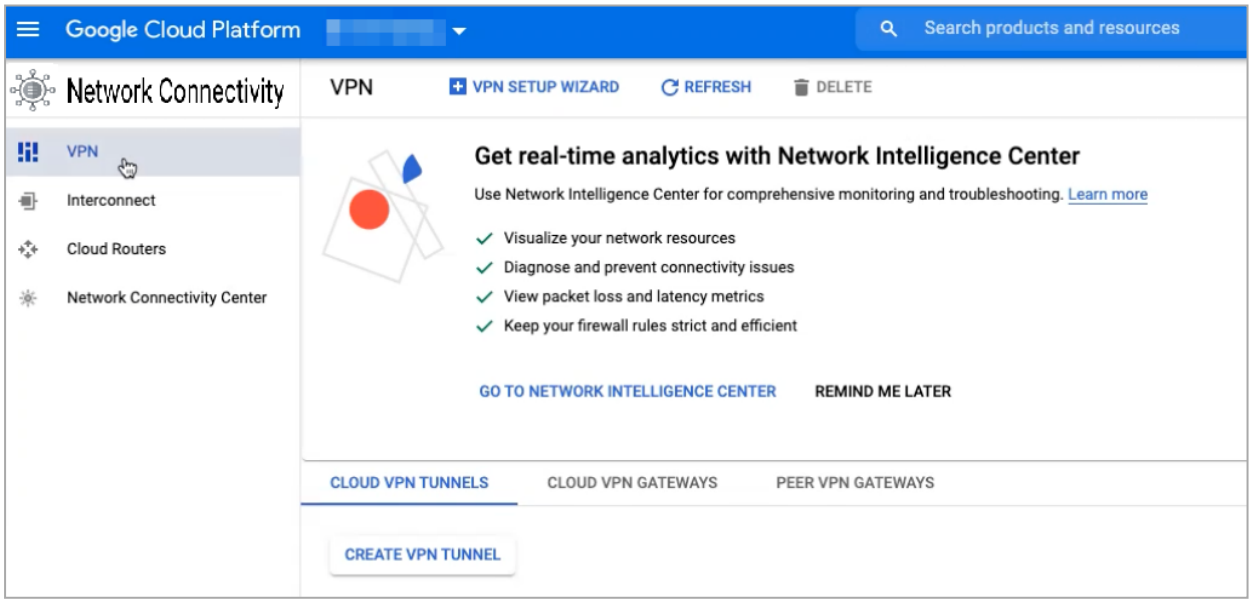
Notes -

- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the GCP Console

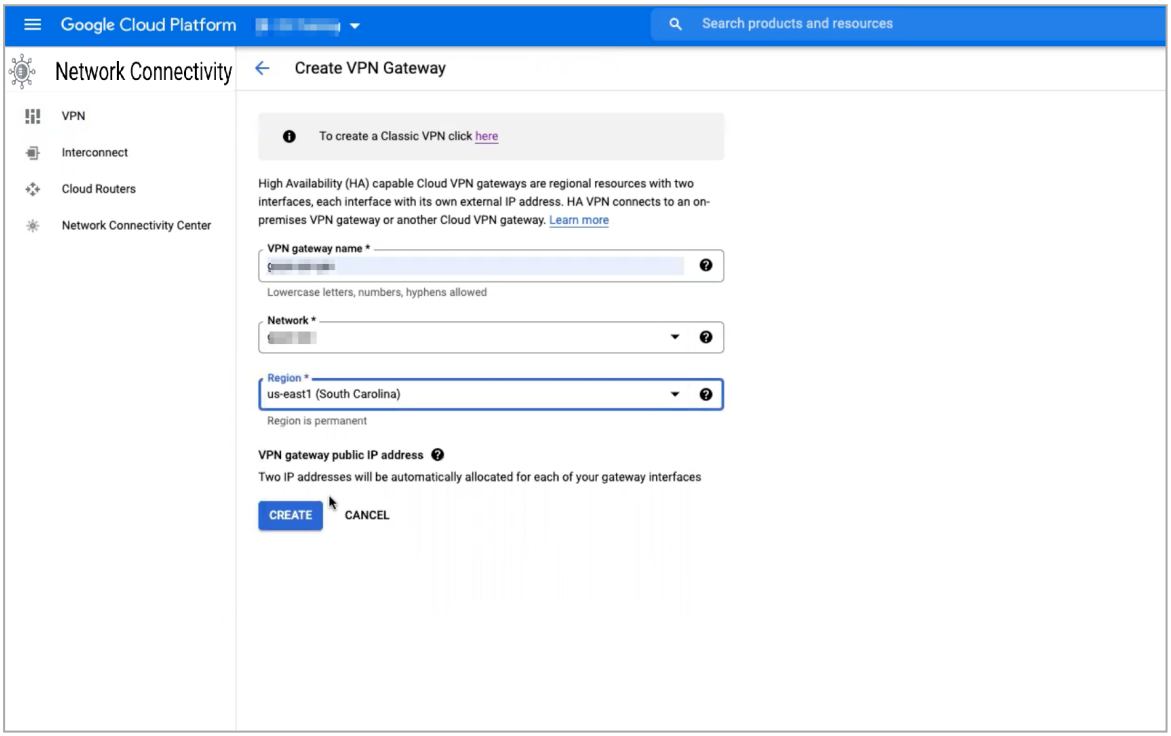
Creating a VPN Gateway

1. Access the GCP console and in the **Network Connectivity** section, click **VPN**.



2. Click **Cloud VPN Gateways** > **Create VPN Gateway**.

3. Enter these:
   a. **Name** - Name of the gateway.
   b. **Network** - GCP network you want to access through Check Point SASE.
   c. **Region** - Region where your resources are located.

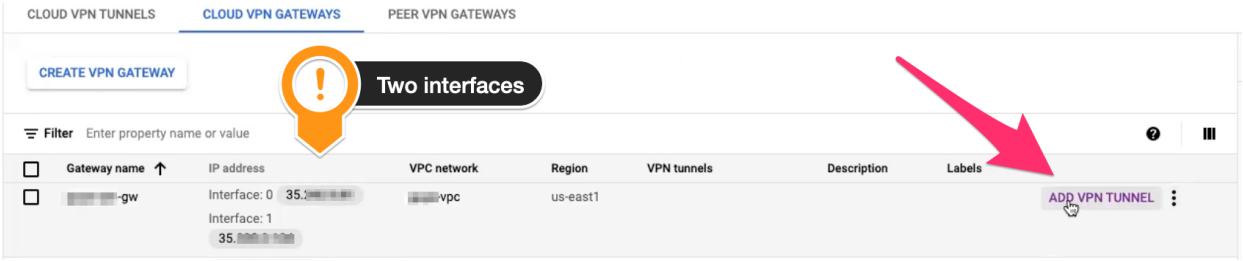


4. Click **Create**.

   The system creates two interfaces, **Interface 0** and **Interface 1**.

Adding a Redundant VPN Tunnel

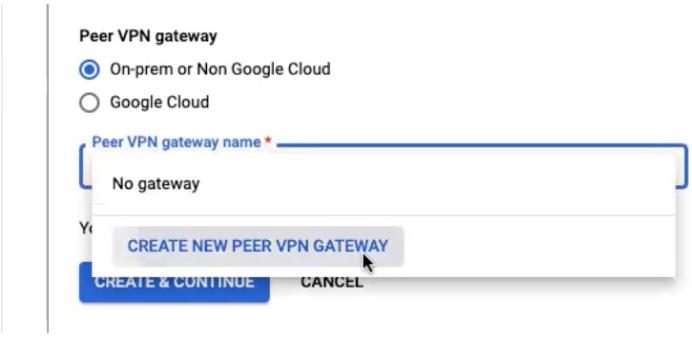
1. Access the GCP console and go to the VPN gateway you created and click **Add VPN Tunnel**.



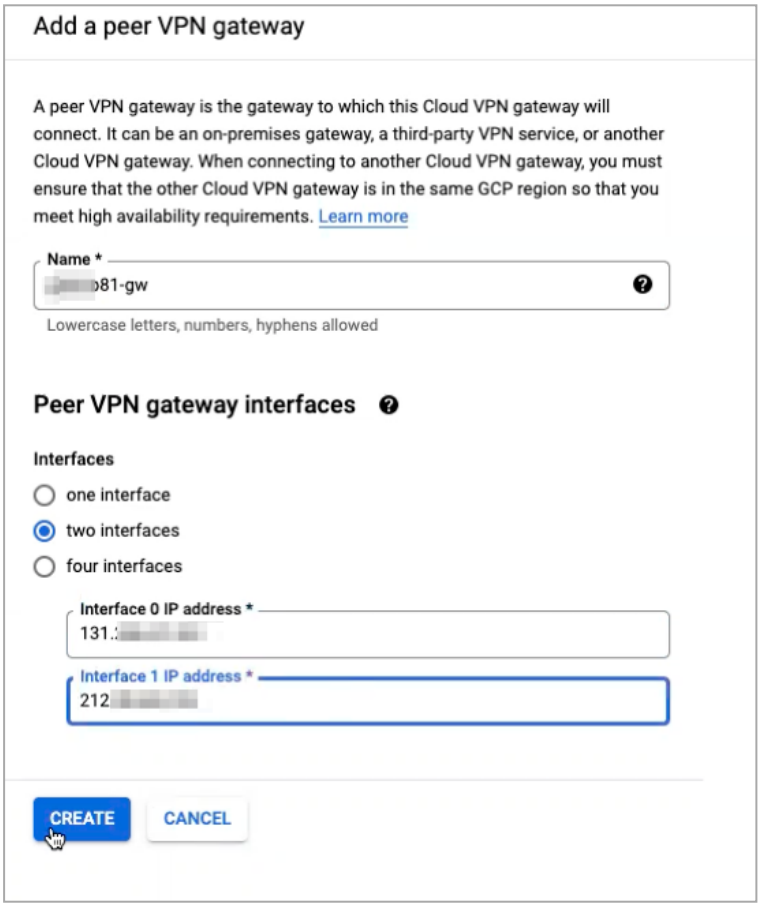
2. Enter these:

a. **Peer VPN gateway** - On-prem or Non-Google Cloud.

b. Click the drop-down menu in **Peer VPN gateway name** and select **Create new peer VPN gateway**.



The **Add a peer VPN gateway** window appears.



c. In the **Name** field, enter the name of the peer VPN gateway that represents the setup at the Check Point SASE side.

d. In the **Peer VPN gateway interfaces** section, select **two interfaces**.

e. In the**Interface 0 IP address** field, enter the IP address of the first Check Point SASE gateway.

f. In the**Interface 1 IP address** field, enter the IP address of the second Check Point SASE gateway.

g. Click **Create**.

h. In the **High availability** section, select **Create a pair of VPN tunnels**.

i. In the **Routing options** section, click the **Cloud Router** drop-down menu, and select **Create a new router**.

   The Cloud router in GCP manages your BGP ASN routes.

   I. Name your Cloud router.

   II. Set **Google ASN** to 65511 (This can be any value. Note this value as it is required to configure the tunnel in the Check Point SASE Administrator Portal).

      Following steps are optional. Perform them only if you have a peered VPC to reach through the tunnel:

      i. In **Advertised routes**, select **Create custom routes**.

      ii. Select Advertise all subnets visible to the Cloud Router.

      iii. In **Custom ranges**, click **Add Custom Route**.

      iv. In **New custom route**, enter the network CIDR for the peered VPC and click **Done**.

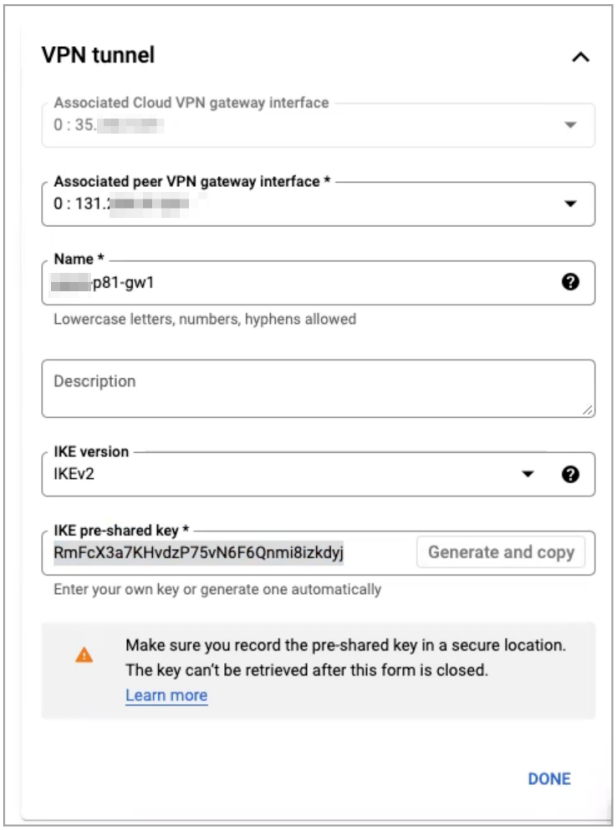
      v. Repeat the last two steps for each range you need to route through the tunnel.

   III. Click **Create**.

j. In the **VPN tunnel** section, select the first VPN tunnel and name it according to the gateway you created in Check Point SASE.

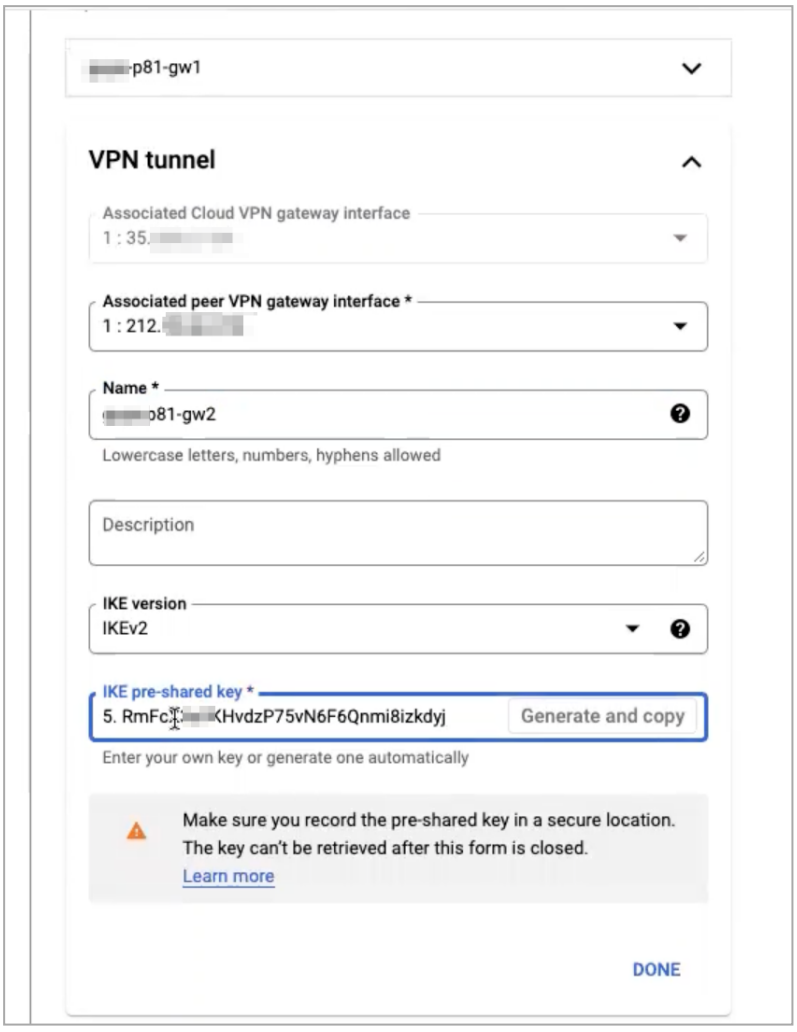
   i. In the **IKE pre-shared key** field, click **Generate and copy**.

   Special characters except dot (.) and underscore (_) are not allowed.



k. Select the second VPN tunnel and name it according to the gateway you created in Check Point SASE.

i. In the **IKE pre-shared key** field, paste the IKE pre-shared key you copied in the previous step.



Note - This IKE Pre-shared key is used later to establish a handshake between the sites.

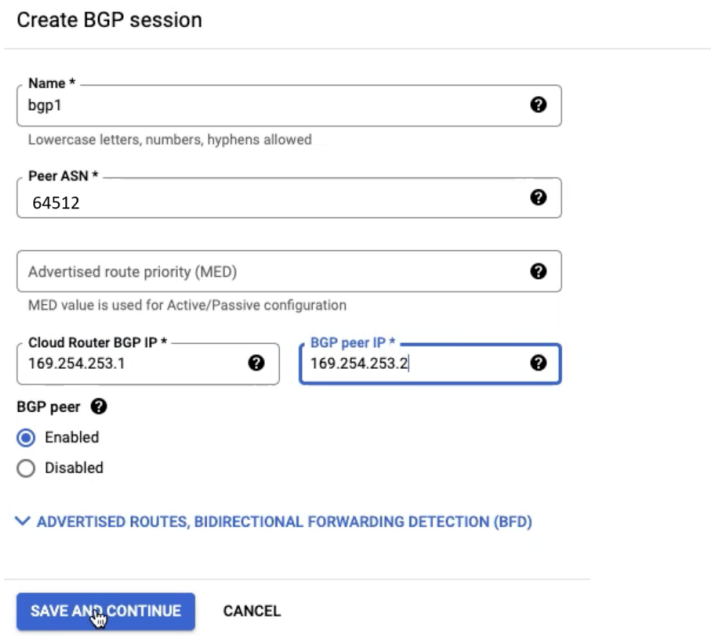
ii. Click **Done**.

l. Click **Create and continue**.

Configuring Border Gateway Protocol (BGP) Routes

1. Access the GCP console and go to the tunnel where you want to configure the route and click **Configure**.

2. For Tunnel 1, set the BGP routes according to this image.

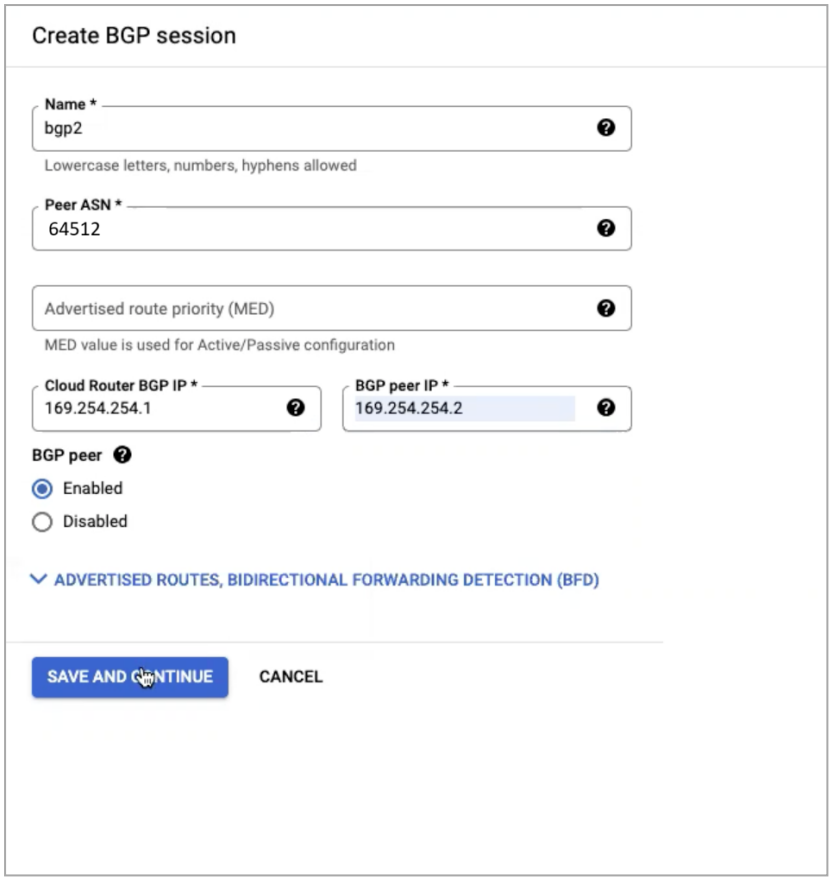


   a. In the **Peer ASN** field, set the value as 64512. It represents the BGP route for Check Point SASE.

   b. For **Cloud Router BGP IP** and **BGP peer IP** fields, select a unique Link-local address.

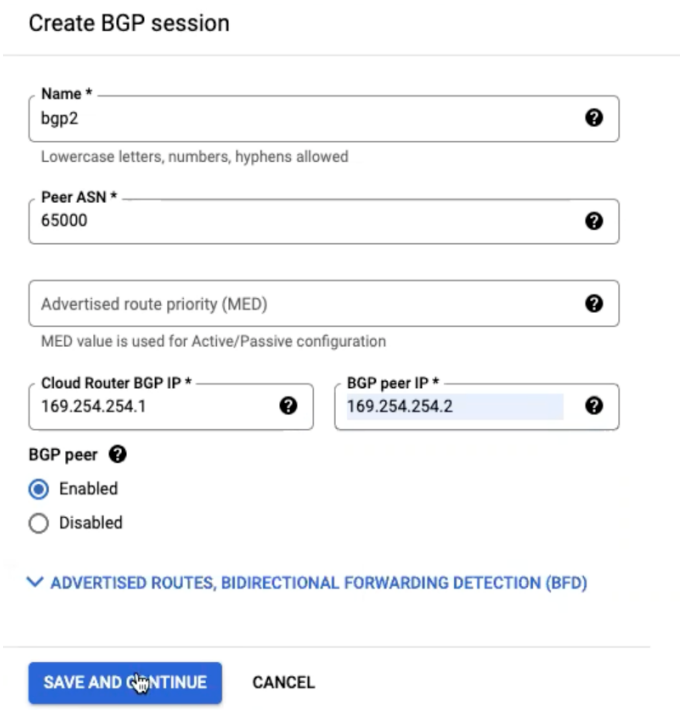
3. Click **Save and Continue**.

4. For Tunnel 2, set the BGP routes according to this image.

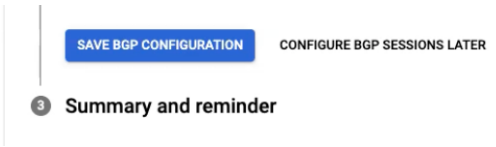


a. In the **Peer ASN** field, set the value as 64512. It represents the BGP route for Check Point SASE.

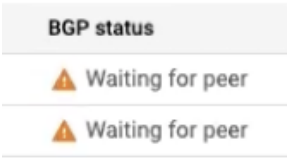
b. For **Cloud Router BGP IP** and **BGP peer IP** fields, select a unique Link-local address.



5. Click **Save and Continue**.
6. Click **Save BGP Configuration**.



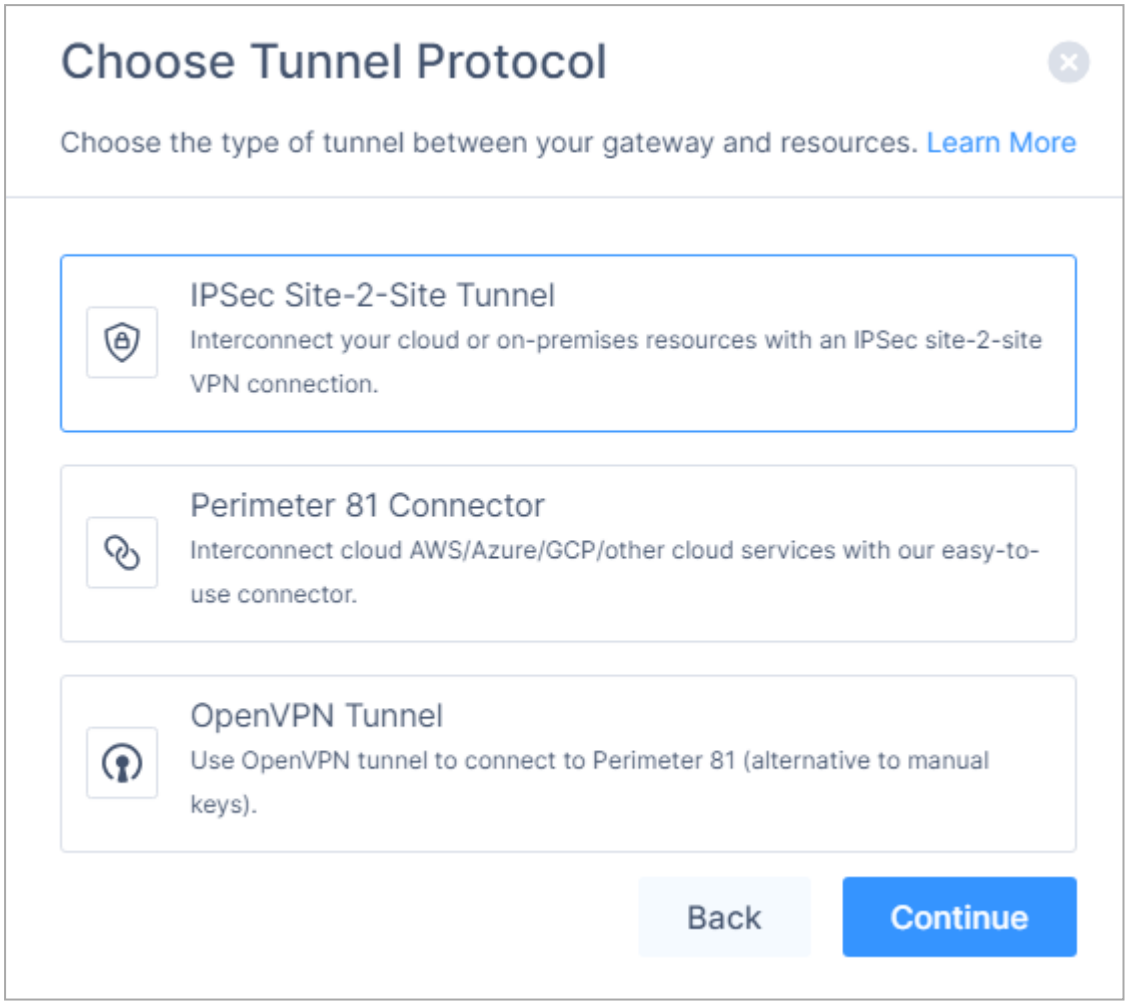
When the tunnel setup is complete, the **BGP status** is displayed as **Waiting for peer** until the tunnels are setup in Check Point SASE.



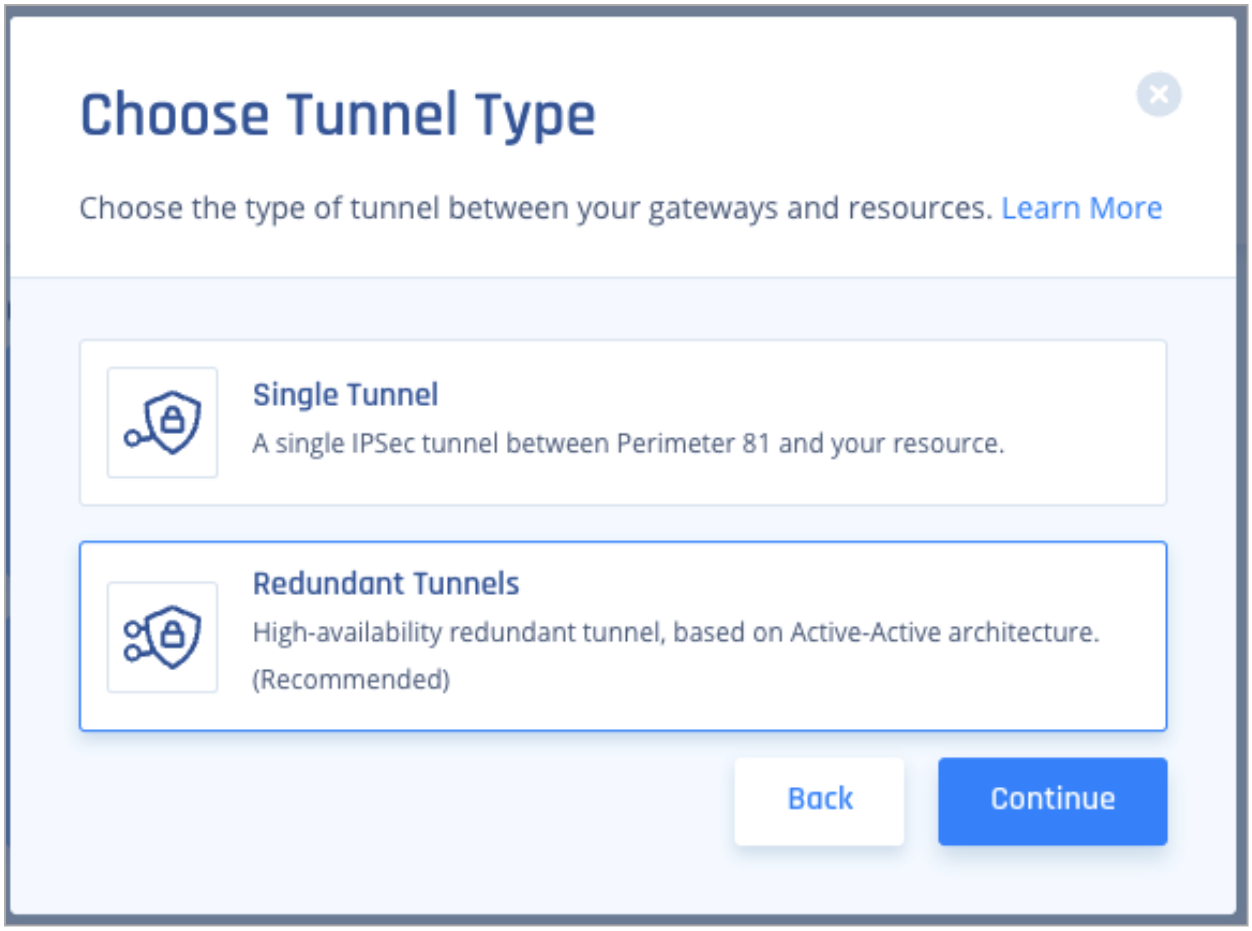
Step 2 - Creating the Tunnels in the Check Point SASE Administrator Portal

1. Access the Check Point SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.

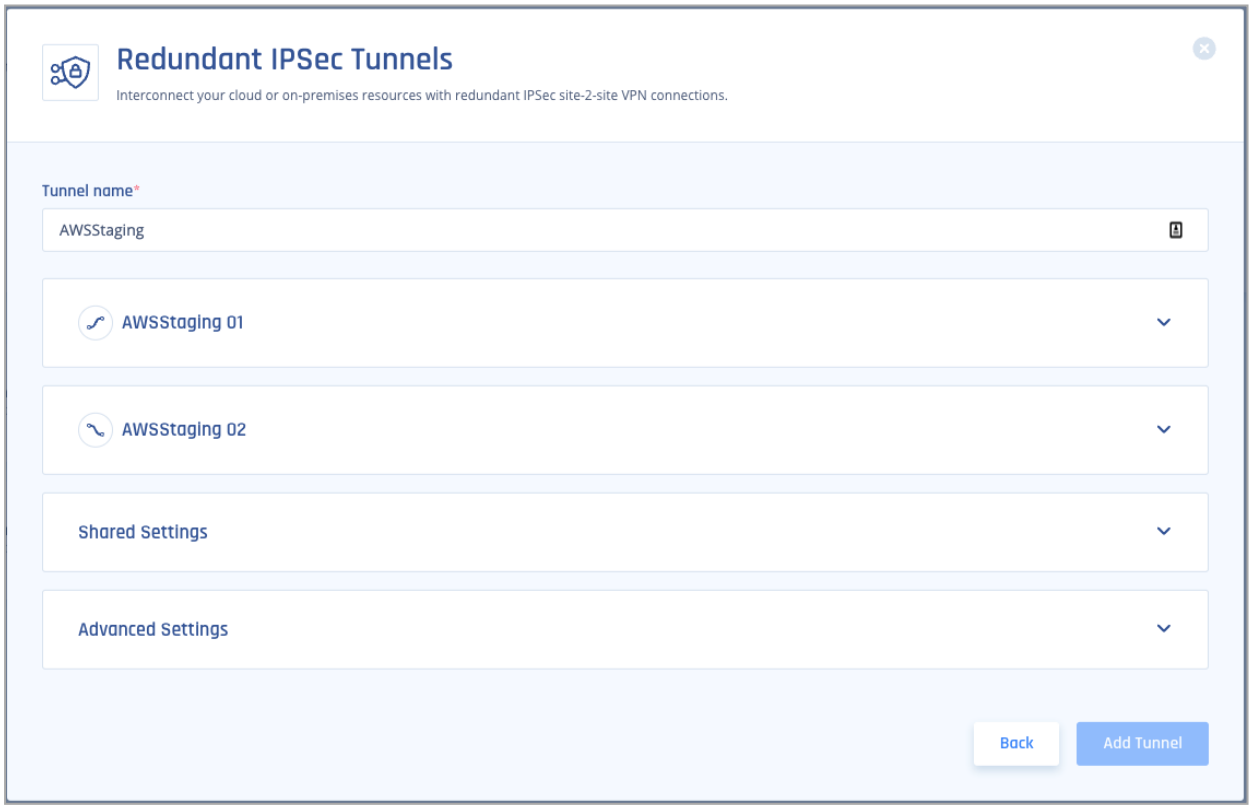
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.

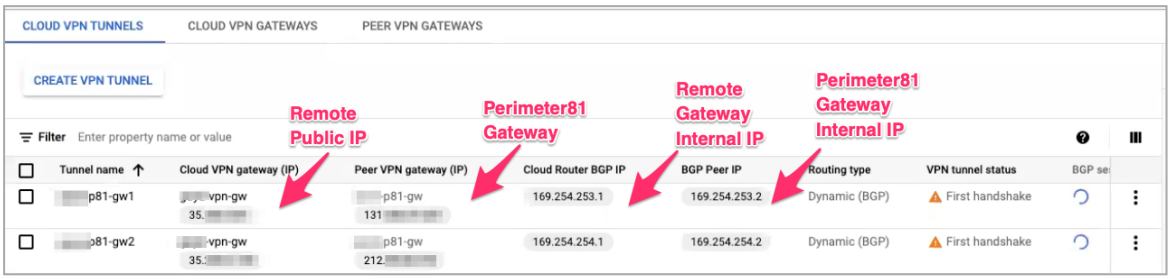


6. In the **General Settings** section:

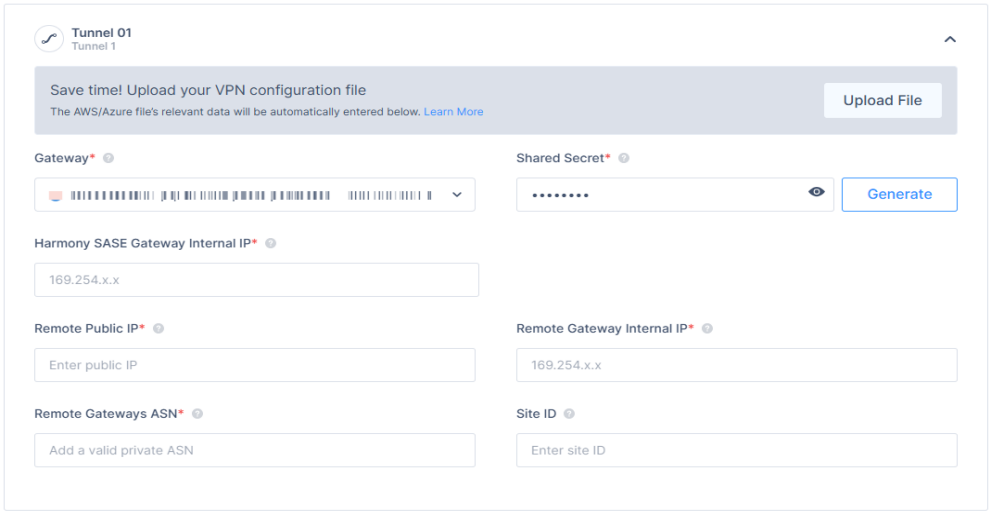
   a. In the **Name** field, enter a name for your tunnel.

   b. In your GCP console, in **Network Connectivity** > **VPN**, copy and paste the values for Tunnel 1 and Tunnel 2 according to the image below.

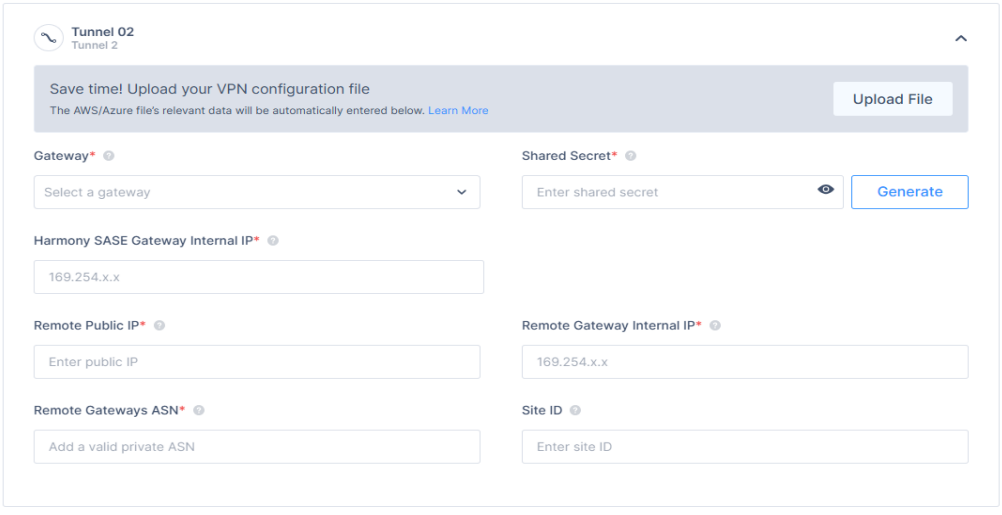
   Enter **ASN** value as 65511 for both tunnels.



Example - Tunnel 1



Example - Tunnel 2

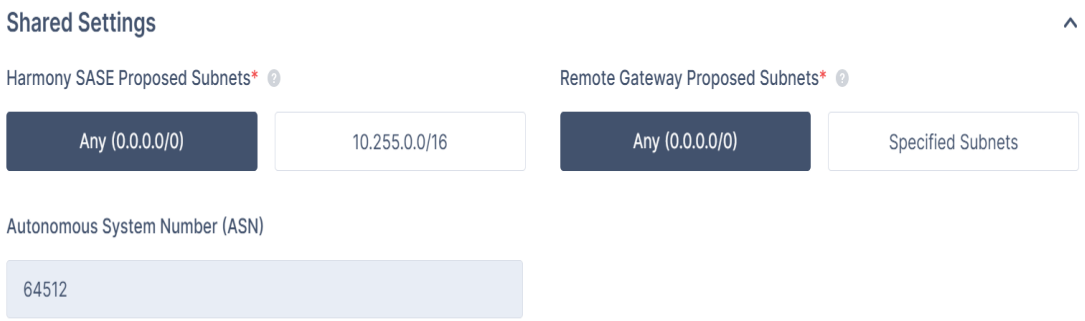


7. In the **Shared Settings** section:

a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.

b. Set **ASN** as 64512.

Warning - You cannot edit the ASN in Check Point SASE after you create the tunnel.



8. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

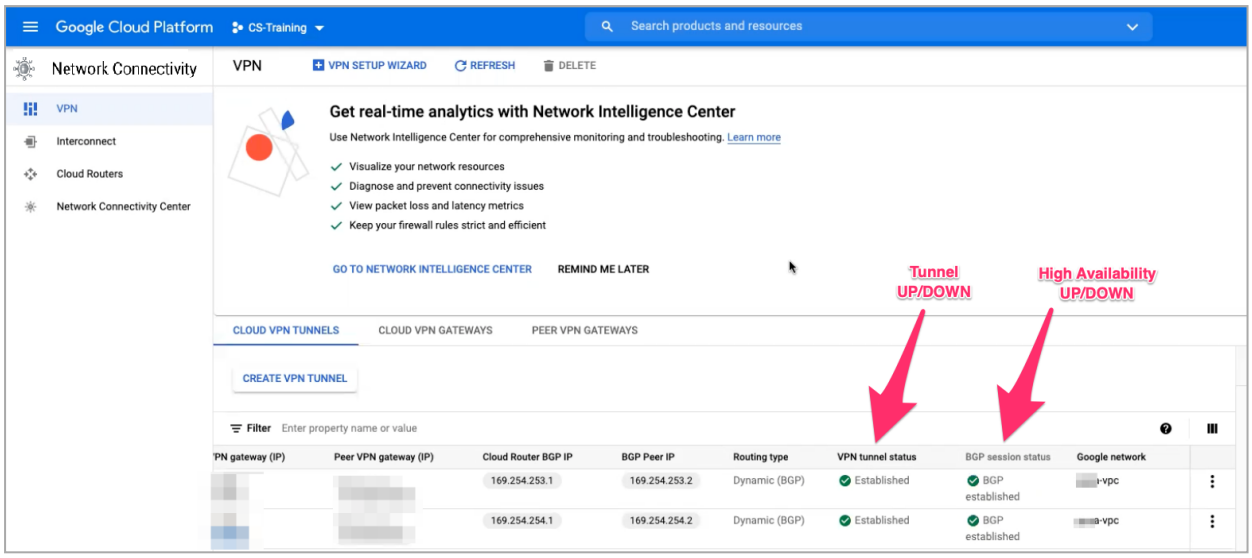
[1] Suggested values. For other supported ciphers, see this Google article.

9. Click **Add Tunnel**.

Verifying the Setup in GCP Console

1. Access the GCP console and go to **Network Connectivity** > **VPN**.
2. Verify that the **VPN tunnel status** and **BGP session status** appears with a green tick

mark.

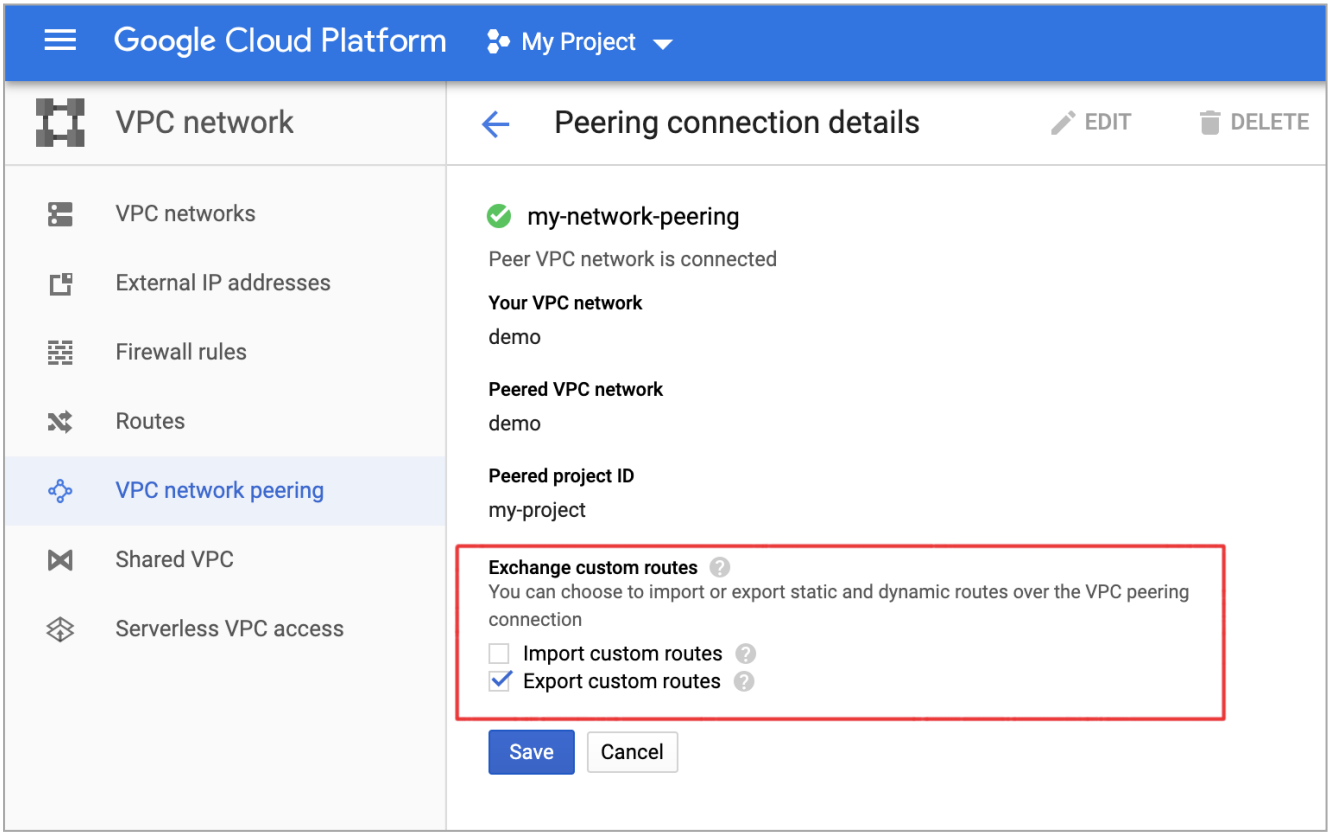


Google Cloud VPC Peering

VPC peering allows you to connect Check Point SASE with Google Cloud Platform by exporting the route of your Check Point SASE network to the VPC.

With VPC peering, you need only a single tunnel from Check Point SASE to the shared Google Cloud VPC. The other peered VPC recognizes the Check Point SASE subnets by having its route in their routing table.

Export the custom routes from your shared VPC.



Google Cloud DNS

You can integrate Google Cloud's Private Zone/Private DNS feature with SASE gateway. This enables you to utilize the capabilities of private DNS zones, that allows resolution of external records.

Prerequisites

- Google Cloud Platform (GCP) project
- VPC Network (you can create one or use Google's predefined subnets)
- Site-to-Site VPN tunnel to the VPC from SASE

Enabling Private DNS with SASE Gateway

To allow administrator to expose Google Cloud DNS through a private IP within one or multiple networks defined in your VPC through GUI/Web Interface, do this:

1. Log in to Google Cloud Platform.
2. Go to **Networking** > **Network services** > **Cloud DNS**.
3. Click the **DNS Server Policies** tab.
4. Click **Create Policy**.

   The **Create a DNS policy** page appears.
5. In the **Name** field, enter a name for the DNS policy. Use lowercase and no space.
6. In the **Description** field, add a description.
7. In the **Logs** section, select one of these:
   - **On**
   - **Off**
8. In the **Inbound query forwarding** section, select **On**.
9. In the **Alternate DNS servers** section, from the **Networks list**, select all desired networks.
10. Click **Create**.

    The system generates a private IP address that you can use to configure Private DNS in SASE Administrator Portal.
11. Install Google Cloud Software Development Kit (SDK).
12. To authenticate or initialize your gcloud CLI environment, run:

    ```
    gcloud auth login
    ```

13. To create an inbound server policy for DNS, run:

    ```
    gcloud dns policies create {{NAME}} --description=
    {{DESCRIPTION}} --networks={{VPC_NETWORK_LIST}} --enable-
    inbound-forwarding
    ```

    where, `{{NAME}}` is the name for the policy, `{{DESCRIPTION}}` is the description of the policy, and `{{VPC_NETWORK_LIST}}` is the comma separated list of VPC networks (not subnets).

    For example:

    ```
    ops-vlad:~ vbekker$ gcloud dns policies create inbounddnsvlad --
    description=inboundDNSVlad --networks=vladvpc --enable-inbound-
    forwarding
    Created Policy
    [https://dns.googleapis.com/dns/v1/projects/vladgcp/policies/inbo
    unddnsvlad].
    {
      "description": "inboundDNSVlad",
      "enableInboundForwarding": true,
      "enableLogging": false,
      "id": "8199820556025819315",
      "kind": "dns#policy",
      "name": "inbounddnsvlad",
      "networks": [
        {
          "kind": "dns#policyNetwork",
          "networkUrl":
    "https://compute.googleapis.com/compute/v1/projects/vladgcp/globa
    l/networks/vladvpc"
        }
      ]
    }
    ```

14. Validate the setup by performing the successful DNS lookup from the gateway directly to the server and also to DNS forwarder.

    For example:

- Directly querying the name server:

```
vlad@vodFpGngx3:~$ dig www.vpcdnszone.com  @192.168.128.2

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.vpcdnszone.com
@192.168.128.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51251
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.vpcdnszone.com.        IN    A

;; ANSWER SECTION:
www.vpcdnszone.com.    300    IN    A    192.168.128.50

;; Query time: 161 msec
;; SERVER: 192.168.128.2#53(192.168.128.2)
;; WHEN: Fri Mar 05 00:11:01 UTC 2021
;; MSG SIZE  rcvd: 63
```

- Through local forwarder:

```
vlad@vodFpGngx3:~$ dig www.vpcdnszone.com

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.vpcdnszone.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46053
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.vpcdnszone.com.         IN    A

;; ANSWER SECTION:
www.vpcdnszone.com.    300    IN    A    192.168.128.50

;; Query time: 156 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 05 01:38:15 UTC 2021
;; MSG SIZE  rcvd: 70
```

15. Enable Private DNS on the network in SASE Administration Guide. For more information on how to enable, see Private DNS.

Heroku Enterprise

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Configuration Steps

After you obtain your private Check Point SASE gateway, to set up a VPN gateway for the Private Space, run:

```
* Shell
```

```
Copy ```
heroku spaces:vpn:connect \
```

```
     --name   perimeter81 \   --ip   PUBLIC_IP_OF_YOUR_VPN_GATEWAY
\   --cidrs     '10.255.248.0/21'   \   --space   SPACE
```

Setting up the gateway takes a few minutes. Run the `Wait` command to wait for the gateway to be ready:

```
* Shell

Copy ```
heroku   spaces  :vpn  :wait   --space    SPACE   perimeter81
```

When the gateway is ready, to get the configuration, run:

```
* Shell

Copy ```
heroku   spaces  :vpn  :info   --space    SPACE   perimeter81
```

The above command returns a table that contains all the details you need to configure Check Point SASE.

Sample output:

```
* Text
Copy ```
heroku spaces:vpn:info --space SPACE perimeter81
=== SPACE VPNs
VPN Tunnel  Customer Gateway  VPN Gateway    Pre-shared Key
Routable Subnets  IKE Version
_________  _________________  _____________ _______________
_________________  ___________
Tunnel 1 52.91.173.226 34.203.187.158 abcdef12345     10.0.0.0 /16 1
Tunnel 2 52.91.173.226 34.227.70.143 123456abcdef    10.0.0.0 /16 1
```

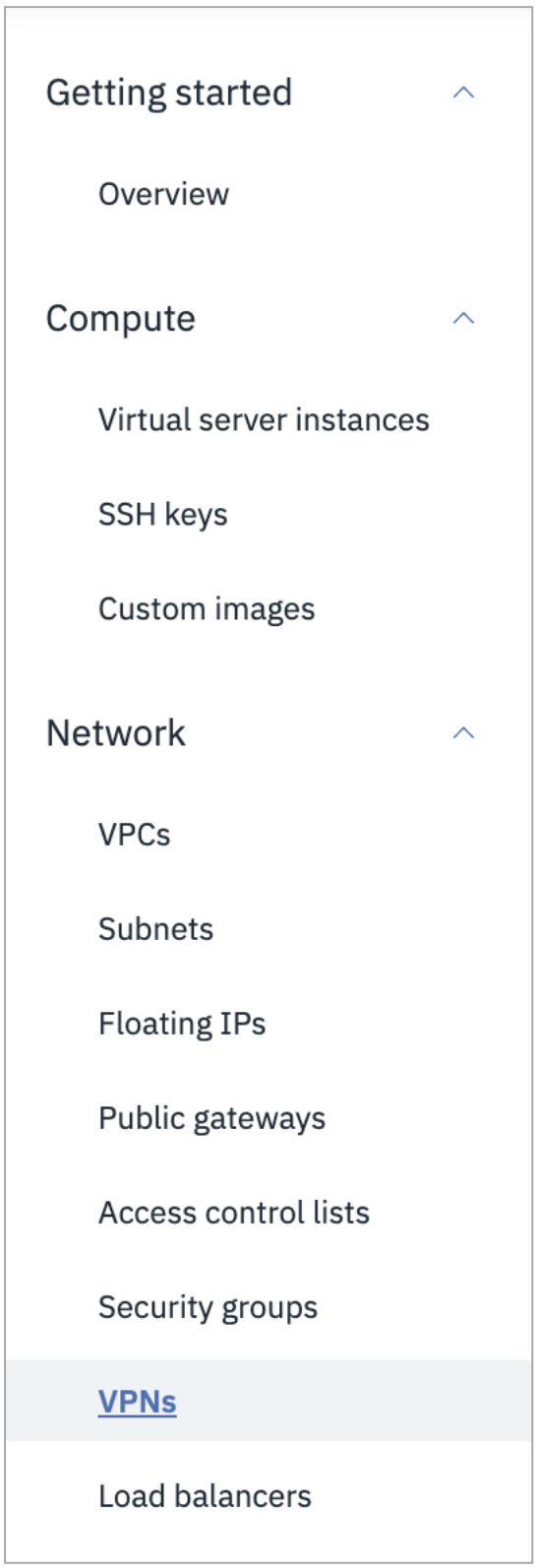
IBM Cloud

Prerequisites

- An active Check Point SASE Administrator Portal account and network.
- Make sure you have installed the Check Point SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

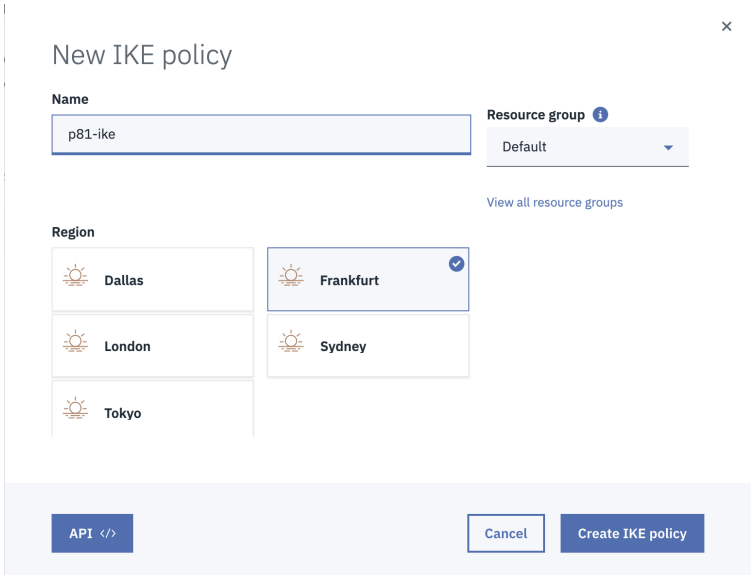
Step 1 - Configuring a VPN Gateway at the IBM Cloud Console

1. Access the IBM Cloud Console and open the **VPC** section and go to **Network** > **VPNs**.



2. Go to the **IKE policies** tab and click **New IKE policy**.

3. The **New IKE policy** window appears.

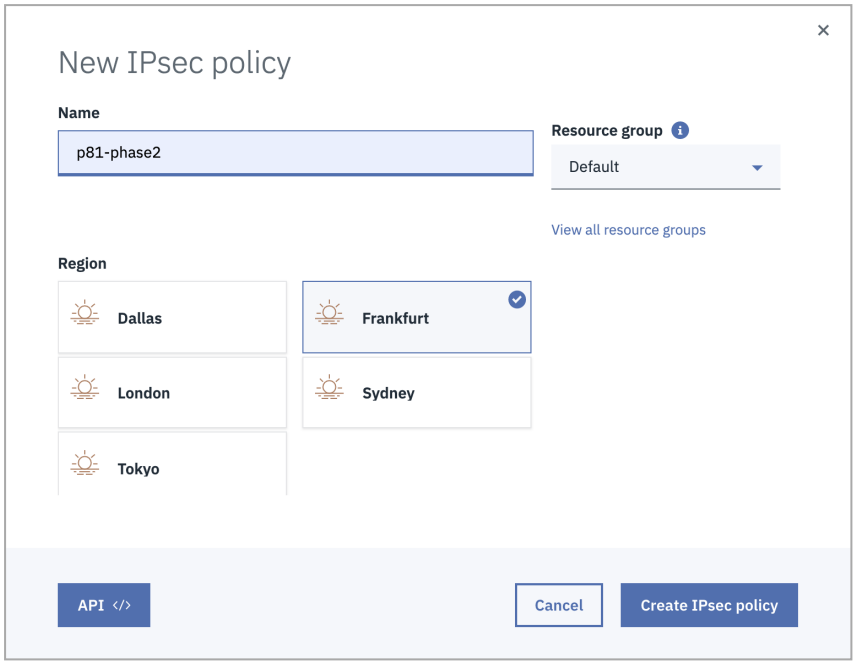


4. Enter these:
   a. **Name** - Name of the policy.
   b. **Resource group**
   c. **Region** - Region in which the VPC is located.
5. Click **Create IKE policy**.

   The system creates the IKE policy.
6. Click ··· and then **Edit**.
7. Enter these:
   a. **IKE Version** - 1
   b. **DH Group** - 2
   c. **Authentication** - sha256
   d. **Key Lifetime** - 28800
   e. **Encryption** - aes256
8. Click **Save IKE policy**.

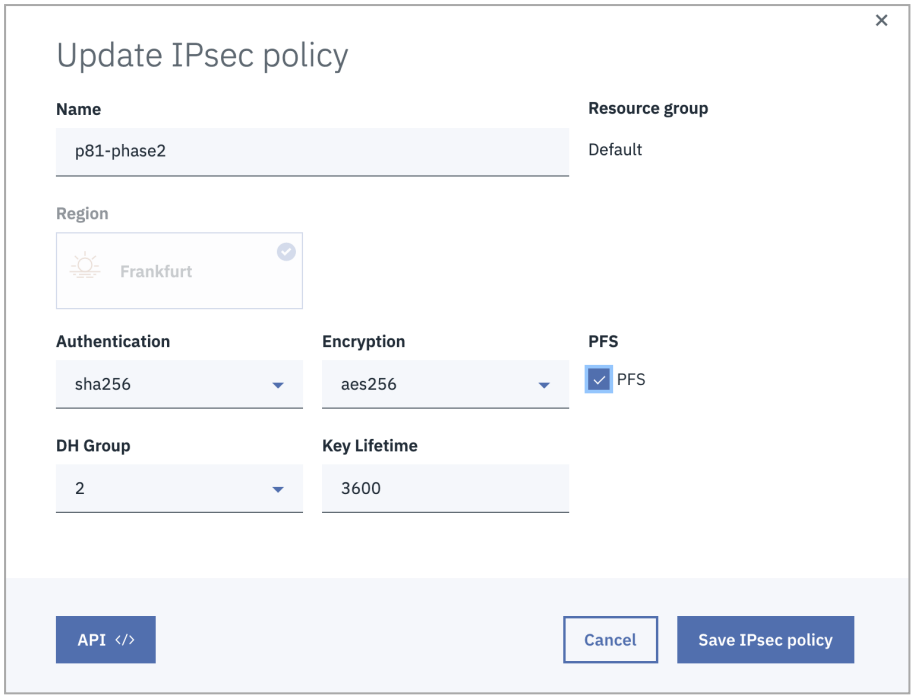
9. Go to the **IPSec Policies** tab and click **New IPSec Policy**.

   The **New IPSec policy** window appears.



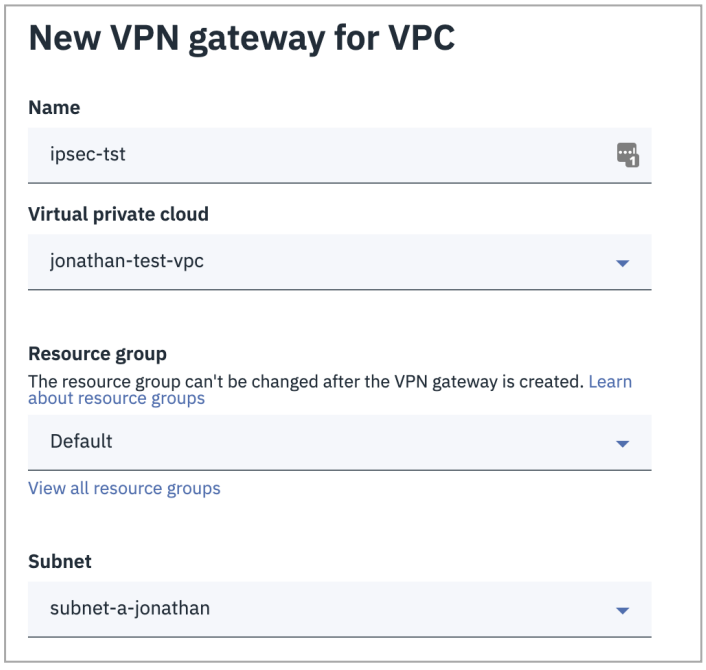
10. Enter these:
    a. **Name** - Name of the policy.
    b. **Resource group**
    c. **Region** - Region in which the VPC is located.
11. Click **Create IPSec policy**.

    The system creates the IPSec policy.
12. Click ··· and then **Edit**.
13. Enter these:
    a. **Authentication** - sha256
    b. **Encryption** - aes256
    c. **PFS** - Select the checkbox.
    d. **DH Group** - 2
    e. **Key Lifetime** - 3600
14. Click **Save IPSec policy**.



15. Go to the **VPN gateways** tab and click **New VPN gateway**.

    The **New VPN gateway for VPC** window appears.



16. Enter these:

    a. **Name** - Name of the VPN gateway.

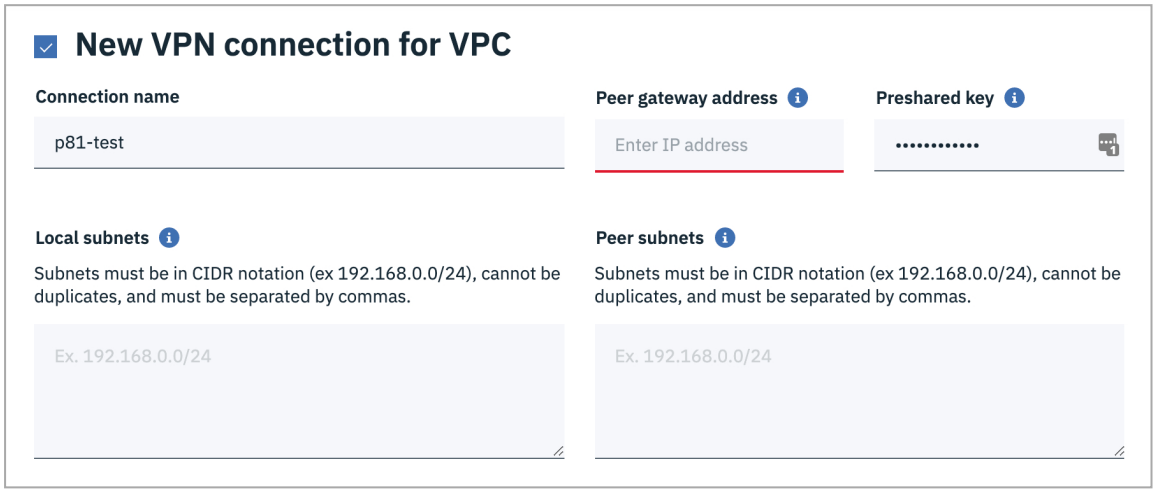
    b. **Virtual private cloud** - Select the required cloud.

c. **Resource group** - Select the resource group.

d. **Subnet** - Select the required subnet.

17. Select **New VPN Connection for VPC**.

The **New VPN connection for VPC** window appears.



18. Enter these:

a. **Connection name** - Name of the VPN connection.

b. **Peer gateway address** - IP address of your Check Point SASE gateway.

c. **Preshared key** - A string with at least 8 characters that contains upper-case letters and numbers.

d. **Local subnets** - Specify one or more subnets in the VPC you want to connect.

e. **Peer subnets** - 10.255.0.0/16 (Unless you have custom configurations or multiple tunnels to the same Check Point SASE gateway).

f. **Dead peer detection action** - Restart

g. **Interval** - 10 seconds

h. **Timeout** - 30 seconds

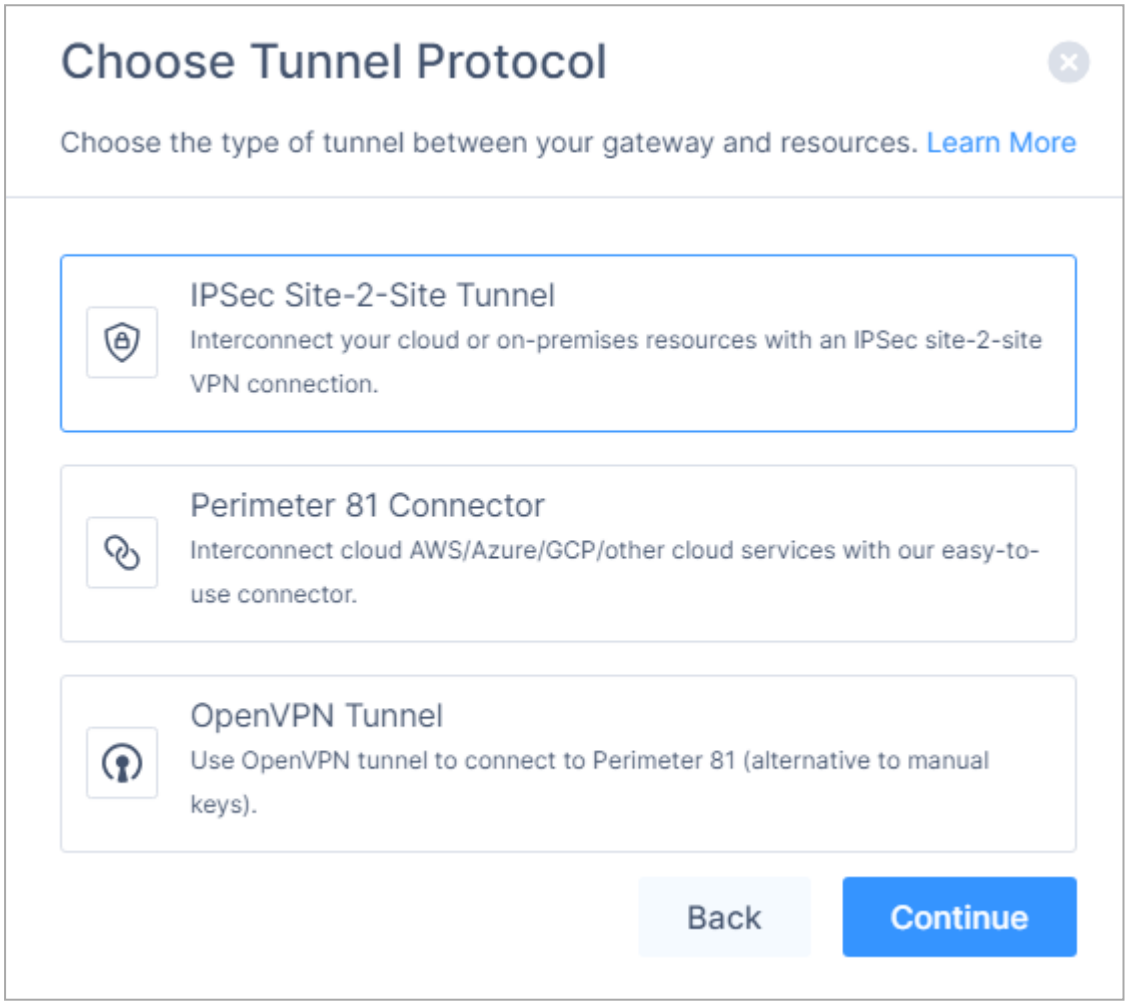
i. **IKE policy** - Select the IKE policy created earlier.

j. **IPSec policy** - Select the IPSec policy created earlier.

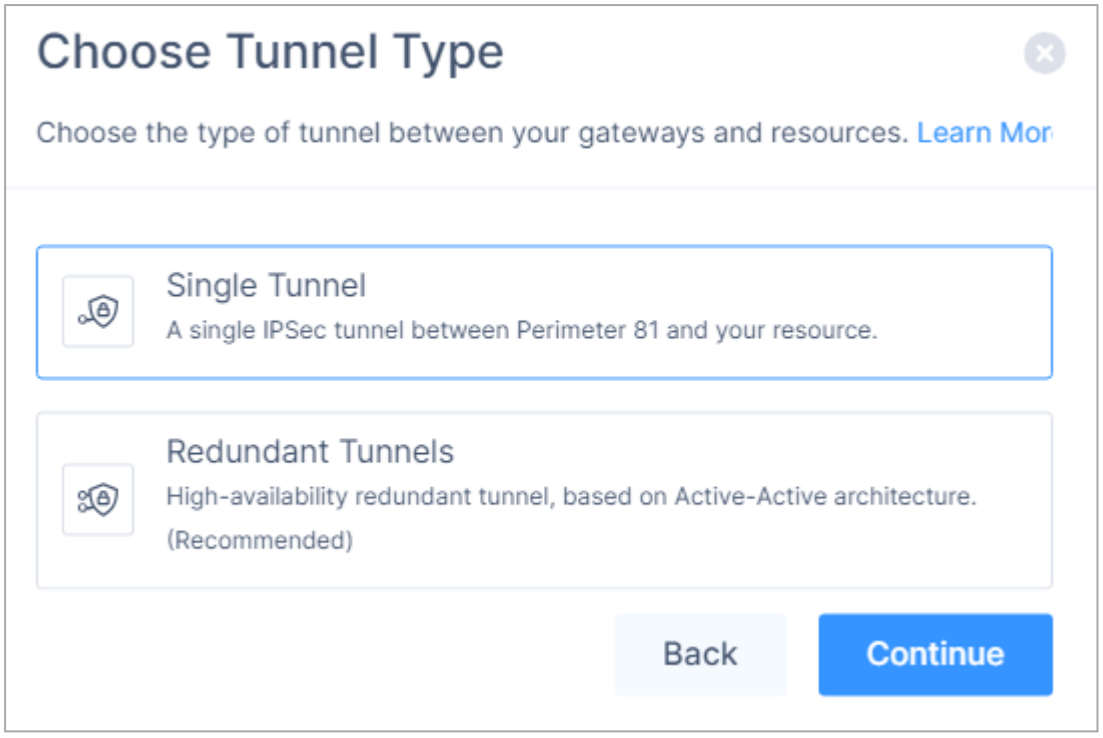
Step 2 - Creating the Tunnel in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

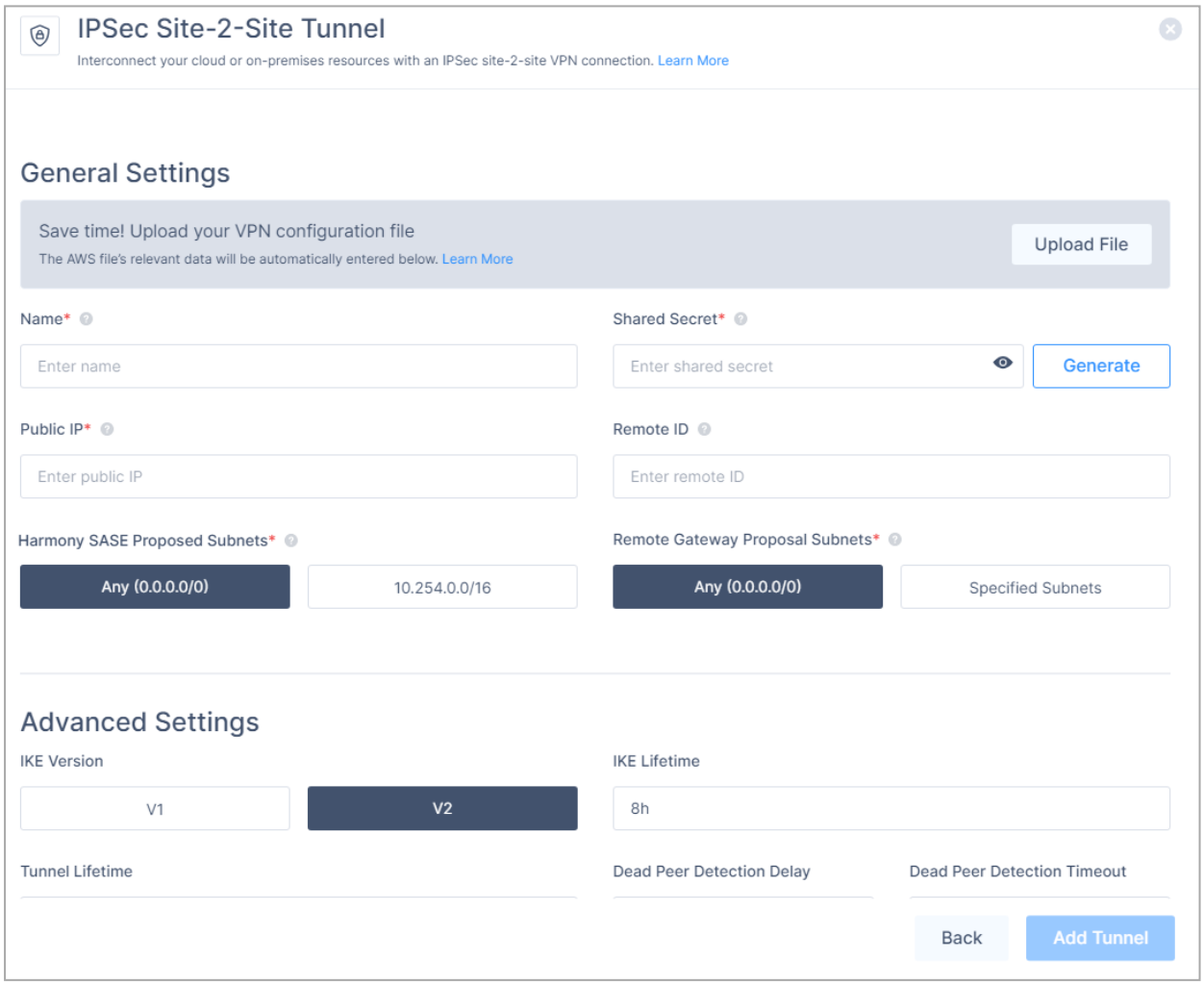
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
   a. **Name** - Name of the tunnel.
   b. **Public IP** - IP address of the VPN Gateway defined in the IBM Cloud console.
   c. **Remote ID** - Identical to Remote IP.
   d. **Shared Secret** - Preshared key in the IBM Cloud console.
   e. **Perimeter 81 Gateway Proposal Subnets** - 10.255.0.0/16 or the value defined in the IBM Cloud console.
   f. **Remote Gateway Proposal Subnets** - Subnets in the VPC that you want to connect.
7. In the **Advanced Settings** section, enter the information for your tunnel type:

Field Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	ecp521	ecp521
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	modp1024	modp1024
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024

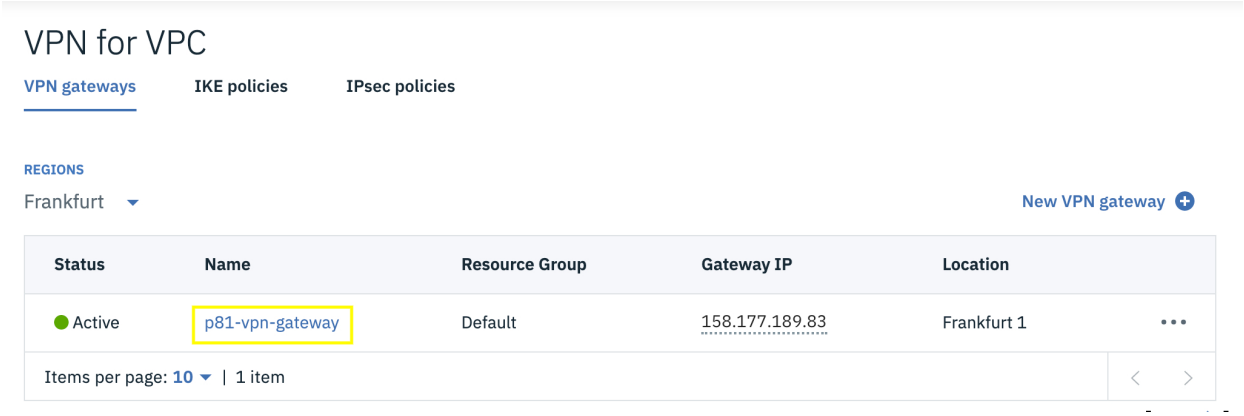
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	modp2048	modp2048
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	modp1024	modp1024
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	ecp521	ecp521

[1] Suggested values. For other supported ciphers, see this Google article.

8. Click **Add Tunnel**.

Verifying the Setup in IBM Cloud Console

1. Access the IBM Cloud console and go to the **VPN gateways** tab.
2. Select the name of the VPN Gateway associated with the tunnel.



3. Scroll down and click **View all connections**.

   Verify whether the tunnel **Status** as active.

Verifying the Setup

1. In the Check Point SASE Administrator Portal, click **Networks** and verify that the tunnel is up.
2. In the Check Point SASE Agent, connect to the network and access a resource. If you are unable to connect to the resource, contact *Check Point Support*.

Private Access

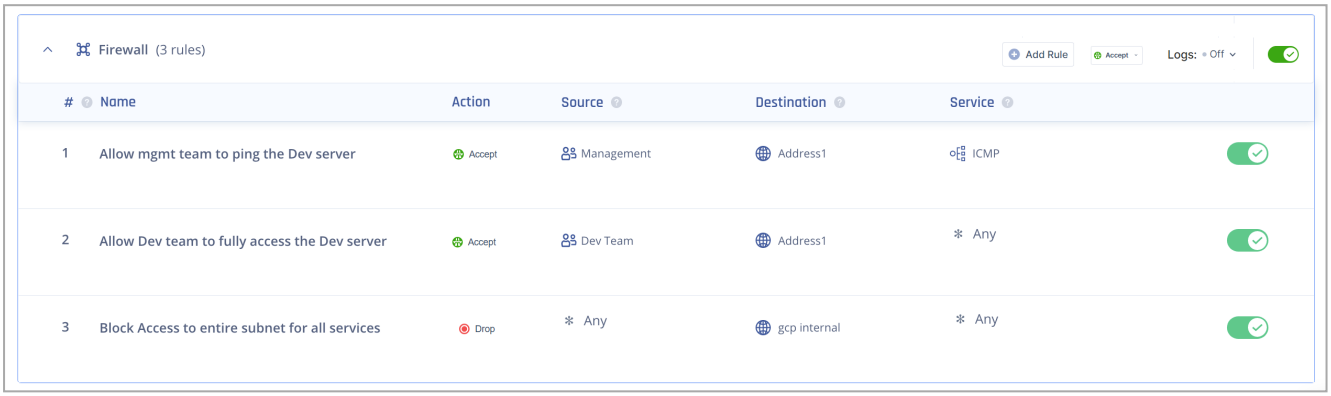
Private Access allows you to:

- Create firewall rules for your network.
- Define applications for Zero Trust Access.
- Create policies for application access.

Firewall

The **Firewall** page allows you to create access rules for your network.

To view the **Firewall** page, access the Check Point SASE Administrator Portal and click **Private Access** > **Firewall**.



Note - Contact your account manager to request firewall logging functionality.

Use Case

- Create rules for specific user groups, resources, and protocols. For example, deny access to the management user group to a certain resource if accessed through the Internet Control Message Protocol (ICMP).
- Create a comprehensive rule for the entire network traffic. For example, block all traffic on a specific port.

Prerequisite

Define your network with IPSec or Check Point SASE Connector tunnel. See *"Adding a Tunnel" on page 198*.

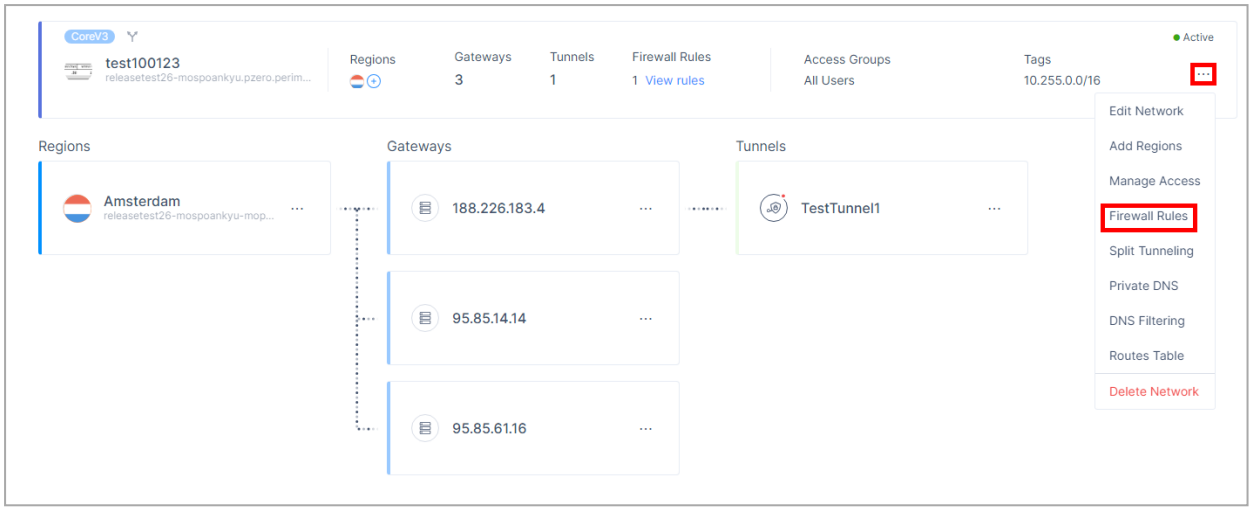
Access Rules Order

The order of the rules indicate the sequence in which the system checks and applies the rules. For example, if a user tries to access a resource, then the system first checks if the traffic matches rule #1. If it does, it applies the rule. Otherwise, the system checks if the traffic matches rule #2, and so on. If none of the rules match, then the system applies the default rule.

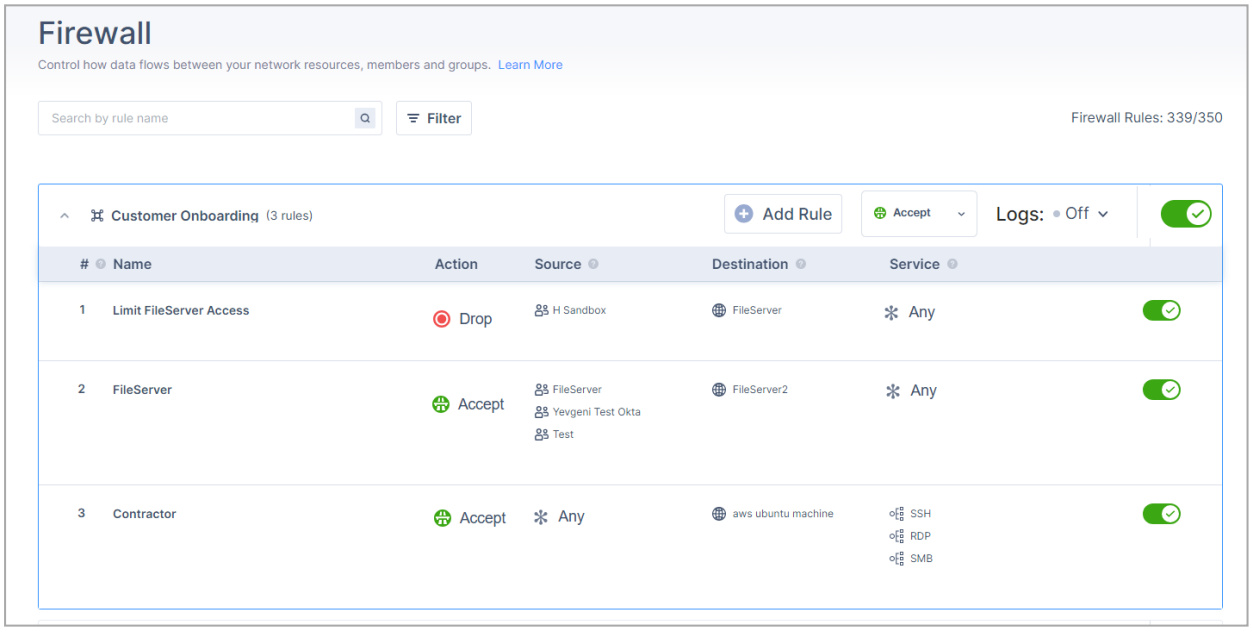
Creating a Firewall Access Rule

1. Access the Check Point SASE Administrator Portal and click **Networks**.
2. Select the network for which you want to create firewall access rules.

3. Click ··· and then click **Firewall Rules**.

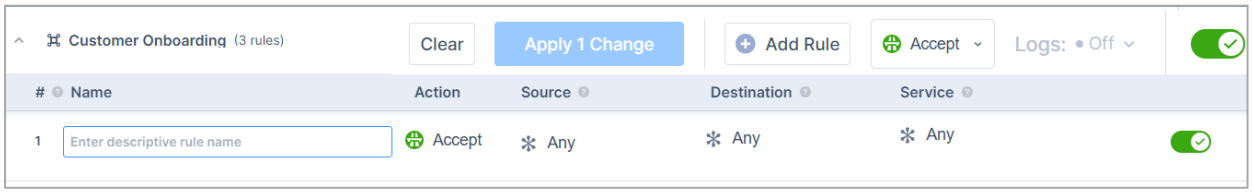


The **Firewall** page appears.



4. Click **Add Rule**.

The system places the new rule at the top, and it is enabled by default.



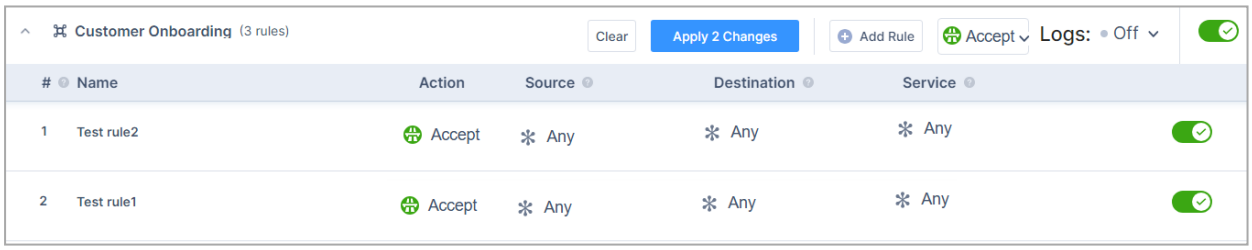
5. In the **Name** field, enter a name that describes the rule.
6. From the **Action** list, select the action type:

- **Allow**
- **Deny**

7. In the **Source** field, click **Add Source** and select the traffic source for this rule.
8. In the **Destination** field, click **Add Destination** and select the traffic destination for this rule.

   Note - The **Source** and **Destination** define the conditions for the **Action** to be applied to the traffic.
   You can specify three types of objects in the **Source** and **Destination** fields:
   - **Any** - All traffic (any address or member).
   - **Groups or Members** - All traffic routed from/to a specific member or member group.
   - **Addresses** - Traffic routed from/to an FQDN, IP address, subnet, or list of IP addresses.

9. In the **Service** field, select one of these:
   - **Any** - Traffic routed on all protocols and ports.
   - **Services** - Traffic routed on a specific protocol or port.
10. Drag the rule and place it in required position in the order.
11. Click **Apply Changes**.



   The **Apply Changes** window appears.

12. Click **Apply**.

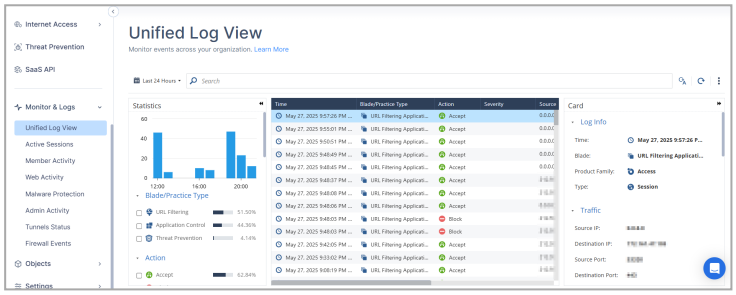
Enabling or Disabling Firewall Logs

1. Access the SASE Administrator Portal and go to **Private Access** > **Firewall**.
2. For the network you want to enable or disable blocked firewall logs, from the **Logs** list, select one of these:
   - **Enable** - On

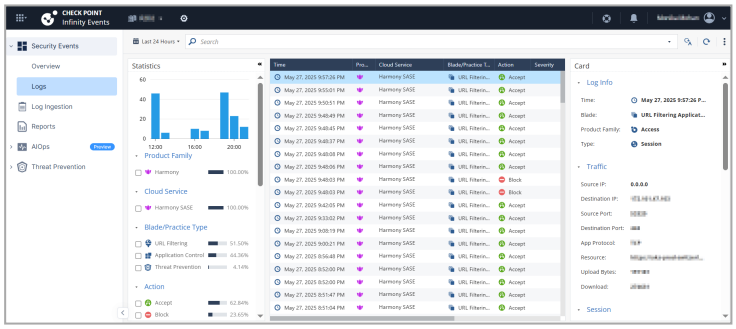
- **Disable** - Off

Notes :

- To enable firewall logs, contact *Check Point Support*.
- To view the logged events, do either of these:
  - Go to **Monitor & Logs** > **Unified Log View**.



  - Access the **Infinity Events** Administrator Portal, and click **Logs**.



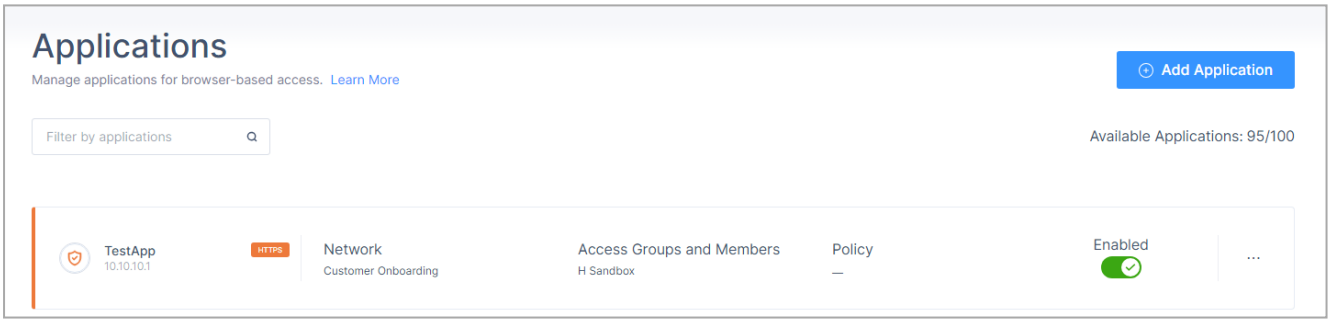
Applications

The **Applications** page allows to you add your web-applications and offer an agent-less access to these applications through customized protocols.

The supported application protocols are:

Protocol	Sample Application
HTTP/HTTPS	Bitbucket
RDP	My Desktop
SSH	Staging Web Server
VNC	Build PC

To view the **Applications** page, access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.



Use Case

You want to provide agentless access only to specific applications for members or third-party users with official devices or BYOD in your organization.

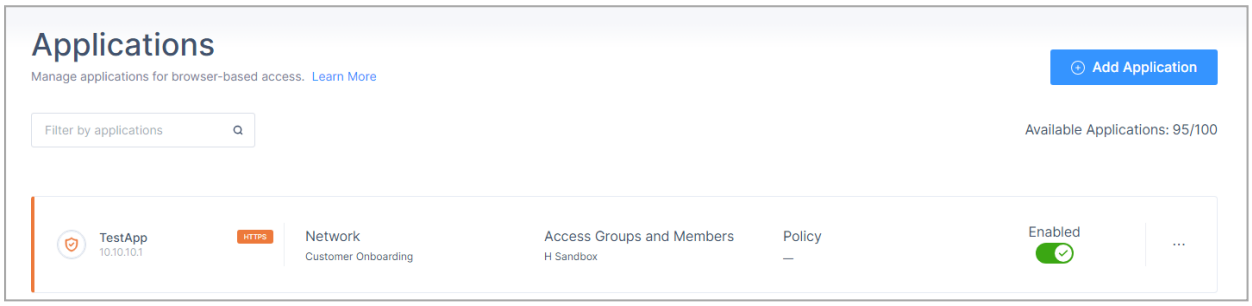
Note - To provide secure access for public SaaS applications, such as Microsoft Office 365, Gmail and so on, use the Check Point SASE Agent.

Prerequisites

1. Define your network with IPSec or Check Point SASE Connector tunnel. See *"Networks" on page 156*.
2. Verify that the application is accessible through the Check Point SASE Agent.

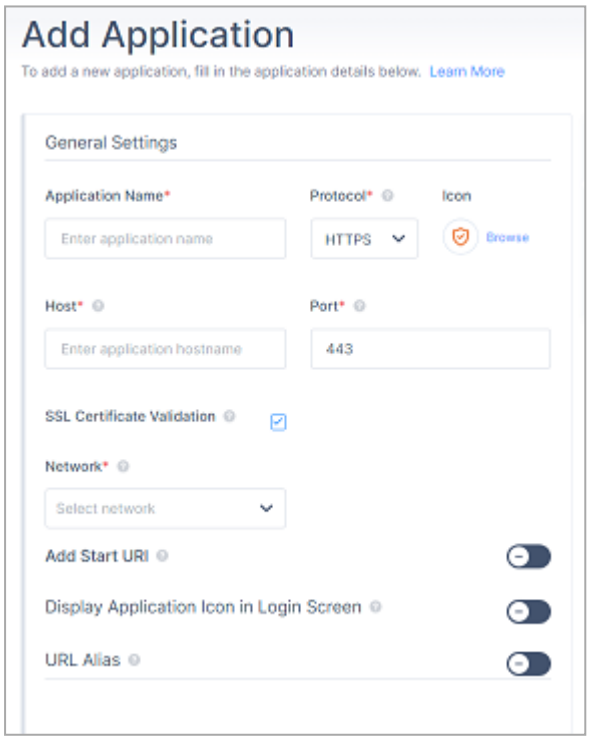
Adding an Application

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.



2. Click **Add Application**.

   The **Add application** window appears.

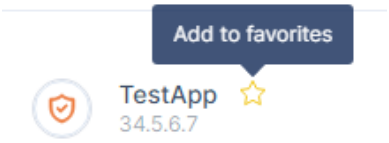


3. Select the application type:

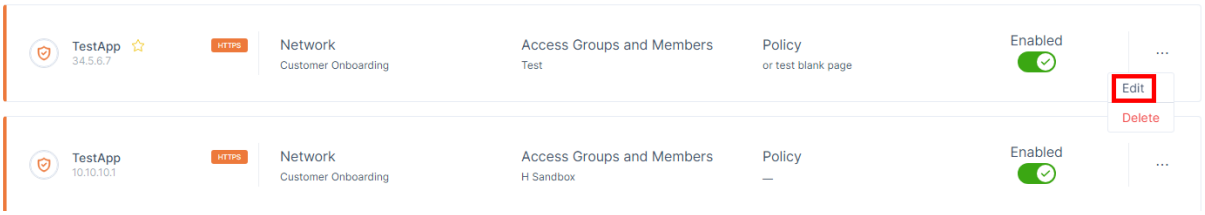
- HTTP/HTTPS application
- RDP application
- SSH application
- VNC application

After you add an application, it is enabled by default.

4. To add the application to favorites, hover over the application name and click the ☆ icon.



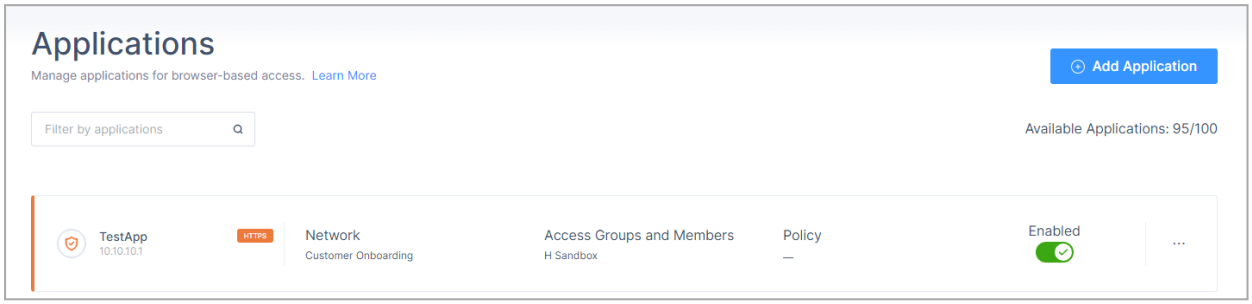
5. To edit the application details, click ··· and then click **Edit**.



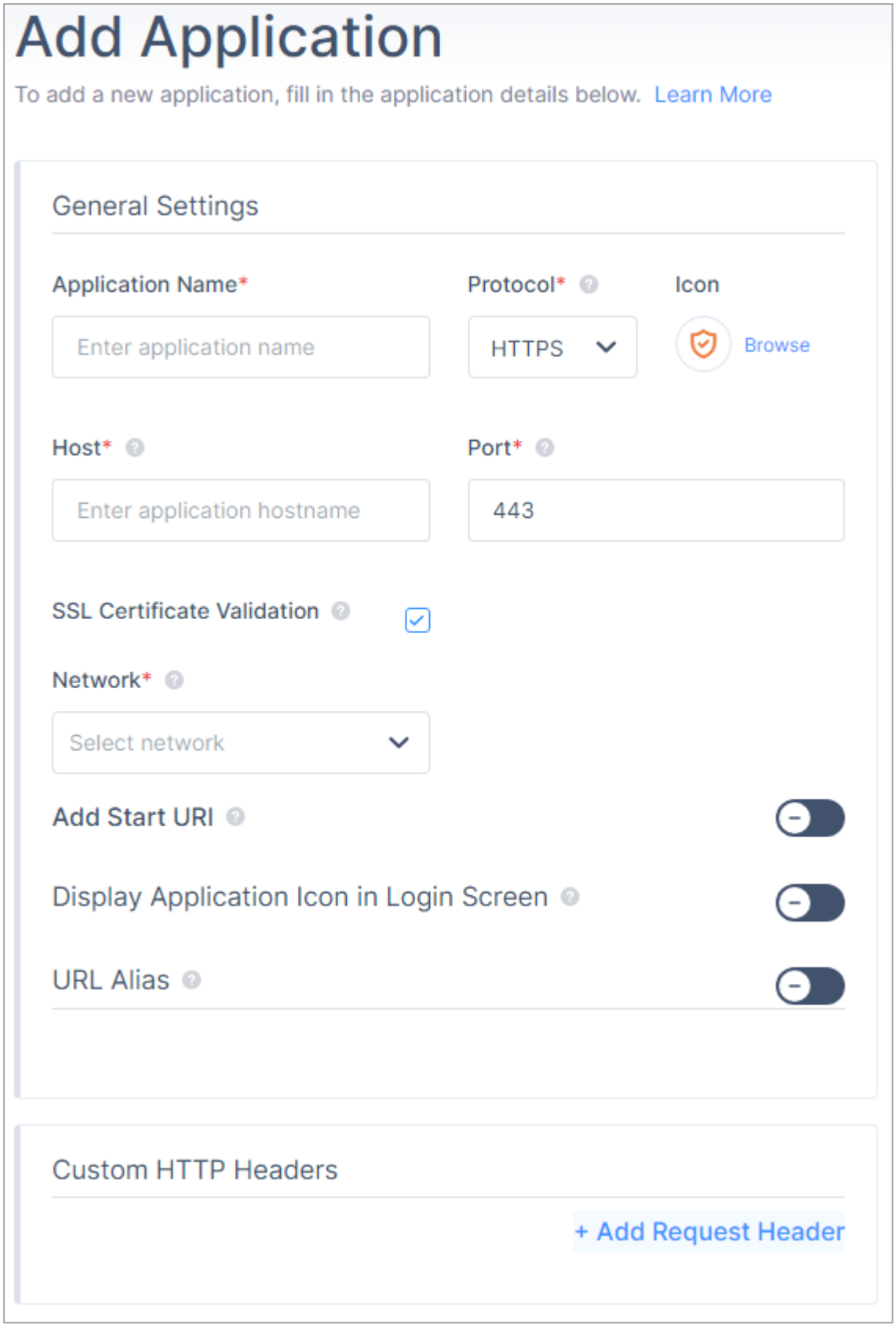
6. Make the required changes and click **Apply**.
7. For members to access the application, see *"Providing Application Access to Members" on page 768*.

Adding an HTTP/HTTPS Zero Trust Application

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.



The **Add application** window appears.



3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - HTTP or HTTPS

c. **Icon** - Icon for the application.

d. **Host** - Internal IP address of the server hosting the application. If custom DNS is configured, enter the hostname.

e. **Port** -

   - 80 for HTTP
   - 443 for HTTPS

f. (HTTPS Only) **SSL Certificate Validation** - Indicates that the application is accessible only if the application has a valid SSL certificate.

g. **Network** - Network that hosts the application.

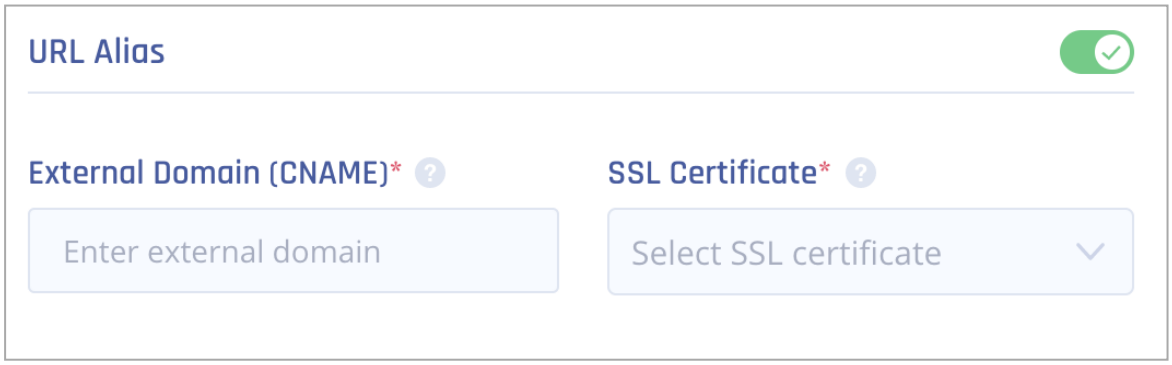
h. (Optional) **Add Start URI** - Subpath to which the system must redirect after the member launches the application.

   For example, if a member enters *www.company.com* and if you want to be redirect to *www.company/careers*, then enter */careers*.

i. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

j. (Optional) **URL Alias** - URL for members to access the application.

   Important - You cannot add a URL alias after you create the application.

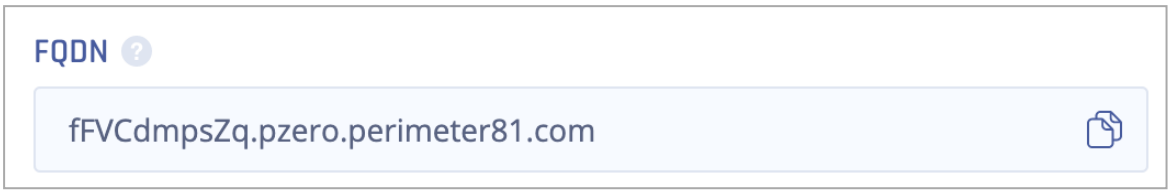


k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

l. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

m. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

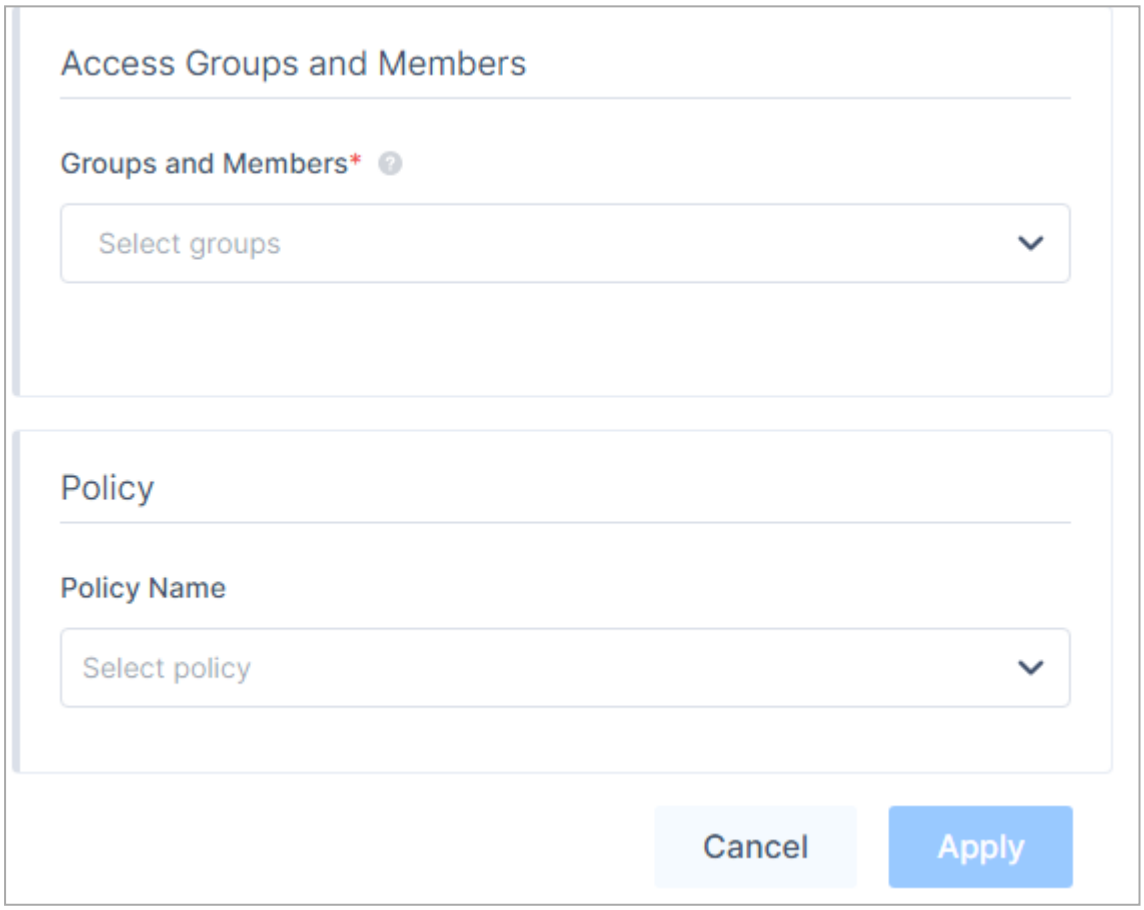
Under your domain, use the CNAME specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.



n. **Custom HTTP Headers** - Click **Add Request Header** and enter **Name** (host) and **Value** (internal FQDN).

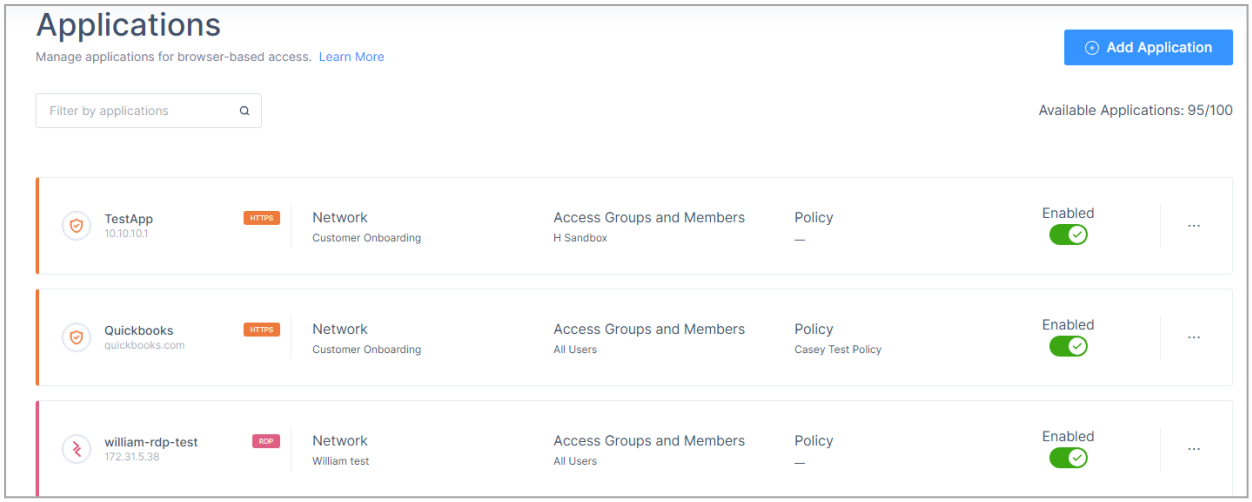
Mandatory if you have specified DNS in the **Host** field.

4. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



5. (Recommended) In the **Policy Name** list, select an application policy.
6. Click **Apply**.

The system lists the application in the **Applications** page and enables it by default.



7. For members to access the application, see *"Providing Application Access to Members" on page 768*.

Adding an RDP Zero Trust Application

SASE allows you to create an RDP Zero Trust Application (ZTA) as either:

- Web Client Type - A browser-based solution providing convenient and quick remote desktop access without installation.
- Native Client Type - A locally installed application offering robust performance and advanced features for remote desktop access.

For networks created or upgraded after September 2024, the administrators can configure a property in the IdP Attribute for Host and/or Port fields, that allows each member to access the dedicated RDP server. For more information, see *"RDP Server Access Based on IdP" on page 755*.

Prerequisite

Make sure you have the credentials to access the application over RDP.

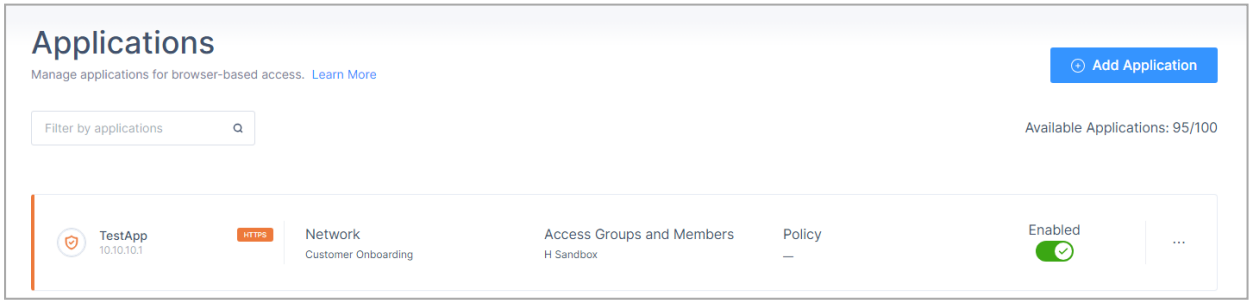
Known Limitation

Native applications launched directly from the Check Point Portal Applications Management page might disconnect after a few minutes. To avoid this issue, launch them from Access for Members.

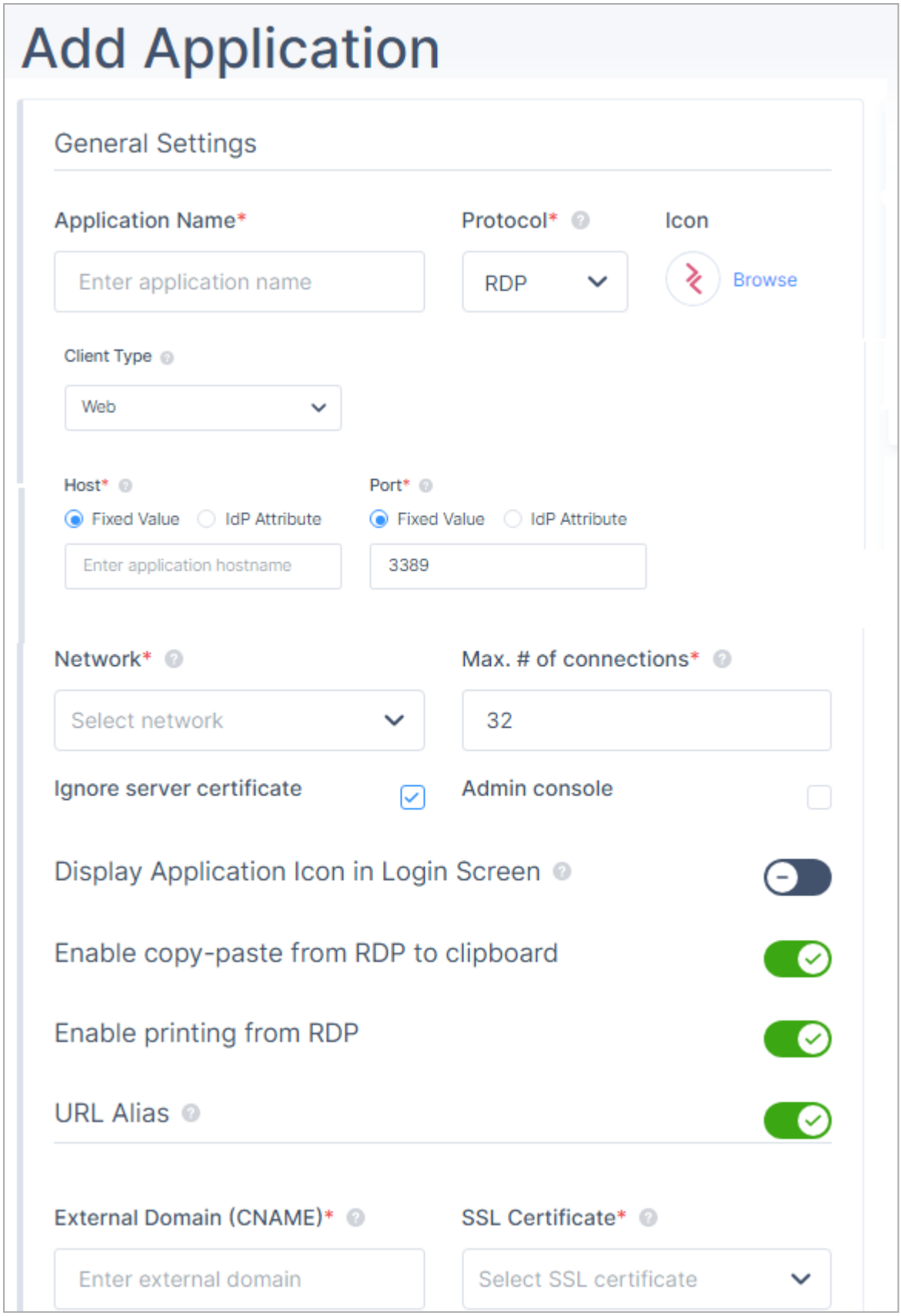
Adding an RDP ZTA

To add an RDP Zero Trust Application:

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.



The **Add application** window appears.



3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - RDP

c. **Icon** - Icon for the application.

d. **Client Type** - Select one of these:

   - **Web**
   - **Native**

   Note - For Native Client Type, these are the supported clients: Windows 10, Windows 11, Android, iOS, Mac, with latest MSTSC or MSRDC applications from Microsoft.

e. **Host** - Internal IP address of the server to which you want to connect. Select one of these and enter the value:

   - **Fixed Value** - A predefined, unchanging value set by the administrator.
   - **IdP Attribute** - Information provided by the Identity Provider during user authentication. For more information, see *"RDP Server Access Based on IdP" on page 755*.

   Notes:
   - IdP Attribute:
     - This feature is available only for networks created after September 2024. To use it for existing networks, contact *Check Point Support*.
     - This feature is supported only for Active Directory/LDAP and Azure Active Directory IdPs.
     - The administrator must store the hostname and/or port number in the IdP for each member.

f. **Port** - Select one of these and enter the value:

   - **Fixed Value** - 3389
   - **IdP Attribute**

g. **Network** - Network that hosts the application.

h. **Max number of connections** - Maximum number of concurrent RDP sessions.

   Note - Disabled when you select **Client Type** as **Native**.

i. **Ignore server certificate** - Select **Yes** to ignore the SSL certificate, unless you activate RDP over SSL.

j. **Admin console** - Select the checkbox to connect directly to the console session on the Windows server.

k. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

Note - Disabled when you select **Client Type** as **Native**.

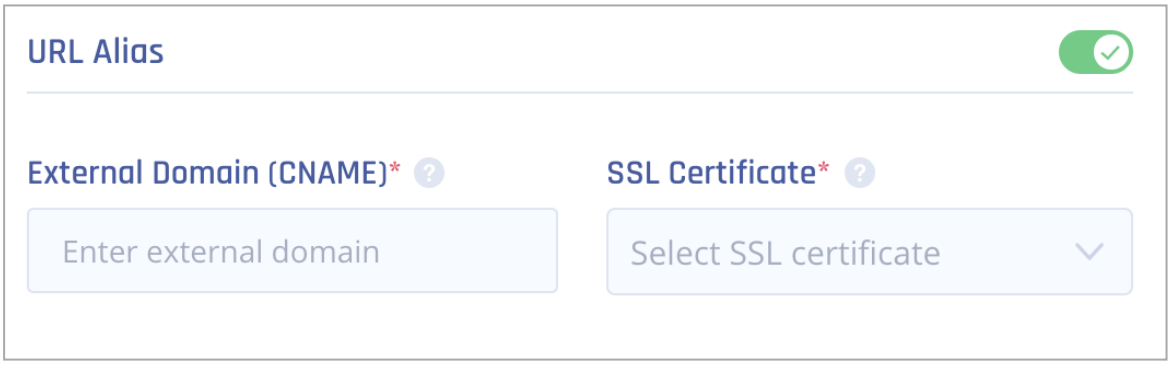
l. (Optional) **Enable copy-paste from RDP to clipboard** - Enables to copy data from RDP to clipboard.

m. (Optional) **Enable printing from RDP** - Enables to print data from RDP.

- Native RDP - Once enabled, the user's local printer should appear in the list of available printers in addition to the remote printers on the remote site.
- Web RDP - Once enabled, the **Perimeter81 VirtualPrinter** printer appears in the list of available printers and lets you download a PDF file to the user's machine that can be printed using the user's local printer.

n. (Optional) **URL Alias** - URL for members to access the application.

Important - You cannot add a URL alias after you create the application.

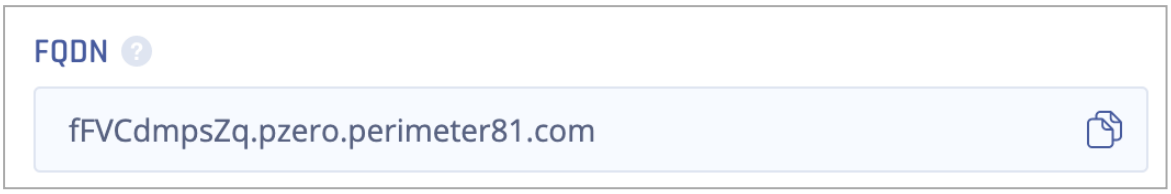


o. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

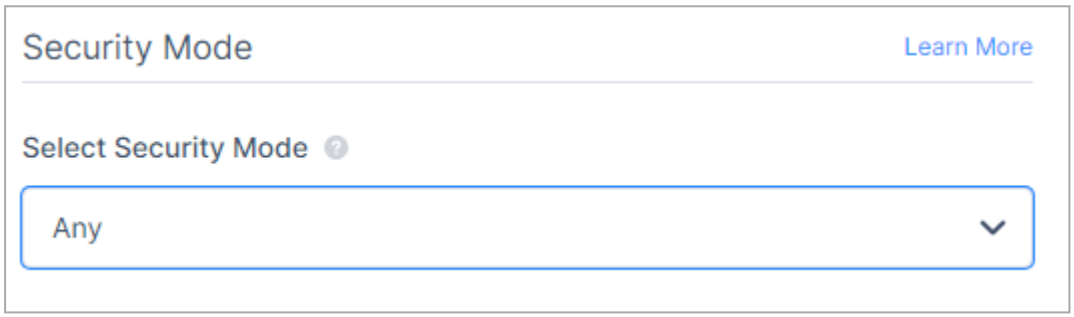
p. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

q. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CNAME specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.



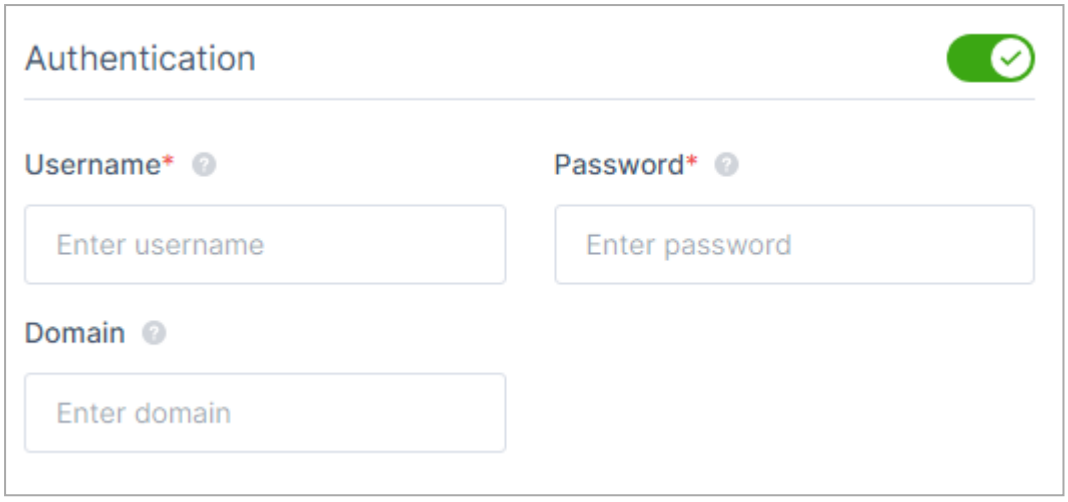
4. From the **Select Security Mode** list, select a security mode. It indicates the encryption and authentication mode.



- **Any** (default) - Select the security mode automatically based on the security protocols supported by the client and the server.
- **Network Level Authentication (NLA)** - Uses the TLS encryption and requires credentials to access the application. Also referred to as hybrid or CredSSP (the protocol that drives NLA).
- **Extended Network Level Authentication (NLA-EXT)** - Sends Early User Authorization Result from the server to the client after the NLA handshake.
- **Transport Layer Security (TLS)** - RDP authentication and encryption through TLS (RDPTLS). This is suitable for load balancing where the primary RDP server redirects the connection to secondary servers.
- **VMconnect** - Selects a security mode supported by Hyper-V or VMConnect automatically based on the supported protocol by client and server.
- **Remote Desktop Protocol (RDP)** - Suitable for machines running old Windows version where a login screen is required.

Note - Disabled when you select **Client Type** as **Native**.

5. In the **Authentication** section, enter these:



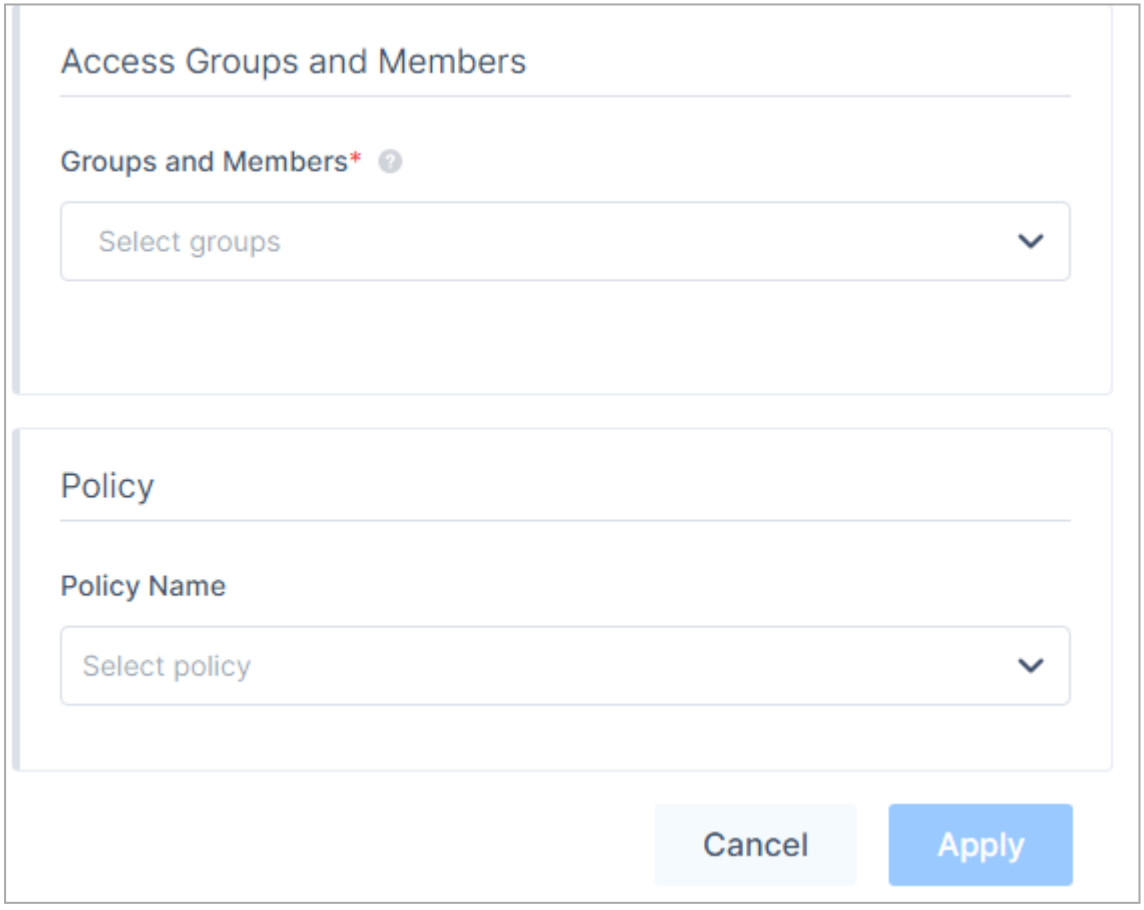
a. **Username** and **Password** - Server credentials.

b. **Domain** - Your active directory FQDN.

Notes:

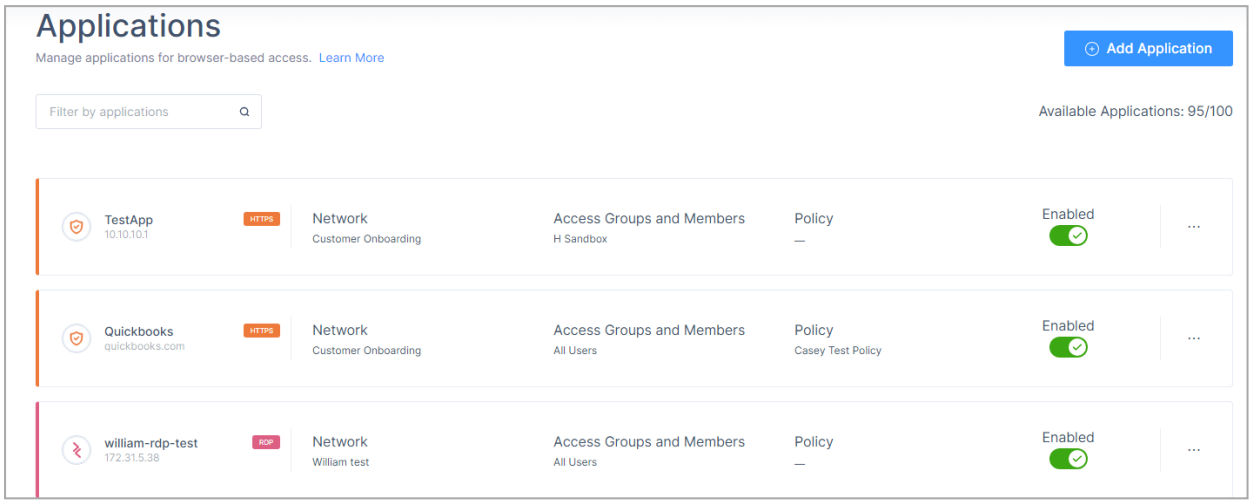
- If you disable **Authentication**, then the member must enter the credentials when accessing the application.
- This section is disabled when you select **Client Type** as **Native**.

6. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



7. (Recommended) In the **Policy Name** list, select an application policy.
8. Click **Apply**.

   The system lists the application in the **Applications** page and enables it by default.



9. For members to access the application, see *"Providing Application Access to Members" on page 768*.

RDP Server Access Based on IdP

For the RDP Zero Trust Application, the administrators can configure a property in the IdP Attribute for Host and/or Port fields, that allows each member to access the dedicated RDP server.

Notes:

- Hostname must be an IP address or Fully Qualified Domain Name(FQDN).
- The administrator must store the hostname and/or port number in the IdP to redirect the member to the appropriate RDP server.
- For the list of supported IdP Attribute properties, see Microsoft Graph User Properties.
- Custom properties are not supported.
- For Azure AD, make sure to configure the Azure application to have these permissions:
  - `Directory.Read.All`
  - `User.Read`

  For more information, see *"Microsoft Entra ID (formerly Azure AD) (Enterprise Application)" on page 1050*.
- To map the AD/LDAP attributes to the property name in AD/LDAP, see Map AD/LDAP Profile Attributes to Auth0 User Profile.
- Working with Active Directory Federation Services (ADFS) is available on demand. For more information, contact *Check Point Support*.

Additional Registry Configuration

Windows 7

1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE** > **Software** > **Microsoft** > **Windows NT** > **Terminal Services**.
3. Select **fServerEnableRDP8**.
4. Set the value type to **REG_DWORD**.
5. Set the value to **1**.
6. Reboot the machine.

Windows Server 2016

1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
3. Select **SecurityLayer** and change the value to **1**.
4. Select **UserAuthentication** and change the value to **0**.

Windows Server 2019

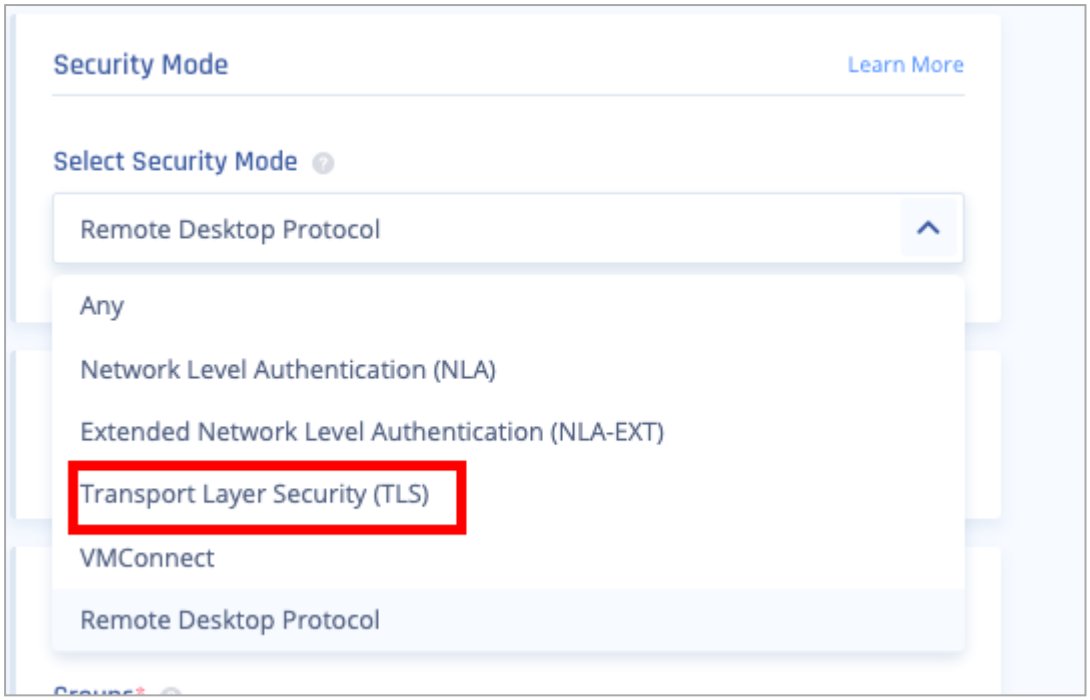
1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
3. Select **SecurityLayer** and change the value to **0**.
4. Reboot the machine.

Troubleshooting

Upstream Error

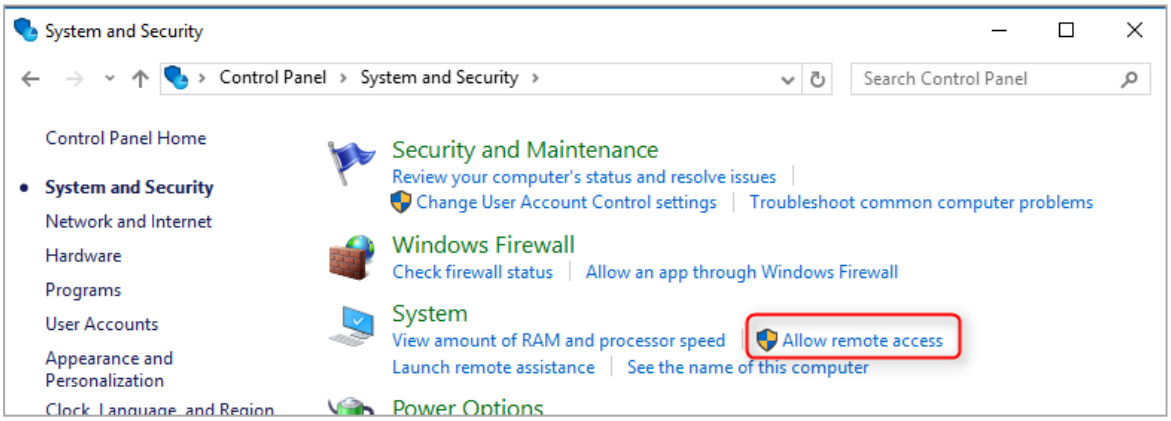
1. If **Authentication** is enabled (see Authentication), verify the credentials.

   If it is disabled, change the security mode to **Transport Layer Security (TLS)**.



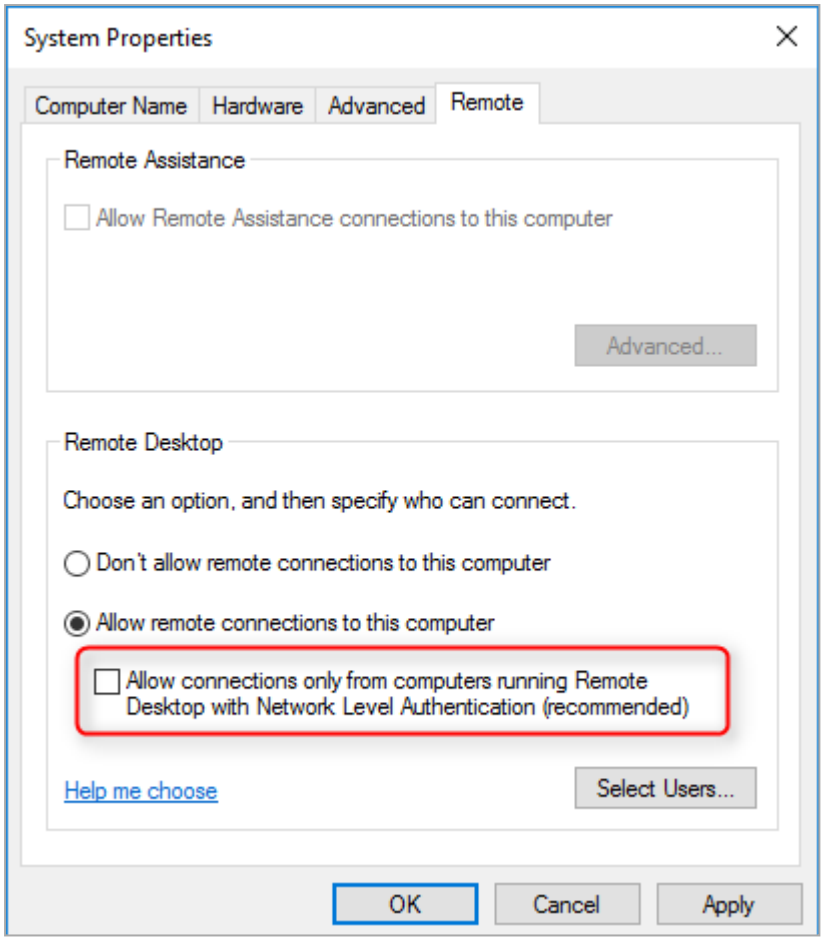
Additional Troubleshooting Steps

1. Disable NLA on the remote machine:
   a. Open the **Control Panel**.
   b. Click **System and Security** and under **System**, click **Allow remote access**.



   The **System Properties** window appears.

2. Go to the **Remote** tab and in the **Remote Desktop** section, clear the **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** checkbox.


System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply

3. Click **OK**.

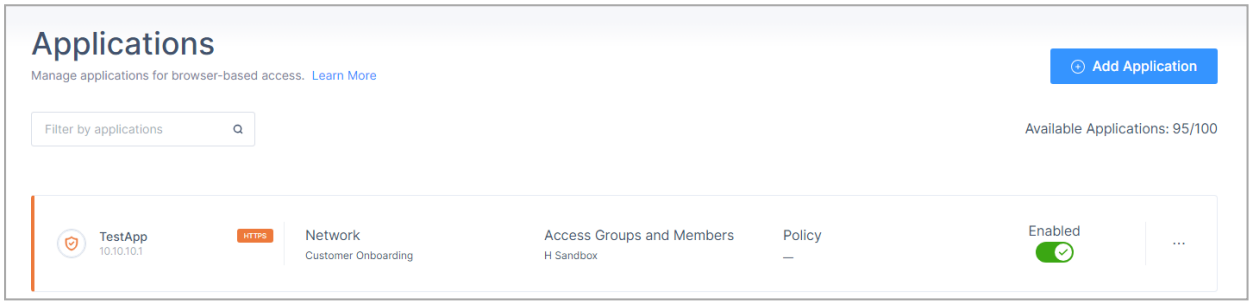
Adding a SSH Zero Trust Application

Prerequisite

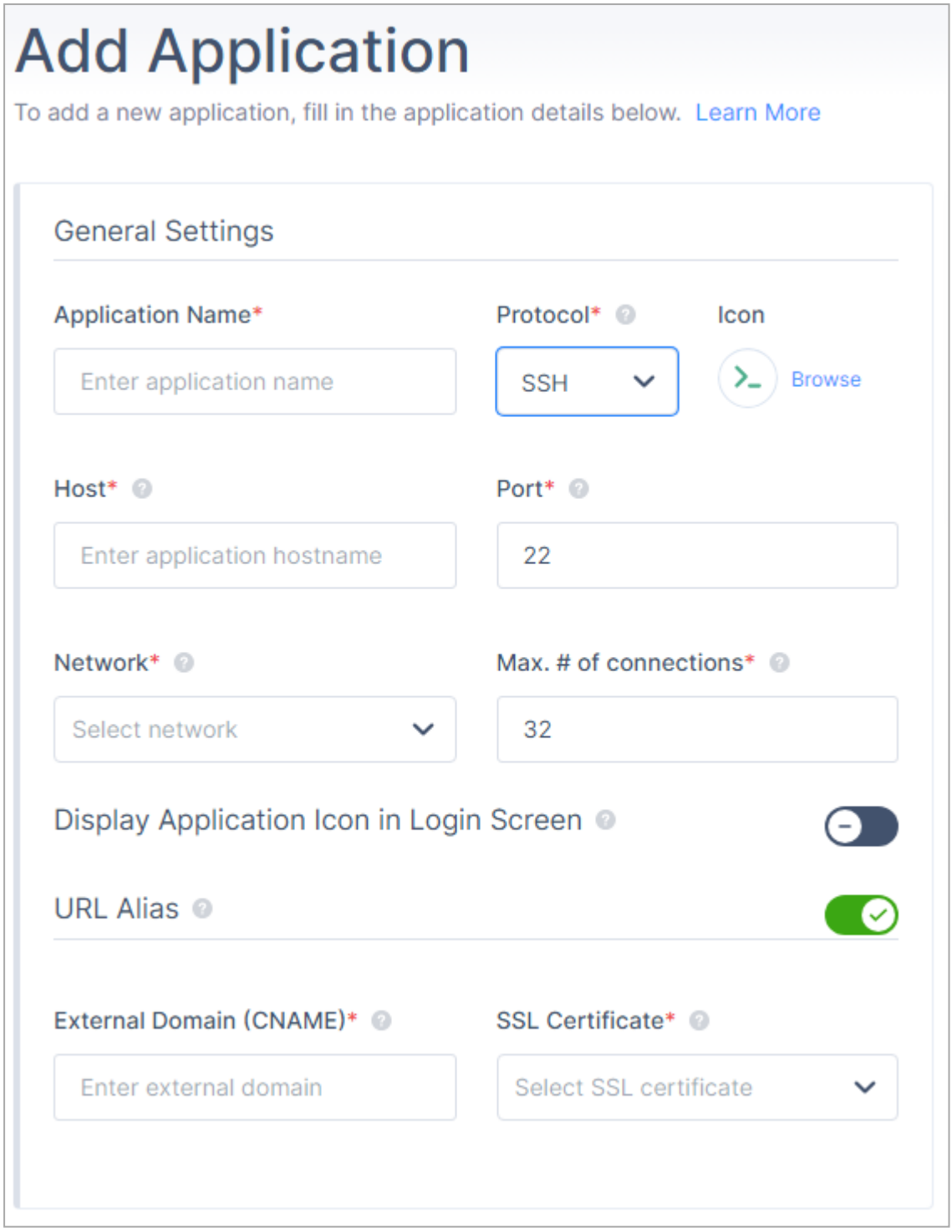
Make sure you have the credentials to access the application over SSH.

To add an SSH Zero trust Application:

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.



The **Add application** window appears.



3. In the **General Settings** section, enter these:
   a. **Application Name** - Name of the application.
   b. **Protocol** - SSH
   c. **Icon** - Icon for the application.
   d. **Host** - Internal IP address of the server to which you want to connect.

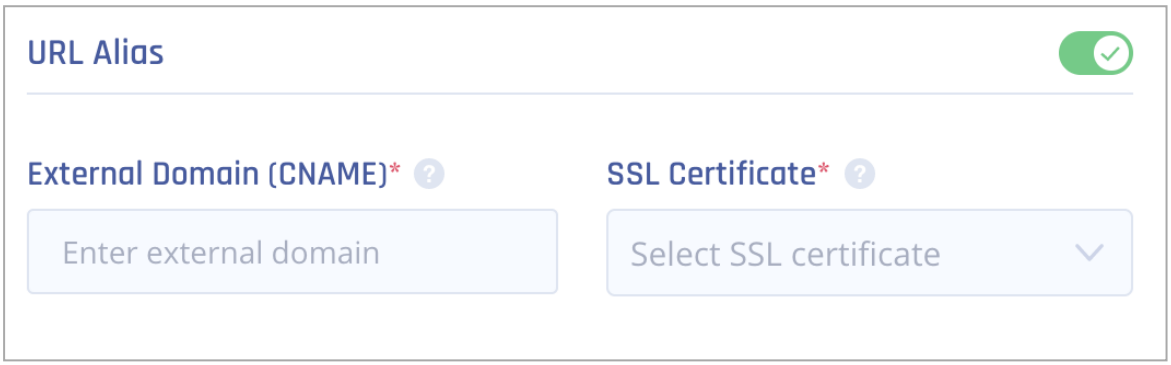
e. **Port** - 22

f. **Network** - Network that hosts the application.

g. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

h. (Optional) **URL Alias** - URL for members to access the application.

Important - You cannot add a URL alias after you create the application.

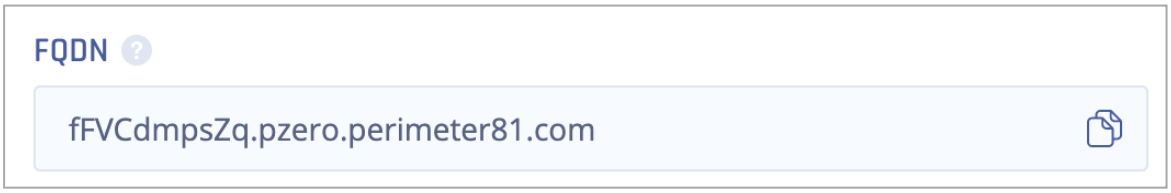


i. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

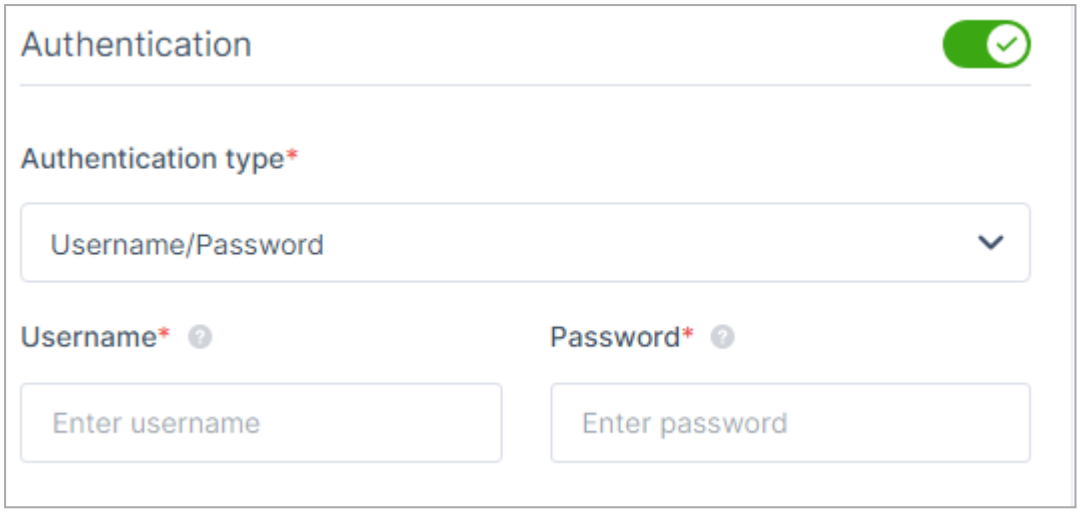
j. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

k. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CNAME specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.



4. In the **Authentication** section, select the **Authentication type**:



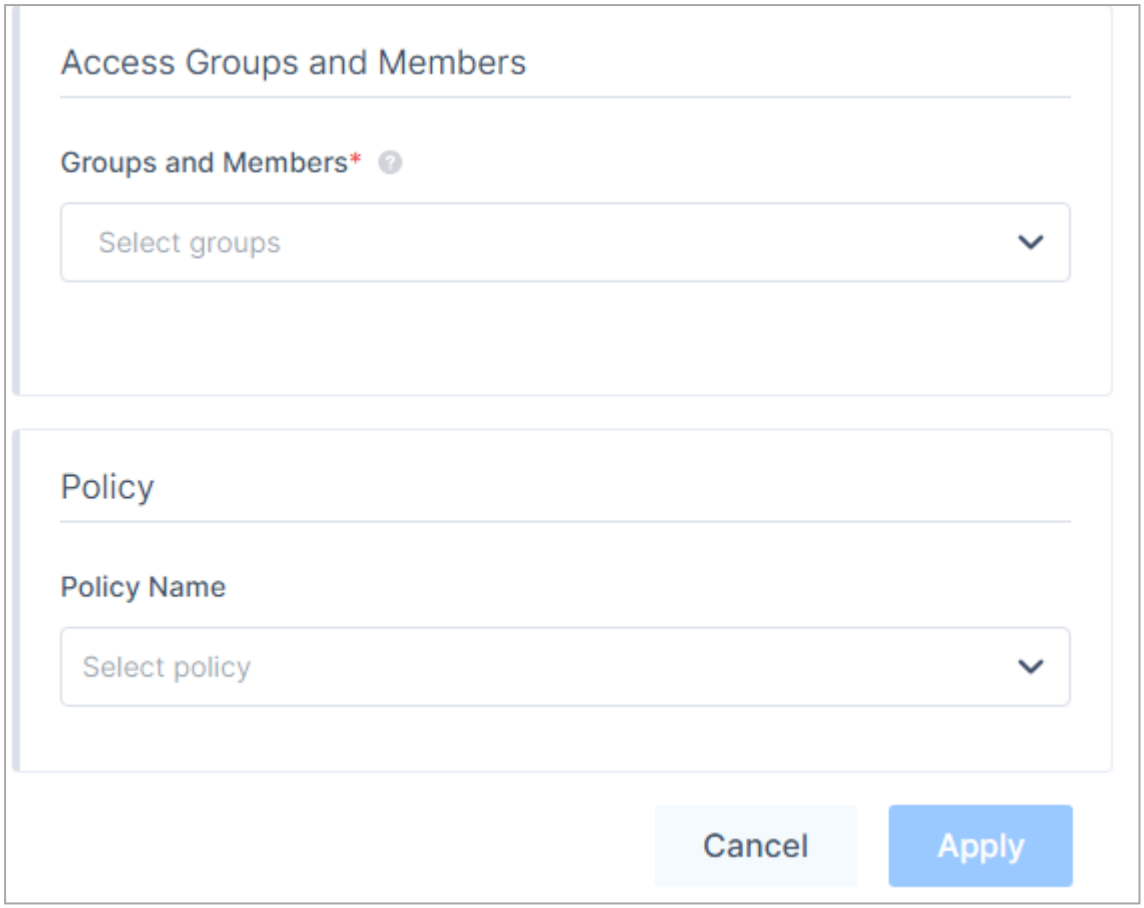
- For **Username/Password**, enter the username and password as predefined on the server.
- For **Private Key/Username/Passphrase**, enter these:
  a. **Username**: Username predefined on the server.
  b. **Private Key**: Your RSA-SSH key. Note that a certificate typically starts with a prefix and a suffix such as the following:

     ```
     -----BEGIN RSA PRIVATE KEY-----
     -----END RSA PRIVATE KEY-----
     ```

  c. **Passphrase**: The passphrase set with SSH key. If there is no passphrase, leave as blank.

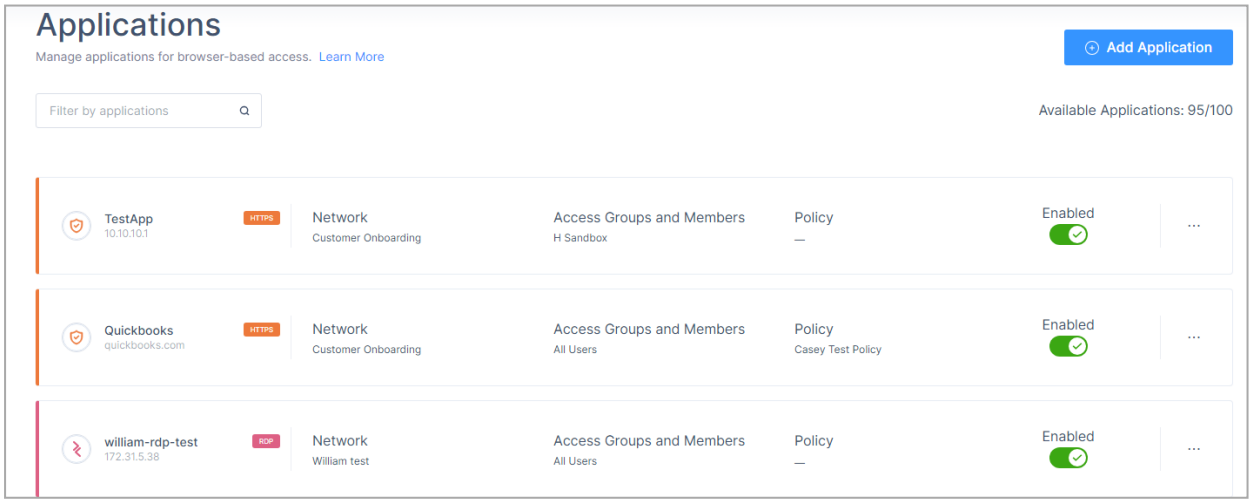
Note - If you disable **Authentication**, then the member must enter the credentials when accessing the machine.

5. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



6. (Recommended) In the **Policy Name** list, select an application policy.
7. Click **Apply**.

   The system lists the application in the **Applications** page and enables it by default.



8. For members to access the application, see *"Providing Application Access to Members" on page 768*.

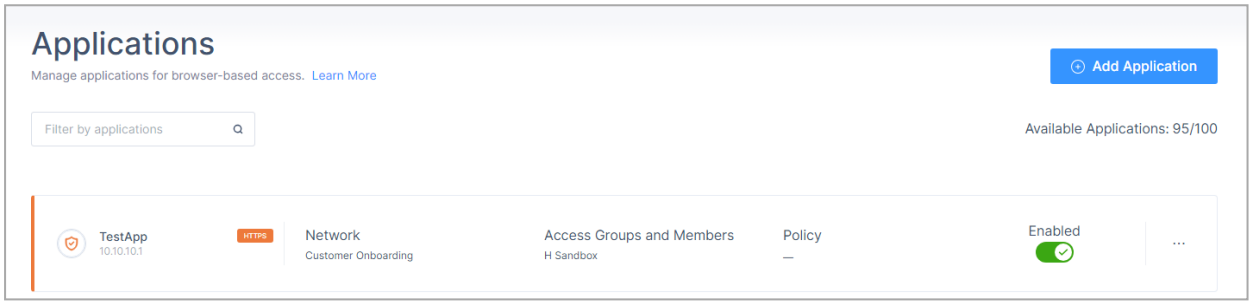
Adding a VNC Zero Trust Application

Prerequisite

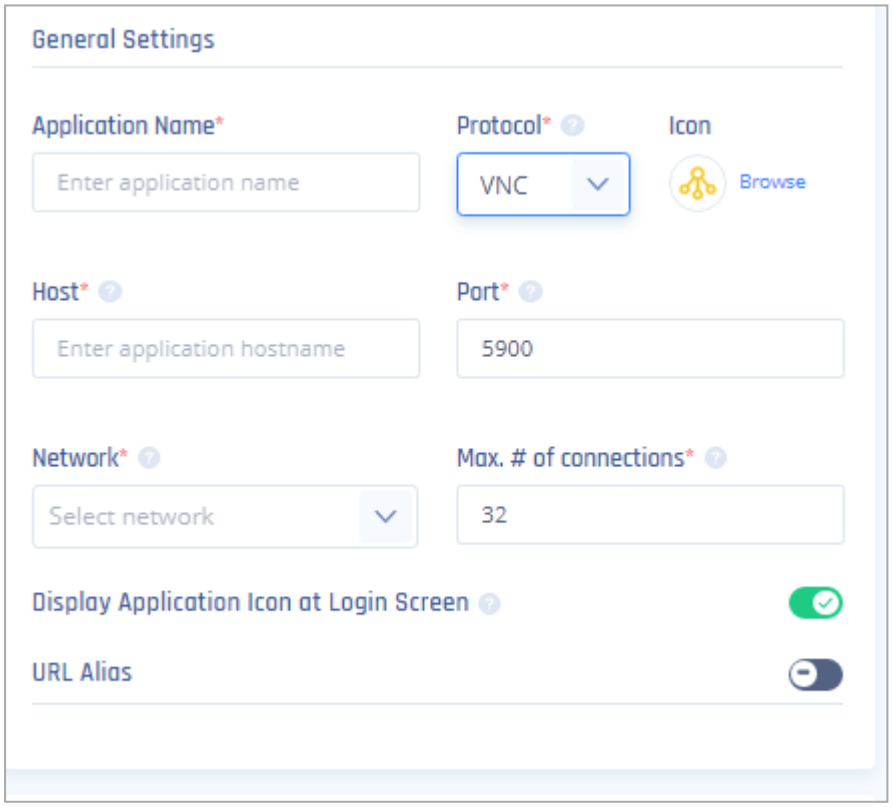
Make sure you have the credentials to access the application over VNC.

To add a VNC Zero trust Application:

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.



The **Add application** window appears.



3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - VNC

c. **Icon** - Icon for the application.

d. **Host** - Internal IP address of the server to which you want to connect.

e. **Port** - 5900

f. **Network** - Network that hosts the application.

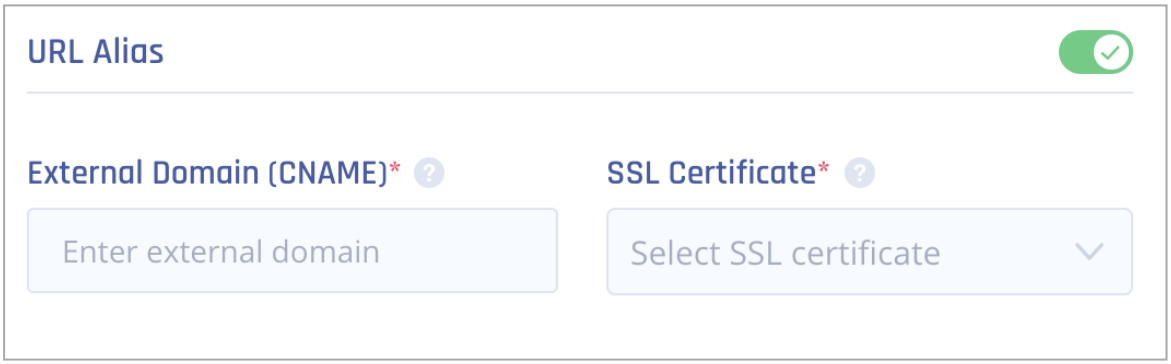
g. **Max number of connections**: 1

h. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

i. (Optional) **Enable copy-paste from VNC to clipboard** - Enables to copy data from VNC to clipboard.

j. (Optional) **URL Alias** - URL for members to access the application.

Important - You cannot add a URL alias after you create the application.

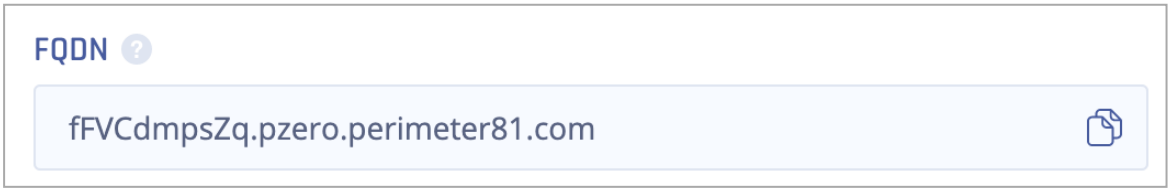


k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

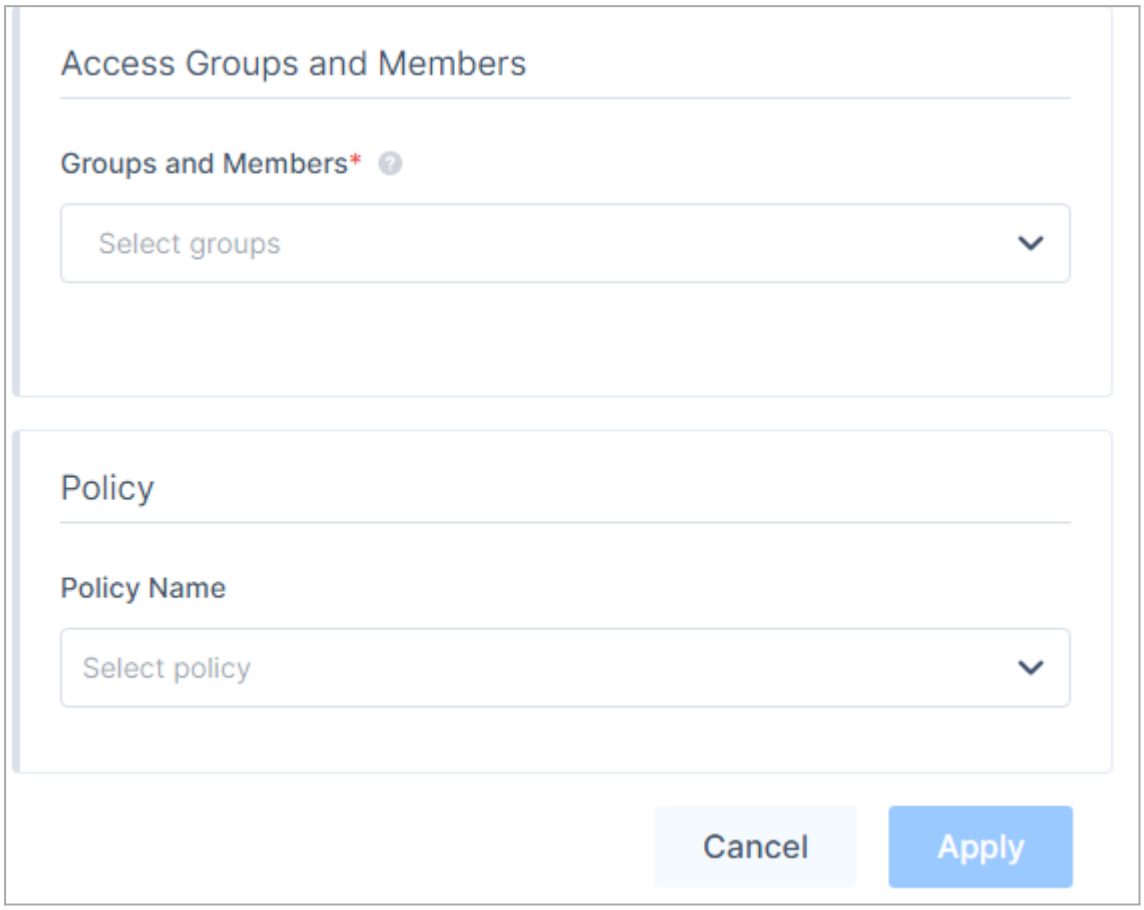
l. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

m. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CNAME specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.

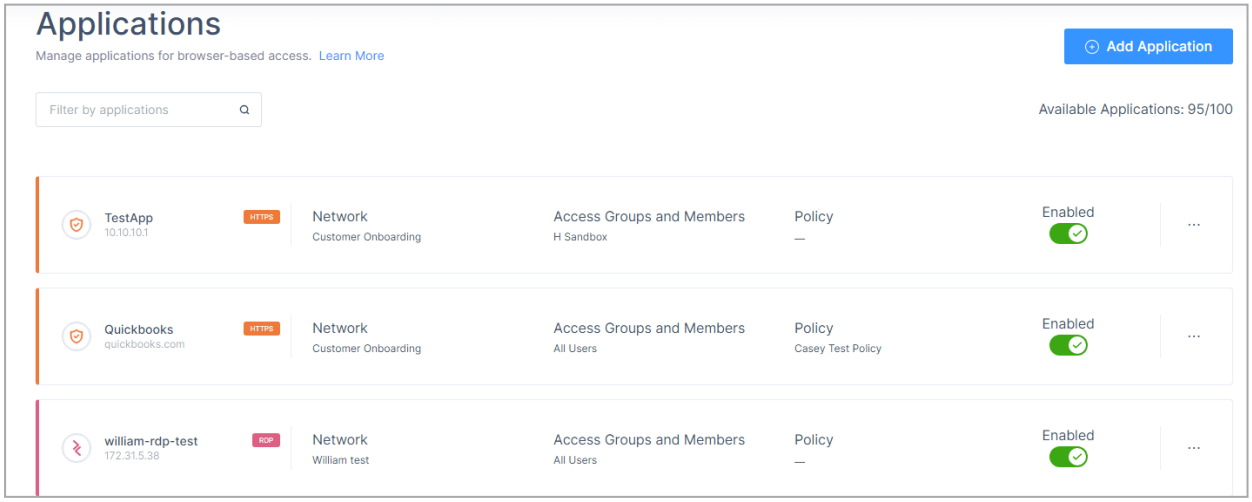


4. In the **Authentication** section, in the **Password** field, enter the password predefined in your VNC.
5. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



6. (Recommended) In the **Policy Name** list, select an application policy.
7. Click **Apply**.

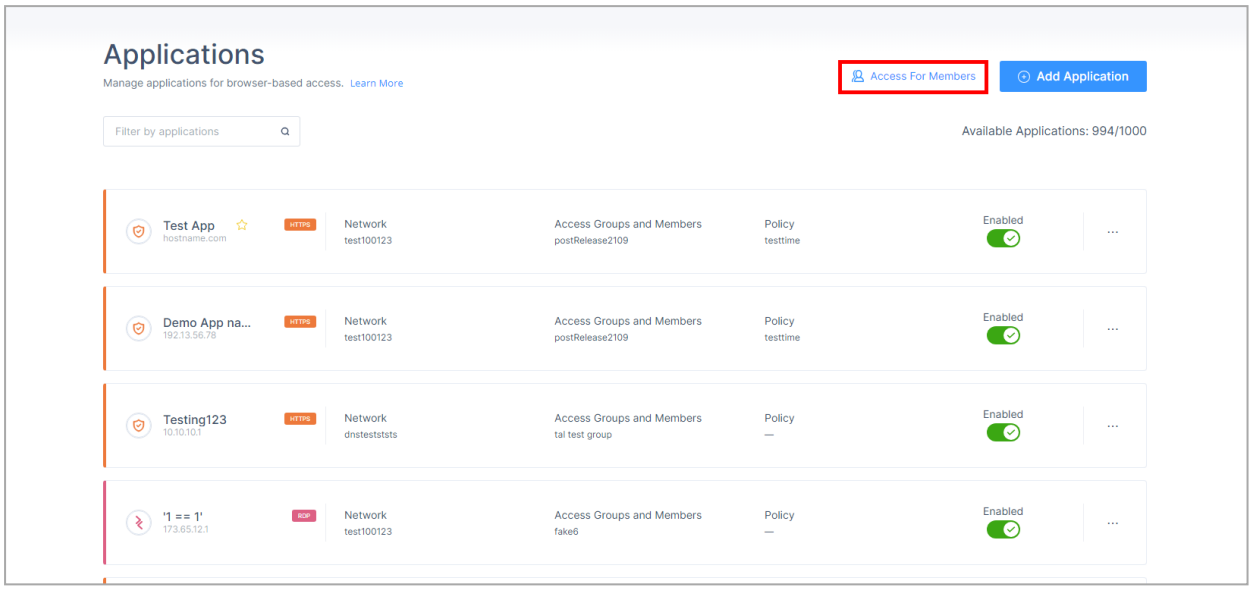
   The system lists the application in the **Applications** page and enables it by default.



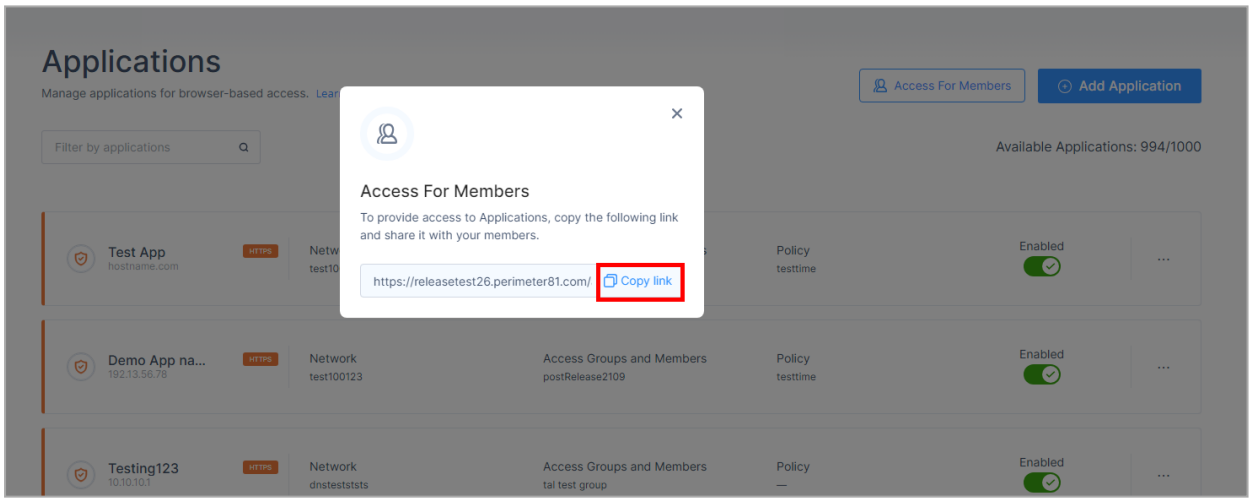
8. For members to access the application, see *"Providing Application Access to Members" on page 768*.

Providing Application Access to Members

1. On the **Applications** page, click **Access For Members**.

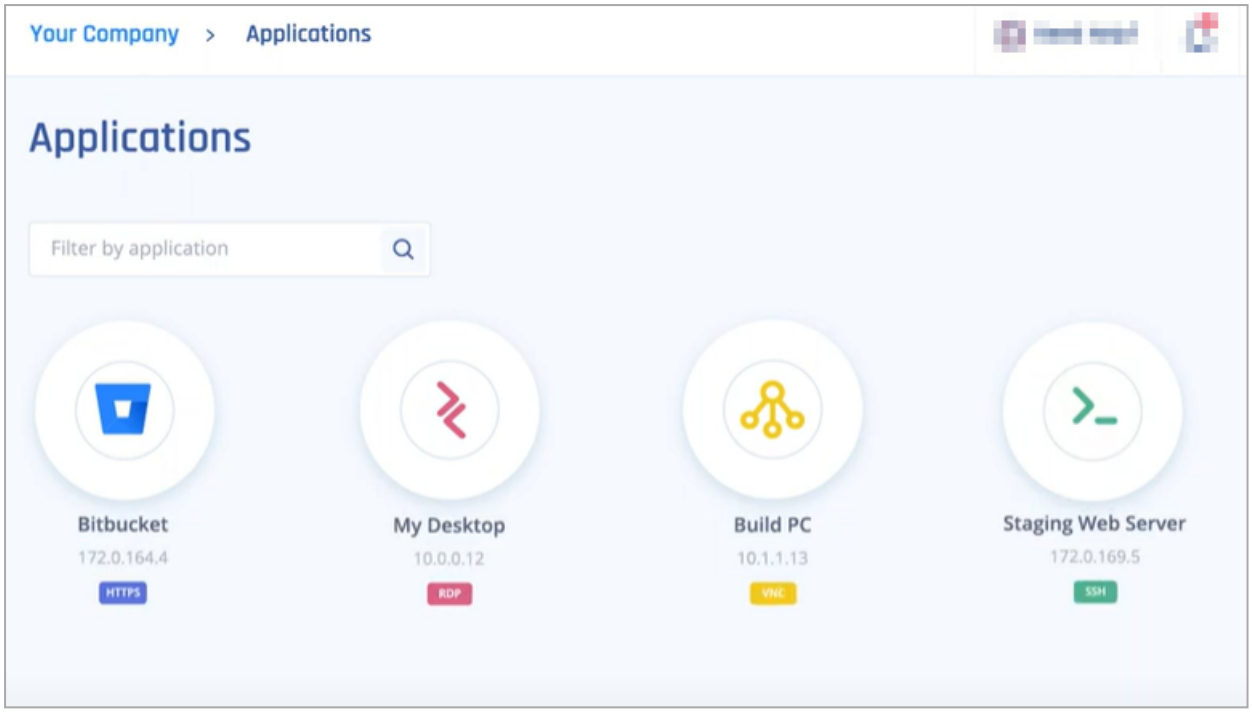


2. Click **Copy link**. Share this link with your members.



3. Member needs to log in to the Check Point SASE portal using the above link.

   After logging in to the portal, the member can view the list of authorized applications.

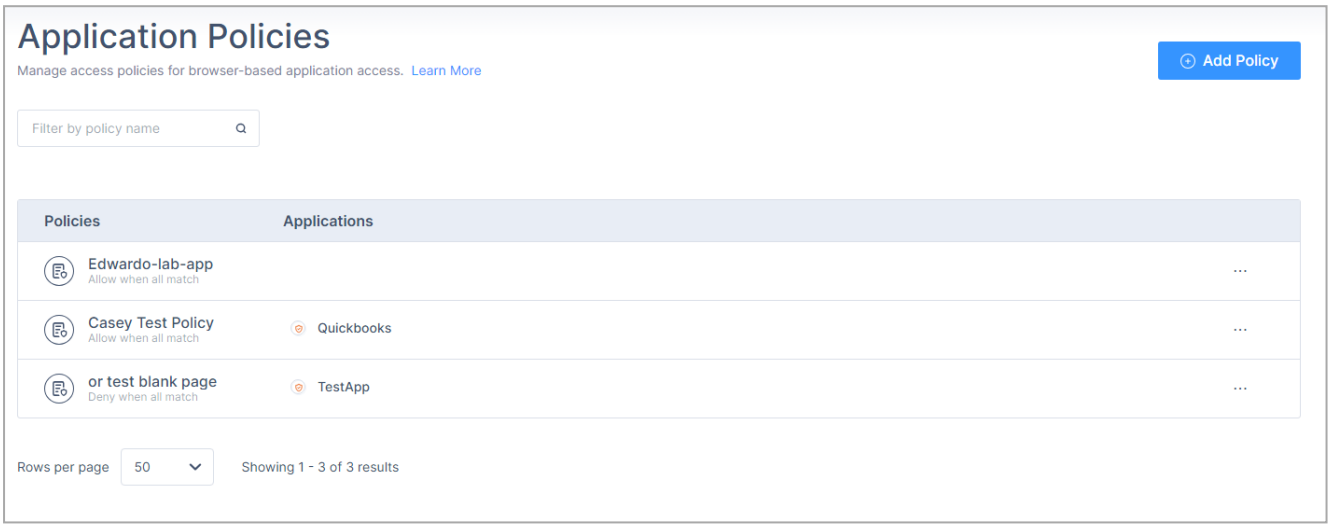


4. Click the application to access it.

Application Policies

The **Application Policies** page allows you create policies to grant authorized users permission to access applications.

To view the **Application Policies** page, access the Check Point SASE Administrator Portal and click **Private Access** > **Application Policies**.



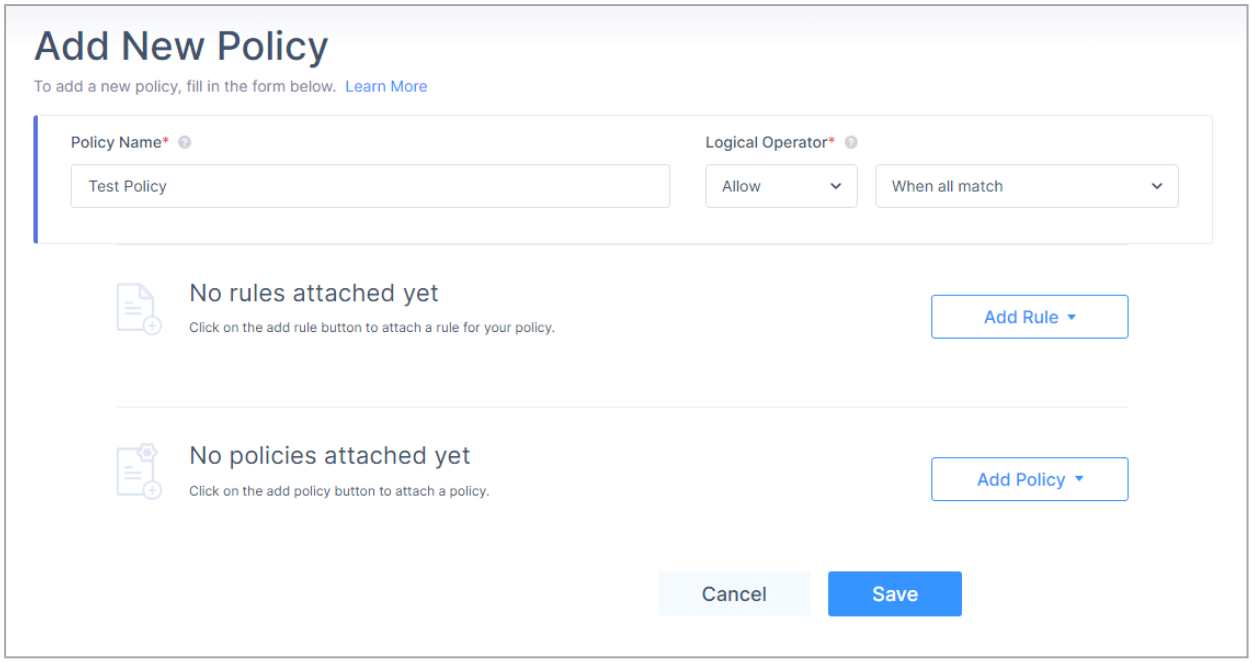
Best Practices -

- Review your policies periodically to align with your organizational requirements.
- Test policies on a small test group before enforcing it at the organizational level.

Creating an Application Access Policy

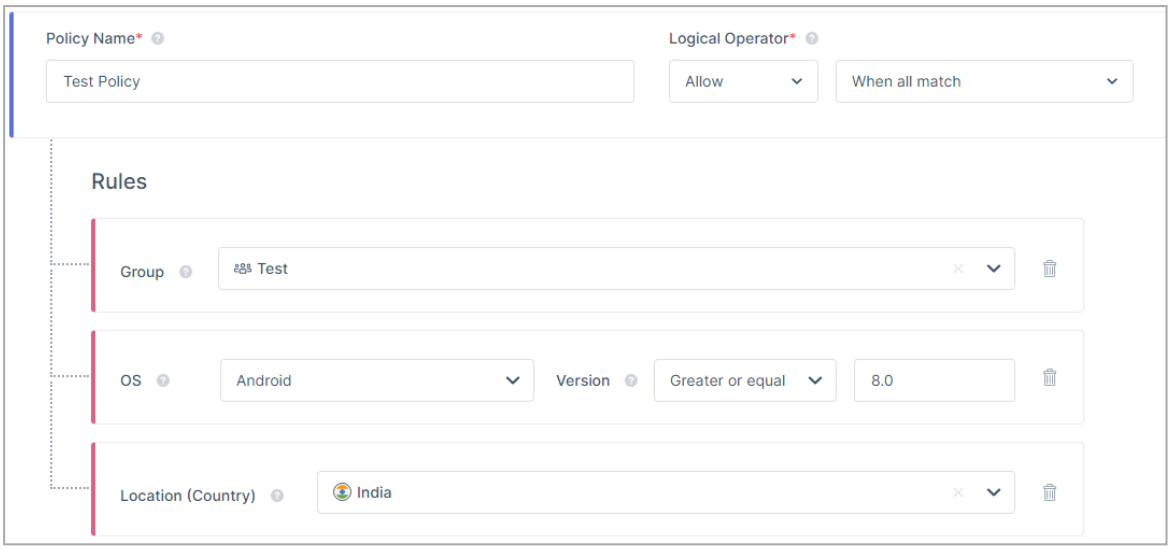
1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Application Policies**.
2. Click **Add Policy**.

   The **Add New Policy** page appears.



3. Enter these:
   a. **Policy Name** - Name of the policy.
   b. **Logical Operator**:
      - From the policy action list, select either of these:
        - **Allow**
        - **Deny**
      - From the list, select one of these:
        - **When all match** – The policy is considered compliant only if all defined rules are met.
        - **When some match** – The policy is considered compliant if at least one defined rule is met.
4. To add the rules for the policy, click **Add Rule** and specify one or more of these options:
   - Group
   - Date and Time
   - Location (IP)
   - Location (Country)
   - Browser

- OS and Version



5. To attach an existing policy with the new policy, click **Add Policy** and select a policy.
6. Click **Save**.

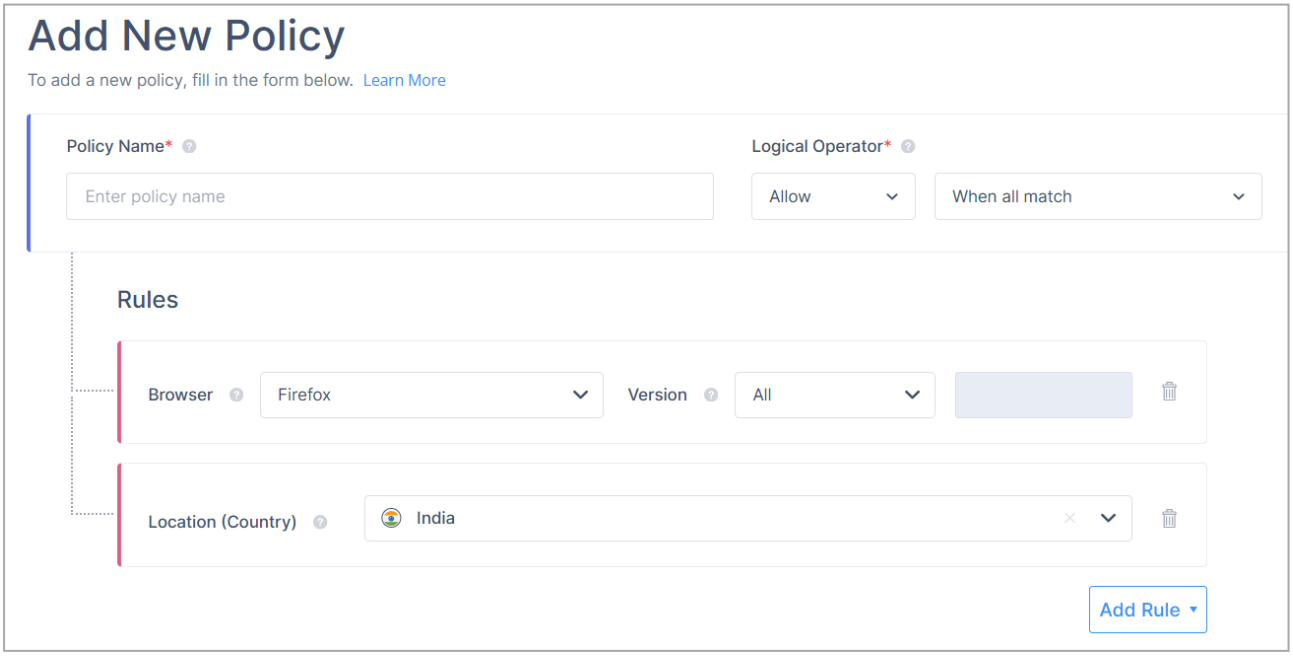
The new policy gets listed in your **Policy** page.

Here are some examples about how the policy works:

Example 1: When all match

Assume you have configured an application policy with the **Allow** action and the **When all match** condition for these parameters:

- **Browser**: Firefox
- **Location (Country)**: India

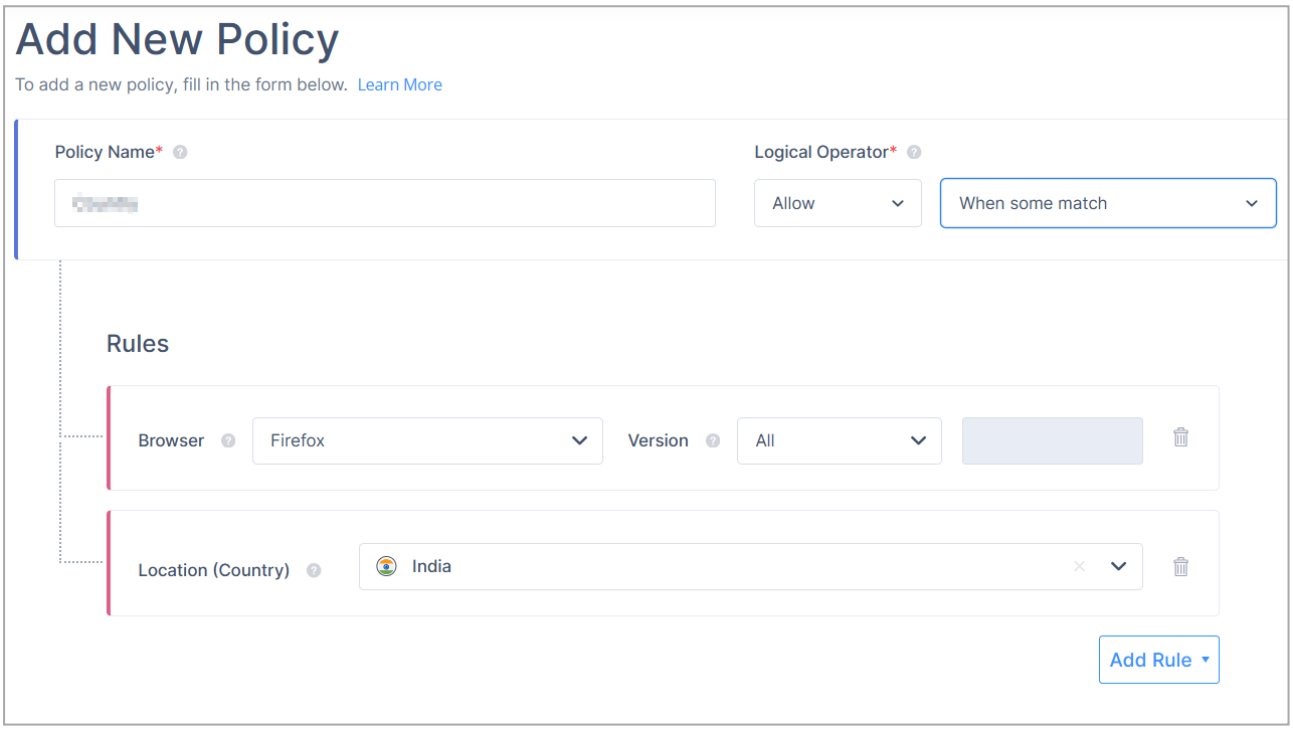


In this case, access is allowed only if the user is accessing the application from the Firefox browser and is located in India.

Example 2: When some match

Now, assume the same application policy is configured with the **Allow** action and the **When some match** condition:

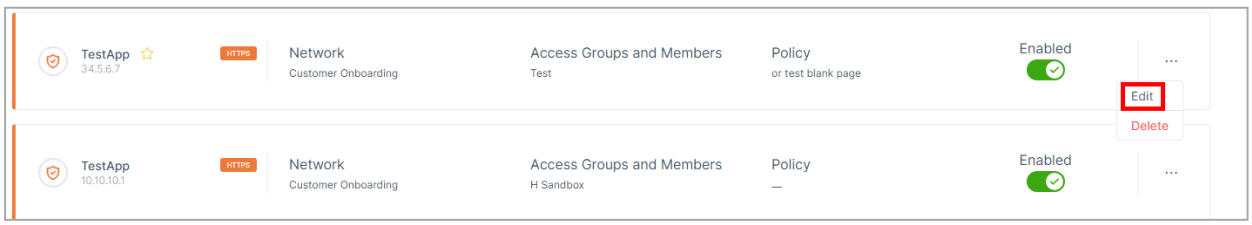
- **Browser**: Firefox
- **Location (Country)**: India



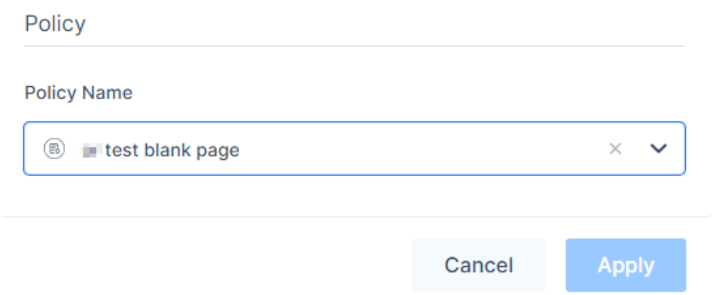
In this scenario, access is allowed if either the user is accessing the application from the Firefox browser or is located in India.

Assigning a Policy to an Application

1. Access the Check Point SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click ··· for the application and click **Edit**.



3. In the **Policy** section, from the **Policy Name** list, select a policy.



4. Click **Apply**.

Internet Access

Internet Access allows you to configure:

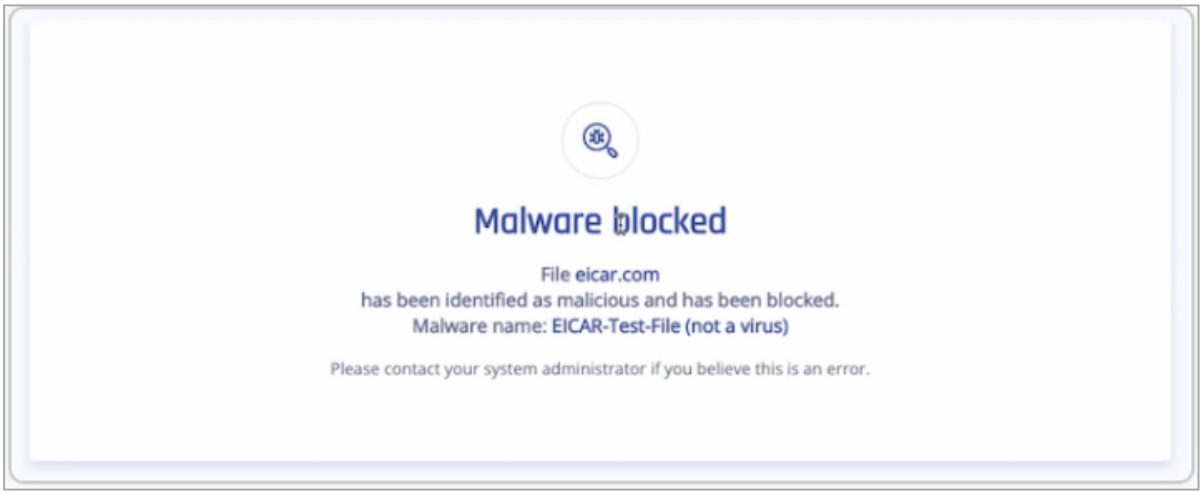
- *"Access Policy" on page 778*
- *Bypass Rules*

The *"Access Policy" on page 778* are directly applied on the device through the SASE Agent. The agent uses the in-built Secure Web Gateway (SWG) equipped with a Malware Protection Engine that:

- Scans the file and blocks access if it is malicious.
- Scans the traffic on the device without affecting the SWG performance.

Notes:

- The Malware Protection Engine can scan files less than 10 MB only.



- This is applicable only to internet traffic through a browser.
- The SWG inspects TLS traffic through the Check Point SASE Agent on port 443.

High-level Procedure

1. Create your internet access policy. See *"Access Policy" on page 778*.
2. (Optional) Configure bypass rules. See *"Creating a Bypass Rule" on page 790*.
    a. Configure the Secure Web Gateway (SWG) to bypass applications known to utilize certificate pinning. For more information, see *"Bypass Rules for Certificate Pinning" on page 800*.

Unified Internet Access Policy with Check Point Firewall

If your organisation uses Check Point Firewall Security Gateways, you can manage Check Point SASE Internet Access policy from SmartConsole.

This setup uses one Access Control policy and one HTTPS Inspection policy for on-premises users and remote users.

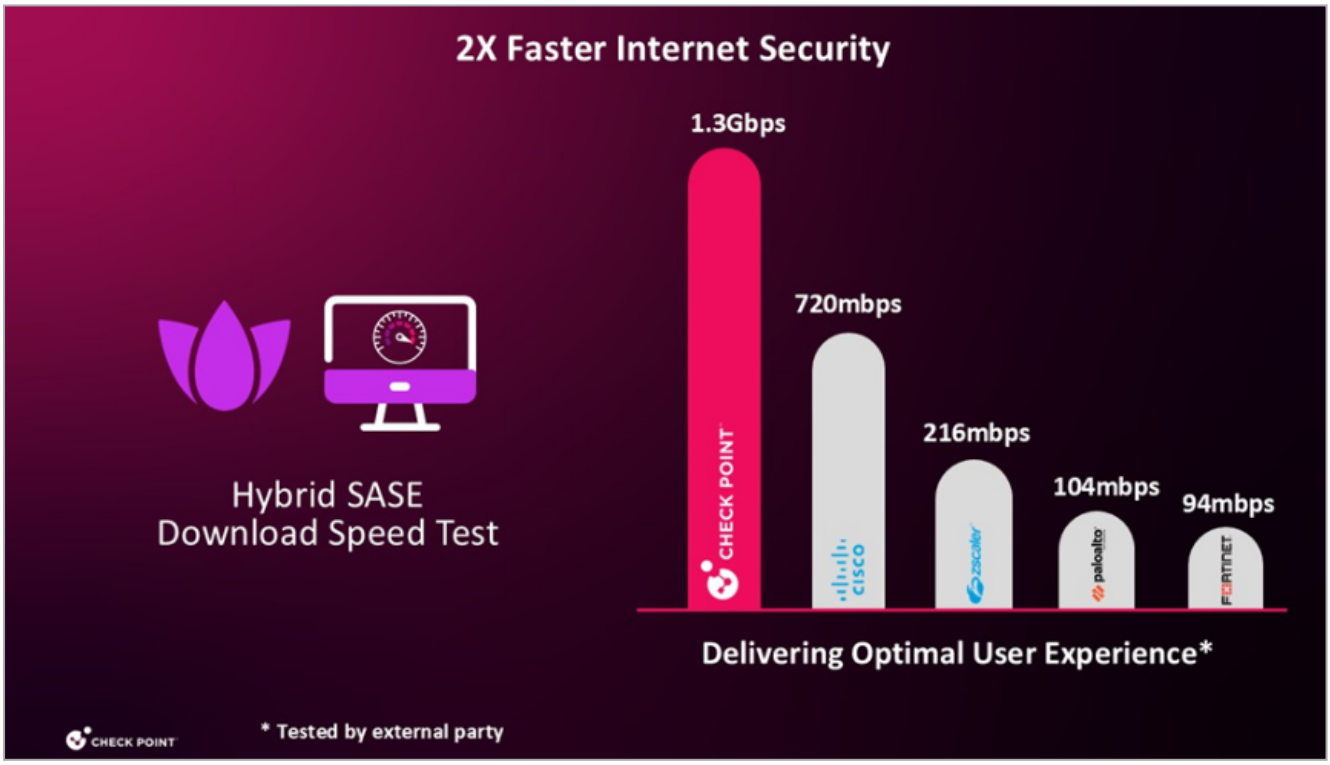
This setup removes the need to maintain separate policies across platforms.

For setup instructions and details, see:

- Unified Access Policy for SASE and Network Security
- Unified Internet Access Policy for Check Point SASE and Quantum Management Server

Internet Access Speed

Check Point SASE's hybrid Secure Web Gateway (SWG) architecture enhances internet performance, delivering speeds up to 10 times faster than competing solutions, as validated by independent Miercom benchmarking tests.



This architecture optimizes bandwidth allocation to support enterprise workloads, including latency-sensitive applications such as videoconferencing and real-time collaboration tools.

Factors Affecting Remote User Internet Speed

When evaluating remote user internet performance, consider these variables:

- **Internet Service Provider (ISP) performance** – Latency, jitter, and bandwidth availability impact connection quality.
- **Security policy enforcement** – Advanced threat prevention, data loss prevention (DLP), and traffic inspection can introduce processing overhead.
- **Network congestion** – The number of concurrent users and bandwidth-intensive applications (e.g., streaming, gaming, or cloud workloads) influence available throughput.

Check Point continuously enhances Check Point SASE by investing in network optimization, intelligent traffic routing, and adaptive security measures to deliver an optimal user experience.

Access Policy

The **Access Policy** defines what users are allowed or denied access to when browsing the internet. It enables administrators to:

- Control access to web categories, for example, social media, news, gambling
- Allow or block specific URLs or domains
- Manage access to cloud-based and web applications, for example, Dropbox, YouTube, ChatGPT

These controls can be tailored per user or user group, ensuring policies are aligned with business roles and security requirements. For example, marketing teams might be granted access to social media platforms, while finance users are restricted to business-related sites only.

Note - Updatable Objects feature is available in Early Availability (EA) only. To enable, contact Check Point Support.

Note - For Check Point SASE Linux clients, Secure Web Gateway (SWG) Access Policy rules do not support wildcard domain patterns (for example, **.example.com*). Using wildcards may cause incorrect traffic evaluation or policy bypass. Use explicit domain names instead.

To view the **Access Policy** page, access the SASE Administrator Portal and click **Internet Access** > **Access Policy**.

Column	Description
Name	Name of the Rule.
Source	▪ Any ▪ Groups or members to which the rule is applied.
Destination	Destination of the web traffic generated by the source (**Any, Web categories**, **Custom URLs**or **Applications** or **Updatable Onjects**).
Conditions	Allows admin to define time-based constraints for each rule. When a condition is applied, the rule is enforced only during the specified time frame (example: weekdays between 9:00 AM and 6:00 PM). This enables administrators to create policies that adapt to business hours, shift schedules, or specific access windows, for example, restricting access to social media sites outside of working hours. If no condition is set, the rule applies at all times.

Column	Description
Action	Action for web traffic: ■ **Drop** - Blocks web traffic. ■ **Accept** - Permits web traffic. ■ **Warn**[1] - Allows web traffic and logs the event. See Web Activity.

[1]The end user needs to confirm the warning message, so it do not show the alert for the inspected resource for the next 24 hours.

Application Policy

Application Policy enables you to monitor, manage, and enforce access control over the SaaS applications used in an organization. It uses state of the art applications catalog and detection engine to accurately recognize and classify SaaS applications based on their behavior, signatures, and traffic patterns.

Support

Minimum agent version supported is 11.5.

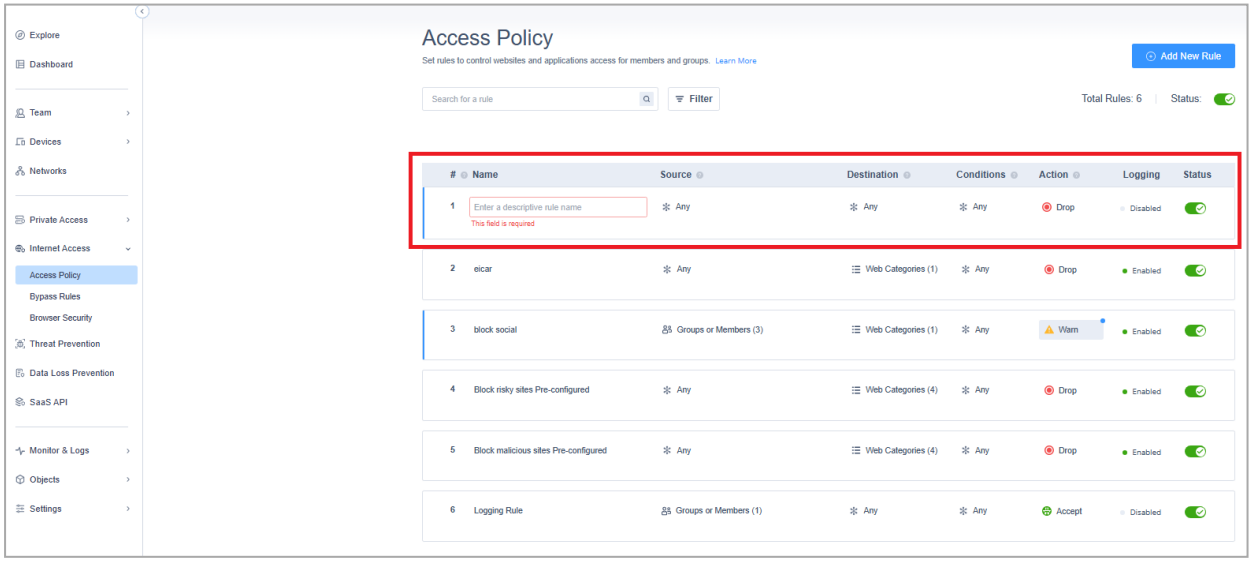
Creating an Access Policy

1. Access the SASE Administrator Portal and click **Internet Access** > **Access Policy**.

   Note - The access policy is a first-match-rule base.

2. Click **Add New Rule**.

   A new rule appears in the table.



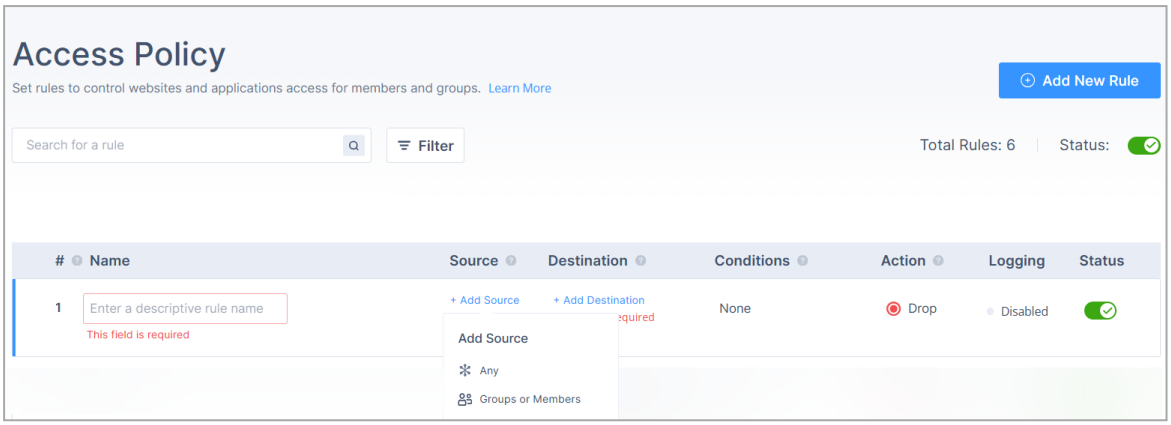
3. In the **Name** field, enter a name for the rule.

4. From the **Action** list, select one:
   - **Drop** (default)
   - **Accept**
   - **Warn**

   Note - Custom URLs support wildcards, see *"Custom URLs" on page 920*.

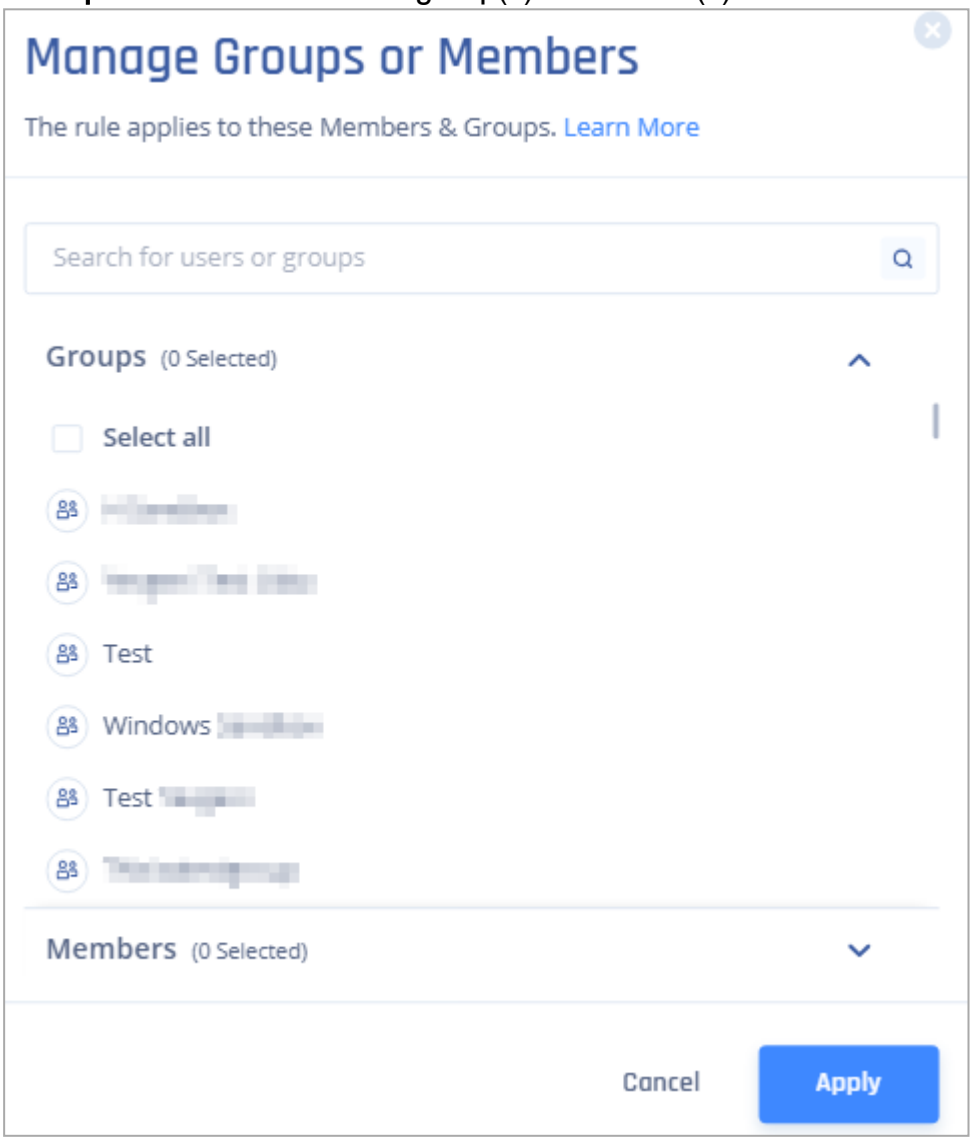
5. In the **Source** field, add user or group list to which you want to apply the rule.

a. Click **Add Source** and select any one from these:



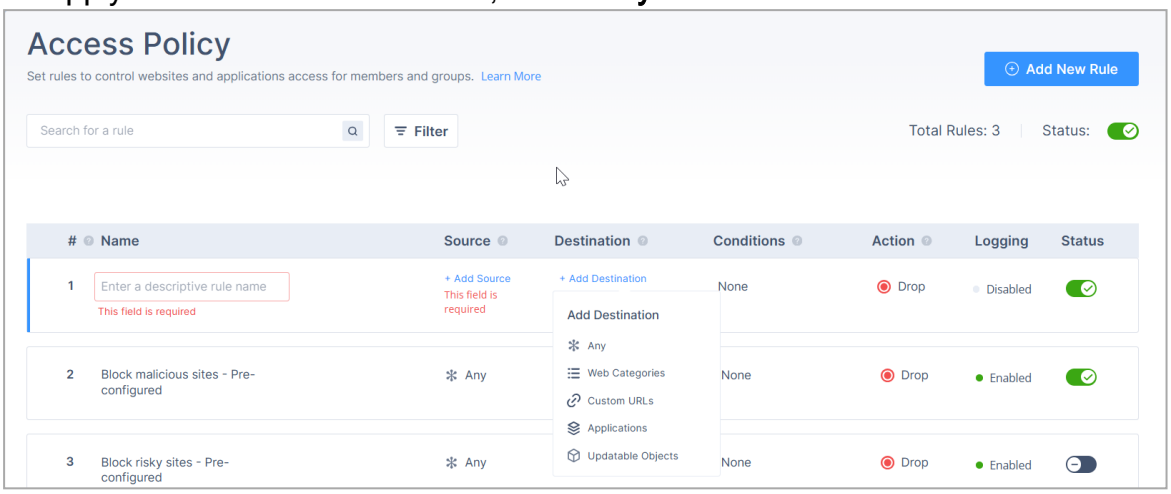
i. **Any**

ii. **Groups or Members**: Select group(s) or member(s) from the list.



b. Click **Apply**.

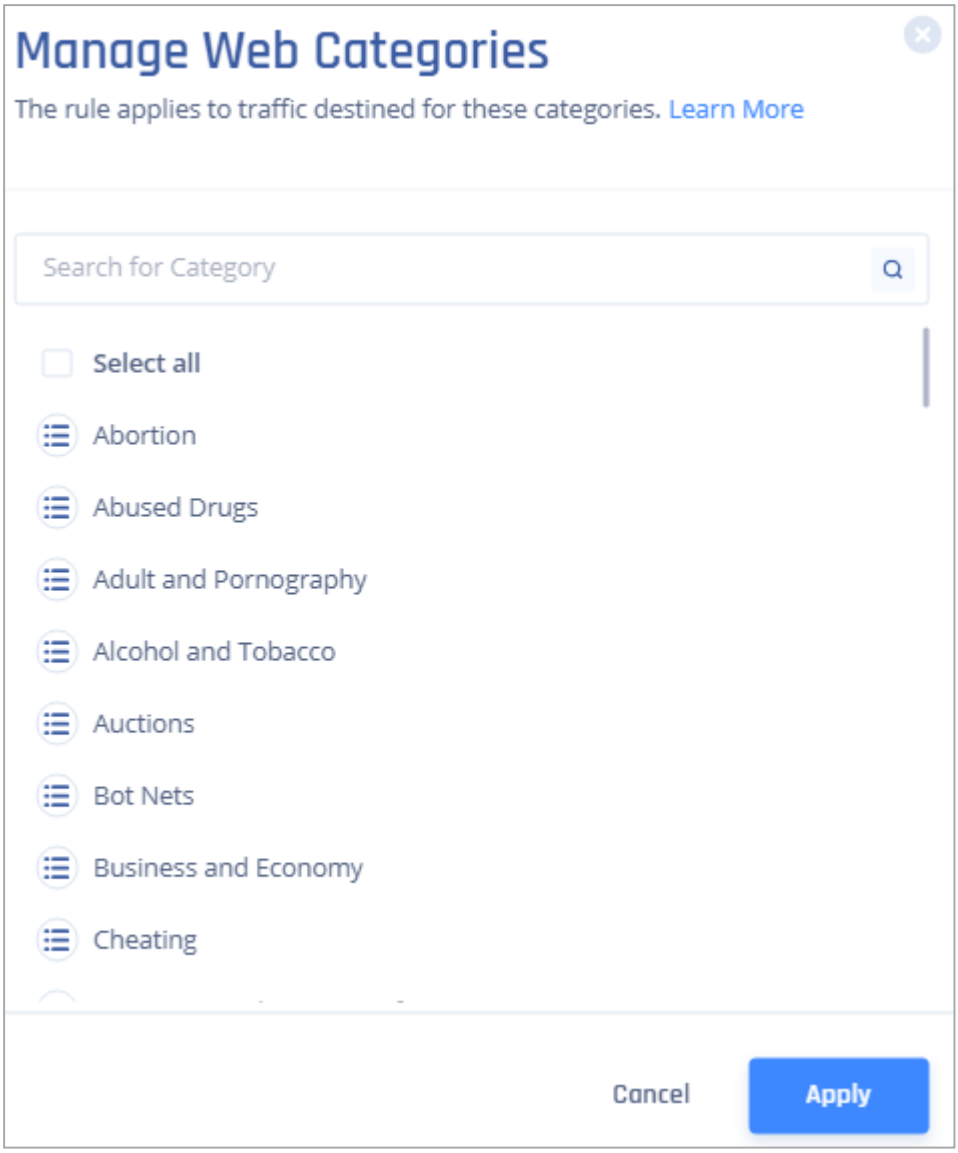
6. In the **Destination** field, select the destination.
   a. Click **Add Destination**.
   b. To apply the rule to all destinations, select **Any**.



   c. Click **Apply**.

d. To add web categories, select **Web Categories**.

The **Manage Web Categories** window appears.

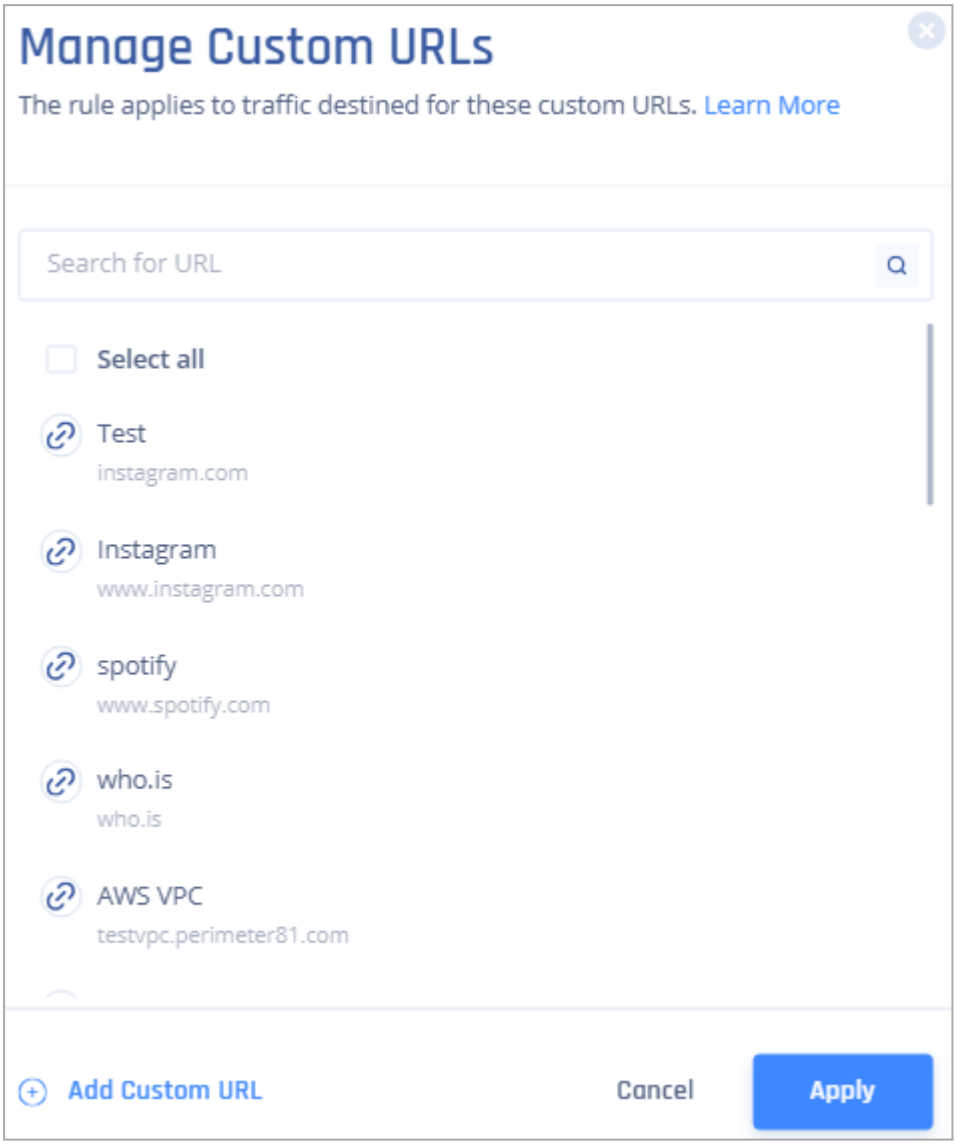


e. Select the categories from the list.

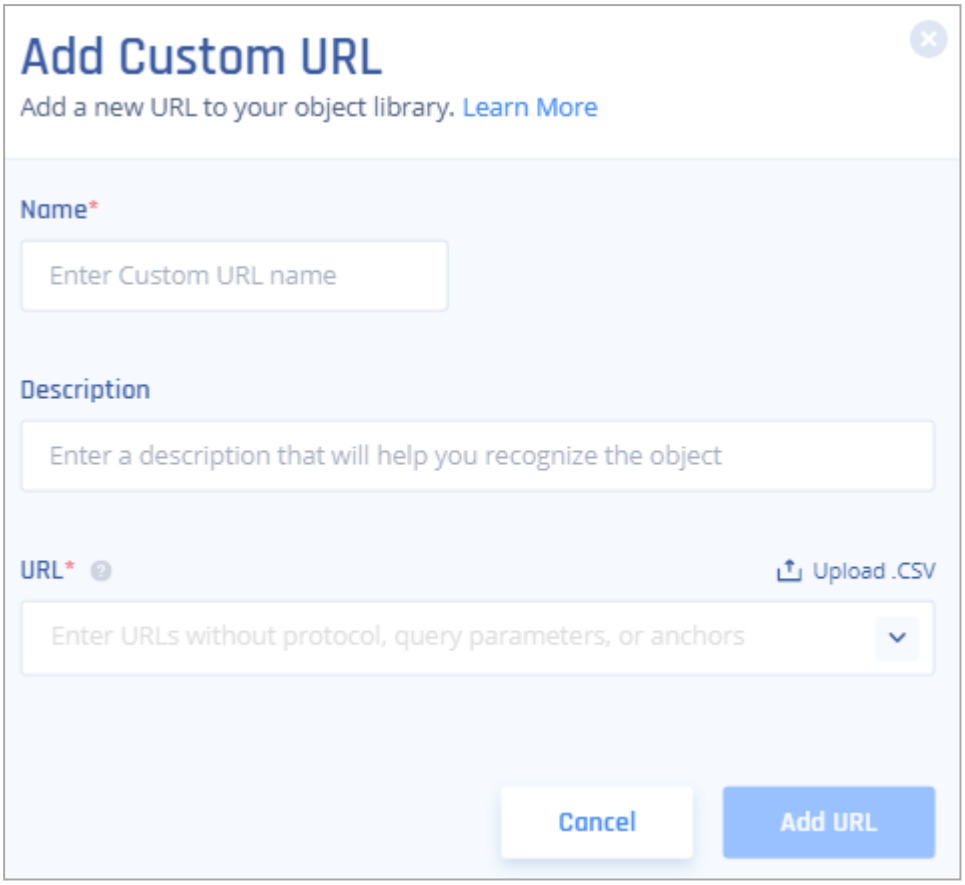
f. Click **Apply**.

g. To add custom URLs, select **Custom URLs**.

The **Manage Custom URLs** window appears.



h. Select the custom URL. If the URL is not listed, click **Add Custom URL** and specify these and click **Add URL**:



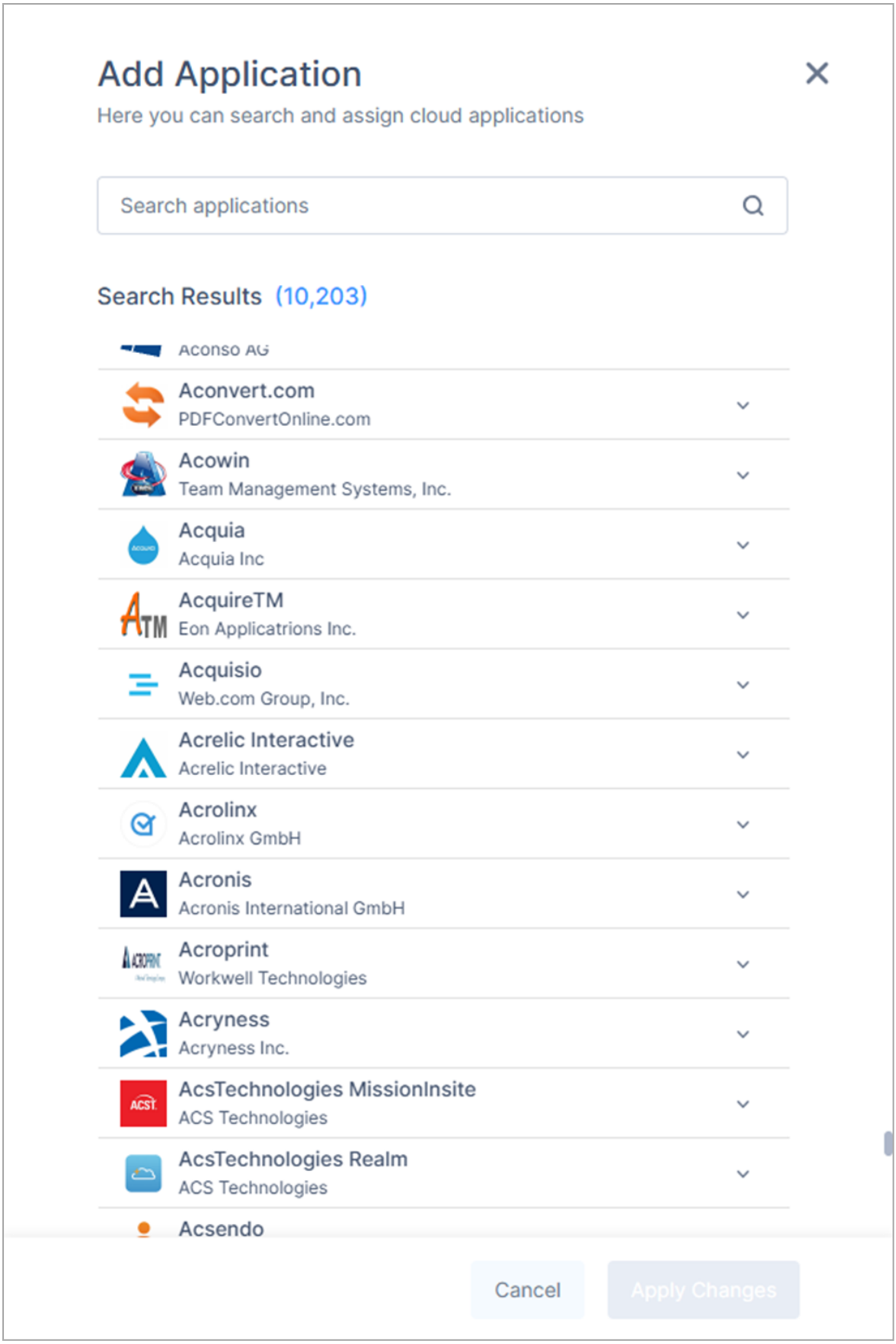
- **Name**
- **Description**
- **URL**

Optionally, click **Upload .CSV** to upload a .csv file with list of URLs.

i. Click **Apply**.

j. To add applications, select **Applications**.

The **Add Application** window appears.

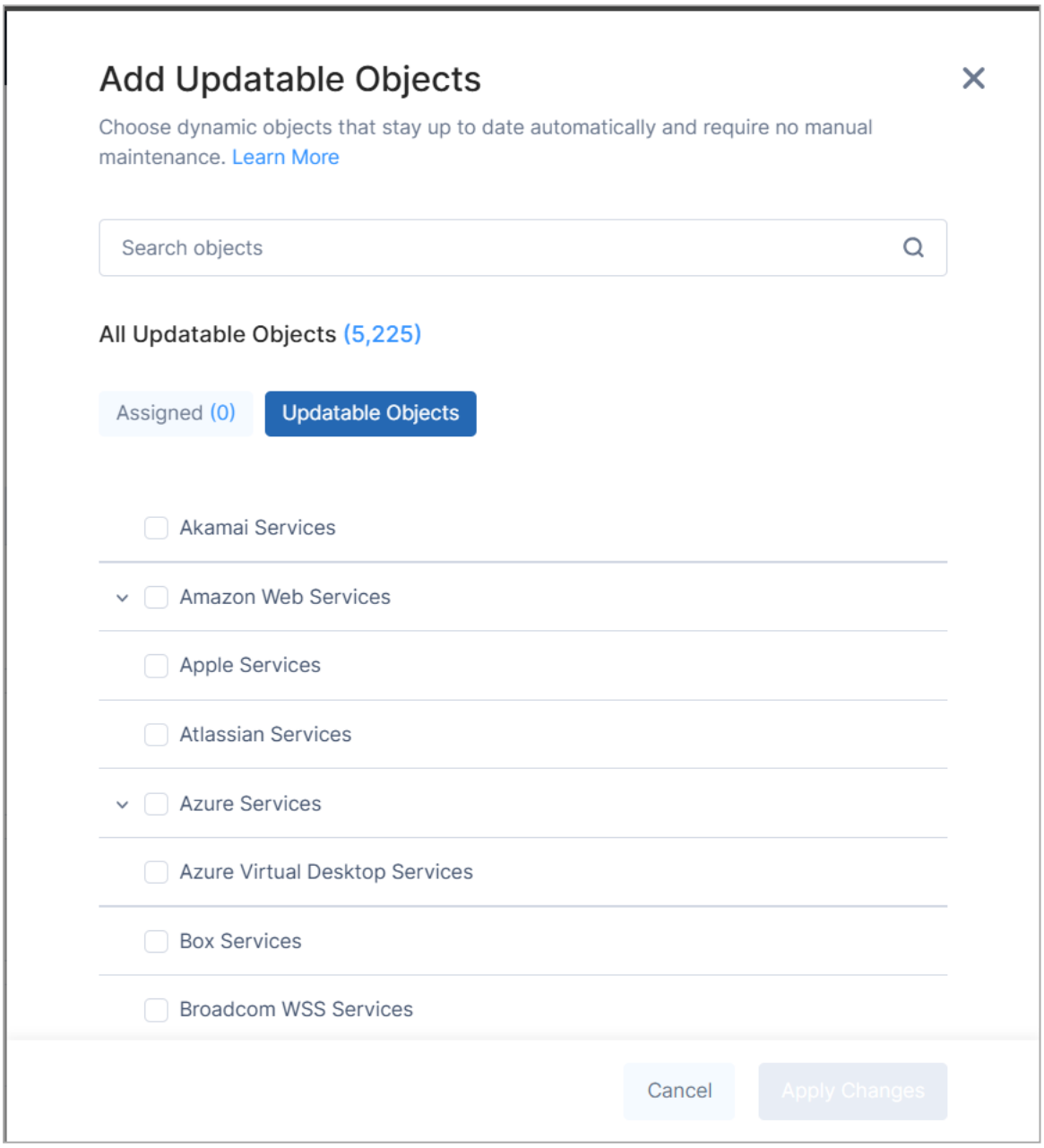


k. Search the application and click + to select the application.

l. Click **Apply Changes**.

m. To add updatable objects, select **Updatable Objects**.

n. For more information, see *"Updatable Objects" on page 923*.



o. The **Add Updatable Objects** window appears.

p. Use the **Search Objects** field to find services, or click **Updatable Objects** to select the required services.

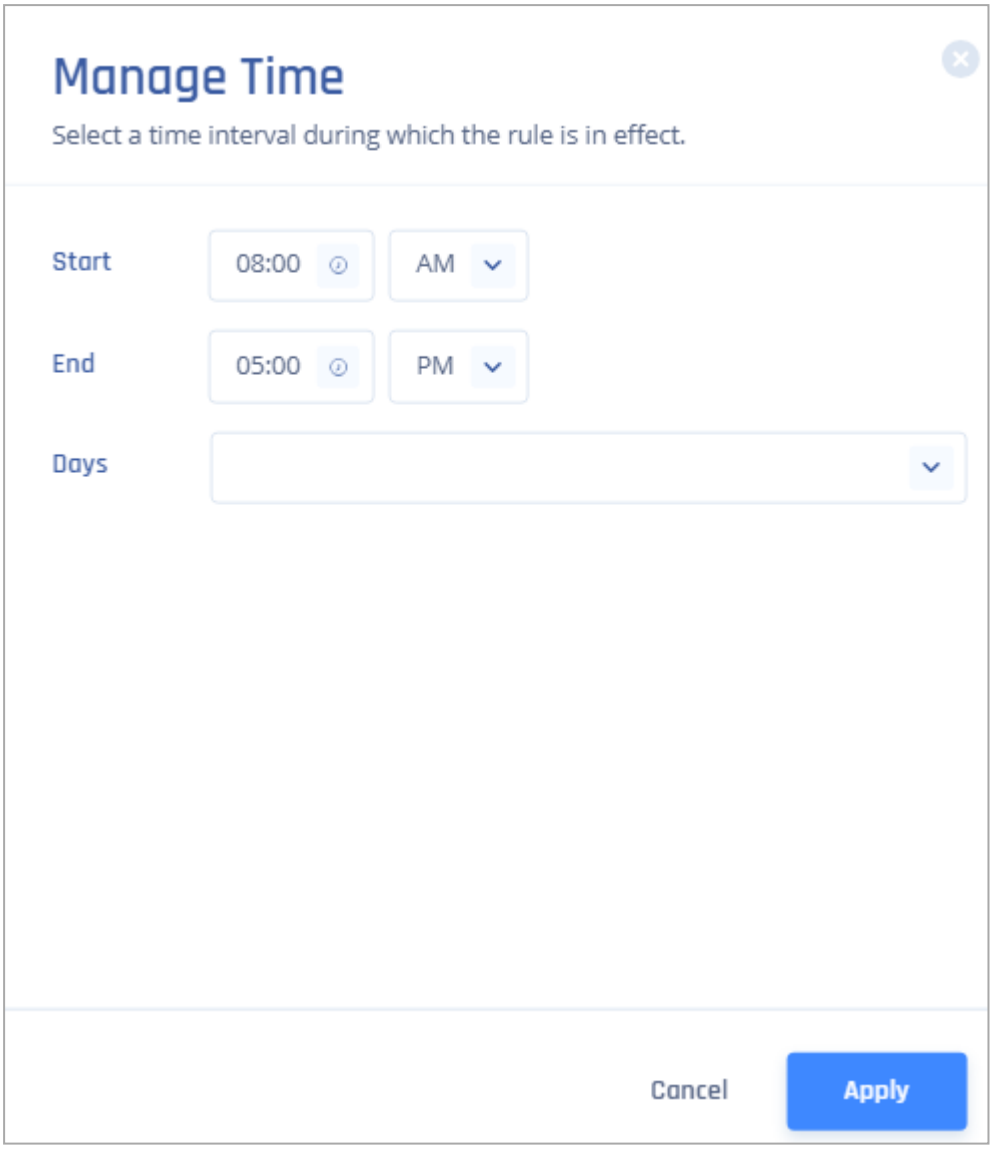
q. Selected services appear under the **Assigned** tab.

r. Click **Apply Changes**.

7. In the **Conditions** field, specify the timeframe for which the rule must be active.

a. Click **Add Condition** > **Time**.

The **Manage Time window** appears.



b. Select the **Start** time from the list.

c. Select the **End** time from the list.

d. Select the **Days** from the list.

e. Click **Apply**.

8. To activate the rule, turn on the **Status** toggle button.
9. Click **Apply** in the bottom of the page.

10. Click **Apply**.

The page allows you to specify traffic that must be ignored by the *"Access Policy" on page 778*.

To view the **Bypass Rules** page, access the SASE Administrator Portal and click **Internet Access** > .

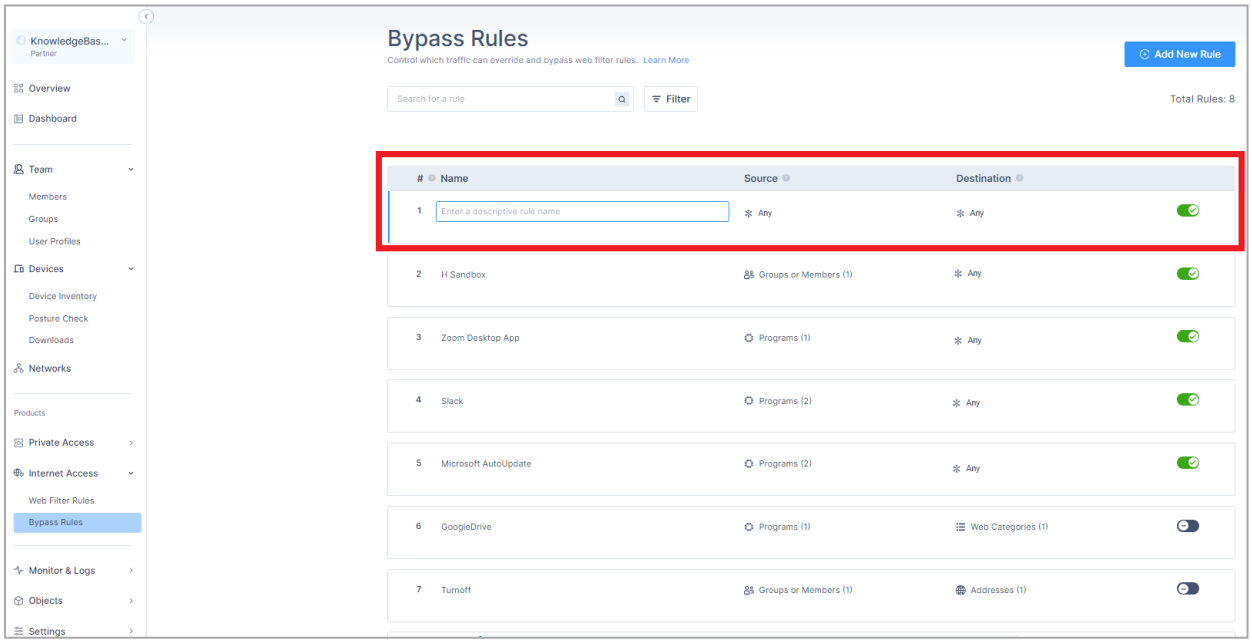
Note - Updatable Objects feature is available in Early Availability (EA) only. To enable, contact Check Point Support.

Column	Description
Name	Name of the bypass rule.
Source	
Destination	Destination of the web traffic.

Creating a Bypass Rule

1. Access the SASE Administrator Portal and click **Internet Access** > **Bypass Rules**.
2. Click **Add New Rule**.

   A new rule appears in the table.

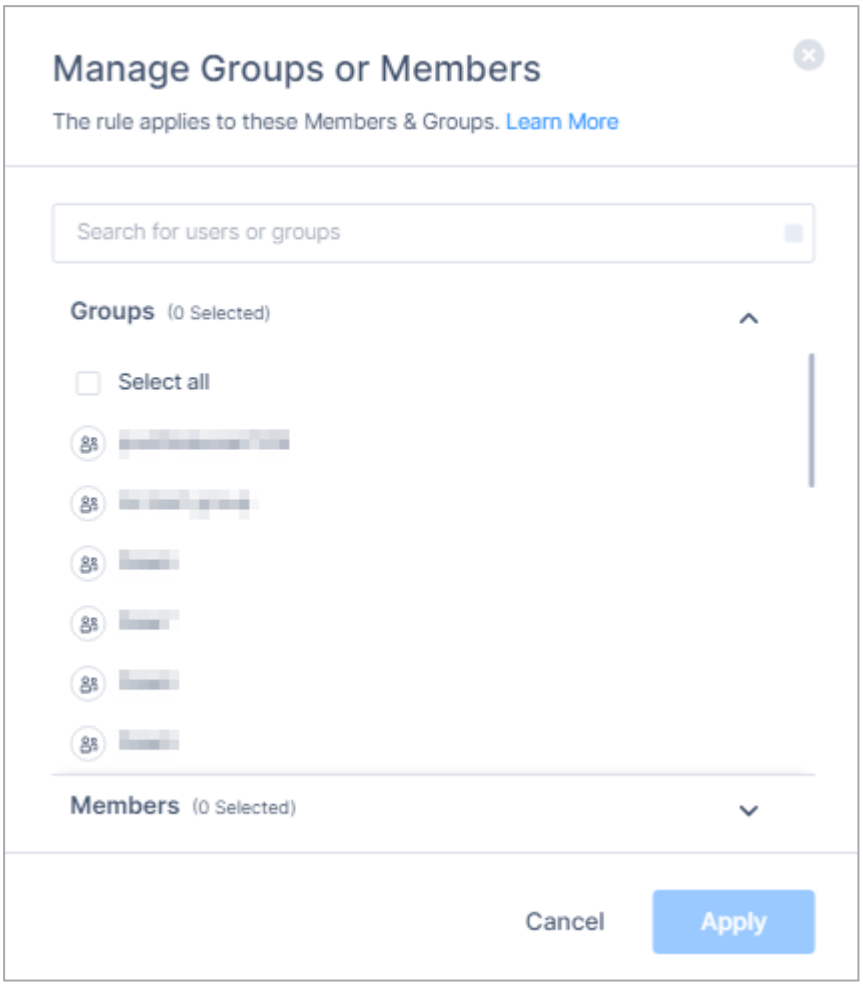


3. In the **Name** field, enter a name for the rule.
4. In the **Source** field, add user or group list to which you want to apply the rule. Default is **Any**.

a. Click **Any** > **Add Source**.

b. To add groups or members, select **Groups or Members**.

The **Manage Groups or Members** window appears.

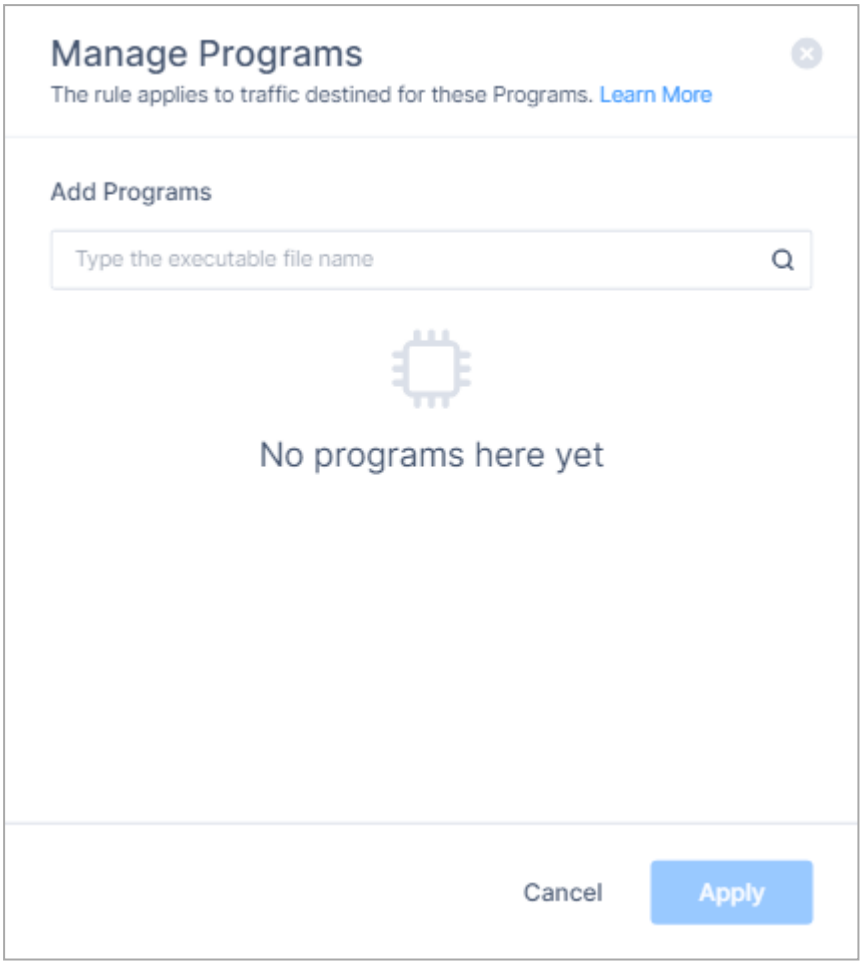


c. Select group(s) or member(s) from the list.

d. Click **Apply**.

e. To add programs, select **Programs**.

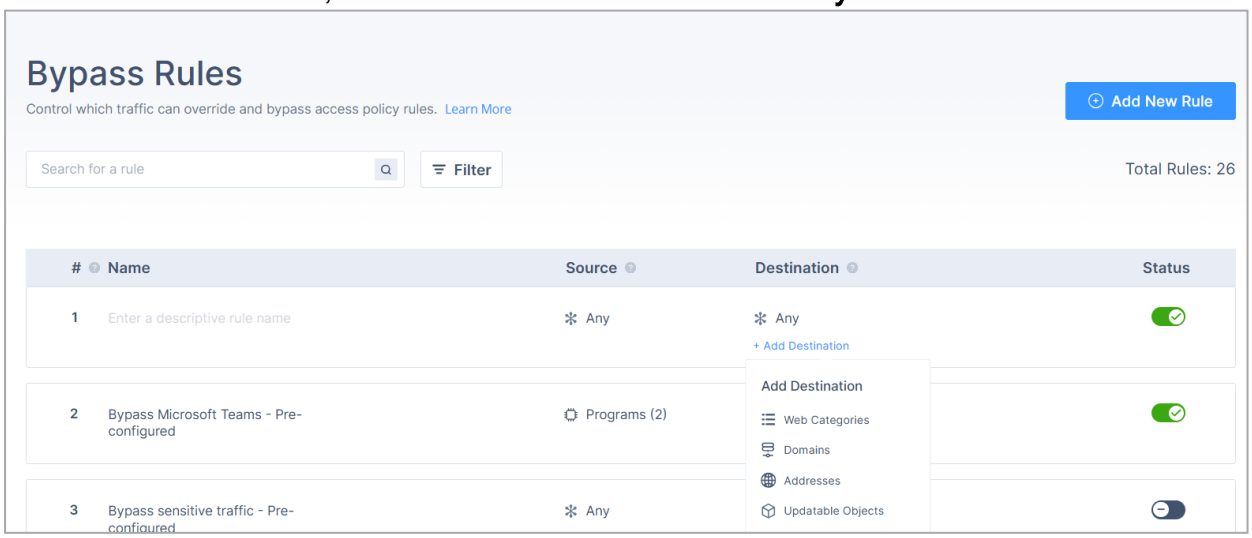
The **Manage Programs** window appears.



f. Enter the program name and press **Enter**.

g. Click **Apply**.

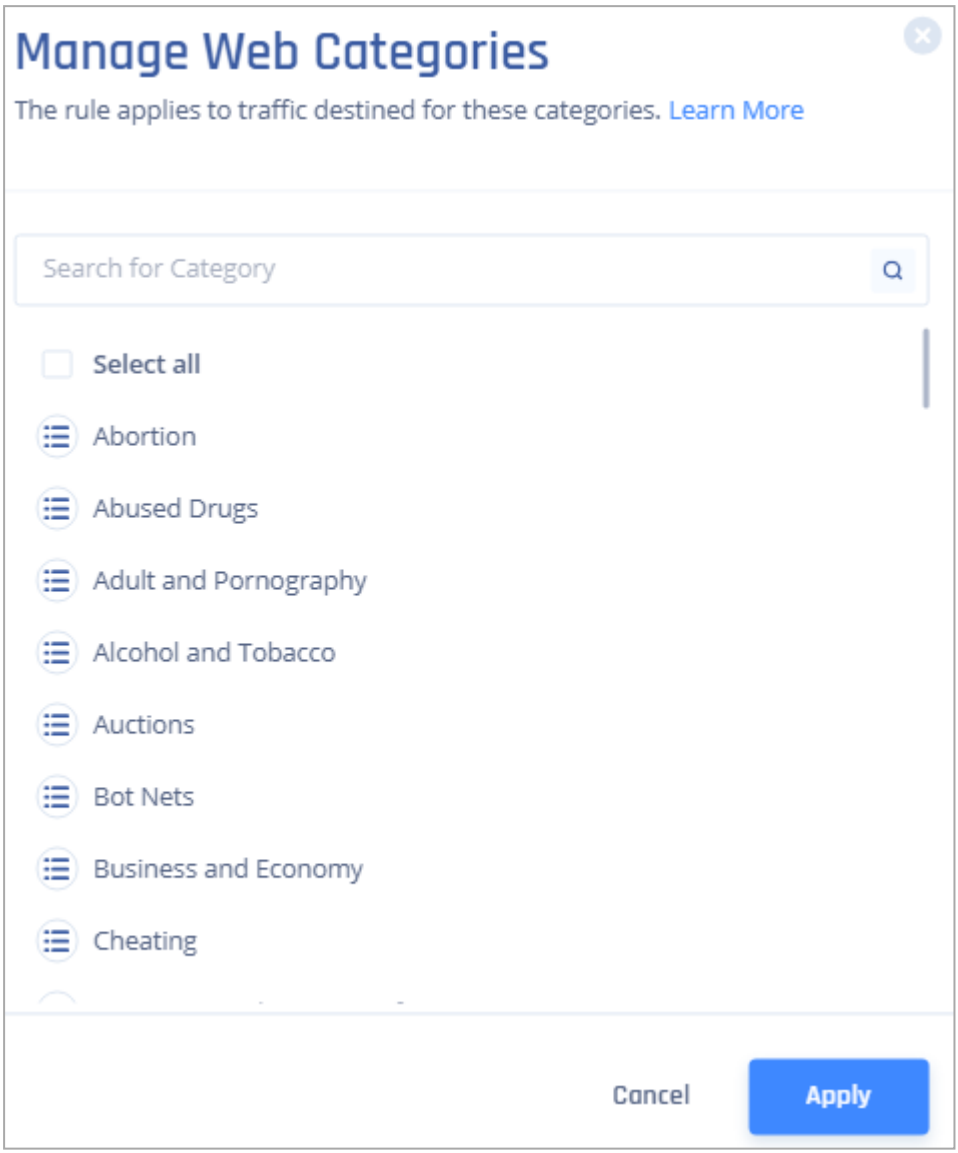
5. In the **Destination** field, select the destination. Default is **Any**.



a. Click **Any** > **Add Destination.**

b. To add web categories, select **Web Categories**.

The **Manage Web Categories** window appears.

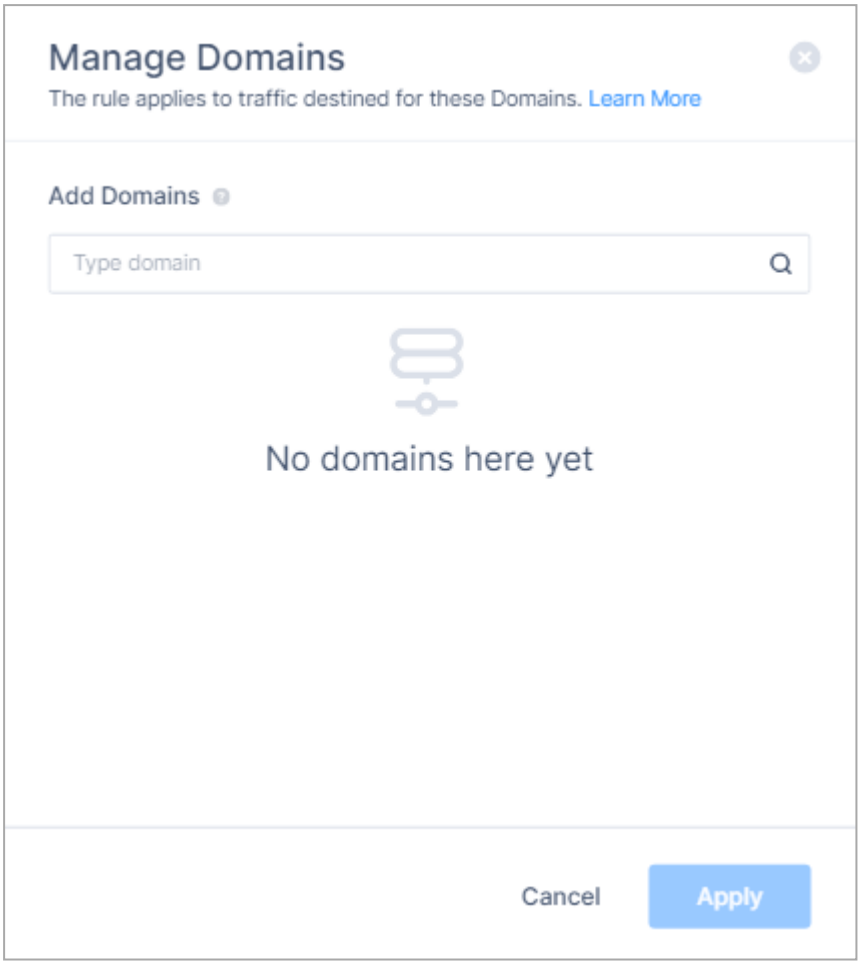


c. Select the categories from the list.

d. Click **Apply**.

e. To add domains, select **Domains**.

The **Manage Domains** window appears.

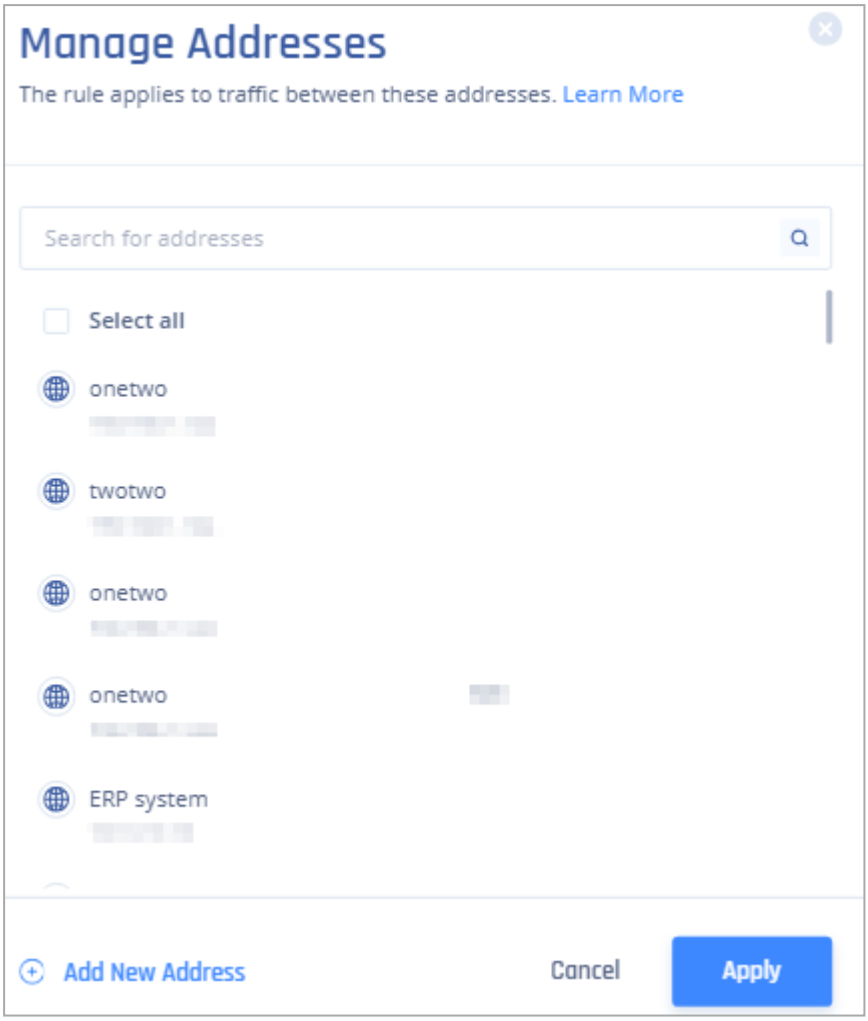


f. Enter the domain name and press **Enter**. For example, `google.com`.

g. Click **Apply**.

h. To add addresses, click **Addresses**.

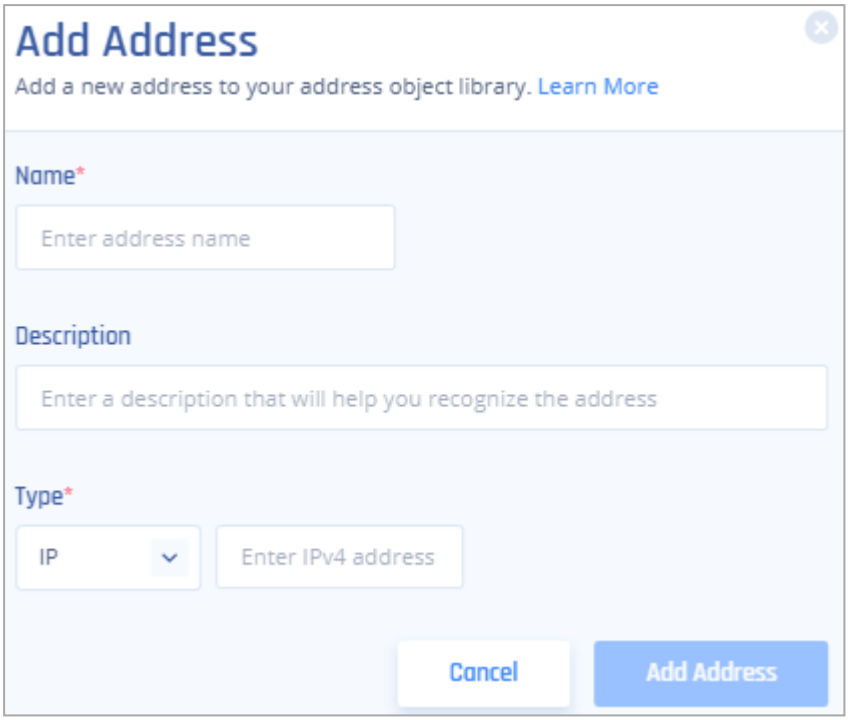
The **Manage Addresses** window appears.



i. Select the address from the list and click **Apply**.

j. To add address, click **Add New Address**.

The **Add Address** window appears.



k. In the **Name** field, enter address name.

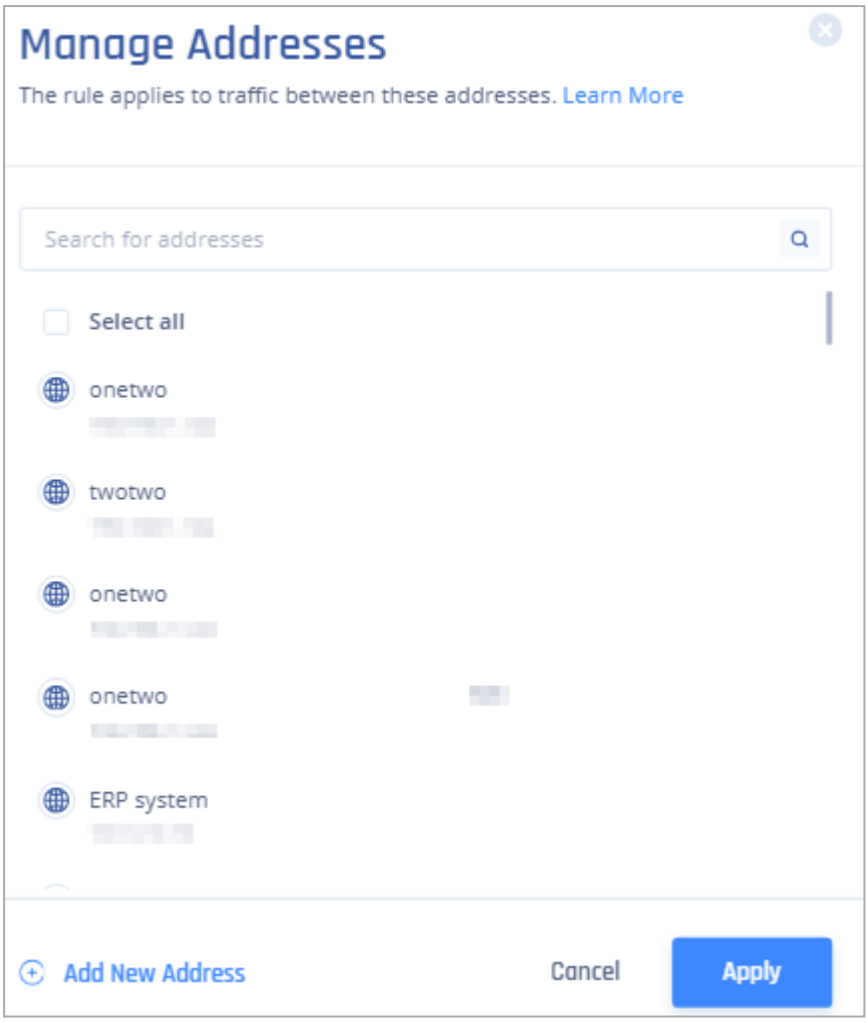
l. In the **Description** field, enter a description.

m. In the **Type** list, select **IP**, **Subnet**, **List**, or **FQDN**.

n. Enter a value, For example:

- For IP, enter the IPv4 address *139.1.1.1*.
- For subnet, enter *10.10.10.0/24*.
- For list, enter IP addresses separated by commas *172.16.254.1, 172.16.254.2*.
- For FQDN, enter the Fully Qualified Domain Name *www.example.com*.

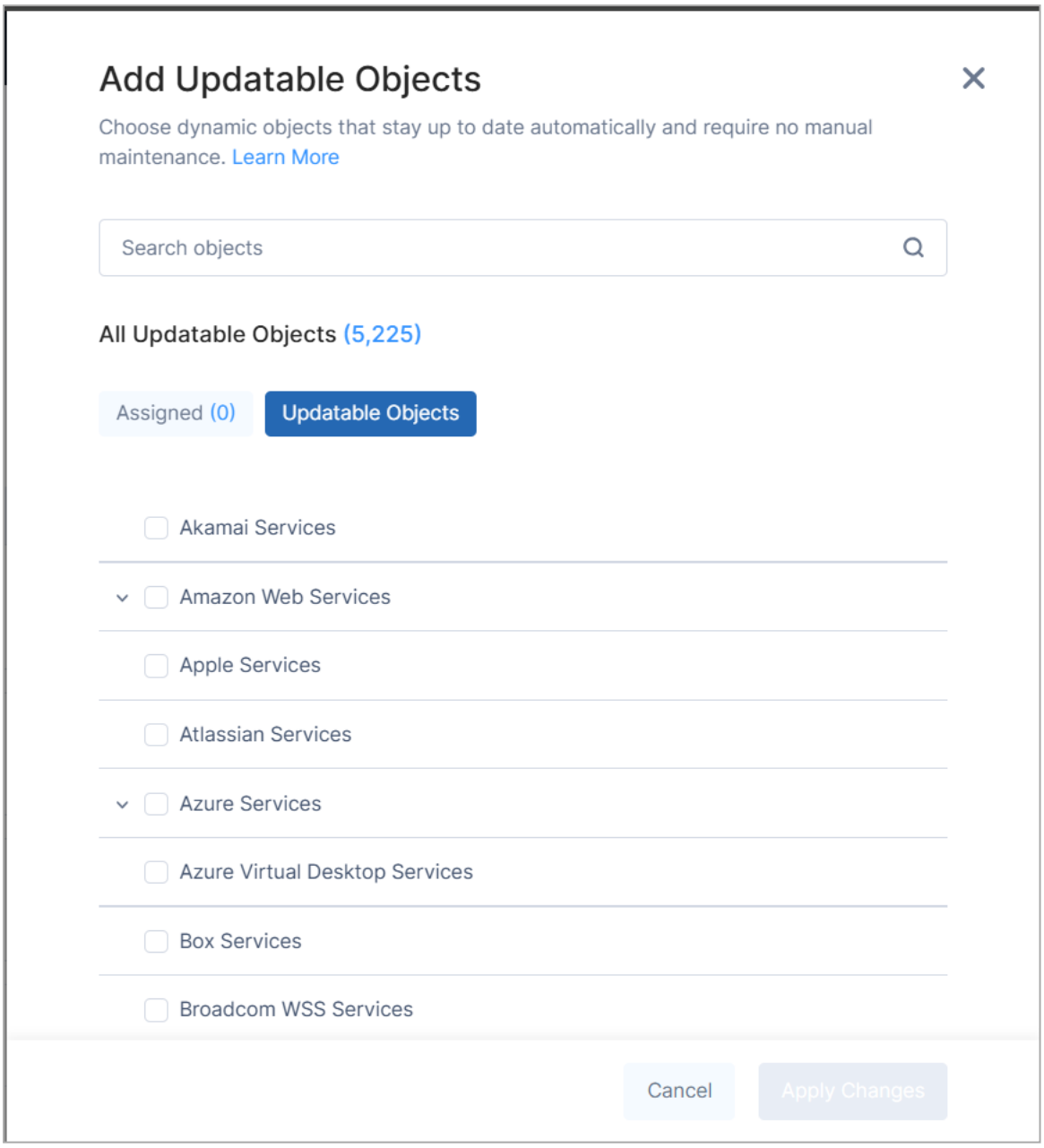
o. Click **Add Address**.



p. Select the address from the list and click **Apply**.

q. To add updatable objects, select **Updatable Objects**.

r. For more information, see *"Updatable Objects" on page 923*.



The **Add Updatable Objects** window appears.

s. Use the **Search Objects** field to find services, or click **Updatable Objects** to select the required services.

t. Selected services appear under the **Assigned** tab.

u. Click **Apply Changes**.

v. Turn on the **Status** toggle button.

w. Click **Apply** in the bottom of the page.

x. Click **Apply**.

Bypass Rules for Certificate Pinning

Certificate Pinning is a security technique used by applications to ensure sever's certificate adheres to certain rules to enhance data security against potential threats. As a result, these applications may not recognize the SASE certificate as valid and blocks the connection.

Check Point recommends to use process name or domain to bypass the traffic to applications that use certificate pinning.

The table lists some of the popular applications that use certificate pinning and provides their domains to bypass:

Application	Program	Domain
Adobe Suite (including Acrobat Reader, Creative Cloud and software updates)	N/A	Fill in these domain lists: ■ List 1 ■ List 2
Apple's iMessages, iTunes, App Store, Mail	N/A	■ p24-keyvalueservice.icloud.com ■ apps.apple.com ■ itunes.apple.com ■ mzstatic.com ■ gs-loc.apple.com ■ gsa.apple.com ■ securemetrics.apple.com ■ swscan.apple.com ■ xp.apple.com ■ ppq.apple.com ■ akadns.net ■ mail.me.com ■ music.apple.com

Application	Program	Domain
AWS Console	N/A	■ console.aws.amazon.com ■ docs.aws.amazon.com ■ signin.aws.amazon.com ■ fls-na.amazon.com ■ cdn.assets.as2.amazonaws.com ■ aws-signin-website-assets.s3.amazonaws.com ■ opfcaptcha-prod.s3.amazonaws.com ■ d1dgtfo2wk29o4.cloudfront.net ■ images-na.ssl-images-amazon.com
Bitdefender	N/A	■ cdn.bitdefender.net ■ download.bitdefender.com ■ login.bitdefender.net ■ login.bitdefender.com ■ nimbus.bitdefender.net ■ push.bitdefender.net ■ upgrade.bitdefender.com
DropBox	■ Dropbox.exe ■ DropboxUpdate.exe DbxSvc.exe ■ com.getdropbox.dropbox ■ com.getdropbox.dropbox.garcon ■ com.getdropbox.dropbox.activityprovider ■ com.getdropbox.dropbox.fileprovider	N/A
Evernote	evernote.exe	■ announce.evernote.com ■ cd1. evernote.com ■ evernote-a.akamaihd.net ■ www.evernote.com

Application	Program	Domain
Google Drive	■ **Windows**: googledrivesync.exe ■ **macOS**: • com.google.drivefs • com.google.drivefs.finderhelper.findersync	N/A
Google Services	N/A	■ alt2-mtalk.google.com ■ android.clients.google.com ■ www.google.com ■ android.googleapis.com ■ cryptauthenrollment.googleapis.com ■ device-provisioning.googleapis.com ■ digitalassetlinks.googleapis.com ■ fcmconnection.googleapis.com ■ fcmtoken.googleapis.com ■ firebaseperusertopics-pa.googleapis.com ■ play.googleapis.com ■ semanticlocation-pa.googleapis.com ■ lh3.googleusercontent.com ■ play-lh.googleusercontent.com ■ gstatic.com ■ gvt1.com
Java Updates	N/A	■ sjremetrics.java.com ■ javadl-esd-secure.oracle.com
LogMeIn	logmein.exe	Fill in this domain list
Microsoft Defender	N/A	Fill in this domain list

Application	Program	Domain
Microsoft Lync and Skype	N/A	▪ lync.com ▪ az801095.vo.msecnd.net ▪ i.s-microsoft.com
Microsoft Office365	Configure within Office365: Go to **Policy** > **URL & Cloud App Control** > **Advanced Settings**.	For outlook, add these domains: ▪ office365.com ▪ office.com
Microsoft OneDrive	N/A	▪ cdn.funcaptcha.com ▪ fpt.live.com ▪ login.live.com ▪ odc.officeapps.live.com ▪ skyapi.policies.live.net ▪ signup.live.com ▪ skyapi.live.net ▪ pipe.aria.microsoft.com ▪ data.microsoft.com ▪ svc.ms ▪ msauth.net ▪ cdn.onenote.net
Microsoft Windows Store	N/A	▪ eus-streaming-video-msn-com ▪ wns.windows.com ▪ live.com ▪ clientconfig.passport.net ▪ wustat.windows.com ▪ windowsupdate.com ▪ msftncsi.com ▪ microsoft.com
Microsoft Updates	N/A	▪ settings-win.data.microsoft.com ▪ vortex-win.data.microsoft.com ▪ delivery.mp.microsoft.com ▪ tsfe.trafficshaping.dsp.mp.microsoft.com ▪ update.microsoft.com ▪ sls.update.microsoft.com

Application	Program	Domain
Slack	■ **Windows**: slack.exe ■ **macOS**: • com.tinyspeck.slackmacgap • com.tinyspeck.slackmacgap.helper	N/A
Spotify	N/A	spotify.com
Webex	■ atmrg.exe ■ wmlhost.exe ■ webexmta.exe ■ washost.exe	webex.com
Zoom	**Windows**: zoom.exe **macOS**: us.zoom.xos	zoom.us

Default Bypass Rules

SASE provides a list of preconfigured bypass rules for applications that use certificate pinning.

Important - Traffic that matches a bypass rule is not inspected and is excluded from Internet Access Policy enforcement, Threat Prevention, and DLP controls. If your organization uses Tenant Restrictions, some of the default bypass rules below may include domains that must be inspected for tenant restriction enforcement. Review your bypass rules and ensure they do not conflict with the required domains listed in the Tenant Restrictions configuration requirements.

To view the default bypass rules, access **Check Point SASE** and click **Internet Access** > **Bypass Rules**. The default bypass rules disappear if you add new bypass rules.

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Microsoft Teams - Pre-configured	Enabled	Any	▪ com.microsoft.teams ▪ Teams.exe	N/A	N/A
Bypass sensitive traffic - Pre-configured	Disabled	Any	Any	N/A	Financial Services, Government, Health and Medicine, Legal
Bypass Microsoft Outlook - Pre-configured	Enabled	Programs	▪ com.microsoft.Outlook.exe ▪ outlook.exe	N/A	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Microsoft updates - Pre-configured	Enabled	Any	Any	▪ settings-win.data.microsoft.com ▪ vortex-win.data.microsoft.com ▪ delivery.mp.microsoft.com ▪ tsfe.trafficshaping.dsp.mp.microsoft.com ▪ update.microsoft.com ▪ sls.update.microsoft.com	N/A
Bypass Adobe updates - Pre-configured	Enabled	Any	Any	▪ adobe.com ▪ adobetag.com	N/A
Bypass Java updates - Pre-configured	Enabled	Any	Any	▪ sjremetrics.java.com ▪ javadl-esd-secure.oracle.com	N/A
Bypass Mozilla Firefox updates - Pre-configured	Enabled	Any	Any	download-installer.cdn.mozilla.net	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass AWS console - Pre-configured	Enabled	Any	Any	▪ console.aws.amazon.com ▪ docs.aws.amazon.com ▪ signin.aws.amazon.com ▪ fls-na.amazon.com ▪ cdn.assets.as2.amazonaws.com ▪ aws-signin-website-assets.s3.amazonaws.com ▪ opfcaptcha-prod.s3.amazonaws.com ▪ d1dgtfo2wk29o4.cloudfront.net ▪ Images-na.ssl-images-amazon.com	N/A
Bypass Dropbox - Pre-configured	Enabled	Programs	▪ Dropbox.exe ▪ DropboxUpdate.exe ▪ DbxSvc.exe ▪ com.getdropbox.dropbox ▪ com.getdropbox.dropbox.garcon ▪ com.getdropbox.dropbox.activityprovider ▪ com.getdropbox.dropbox.fileprovider	N/A	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Google services - Pre-configured	Enabled	Any	Any	▪ alt2-mtalk.google.com ▪ android.clients.google.com ▪ www.google.com ▪ android.googleapis.com ▪ cryptauthenrollment.googleapis.com ▪ device-provisioning.googleapis.com ▪ digitalassetlinks.googleapis.com ▪ fcmconnection.googleapis.com ▪ fcmtoken.googleapis.com ▪ firebaseperusertopics-pa.googleapis.com ▪ play.googleapis.com ▪ semanticlocation-pa.googleapis.com ▪ lh3.googleusercontent.com ▪ play-lh.googleusercontent.com ▪ gstatic.com ▪ gvt1.com	N/A
Bypass Google Drive - Pre-configured	Enabled	Programs	▪ googledrivefs.exe ▪ com.google.drivefs ▪ com.google.drivefs.finderhelper.findersync	N/A	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass OneDrive - Pre-configured	Enabled	Any	Any	▪ cdn.funcaptcha.com ▪ fpt.live.com ▪ odc.officeapps.live.com ▪ skyapi.policies.live.net ▪ signup.live.com ▪ skyapi.live.net ▪ pipe.aria.microsoft.com ▪ data.microsoft.com ▪ svc.ms ▪ msauth.net ▪ cdn.onenote.net	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Goto [LogMeIn] - Pre-configured	Enabled	Any	Any	■ *.accounts.logme.in ■ *.app.goto.com ■ *.cdn.walkme.com ■ *.cdngetgo.com ■ *.clientstream.launchdarkly.com ■ *.cloudfront.net ■ *.expertcity.com ■ *.filestackapi.com ■ *.getgo.com ■ *.getgocdn.com ■ *.getgoservices.com ■ *.getgoservices.net ■ *.gofastchat.com ■ *.goto.com ■ *.goto.eu ■ *.goto-rtc.com ■ *.gotoinc.com ■ *.gotostage.com ■ *.gotowebinar.com ■ *.ingest.sentry.io ■ *.internap.net ■ *.internapcdn.net ■ *.joinwebinar.com ■ *.launchdarkly.com ■ *.logmein.com ■ *.logmein.eu ■ *.logmeininc.com ■ *.psyjs-cdn.nuvixa.com ■ *.psyjs-cdn.personify.live ■ *.webinar.com ■ api.filepicker.io ■ builds.cdn.getgo.com ■ builds.cdn.goto.com	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
				▪ goto-desktop.s3.amazonaws.com ▪ launch.getgo.com ▪ meet.goto.com	
Bypass Microsoft Lync and Skype - Pre-configured	Enabled	Any	Any	▪ lync.com ▪ az801095.vo.msecnd.net ▪ i.s-microsoft.com	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Apple services - Pre-configured	Enabled	Any	Any	▪ p24-keyvalueservice.icloud.com ▪ apps.apple.com ▪ itunes.apple.com ▪ mzstatic.com ▪ gs-loc.apple.com ▪ gsa.apple.com ▪ securemetrics.apple.com ▪ swscan.apple.com ▪ xp.apple.com ▪ ppq.apple.com ▪ akadns.net ▪ mail.me.com ▪ music.apple.com ▪ configuration.apple.com ▪ gdmf.apple.com ▪ gg.apple.com ▪ gs.apple.com ▪ ig.apple.com ▪ mesu.apple.com ▪ oscdn.apple.com ▪ osrecovery.apple.com ▪ skl.apple.com ▪ swcdn.apple.com ▪ swdist.apple.com ▪ swdownload.apple.com ▪ updates-http.cdn-apple.com ▪ updates.cdn-apple.com	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Bypass Bitdefender services - Pre-configured	Enabled	Any	Any	▪ cdn.bitdefender.net ▪ download.bitdefender.com ▪ login.bitdefender.net ▪ login.bitdefender.com ▪ nimbus.bitdefender.net ▪ push.bitdefender.net ▪ upgrade.bitdefender.com	N/A
Bypass Zoom - Pre-configured	Enabled	Any	▪ Zoom.exe ▪ com.zoom.video	N/A	N/A
Bypass Webex - Pre-configured	Enabled	Any	Any	webex.com	N/A
Bypass Spotify - Pre-configured	Enabled	Any	Any	spotify.com	N/A
Check Point Updates - HTTPS bypass	Enabled	Any	Any	▪ avupdates.checkpoint.com ▪ secureupdates.checkpoint.com ▪ updates.checkpoint.com	N/A

Rule Name	Default Status	Source	Programs	Domains	Categories
Dashlane - HTTPS bypass	Enabled	Any	Any	▪ dashlane.com ▪ *.dashlane.com	N/A
Facebook - HTTPS bypass	Disabled	Any	Any	*.facebook.com	N/A
Finch VPN - HTTPS bypass	Enabled	Any	Any	▪ amber.finchapi.com ▪ www.finchvpn.com	N/A
MyQuickCloud - HTTPS bypass	Enabled	Any	Any	*.myquickcloud.com	N/A

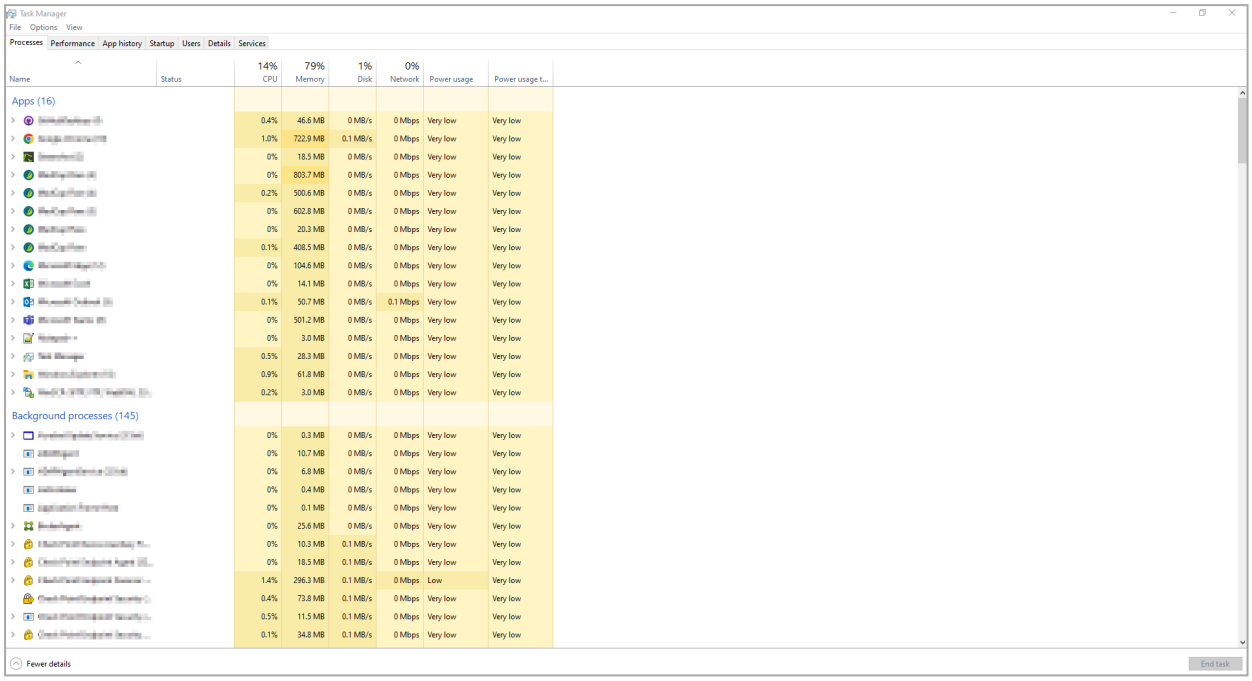
Rule Name	Default Status	Source	Programs	Domains	Categories
Elsterde - HTTPS bypass	Enabled	Any	Any	▪ *.elster.de ▪ datenannahme1.elster.de ▪ datenannahme2.elster.de ▪ datenannahme3.elster.de ▪ datenannahme4.elster.de ▪ datenannahme5.elster.de ▪ datenannahme6.elster.de ▪ datenannahme7.elster.de ▪ datenannahme8.elster.de ▪ datenannahme9.elster.de ▪ datenannahme0.elster.de ▪ datenannahme.elster.de	N/A

Finding the Process Name of an Application

You can use the process name to bypass the traffic to the application that uses certificate pinning.

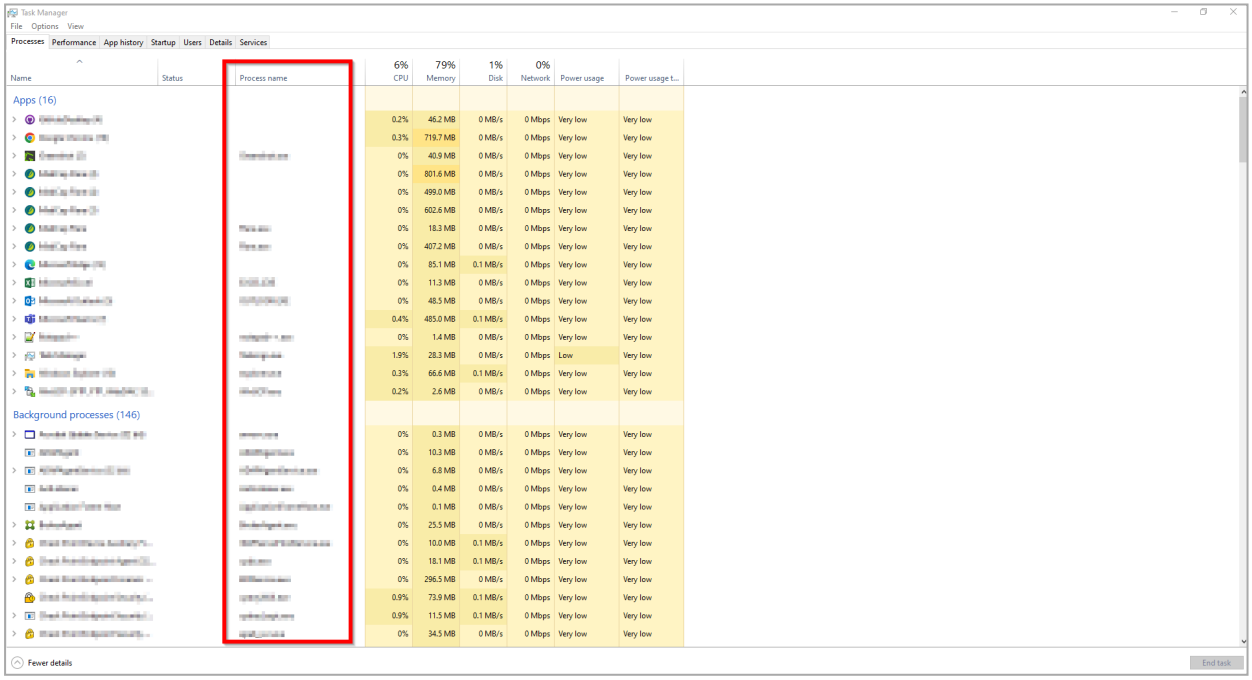
To find the process name in Windows:

1. Open **Task Manager**.



2. Right-click any column in the **Processes** tab and select **Process name**.

   The **Process name** column appears in the table.



3. Search for your application and copy the process name.

To find the process name in macOS, do one of these:

- Go to **Activity Monitor**:
  a. Select the application's process.
  b. Click **View** and select **Inspect Process**.
  c. Go to **Sample** > **Binary Images**.
  d. Identify the process name from the first item in the list.
- Go to **Finder**:
  a. Navigate to the **Applications** folder.
  b. Select the application.
  c. Right-click the application and select **Show Package Contents**.
  d. Go to the **Contents** folder and open the **Info.plist** file.
  e. Find the process name next to the **CFBundleIdentifier** key.

To find the process name in Linux:

1. Run this command in the terminal:

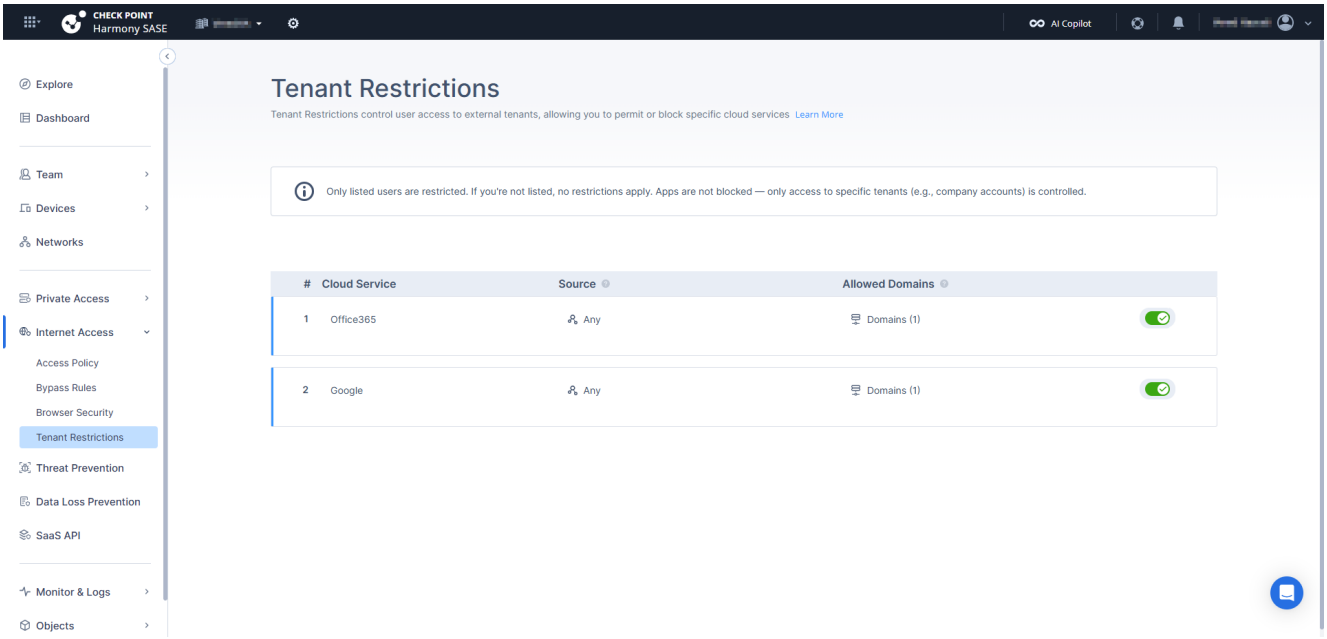
   ```
   ps aux | grep <application_name>
   ```

   The process name is displayed in the second-to-last column of the output.

Tenant Restrictions

Tenant Restrictions allow administrators to control which Microsoft Office 365 and Google Workspace tenants users can access. It helps prevent unauthorized access to personal or unapproved corporate tenants, ensuring users only connect to organization approved environments. This reduces the risk of data leaks and unauthorized third-party collaborations.

To view the **Tenant Restrictions** page, access the SASE Administrator Portal and click **Internet Access** > **Tenant Restrictions**.



Column	Description
Cloud Service	Displays the cloud service for which the restriction is applied: ■ Microsoft Office 365 ■ Google Workspace This column is auto-populated and cannot be edited.
Source	Defines the groups or members the restriction applies to: ■ Any (default)- Applies to all users. ■ Groups or Members - Applies to selected groups or users from your identity provider.
Allowed Domains[1]	Specifies the domains that users in the selected source groups and users are allowed to access. You can add domains and tenant IDs in various formats: ■ Standard domain, for example, `contso.com` ■ Microsoft domain, for example, `fabrikam.onmicrosoft.com` ■ Tenant identifier, for example, `aaaabbbb-0000-cccc-1111-dddd2222eeee`

[1]Avoid setting the Allowed Domains value to **Any**, as this configuration has no effect on domain restrictions and does not limit access. Specify one or more domains explicitly to ensure the restriction is applied as intended.

Configuration Requirements for Tenant Restrictions

To enable tenant restrictions enforcement:

- Ensure that traffic to Microsoft Office 365 and Google Workspace is inspected. The following domains must be inspected and not bypassed:
  - Microsoft 365:
    - login.microsoftonline.com
    - login.microsoft.com
    - login.windows.net
    - login.live.com

    For more information, see Microsoft 365 documentation.
  - Google Workspace: *.google.com

    For more information, see Google Workspace documentation.
- Do not bypass these applications in the Bypass policy. For more information, see Certificate Pinning.
- Do not block these applications in the Access policy.

This configuration allows SASE to apply tenant restriction rules and validate user access to authorized tenants.

Supported Applications

Tenant Restrictions supports these applications:

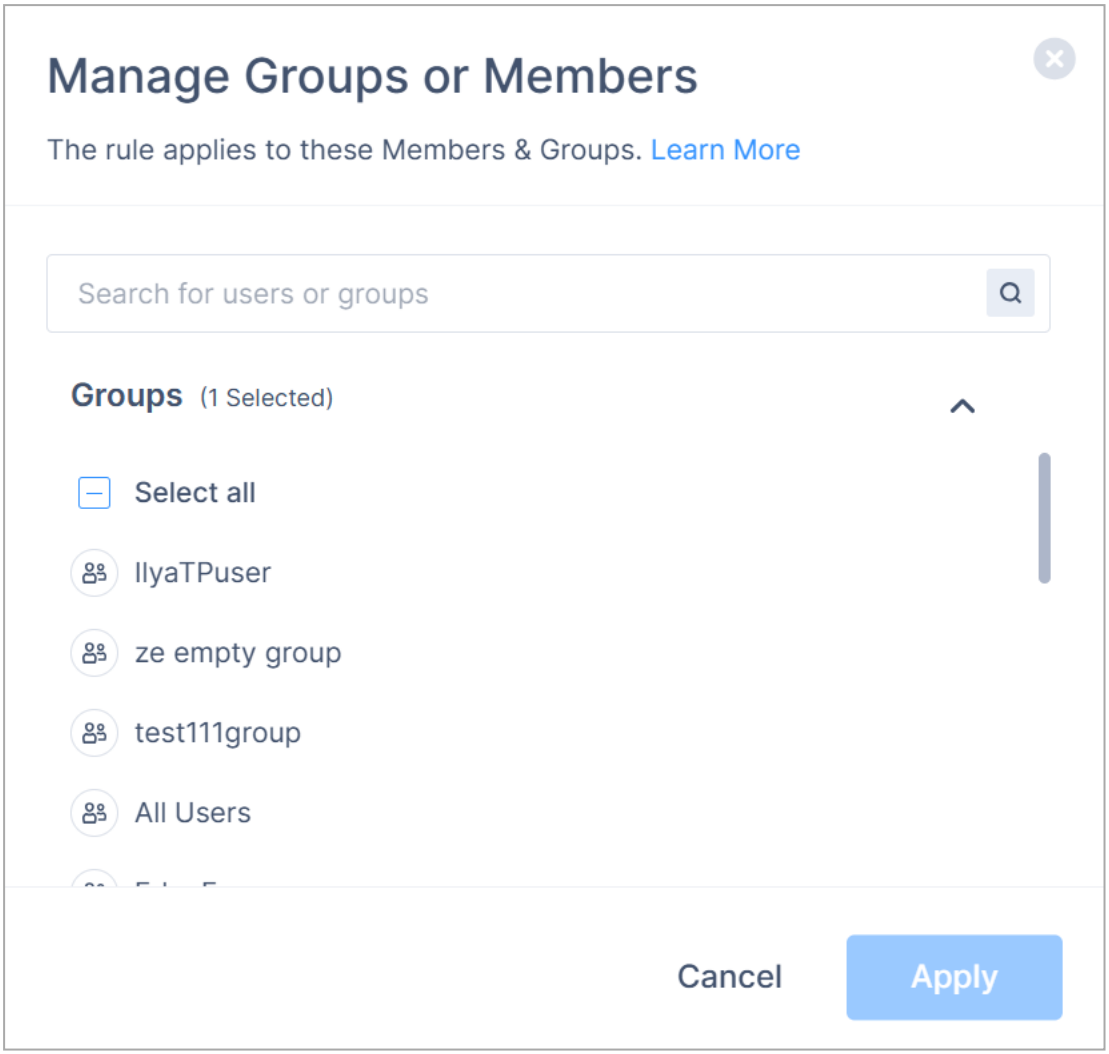
- Microsoft Office 365
- Google Workspace

Creating a Tenant Restriction

1. Access the SASE Administrator Portal and click **Internet Access**.
2. Go to **Tenant Restrictions**.
3. For the cloud service you want to add a restriction, do these:
   a. In the **Source** field, add groups or users list to which you want to apply the rule. Default is **Any**.

b. Click **Any** > **Add Source** > **Groups or Members**.

The **Manage Groups or Members** window appears.



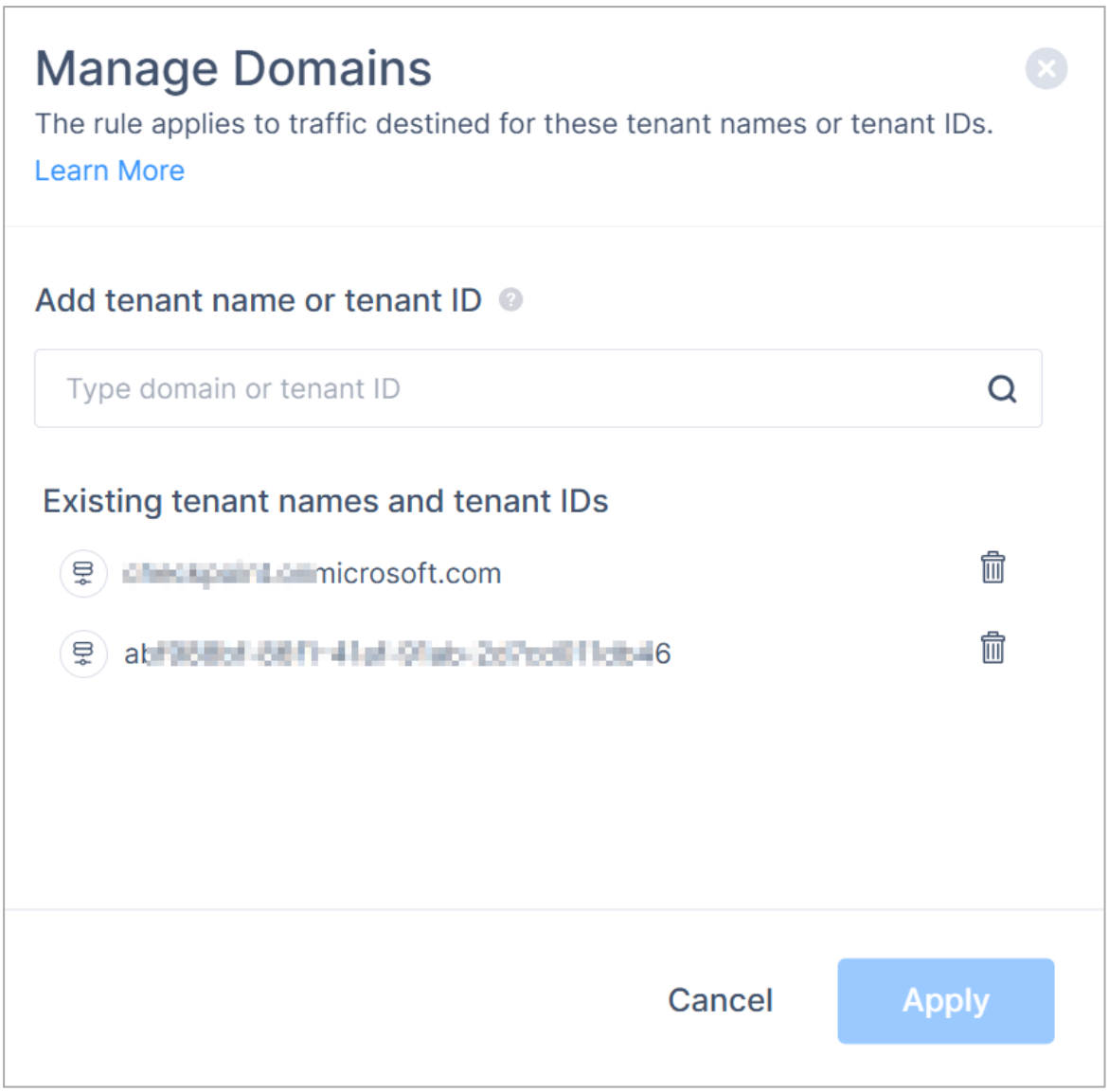
c. Select group(s) or member(s) from the list.

d. Click **Apply**.

e. In the **Allowed Domains** field, select the domain(s) or tenant ID(s) that you want to allow or restrict for access.

f. Click **None** > **Add Allowed Domain** > **Domains or Tenant IDs**.

The **Manage Domains** window appears.



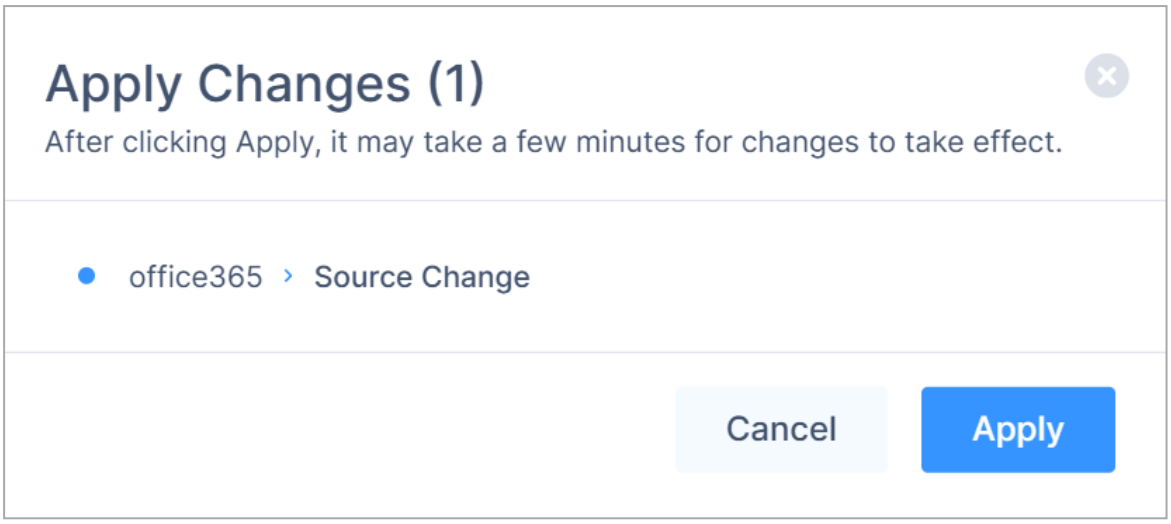
g. Select the domain(s) or tenant ID(s).

h. Click **Apply**.

i. To activate the rule, turn on the **Status** toggle button.

j. Click **Apply** in the bottom of the page.

k. Click **Apply**.



Notes:

- Each application support a single configuration. Rules are not prioritized or matched in order.
- All changes to the Tenant Restrictions configuration (for example, domain updates, enabling or disabling rules) are recorded in the administrator audit log.
- Restriction enforcement occurs on the end user side within the SaaS application. For more information, see Microsoft 365 documentation.
- Changes are applied as part of the Internet Access policy and are enforced by the Internet Access engine once you click **Apply**.

End User Behavior

When Tenant Restrictions are enabled, users experience these behaviors based on their actions:

Scenario	User Experience
User accesses an allowed tenant	Access proceeds normally.
User accesses a disallowed tenant	A block page is displayed by the SaaS application (for example, Microsoft Office 365 and Google Workspace), indicating that access is not permitted.
User accesses another SaaS application	No restriction is enforced, and access is allowed (for example, Salesforce and Atlassian).

Threat Prevention Policy

Threat Prevention is a security solution that protects your workspace from advanced threats.

This topic explains how to configure and manage the Threat Prevention policy to secure your organization against cyber risks.

Threat Prevention extends the Secure Web Gateway capabilities in SASE, offering advanced protection against cyber threats. It integrates three key security technologies:

1. Malware Protection: Scans files, downloads, and web content to detect and block malicious code before it infects your systems. It uses advanced detection engines to identify known malware signatures and suspicious behavior.
2. Threat Emulation: Leverages sandboxing technology to analyze suspicious files in a controlled environment. This detects zero-day threats and advanced attacks that may bypass traditional defenses by analyzing files for malicious behavior without affecting your production systems.
3. Anti-Bot: Protects users by blocking access to malicious websites and preventing communication with command-and-control servers. It assesses website reputation and prevents infected devices from reaching harmful servers.

The integration of these three technologies creates multiple layers of protection against various attack vectors:

- **Pre-execution Protection**: Blocks known threats before execution.
- **Behavioral Analysis**: Monitors file behavior in the sandbox to detect suspicious activities.
- **Post-infection Control**: Stops infected devices from communicating with malicious servers.

This multi-layered approach significantly enhances your security posture by addressing threats at different stages of the attack lifecycle.

Threat Prevention Components

To challenge today's malware landscape, Threat Prevention solution offers a multi-layered, pre- and post-infection defence approach and a consolidated platform that enables enterprise security to detect and block modern malware.

These Threat Prevention protections are available:

- **Malware Protection** - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus protection is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.

- **Threat Emulation** - Each protection is unique. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention protections and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention protections.
- **Anti-Bot** - Prevents damage by blocking communication with dangerous URLs, particularly command-and-control servers for malicious bots. Anti-Bot is continuously updated from ThreatCloud, an AI-powered collaborative, distributed defense network and database to fight security threats.

Malware Protection

Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats (combinations of malicious code and vulnerabilities for infection and dissemination) and trojans.

The Malware protection scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from threats contained in these files. The Malware protection is also supported by the Threat Prevention API.

The Malware protection:

- Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository:
  - Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance.
  - Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place.
- Uses the ThreatCloud repository to receive binary signature updates and query the repository for Anti-Bot and malware protection classification.

Threat Emulation

Threat Emulation gives networks the necessary protection against unknown threats in web downloads. The Threat Emulation engine picks up malware at the exploit phase, before it enters the network. It quickly quarantines and runs the files in a virtual sandbox, which imitates a standard operating system, to discover malicious behavior before hackers can apply evasion techniques to bypass the sandbox.

Threat Emulation receives files through these methods of delivery

- Web downloads
- Files sent to Threat Emulation through the Threat Prevention API

When emulation is done on a file, it is observed for malicious behavior in a cloud-based security sandbox.

If the file is found to be not malicious, you can download the file after the emulation is complete.

Anti-Bot

A bot is malicious software that can infect your computer. It is possible to infect a computer when you open attachments that exploit a vulnerability or go to a web site that results in a malicious download.

When a bot infects a computer, it connects to a command-and-control server where it receives instructions to carry out malicious tasks.

One bot can often create multiple threats. Bots are frequently used as part of Advanced Persistent Threats (APTs) where cyber criminals try to damage individuals or organizations.

Our Anti-Bot mechanism prevents bots from communicating with their command-and-control servers, which reduces their threat significantly.

After the discovery of a communication attempt, SASE blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and prevents sensitive information from being sent out.

Risk Calculation

Threat Prevention uses a risk-based approach with values from 0-100, which simplifies threat assessment through a single interpretable value:

Risk Range	Description	Confidence	Severity
Risk = 0	Indications of a legitimate website	High	N/A
0 < Risk < 10	Internet long tail (low-traffic sites)	Low or Medium	Low
10 <= Risk < 50	Adware servers, rogue popup URLs	Low, Medium, or High	Low or Medium
Risk = 50	Anonymizers, parked websites, unknown files	Medium or High	Medium

Risk Range	Description	Confidence	Severity
50 < Risk < 80	No proven legitimate activity observed	Low	High or Critical
80 <= Risk < 100	No proven legitimate activity, suspicious behavior	Medium	High or Critical
Risk = 100	Known malicious resource, identified by a trusted vendor	High	High or Critical

Risk Range is determined by combining:

- **Confidence** - The threat intelligence teams certainty about the assessed severity level.
- **Severity** - The inherent danger of the threat itself.

Higher Confidence and higher Severity generally result in higher Risk Ranges, calculated through a weighted scoring system.

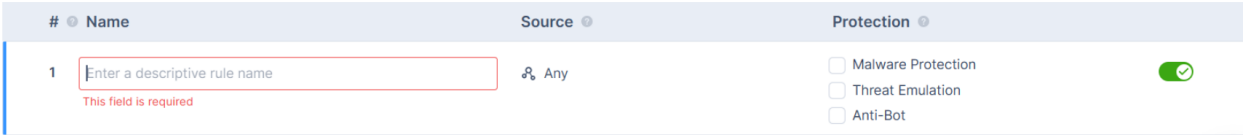
Configuring and Managing Threat Prevention Policy

Note - The Threat Prevention policy runs only in prevent mode (blocks the detected threats).

To create a Threat Prevention policy:

1. Access the SASE Administrator Portal and click **Threat Prevention**.
2. Click **Add New Rule**.

   A new row appears in the table.



3. Specify these:

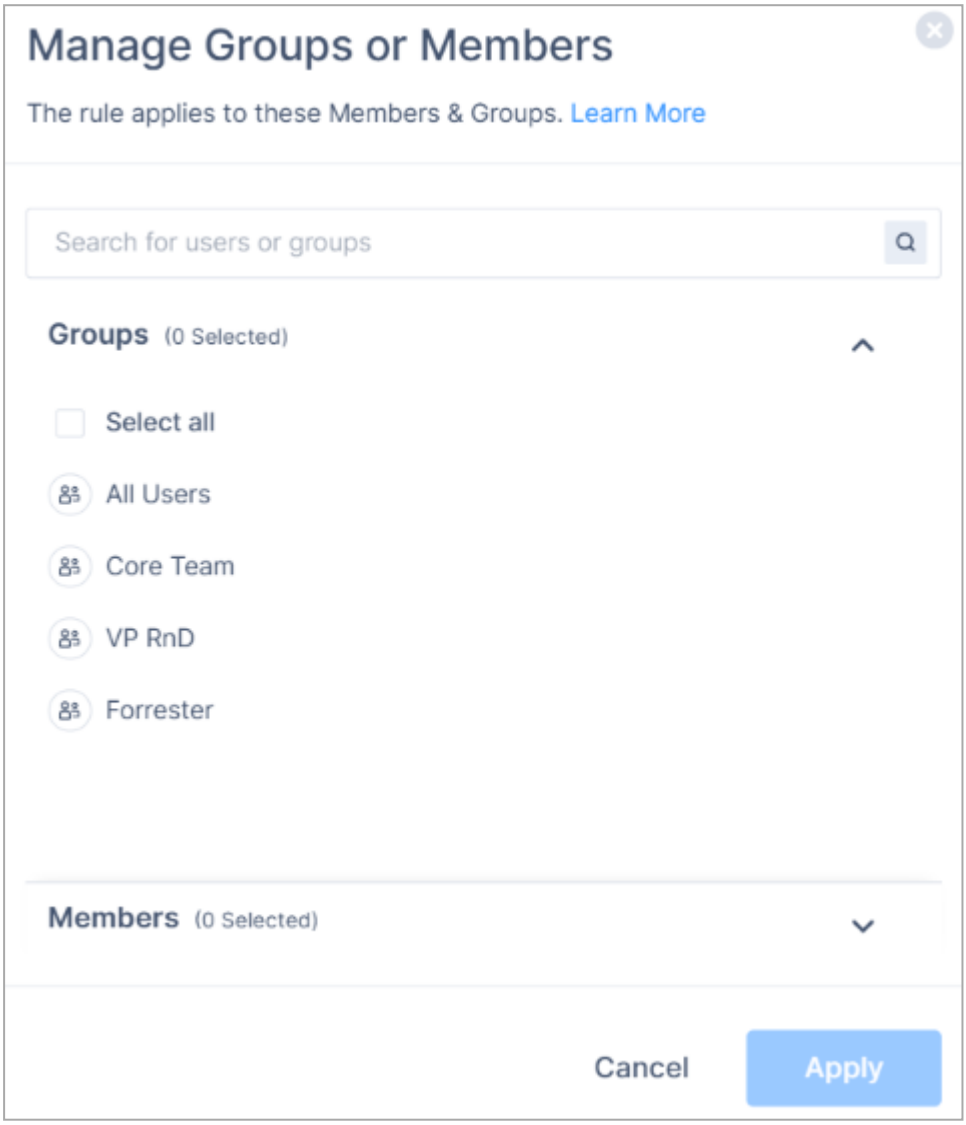
a. In the **Name** column, enter a descriptive name for the rule.

b. In the **Source** column, select to whom this rule should apply:

   i. **Any** (default) - Applies to all resources.

   ii. **Groups or Members** - To add groups or members, hover over the source column and click **Add Source**.

   The **Manage Groups or Members** window appears.



   i. From the **Groups** section, select group(s).

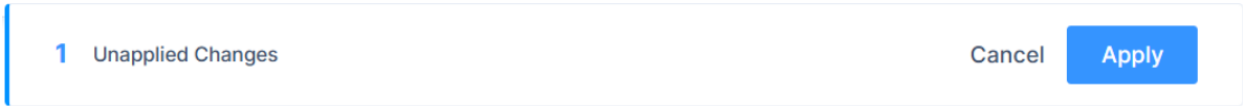
   ii. From the **Members** section, select user(s).

   iii. Click **Apply**.

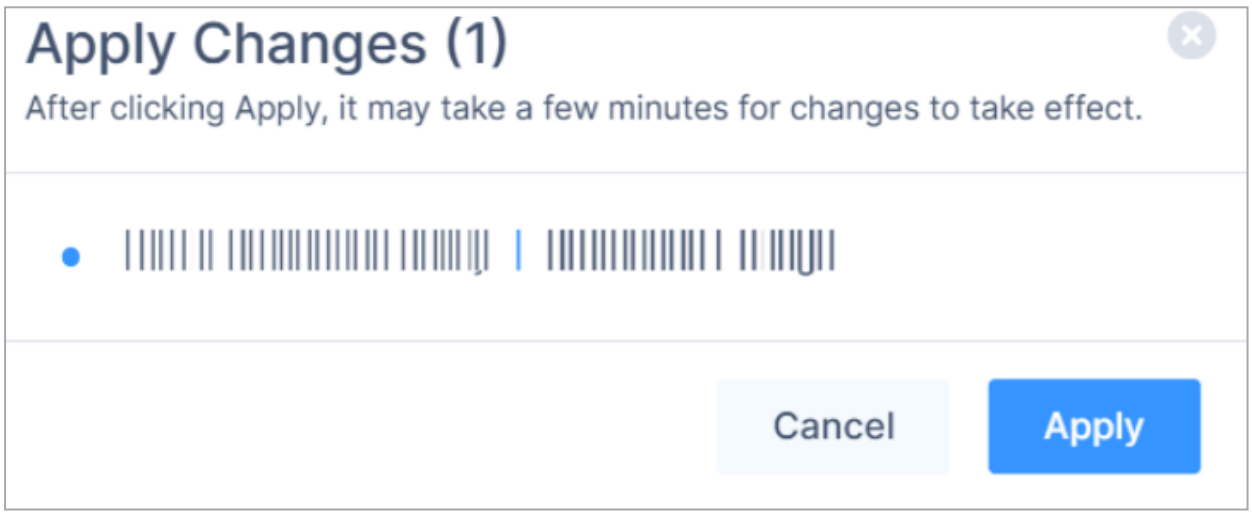
c. In the **Protection** column, select the types of protection this rule should provide:
   - Malware Protection
   - Threat Emulation
   - Anti-Bot

d. Turn on the toggle button, to enable the rule.

4. Click **Apply**.



5. The **Apply Changes** window appears.



6. Click **Apply**.

Notes:

- Rule Enforcement Considerations:
  - **Top-down Processing**: Rules are processed from top to bottom.
  - **First Match Application**: Only the first matching rule is applied to a user, even if other rules also match.
  - **Rule Order**: Carefully order rules to ensure that more general rules don't override more specific ones. Since the system only enforces the first matching rule, rule order directly impacts enforcement.
  - **Logging**: Logging is enabled by default for all threat prevention rules and cannot be disabled.
- Licensing and Deployment:
  - Threat Prevention is part of the Internet Access (SWG) Suite.
  - Activate all features with the correct license to enable all Threat Prevention features.
  - The Agent version is v11.5 or later for full policy enforcement.
- File Inspection:
  - Threat Prevention supports unencrypted files up to 10 MB.
  - Encrypted files or files larger than 10 MB are not inspected. A Skip log entry is recorded.

Logs and Monitoring

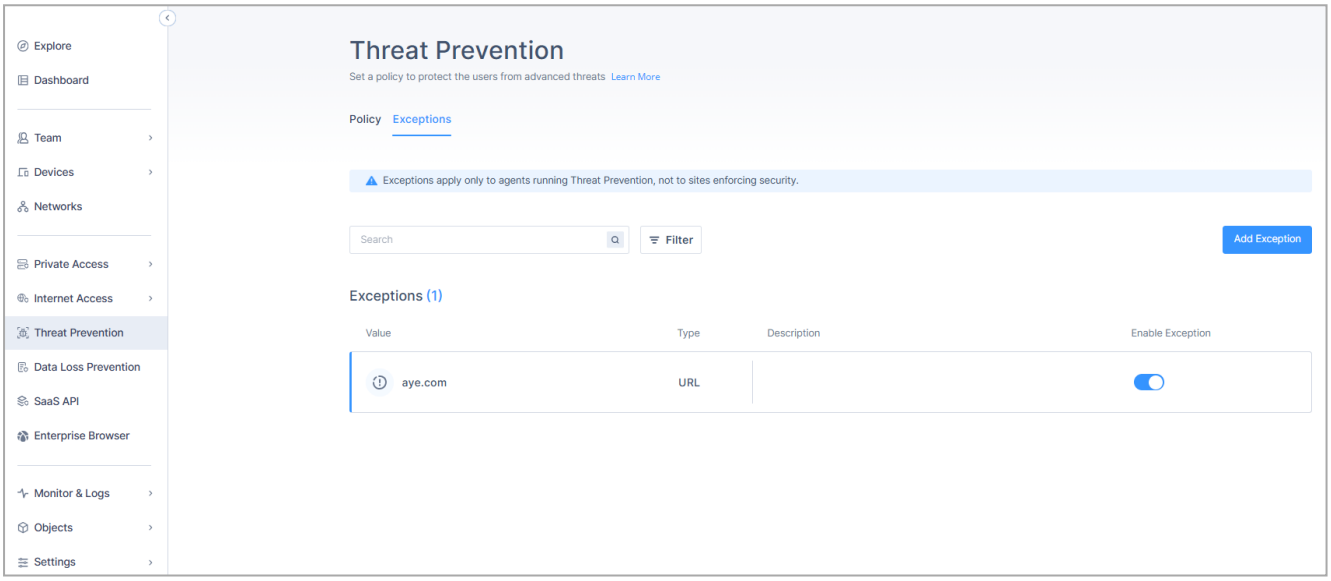
- All Threat Prevention events are sent to Infinity Events.
- Each protection type (Malware Protection, Threat Emulation, and Anti-Bot) generates specific log entries.
- Logs include details, such as risk score, action taken, and threat information.

Threat Prevention Exceptions

Threat Prevention exceptions allow administrators to handle false positives safely without disabling entire security blades. By defining exceptions for specific URLs or files, organizations can maintain user productivity while preserving a strong security posture.

You can manage all exceptions from the Exceptions tab. This page allows you to create, edit, delete, and search for exceptions efficiently.

To access the **Exceptions** tab, access the SASE Administrator Portal, click Threat Prevention, and then click the **Exceptions** tab.



Example Use Case

- Whitelisting a false-positive file based on its SHA256 hash.
- Creating exceptions from user-submitted false-positive reports.

Key Concept

Threat Prevention exceptions provide flexibility in managing cases where legitimate resources are blocked by security policies.

Key Principles

- URL exceptions take precedence over file exceptions.
- File identification uses SHA256 hash values.
- URL exceptions apply to both HTTP and HTTPS protocols.

- Domain-level exceptions include all subdomains and paths (example, `*.microsoft.com*` or `*.microsoft.com/*`).
- SHA-256-based exceptions are not supported by the Anti-Bot blade.

Note - The exceptions apply globally across the entire Threat Prevention policy and all security profiles. They are not limited to individual rules and across all profiles.

URL Exceptions

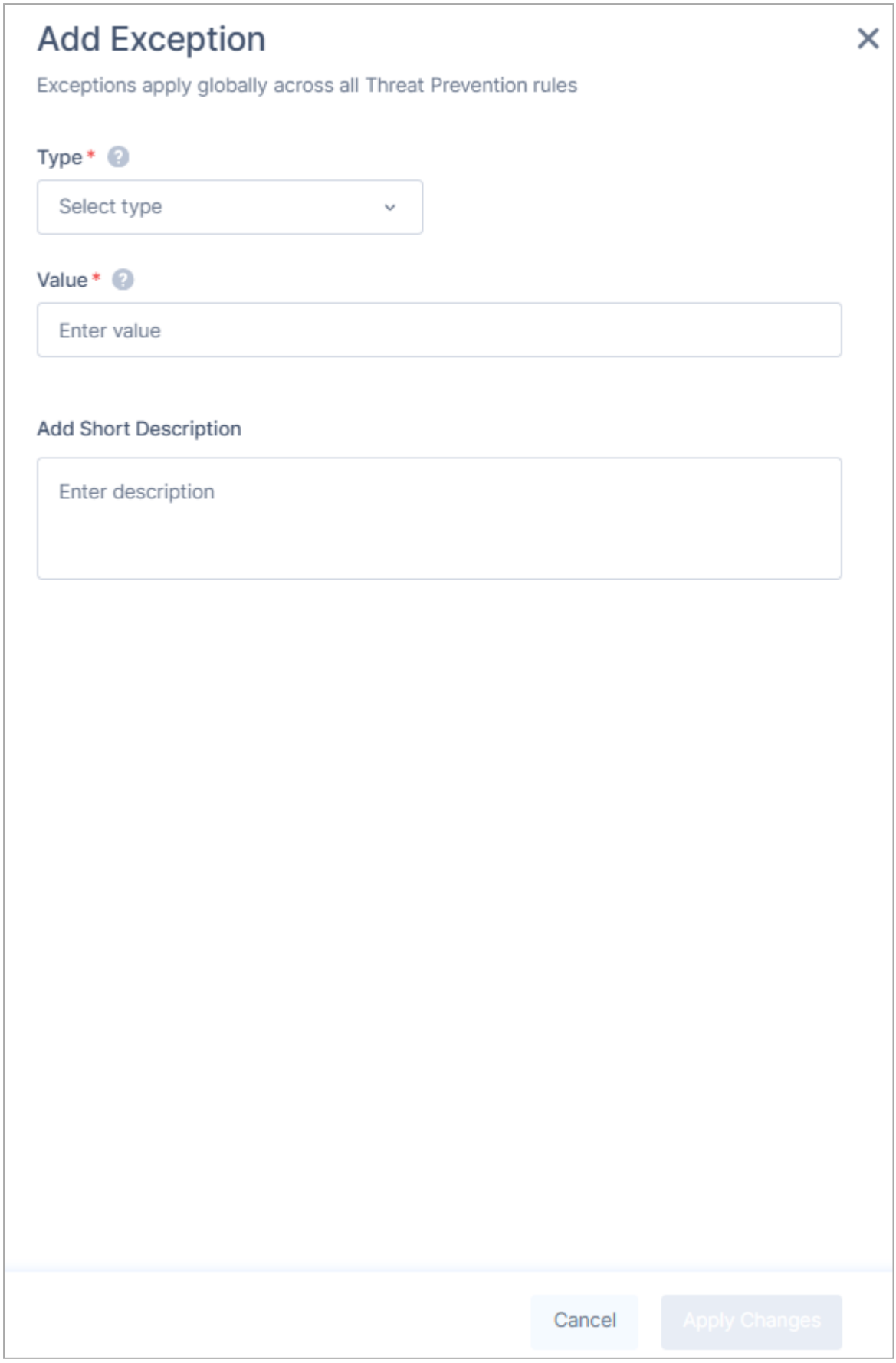
URL exceptions allow administrators to whitelist specific domains or URLs that were previously identified as malicious or risky. URL exceptions support wildcard entries and apply to both HTTP and HTTPS traffic.

Creating URL Exceptions

To create a URL Exception:

1. Access the SASE Administrator Portal, click **Threat Prevention**, and then click the **Exceptions** tab.
2. Click **Add Exception**.

   The **Add Exception** window appears.



3. From the **Type** list, select **URL**.

4. In the **Value** field, enter the full domain or URL. To allow all subdomains, use a wildcard (example, `*.microsoft.com`).

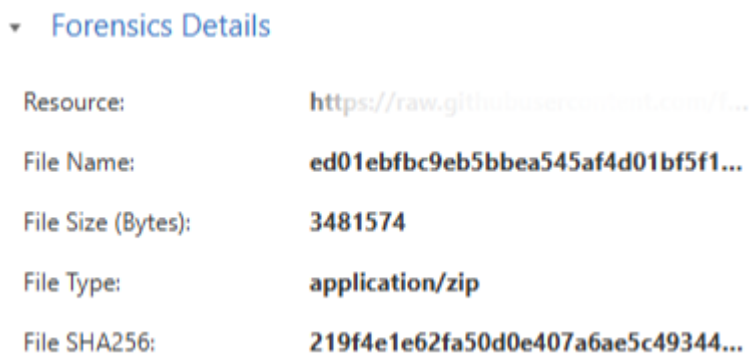
   Note - Use a valid URL without `http/https`, `?`, or `#`. Include `www` if part of the domain. Wildcards (*) are allowed only at the start of the domain (example, `*.example.com`).

5. (Optional) In the **Add Short Description** field, enter a description with expiration date.
6. Click **Apply Changes**.

File Exceptions

File exceptions are used when legitimate files are flagged as malicious by Threat Prevention. The system supports the SHA256 hash identifier.

Note - The hash identifier can be obtained from the security log which blocked the file.

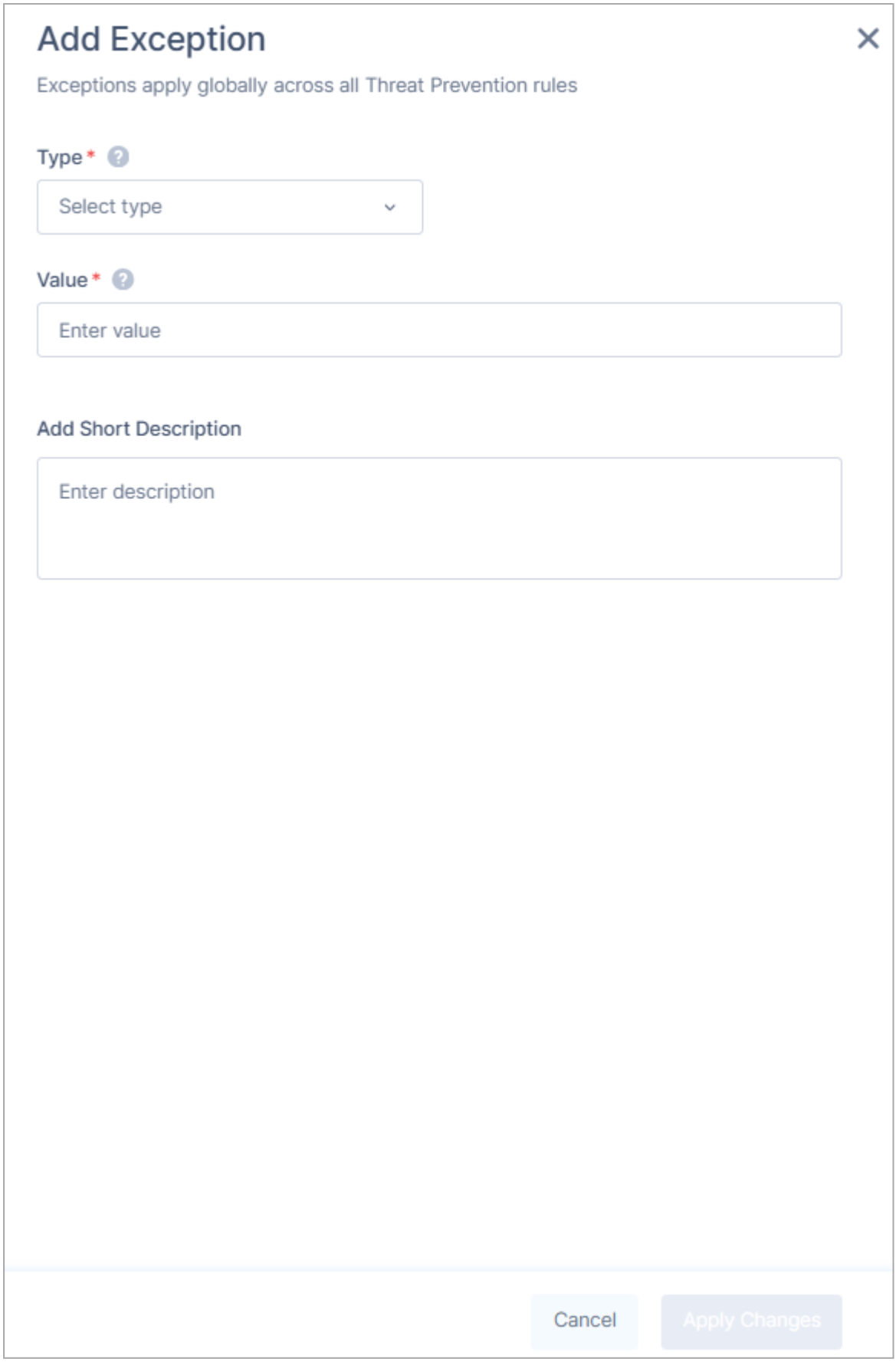


Creating File Exceptions

To create a File Exception:

1. Access the SASE Administrator Portal, click **Threat Prevention**, and then click the **Exceptions** tab.
2. Click **Add Exception**.

   The **Add Exception** window appears.



3. From the **Type** list, select **File Hash**.

4. In the **Value** field, enter the file's SHA256 hash exactly as it appears (64 characters, in hexadecimal format).
5. (Optional) In the **Add Short Description** field, enter a description.
6. Click **Apply Changes**.

Managing Exceptions

The Exceptions page provides a complete list of all configured exceptions.

1. To delete an exception, hover over the exception row that you want to delete, scroll to the end of the table, and click .
2. To duplicate an exception, hover over the exception row that you want to duplicate, scroll to the end of the table, and click .
3. To edit an exception, do either of these:
   - Hover over the exception row that you want to edit, scroll to the end of the table, and click .
   - Click the exception row that you want to edit.

     The **Manage Exception** window appears.
4. Make the required changes.
5. Click **Apply Changes**.

Exception Properties Reference

Property Name	Type	Description
Type	List	Values: ■ URL ■ SHA256
Value	String (500)	The URL or Hash value
Description	String (1000)	Optional description
Status	Boolean	Enabled or Disabled. The default value is Enabled.

Notes:

- Use wildcards carefully, and avoid broad exceptions that may reduce protection.
- Regularly review and clean expired exceptions.
- Always validate hash values before adding file exceptions.

Data Loss Prevention

Data Loss Prevention (DLP) detects and prevents unauthorized sharing or retrieval of confidential information, such as social security numbers, credit card numbers, and bank account numbers.

DLP enforces policies by associating data types with specific rules. It supports both file upload and file download, inspecting web-based transfers to prevent exposure of sensitive data.

Use Case

You are a financial organization aiming to prevent the upload or download of files containing confidential and sensitive data, such as bank account numbers, tax and revenue details, by unauthorized users.

Actions in DLP Rules

You can configure these actions within DLP rules:

- **Detect** - Performs the DLP scan and detects the confidential information, but does not block the data.
- **Prevent** - Performs the DLP scan and prevents data transfer if it finds a match to a data type.

Known Limitations

- DLP applies only to files being uploaded or downloaded over a browser.
- Traffic to or from native applications (EXE-based clients) is not supported.
- The system must inspect the traffic (and not bypass it in the HTTPS Inspection policy) for DLP to take place.

Operations

File Upload

- DLP inspection is supported for files up to 16 MB.
- Supports Agent version 11.7 and higher.
- File type supported - see sk181662.

File Download

Note - The File Download feature is available only in Early Availability (EA) and appears in the UI only for EA tenants.

- DLP inspection is supported for files up to 10 MB.
- Supports Agent version 12.3 and higher.
- When Transfer Type is selected as File Download, at least one Service must be selected.
- Encrypted files or files larger than the maximum size limit are not inspected, and a Skip log entry is recorded.
- Websites:

  DLP supports download inspection for these web services:

  - Box
  - ChatGPT
  - Dropbox
  - GitHub
  - GitLab
  - Gmail
  - Google Drive
  - Google Gemini
  - Jira
  - Microsoft Copilot
  - Microsoft Teams
  - Monday.com
  - OneDrive
  - Outlook
  - Salesforce
  - Slack
- File Types:

Category	Extensions
Microsoft Office	• **Word**: .doc, .dot, .docm, .docx, .dotx, .dotm • **Excel**: .xls, .xlt, .xlm, .xlsx, .xlsm, .xlsb, .xltx, .xltm, .xlam, .xlr, .csv, .xlc • **PowerPoint**: .ppt, .pps, .pot, .pptx, .pptm, .ppsx, .ppsm, .potx, .potm • **OneNote**: .one, .onepkg, .onetoc2 • **Outlook**: .msg, .oft, .pst, .ost • **Publisher**: .pub, .pubx • **Access**: .mdb, .accdb, .accft • **Project**: .mpp • **Other**: .rtf, .snp, .xsn, .thmx
OpenOffice / LibreOffice	.odt, .ods, .odp, .odg, .sxw, .sxc, .sxi, .sxd, .sdw, .sdc, .sdp
Adobe	.pdf, .ai, .indd, .inx, .psd, .psb, .ps
Apple iWork	.pages, .pht, .key, .kth, .numbers, .nth, .num
Archives	.arc, .rar, .zip, .7z, .lzh, .sit, .gz, .tar, .bz2, .xz, .arj, .cab, .z
Text & CSV	.txt, .log, .csv
Email	.eml, .nws, .mbox
WordPerfect	.wpd, .wp, .wp5, .wp6, .wpf, .wps
Lotus	.wk1, .wk3, .wks, .lwp, .mwp, .prz, .nsf, .lif, .pic
Hangul Word Processor	.hwp, .hna, .hbo
Databases	.dbf, .db, .wdb, .dat, .sdb
CAD	.dwg, .dxf, .dxb, .dwf, .dgn, .dx
Programming & Executables	.class, .dll, .exe, .com
Other Document Processors	.sam, .wri, .wpt, .jtd, .jw, .mw2
Spreadsheets	.qpw, .et
QuarkXPress	.qxp

Category	Extensions
FrameMaker	.fm
Visio	.vsd, .vdx
Digital Signatures	.p7m, .p7s, .sef
Other Files	.env, .chm, .hlp, .fd, .efx, .vcf, .ami, .rnd, .hqx, .c4, .rep, .cpi, .xys, .dwd, .es, .fc, .sh3, .dxl, .dca, .icf, .m11, .m4, .m5, .scf, .mpeg7, .obd, .wpm, .met, .p1, .awb, .awp, .pfs, .ppp, .tka, .psw, .q\&a, .wb3, .wb2, .qf, .rdf, .ras, .sda, .sig, .sxl, .svm, .sc5, .wrk, .uue, .vw, .vpd, .clp, .cur, .dib, .wmc, .en, .ws2, .ws, .wr1, .wbk, .yenc, .xxe

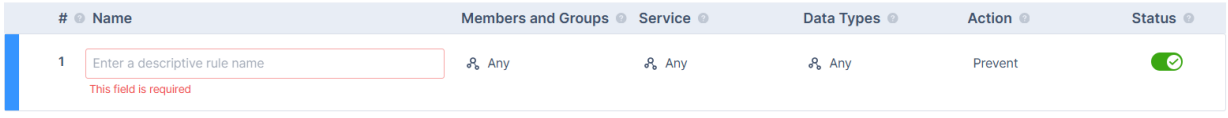
- To maintain optimal internet performance, the system does not scan these file types:

Category	Extension
Media	.mp3, .mp4, .mpg, .mpeg, .avi, .mov, .asf, .wmv, .wma, .rm, .wav, .mid, .swf, .flv
Graphics	.gif, .jpg, .jpeg, .png, .bmp, .tif, .tiff, .pct, .pict, .pnt, .pcx, .img, .tga, .pbm, .pgm, .ppm, .xbm, .xpm, .xwd, .svg, .emf, .wmf, .cgm, .cmx, .eps, .hgl, .hpg, .cal, .g3, .dcm, .fpx, .pcd, .orf
HTML/Web	.html, .htm, .xhtml, .css, .xml, .xmp, .js, .wml, .wmlb, .hdml, .chtml, .phtml
Fonts	.ttf, .ttc

Creating a DLP Rule

1. Sign in to the Check Point Infinity Portal and access the SASE Administrator Portal.
2. Click **Data Loss Prevention**.
3. Click the **Policy** tab.
4. Click **Add New Rule**.

   A new row appears in the table.



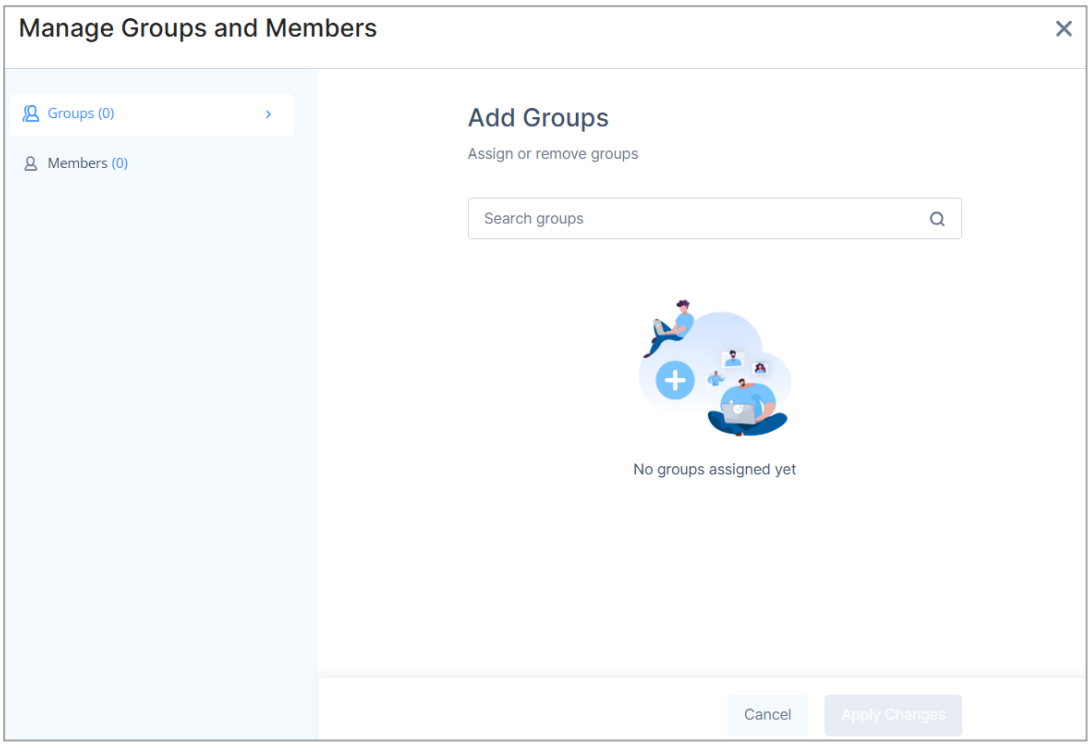
5. Specify these:

a. In the **Name** column, enter a rule name.

b. In the **Members and Groups** column, select a user or a group to which you want to apply the rule. The default value is **Any**.

   i. Hover over the **Members and Groups** column and click **Add Source** > **Groups or Members**.

   The **Manage Groups and Members** window appears.



   ii. To add a group, select **Groups** and in the search groups field, search and select a group(s).

   iii. To add a member, select **Members** and in the search members field, search and select a member(s).

   iv. Click **Apply Changes**.

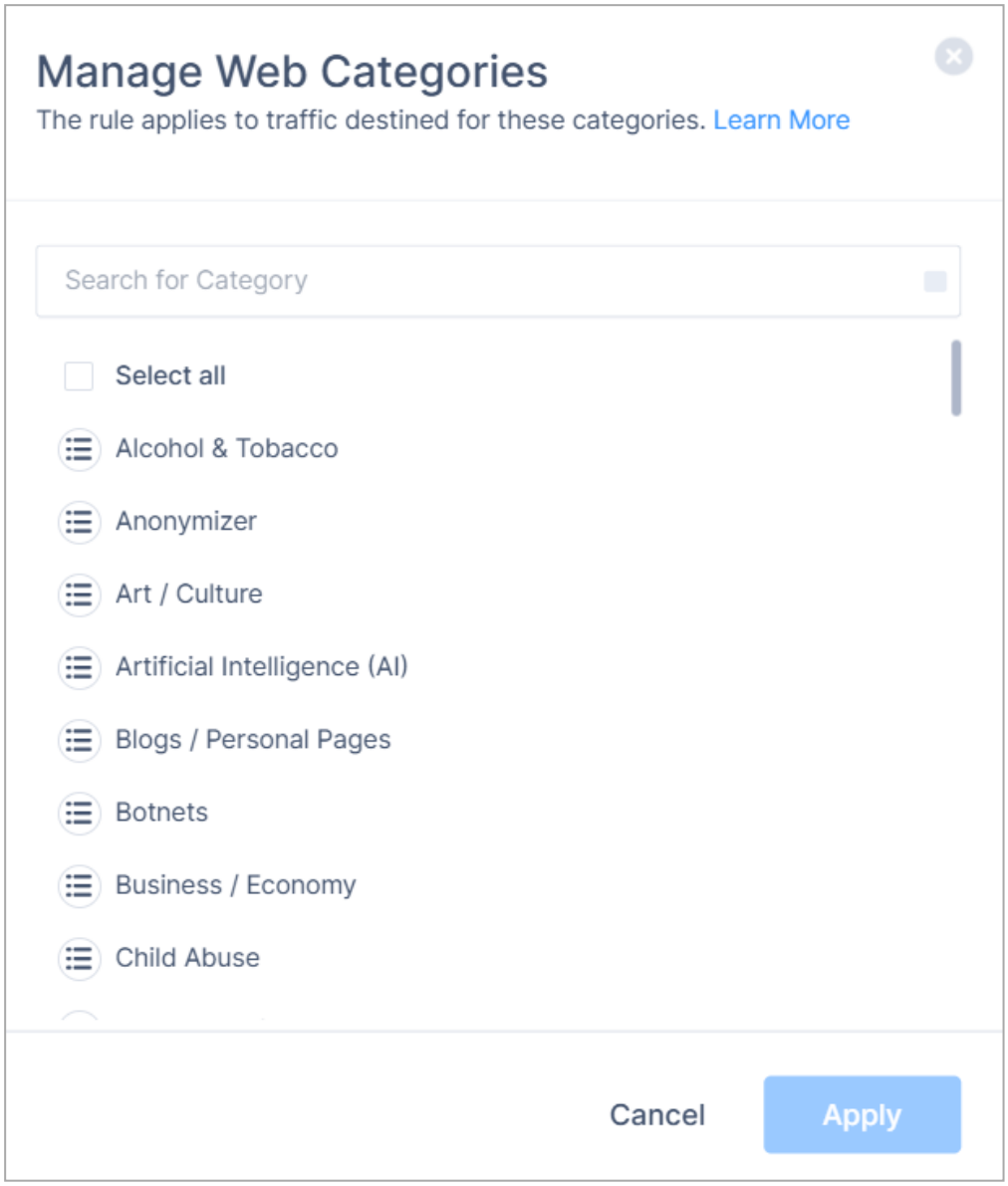
c. In the **Service** column, add a service to which you want to apply the rule. The default value is **Any**.

d. Hover over the Service column, click **Add Service**, and select one of these:

- **Web Categories**:

  i. Select **Web Categories**.

  The **Manage Web Categories** window appears.

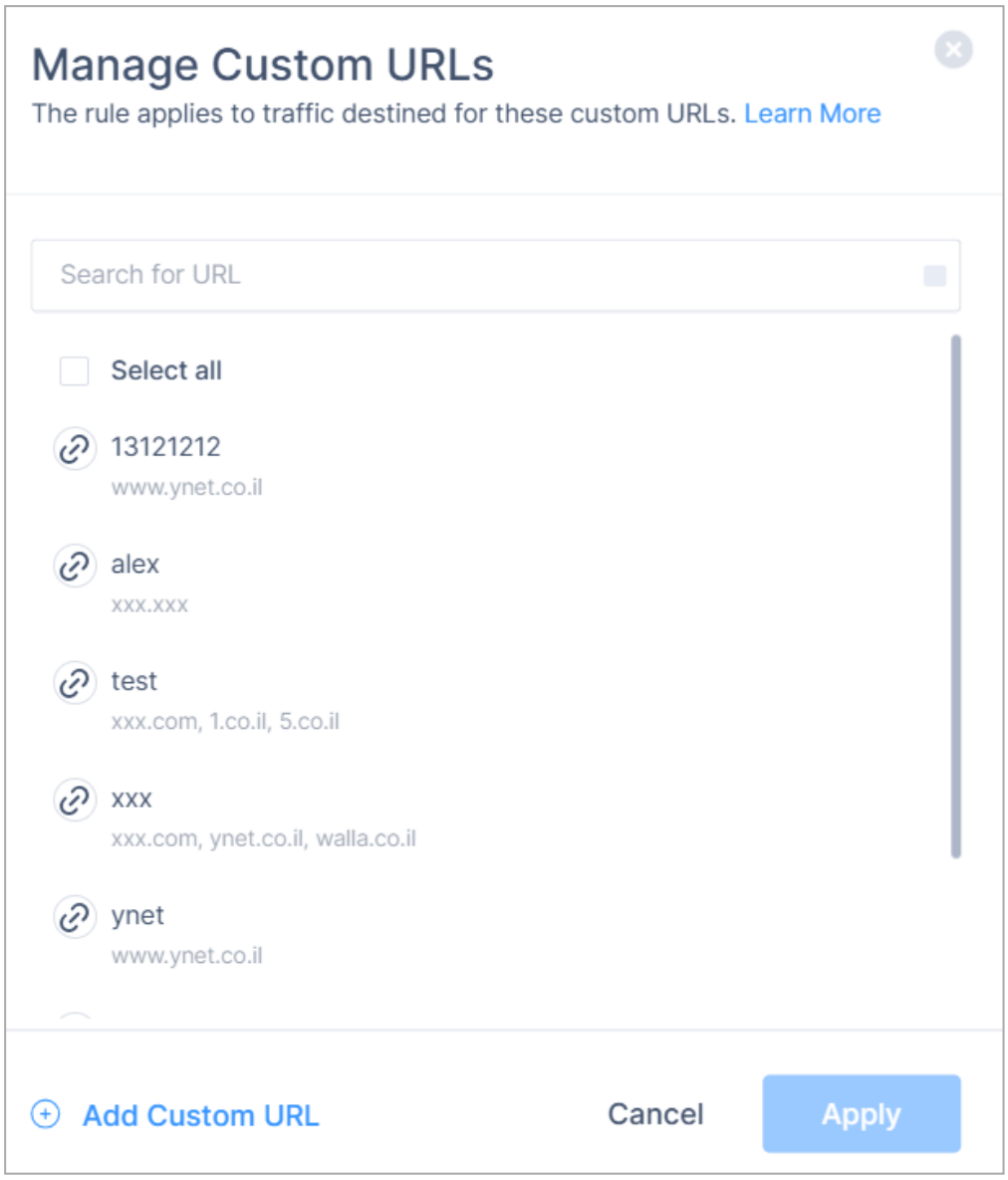


  ii. Search and select one or more categories and click **Apply**.

- **Custom URLs**:

  i. Select **Custom URLs**.

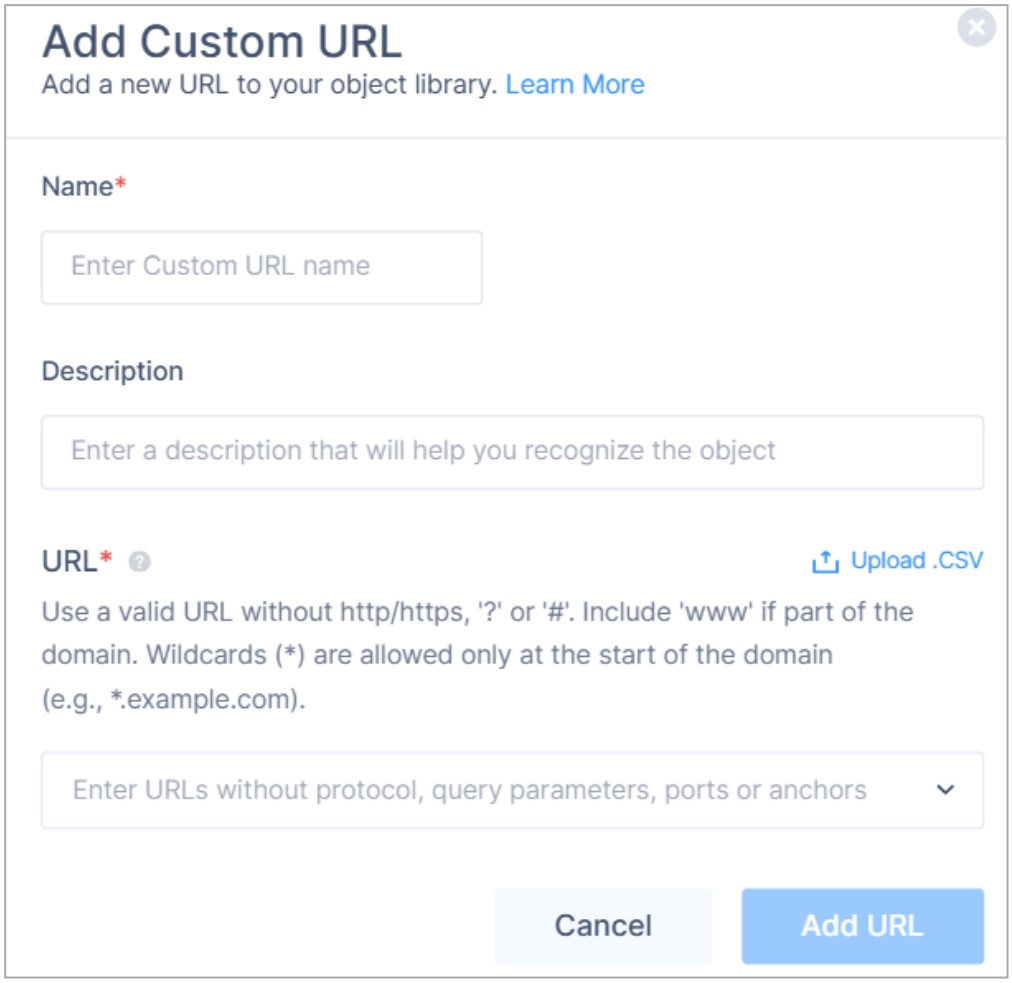
  The **Manage Custom URLs** window appears.



  ii. Search and select one or more URLs and click **Apply**.

iii. To add a new custom URL, click **Add Custom URL**.

The **Add Custom URL** window appears.



iv. Enter these:

i. **Name** - Name of the custom URL.

ii. (Optional) **Description**

iii. In the **URL field**, enter the list of URLs or upload a .CSV file with the list of URLs.

Note -

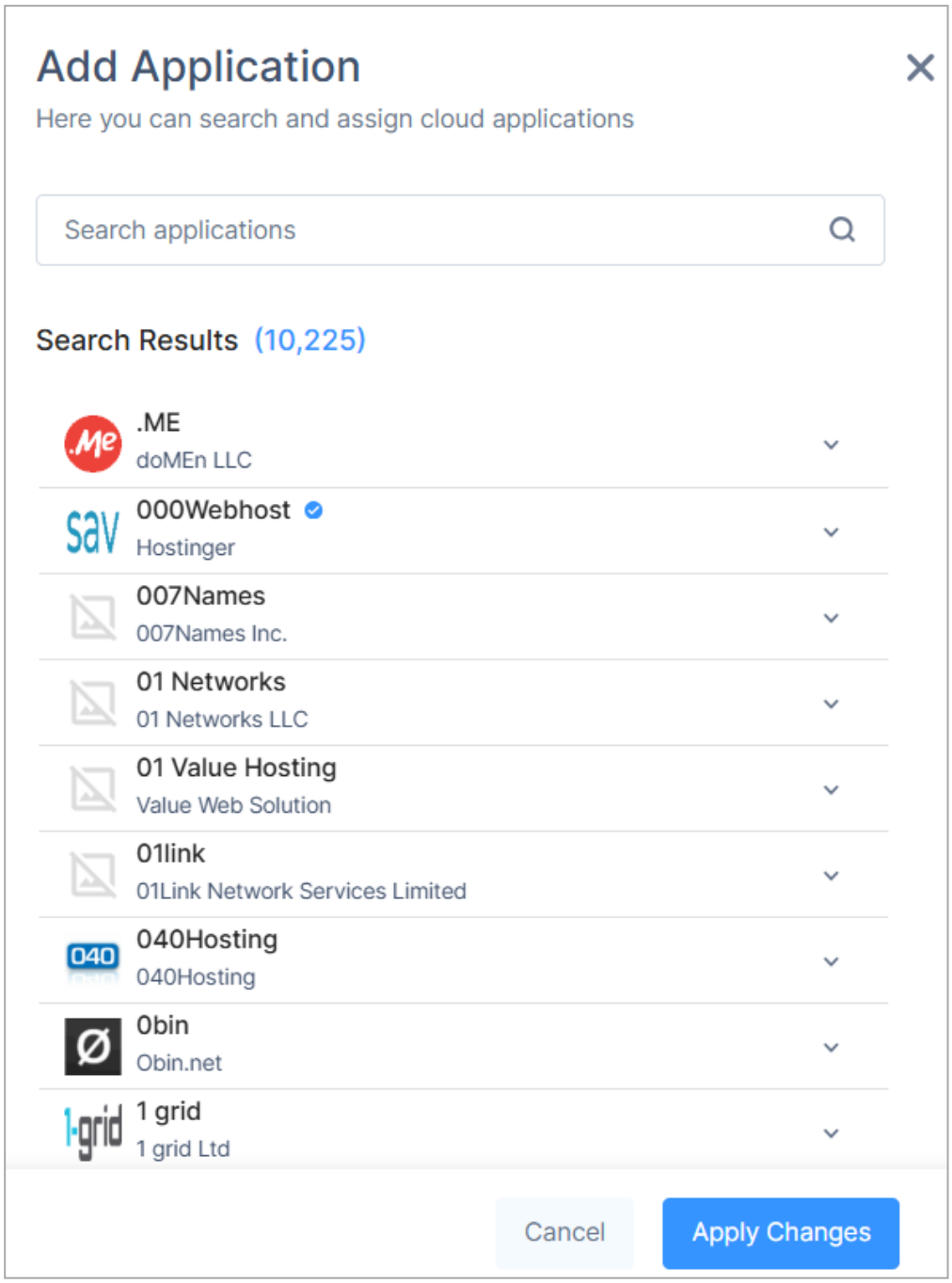
- Do not add any protocols (http:// , https://) , query parameters (?) or anchors (#). If the URL includes a www prefix, include it as part of the domain. Wildcard (*) is supported and can only be used at the beginning of the domain, for example, *.example.com.
- When uploading a CSV file with custom URLs, make sure the file does not include a header or subject line. Each row should contain only a single URL.

iv. Click **Add URL**.

The system creates the URL and displays it in the Custom URLs page.

- **Applications**:
  i. Select **Applications**.

  The **Add Applications** window appears.



  ii. Search the application for which you want to apply the rule.

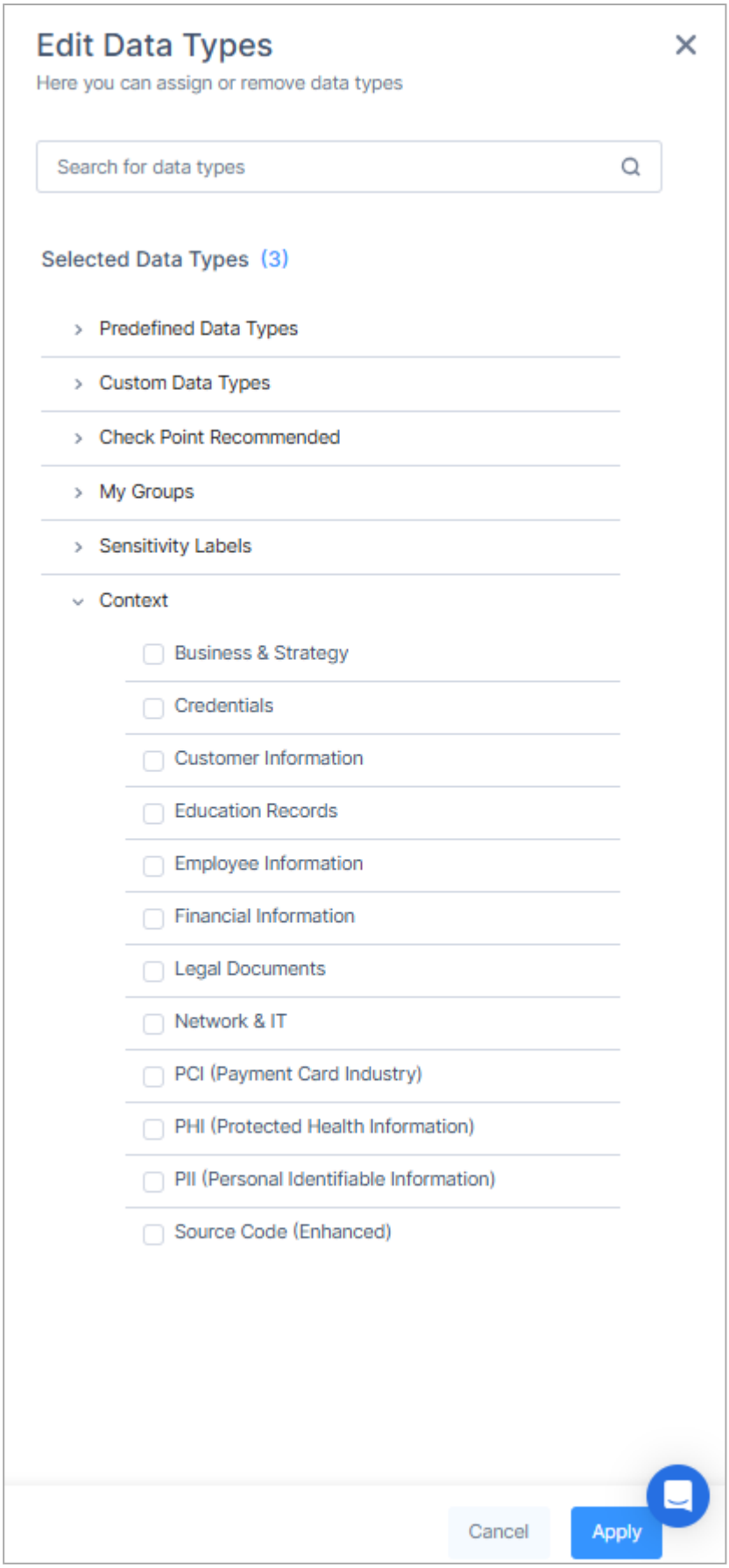
  iii. Hover over the application and click +.

  iv. Click **Apply Changes**.

e. In the **Data Types** column, add a data type to which you want to apply the rule. The default value is **Any**.

i. Hover over the **Data Types** column, click **Add Data Type**, and select **Add Data Types**.

   The **Edit Data Types** window appears.


Edit Data Types
Here you can assign or remove data types
Search for data types
Selected Data Types (3)
Predefined Data Types
Custom Data Types
Check Point Recommended
My Groups
Sensitivity Labels
Context
Business & Strategy
Credentials
Customer Information
Education Records
Employee Information
Financial Information
Legal Documents
Network & IT
PCI (Payment Card Industry)
PHI (Protected Health Information)
PII (Personal Identifiable Information)
Source Code (Enhanced)
Cancel
Apply

ii. Search and select the data type or a group.

You can specify up to 100 data types.

iii. Click **Apply**.

f. In the **Action** column, select either of these:

i. **Prevent** - Block actions if sensitive data is detected and log the event.

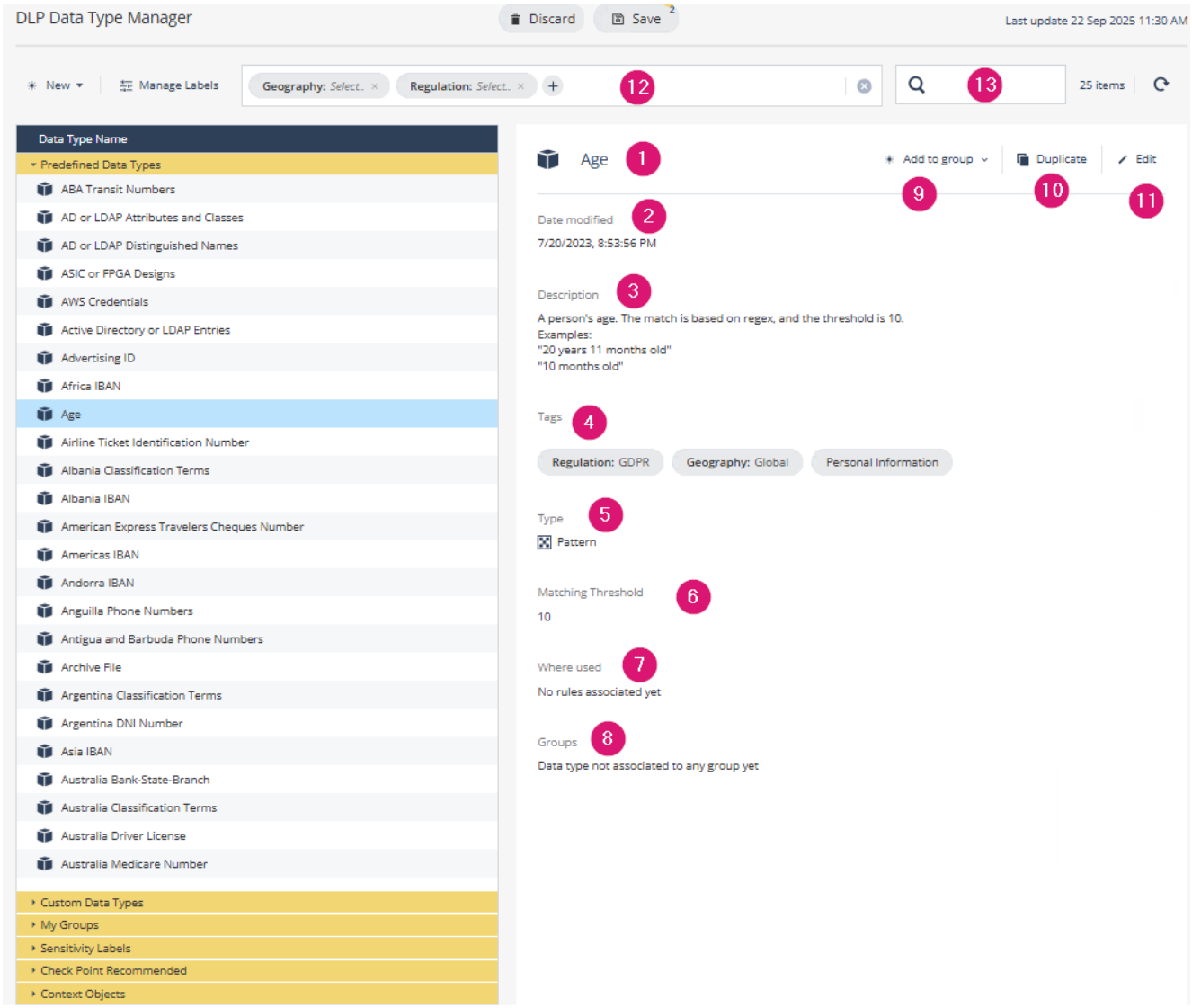
ii. **Detect** - Log the event.

g. Turn on the **Status** toggle button.

Notes:

- To create a rule above or below a particular rule, hover over the rule and scroll to the end of the row, click and select **Create Above** or **Create Below**.
- To duplicate a rule above or below a particular rule, hover over the rule and scroll to the end of the row, click and select **Duplicate Above** or **Duplicate Below**.
- To delete a rule, hover over the rule and scroll to the end of the row, click , and select **Delete**.

Data Type Manager



Legends	Description
1	Name of the data type.
2	Date and time (in MM/DD/YY, HH:MM:SS XM format) when the data type was last modified.
3	Brief description of the data type.
4	Custom tags (category) for the data type. Helps in searching for data types.

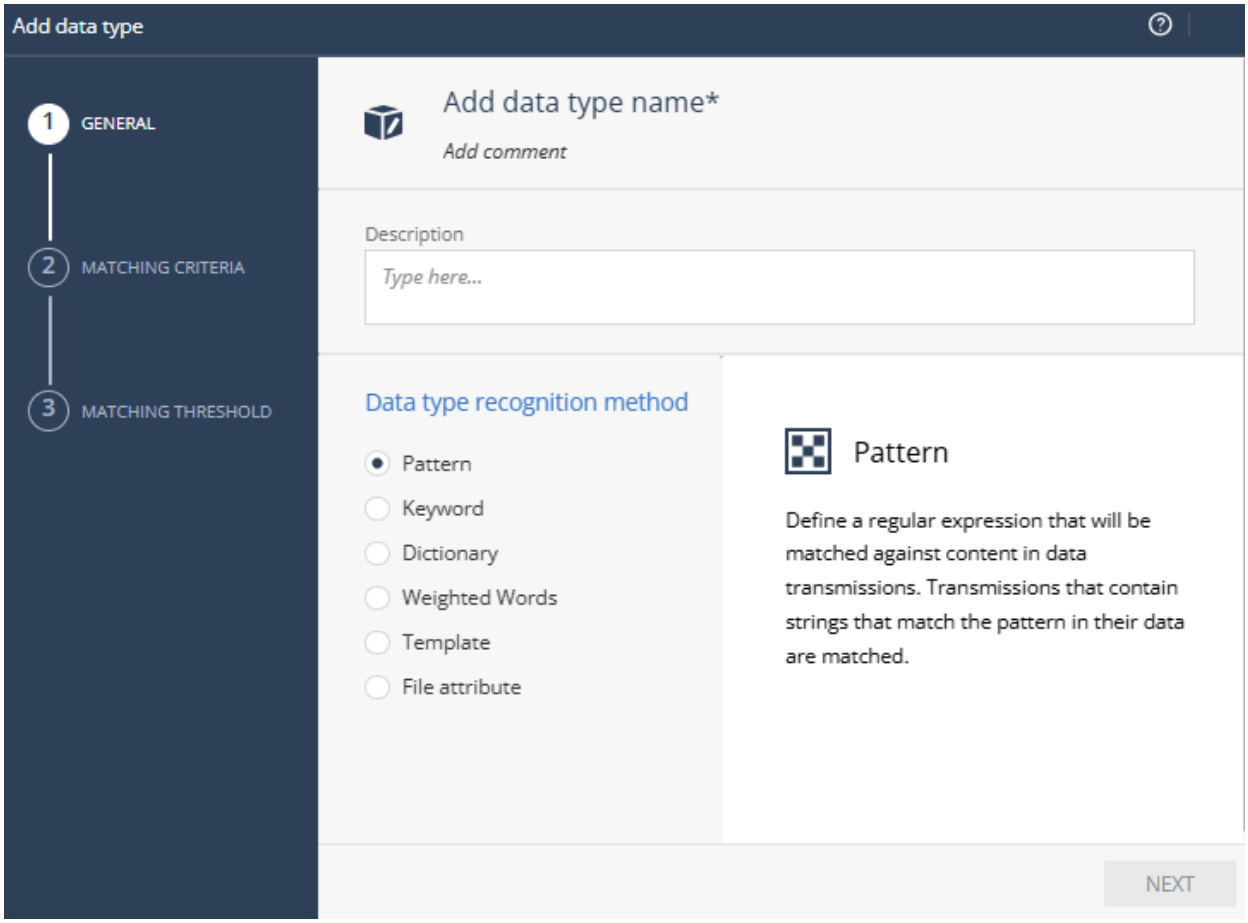
Legends	Description
5	Matching criteria: ■ Pattern ■ Keyword ■ Dictionary ■ Weighted Words ■ Template ■ File attribute ■ Compound (Combination of data types with a logical separator) ■ Group (Data type group)
6	The minimum number of times the matching criteria must be present in the file to trigger the DLP action specified in the policy capability rule. For example, if the matching criteria is **Keyword**, the value is **credit** and the **Matching Threshold** is **5**, then the system takes the action specified by the policy capability rule if the file contains the term **credit** five times or more.
7	Policy capability rules where the data type is used.
8	Groups associated with the data type.
9	Add the data type to a group.
10	Duplicate the data type.
11	Edit the data type.
12	Filter data type by category.
13	Search for a data type.

Creating a Custom Data Type

To create a custom data type:

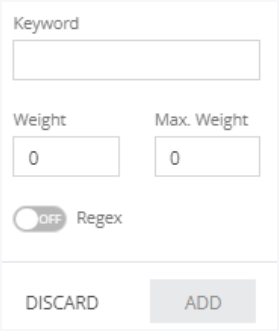
1. Sign in to the Check Point Infinity Portal and access the SASE Administrator Portal.
2. Click **Data Loss Prevention**.
3. Click the **Data Type Manager** tab.
4. Click **New** and select **Data type**.

   The **Add data type** wizard appears.



5. Enter the data type name, object comment (optional) and description.
6. From the Data type recognition method list, select a recognition method:

Recognition method	Description	Action
Pattern	Applies the action specified in the policy capability rule if the file contents match the threshold for the pattern. For example: ■ Matches a sequence - **5523-2342** ■ Employee numbers that have an EMP prefix, followed by 5 digits - **EMP-\d{5}** ■ Where, **EMP-** is the fixed prefix for all employee IDs, and \d{5} is exactly 5 digits (\d represents a digit, and {5}indicates that it must be exactly 5 digits long) • Match example: **EMP-12345**	In the **Patterns** section, enter the pattern and click +.
Keyword	Applies the action specified in the policy capability rule if the file contents match the threshold for the keyword. For example, *Confidential*, *Secret*.	In the **Keywords** section, enter the keywords and click +.
Dictionary	Applies the action specified in the policy capability rule if the file contents match the threshold for the terms in the dictionary. For example, *Spain, China, United Kingdom*. Each keyword must be specified in a single line in the UTF-8 format. **Note** - The recommended file formats are *.doc*, *.docx* and *.txt*.	Upload the dictionary file.

Recognition method	Description	Action
Weighted Words	Applies the action specified in the policy capability rule if the file contains keywords and the cumulative weight matches or exceeds the threshold. Use this method to specify multiple keywords. For example, consider two keywords: ▪ **credit** with **Weight**=1 and **Max. Weight**=3 ▪ **transaction** with **Weight**=2 and **Max. Weight**=30 and **Matching Threshold**=15. If the file contains six occurrences of **credit**, each contributing a **Weight** of 1. That is, 1x6=6. As the **Max. Weight**=3, the final weight is 3. If the file contains eight occurrences of **transaction**, each contributing a **Weight** of 2. That is, 2x8=16. As the **Max. Weight**=30, the final weight is 16. As the sum of final weights of **credit** and **transaction**, that is, 16+3=19 is greater than the **Matching Threshold**, the system applies the specified action in the policy capability rule. If the sum of the final weights of the keywords is less than the **Matching Threshold**, then the file is uploaded or downloaded.	a. Click **New**.  b. Enter these: ▪ **Keyword** ▪ **Weight** - Weight for each occurrence of the keyword. ▪ **Max. Weight** - Maximum allowed weight for the keyword. c. If the keyword is a regular expression, turn on the **Regex** toggle button. d. Click **Add**. e. Repeat steps *a* through *d* to add the next keyword.

Recognition method	Description	Action
Template	Applies the action specified in the policy capability rule if the file contents match the threshold for the terms in the template. For example, a template with a set header, footer and logo. If the template contains images, the DLP is triggered only if the file contains the images in the same format as in the specified template.	Upload the template file.
File attribute	Applies the action specified in the policy capability rule if the file: ■ Matches the specified file name. ■ Size is equal to or greater than the specified file size. ■ Type matches the specified file type.	Select any of these and enter a value: ■ **File name**: For example, *Account Numbers, Employee Details*. ■ **File size**: File size in Byte, KB, MB or GB. ■ **File type**: • Click + and select the file type(s) from the list.

7. Click **Next**.

   Note - This step does not apply to **Template** and **File attribute** recognition methods.

8. Select the matching threshold.

   The minimum number of times the matching criteria must be present in the file to trigger the DLP. For example, if the matching criteria is Keyword, the value is credit and the Matching Threshold is 5, then the system takes the action specified by the policy capability rule if the file contain the term credit five times or more.

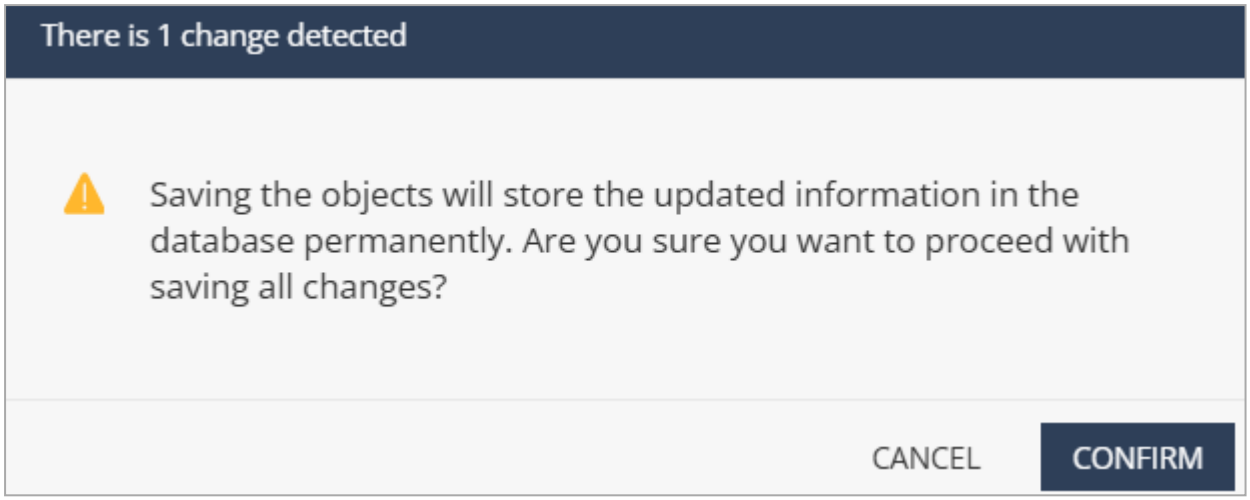
   Note - This step does not apply to **Template** and **File attribute** recognition methods.

9. Click **Finish**.

   The new custom data type is listed under **Custom Data Types**.

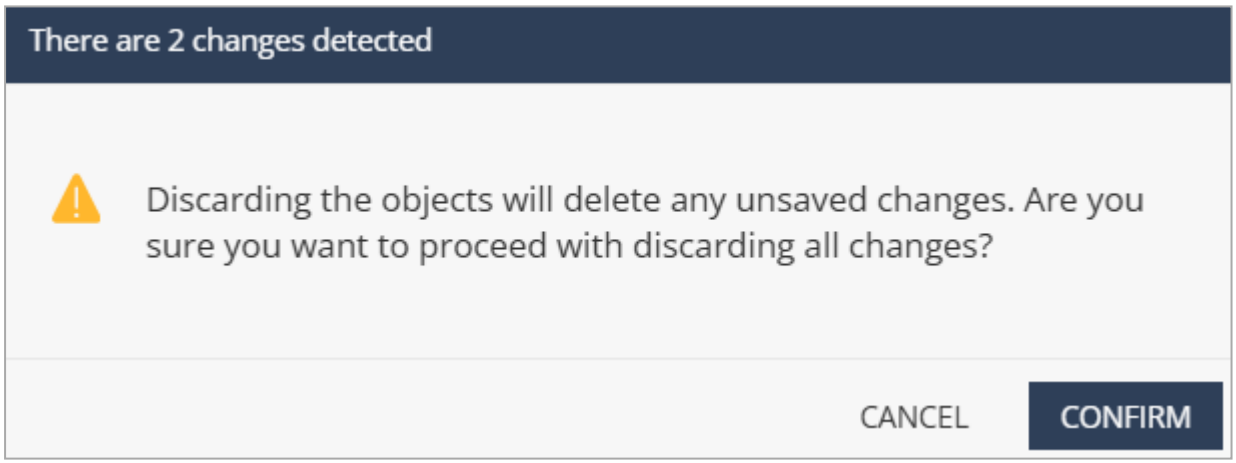
10. To permanently save all the changes to the database, click **Save** at the top.

    The **change detected** window appears.



11. Click **Confirm**.
12. To discard all the changes, click **Discard** at the top.

    The **change detected** window appears.



13. Click **Confirm**.

Creating a Custom Data Type Group

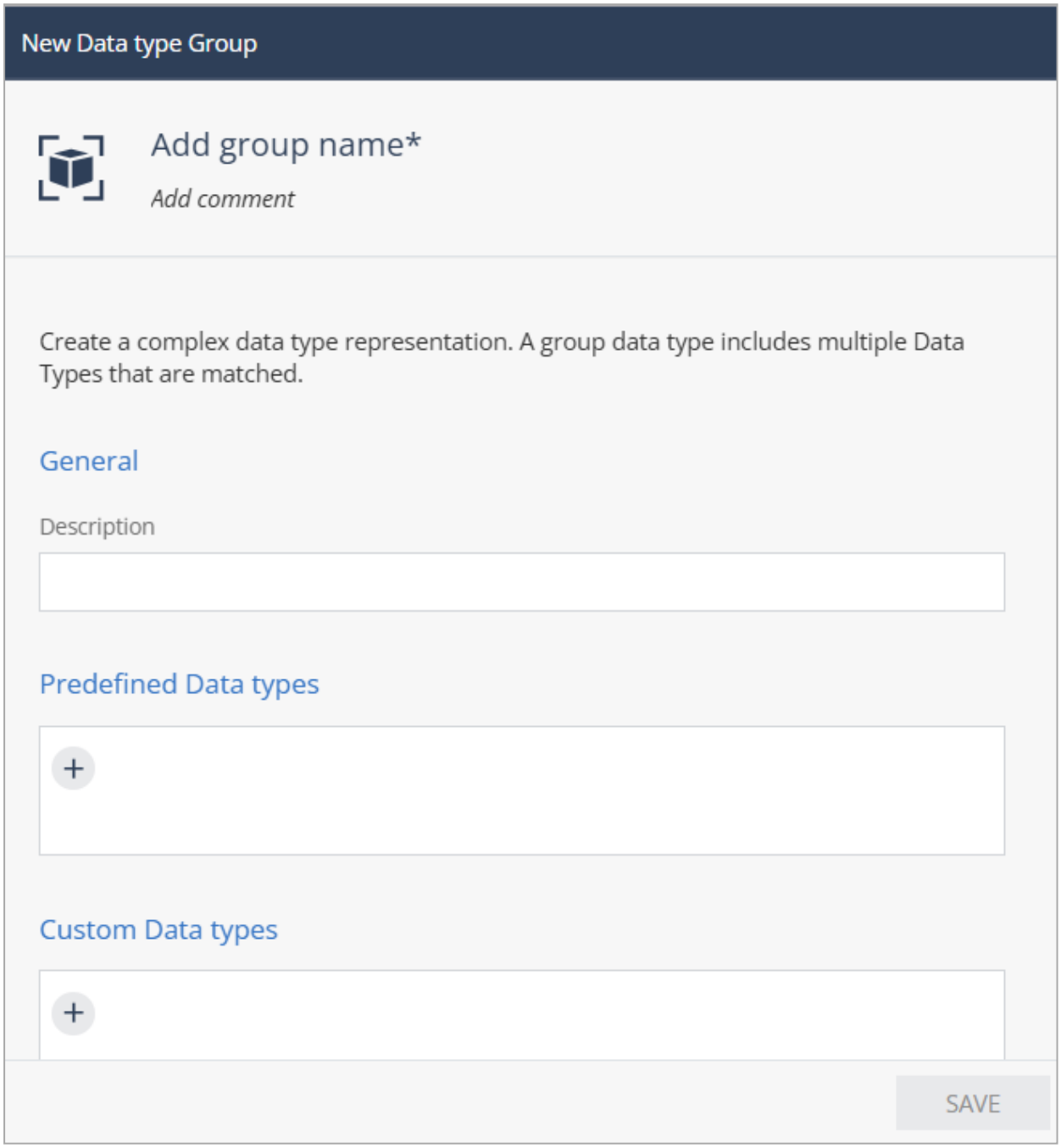
To create a custom data type group:

Note - Nested groups are not supported.

1. Sign in to the Check Point Infinity Portal and access the SASE Administrator Portal.
2. Click **Data Loss Prevention**.
3. Click the **Data Type Manager** tab.

4. Click **New** and select **Group**.

   The **New Data type Group** window appears.

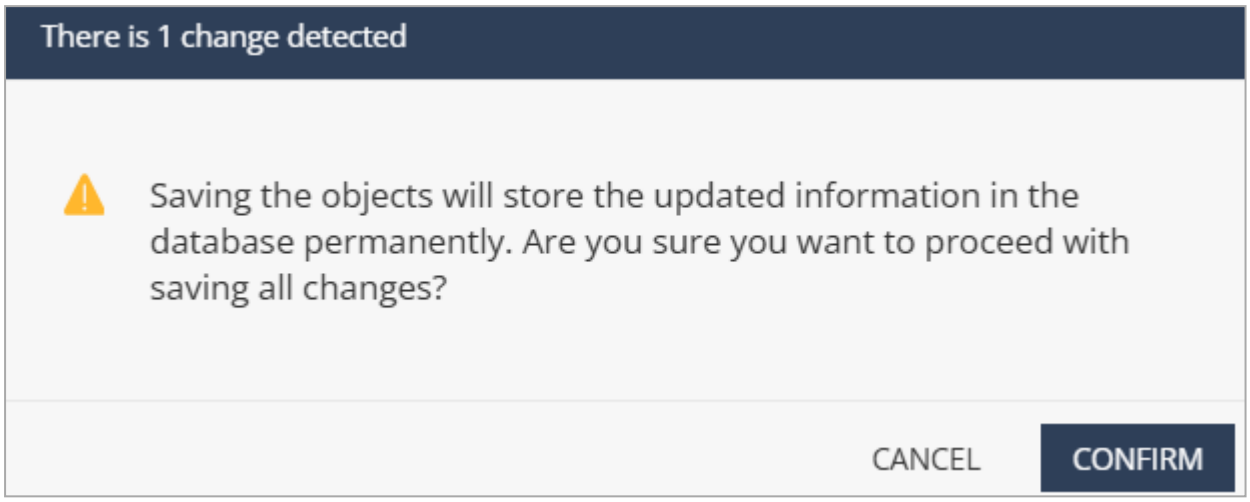


5. Enter a group name, object comment (optional) and description.
6. To add predefined data types to the group, click in the **Predefined Data types** field and select the data type.
7. To add custom data types to the group, click in the **Custom Data types** field and select the data type.
8. Click **Save**.

The new data type group is listed under **My Groups**.

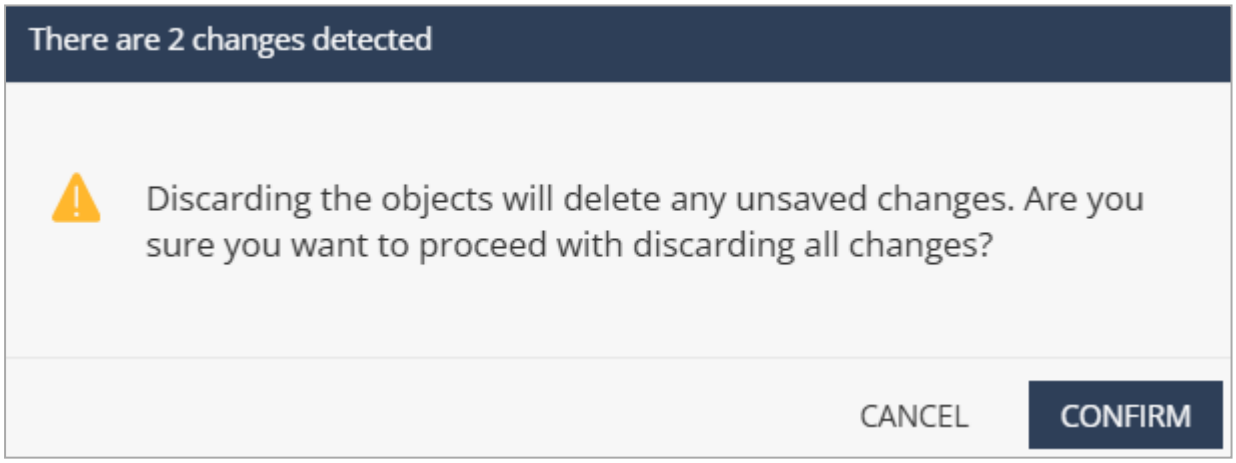
9. To permanently save all the changes to the database, click **Save** at the top.

   The **change detected** window appears.



10. Click **Confirm**.
11. To discard all the changes, click **Discard** at the top.

    The **change detected** window appears.



12. Click **Confirm**.

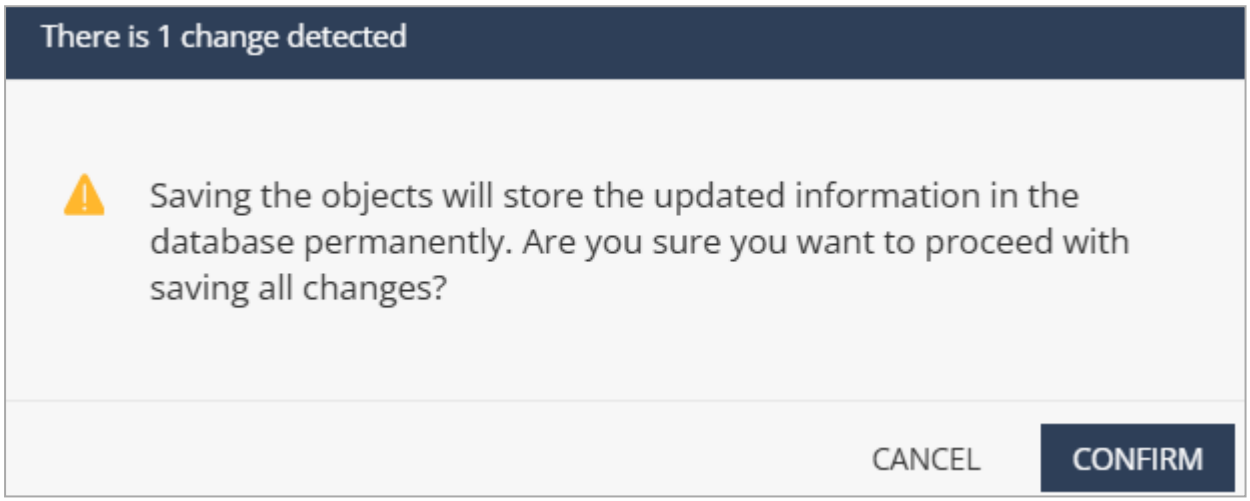
Adding an existing Data Type to a Group

To add an existing data type to a group:

1. Sign in to the Check Point Infinity Portal and access the SASE Administrator Portal.
2. Click **Data Loss Prevention**.
3. Click the **Data Type Manager** tab.

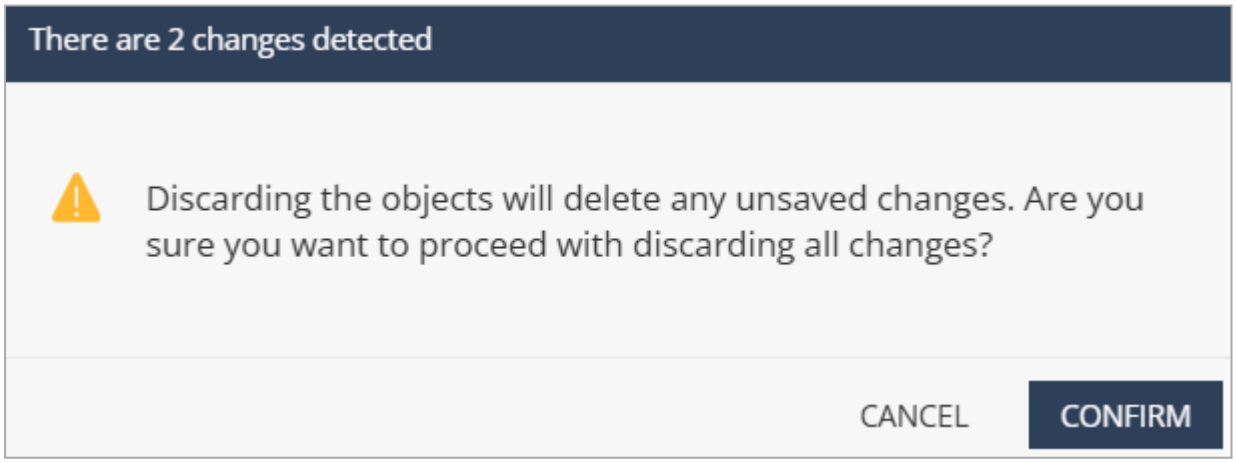
4. In the **Data Type Name** list, expand **Custom Data Types** or **Predefined Data Types** and select the data type.
5. Click **Add to group**.
6. Select the group(s) from the list.
7. Click **Add**.
8. To permanently save all the changes to the database, click **Save** at the top.

   The **change detected** window appears.



9. Click **Confirm**.
10. To discard all the changes, click **Discard** at the top.

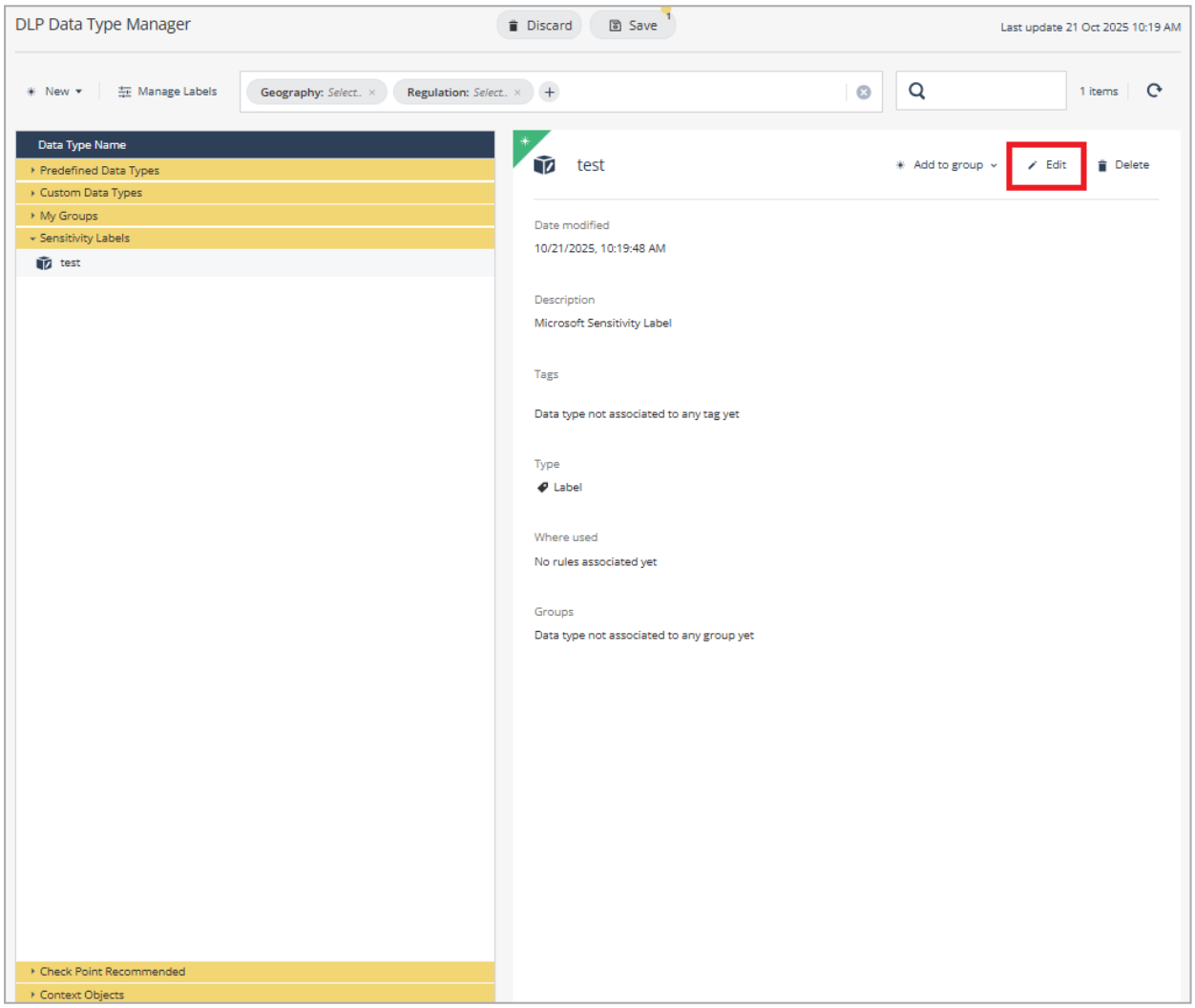
    The **change detected** window appears.



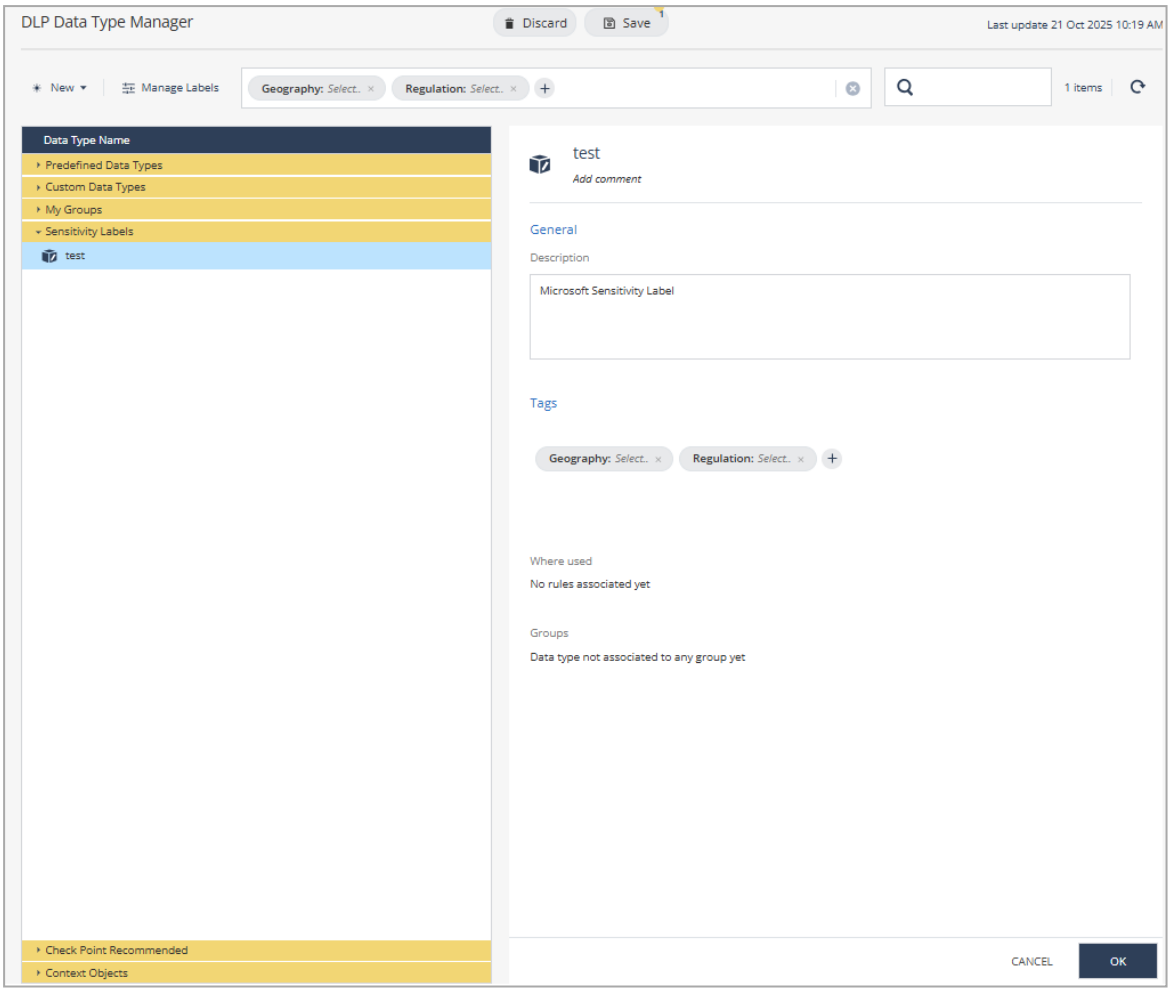
11. Click **Confirm**.

Managing a Data Type or Group

1. Sign in to the Check Point Infinity Portal and access the SASE Administrator Portal.
2. Click **Data Loss Prevention**.
3. Click the **Data Type Manager** tab.
4. In the **Data Type Name** list, expand the **DLP group** and select the data type or the group.
5. To edit a data type or group, click **Edit**.



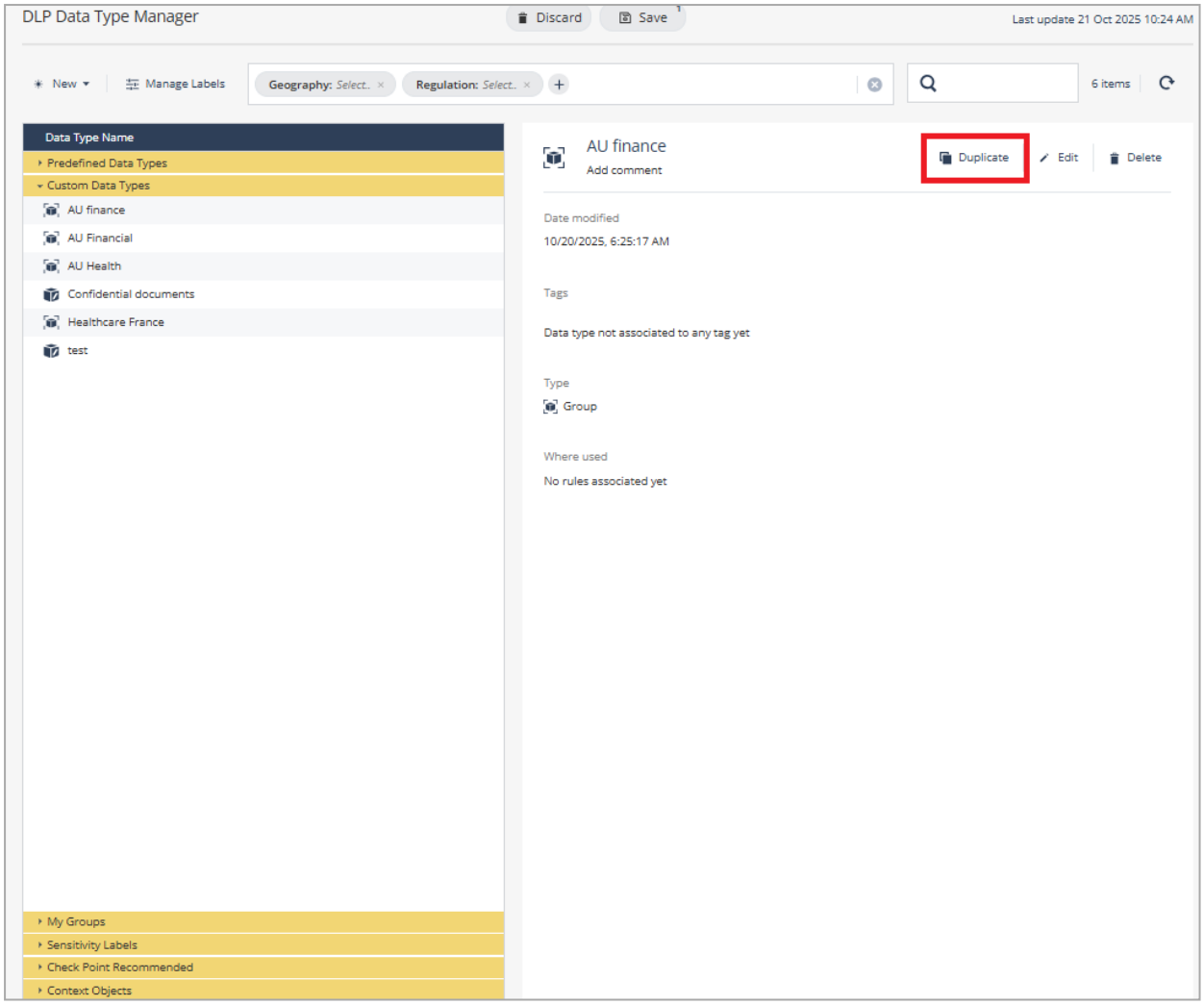
a. Make the required changes.



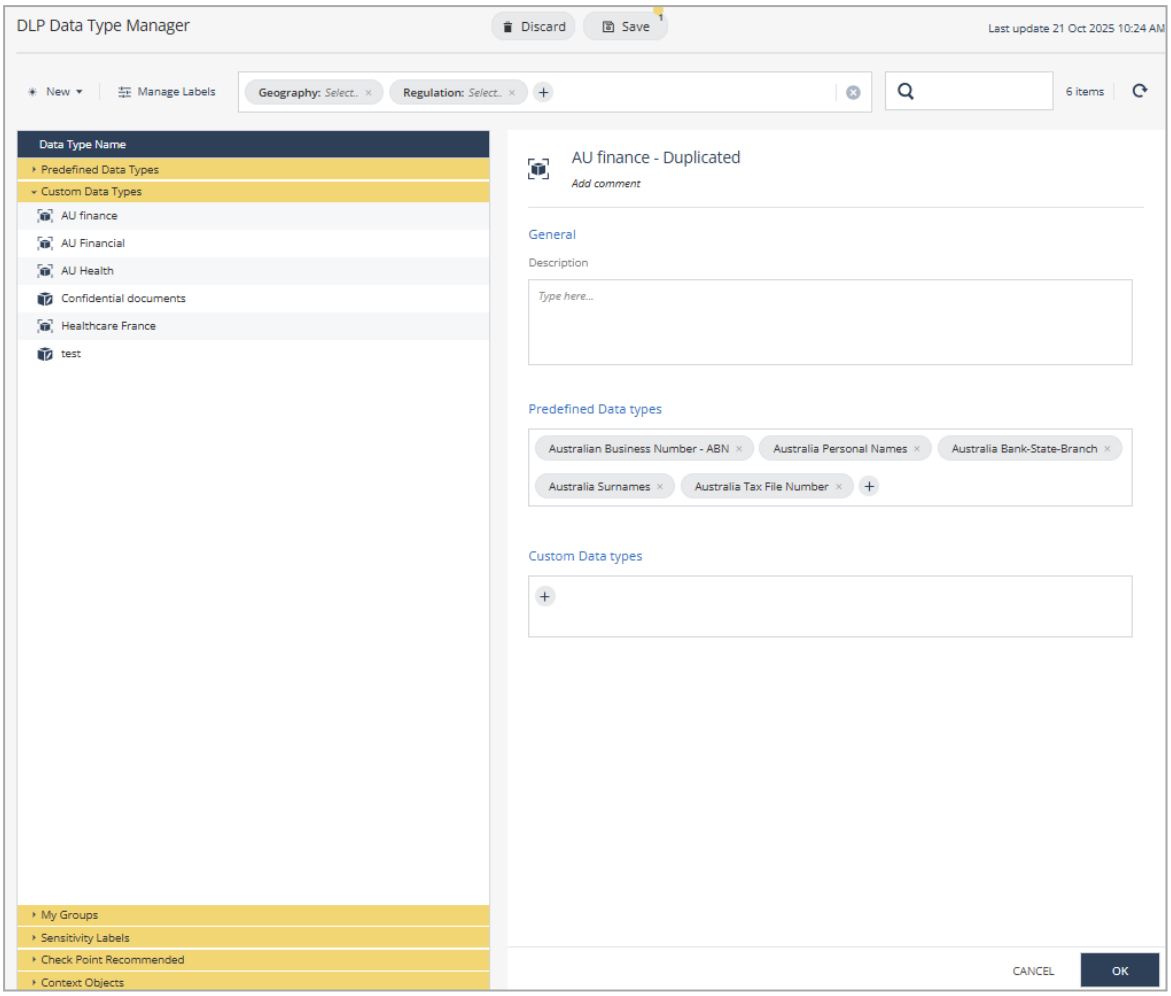
Note - If you edit a data type, the changes are reflected in all the groups that contain this data type.

b. Click **OK**.

6. To duplicate a data type or group, click **Duplicate**.


DLP Data Type Manager
Discard
Save
Last update 21 Oct 2025 10:24 AM
New
Manage Labels
Geography: Select..
Regulation: Select..
6 items
Data Type Name
Predefined Data Types
Custom Data Types
AU finance
AU Financial
AU Health
Confidential documents
Healthcare France
test
My Groups
Sensitivity Labels
Check Point Recommended
Context Objects
AU finance
Add comment
Duplicate
Edit
Delete
Date modified
10/20/2025, 6:25:17 AM
Tags
Data type not associated to any tag yet
Type
Group
Where used
No rules associated yet

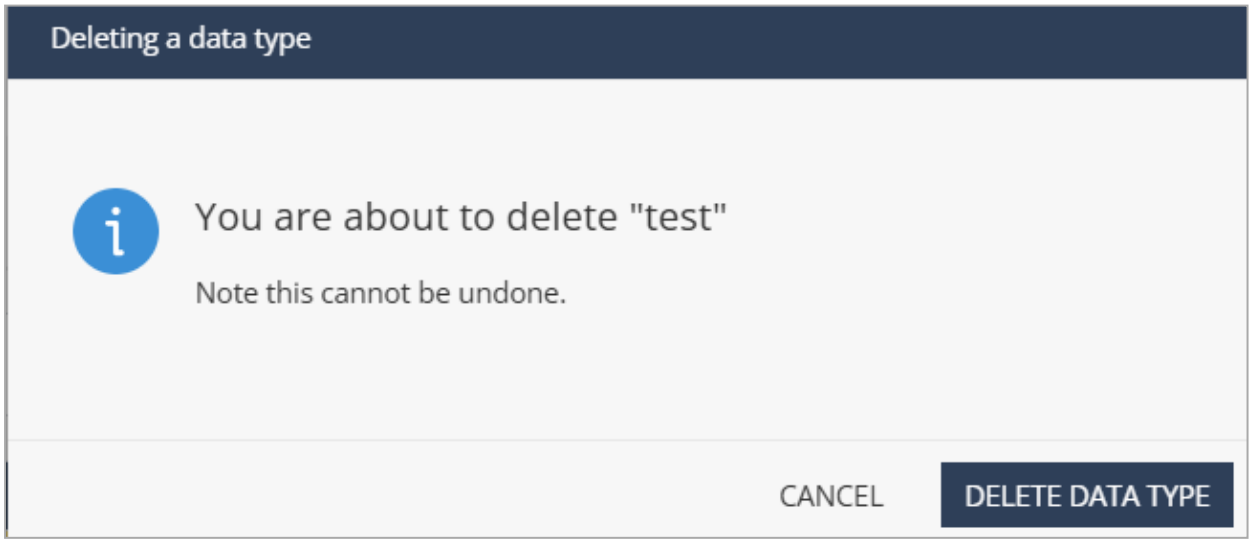
a. Make the required changes.



b. Click **OK**.

7. To delete a data type or group, click **Delete**.

   The **Deleting a data type** window appears.

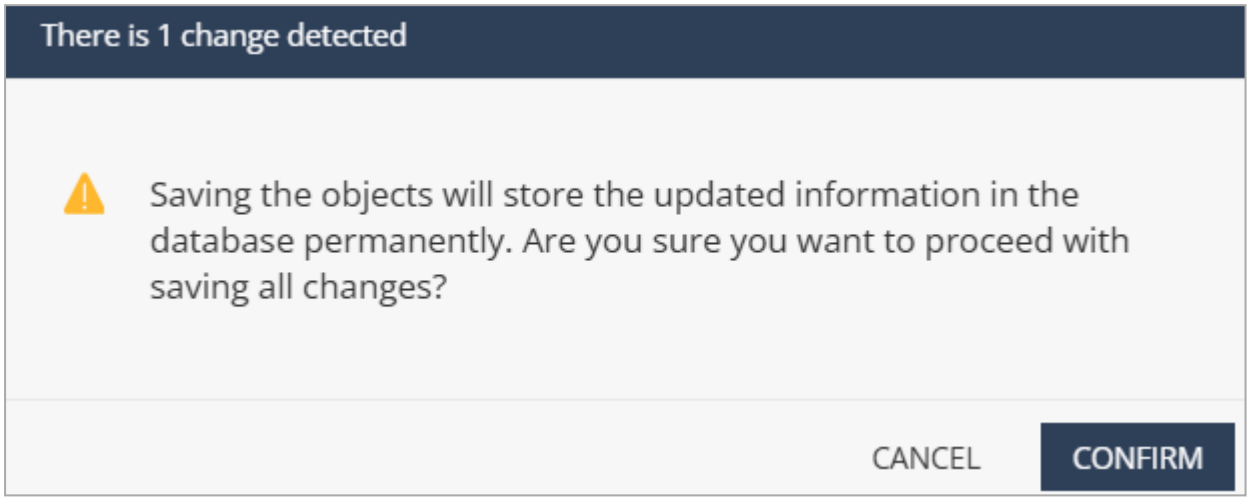


Note - Before you delete a data type, make sure to remove the data type from the group(s) and policy capability rules.

a. Click **Delete Data Type**.

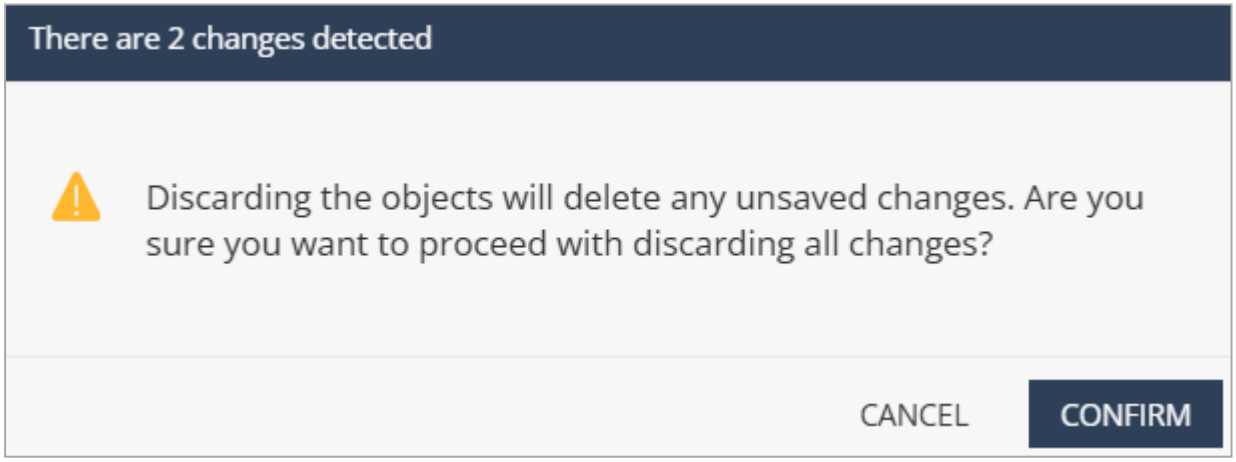
8. To permanently save all the changes to the database, click **Save** at the top.

   The **change detected** window appears.



9. Click **Confirm**.
10. To discard all the changes, click **Discard** at the top.

    The **change detected** window appears.



11. Click **Confirm**.

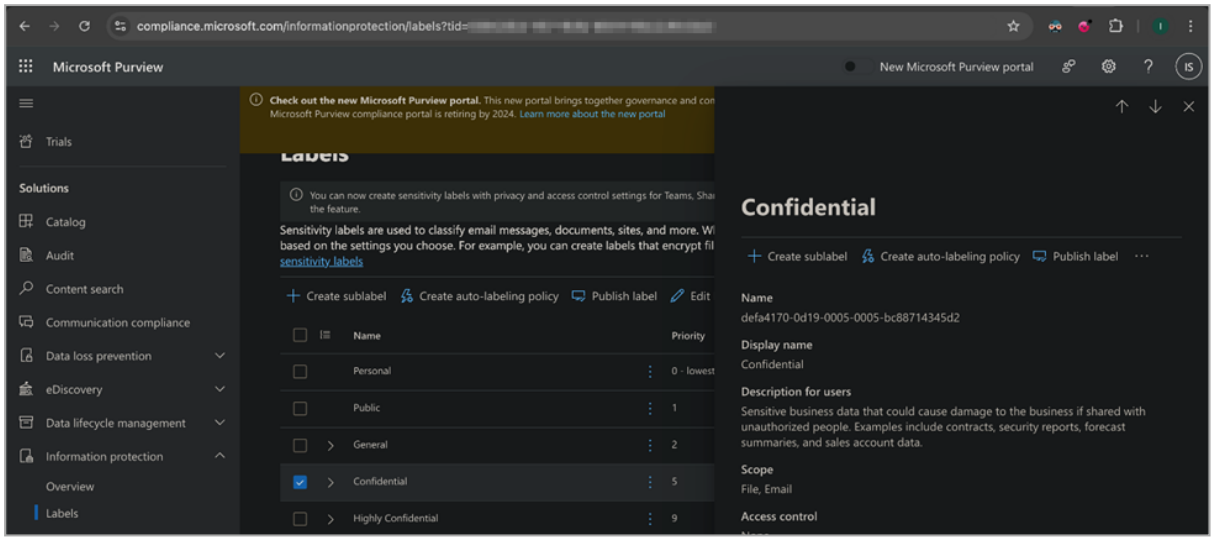
Managing Microsoft Sensitivity Labels for DLP

SASE allows you to integrate Sensitivity labels from Microsoft Purview Information Protection into your DLP system, providing an additional layer of data protection based on predefined sensitivity classifications.

Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview

Finding the UUID of labels in the Old Microsoft Purview portal

1. Log in to Microsoft Purview Portal: https://purview.microsoft.com/
2. Go to **Solutions** > **Information protection** > **Labels**.



3. Click the label name for which you want to find the UUID.
4. Copy the UUID in the **Label ID** or **GUID** section.

Finding the UUID of labels in the New Microsoft Purview portal

1. Install the Exchange Online Management Module

   The Microsoft Purview Security & Compliance PowerShell uses the Exchange Online Management Module for connection.

   a. Open PowerShell as an administrator.

   b. Run the following command:

   ```
   Install-Module -Name ExchangeOnlineManagement -Force
   ```

   c. If the system prompts to install `NuGet` or trust the repository, enter `Y` and click **Enter**.

2. Connect to the Microsoft Purview Security & Compliance Center.

   a. Run the following command to create a session:

   ```
   Connect-IPPSSession
   ```

b. In the Microsoft login page that appears, authenticate with the Microsoft 365administrator credentials.

Note - The administrator must have **Compliance Administrator** or **Information Protection Administrator** roles.

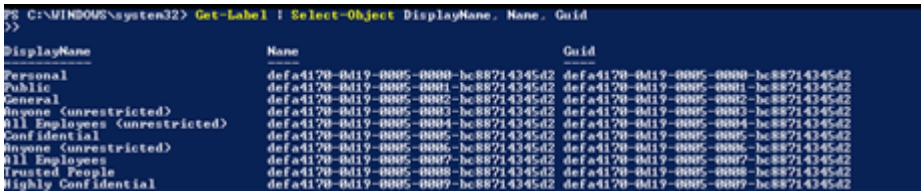
c. If your Microsoft Purview portal has Multi-Factor Authentication (MFA), complete the MFA process.

Once authenticated, the session connects to the Microsoft Purview Security & Compliance Center.

Now, you can run Microsoft Purview Security & Compliance PowerShell commands, such as managing labels, policies, or settings.

3. To view the UUID of the labels, run the following commands:

```
Get-Label | Select-Object DisplayName, Name, Guid
```

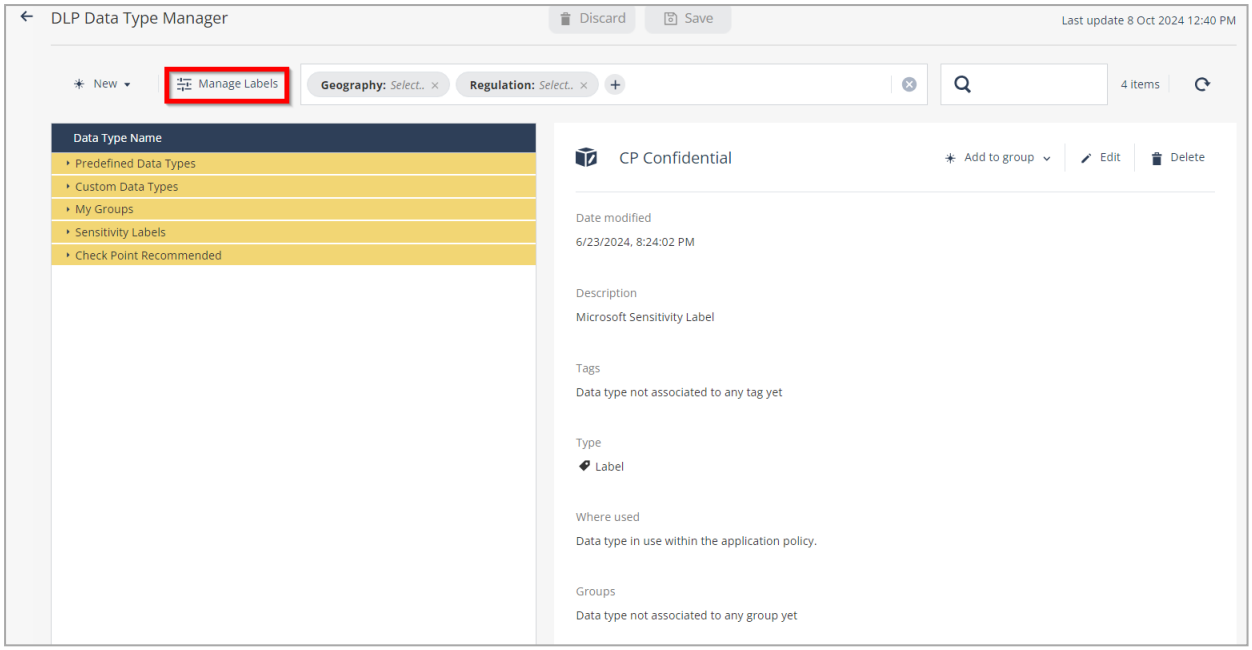


4. Copy the UUID of the labels.
5. To disconnect the session, run the following command:

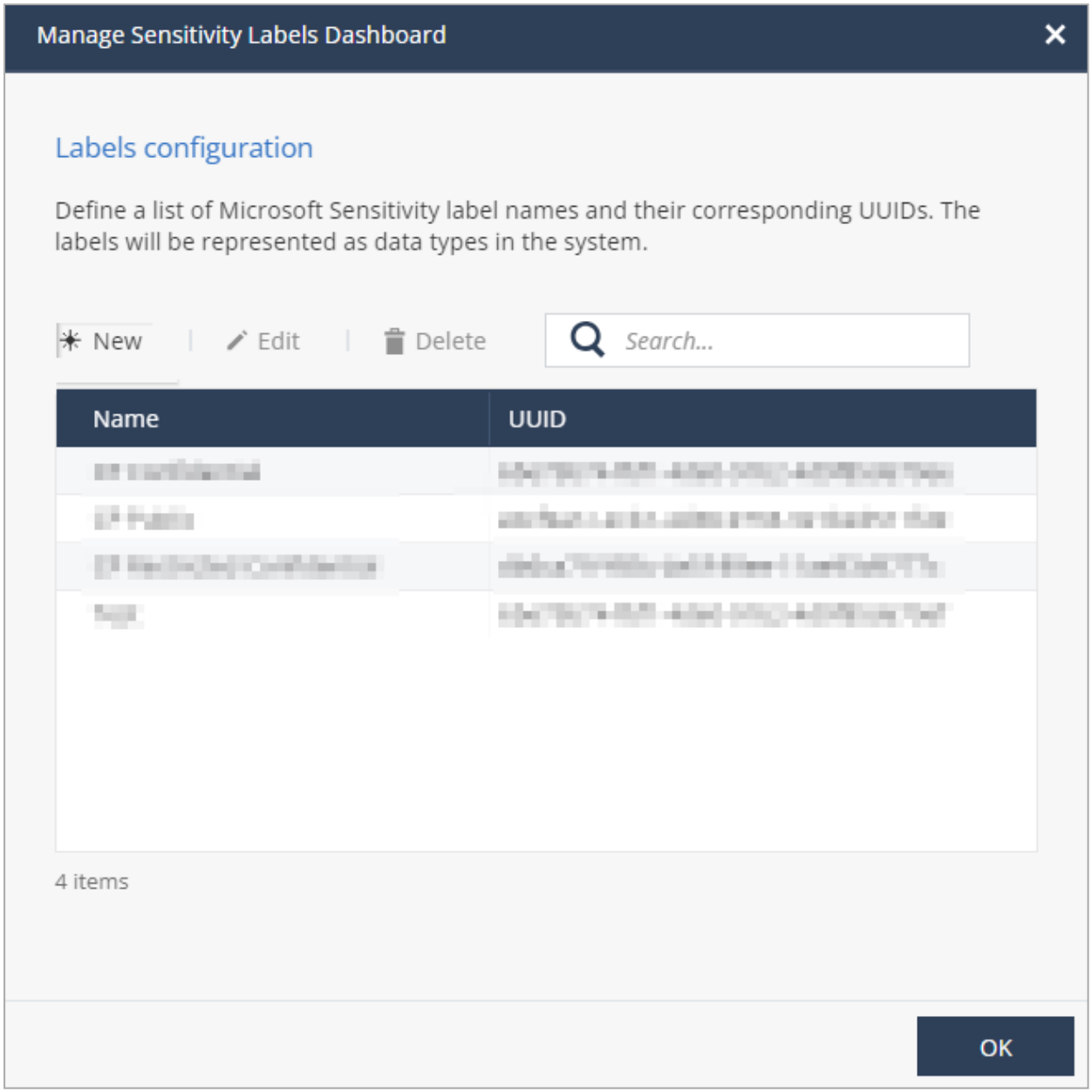
```
Disconnect-ExchangeOnline
```

Step 2 - Creating Microsoft Sensitivity Labels in SASE

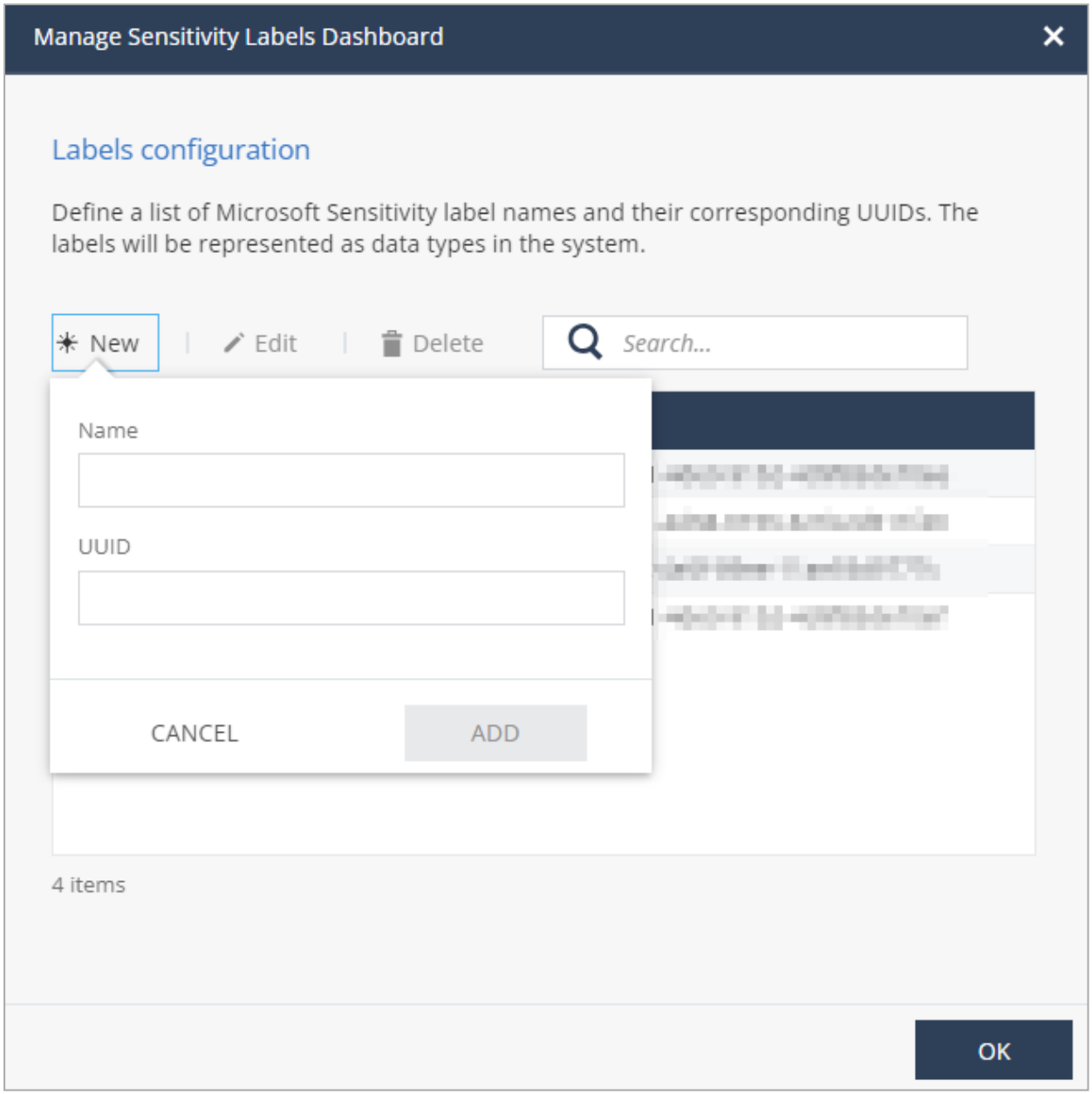
1. Log in to Check Point Portal and access the SASE Administrator Portal:
2. Go to **Policy** > **Data Loss Prevention** and click **DLP Data Type Manager**.
3. Click **Manage Labels**.



The **Manage Sensitivity Labels Dashboard** window appears.


Manage Sensitivity Labels Dashboard
Labels configuration
Define a list of Microsoft Sensitivity label names and their corresponding UUIDs. The labels will be represented as data types in the system.
New
Edit
Delete
Search...
Name
UUID
4 items
OK

4. Click **New**.

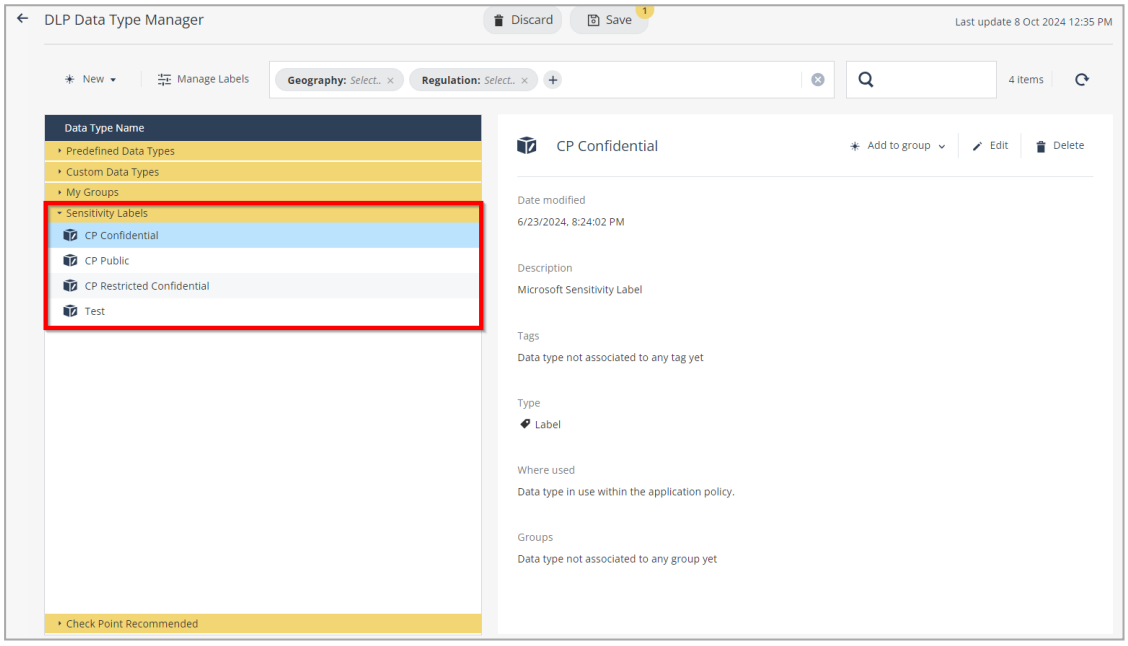


5. In the **Name** field, enter a name for the label. For example, *R&D Source Code*.
6. In the **UUID** field, enter the label UUID. For more information, see *"Step 1 - Copy the Microsoft Sensitivity label names and their UUIDs from Microsoft Purview" on page 865*.
7. Click **Add**.
8. Click **OK**.

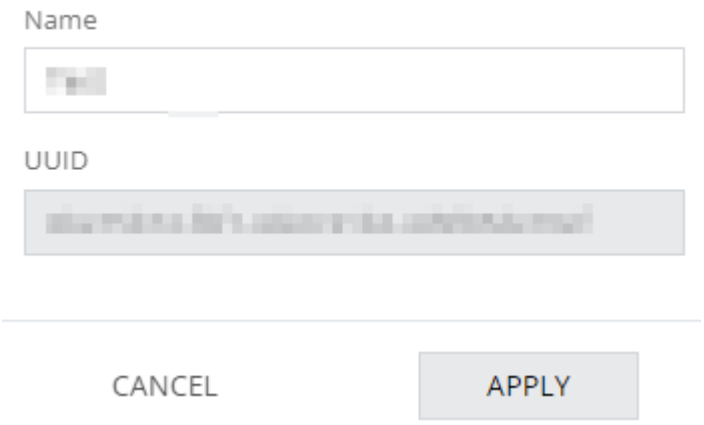
Note - The newly created label is now listed in **Sensitivity Labels** under **Data Type Name** section.
It also shows the label details:

- Date modified
- Description
- Tags - Shows tags assigned, if any, for further categorization
- Where used - Shows the DLP rule name that uses this label to enforce protection.
- Groups - Shows if the label is part of any group.

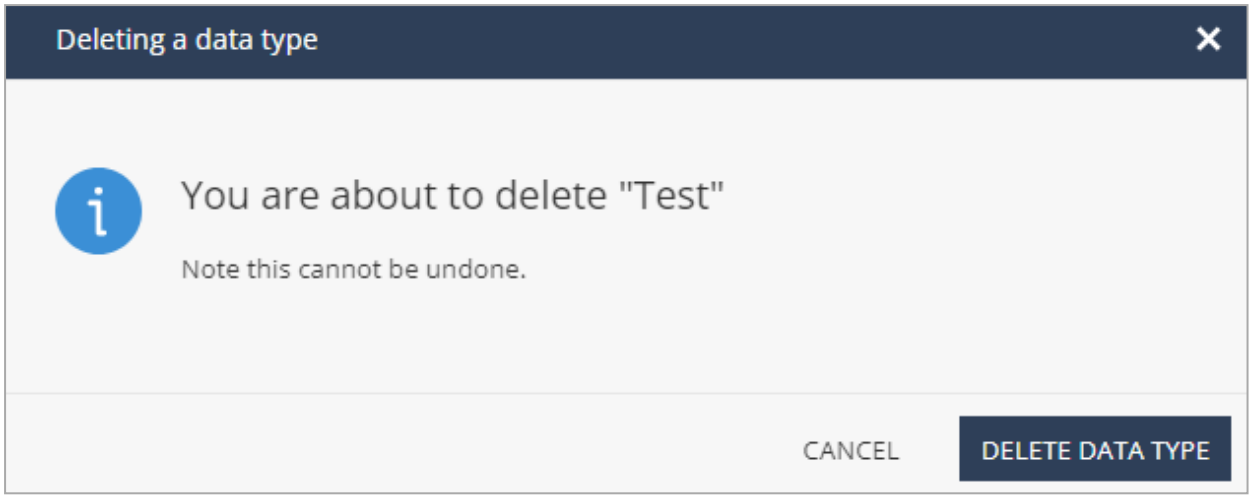
You can use Tags and Groups to better organize and manage the sensitivity labels.



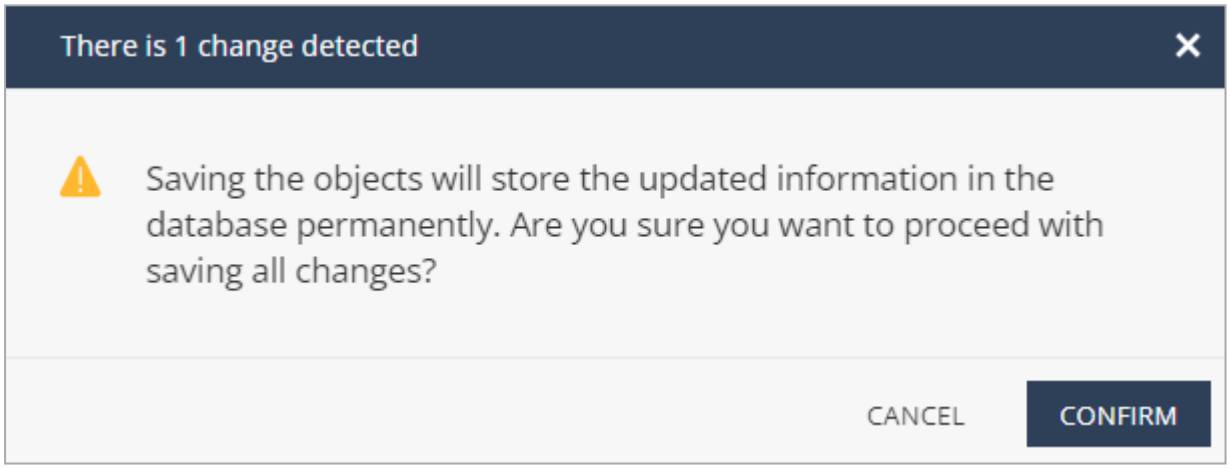
9. To edit a label, select the label you want to edit, click **Edit**, update the fields and then click **Apply**.



10. To delete a label, select the label you want to delete, click **Delete** and then click **Delete Data Type**.



11. Click **Save**.



12. Click **Confirm**.

Step 3 - Assign Sensitivity Labels to DLP Rules

After creating Sensitivity labels in SASE, you must assign them to the DLP rules to enforce data protection based on these sensitivity labels.

To assign sensitivity labels to a DLP rule, see Creating a DLP Rule.

DLP Logs

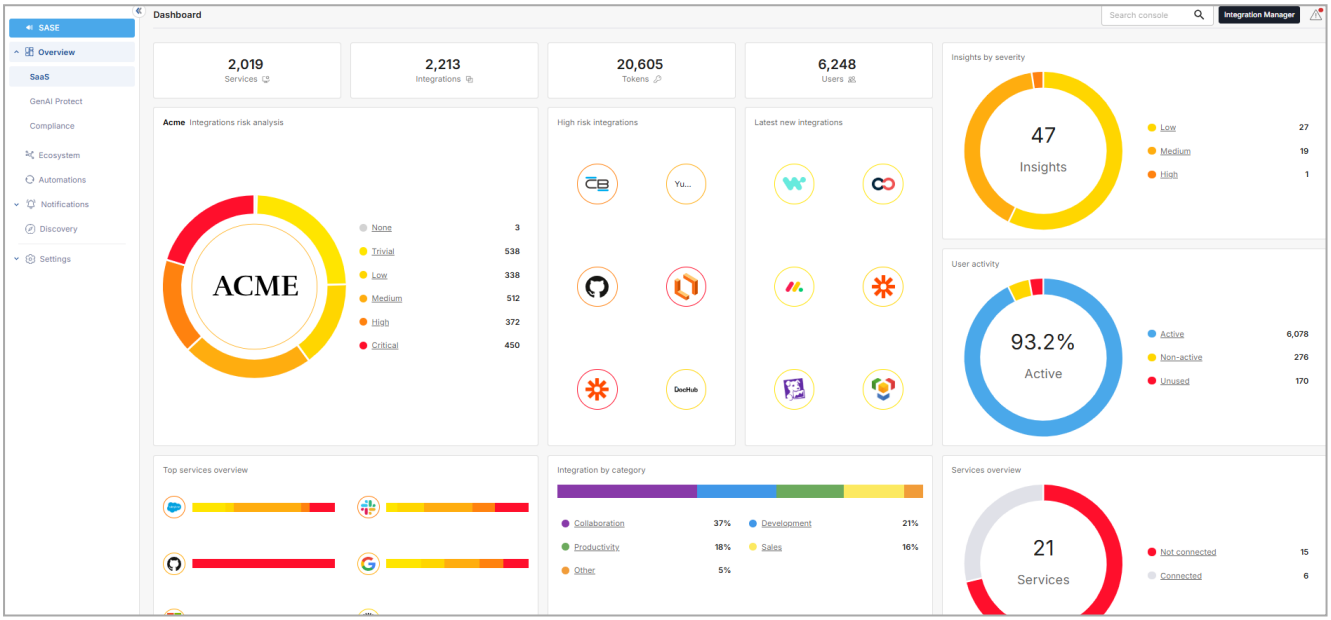
- Logs are sent for **Prevent** and **Detect**.
- File upload event generates a log for each handled file, regardless of whether the event is prevented, or detected.

SaaS API

SaaS Security provides automated monitoring and threat prevention for your organization's SaaS ecosystem, protecting against data theft, cyber espionage, unauthorized access, risky connections, and poor security configurations like missing MFA or SSO.

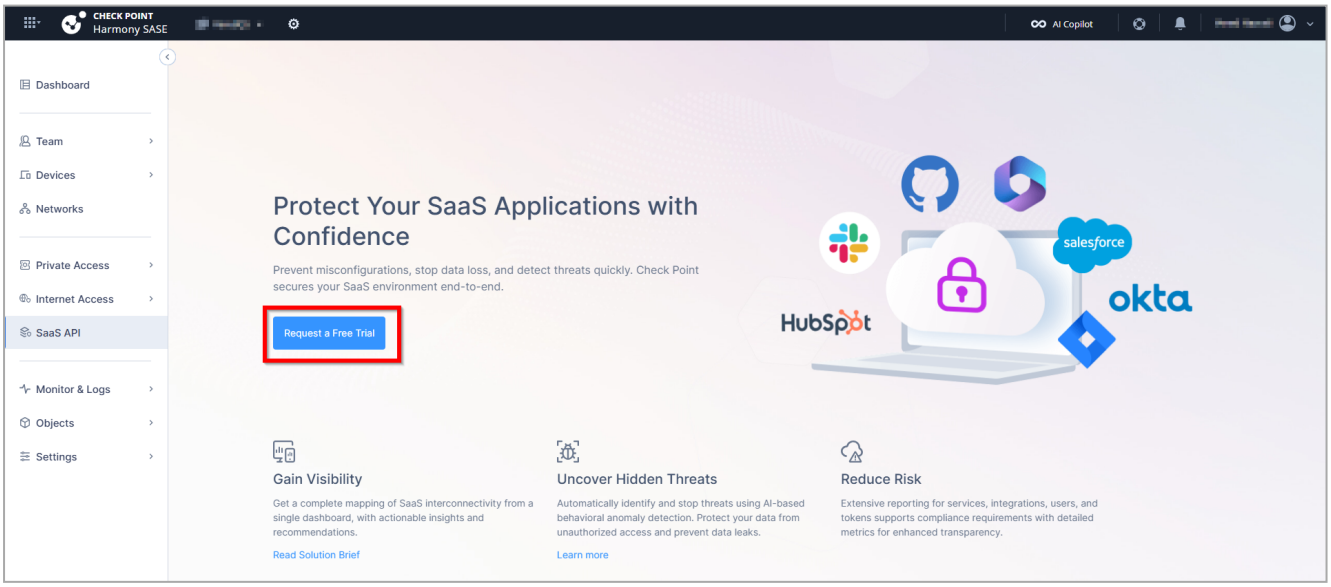
To access the **SaaS API** page, access the SASE Administrator Portal and click **SaaS API**.

The SaaS Security application page appears.



Note - To return to the SASE Administrator Portal, click **SASE** in the left navigation pane.

If you are accessing SaaS API for the first time, the SaaS Security introduction page appears. Click **Request a Free Trial** to explore SaaS Security.



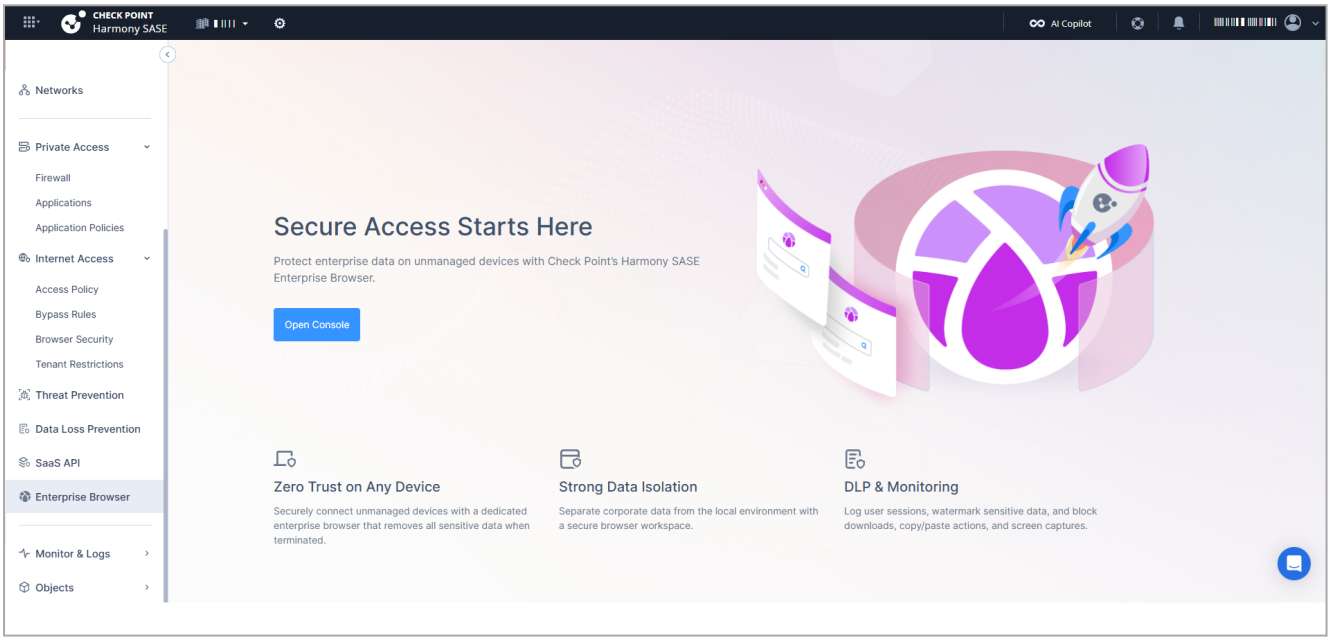
For information on integrating your SaaS applications, refer to the SaaS Security Administration Guide.

Enterprise Browser

The Enterprise Browser is a Chromium-based browser integrated with Check Point SASE. It is built on the SURF Security application. It can be used independently or as an extension within the SASE environment. The browser provides enhanced security features, including support for Zero Trust Network Access (ZTNA) and Single Sign-On (SSO) integration with Check Point platforms.

Enterprise Browser supports both managed and unmanaged devices, providing more flexibility and capabilities.

To access the Enterprise Browser page, access the SASE Administrator Portal and click **Enterprise Browser**.



For additional details, see the SURF Support and Document Portal.

Key Capabilities

- Data Isolation - Secure browser container isolates corporate data from device OS.
- DLP Controls - Block uploads, downloads, copy and paste, print, and screen capture. Files can be encrypted and scanned before access. Watermarks deter screen capture. Password managers are blocked and credentials are never stored locally.
- Agentless Device Posture Check - Validates AV, disk encryption, OS, and running processes without installing agents. Ideal for unmanaged devices.

- Full Session Visibility and Auditing - Logs navigation, usage, keystrokes, and system metrics. Supports audit, compliance, and incident response. Monitoring is role-based and context-aware. Defends against MITM attacks on insecure networks.

Use Case

- Third-Party Contractors - Grant temporary access with download restrictions, session termination, and activity monitoring.
- BYOD Compliance - Enforce HIPAA, GDPR, and NIS2 compliance with data isolation and audit logging.
- Short-Term Access - Enable secure access without provisioning devices for projects or Mergers and Acquisitions (M&A).
- Privileged Users - Restrict tool usage and monitor activity for developers, admins, and support teams.

Prerequisites

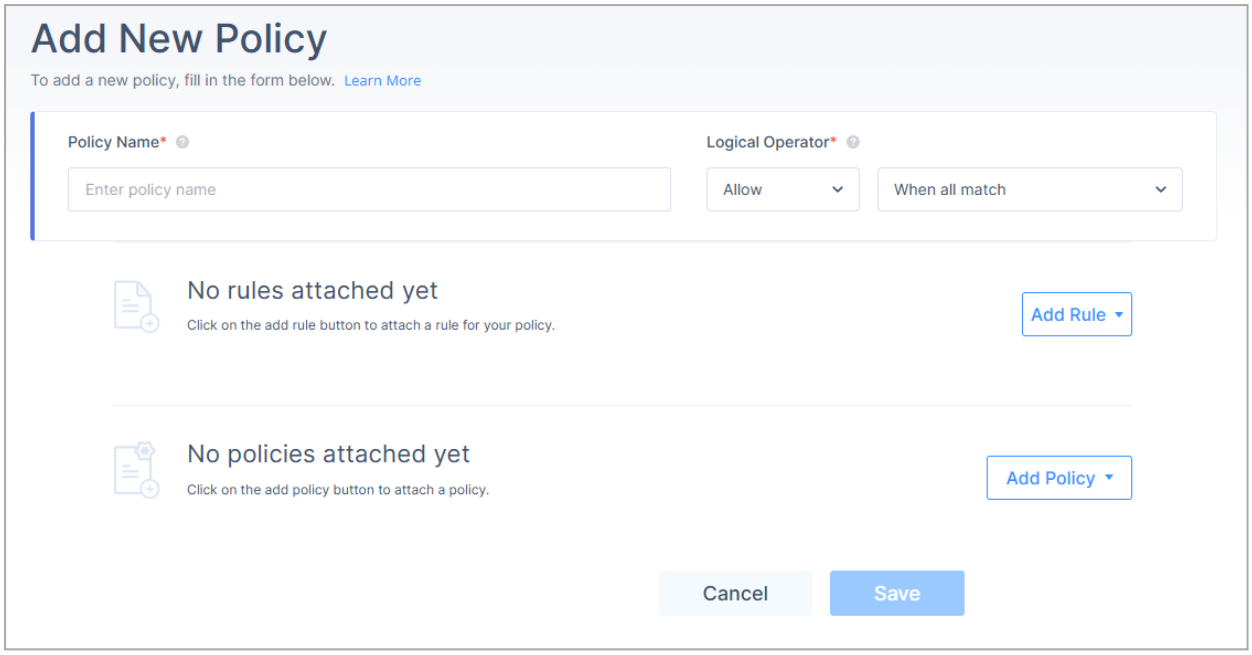
Admin access to both the SURF Security platform and the Check Point Portal.

Configuring Enterprise Browser

Step 1: Creating an Application Access Policy

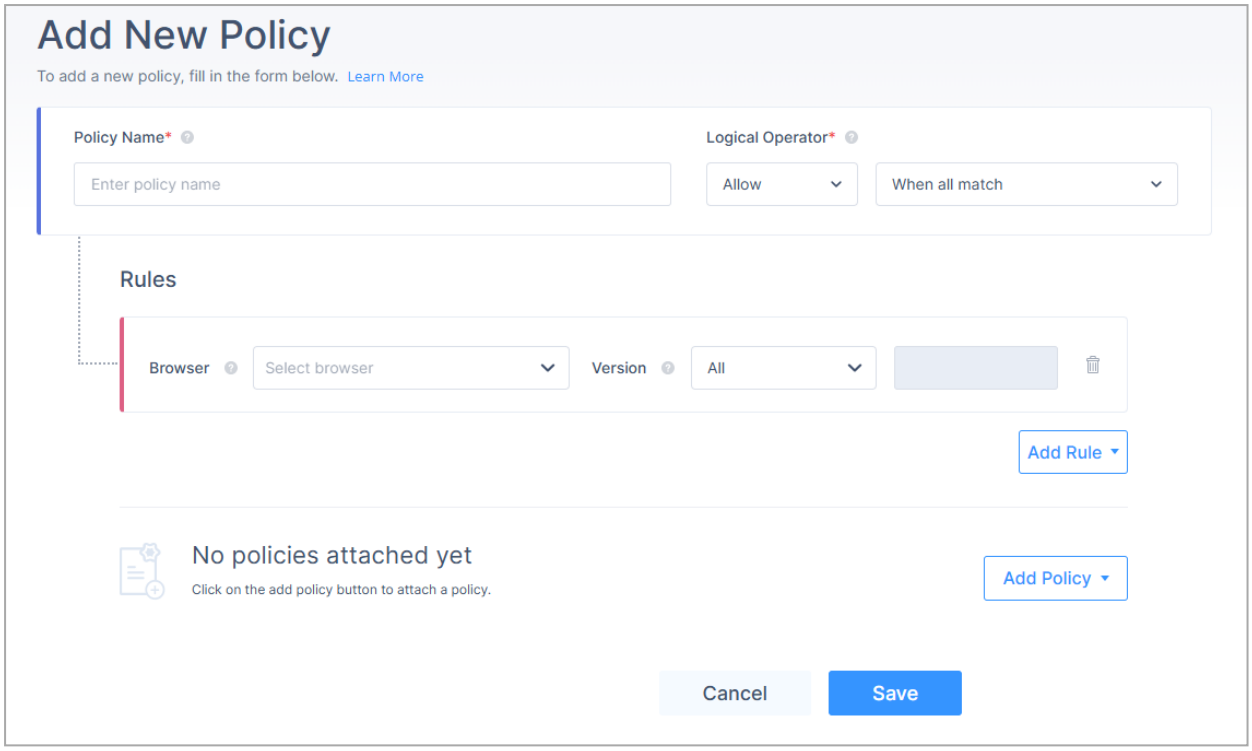
1. Access the SASE Administrator Portal and click **Private Access** > **Application Policies**.
2. Click **Add Policy**.

   The **Add New Policy** page appears.



3. Enter these:
   a. **Policy Name** - Name of the policy.
   b. **Logical Operator**:
      - From the **Policy Action** list, select either of these:
        - **Allow**
        - **Deny**
      - From the list, select one of these:
        - **When all match** – The policy is considered compliant only if all defined rules are met.
        - **When some match** – The policy is considered compliant if at least one defined rule is met.
4. To add the rules for the policy, click **Add Rule** and select **Browser**.

   The **Rules** section appears.

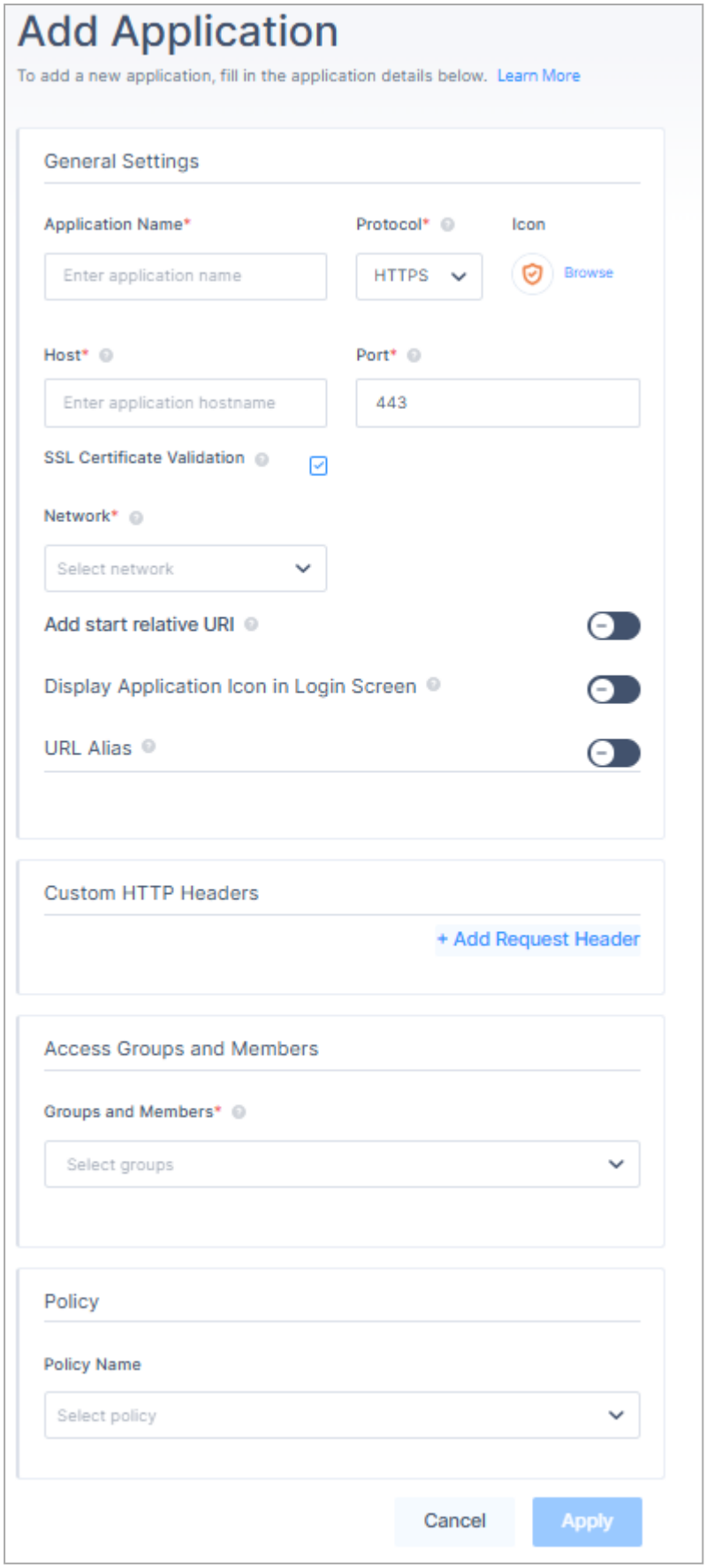


5. From the **Browser** list, select **Check Point SASE Enterprise Browser**.
6. Click **Save**.

Step 2: Defining Application Policy

1. Go to **Private Access** > **Applications**.
2. Click **Add Application**.

   The **Add application** window appears.



3. Specify these:

a. **Application Name**

b. **Protocol**

- **HTTPS**
- **RDP**
- **SSH**
- **VNC**

c. **Host**

d. **Port**

e. **Network**

f. **Groups ad Members**

g. **Policy Name** - Select the policy name that you created in Step 3.a while Creating an Application Access Policy.

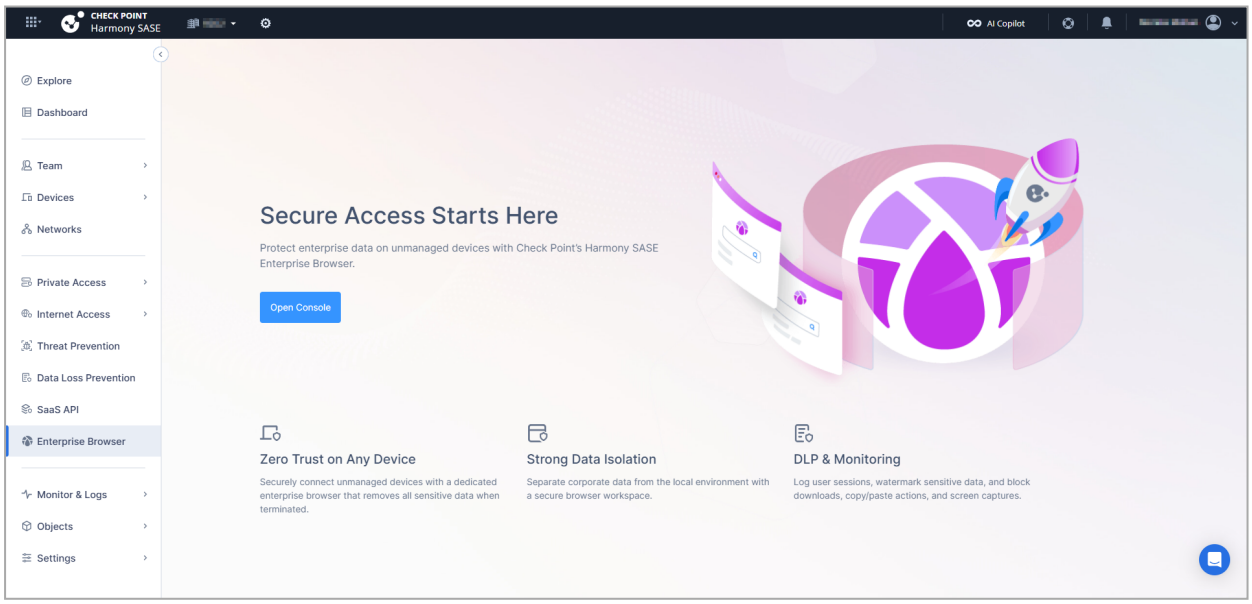
For information on how to add an application, see Adding an Application.

4. Click **Apply**.

The system lists the application in the **Applications** page and enables it by default.

Step 3: Accessing the Admin Console of Enterprise Browser

1. Access the SASE Administrator Portal and click **Enterprise Browser**.



2. Click **Open Console**.

The Enterprise Browser Admin Console is launched.

3. Sign in through SSO.

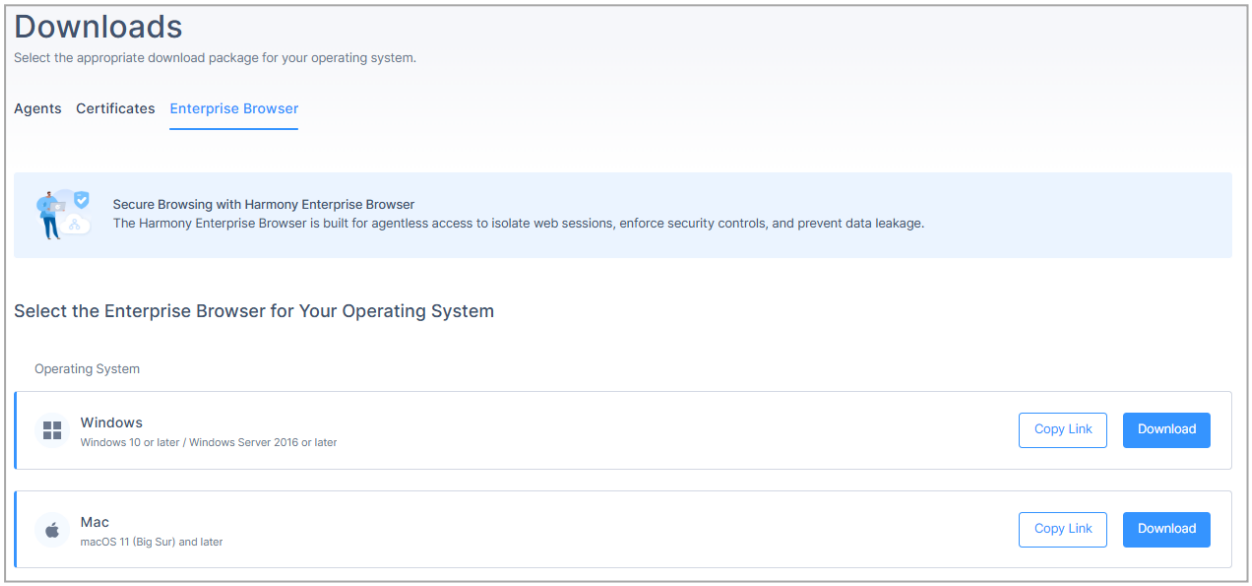
   Note - Only users with admin role can access the console.

4. To download the enterprise browser, go to **Devices** > **Downloads** > **Enterprise Browser** and then select the enterprise browser for your Operating System, and click **Download**.

   For more information, see Downloads.

Step 4: Downloading the Enterprise Browser

1. Access the SASEAdministrator Portal and click **Devices** > **Downloads**.
2. Click the **Enterprise Browser** tab.



3. Do one of these:
   - Click **Download**.

     The system downloads an EXE file.
   - Click **Copy Link** to copy the download link. Share the link with members.

Monitor & Logs

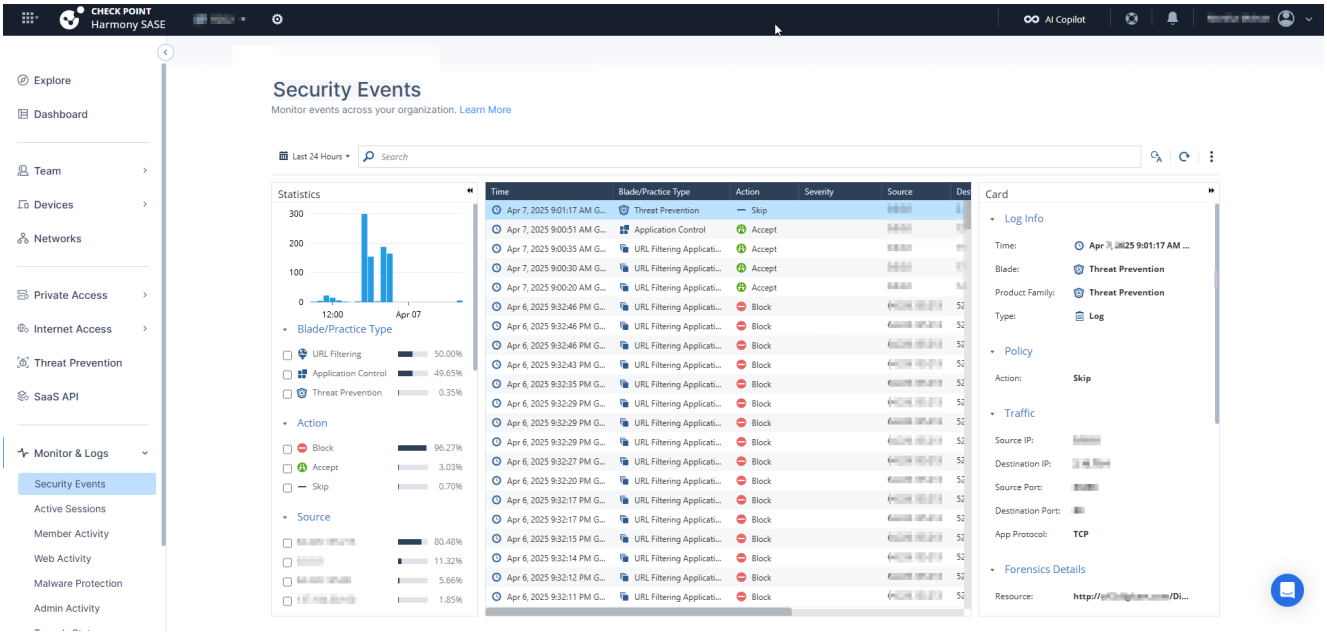
Monitor & Logs allows you to view:

- *"Security Events" below*
- *"Operational Events" on page 887*
- *"Active Sessions" on page 892*
- *"Member Activity" on page 895*
- *"Web Activity" on page 897*
- *"Malware Protection" on page 900*
- *"Admin Activity" on page 903*
- *"Tunnels Status" on page 907*
- *"Firewall Events" on page 908*

Security Events

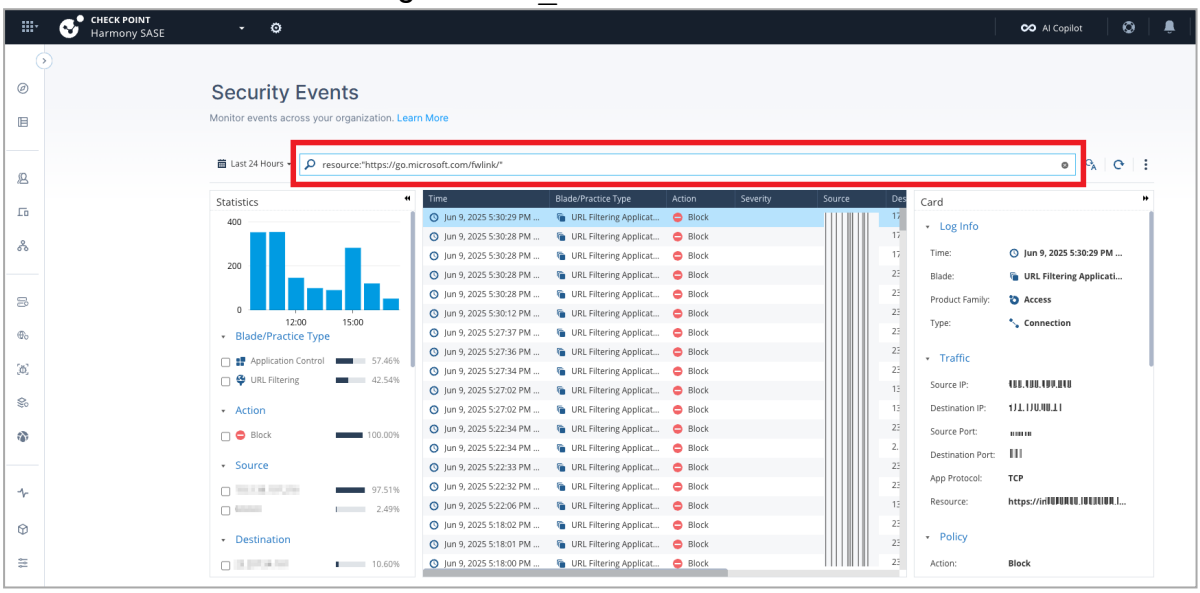
The Security Events provides an integrated view of security events directly within the SASE platform. It allows easy monitoring, searching, and filtering of SASE related security events.

To view the **Security Events** page, access SASE and go to **Monitor & Logs** > **Security Events**.



Notes:

- Security Events limit the number of events to 300 per search.
- You can also search for additional parameters that do not appear as quick filters. For example:
  - The URL resource using `resource:"https://go.microsoft.com/fwlink/"`
  - The Destination Port by using `dst_port: 443`
  - The Source Port by using `src_port:55321`
  - The Device name using `device_name: "DESKTOP-123"`

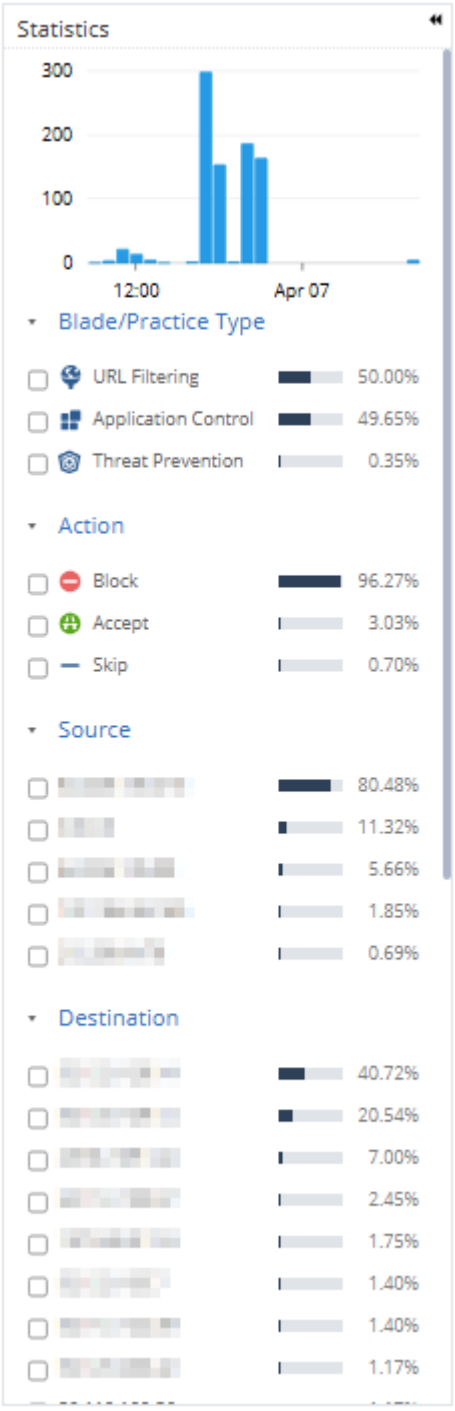


Supported Events

The Security Events supports these event types:

- URL Filtering and Application Control
- Threat Emulation
- Malware Protection
- Anti-Bot
- Firewall Events

Statistics



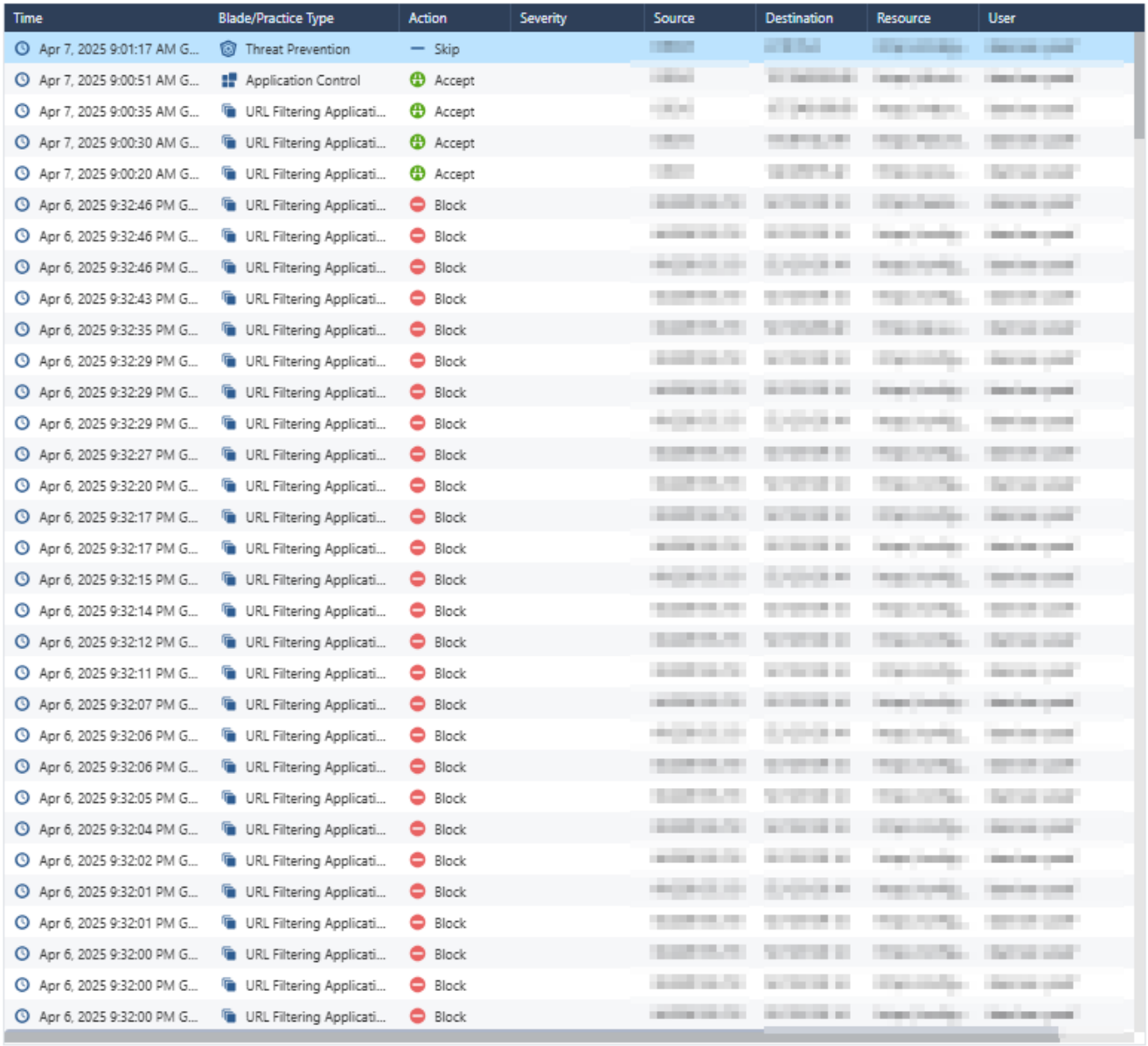
The Statistics panel provides a visual summary including these:

- Event distribution by Blade Type
- Breakdown by Actions:

- Accept
- Block
- Detect
- Skip

- Source IP distribution

Events

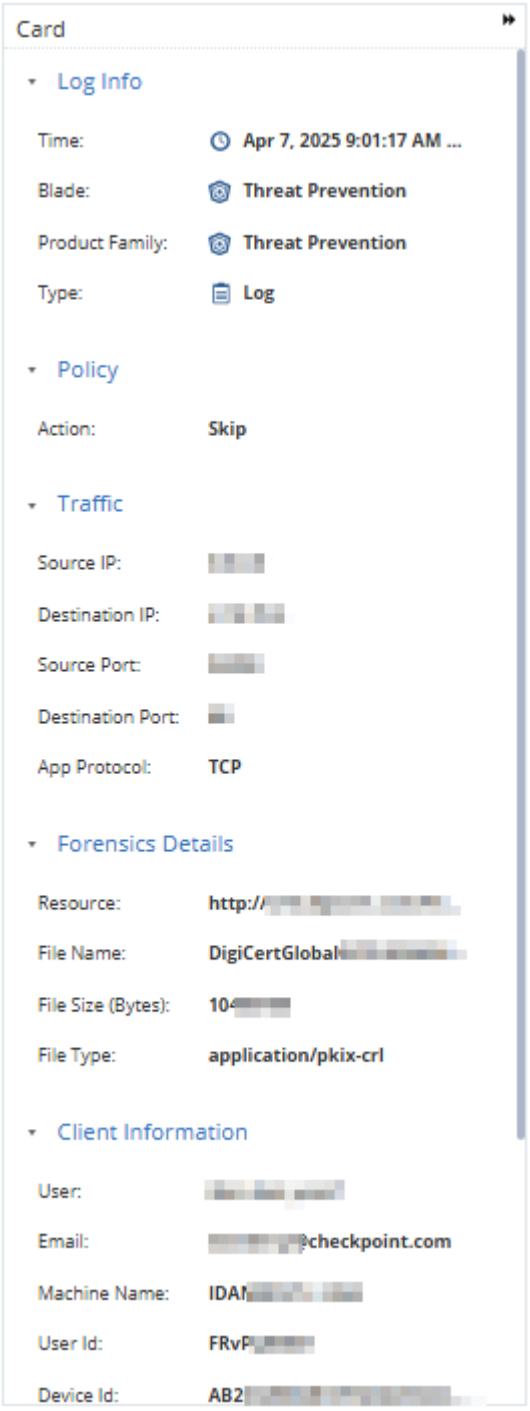


Time	Blade/Practice Type	Action	Severity	Source	Destination	Resource	User
Apr 7, 2025 9:01:17 AM G...	Threat Prevention	Skip					
Apr 7, 2025 9:00:51 AM G...	Application Control	Accept					
Apr 7, 2025 9:00:35 AM G...	URL Filtering Applicati...	Accept					
Apr 7, 2025 9:00:30 AM G...	URL Filtering Applicati...	Accept					
Apr 7, 2025 9:00:20 AM G...	URL Filtering Applicati...	Accept					
Apr 6, 2025 9:32:46 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:46 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:46 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:43 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:35 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:29 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:29 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:29 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:27 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:20 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:17 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:17 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:15 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:14 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:12 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:11 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:07 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:06 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:06 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:05 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:04 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:02 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:01 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:01 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:00 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:00 PM G...	URL Filtering Applicati...	Block					
Apr 6, 2025 9:32:00 PM G...	URL Filtering Applicati...	Block					

Column	Description
Time	Timestamp when the event occurred.

Column	Description
Blade/Practice Type	Specific security module responsible for the event, for example, URL Filtering and Malware Protection.
Action	Security action taken: ■ Accept - Accepts the event ■ Block - Blocks the event ■ Detect - Detects the event ■ Skip - Bypasses the event
Severity	Severity level of the event.
Source/Destination IP	Network endpoints involved.
Resource	URL or resource accessed.
User	User name.

Card



You can click on a specific event entry to open a detailed event card, which provides:

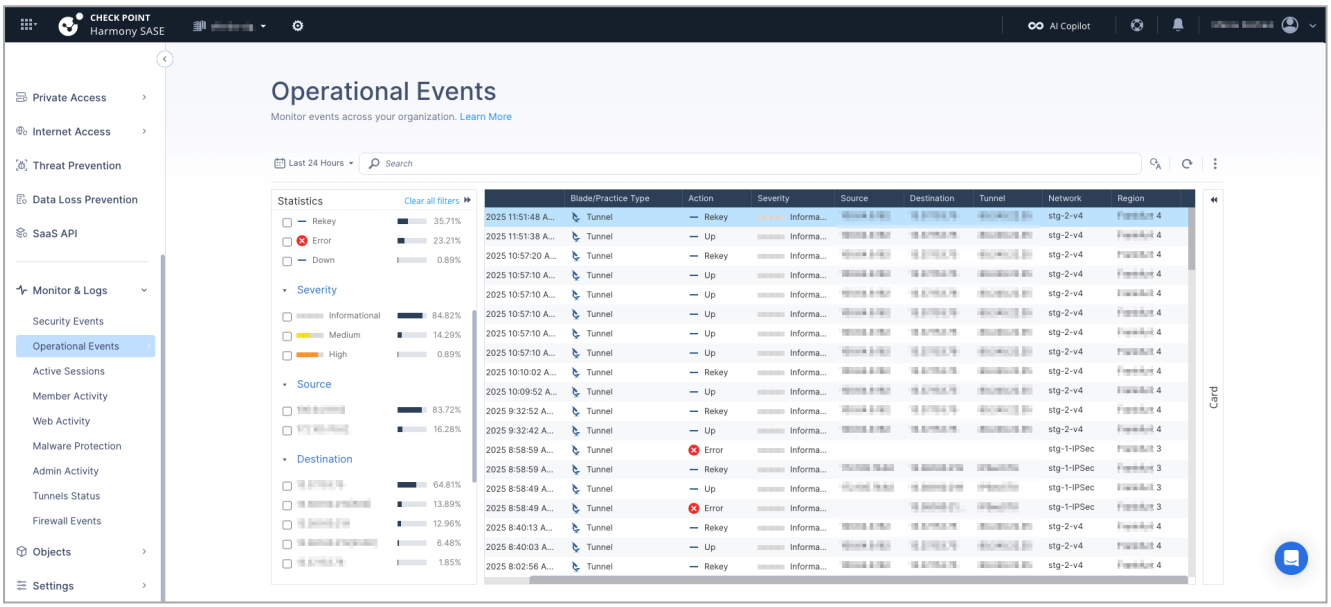
- Complete event description.
- Session details, such as ports, URLs, downloaded data and so on.

The card offers an in-depth view for thorough analysis.

Operational Events

The Operational Events provides an integrated view of Operational events directly within the Check Point SASE platform. It allows easy monitoring, searching, and filtering of Check Point SASE related Operational events.

To view the **Operational Events** page, access Check Point SASE and go to **Monitor & Logs** > **Operational Events**.



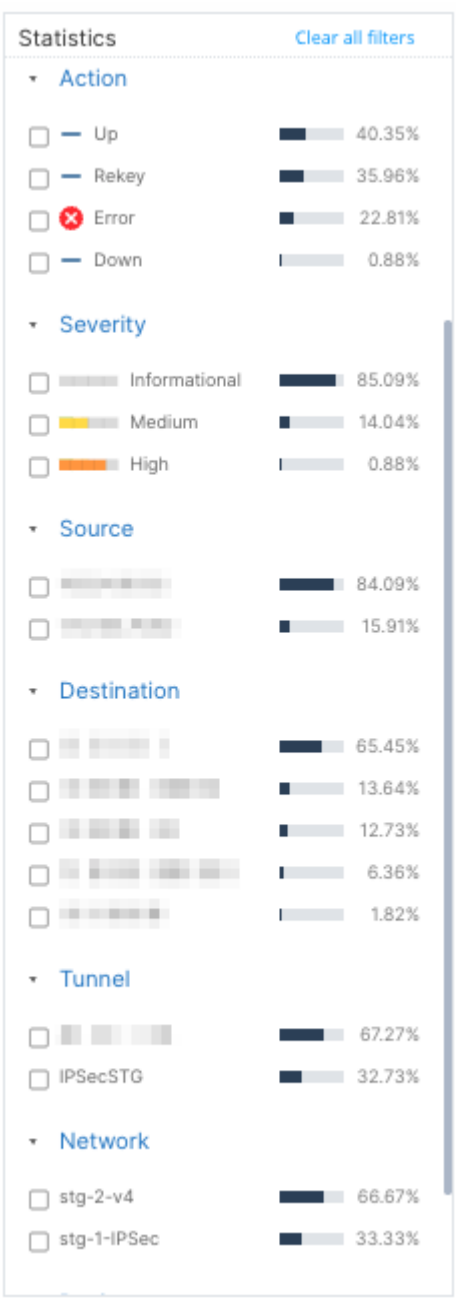
Note - The Operational Events limit the number of events to 300 per search.

Supported Events

The Operational Events supports these event types:

- Tunnel Status Events
- IPSec Events

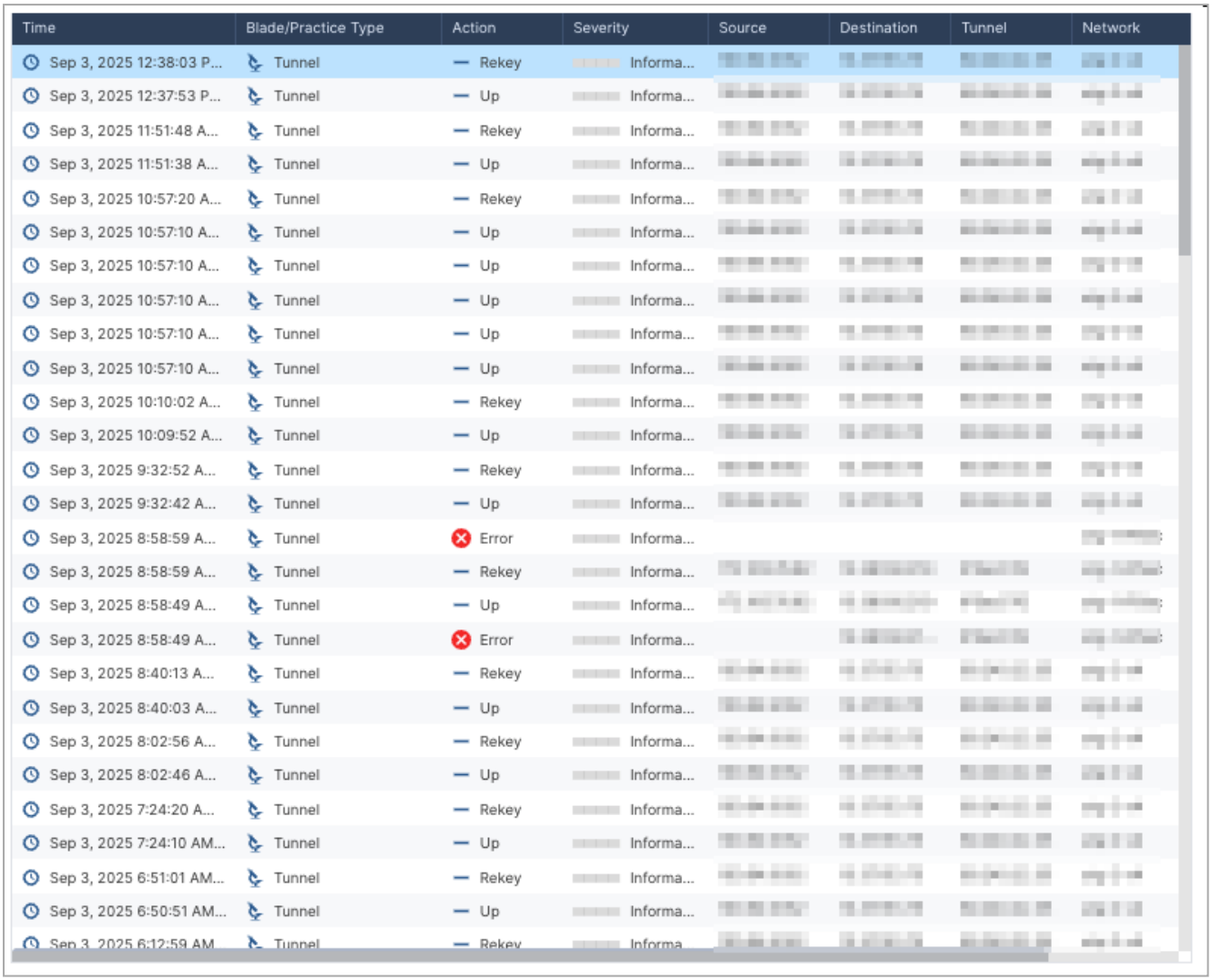
Statistics



The Statistics panel provides a visual summary including these breakdown by Actions:

- Severity
- Source
- Destination
- Tunnel
- Network

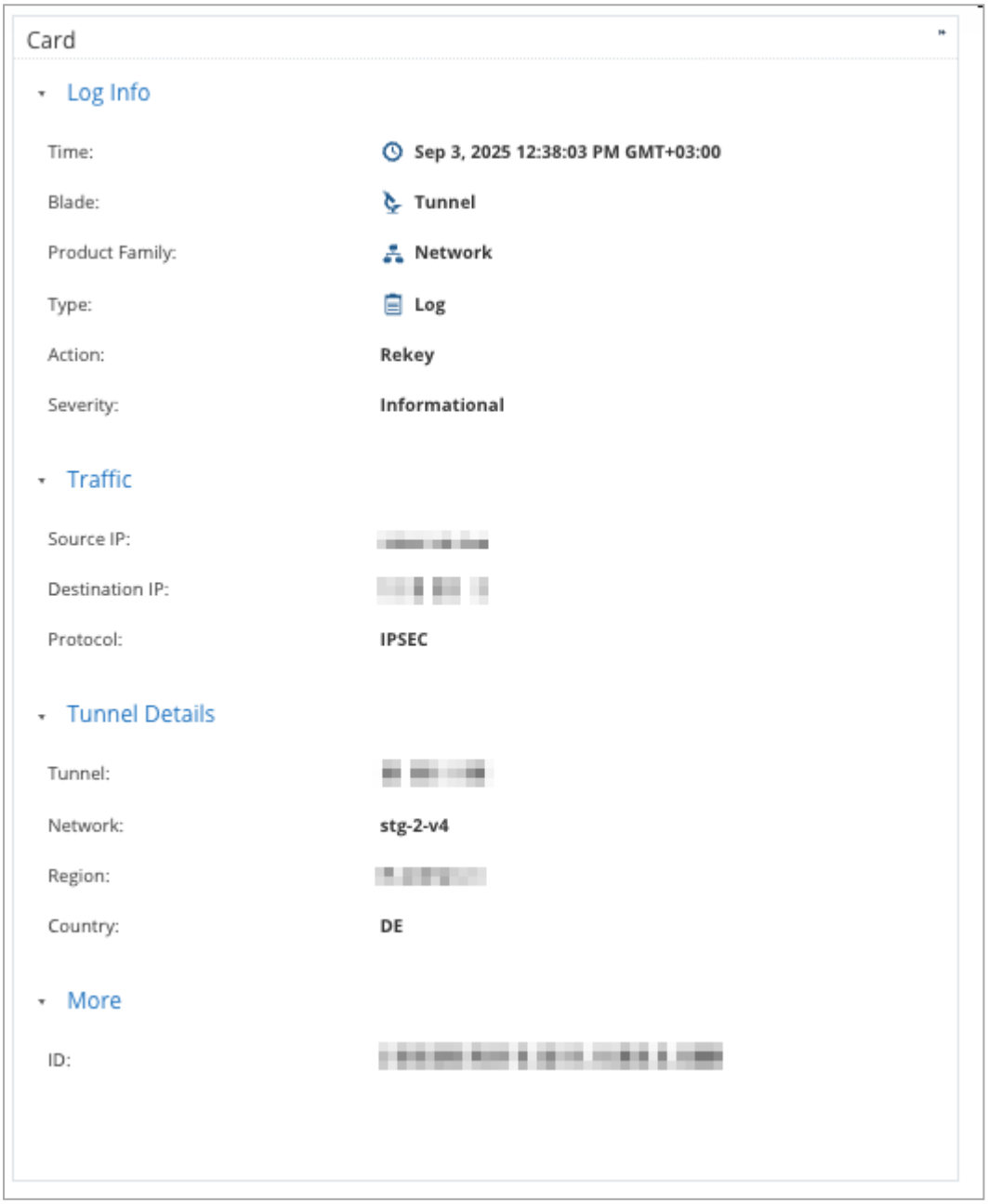
Events



Column	Description
Time	Timestamp when the event occurred
Blade/Practice Type	Supports only Tunnel
Action	Security action taken: ■ Up - Tunnel Up Event Occurred ■ Down - Blocks the event Initiation ■ Failed - Detects the event ■ ReKey - Bypasses the event ■ Error - IPSec Error
Severity	Severity level of the event

Column	Description
Source/Destination IP	Tunnel Endpoints
Tunnel	Tunnel name
Network	Network name
Region	Region

Card



To view a detailed event card, click on a specific event entry. It provides the complete event description.

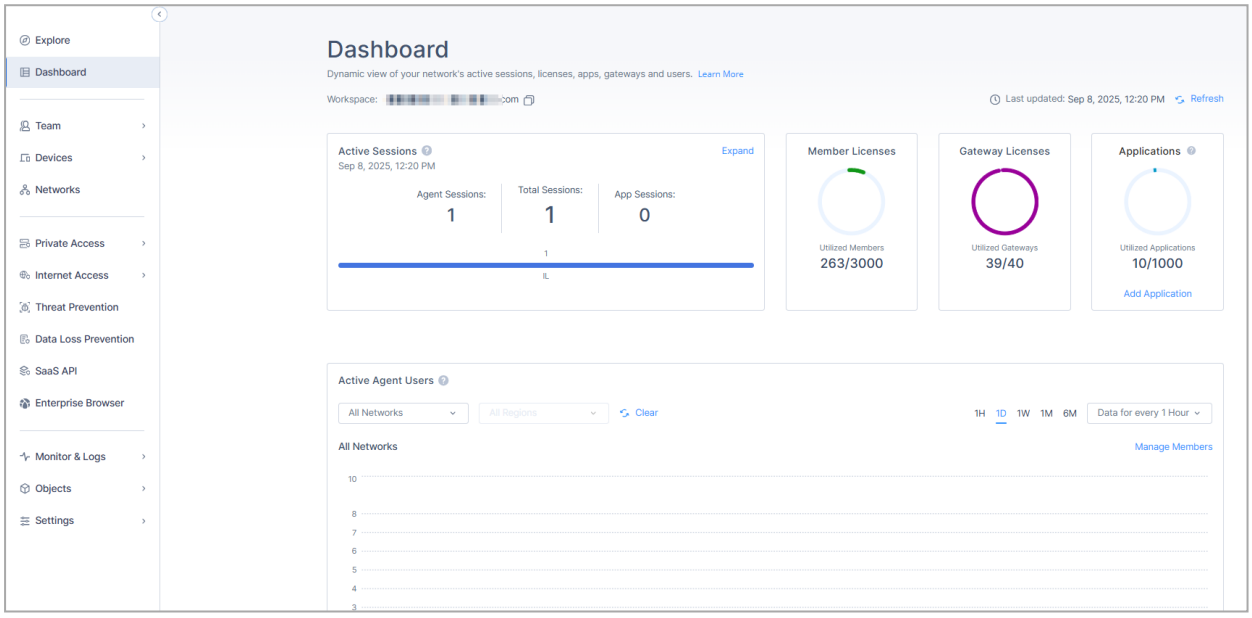
The card offers an in-depth view for thorough analysis.

Active Sessions

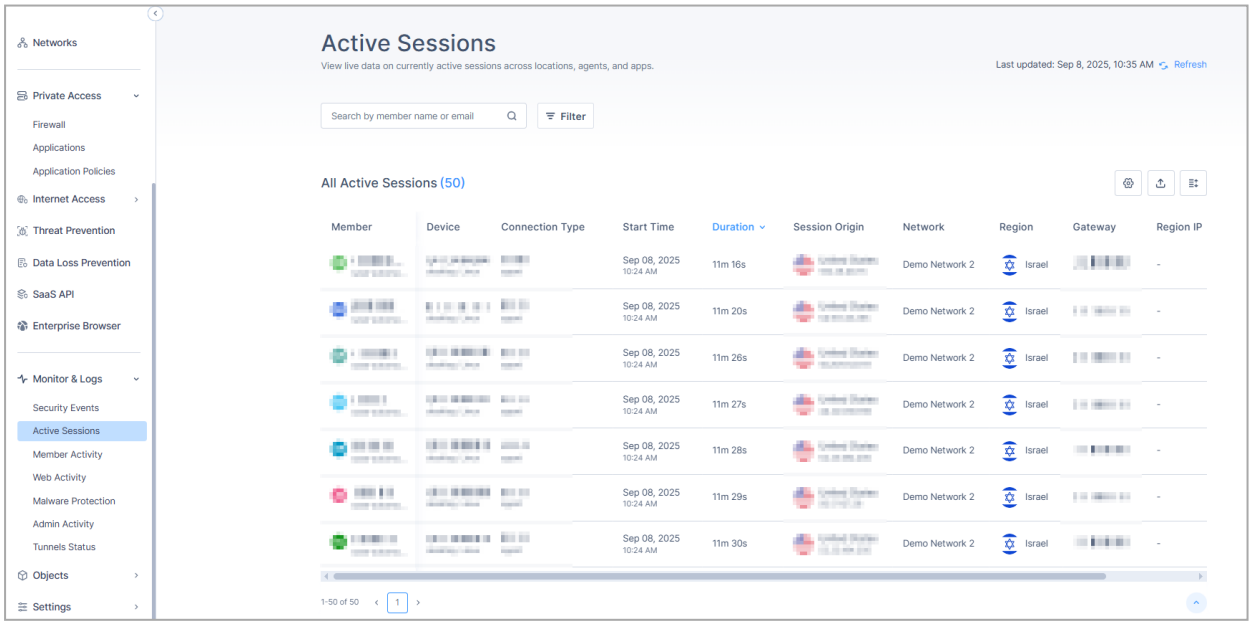
The **Active Sessions** page allows you to view detailed device information and perform actions such as logging out or removing devices.

To view the **Active Sessions** page, do either of these:

- Access the Check Point SASE Administrator Portal and click **Dashboard**, in the **Active Sessions** widget, click **Expand**.



- Access the Check Point SASE Administrator Portal and click **Monitor & Logs** > **Active Sessions**.



Column	Description
Member	Member name
Device	Name of device(s) logged in from.
Connection Type	Type of connection: ■ **app** - Member is connected to an application. ■ **agent** - Member is connected to the Check Point SASE Agent.
Start Time	Start date and time of the connection.
Duration	Duration of the connection.
Session Origin	Location of the connected network gateway. For the SASE Agent, it shows the IP address.
Network	Connected network name.
Region	Connected network region.
Gateway	SASE gateway IP address.

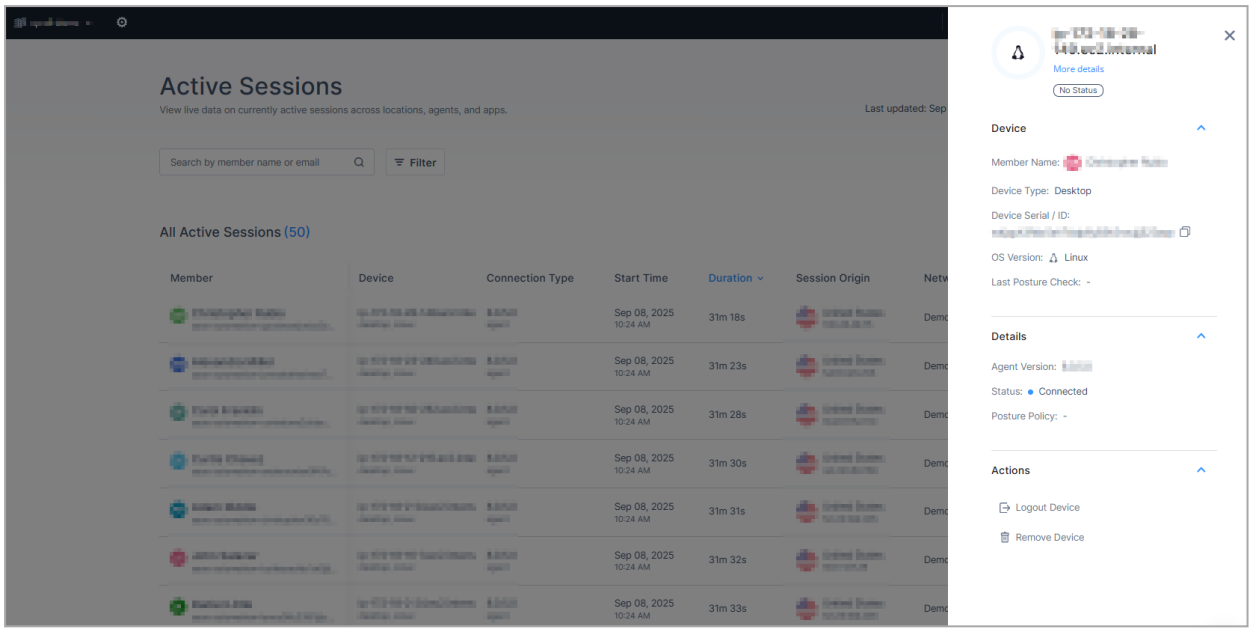
Action

- To select the columns required in the table, click the icon and select the columns.
- To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

  Note - You can export only the latest 1000 active sessions at a time.

- To view Member Activity Events, hover over a member row in the table, and when a view activity icon appears at the end of the row, click .
- To view more details about the device and perform actions, click the **Device** column in

the table.

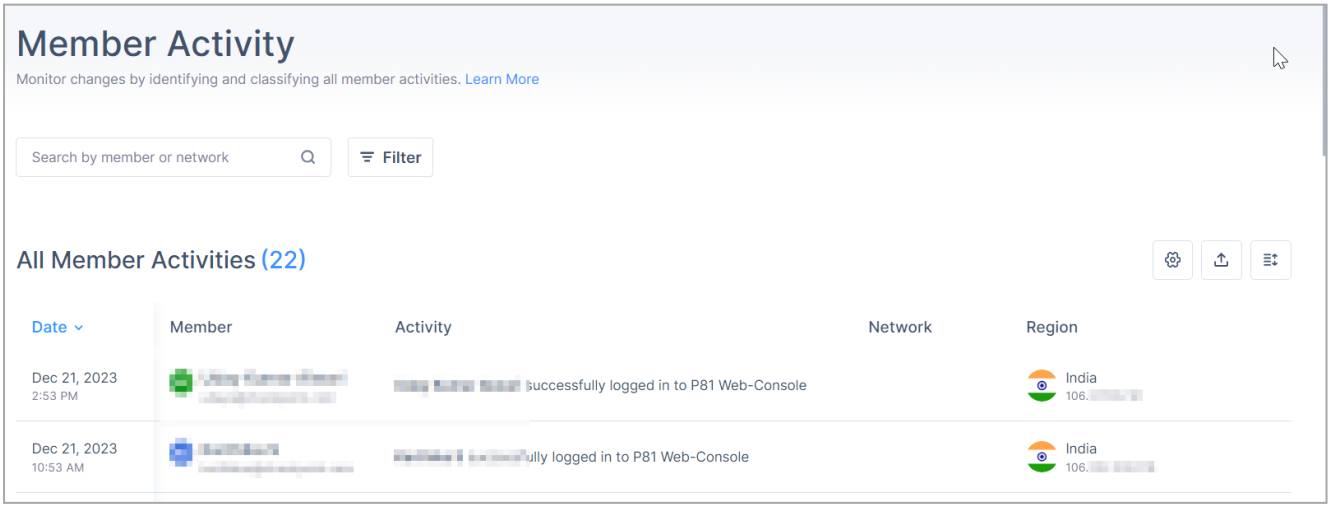

Active Sessions
View live data on currently active sessions across locations, agents, and apps.
Search by member name or email
Filter
All Active Sessions (50)
Member
Device
Connection Type
Start Time
Duration
Session Origin
Sep 08, 2025
10:24 AM
31m 18s
31m 23s
31m 28s
31m 30s
31m 31s
31m 32s
31m 33s
More details
No Status
Device
Member Name:
Device Type: Desktop
Device Serial / ID:
OS Version: Linux
Last Posture Check: -
Details
Agent Version:
Status: Connected
Posture Policy: -
Actions
Logout Device
Remove Device

Member Activity

The **Member Activity** page allows you to view these member activities:

- **Application access**
  - Application authorization successful / failed
  - Application session started / ended
- **Login**
  - Login success / failed
  - Log out success / failed
  - Web console login success / fail
  - User blocked from web console
  - IP blocked from web console
  - Account blocked
  - Device registration success / fail
  - Device unregistration success / fail
  - Network login success / fail
  - Network logout
- Member accepted the invitation
- Support team login / logout

To view the **Member Activity** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Member Activity**.



Column	Description
Date	Date and time of the activity.
Member	Member name.
Activity	Activity description.
Network	Connected network name.
Region	Region and gateway IP address of the connected session.

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

Note - You can export data of only 1000 activities at a time.

Web Activity

Note - This article is only applicable if the customer is not on the Infinity Portal yet.

The **Web Activity** page shows:

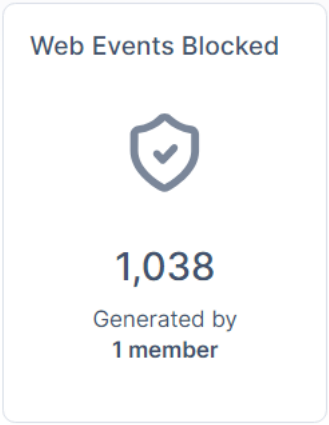
- *"Web Events Blocked" below*
- *"Top Web Categories" on the next page*
- *"Events Per User" on the next page*
- *"All Web Activities" on the next page*

To view the **Web Activity** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Web Activity**.

Insights

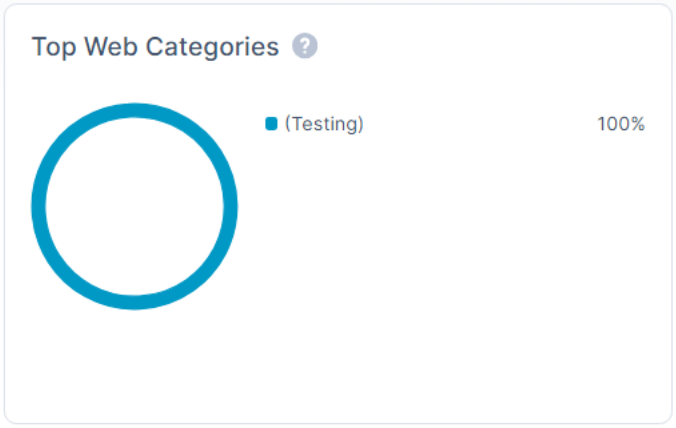
Insights shows the number of blocked web events, top web categories blocked, and top number of events blocked in the last 1 day, 7 days, and 30 days.

Web Events Blocked



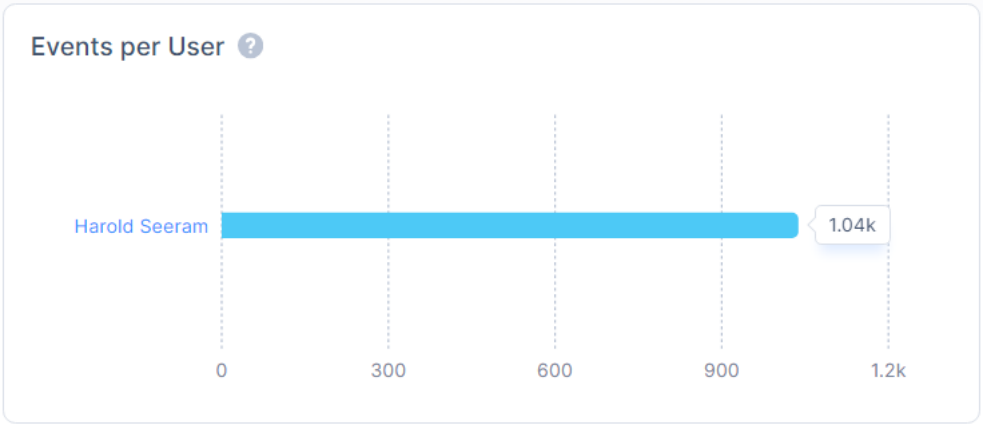
The **Web Events Blocked** widget shows the total number of URLs blocked in the selected time frame.

Top Web Categories



The **Top Web Categories** widget shows the top five web categories blocked in the selected time frame.

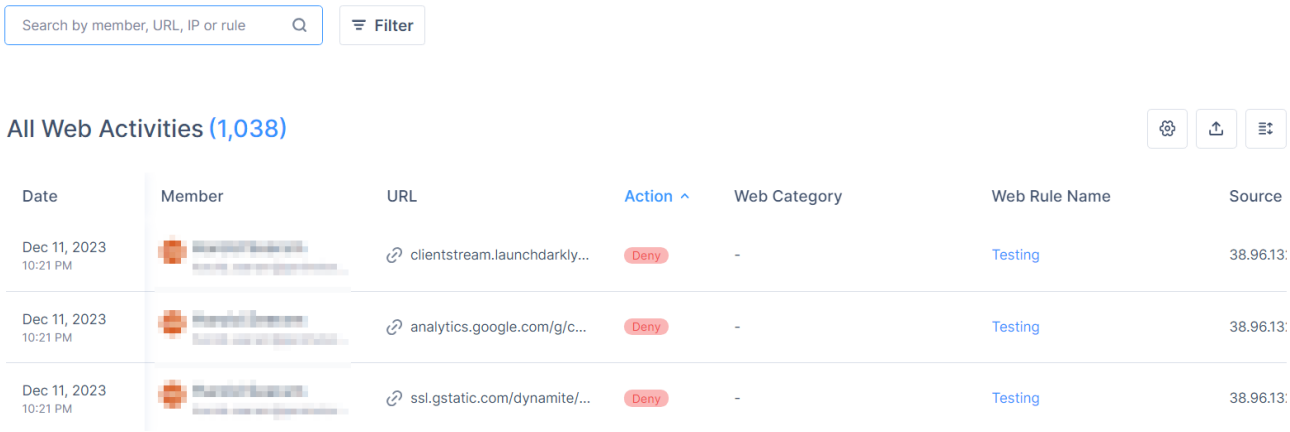
Events Per User



The **Events per User** widget shows the top five users with the highest number of violations for web categories in the selected time frame.

All Web Activities

All Web Activities table shows a log of all the URLs (web traffic) where the user is either warned or denied actions.



Column	Description
Date	Date and time of the activity.
Member	Member name.
URL	Accessed URL.
Action	Action taken by Check Point SASE: ■ Deny - Member is denied access to the URL. ■ Warn - Member is warned before accessing URL.
Web category	Category name configured in the *"Access Policy" on page 778*.
Web Rule Name	Web Rule name configured in the *"Access Policy" on page 778*.
Source IP	IP address of the source.
Destination IP	IP address of the destination.

To select the columns required in the table, click the ⚙ icon and select the columns.

To export the data, click the ⬆ icon. The system downloads an archive file with the data in JSON and CSV file format.

Note - You can export data of only 1000 activities at a time.

Malware Protection

The **Malware Protection** page allows you to view:

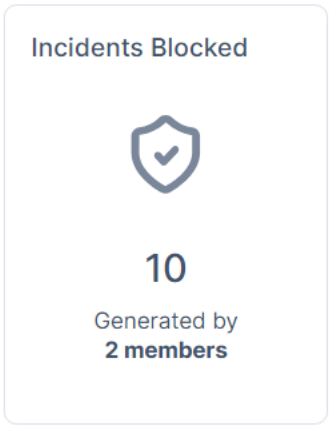
- *"Incidents Blocked" below*
- *"Malware Types" on the next page*
- *"Blocked Malware Per User" on the next page*
- *"All Malware Activities" on the next page*

To view the **Malware Protection** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Malware Protection**.

Insights

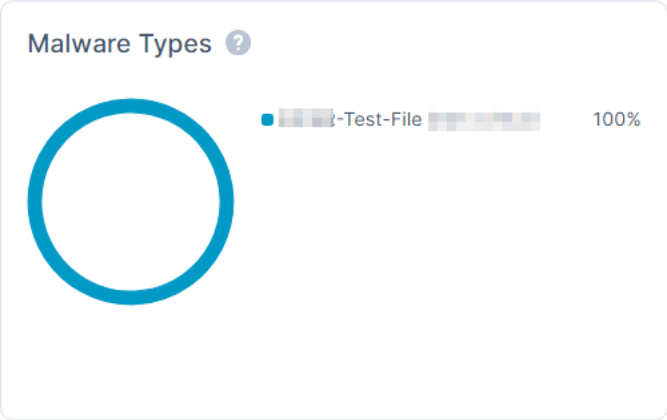
Insights shows the number of blocked malicious events, top malware types blocked, and top number of blocked events per user in the last 1 day, 7 days, and 30 days.

Incidents Blocked



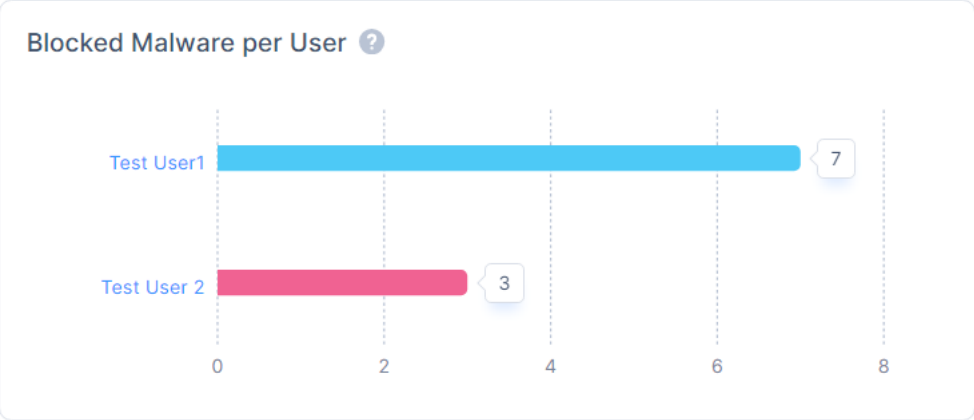
The **Incidents Blocked** widget shows the total number of blocked malicious files and URLs in the selected time frame.

Malware Types



The **Malware Types** widget shows the top categories of malware blocked in the selected time frame.

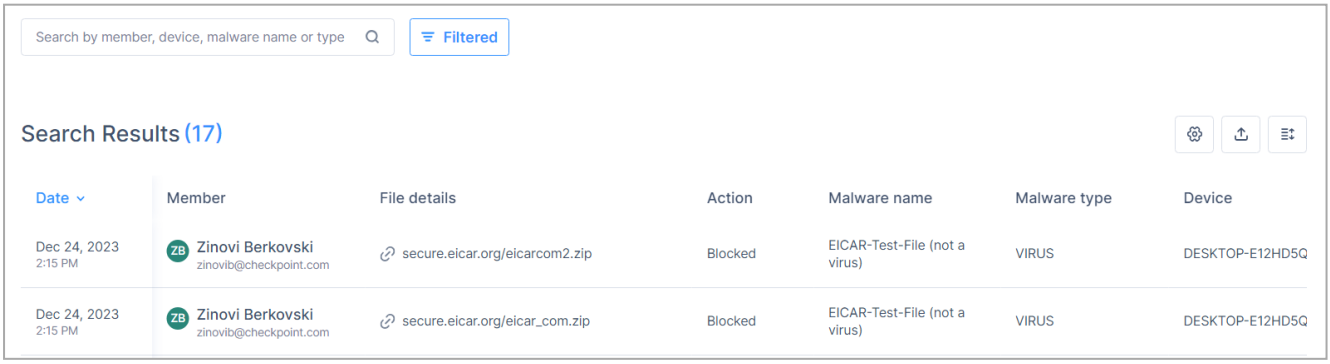
Blocked Malware Per User



The **Blocked Malware per User** widget shows the users that have the highest number of incidents for blocked malicious files and URL in the selected time frame.

All Malware Activities

All Malware Activities show a events of all the malware activities.



Column	Description
Date	Date and time of the activity.
Member	Member name.
File Details	File URL.
Action	Action taken by Check Point SASE: ■ Blocked ■ Scan skipped
Malware name	Malware name.
Malware type	Malware type.
Device	Device from where the malware was detected.

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

Note - You can export data of only 1000 activities at a time.

Admin Activity

The **Admin Activity** page allows to you to view these administrator activities:

- Account unblocked
- Active sessions report exported
- API key created / deleted
- **Application Access**
    - Application created / deleted
    - Application creation failed
    - Application changed / enabled / disabled
    - Policy changed / created / deleted
- **Billing**
    - Application created / deleted
    - Subscription activated / cancelled / reactivated
    - Subscription plan changed
    - Payment method updated
- Bypass rule added / updated deleted / priority updated
- **Configuration Profile**
    - Configuration profile added / updated / deleted
    - Trusted wired network added / deleted / disabled / enabled
    - Trusted WiFi network added / deleted
- **Firewall**
    - Firewall rule added / updated / deleted
    - Firewall rule updated / update failed
    - Firewall rule priority updated
- Gateway license purchased / removed
- **Group**

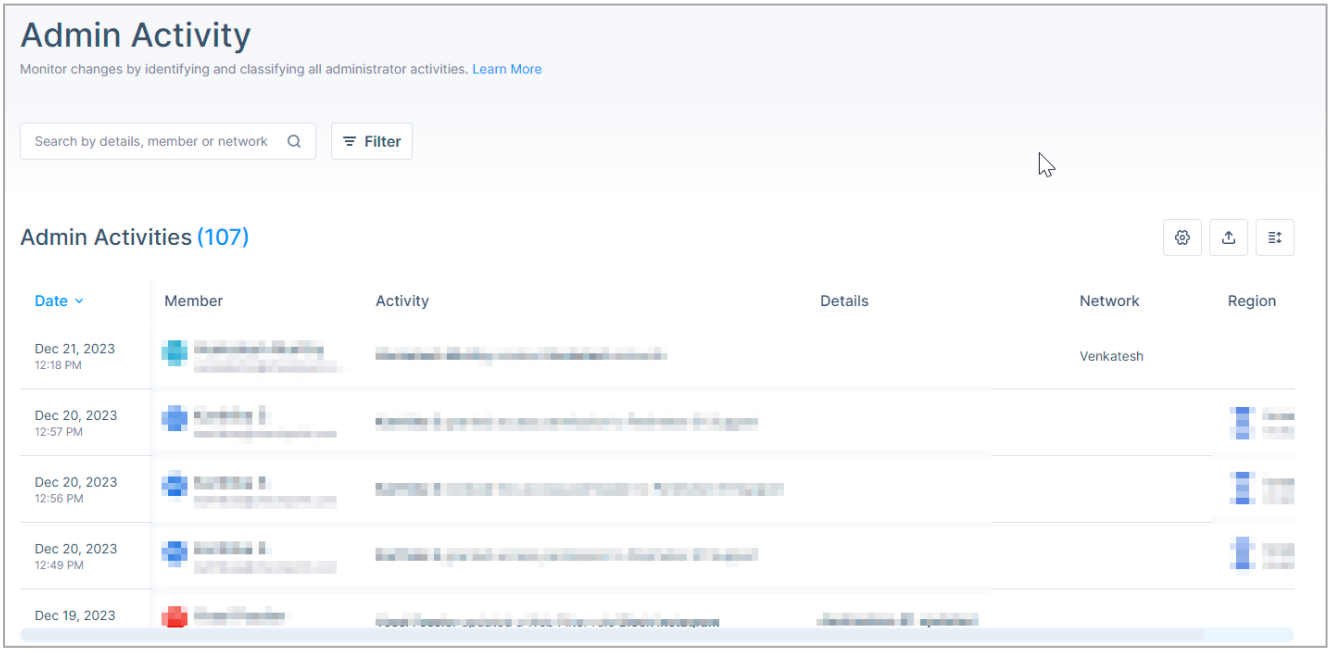
- Group created / updated / deleted
- Group member added / deleted
- Group network added / delete

- **Identity Provider**
  - Identity Provider created / updated / disabled / deleted
  - SCIM integration enabled / disabled
  - SCIM token created
- Integration created / enabled / disabled / deleted
- **Members**
  - Member created / invited / updated / deleted
  - Member Profile updated
  - Exported members list
- Member license purchased / removed
- **Network**
  - Network created / updated / deleted / creation failed
  - Gateway created / deleted / restarted / state changed
  - Custom gateway created
  - Region created / deleted
  - Tunnel created / updated / deleted
  - DNS filtering updated / deleted
  - Private DNS updated / enabled / disabled
  - Regional private DNS updated / enabled / disabled
  - Custom network created / creation failed
  - Custom region created
  - Network Split Tunneling
  - Network groups changed
- **Objects**

- Application created / deleted
- Address updated / deleted / added
- Service added / updated / deleted
- Custom URL added / updated deleted

- Password reset / changed
- **Posture Check**
  - Posture profile created / updated / deleted
  - Posture profile check failed
- Role assigned to a member
- Support access granted / revoked
- Web activity report exported
- **Web Filter Rules**
  - Member license purchased / removed
  - Web filter rule added / updated / deleted
  - Web filter rules policy updated / priority changed / status changed

To view the **Admin Activity** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Admin Activity**.



Column	Description
Date	Date and time of the activity.
Member	Member name.
Activity	Activity description.
Details	Change in the defined values for the activity.
Network	Connected network name.
Region	Region and gateway IP address of the connected session.

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

Note - You can export data of only 1000 activities at a time.

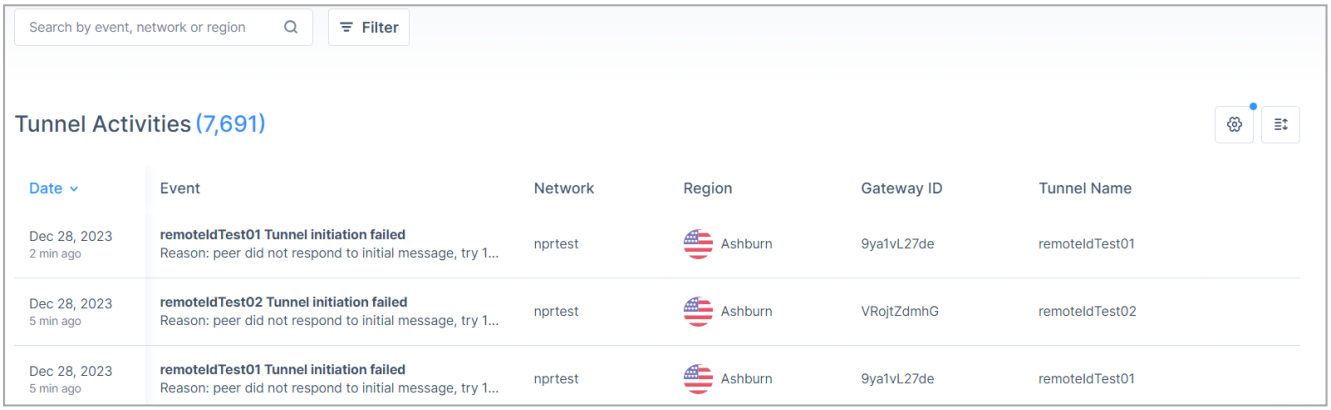
Tunnels Status

Note - This page will be deprecated. Upon deprecation, you will be able to find all the new Tunnel related events from the *"Operational Events" on page 887* page.

The **Tunnels Status** page allows you to monitor the health of tunnels.

- Tunnel up / down
- Tunnel initialization failed

To view the **Tunnels Status** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Tunnels Status**.



Column	Description
Date	Date and time of the activity.
Event	Event type and the reason.
Network	Associated network.
Region	Region of the network.
Gateway ID	SASE gateway ID.
Tunnel Name	Tunnel name.
Tunnel Peer IP	Tunnel peer IP address.
Tunnel Source IP	Tunnel source IP address.
Tunnel Type	Tunnel type.

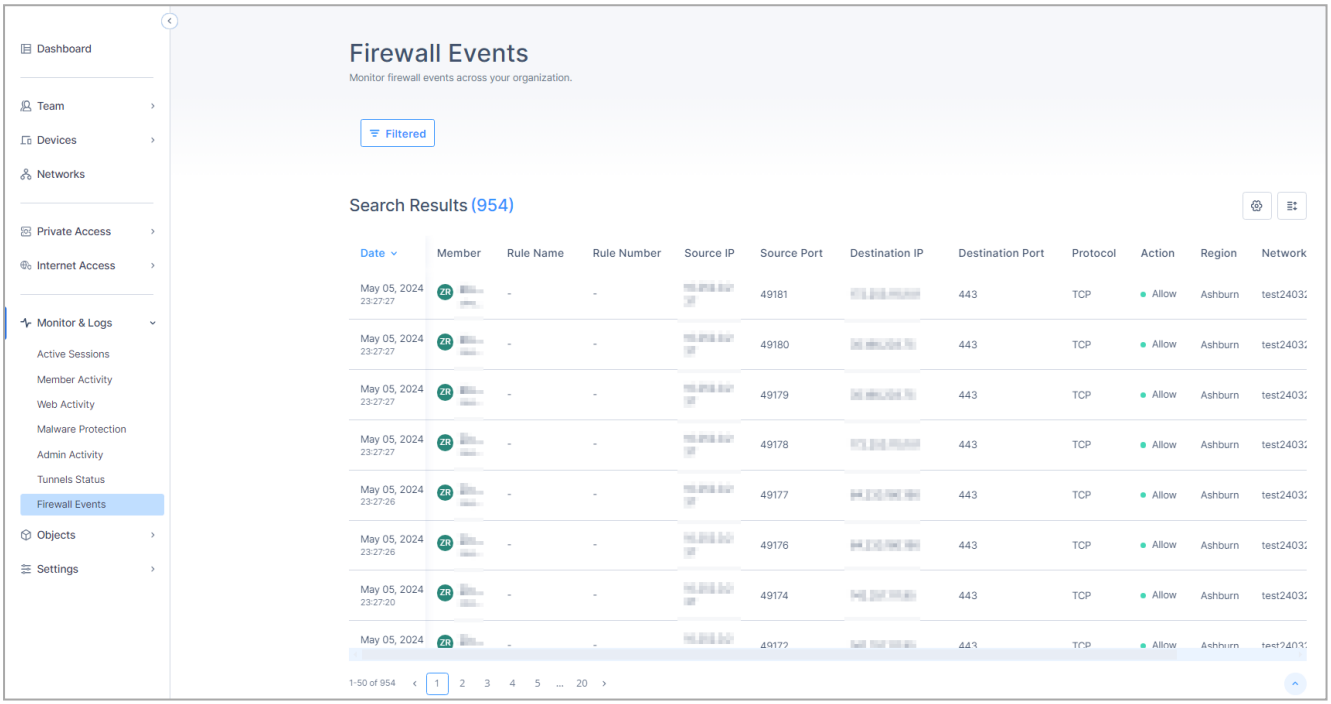
To select the columns required in the table, click the ⚙ icon and select the columns.

Firewall Events

Note - This page will be deprecated. Upon deprecation, you will be able to find all the new Firewall related events from the Security Events page.

The **Firewall Events** page allows you to monitor the firewall events.

To view the **Firewall Events** page, access the SASE Administrator Portal and click **Monitor & Logs** > **Firewall Events**.



Column	Description
Date	Date and time of the activity.
Member	Member name.
Rule Name	Rule name configured in the *"Firewall" on page 737*.
Rule Number	Rule number configured in the *"Firewall" on page 737*.
Source IP	IP address of the source.
Source Port	Port number on the source IP.
Destination IP	IP address of the destination.

Column	Description
Destination Port	Port number on the destination IP.
Protocol	Communication protocol used for the network activity, for example, TCP, UDP, or ICMP.
Action	Action taken on the event: ■ Allow ■ Deny
Region	Region of the network.
Network	Associated network.

To select the columns required in the table, click the icon and select the columns.

Objects

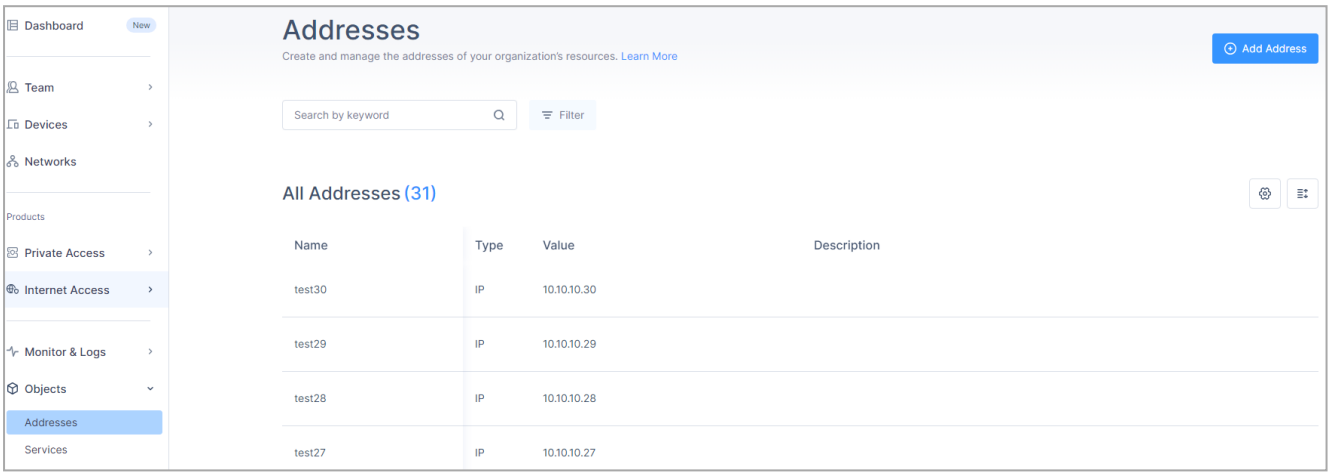
Objects allow you create:

- *"Addresses" on page 911*
- *"Services" on page 916*
- *"Custom URLs" on page 920*

Addresses

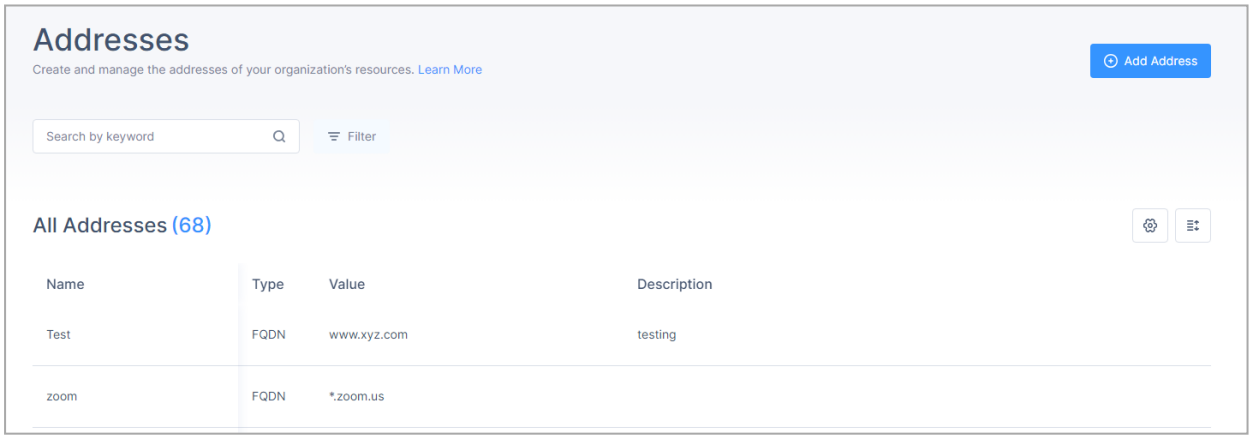
The **Address** object allows you manage the IP addresses and subnets that you use to define your network, firewall rules, application access rules and access policies.

To view the **Address** object, access the Check Point SASE Administrator Portal and click **Objects**.



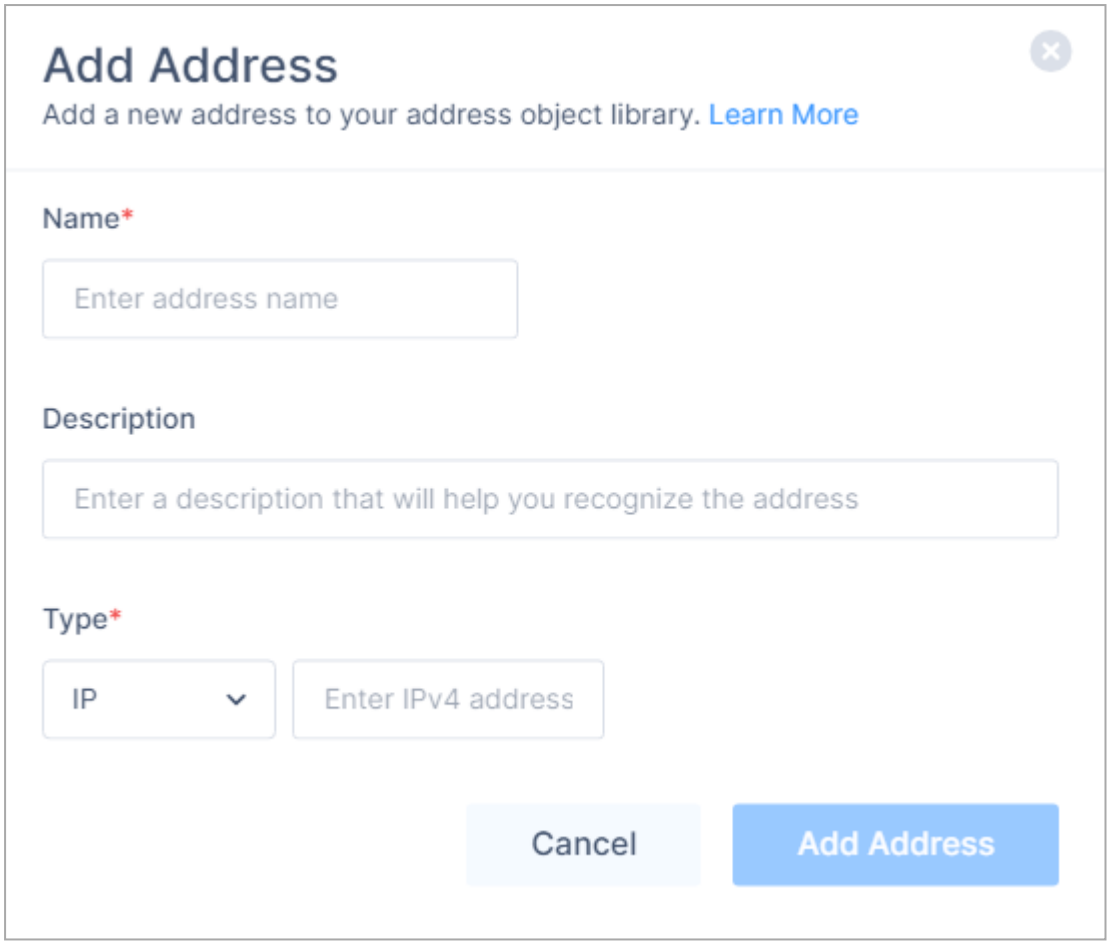
Creating an Address Object

1. Access the Check Point SASE Administrator Portal and click **Objects** > **Addresses**.



2. Click **Add Address**.

   The **Add Address** window appears.



3. Enter these:
   a. **Name** - Name of the address object.
   b. (Optional) **Description**
   c. **Type** - Select the address type and enter the address value.
      - IP
      - Subnet
      - List
      - FQDN
4. Click **Add Address**.

   The system creates the address and displays it in the **Addresses** page.

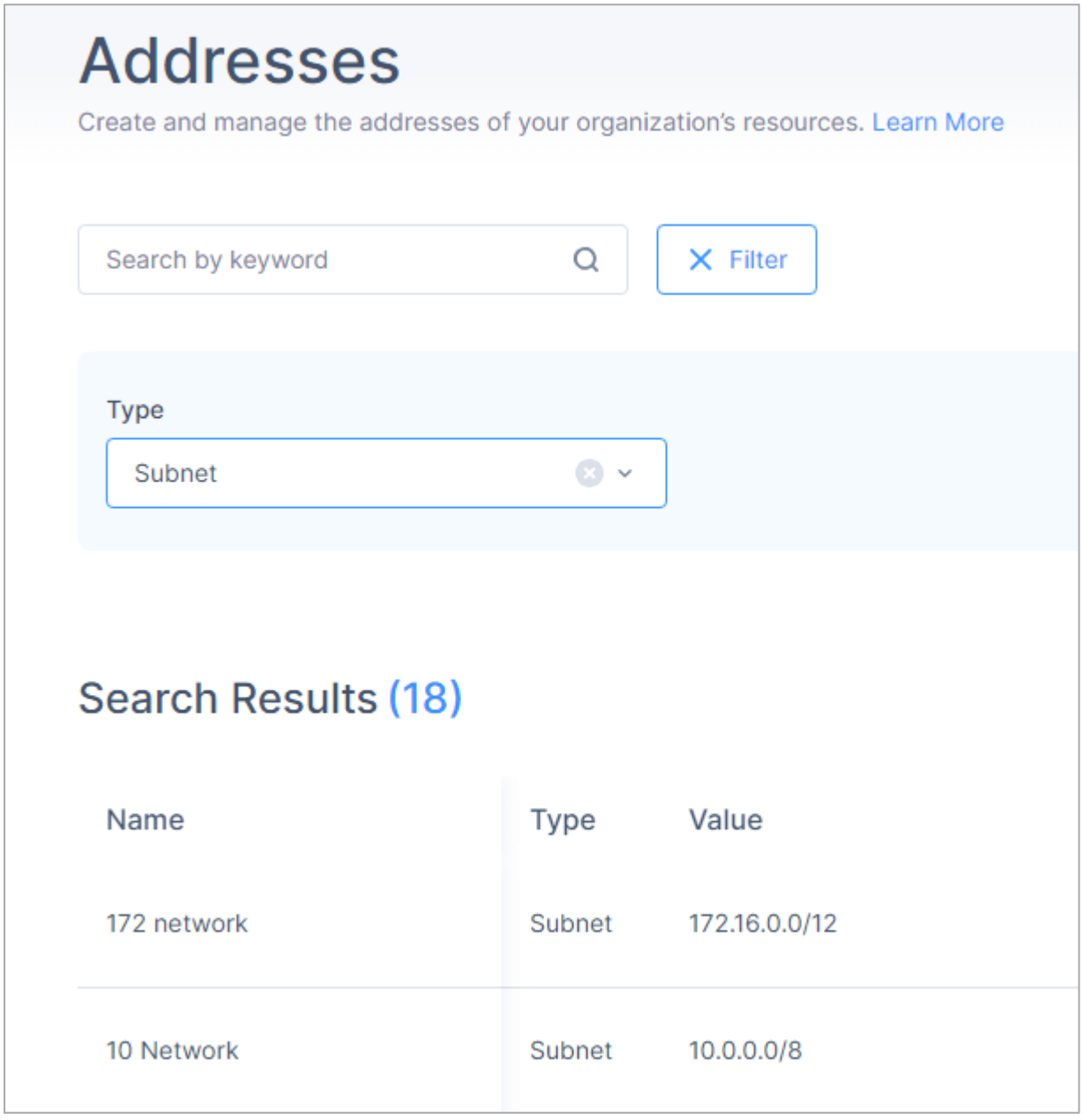
Managing Addresses

1. Access the Check Point SASE Administrator Portal and click **Objects** > **Addresses**.
2. Hover over the address and do one of these:

- To edit, click .

  Make the required changes and click **Apply**.
- To delete, click and then click **Delete**.
- To duplicate, click .

3. To search for an address, enter the address name in the **Search** box.
4. To filter the addresses by their **Type**, click **Filter** and select the address **Type**.



5. To edit the **Addresses** table settings, click .
6. To edit the number of addresses displayed in the table, click .

FQDN-based Firewall Objects

FQDN-based firewall objects allows you to use FQDN as objects in firewall rules. You can use FQND object for services with dynamic IP address and use DNS to eliminate the requirement to manually update the IP address of services.

FQDN Wildcards

You can use the FQDN wildcard support to specify sub-domains. For example, **.example.com* includes all sub-domains, such as *sales.example.com*, *support.example.com* and so on.

Multi-Level Sub-domains

FQDN objects support multi-level subdomains, up to 5 levels.

For example, *one.two.three.four.five.example.com*

Important Considerations

- The firewall supports a total of 100 FQDN objects.

  Examples:

  - **One** FQDN object per rule, across **100x rules**, or:
  - **100x** FQDN objects contained in a **single rule**.
- FQDN objects can contain a maximum of 1000 domains per account.

  Examples:

  - **Ten** FQDN objects containing **100x domains**, or:
  - **100x** FQDN objects containing **ten domains** each.

Limitations

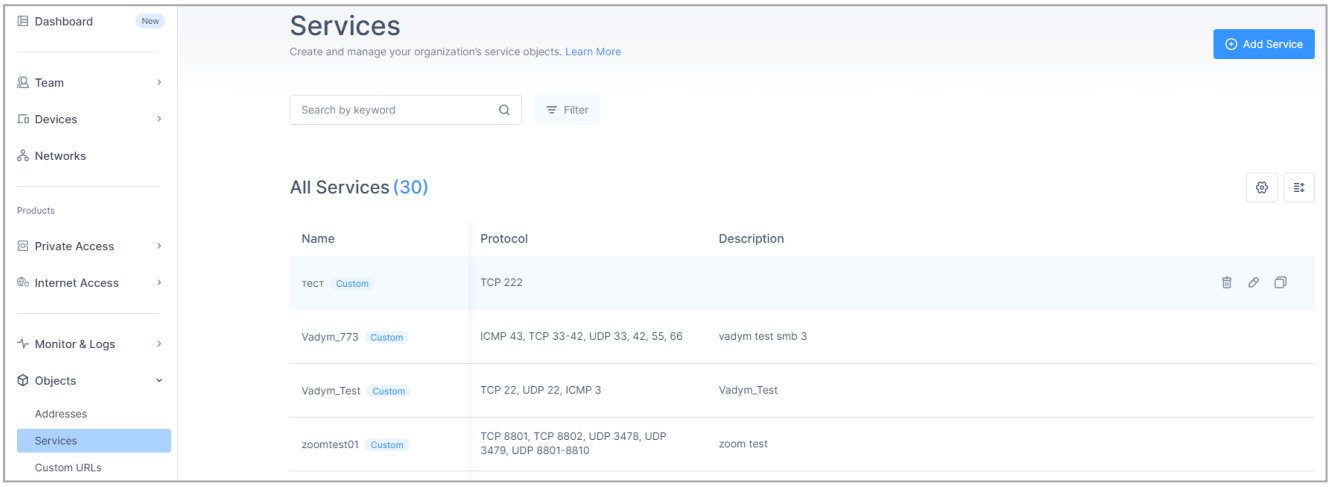
- FQDN firewall rules may be bypassed by using an IP.
- CDN is not permitted, only FQDN.
- If you have two or more FQDNs sharing the same IP, both are affected by the Firewall rule. For example, if you block one FQDN, another resource sharing the same IP is also be blocked.
- Limited compatibility with services supported by multiple FQDN (for example, websites).
- No compatibility with DNS load balancers as they return different IPs for each query.
- The browser and local DNS cache take priority over FQDN Firewall rules.

- No compatibility with third-party DNS services, for example, DoH (The admin must enforce user VPN interface DNS).

Services

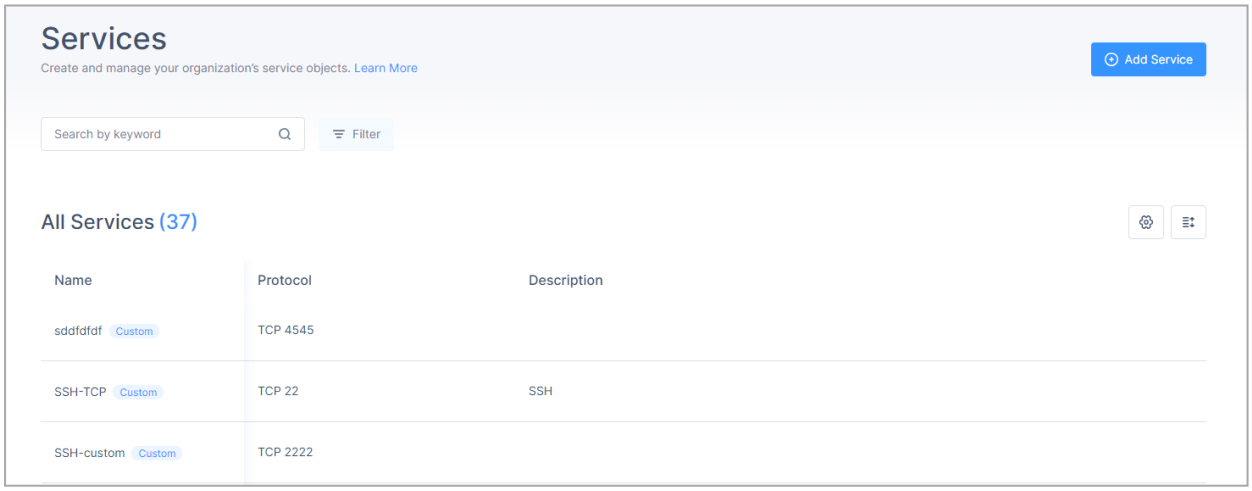
The **Services** object allows you to define the applications that you want to allow access to. These services belong to the Layer 4 of the OSI model with protocol and port combinations. For example, protocol TCP port 80 or protocol UDP port 53.

To view the **Service** object, access the Check Point SASE Administrator Portal and click **Objects**.



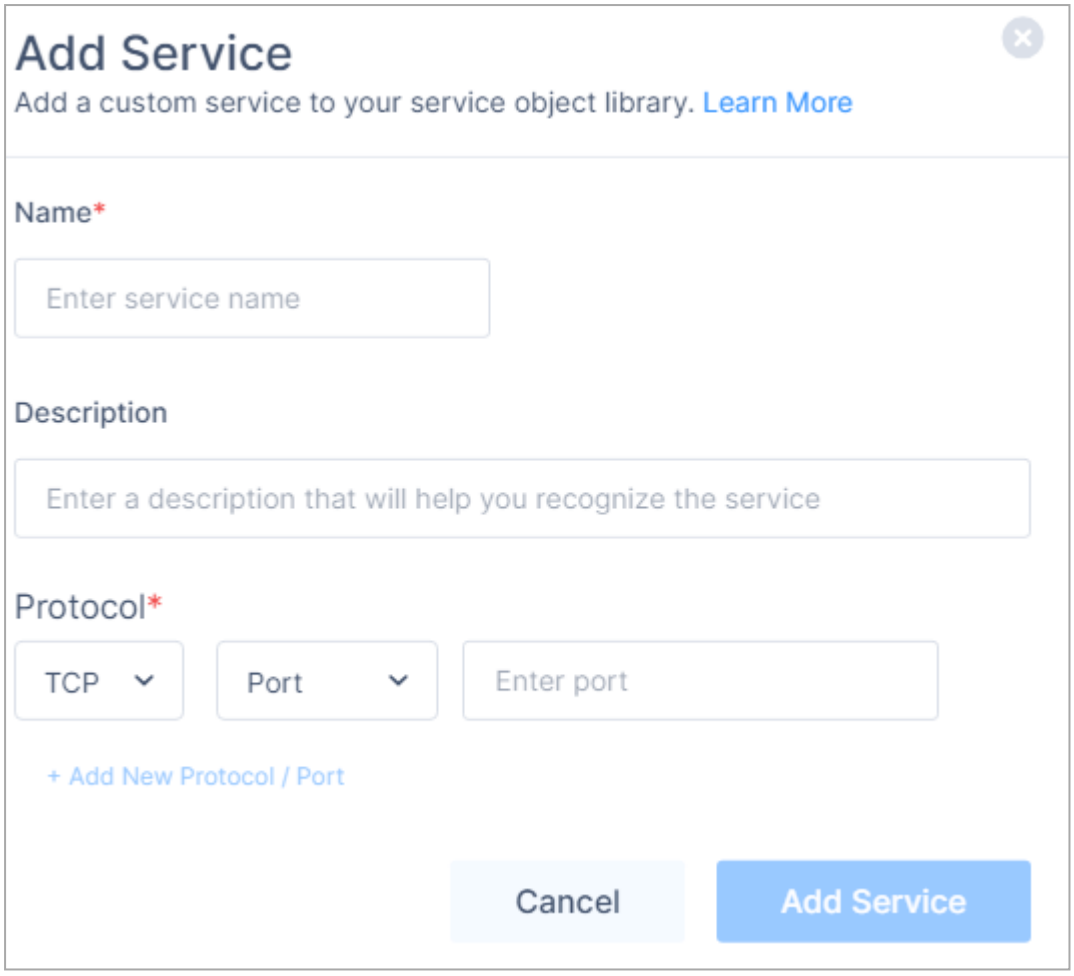
Creating a Service Object

1. Access the Check Point SASE Administrator Portal and click **Objects** > **Services**.



2. Click **Add Service**.

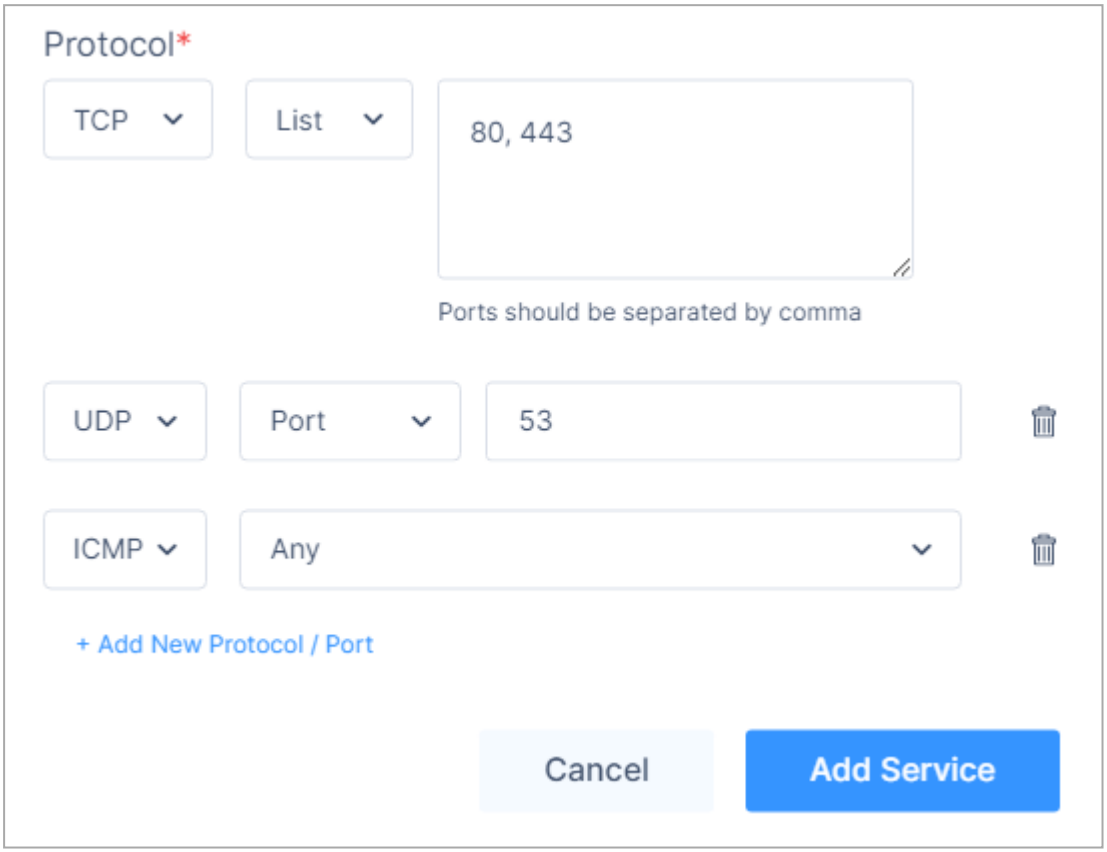
   The **Add Service** window appears.



3. In the **Name** field, enter the name of the service object.
4. (Optional) **Description**
5. In the **Protocol** section:

a. Select the protocol type:

- TCP
- UDP
- IDMP



b. Select how you want to define the protocol:

- Range - A range of port numbers.
- Port - A single port number.
- List - A list of port numbers.

c. Enter the protocol values.

6. To add a new protocol/port pair to the service, click **Add New Protocol / Port**.

   You can combine multiple protocol/port pairs in a single service.

7. Click **Add Service**.

   The system creates the service and displays it in the **Services** page.

Managing Services

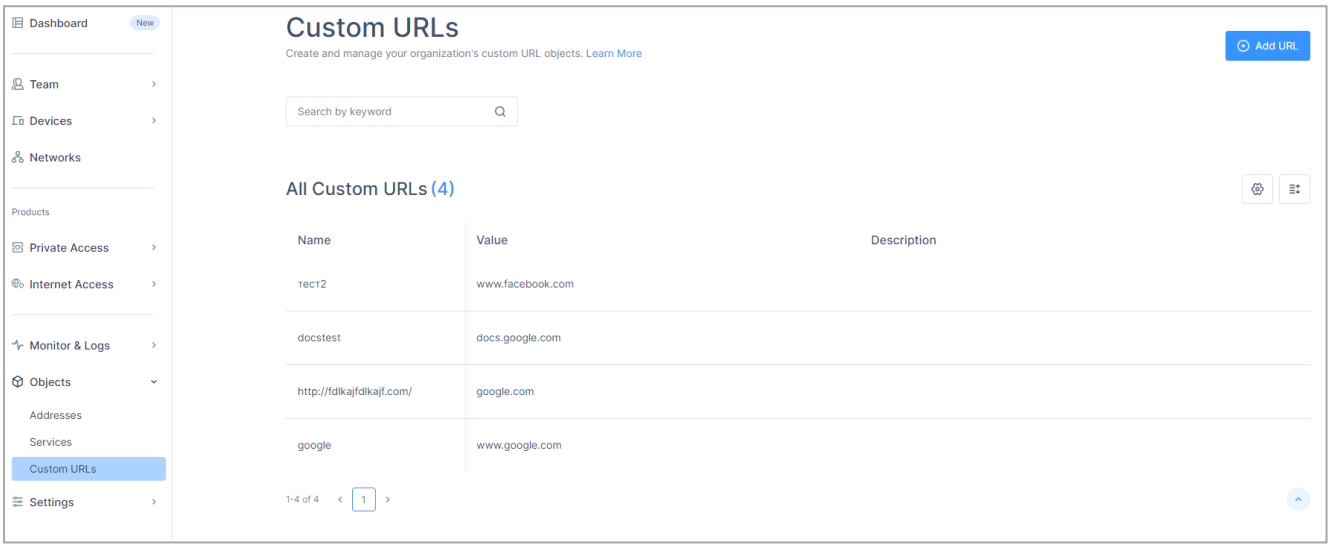
1. Access the Check Point SASE Administrator Portal and click **Objects** > **Services**.
2. Hover over the service and do one of these:
   - To edit, click .

     Make the required changes and click **Apply**.
   - To delete, click and then click **Delete**.
   - To duplicate, click .
3. To search for a service, enter the service name in the **Search** box.
4. To filter the services by their **Protocol**, click **Filter** and select the protocol.
5. To edit the **Services** table settings, click .
6. To edit the number of services displayed in the table, click .

Custom URLs

The **Custom URL** object allows you to specify a URL's specific path in *"Access Policy" on page 778*.

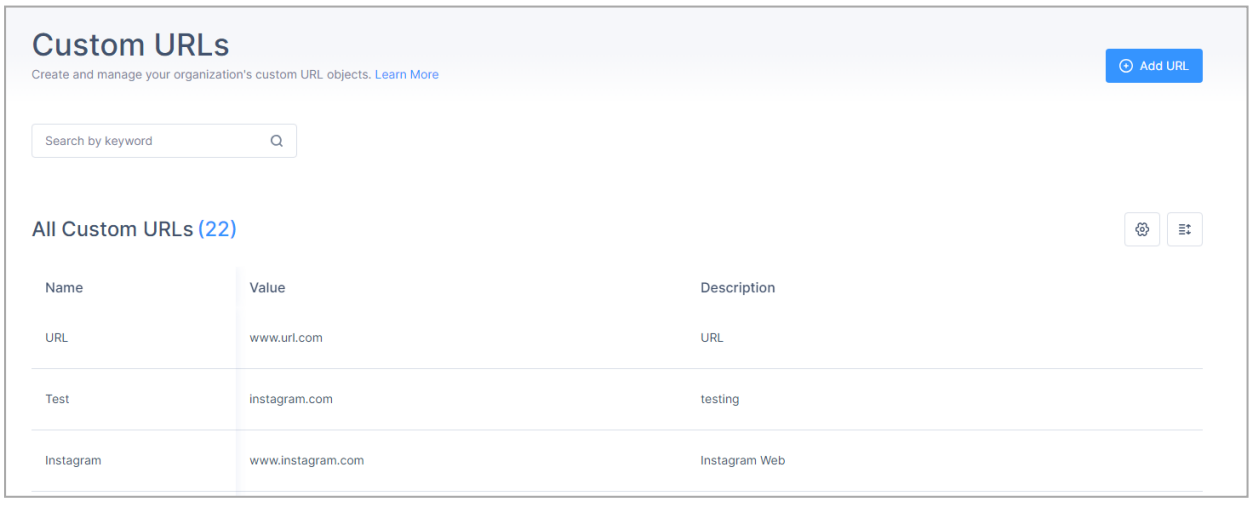
To view the **Custom URL** object, access the Check Point SASE Administrator Portal and click **Objects**.



Creating a Custom URL Object

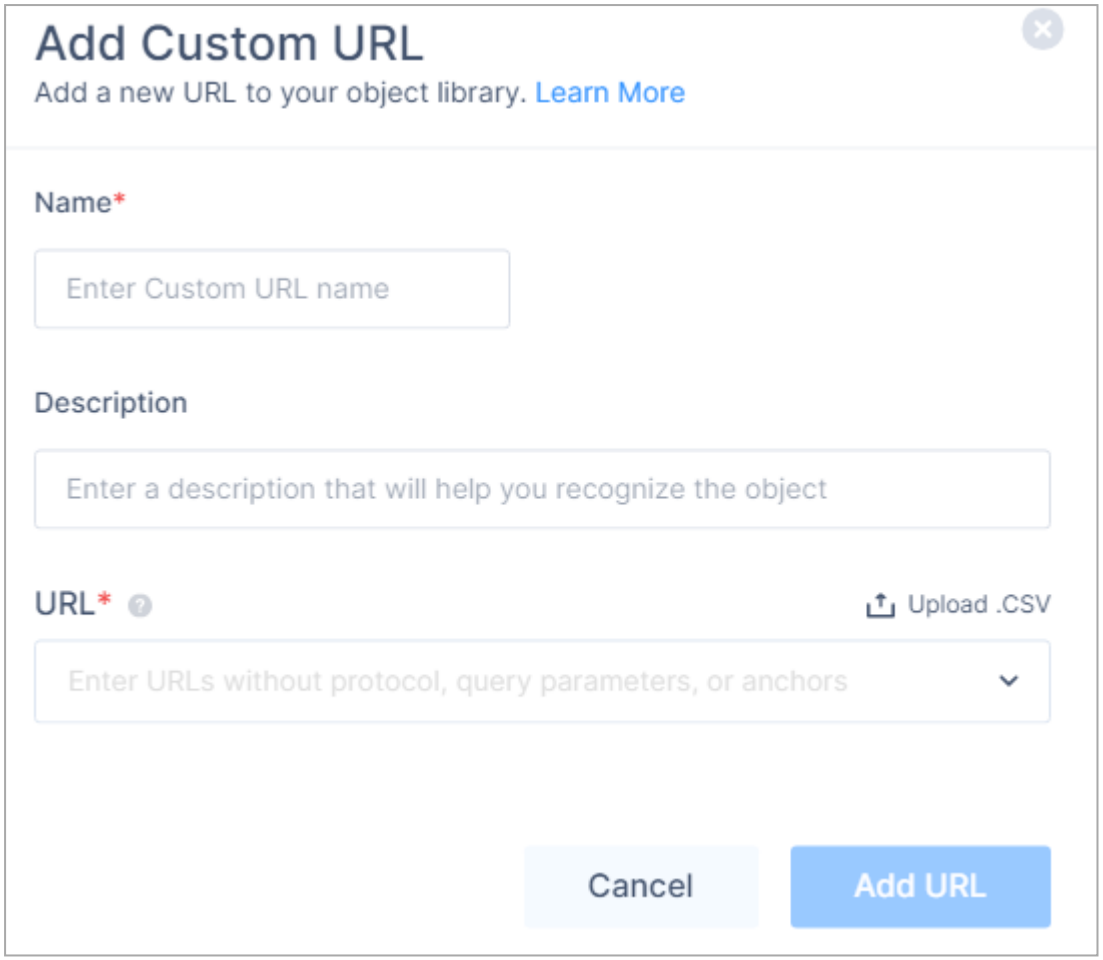
1. Access the Check Point SASE Administrator Portal and click **Objects** > **Custom URLs**.

   The **Custom URLs** page appears.



2. Click **Add URL**.

   The **Add Custom URL** window appears.



3. Enter these:
   a. **Name** - Name of the custom URL.
   b. (Optional) **Description**
4. In the **URL** field, enter the list of URLs or upload a .CSV file with the list of URLs.

   Notes:
   - Do not add any protocols (http:// , https://) , query parameters (?) or anchors (#). If the URL includes a **www** prefix, include it as part of the domain. Wildcard (*) is supported and can only be used at the beginning of the domain, for example, **.example.com*.
   - When uploading a CSV file with custom URLs, make sure the file does not include a header or subject line. Each row should contain only a single URL.
5. Click **Add URL**.

   The system creates the URL and displays it in the **Custom URLs** page.

Managing Custom URLs

1. Access the Check Point SASE Administrator Portal and click **Objects** > **Custom URLs**.
2. Hover over the URL and do one of these:
   - To edit, click .

     Make the required changes and click **Apply**.
   - To delete, click and then click **Delete**.

     Note - The delete and edit options are disabled if the custom URL is used in an access policy.
     Before you delete the URL, remove its references from the *"Access Policy" on page 778* .
   - To duplicate, click .
3. To search for a URL, enter the URL name in the **Search** box.
4. To edit the **Custom URLs** table settings, click .
5. To edit the number of URLs displayed in the table, click .

Updatable Objects

Updatable Objects are predefined destination objects that Check Point maintains and updates automatically. They represent services or groups of destinations whose IP addresses, domains, or endpoints change frequently.

Use Updatable Objects to apply security and routing policies without manually maintaining destination details.

Note - Updatable Objects in Access Policy and Bypass Rules are available in Early Availability (EA) only. To enable, contact Check Point Support.

How Updatable Objects Work

Each Updatable Object represents a specific service or category of destinations. Check Point automatically updates the object to reflect changes published by the service provider.

When a policy references an Updatable Object, the policy applies to the current list of destinations included in that object.

Note - Updatable Objects can also represent geographic locations, such as a continent or a country.

Where Updatable Objects Are Supported

Updatable Objects are supported in these Check Point SASE features:

- *"Split Tunneling" on page 226*

  Note - These services are not available as Updatable Objects for Split Tunneling:
  - Microsoft Azure services
  - Amazon Web Services (AWS)
  - Geolocation-based objects

- *"Access Policy" on page 778*
- *"Creating a Bypass Rule" on page 790*

Supported Vendors

For a complete list of supported vendors and services included in Updatable Objects, see Updatable Objects.

Settings

From the **Settings** tab you can configure:

- *"Integrations" on page 925*
- *"Identity Providers" on page 950*
- *"Two-Factor Authentication" on page 1129*
- *"Certificate Manager" on page 1133*
- *"Support Access" on page 1138*

Integrations

Security Information and Event Management (SIEM) Integrations

Check Point SASE allows you to export logs to these third-party SIEM applications:

- *"Splunk Cloud" below*
- *"Microsoft Sentinel" on page 930*
- *"Amazon S3" on page 934*

Professional Services Automation (PSA) Integrations

Integrate Perimeter 81 with ConnectWise Manage to automate the billing process.

- *"ConnectWise PSA" on page 943*

Note - This is available only for the accounts in the Perimeter 81 workspace.

Splunk Cloud

Splunk Cloud allows you to search, analyze and view data collated from various systems in your IT infrastructure.

Integrating Splunk Cloud

Step 1 - Setting Up the HTTP Event Collector

The HTTP Event Collector (HEC) allows you send data and application events to a Splunk deployment over HTTP and HTTPS protocols. You can use HEC to generate a token and use it to configure a log library with data in a specific format. This eliminates the requirement for a Splunk forwarder when you send application events.

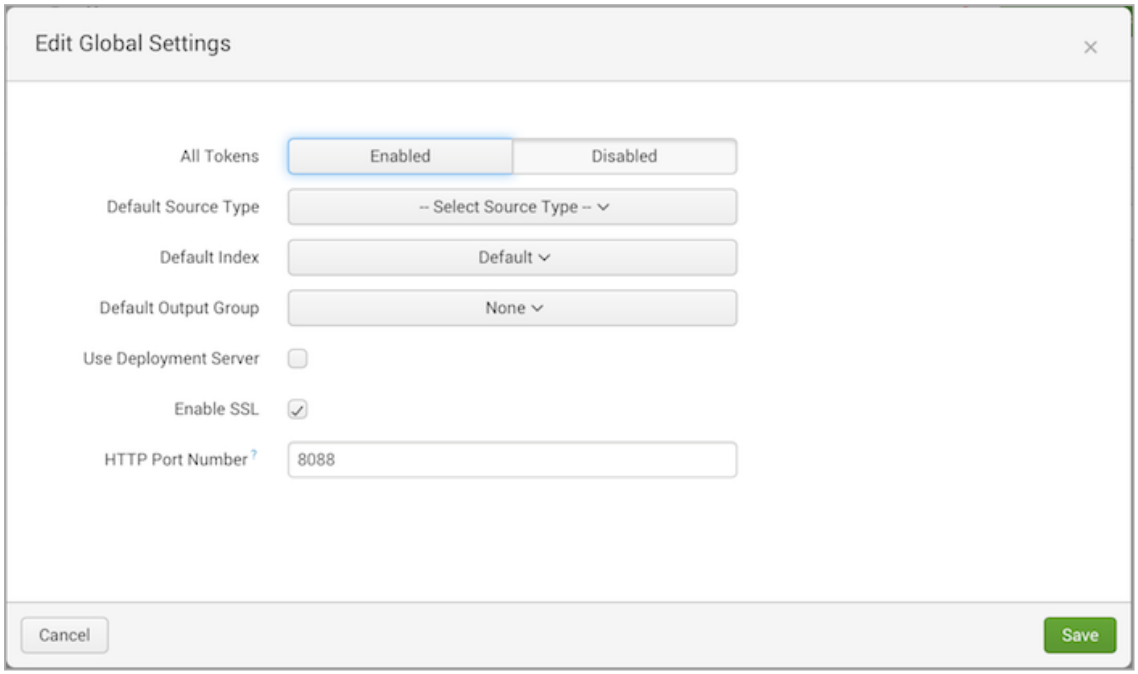
Step 2 - Enabling an HTTP Event Collector

When you enable HEC, applications use the HEC tokens to send data to HEC, eliminating the requirement for Splunk credentials in your application or supported files.

Note - If you have managed Splunk, contact Splunk customer support for assistance.

To enable an HTTP Event Collector:

1. Log in to the Splunk web portal.
2. Click **Settings** > **Data Inputs**.
3. Click **HTTP Event Collector**.
4. Click **Global Settings**.



5. In the **All Tokens** field, select **Enabled**.
6. To enable communication over HTTPs, select the **Enable SSL**checkbox.

   Note - It is enabled by default. You can disable it only through Splunk Enterprise.

7. Click **Save**.

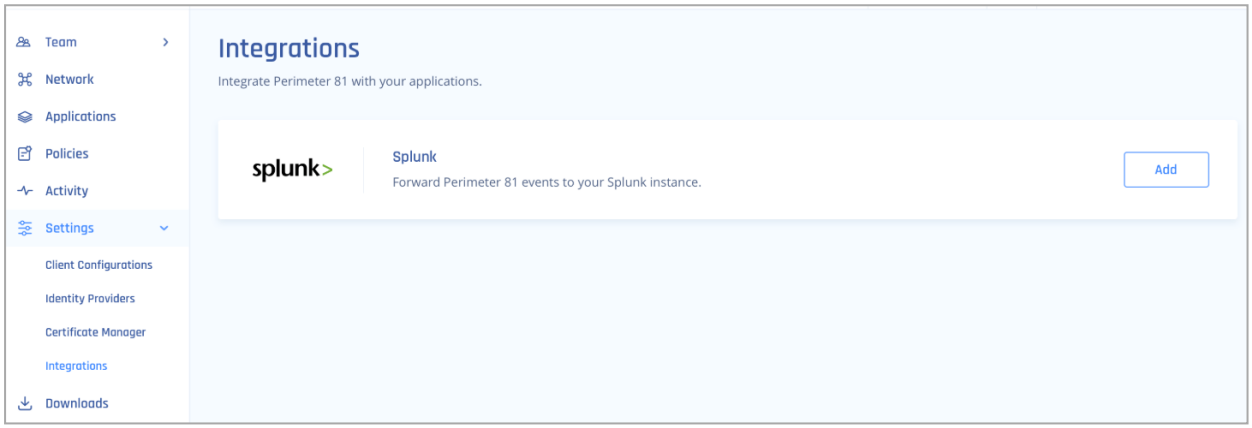
Step 3 - Creating an Event Collector Token

1. Log in to the Splunk web portal.
2. Go to **Settings** > **Add Data**.
3. Click **Monitor**.
4. Click **HTTP Event Collector**.
5. In the **Name** field, enter a name for the token.
6. Make sure indexer acknowledgment is disabled for this token.
7. Click **Next**.

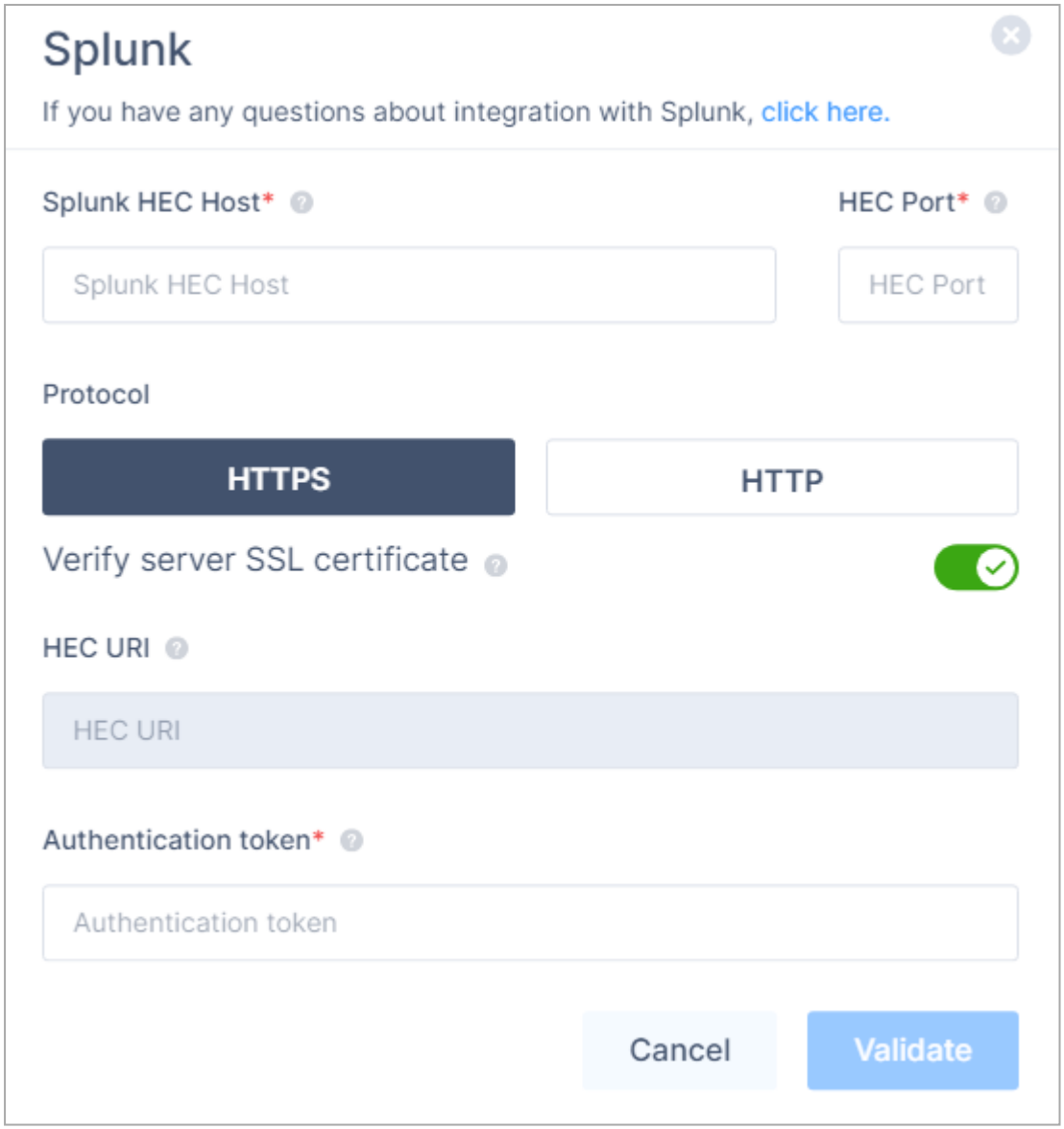
8. Click **Review**.
9. Verify the settings.
10. Click **Submit**.

Configuring the Splunk Integration in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Splunk** row, click **Add**.



3. Enter these:



Item	Description
Splunk HEC Host	Enter an appropriate value according to your Splunk tier. Replace {hostname} with your Splunk server hostname. ■ Splunk Cloud (paid): inputs-<host> ■ Splunk Cloud (free-trial): <host> ORinputs.<host>
HEC Port	■ Splunk Cloud free trial: 8088 ■ Splunk Cloud paid: 443
Protocol	■ Splunk Cloud free trial: HTTP ■ Splunk Cloud paid: HTTPS

Item	Description
(For HTTPS only) **Verify server SSL certificate**:	■ If you are using a self-signed certificate disable SSL verification. ■ If you are using a CA-signed certificate make sure to enable it.
HEC URI	Value is automatically populated.
Authentication token	Enter the token generated in the Splunk web portal.

4. Click **Validate**.

Troubleshooting

This table shows the status codes for all HTTP Event Collector endpoints.

HTTP status code ID	HTTP status code	Status message	Action required
200	OK	Success	None
403	Forbidden	Token disabled	Enable token at Splunk Web.
401	Unauthorized	Invalid authorization	Make sure you entered a valid token.
403	Forbidden	Invalid token	Make sure you entered a valid token.
500	Internal Error	Internal server error	Contact *Check Point Support*.
503	Service Unavailable	Server is busy	There are too many requests pending in the Splunk server queue. Try again later.
400	Bad Request	Data channel is missing	Edit the token at the Splunk web portal and make sure the Indexer Acknowledgement is disabled.
400	Bad Request	Error in handling indexed fields	Contact *Check Point Support* .

Microsoft Sentinel

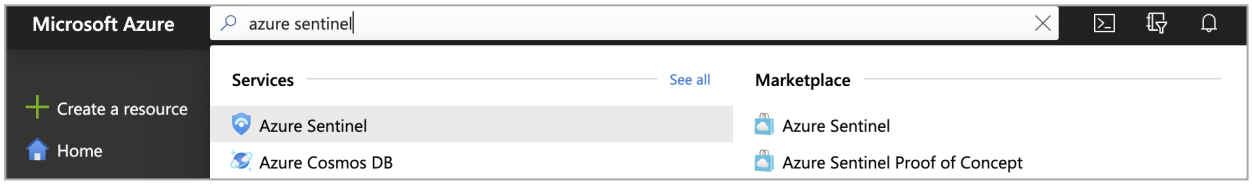
Microsoft Sentinel (formerly Azure Sentinel) is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. It delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Configuring the Integration in the Microsoft Azure Portal

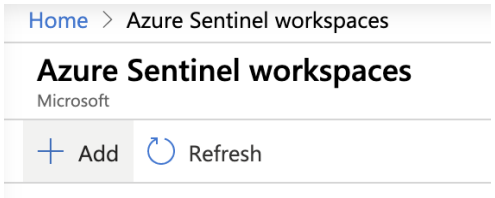
Step 1 - Setting up a Log Analytics Workspace

Note - If you are using an existing log analytics workspace, skip this section.

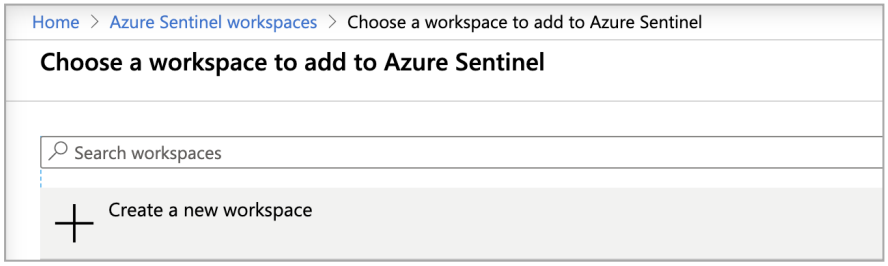
1. Log in to the Microsoft Azure portal.
2. Search for **Azure Sentinel** and select it.



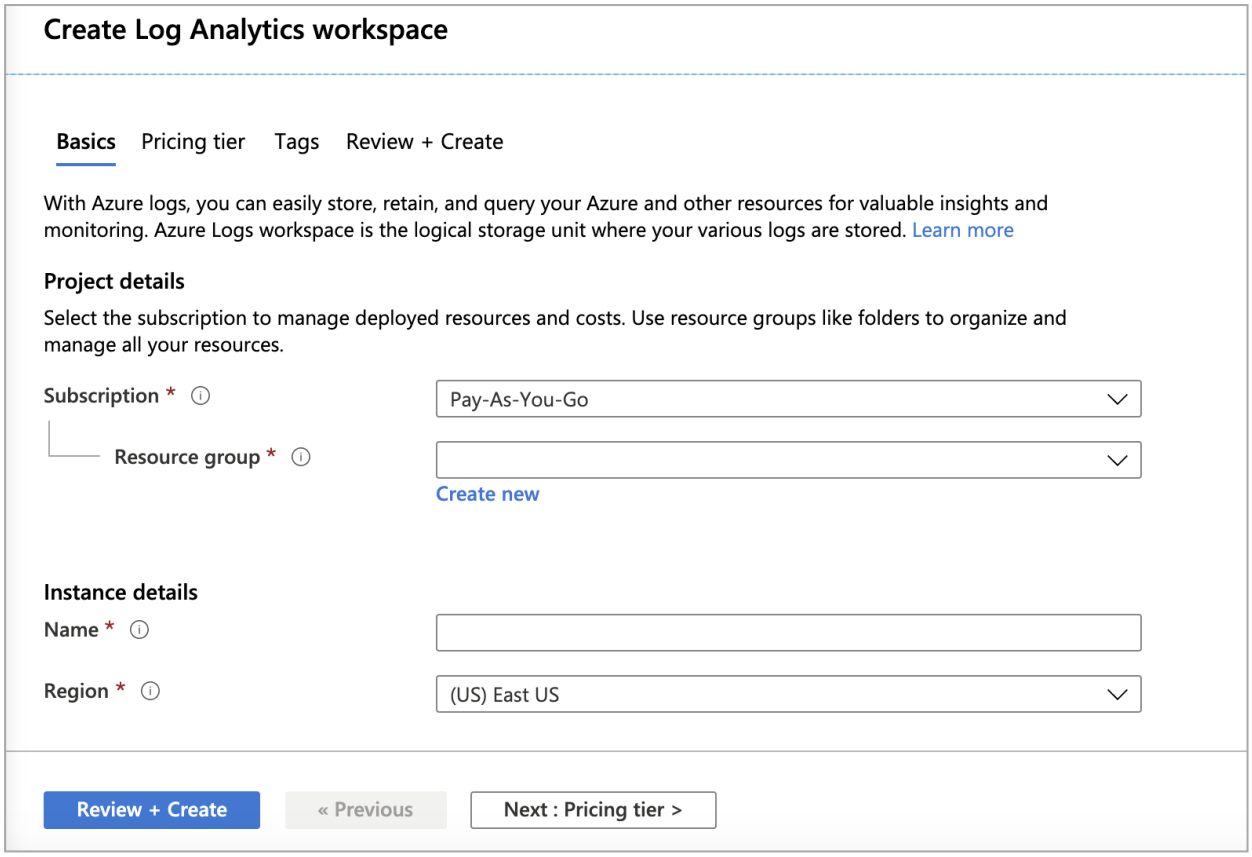
3. Click **Add**.



4. Click **Create a new workspace**.



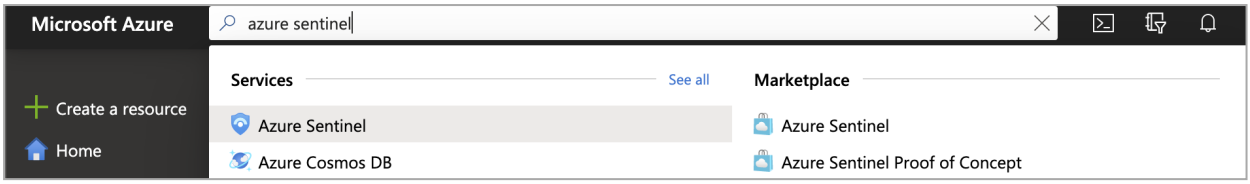
The **Create Log Analytics workspace** window appears.



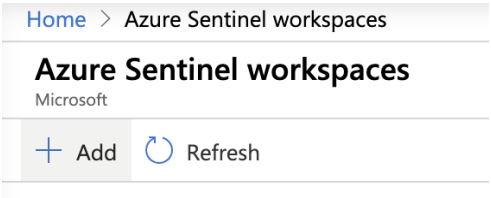
5. Enter these:
   a. **Subscription** - A subscription according to your business needs.
      - **Resource group** - Associate the log analytics workspace with the appropriate business unit.
   b. **Name** - Name of the workspace. It must contain minimum four characters (alphabets, numerals and hyphen) up to 63. Make sure hyphen is not the first or last character.
   c. **Region**: Physical location of the server generating the event collector. Select according to pricing and business requirement.
   d. **(Optional)** Review the pricing tiers and set appropriate tags for the workspace.
6. Click **Review + Create**.

Step 2 - Linking the Log Analytics Workspace to Microsoft Sentinel

1. Log in to the Microsoft Azure portal.
2. Search for **Azure Sentinel** and select it.



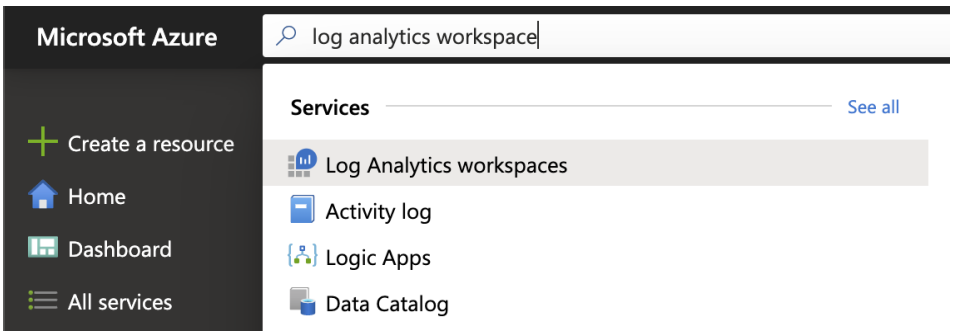
3. Click **Add**.



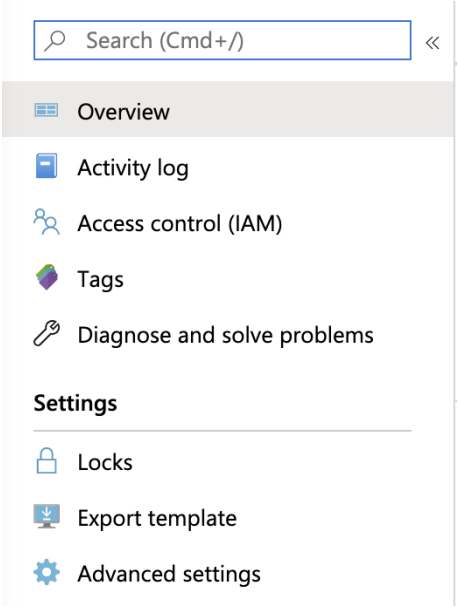
4. Select the Log Analytics Workspace that you have created or an existing one that you want to utilize.

Step 3 - Finding your Log Analytics Workspace ID and Primary Key

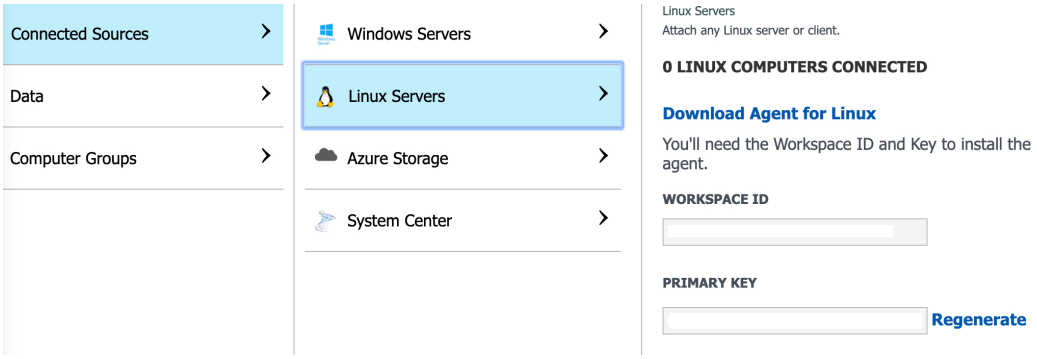
1. Log in to the Microsoft Azure portal.
2. Search for **Log Analytics Workspace** and select it.



3. Select the workspace you connected to Microsoft Sentinel.
4. In the **Settings** section, click **Advanced settings**.

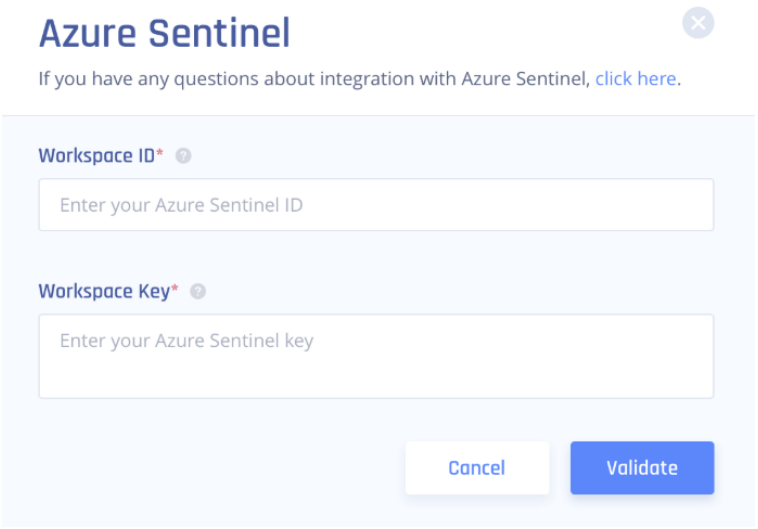


5. Click **Connected Sources** > **Linux Servers** and then copy the **Workspace ID** and the **Primary Key**.



Configuring the Microsoft Sentinel Integration in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Microsoft Sentinel** row, click **Add**.
3. In the **Workspace ID** field, enter the Log Analytics **Workspace ID** from the above section.
4. In the **Workspace Key** field, enter the Log Analytics **Primary Key** from the above section.



5. Click **Validate**.

Troubleshooting

Status Message	Action Required
Success	None.
SENTINEL_INACTIVE_CUSTOMER	The workspace has been deactivated.
SENTINEL_INVALID_CUSTOMER_ID	Make sure you have entered the correct customer ID.
SENTINEL_INVALID_AUTHORIZATION	The service failed to authenticate the request. Verify that the workspace ID and connection key are valid.

Amazon S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Prerequisites

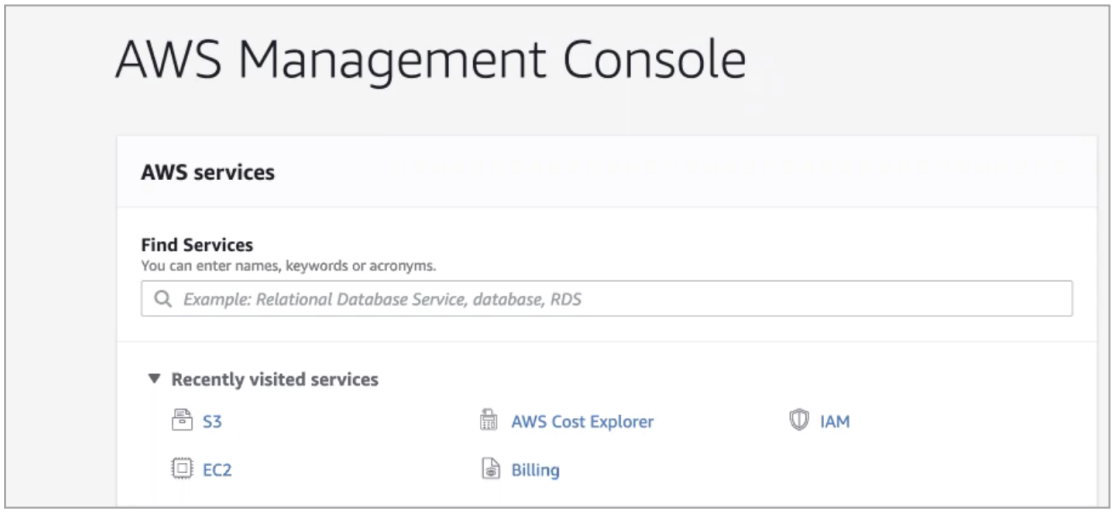
- Ensure that the IAM user has the necessary permissions to access the S3 bucket.
- Check Point SASE uses these IP addresses to deliver SIEM logs:

- US tenant:
  - 44.199.0.186
  - 44.198.227.127
  - 50.19.134.176
  - 23.20.83.77
  - 54.85.165.134
- EU tenant
  - 52.50.186.78
  - 79.125.50.175
  - 34.246.127.40

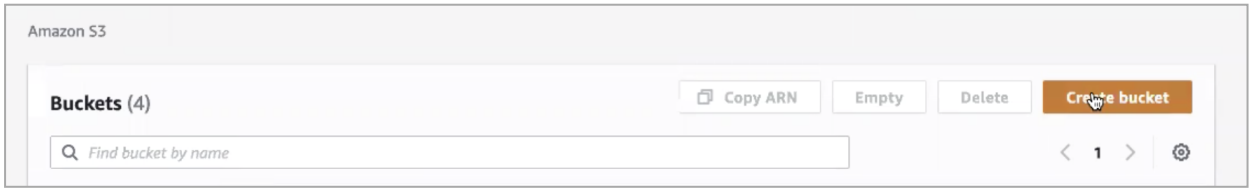
Configuring the Integration in the AWS Management Console

Step 1 - Creating a New Bucket

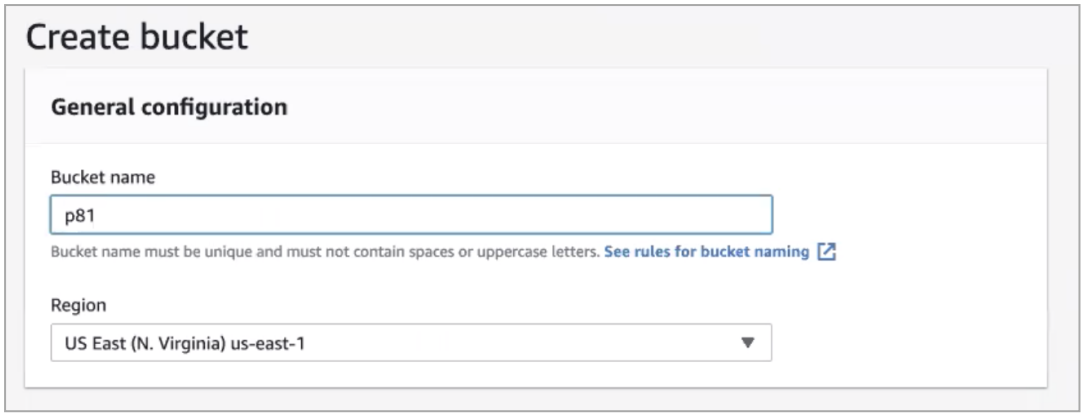
1. Log in to the AWS Management Console.
2. Go to **AWS Services** and select **S3**.



3. Click **Create Bucket**.



The **Create bucket** window appears.

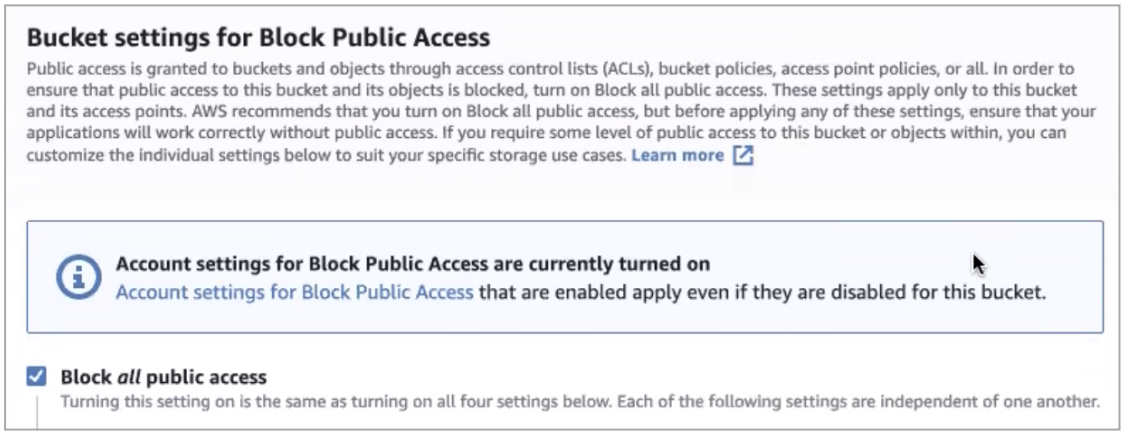


4. In the **Bucket name** field, enter the name of the bucket.

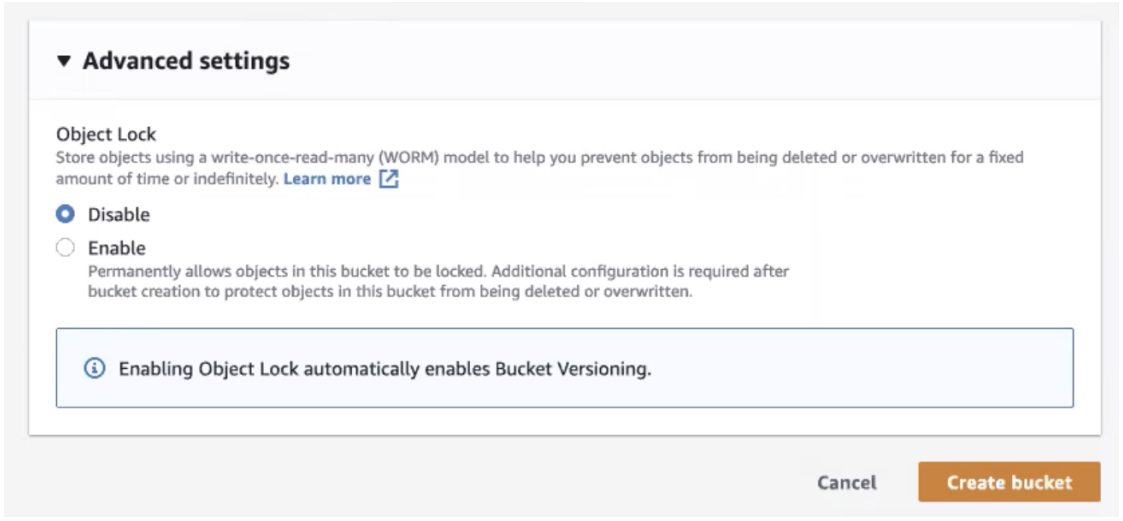
   The name must contain alphabets only. Hypen (-) and period (.) are not supported.

5. In the **Region** field, enter the region where Amazon S3 creates buckets. Select the AWS region geographically nearest to you.

6. Select or clear the **Block all public access** checkbox according to your company policy. It is selected by default.



7. In **Advanced settings** > **Object Lock**, select **Disable**.



8. Click **Create bucket**.

Step 2 - Creating a New IAM Policy

Important - You can grant the user full access to your S3 buckets (by attaching the appropriate AWS managed policy) or create a new policy that applies only to the Check Point SASE bucket. If you grant full access, skip this procedure.

1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Policies** tab and click **Create policy**.
4. Paste this snippet as a JSON file. Replace `test` with the bucket name.

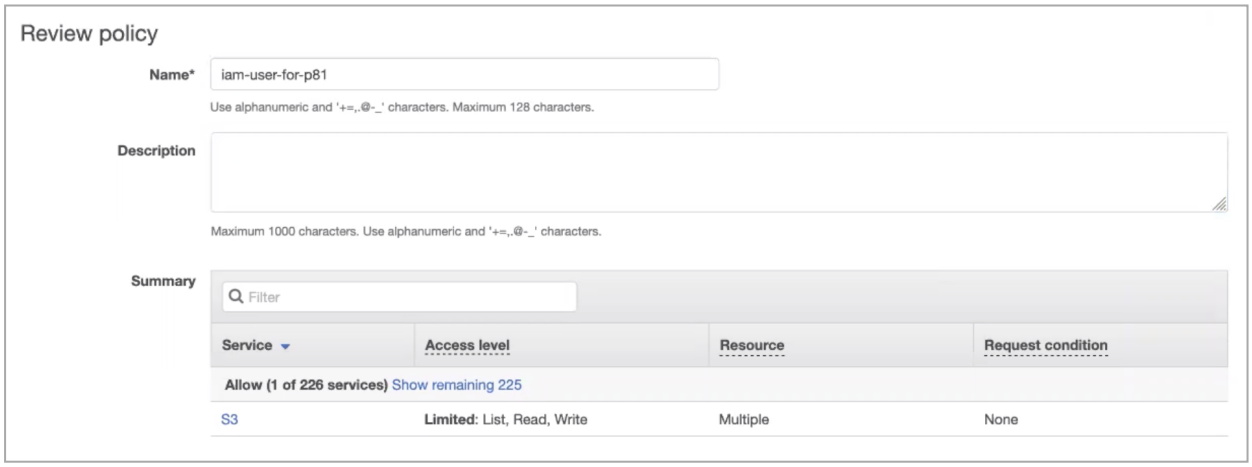
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test"
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test/*"
        }
    ]
}
```

Important - For a full list of permissions granted, see permissions. To restrict the list of permissions, add the highlighted text to the syntax.

```
{
"Version" : "2012-10-17",
"Statement" : [
{
"Effect" : "Allow" ,
"Action" : [
"s3:ListBucket",
"s3:GetBucketLocation"
],
"Resource" : ["${aws_s3_bucket.pm81-logs.arn}"]
},
{
"Effect" : "Allow" ,
"Action" : [
"s3:PutObject" ,
"s3:GetObject" ,
"s3:DeleteObject" ],
"Resource" : ["${aws_s3_bucket.pm81-logs.arn}/*" ]
}
]}
```

5. Click **Review policy**.

   The **Review policy** window appears.

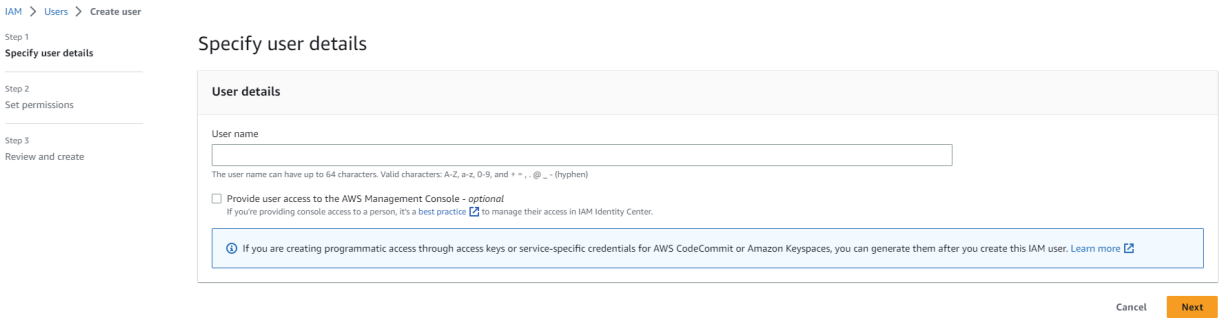


6. Enter these:
   a. **Name**: Name of the policy.
   b. (Optional) **Description**
7. Click **Create policy**.

Step 3 - Creating an AWS User

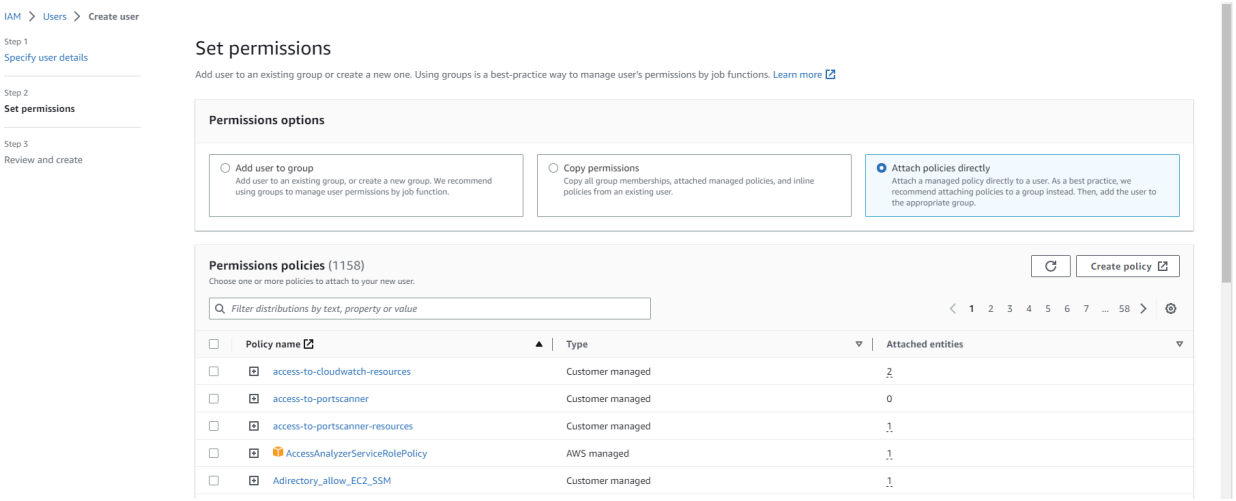
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and click **Create user**.
4. In the **Username** field, enter a name.

   Click **Next**.



5. Click **Attach policies directly** and select the policy you created earlier.

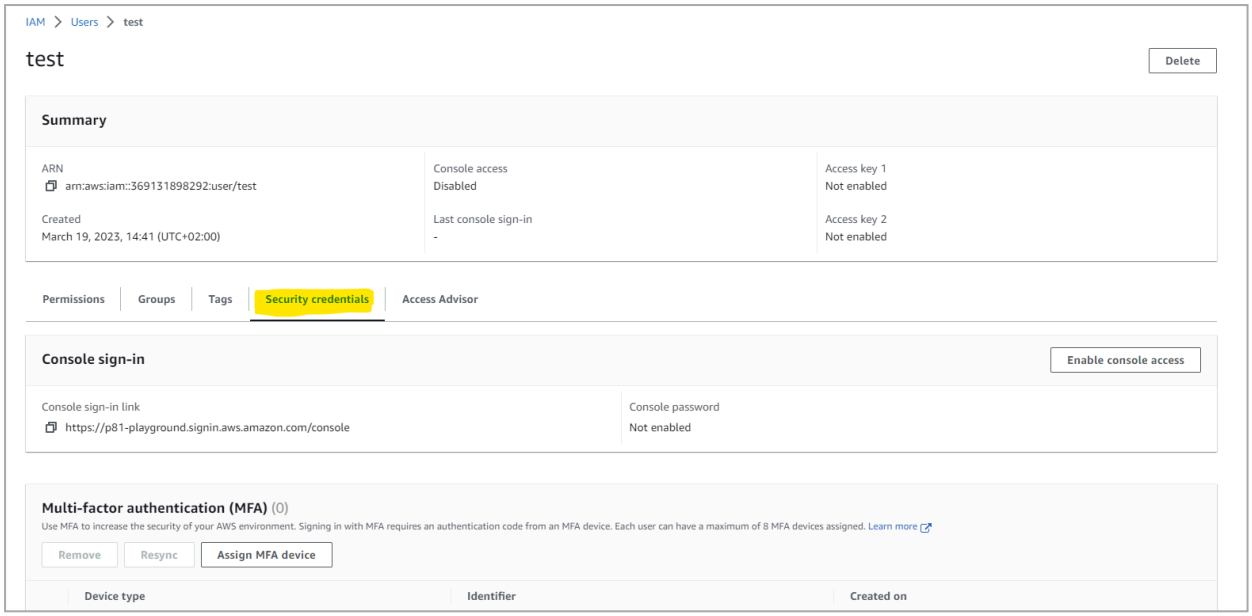
   If you have granted full access, then select the S3 full access AWS managed policy.



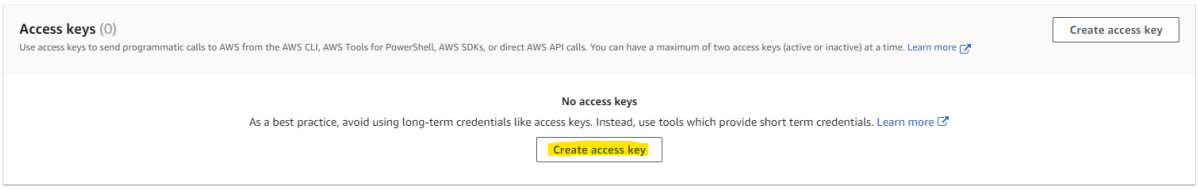
6. Click **Next**.

Step 4 - Creating an AWS Access Key

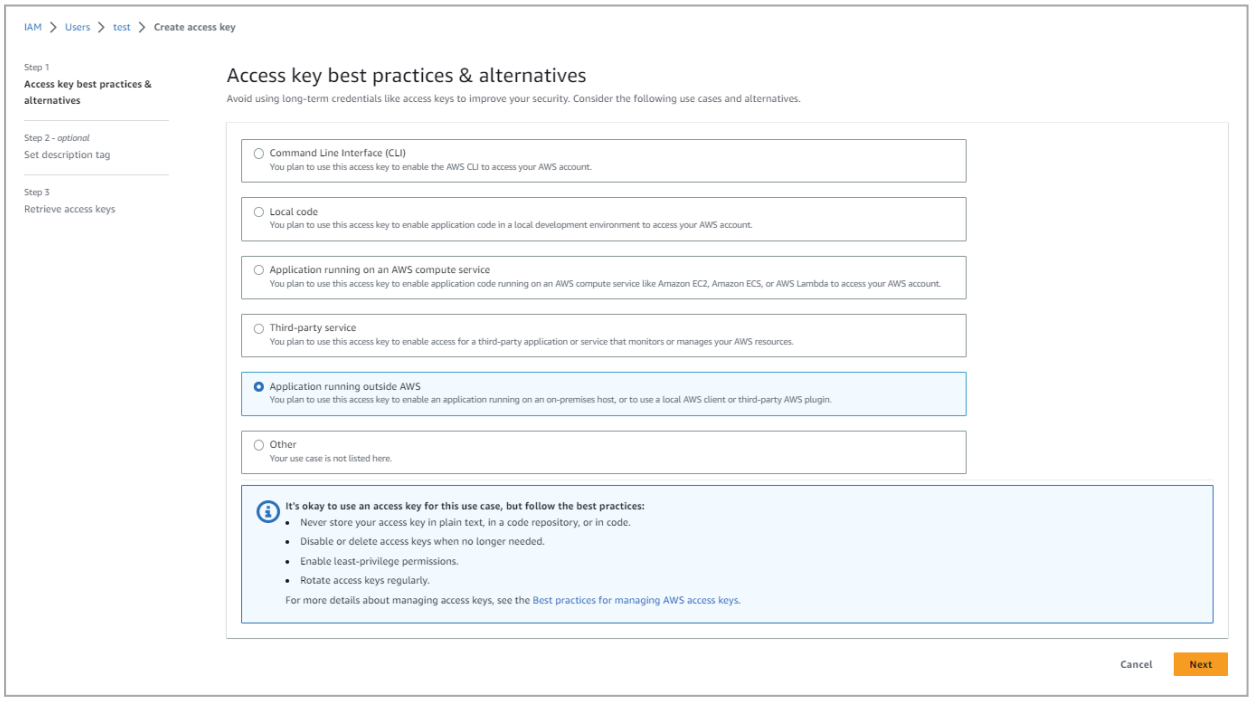
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and select the user you have created.
4. Click the **Security credentials** tab.



5. Scroll down to **Access keys** and click **Create access key**.

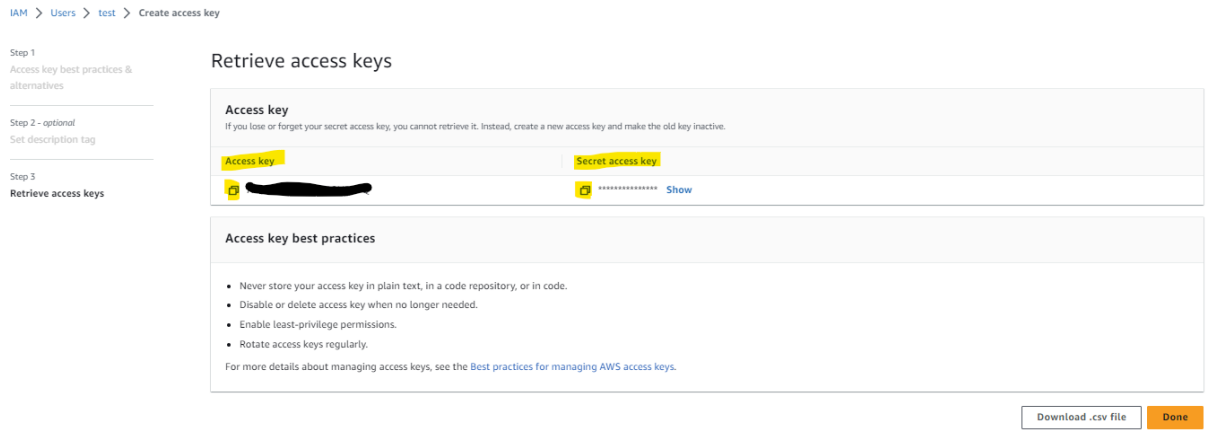


6. Select **Application running outside AWS** and click **Next**.



7. Select **Create access key**.
8. Description tag is optional.

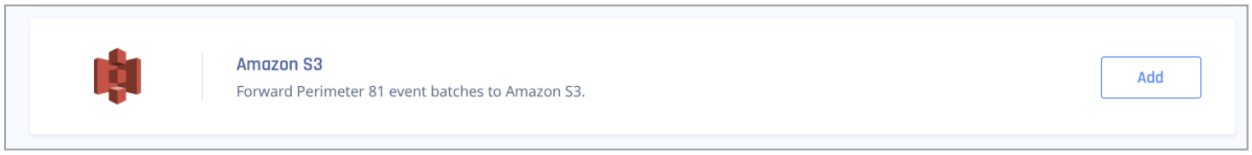
9. Copy the **Secret access key** and the **Access key**.



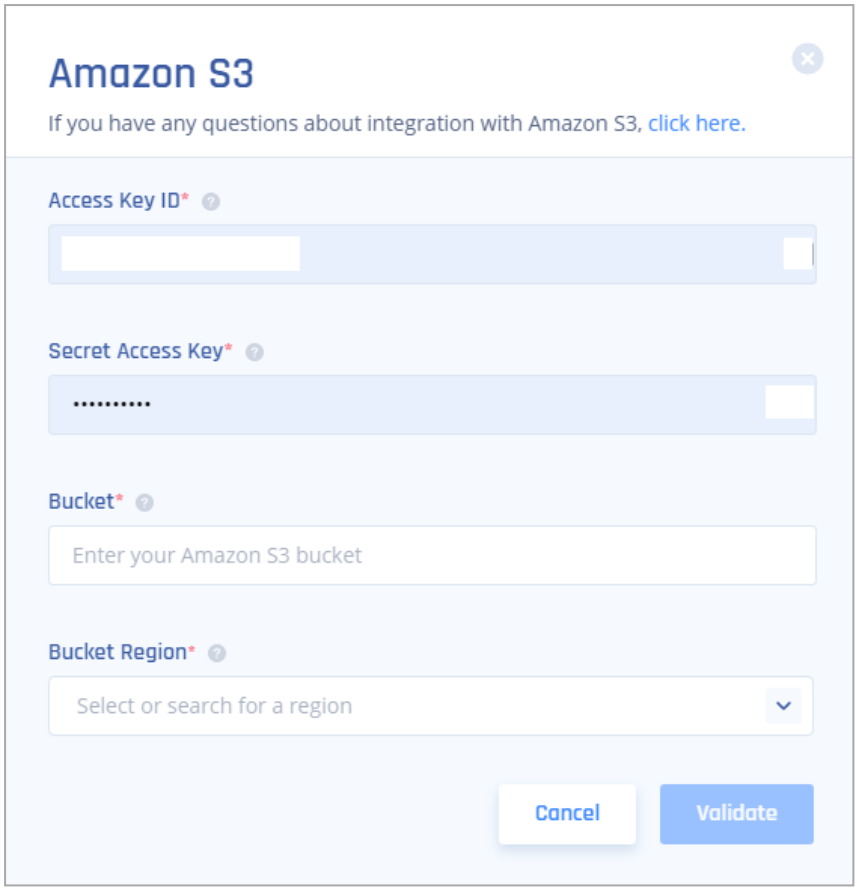
10. Click **Done**.

Configuring the Amazon S3 Integration in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Amazon S3** row, click **Add**.



The **Amazon S3** window appears.



3. In the **Access Key ID** field, enter the **Access key** copied from AWS console.
4. In the **Secret Access Key** field, enter the **Secret access key** copied from AWS console.
5. In the **Bucket** field, enter the Amazon S3 bucket name (for example in this case, arn:aws:s3:::test, the bucket name is test)
6. In the **Bucket region** field, enter the region selected when you created the Amazon S3 bucket.
7. Click **Validate**.

Troubleshooting

Status message	Action required
Success	None
S3_INVALID_ ACCESS_KEY_ID	Make sure you copied the correct access key ID.
S3_INVALID_ SECRET_ACCESS_ KEY	Make sure you copied the correct secret access key.

Status message	Action required
S3_INVALID_ BUCKET	Make sure the Bucket name in Check Point SASE matched the Bucket name in Amazon S3 (case sensitive).
S3_ACCESS_ DENIED_BUCKET	The IAM user does not have the required access permissions to the bucket. Make sure to attach the appropriate policy.

ConnectWise PSA

ConnectWise PSA allows Managed Service Providers (MSPs) to streamline the billing process through automation with ConnectWise Manager.

It can receive product catalog and usage data from Perimeter 81 and automate customer invoices.

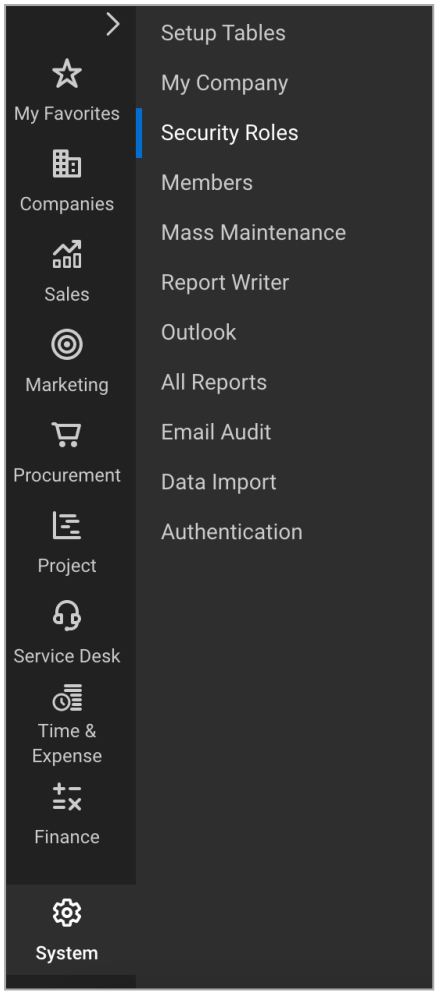
Note - This is available only for the accounts in the Perimeter 81 workspace.

Generating API Key in ConnectWise PSA

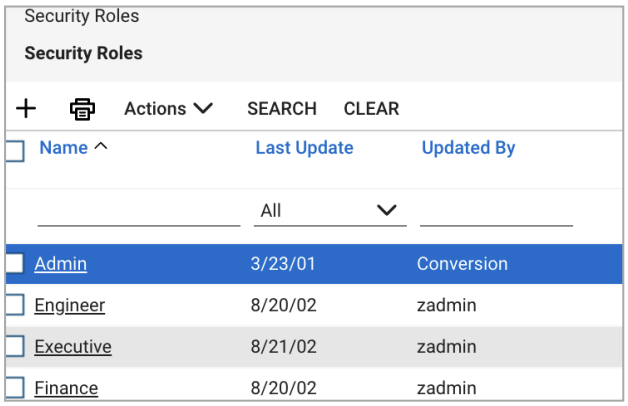
Check Point SASE uses an API key to authenticate the ConnectWise PSA integration.

To generate the API key in ConnectWise PSA:

1. Log in to the ConnectWise PSA portal.
2. Go to **System** > **Security Roles**.



3. Select the role for this integration.



4. Set these permissions:

   a. **Companies > Company Maintenance > Inquire Level= All**

b. **Finance** > **Agreements** > **Inquire Level=All**

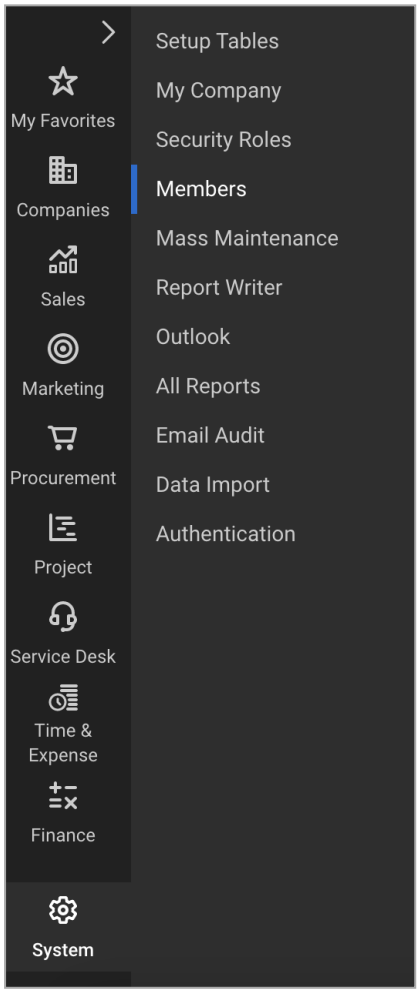
c. **Finance** > **Agreements** > **Add Level=All**

d. **Procurement** > **Product Catalog** > **Inquire Level= All**

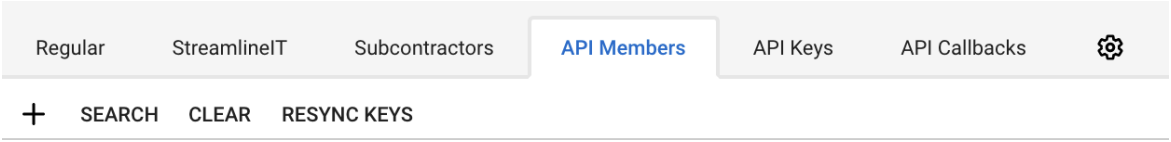
e. **Procurement** > **Product Catalog** > **Add Level= All**

f. **System** > **Table setup** > **Inquire Level= All**

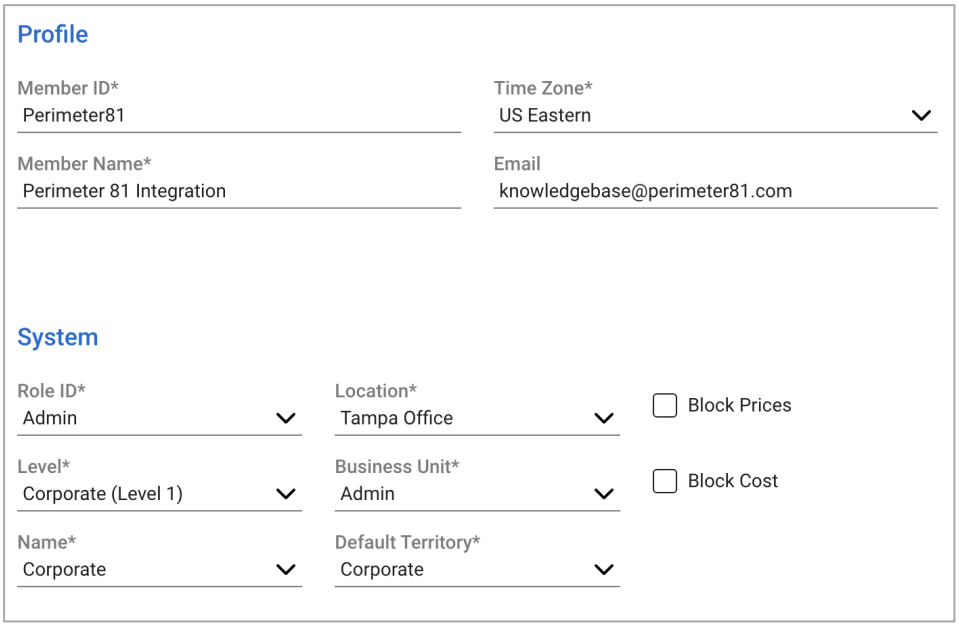
5. Click **Save**.
6. To generate the API key, from the **System** menu, click **Members**.



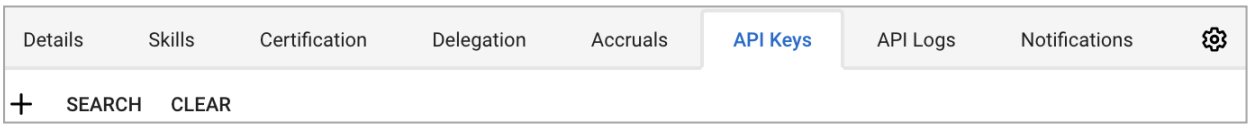
7. To add an API membership for Perimeter 81, click **API Members** tab and then click **+**.



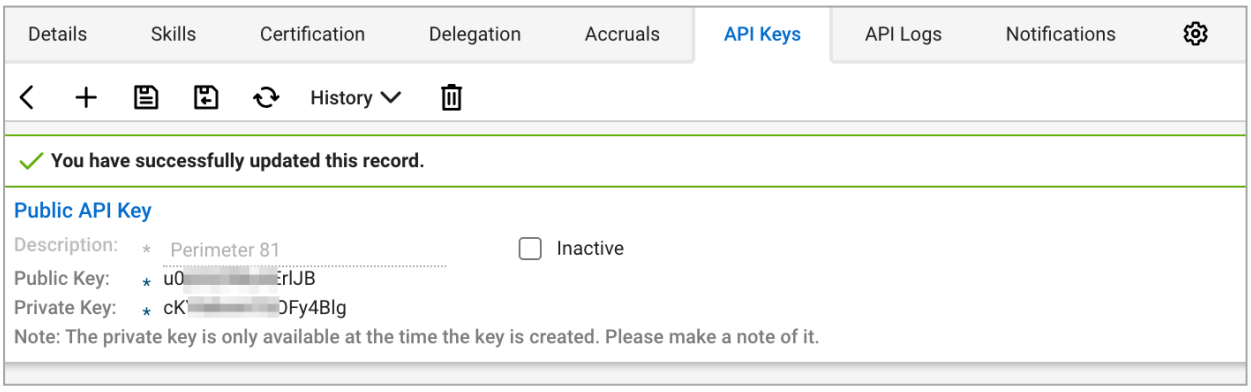
8. Enter the member details and click **Save**.



9. Select the newly created membership from the list of members, and then click the **API Keys** tab.



10. Create a new API key pair.

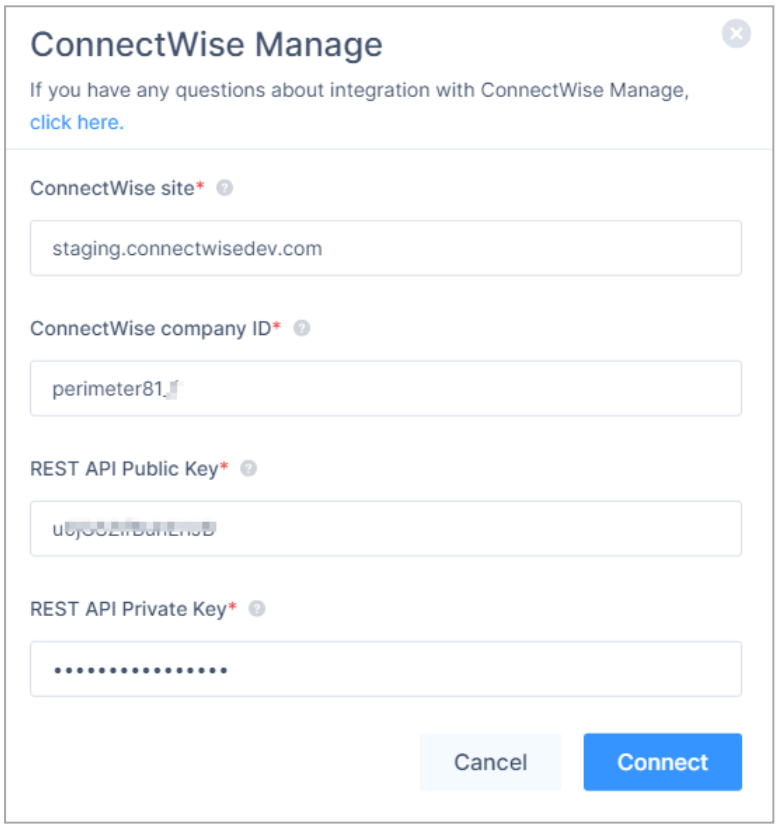


11. Copy the public and private keys.

Configuring the Integration in the Check Point SASE Administrator Portal

1. Access the Check Point SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **PSA integrations** section, in the **ConnectWise Manage** row, click **Add**.

3. Enter these:



Item	Description
ConnectWise site	URL of the ConnectWise PSA portal login screen.
ConnectWise company ID	Company ID registered with ConnectWise PSA portal.
REST API Public Key	API Public Key generated in the ConnectWise PSA portal.

Item	Description
REST API Private Key	API Public Key generated in the ConnectWise PSA portal.

4. Click **Connect**.

   The *Successfully connected to ConnectWise Manage* message appears.

5. Click **Apply**.

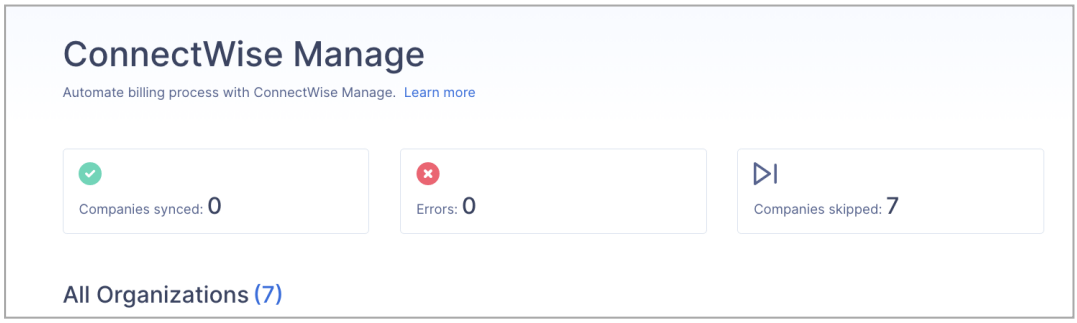
   The *ConnectWise integration has been configured successfully* message appears.

   After a successful integration, the Check Point SASE product catalog is synchronized with ConnectWise PSA.

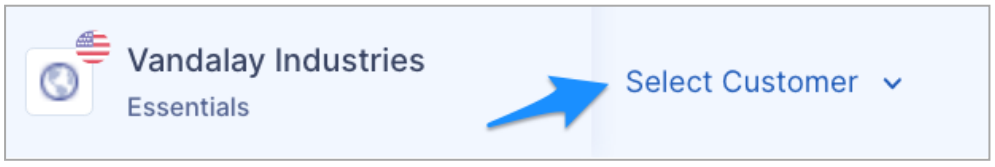
Mapping Customers and Agreements

1. Access the Check Point SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **PSA integrations** section, in the **ConnectWise Manage** row, click **Manage**.

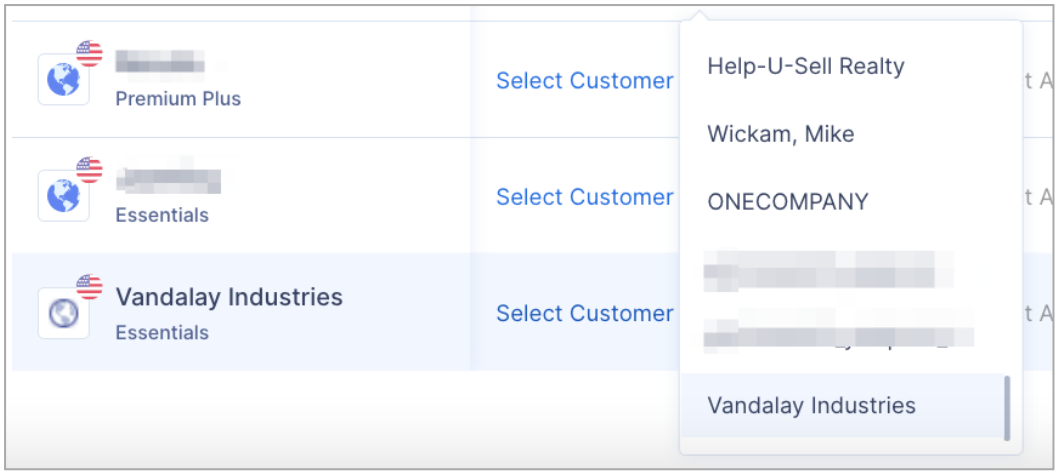
The **ConnectWise Manage** page appears that displays all the organizations you manage in Perimeter 81.



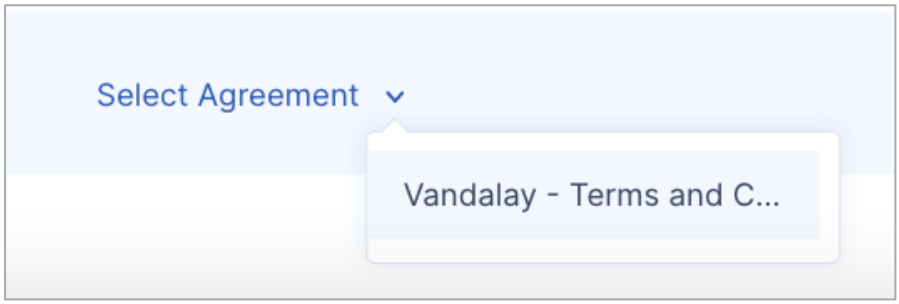
3. For the organization you want to sync with ConnectWise Manage, click **Select Customer**.



4. Select the corresponding account on ConnectWise Manage.

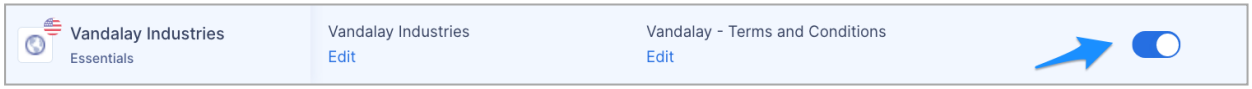


5. Select the ConnectWise Manage agreement that you have with your customer.



6. After you map customers and agreements, enable synchronization for each customer.

   Customers selected for synchronization are synchronized automatically every hour.



Identity Providers

Check Point SASE supports integration with these third-party Identity Providers (IDP) to identify members and allow Single Sign-On (SSO) when logging in with the SASEAgent.

- SAML 2.0
  - *"Generic SAML" on page 951*
  - *"Active Directory Federation Services (AD FS)" on page 954*
  - *"Auth0" on page 964*
  - *"Keycloak" on page 970*
  - *"OneLogin" on page 980*
  - *"PingOne for Enterprise" on page 989*
  - *"PingFederate" on page 995*
  - *"Rippling" on page 998*
  - *"JumpCloud" on page 1007*
  - *"Okta with SAML" on page 1013*
- Google Workspace
  - *"Google Applications with SAML 2.0" on page 1020*
  - *"Google Services" on page 1026*
- Microsoft Azure
  - *"Microsoft Entra ID (formerly Azure AD) (SAML 2.0)" on page 1036*
  - *"Microsoft Entra ID (formerly Azure AD) (Enterprise Application)" on page 1050*
  - *"Microsoft Entra ID (formerly Azure AD) (App Registration)" on page 1067*
- SCIM
  - *"Okta (SCIM)" on page 1085*
  - *Azure Active Directory (SCIM)*
- *"On-Premises Active Directory" on page 1117*

SAML 2.0

Check Point SASE allows users to authenticate using the third-party Identity Providers (IdP) that support Security Assertion Markup Language (SAML) 2.0 protocol.

SAML-based authentication involves two parties:

- Identity Provider (IdP): Authenticates the user and if successful, it provides a *SAML Assertion* to the Service Provider (SP).
- Service Provider (SP): Checks the *SAML Assertion* and if successful, it allows the user to access the service.

Check Point SASE serves as the Service Provider (SP) to authenticate the users and integrates with these Identity Providers that support SAML 2.0 protocol:

- *"Generic SAML" below*
- *"Active Directory Federation Services (AD FS)" on page 954*
- *"Auth0" on page 964*
- *"Keycloak" on page 970*
- *"OneLogin" on page 980*
- *"PingOne for Enterprise" on page 989*
- *"PingFederate" on page 995*
- *"Rippling" on page 998*
- *"JumpCloud" on page 1007*
- *"Okta with SAML" on page 1013*

Generic SAML

Prerequisites

- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the SAML Identity Provider" below*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on the next page*

Step 1 - Configure the SAML Identity Provider

To integrate Check Point SASE with a Generic SAML IdP, create a dedicated Check Point SASE Application in your SAML Identity Provider using these values:

- **Single Sign-OnURL**:
  - For US based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
  - For EU based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
- **Audience URI (SP Entity ID)**:
  - For US based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`
  - For EU based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`
  - For AU based platform: `urn:auth0:qsase-au:{{WORKSPACE}}-oc`
  - For India based platform: `urn:auth0:qsase-in:{{WORKSPACE}}-oc`
- Map these user attributes to Check Point SASE:

User Attributes		Check Point SASE Mapping
IdP Attribute	IdP Object	
Email Address	-	email
First Name	-	given_name
Last Name	-	family_name
-	Groups	groups

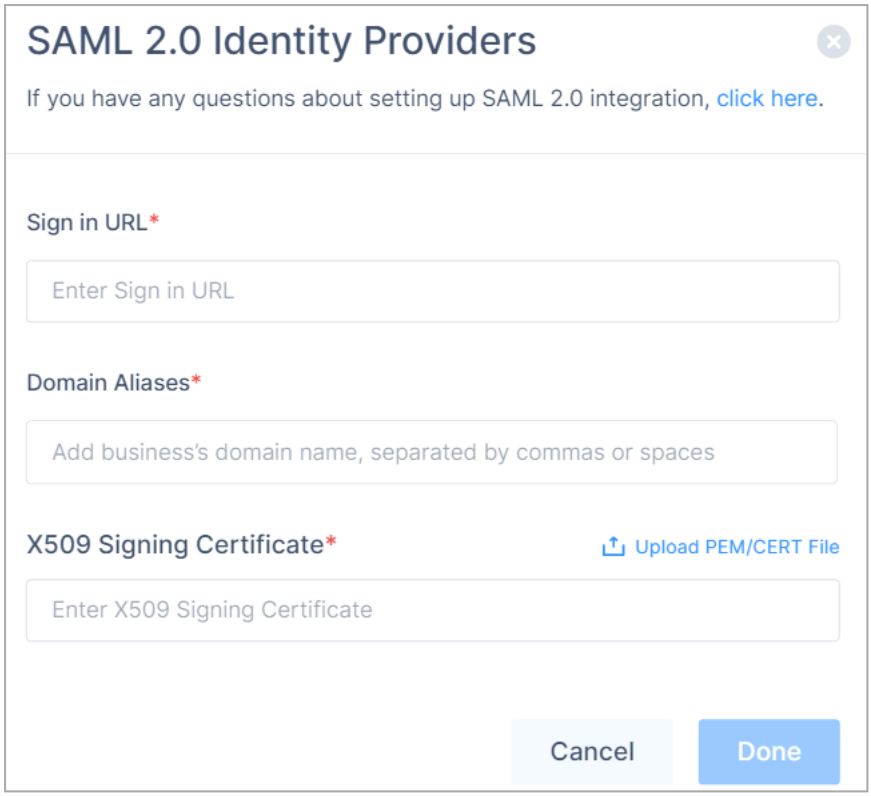
After creating the application, copy these values:

- Identity Provider Sign-in URL
- X.509 Certificate

Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Active Directory Federation Services (AD FS)

Prerequisites

- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

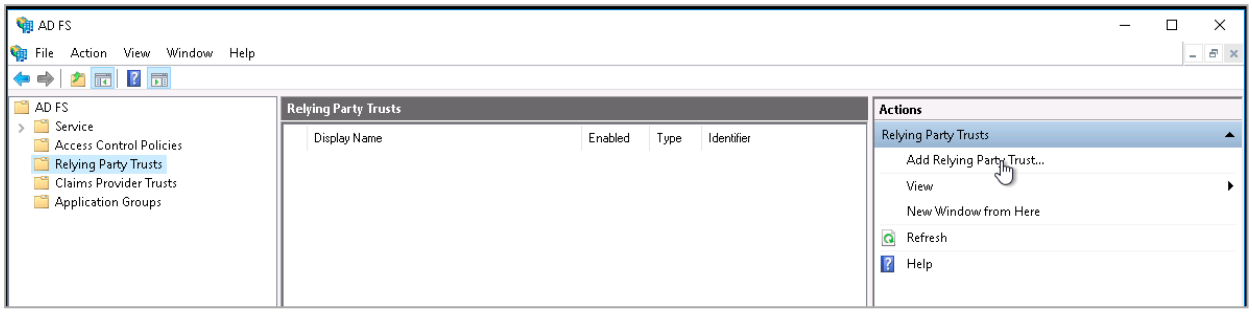
High-Level Procedure

- *"Step 1 - Configure the AD FS Management Portal" on the next page*
  1. *"Create a Relying Party Trust" on the next page*
  2. *"Edit Claim Issuance Policy" on page 959*
  3. *"Export the Signing Certificate" on page 961*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on page 962*

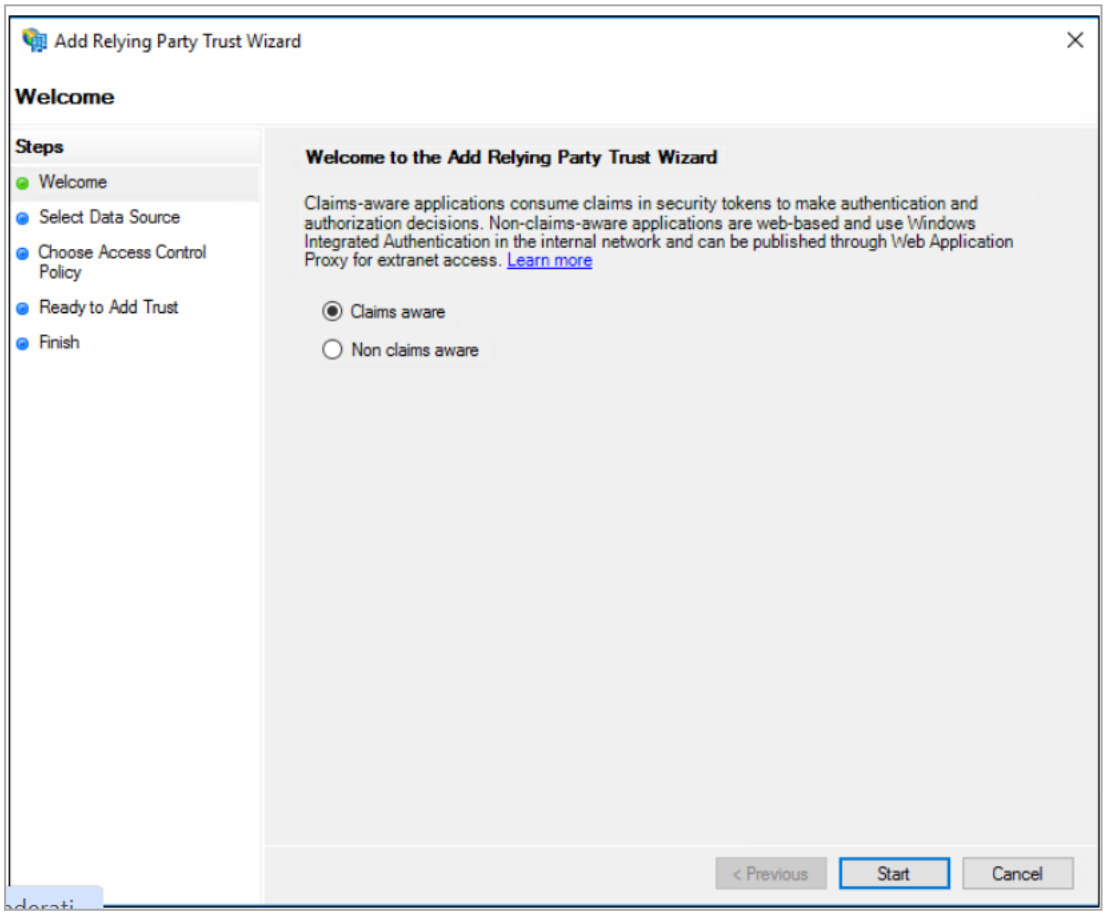
Step 1 - Configure the AD FS Management Portal

Create a Relying Party Trust

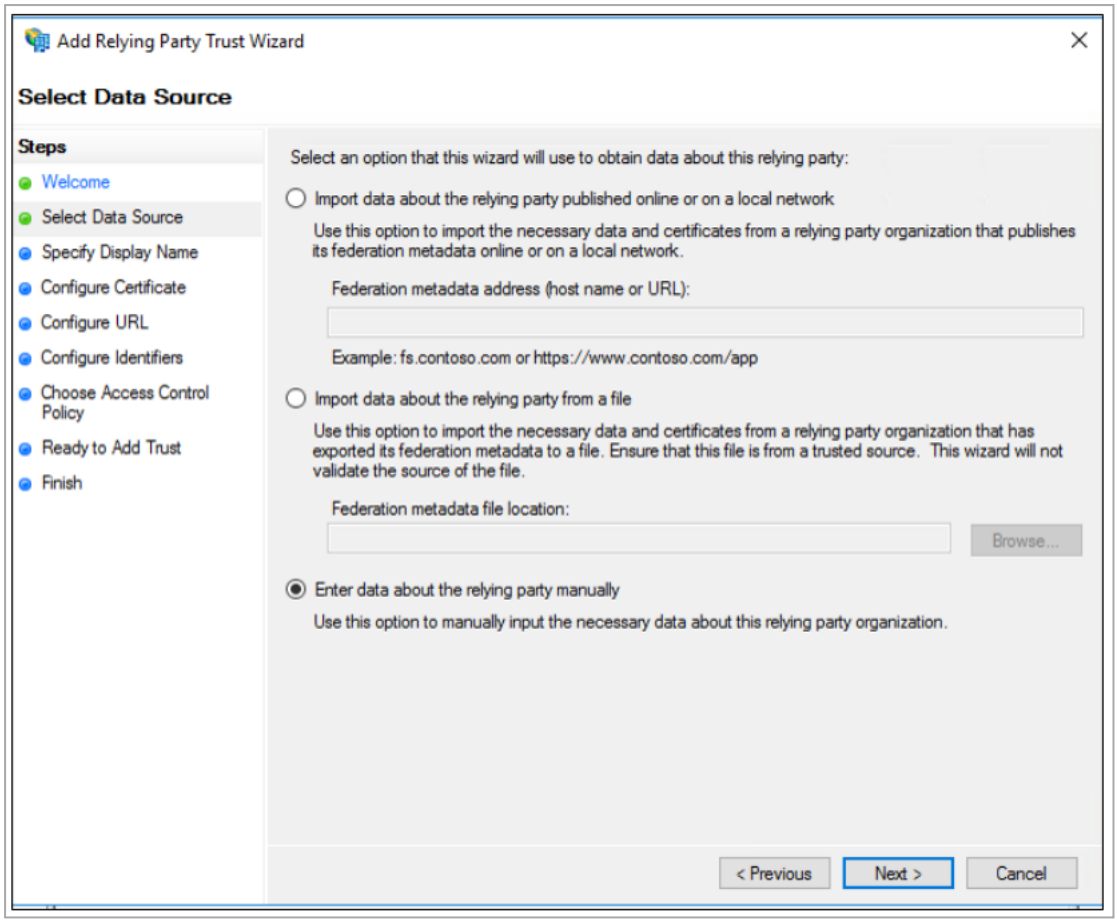
1. In the **Server Manager**, click **Tools**, and then select **AD FS Management**.
2. Under **Actions**, click **Add Relying Party Trust**.



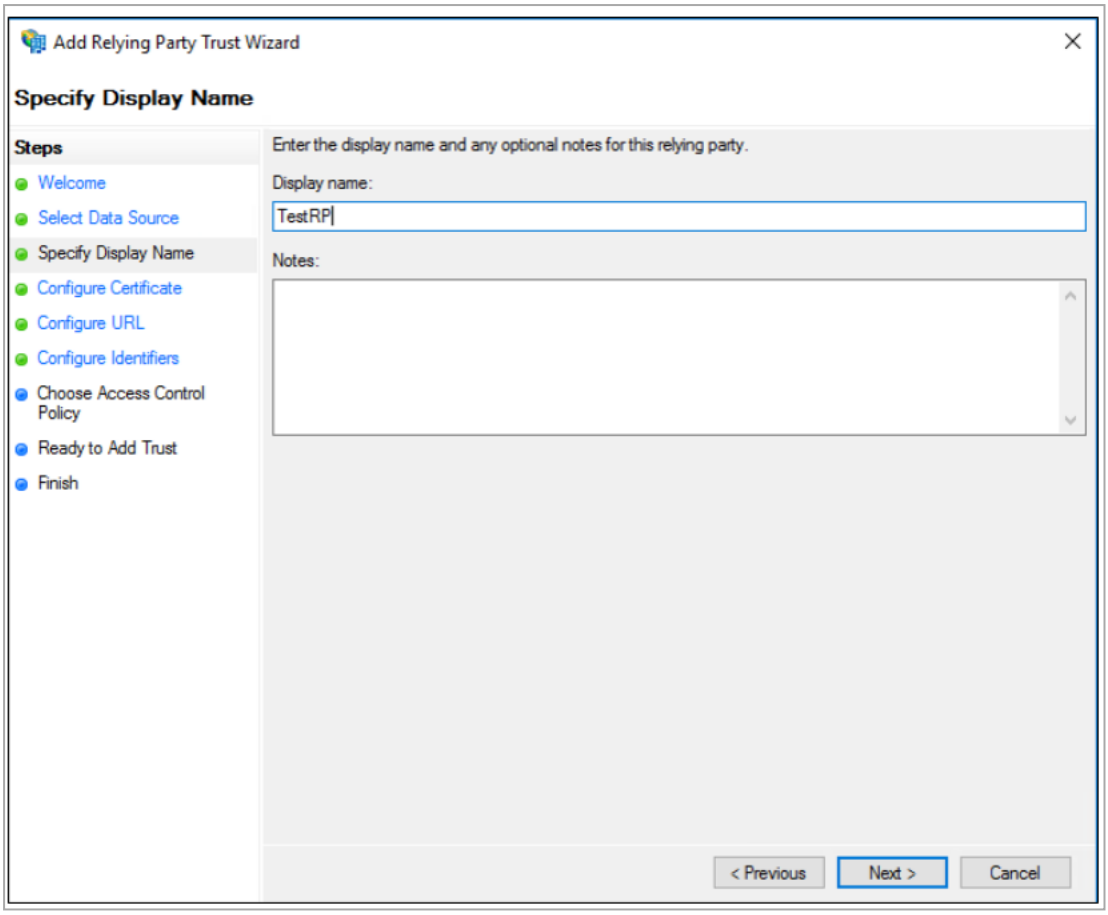
3. On the **Welcome** page, choose **Claims aware** and click **Start**.



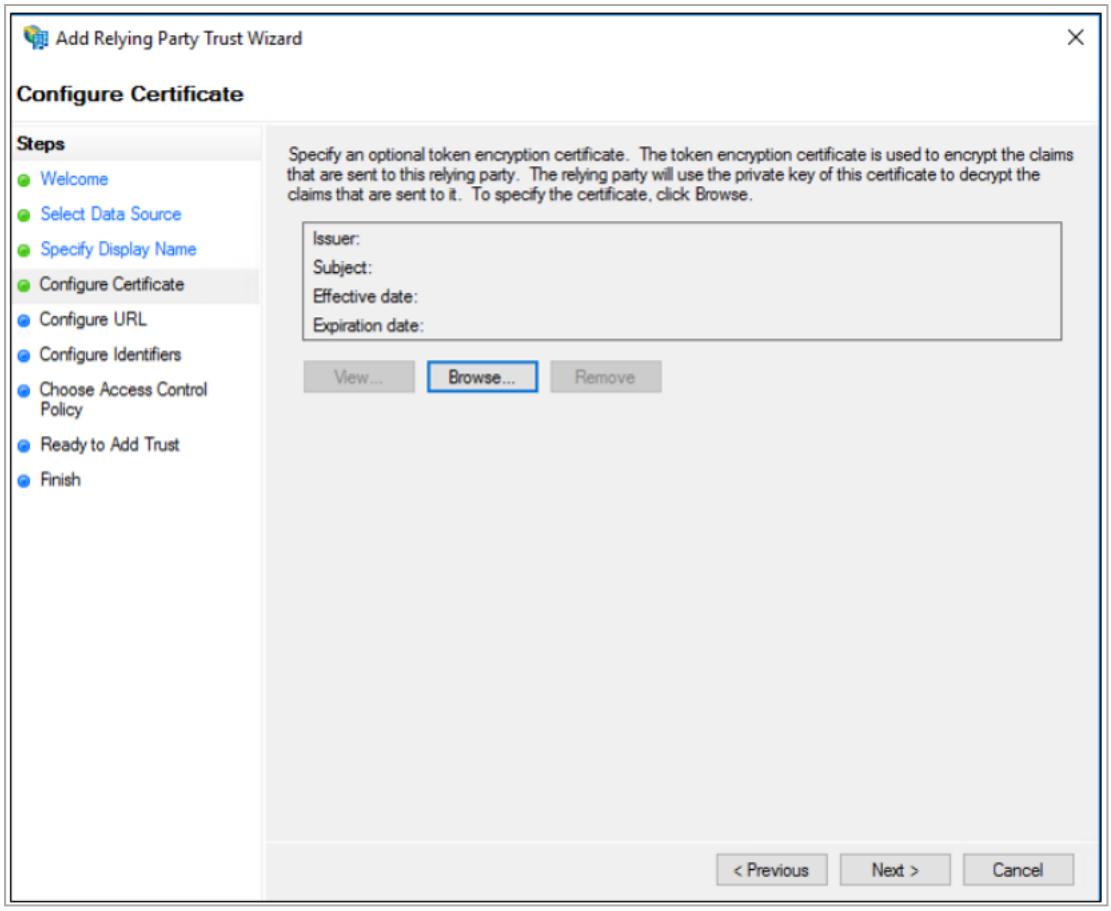
4. On the **Select Data Source** page, click **Enter data about the relying party manually**, and then click **Next**.



5. On the **Specify Display Name** page, type a name in **Display name**, under **Notes** type a description for this relying party trust, and then click **Next**.



6. On the **Configure Certificate** page, click **Next**.



7. On the **Configure URL** page:
   a. Select the **Enable support for the SAML 2.0 WebSSO protocol** checkbox.
   b. Under **Relying party SAML 2.0 SSO service URL**, enter US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
   c. Click **Next**.
8. On the **Configure Identifiers** page:

a. Enter the Relying party trust identifier as US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`

b. Click **Add** to add it to the list, and then click **Next**.

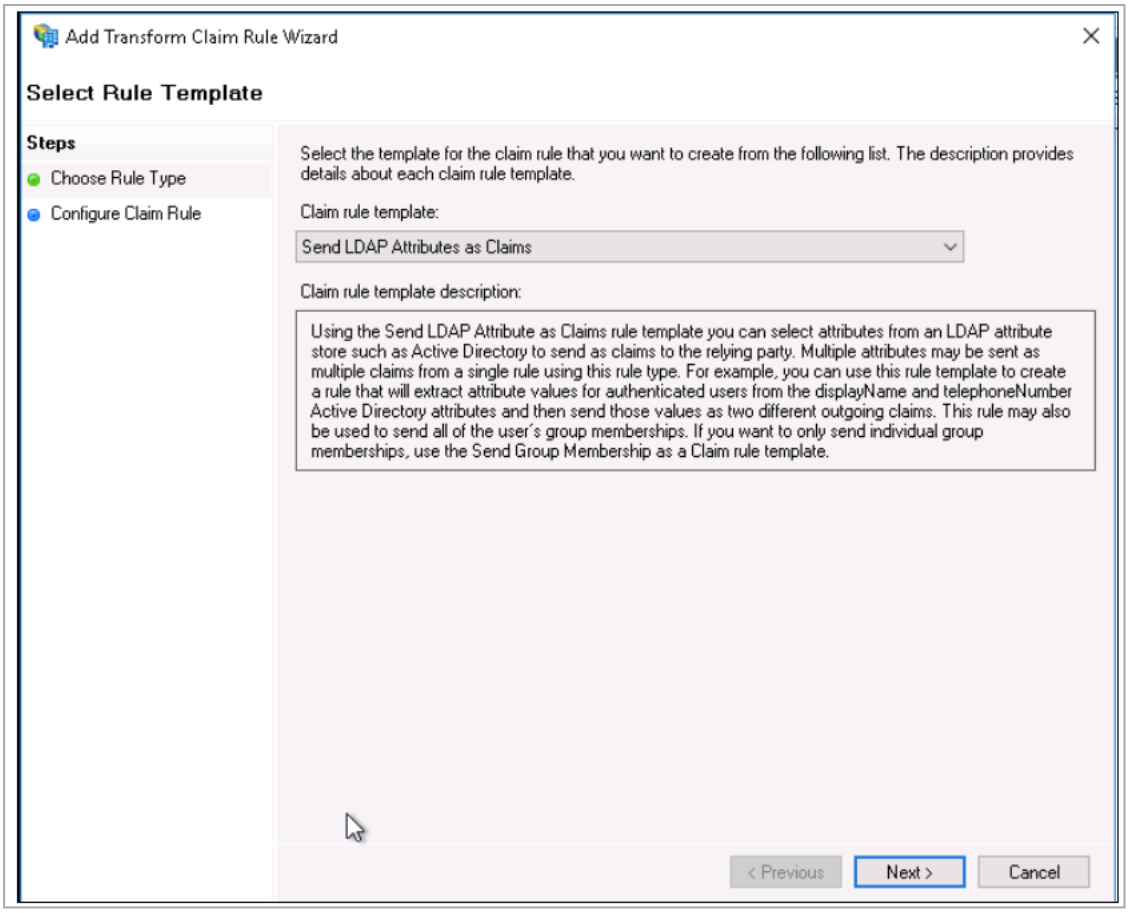
9. On the **Choose Access Control Policy** page, select **Permit everyone** and then click **Next**.
10. On the **Ready to Add Trust** page, review the settings, and then click **Next** to save your relying party trust information.
11. On the **Finish** page, make sure that the **Configure claims issuance policy for this application** checkbox is selected, and then click **Close**.

    This action automatically shows the **Edit Claim Issuance Policy** dialog box.

Edit Claim Issuance Policy

After you have created the Relying Party Trust, the **Edit Claim Issuance Policy** dialog box appears.

1. Click **Add Rule** to launch the wizard.
2. In the **Claim rule template** drop-down, select **Send LDAP Attributes as Claims** and click **Next**.



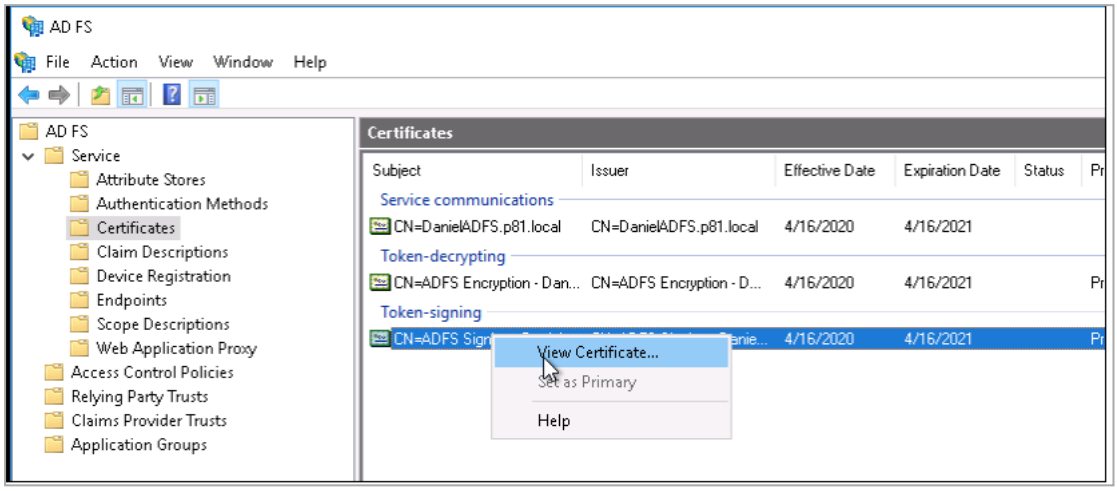
3. Enter a value for the **Claim rule** name, such as **LDAP Attributes**.
4. Choose **Active Directory** as your **Attribute Store**.
5. Map the **LDAP attributes** to these outgoing claim types:

LDAP Attribute	Claim Type
E-mail Addresses	email
Given-Name	given_name
Surname	family_name
Token-Groups Unqualified-Names	groups
User-Principal-Name	user_id

6. Click **Finish**.
7. In the **Edit Claim Issuance Policy** window, click **Apply**.

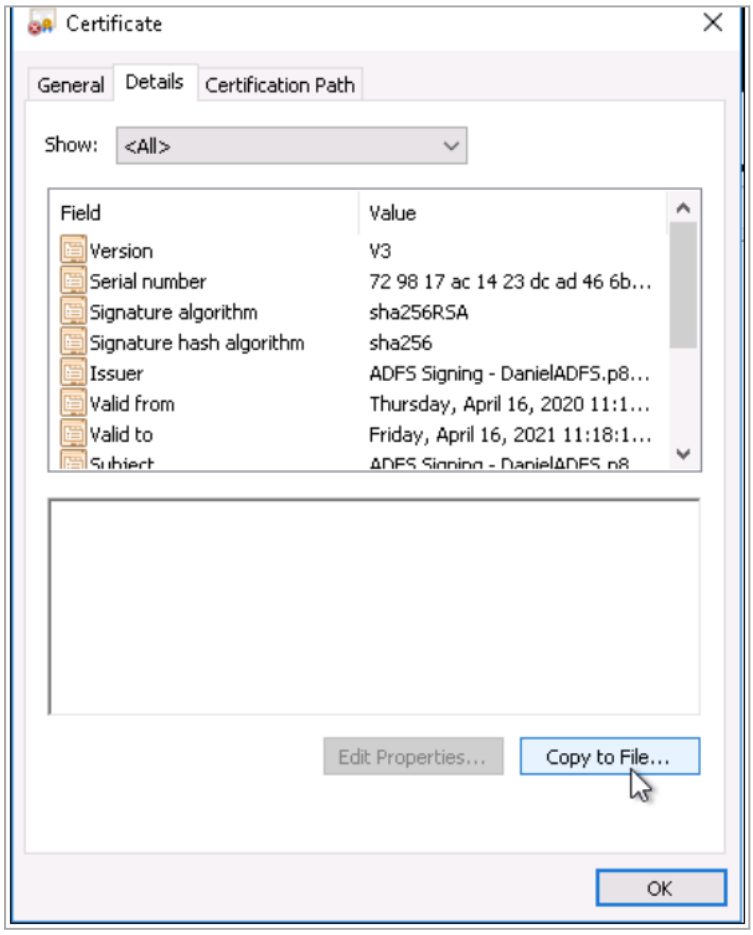
Export the Signing Certificate

1. From the left navigation pane, click **AD FS** > **Service** > **Certificates**.
2. Right-click **Token-signing** and then select **View Certificate**.



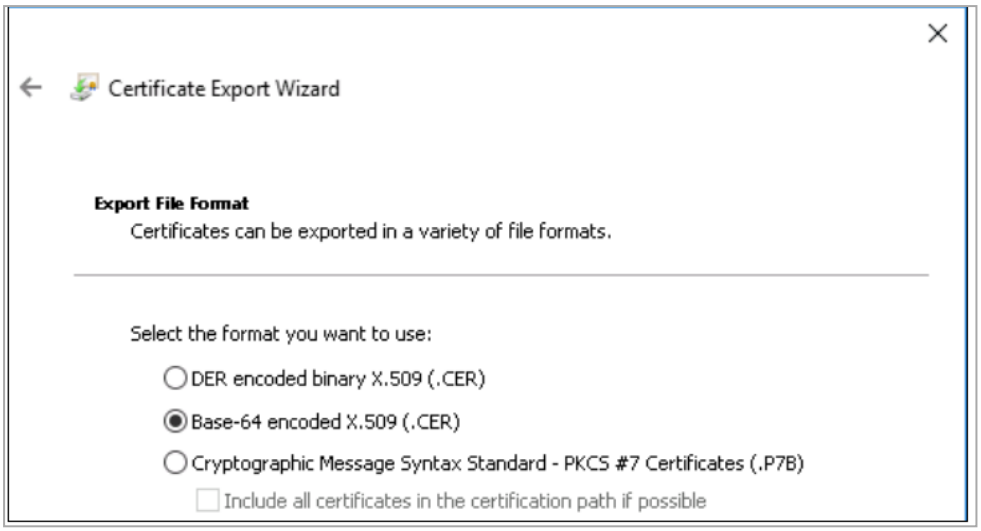
The **Certificate** pop-up appears.

3. Go to the **Details** tab, and click **Copy to File**.



4. In the **Certificate Export Wizard**, click **Next**.

5. Select the file format as **Base-64 encoded X.509 (.CER)** and then click **Next**.

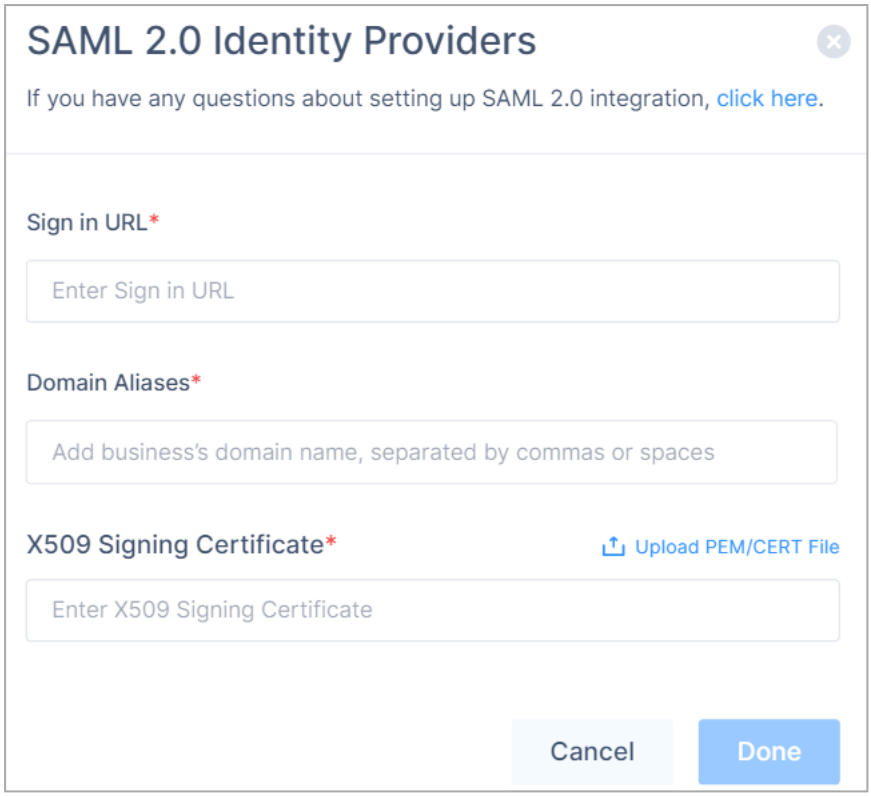


6. Select the location where you want to export the certificate and click **Next**.
7. Click **Finish**.

Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Auth0

Prerequisites

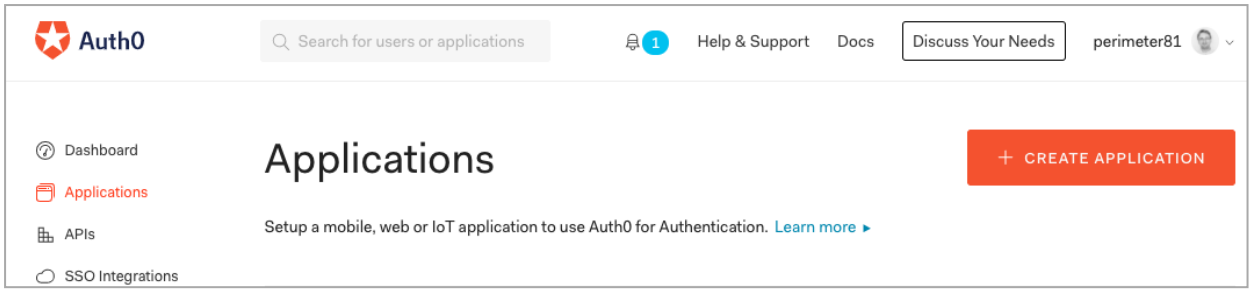
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

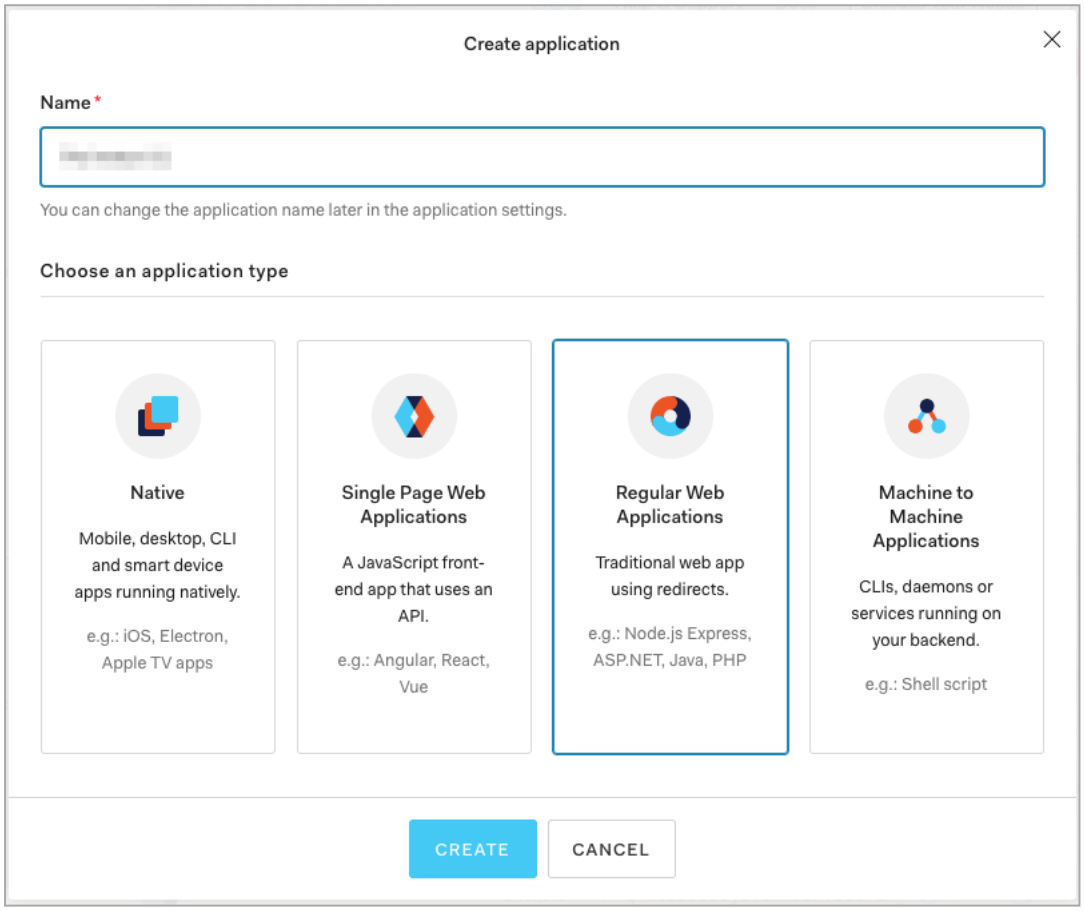
- *"Step 1 - Configure the Auth0 Management Portal" below*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on page 968*

Step 1 - Configure the Auth0 Management Portal

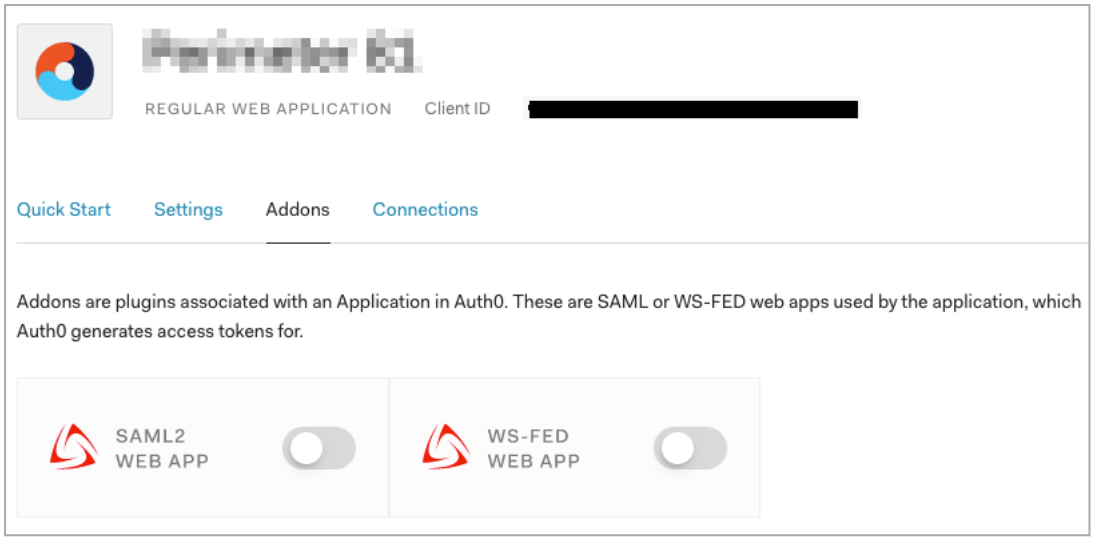
1. Log in to Auth0 Management Portal.
2. From the left navigation pane, click **Applications**.
3. Click **Create Application**.



4. In the **Name** field, enter a name for the application.



5. Select **Regular Web Application** and click **Create**.
6. Go to **Addons** tab and toggle **SAML2 Web App** to **ON**.



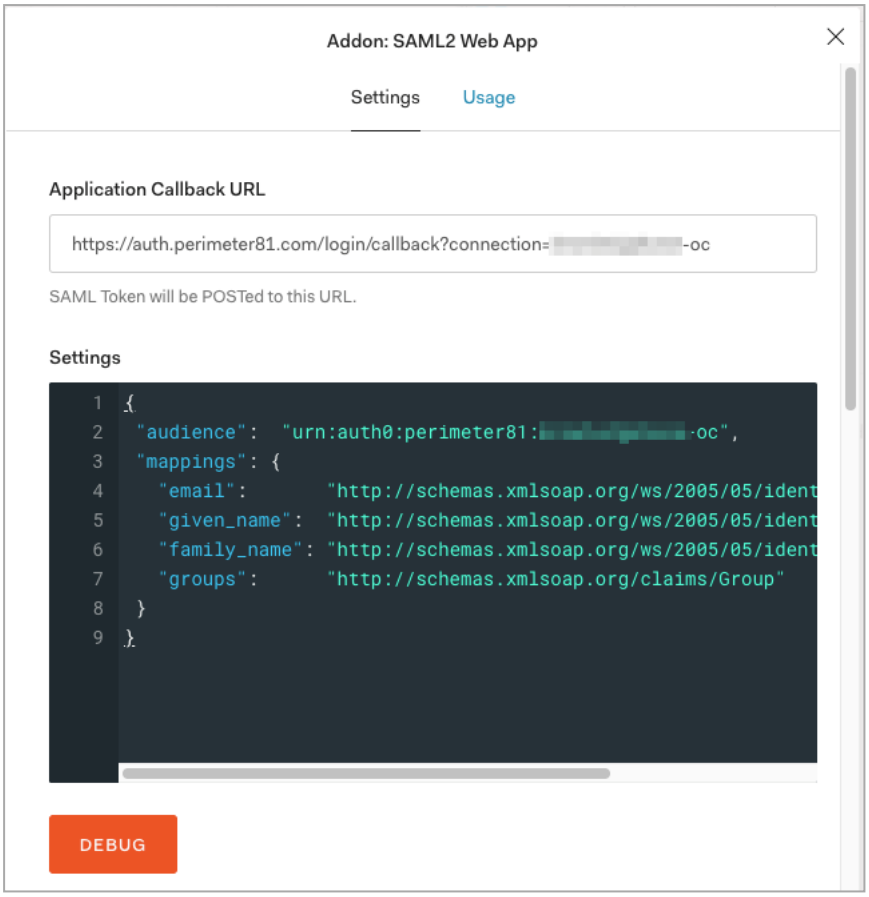
The **SAML2 Web App** window appears.

7. In the **Settings** tab, enter these values:

   - **Application Callback URL**: US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

- **Settings**: Copy the code, replace `{{WORKSPACE}}` with your Check Point SASE workspace name and paste it in **Settings**.

```
{

"audience": "urn:auth0:perimeter81:{{WORKSPACE}}-oc",

"mappings": {

"email":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila
ddress",

"given_name":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn
ame",

"family_name":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surnam
e",

"groups": "http://schemas.xmlsoap.org/claims/Group"

}

}
```

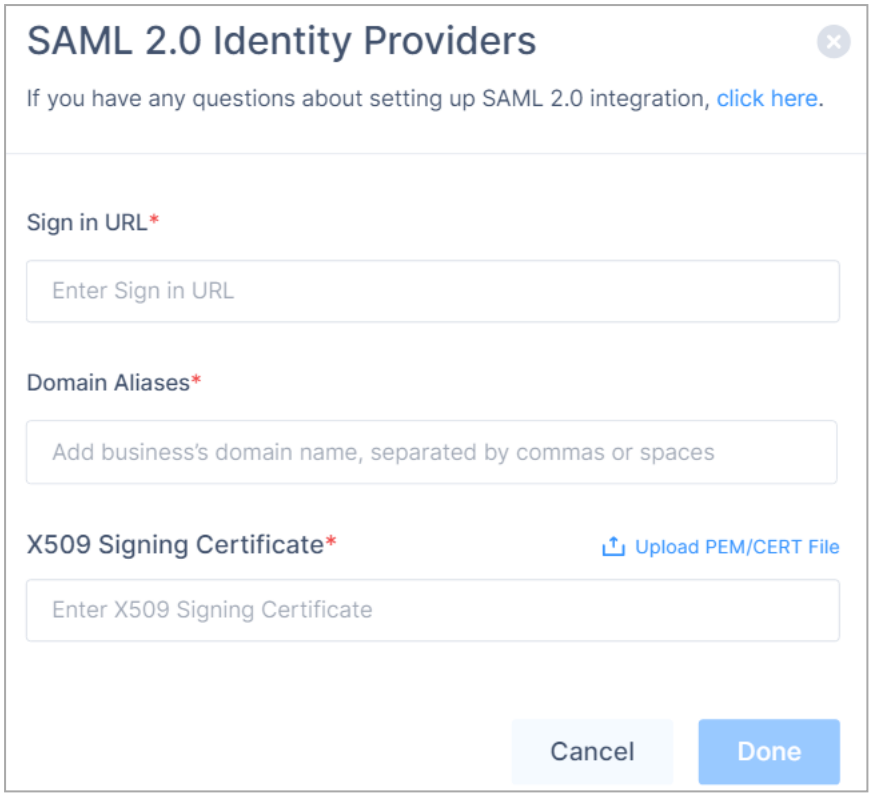


8. Click **Enable** to save and activate the application.
9. Click **Debug** and verify your configuration.
10. Go to the **Usage** tab.
11. Click **Download Auth0 certificate**.
12. Copy the **Identity Provider Login URL**.

Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Keycloak

SASE can authenticate users through Keycloak, ensuring a secure and efficient login process by utilizing the Security Assertion Markup Language (SAML) protocol.

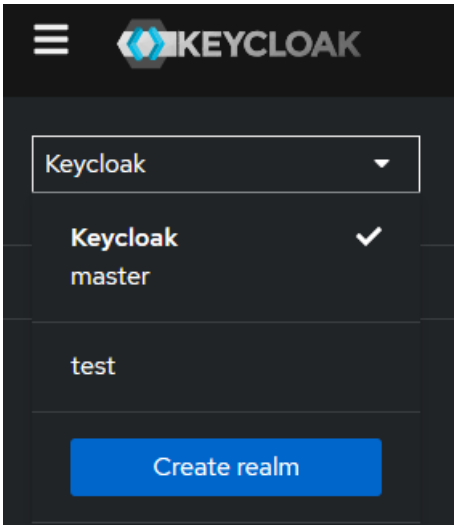
Prerequisites

- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

Integration Procedure

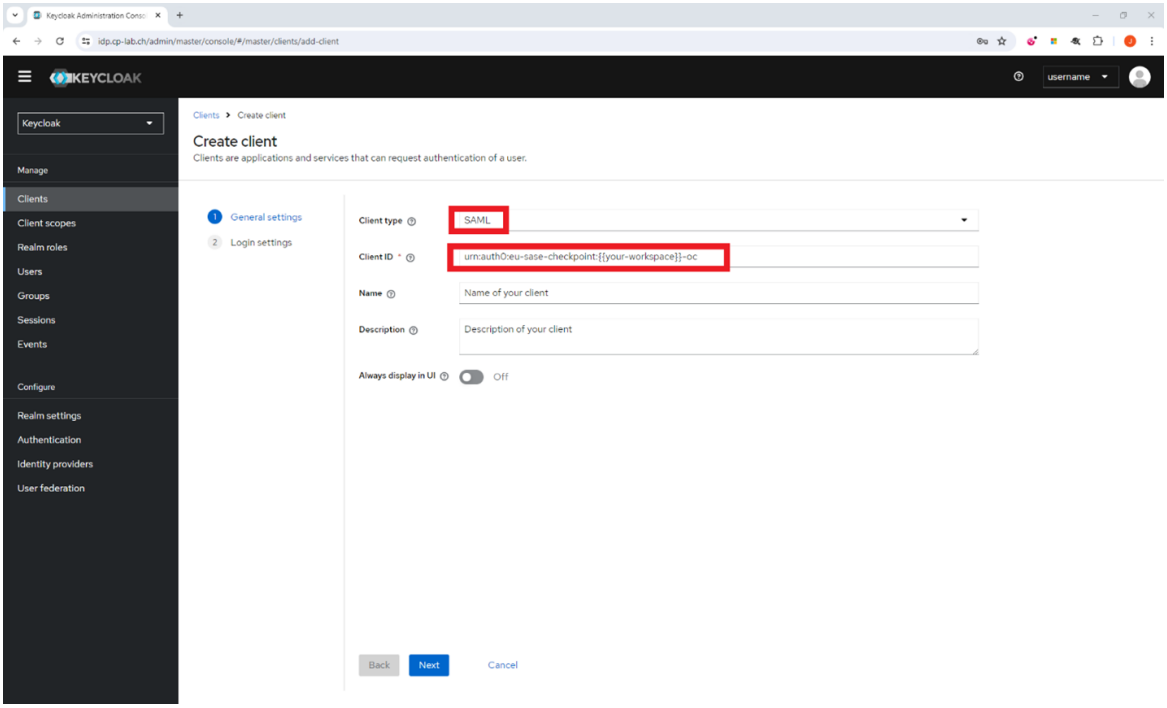
To configure Keycloak as an Identity Provider:

1. Log in to your Keycloak Administrator Console:
   a. Select the realm you want to configure.



   b. Go to **Clients** and click **Create client**.

   The **Create client** page appears.



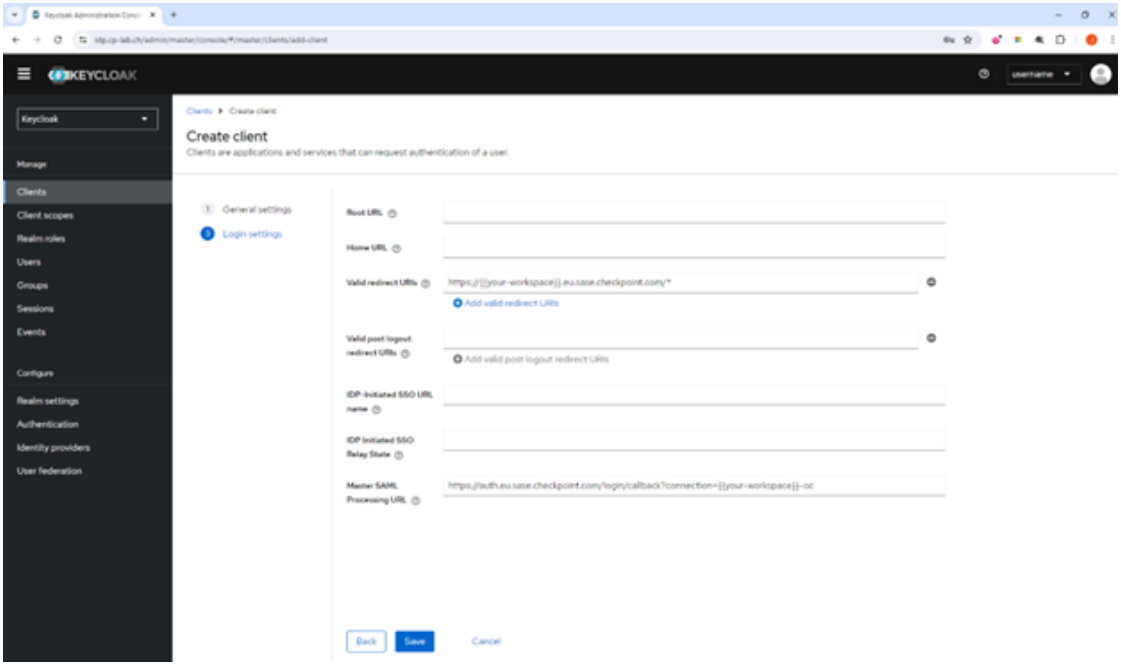
   c. From the **Client type** list, select SAML.

d. In the **Client ID** field, enter the audience URI (SP Entity ID) of your SASE workspace:

   - For US based platform - `urn:auth0:perimeter81:{{WORKSPACE}}-oc`
   - For EU based platform - `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`

     For example - acme.perimeter81.com workspace should translate to `urn:auth0:perimeter81:acme-oc`

e. Click **Next**.



f. In the **Valid redirect URIs** field, enter your workspace URL:

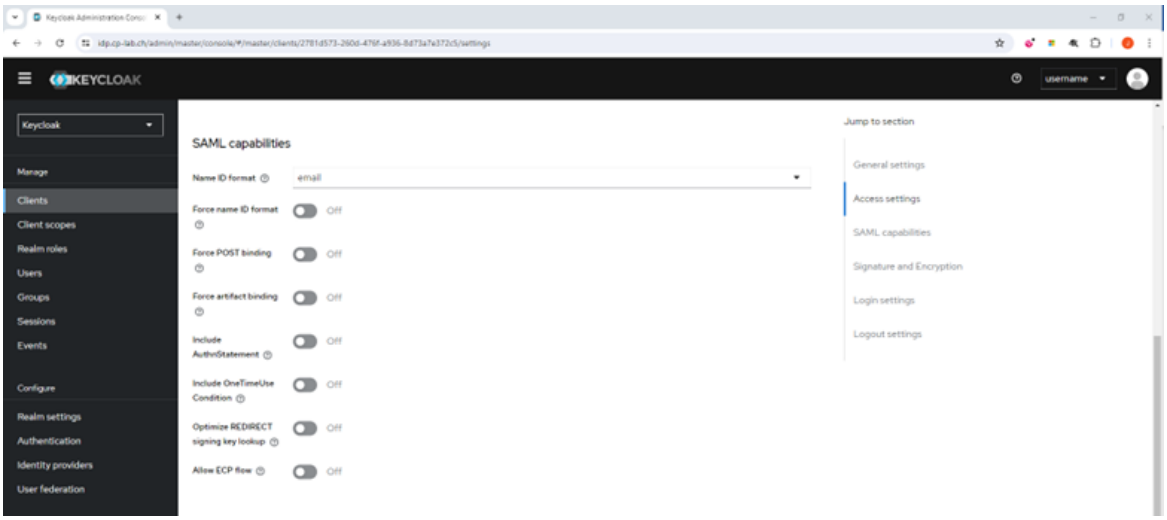
   - For US based platform - `https://{{your-workspace}}.perimeter81.com/*`
   - For EU based platform - `https://{{your-workspace}}.eu.sase.checkpoint.com/*`

g. In the **Master SAML Processing URL** field, enter your Single sign-on URL:

   - For US based platform - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
   - For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

h. Click **Save**.

i. Go to **Access capabilities** and do these in the **SAML capabilities** section.

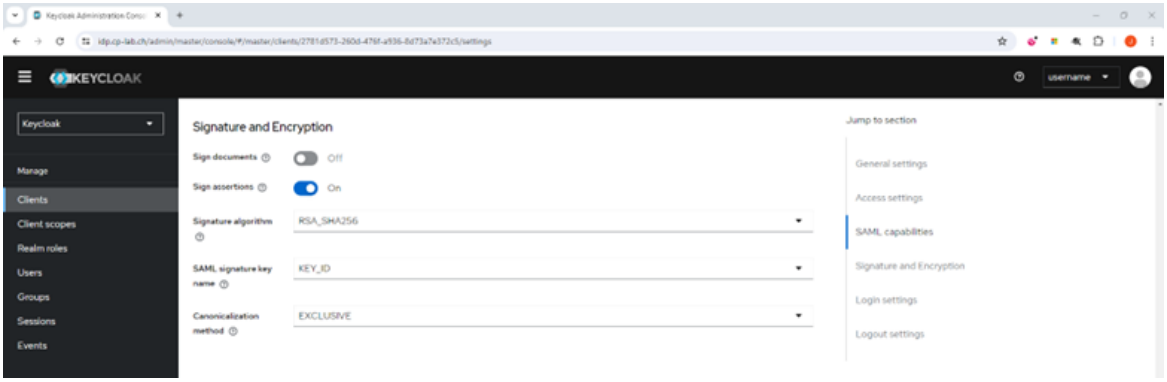


j. From the **Name ID format** list, select your email address.

k. Turn off the **Force POST billing** toggle button.

l. Turn off the **Include AuthnStatement** toggle button.

m. Go to the **Signature and Encryption** section.



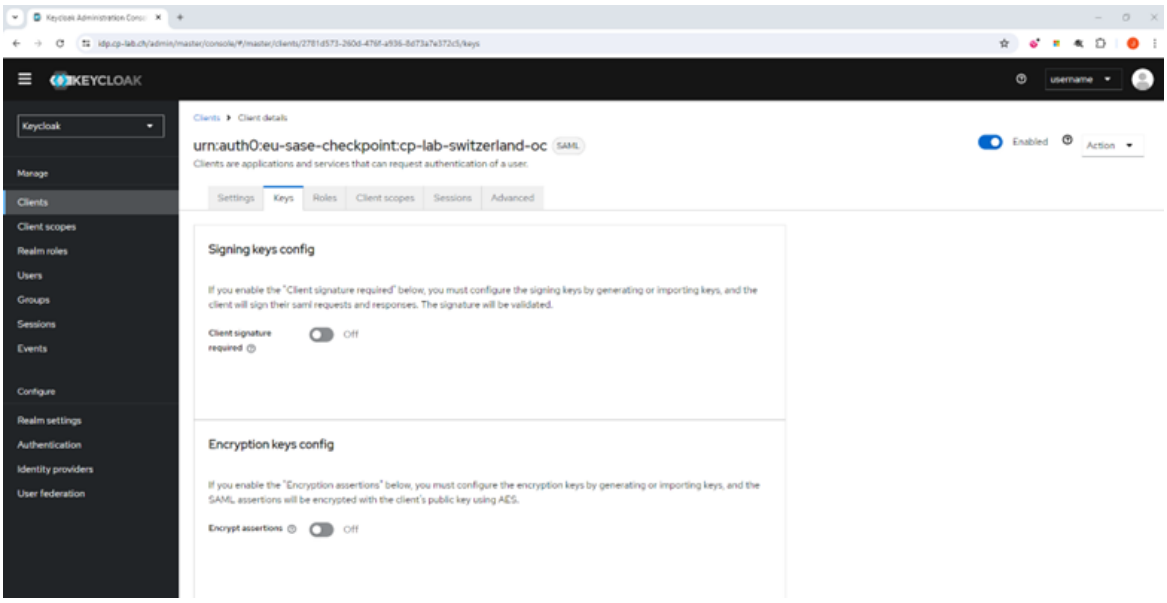
n. Turn off the **Sign documents** toggle button.

o. Turn off the **Sign assertion** toggle button.

p. From the **Signature algorithm** list, select **RSA_SHA256**.

q. From the **SAML signature key name** list, select **KEY_ID**.

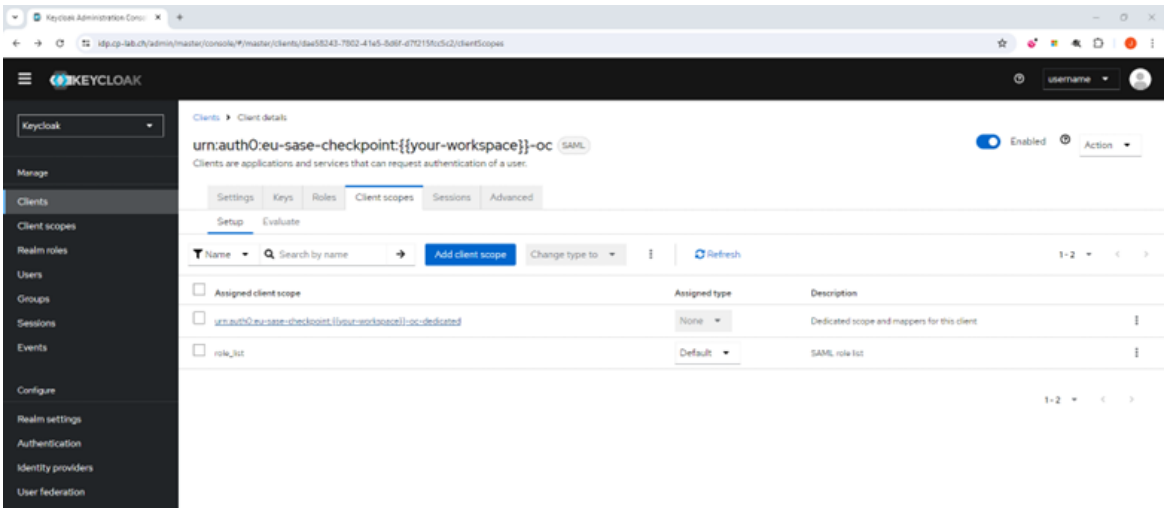
r. Click the **Keys** tab.



s. Turn off the **Client signature required** toggle button.

t. Turn off the **Encrypt assertions** toggle button.

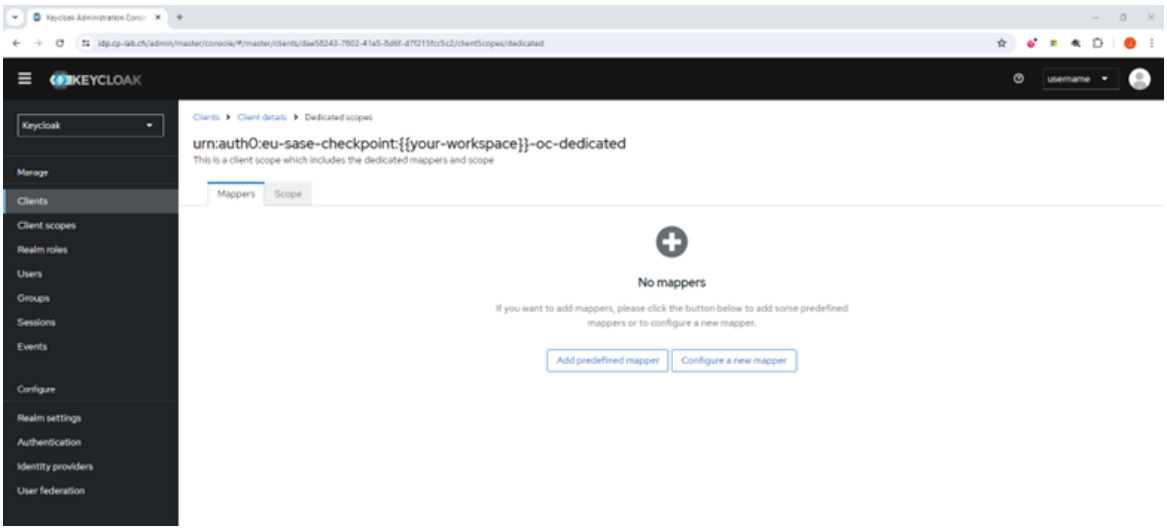
u. Click the **Client scopes** tab.



v. Select the assigned client scope named as your audience URI (SP Entity ID), for example, the name starts with `urn:auth0`.

w. Click the **Mappers** tab.

x. Click **Add predefined mapper**.



y. Select these checkboxes:

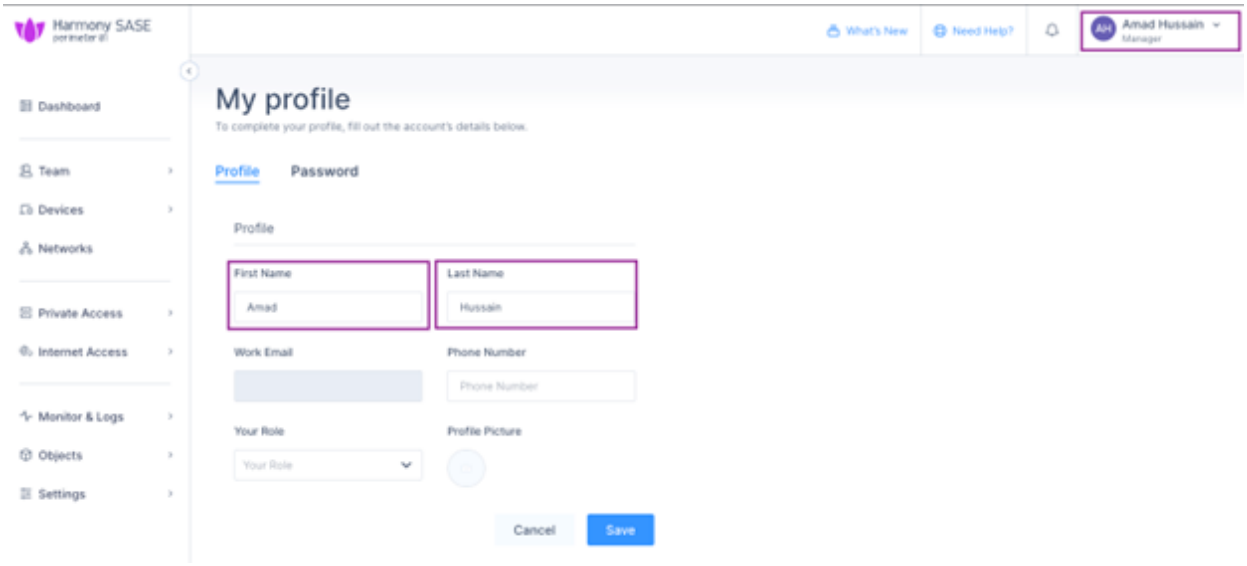
i. **X500 email**

ii. **X500 givenName**

iii. **X500 surname**

This configuration permits to pass through the SAML response the Users given name and surname.

2. To map the user profile, log in to the SASE Administrator Portal, click your profile icon at the top right corner and enter these:

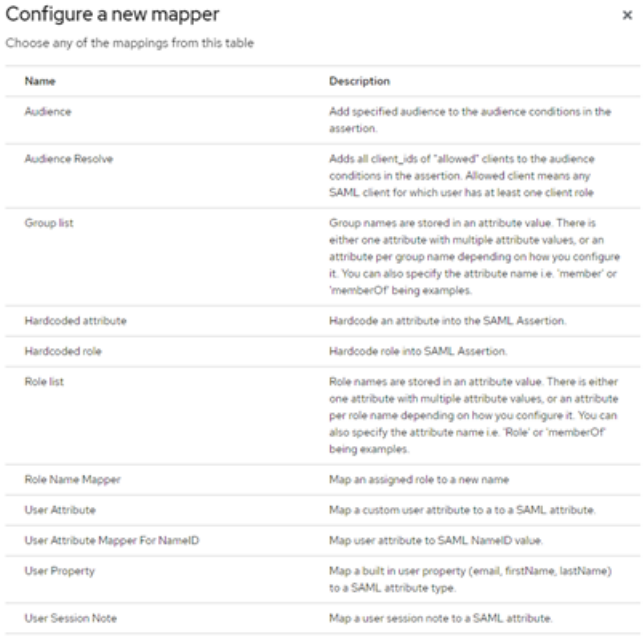


- **First Name**
- **Last Name**

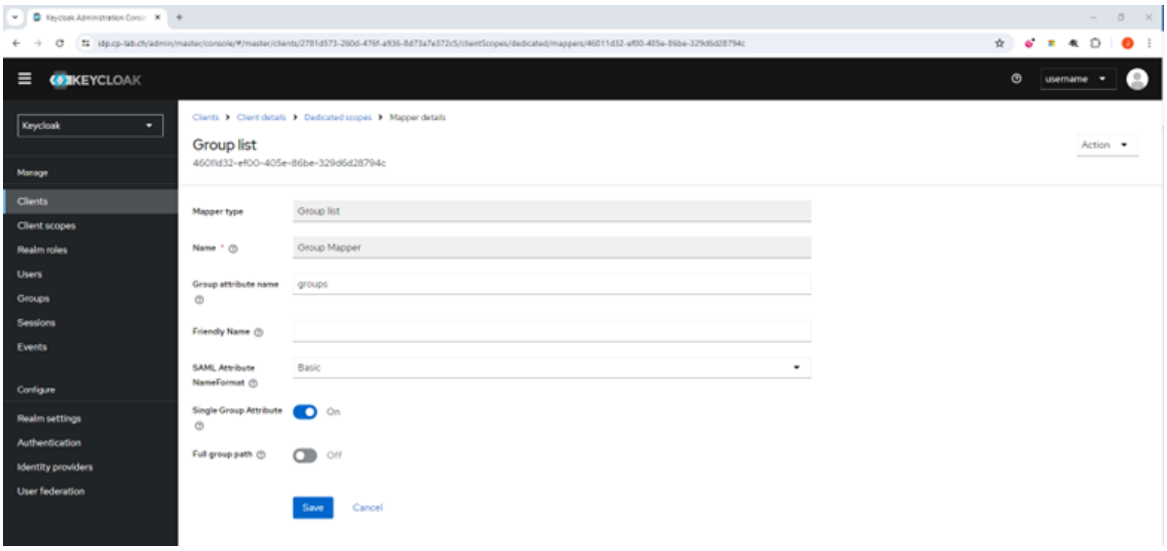
Note - The groups in Keycloak must match the groups in SASE to be able to add the users into the corresponding groups in SASE.

3. Log in to your Keycloak Administration Console:

   a. (Optional) Select **Add mapper**, then **By configuration** and select **Group list** to pass Group membership to SASE.



   b. In the **Name** field, enter **Group Mapper**.



   c. In the **Group attribute name** field, enter **groups**.

   d. From the **SAML Attribute NameFormat** list, select **Basic**.

   e. Turn on the **Single Group Attribute** toggle button.

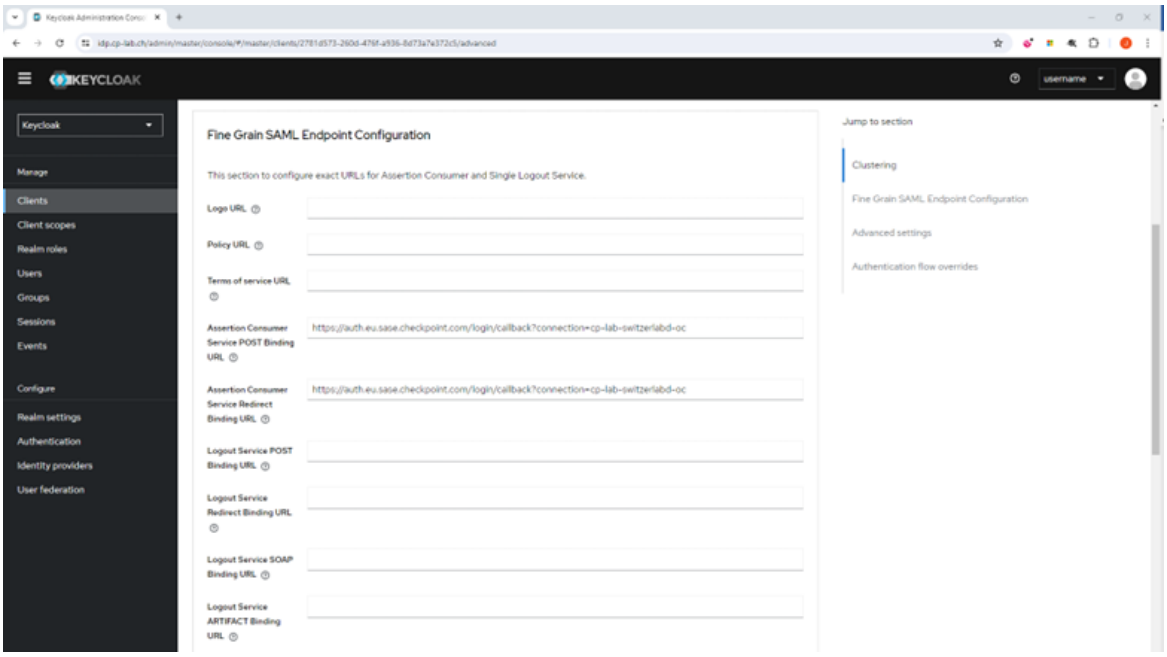
f. Turn off the **Full group path** toggle button.

g. Click **Save**.

h. Go to **Clients** and then click **Create client**.

i. Click the **Advanced** tab.

j. Click **Fine Grain SAML Endpoint Configuration**.



k. In the **Assertion Consumer Service POST Binding URL** field, enter your Single sign-on URL:

- For US based platform - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
- For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

l. In the **Assertion Consumer Service Redirect Binding URL** field, enter your Single sign-on URL:

- For US based platform - **https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc**
- For EU based platform - **https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc**

m. Click **Save**.

n. To collect Sign-in URL and X509 Signing Certificate of your realm to configure the Identity Providers configuration in SASE:

o. Go to **Realm settings**.

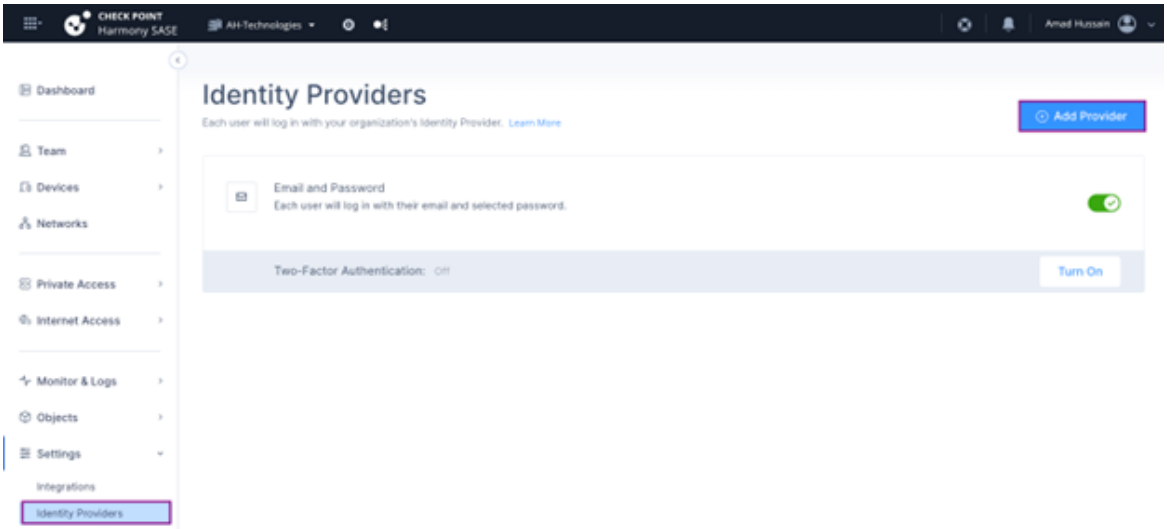
p. Click the **General** tab and click **SAML 2.0 Identity Provider Metadata** under Endpoints.

q. Copy the Sign-in URL and the X509 Signing Certificate.

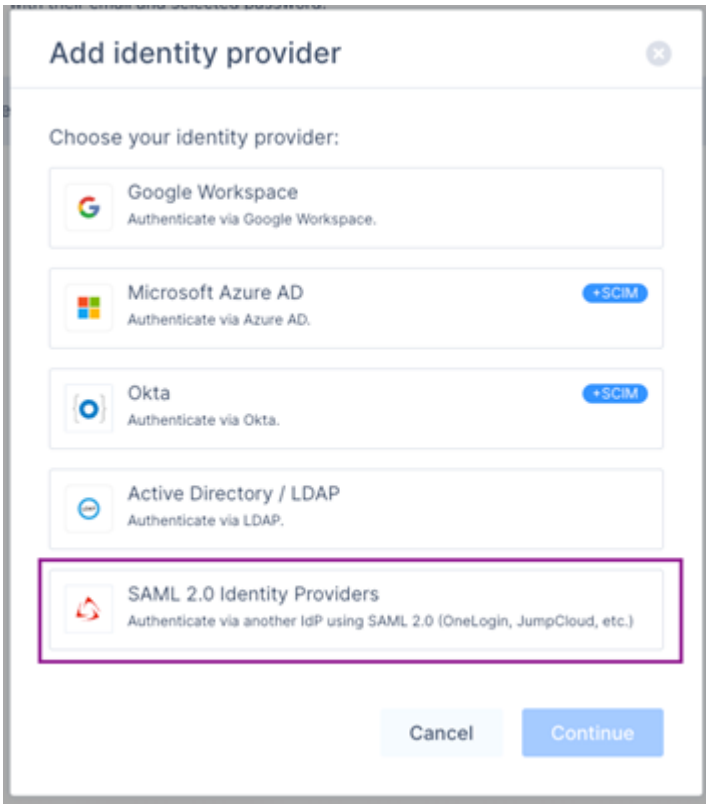
4. To configure SASE, log in to the SASE Administrator Portal:

a. Go to **Settings** > **Identity Providers**.

b. Click **Add Provider**.

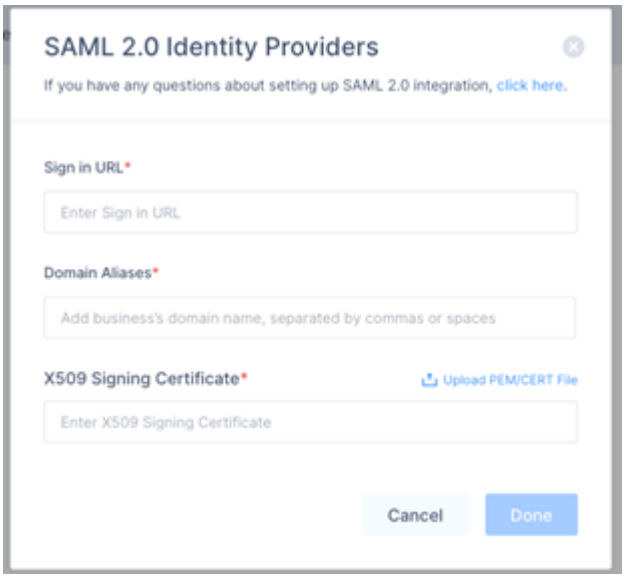


c. Select **SAML 2.0 Identity Providers**.



d. Click **Continue**.

The **SAML 2.0 Identity Providers** window appears.



e. In the **Sign in URL** field, enter the sign-in url copied in step **3.i.i**.

f. In the **Domain Aliases** field, enter your organization domain.

g. In the **X509 Signing Certificate** field, enter the certificate copied in step **3.i.i**.

h. Click **Done**.

OneLogin

Prerequisites

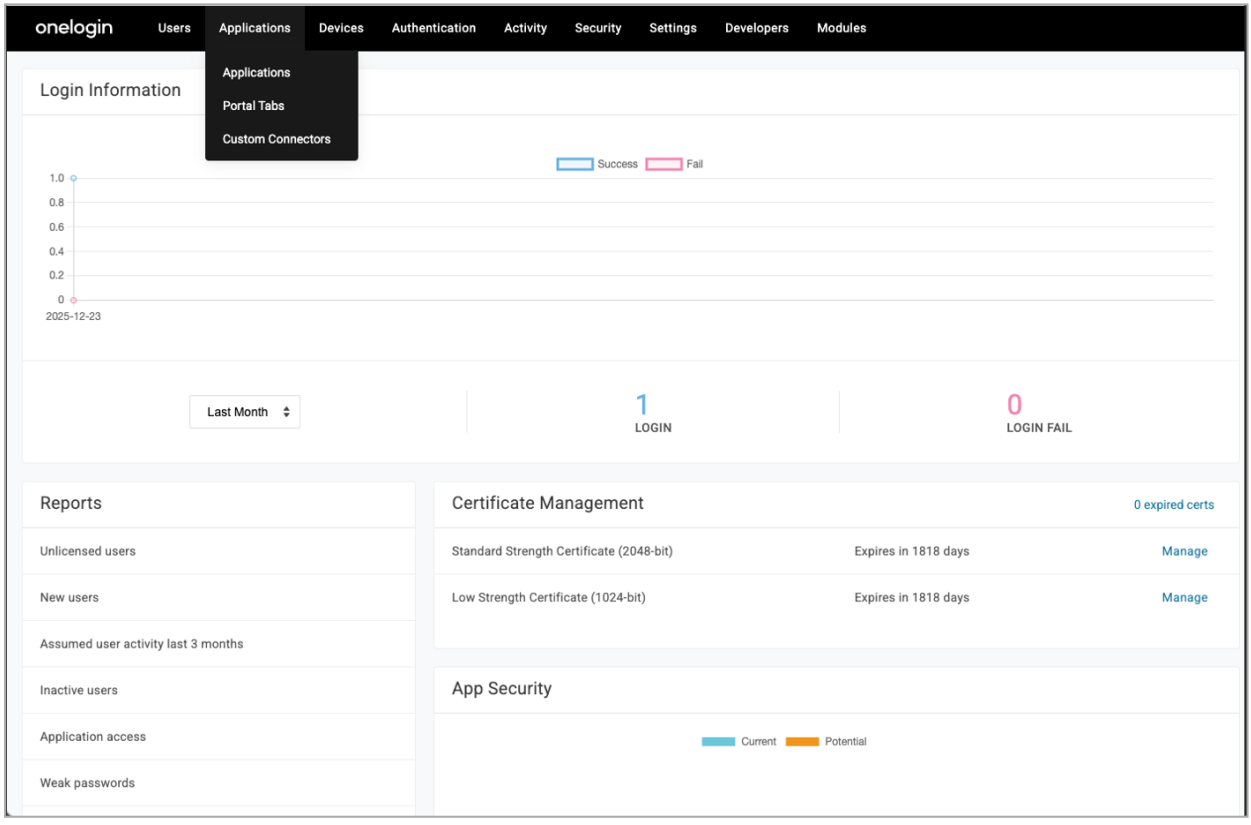
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

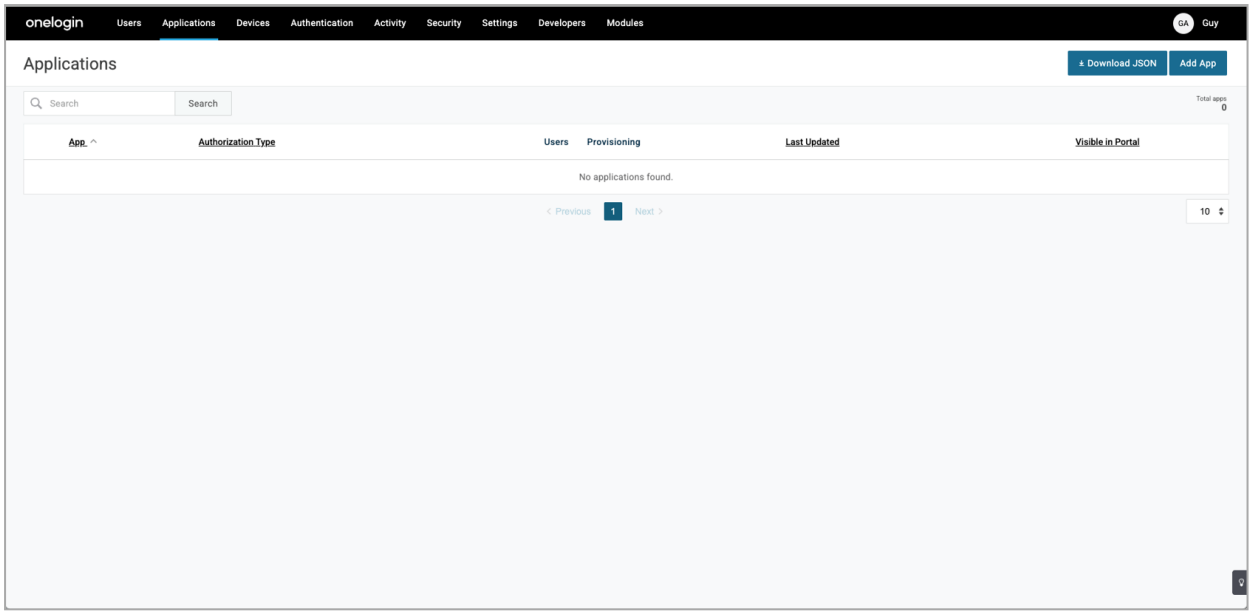
- *"Step 1 - Configure the OneLogin Management Portal" below*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on page 987*

Step 1 - Configure the OneLogin Management Portal

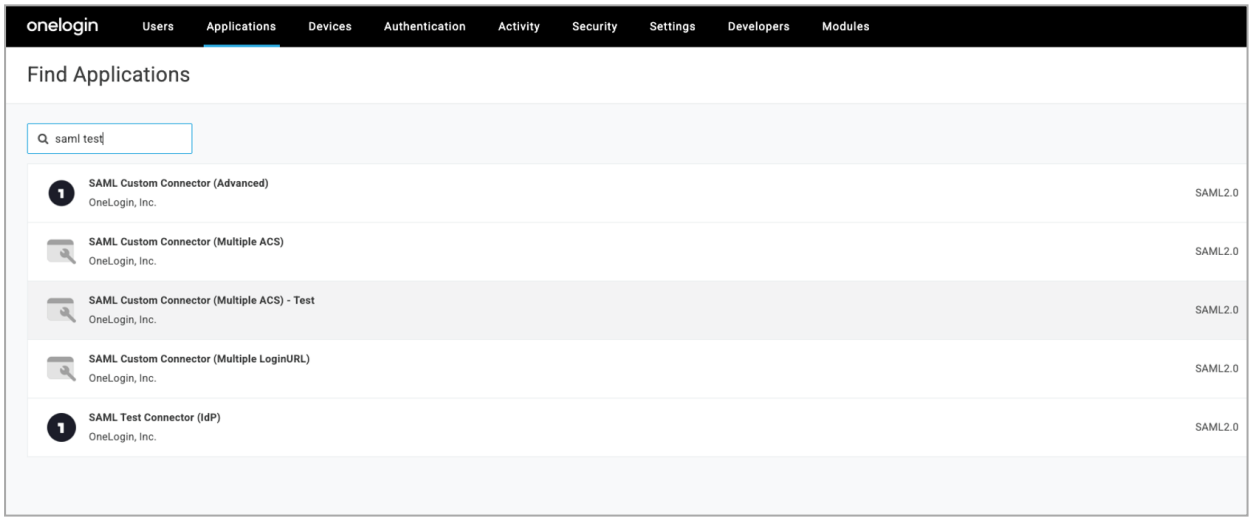
1. Log in to OneLogin Management Portal. If you don't have an account, create one.
2. Go to **Applications** > **Applications**.



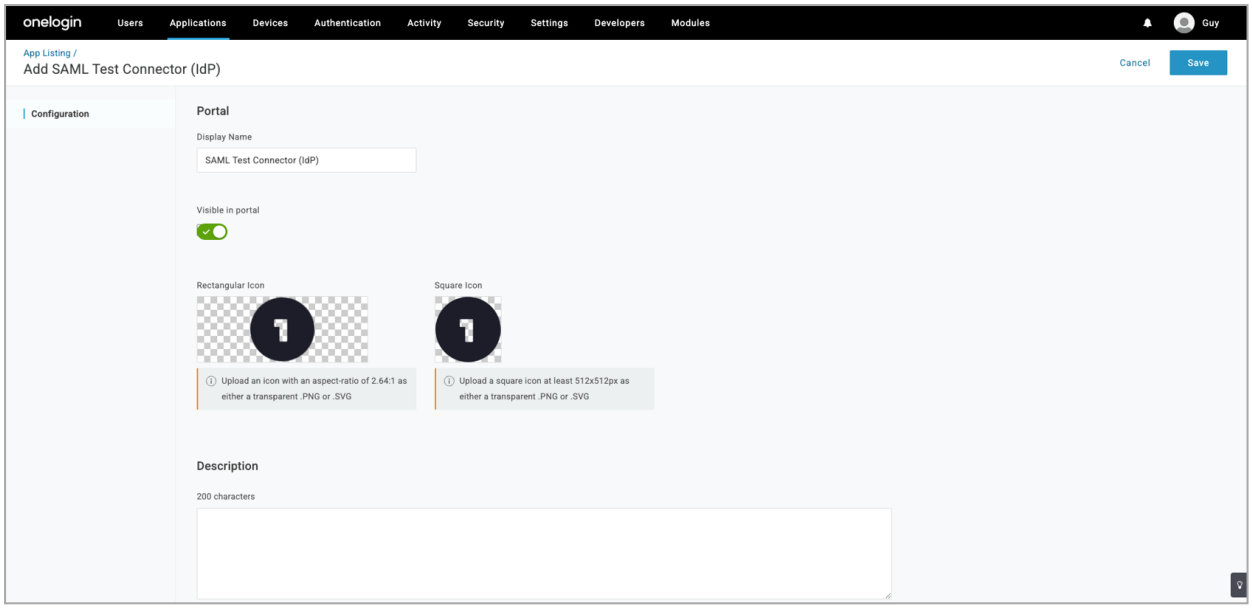
3. Select **Add App**.



4. Search for **saml test**, and select **SAML Test Connector (IdP)**.

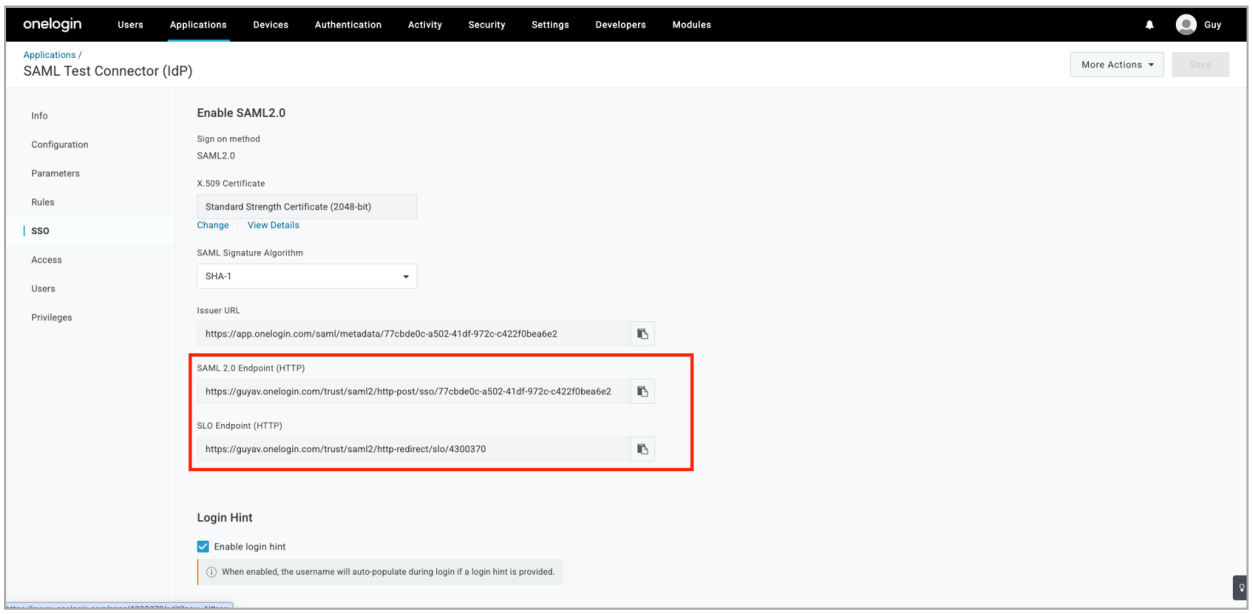


5. Change the **Display Name** to Check Point SASE and click **Save**.

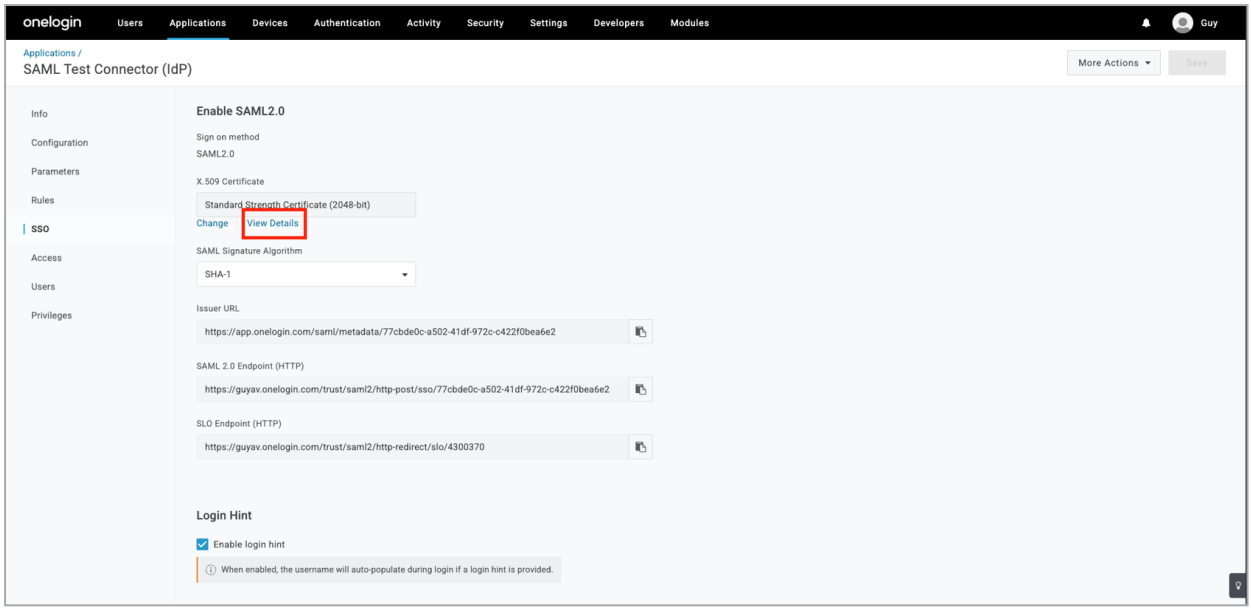


6. Go to the **SSO** tab, and copy these values:

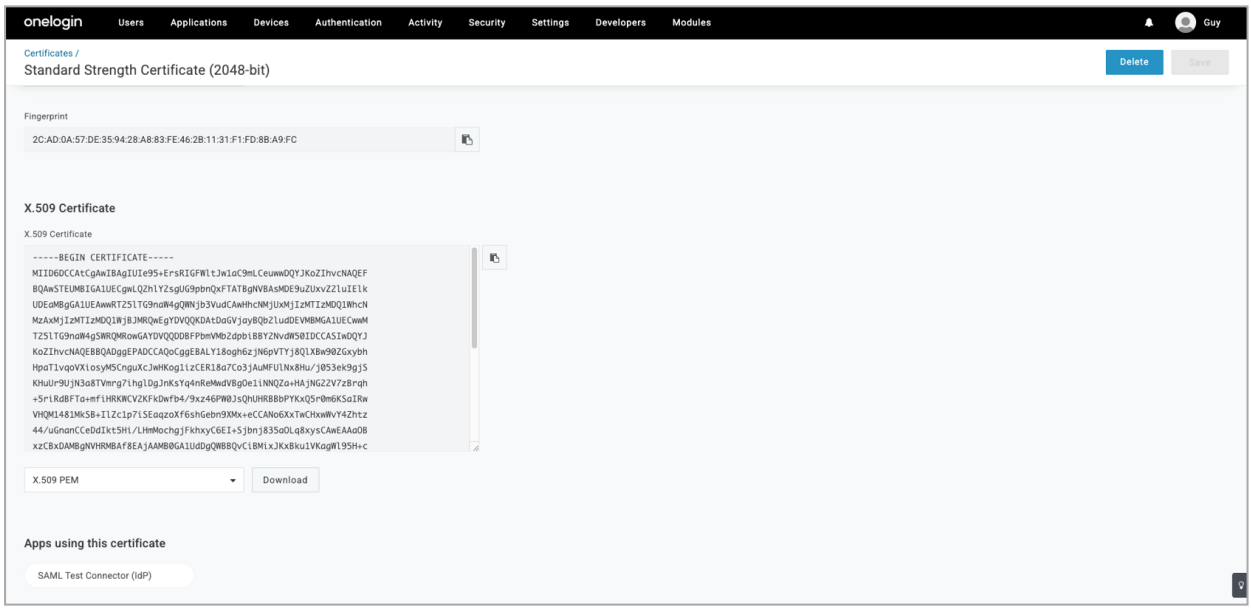
   - SAML 2.0 Endpoint (HTTP) - You need to use this value in the **Sign In URL** field while configuring Check Point SASE Administrator Portal.
   - SLO Endpoint (HTTP).



7. Select the **View Details link** at the X.509 Certificate field.



8. Download the X.509 certificate **onelogin.pem**.



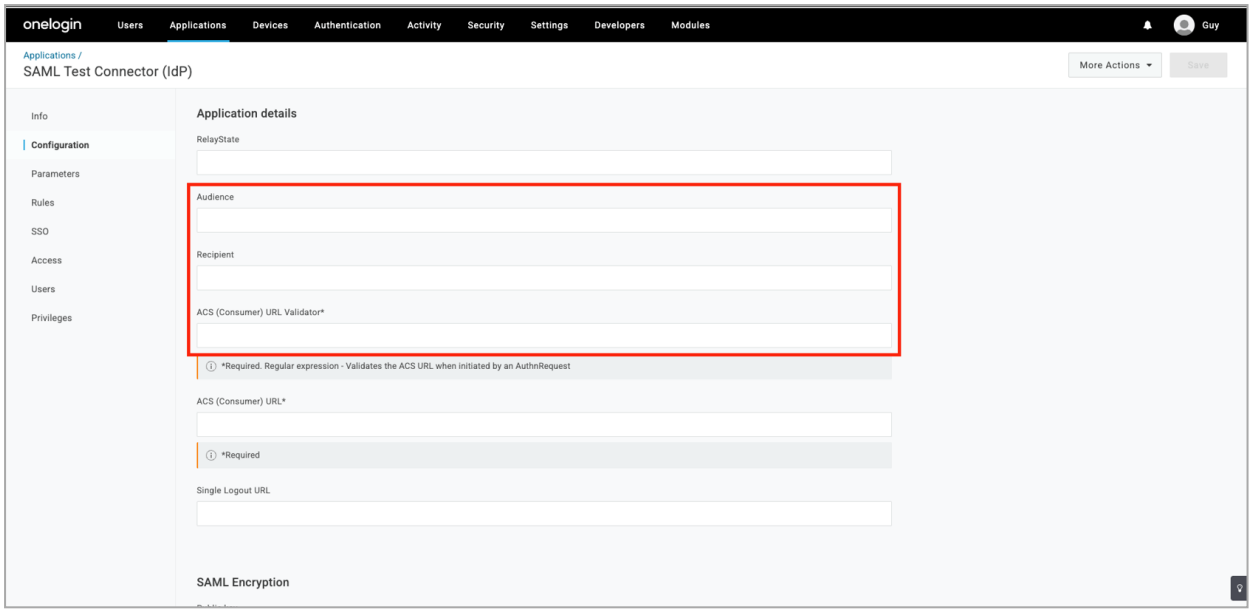
9. Go to the **Configuration** tab.
10. Enter these values into the appropriate fields:

- **Audience**:
  - US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`
  - EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`
  - AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`
  - IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc`

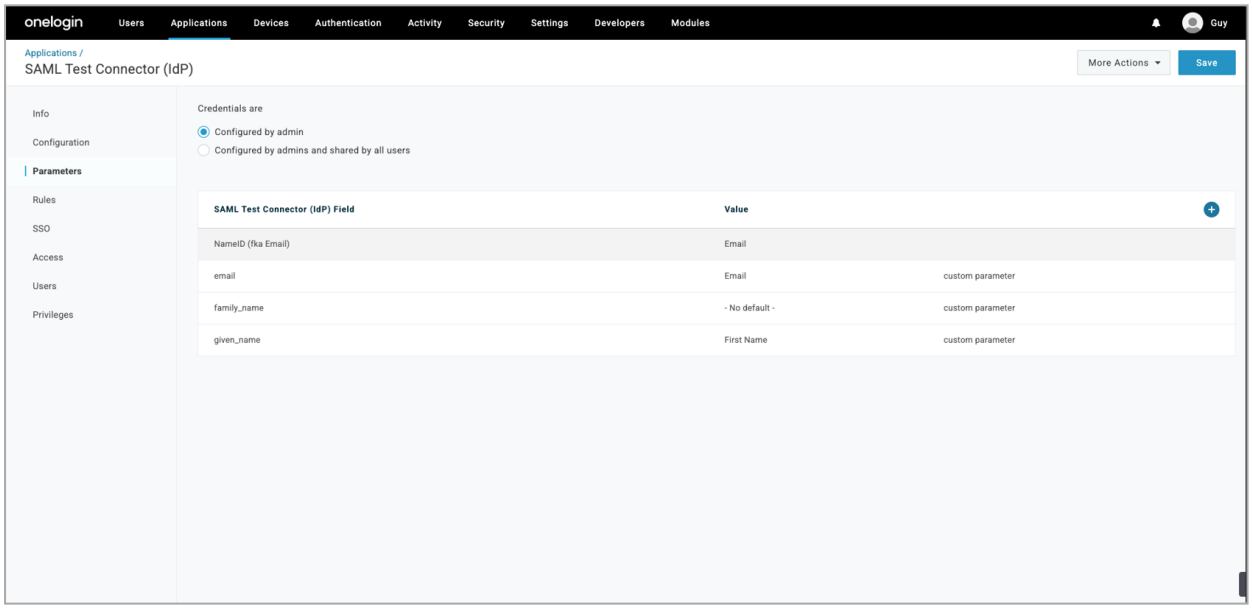
  For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`

- **Recipient**:
  - US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
  - EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

- **ACS (Consumer) URL**:
  - US-based platform:
    `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
  - EU-based platform:
    `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - AU-based platform:
    `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - IN-based platform:
    `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
- **ACS (Consumer) URL Validator**:
  - US-based platform:
    `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
  - EU-based platform:
    `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - AU-based platform:
    `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  - IN-based platform:
    `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`



11. On the **Parameters** tab, select the + sign to **Add Parameter**.



12. In the popup, set a name for your new custom attribute using the **Field name** text box. Make sure you check the Include in the **SAML assertion flag**. Select **Save**.
13. The new attribute you created is displayed. Select the **Value** field, which is currently displaying - **No default**.
14. Change the **No default** value to **Macro**.
15. Add these properties to the Macro:

Field Name	Macro Text Box Value	SAML Assertion Flag
email	{email}	Checked

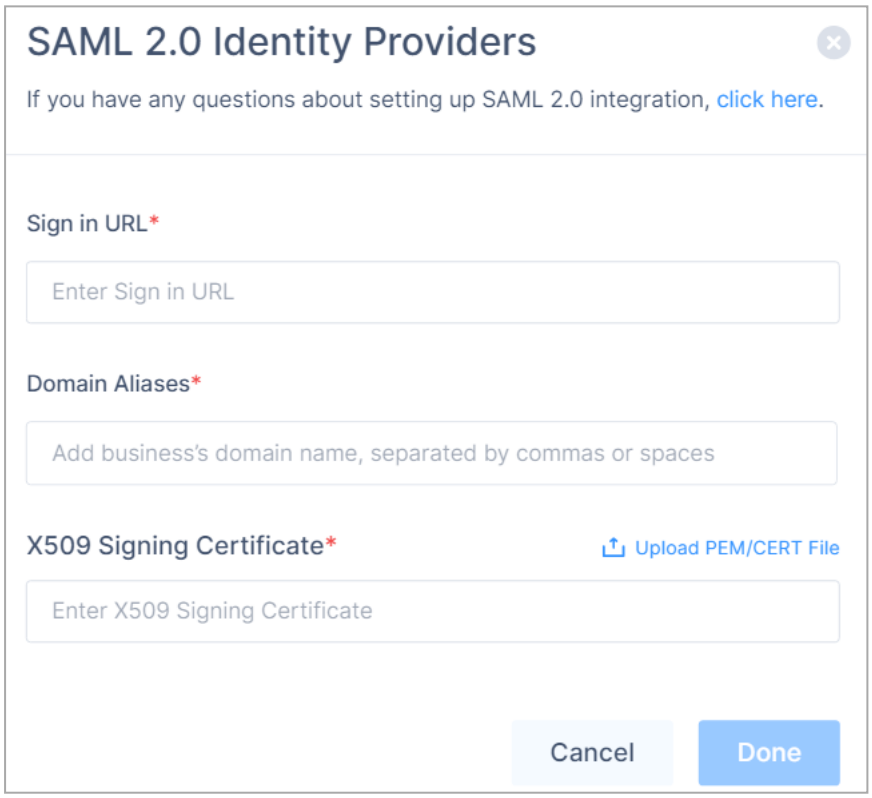
Field Name	Macro Text Box Value	SAML Assertion Flag
given_name	{firstname}	Checked
family_name	{lastname}	Checked

16. Click **Save**.

Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

PingOne for Enterprise

Prerequisites

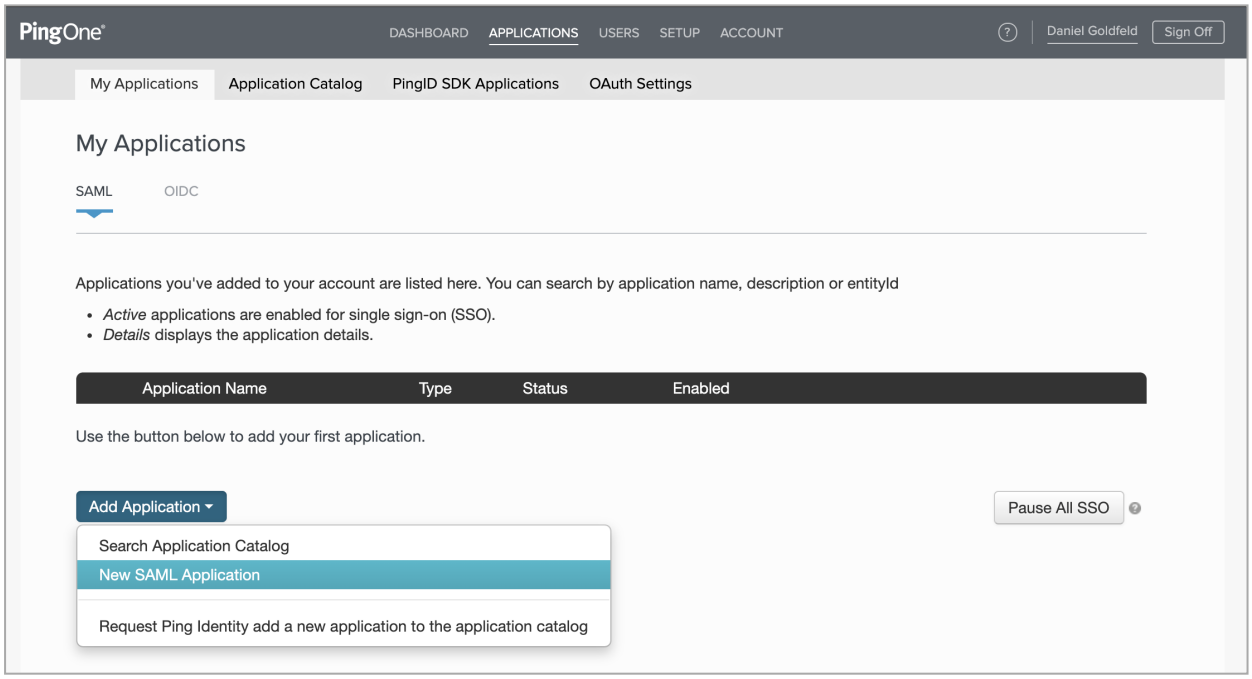
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the PingOne Management Portal" below*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on page 993*

Step 1 - Configure the PingOne Management Portal

1. Log in to PingOne Management Portal.
2. From the top navigation bar, click **Applications**.
3. In the **SAML** tab, click **Add Application** and then select **New SAML Application**.



The **New Application** window appears.

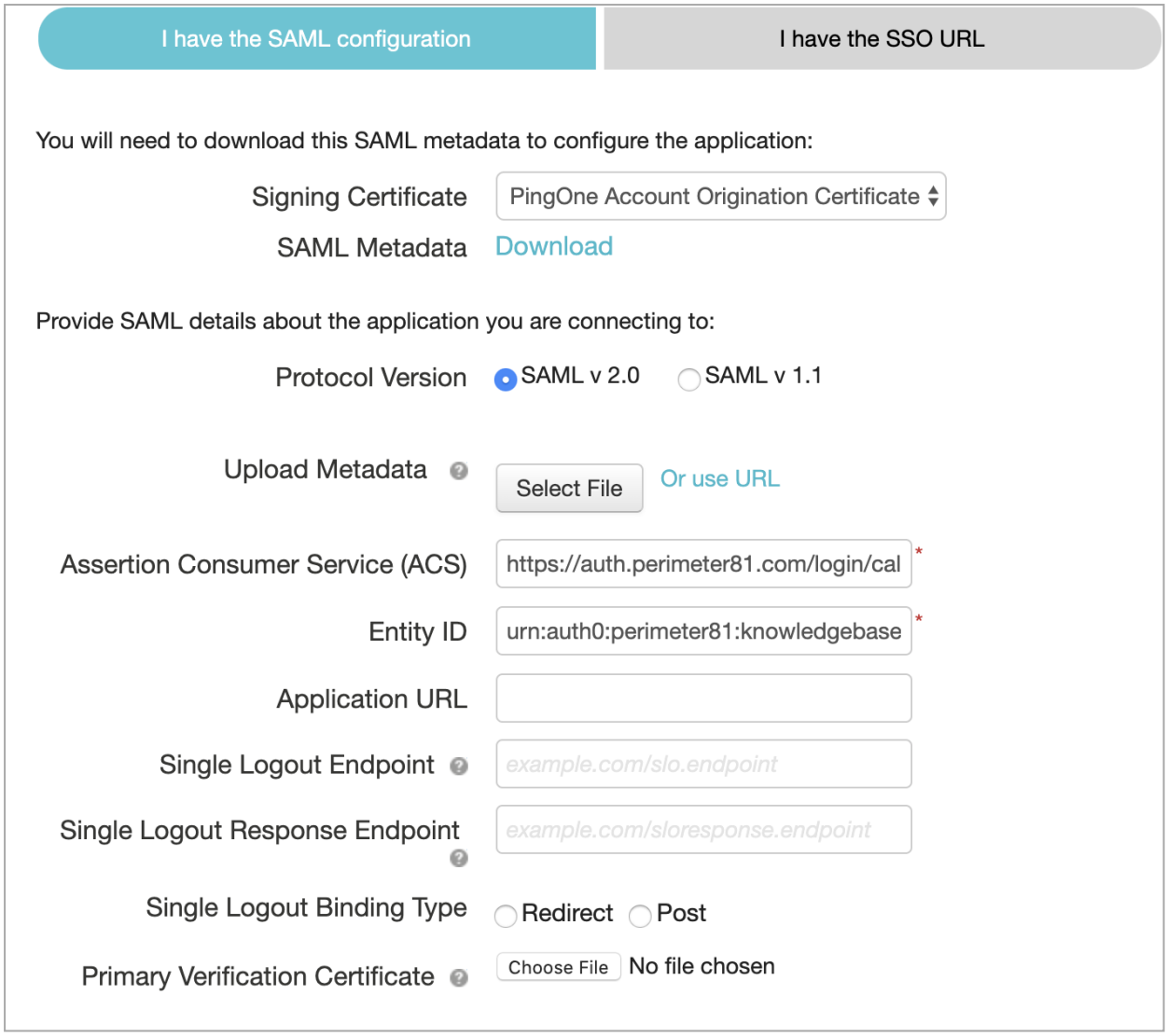
4. Enter these details:
   - **Application Name**: Check Point SASE
   - **Application Description**: Check Point SASE SAML Connection

- **Category**: Information Technology
- **Graphics**: (Optional) Add the Check Point SASE logo

5. Click **Continue to Next Step**.

   The **Application Configuration** window appears.

6. Click **I have the SAML configuration** and then enter these details:
   - **Signing Certificate**: PingOne Account Origination Certificate
   - **Protocol Version**: SAML v 2.0
   - **Assertion Consumer Service (ACS)**: US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
   - **Entity ID**: US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`

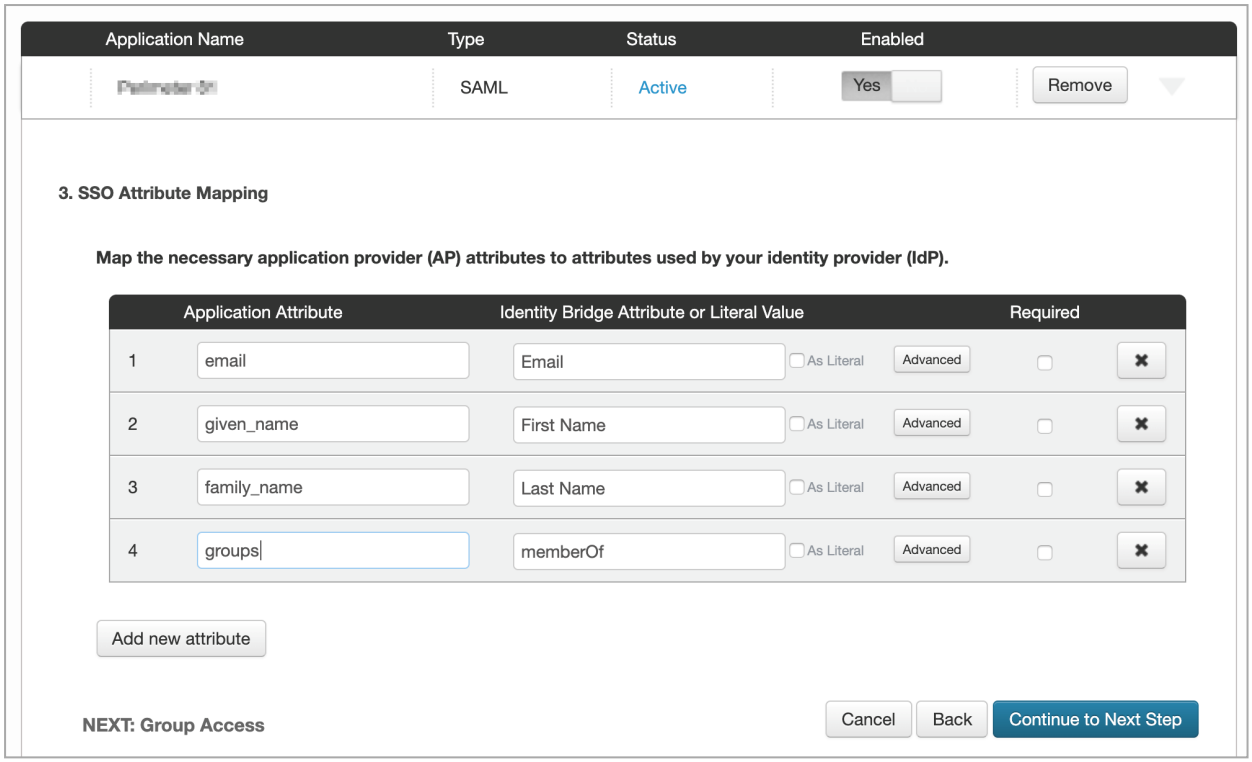


7. Click **Continue to Next Step**.

   The **SSO Attribute Mapping** window appears.

8. Map these attributes:

Application Attribute	Identity Bridge Attribute or Literal Value
email	Email
given_name	First Name
family_name	Last Name
groups	memberOf



9. Click **Continue to Next Step**.

   The **Group Access** window appears.

10. Select the user groups that need access to the PingOne for Enterprise login page.

    Note - To allow access to all users, add **Users@Directory**.

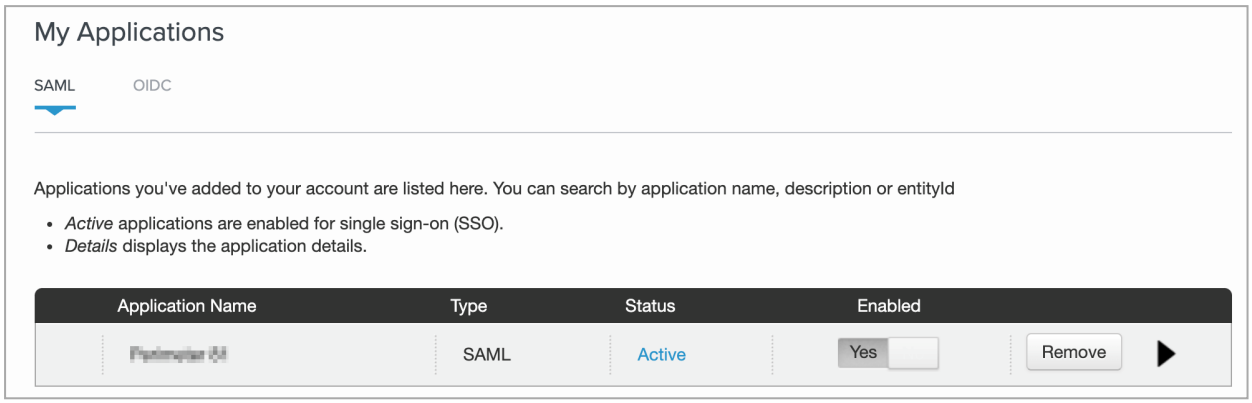
11. Click **Continue to Next Step**.

    The **Review Setup** window appears.

12. Copy the **idpid**.

13. Click **Download** to download the **Signing Certificate**.

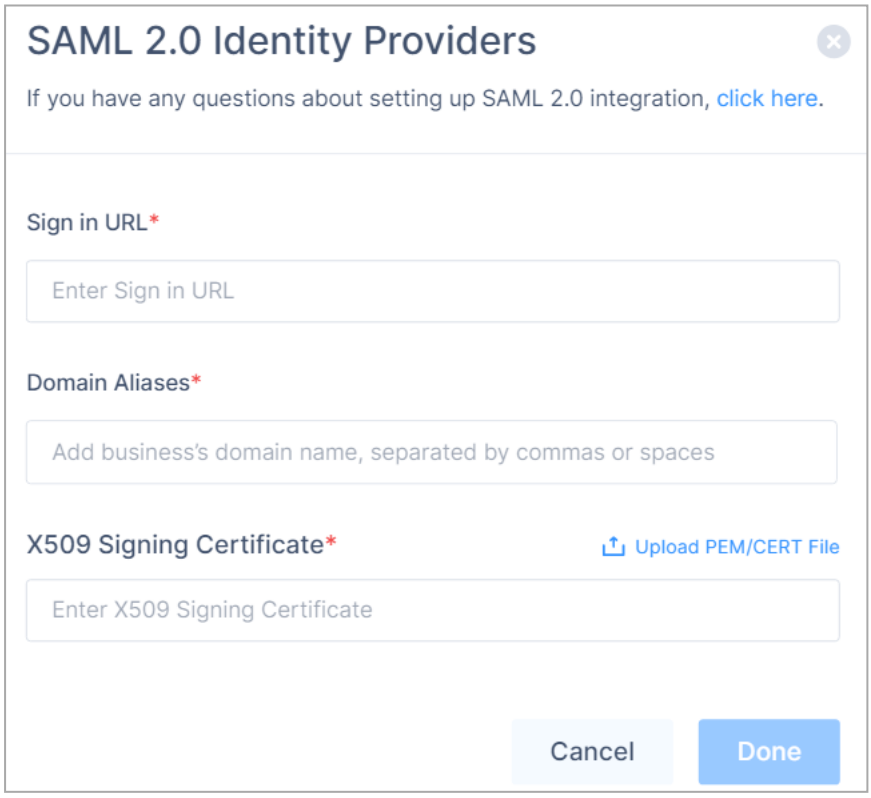
14. Click **Save and Close**.
15. Go to **My Applications** and ensure that the Check Point SASE application is set to **Enabled - Yes**.



Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

PingFederate

Prerequisites

- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the PingFederate Management Portal" below*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on the next page*

Step 1 - Configure the PingFederate Management Portal

1. Log in to PingFederate Management Portal.
2. Go to **SP Connections** and click **Create New**.
3. Select **Browser SSO Profiles** as **Connection Type**.
4. Select **Browser SSO** as **Connection Options**.
5. Configure the parameters and map the attributes.
   - **Entity ID**: US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`
   - **Assertion Consumer Service URL**: US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

- **SAML Request**: HTTP-Redirect Binding
- **SAML Response**: HTTP-POST Binding
- Attributes:

Check Point SASE Attribute	PingFederate Attribute
email	Mail
given_name	Given Name
family_name	Surname

6. Configure **Browser SSO**.
   a. In the SAML Profiles, select **SP-Initiated SSO** and **SP-Initiated SLO**.
   b. Go to **Assertion Creation** section and select **Configure Assertion**.
   c. Accept all defaults for the next two screens.
7. Go to **IdP Adapter Mapping** section and select the existing authentication or add a new one.

   Note - Auth0 only requires the NameIdentifier claim. All other attributes will be passed further to the end application.
8. Configure **Protocol Settings**.

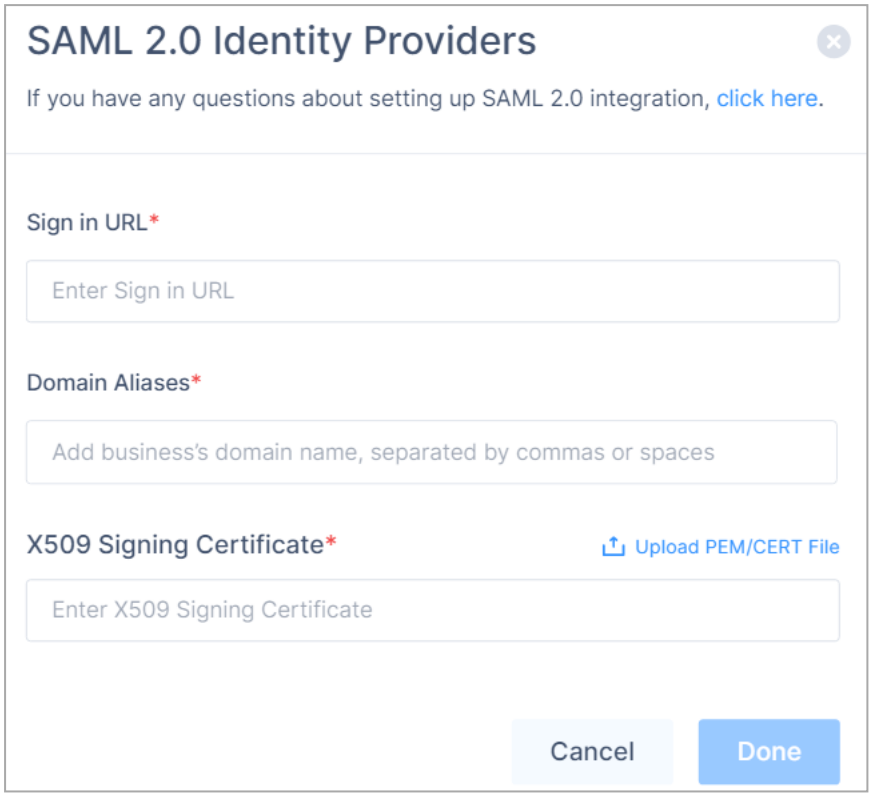
   Values for **Protocol Settings** are imported from the metadata file. Next, you will see the Assertion Consumer Service URL and the Sign-Out URLs. Click Next to the Allowable SAML Bindings section.
9. Leave POST and Redirect enabled. Make sure SAML Assertion is always signed.
10. Configure Credentials. On Digital Signature Settings, select your signing certificate and make sure you check the option to include it in the element.
11. Configure the certificate used to sign incoming requests.
12. Review your settings and set as Active or Inactive.
13. Click Save at the bottom of the screen. You should see the new SP Connection on the Main screen.

Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

The **Add identity provider** pop-up appears.

4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`

Identity Provider	Sign in URL
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Rippling

Prerequisites

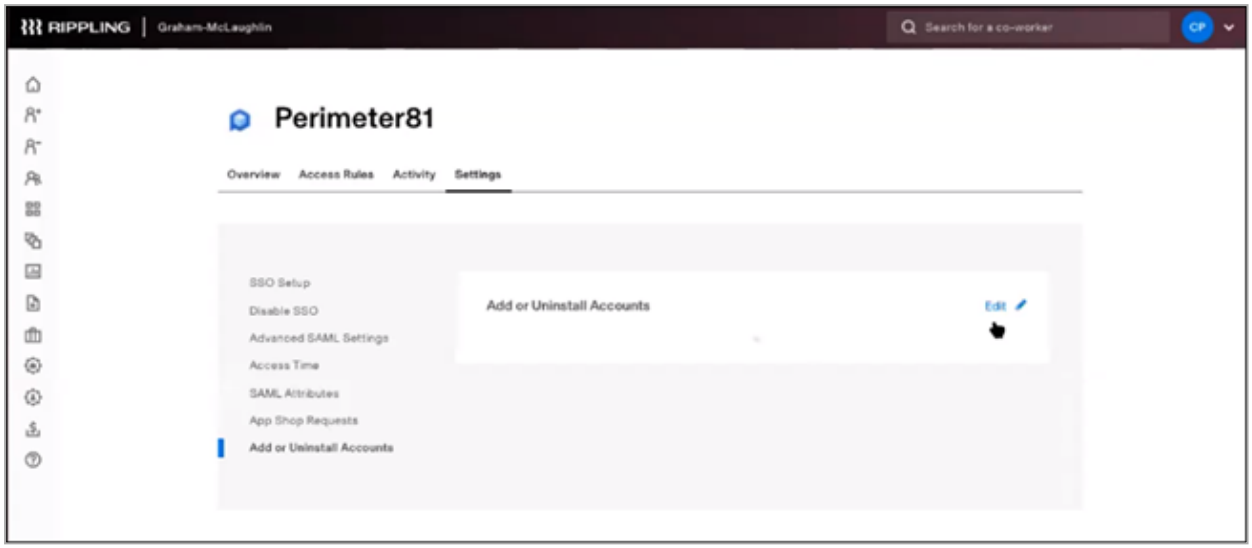
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

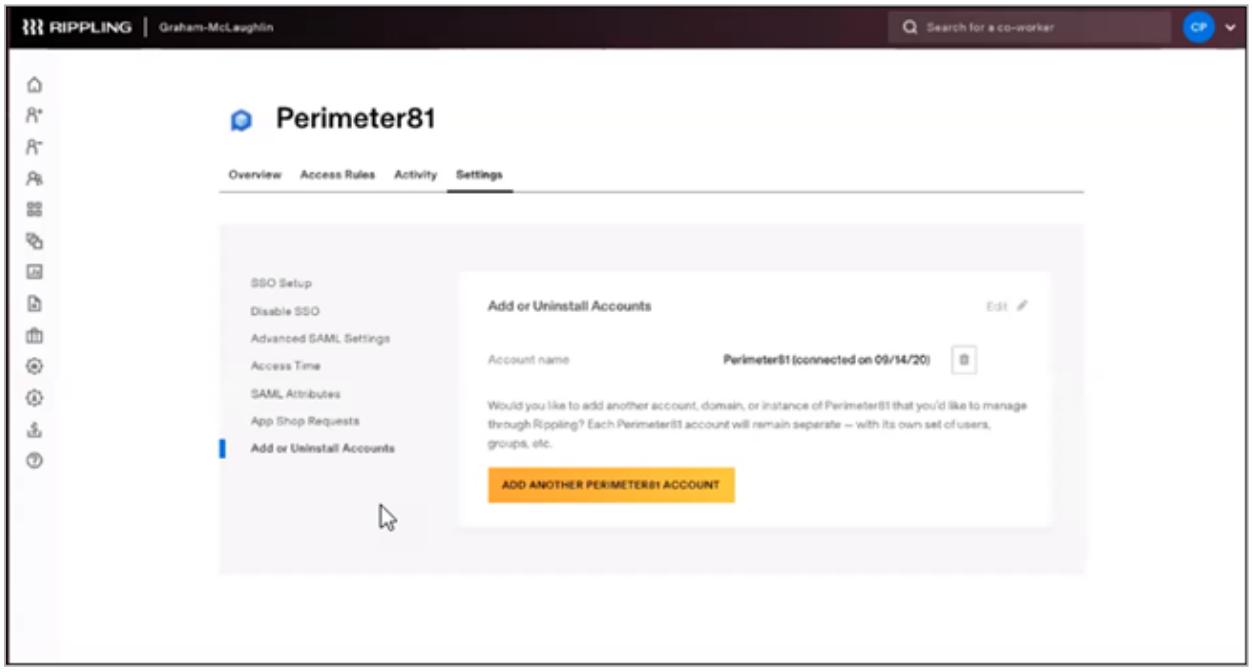
- *"Step 1 - Configure the Rippling Management Portal" on the next page*
- *"Step 2 - Configure the Check Point SASE Administrator Portal" on page 1005*

Step 1 - Configure the Rippling Management Portal

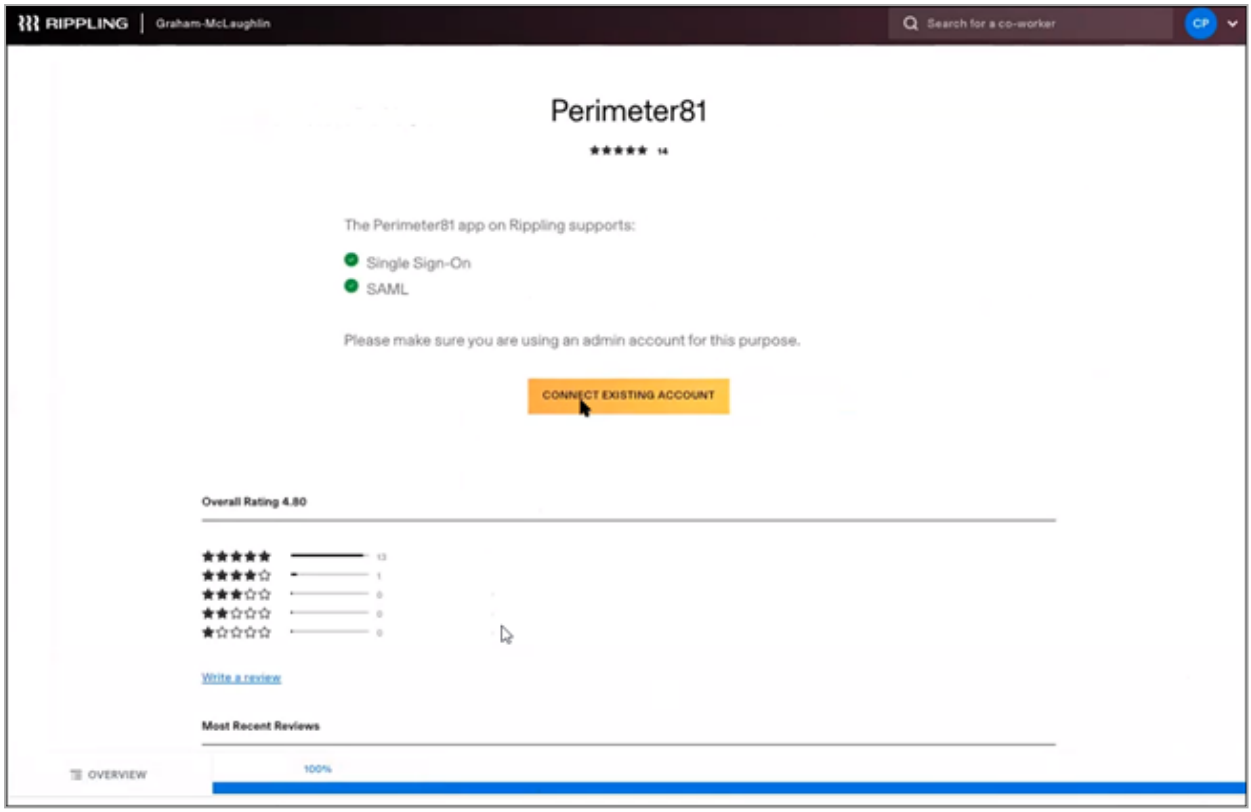
1. Log in to Rippling Management Portal.
2. Go to **Settings** tab and click **Add or Uninstall Accounts**.



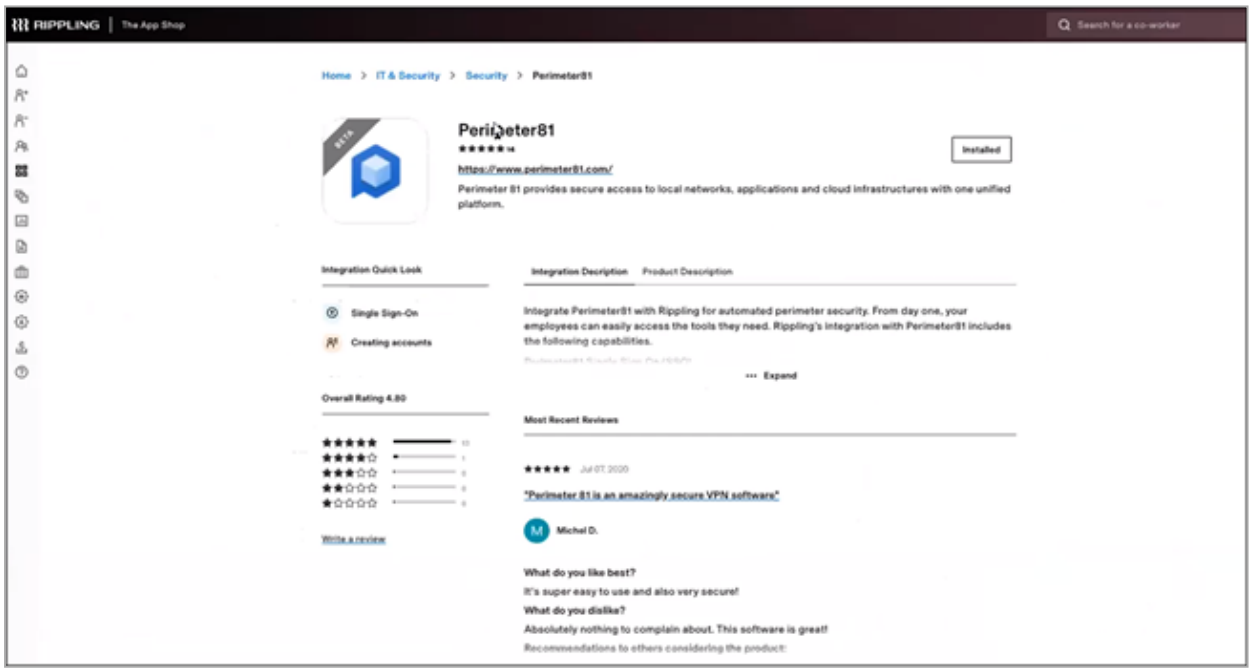
3. Click **Add Another Check Point SASE Account**.



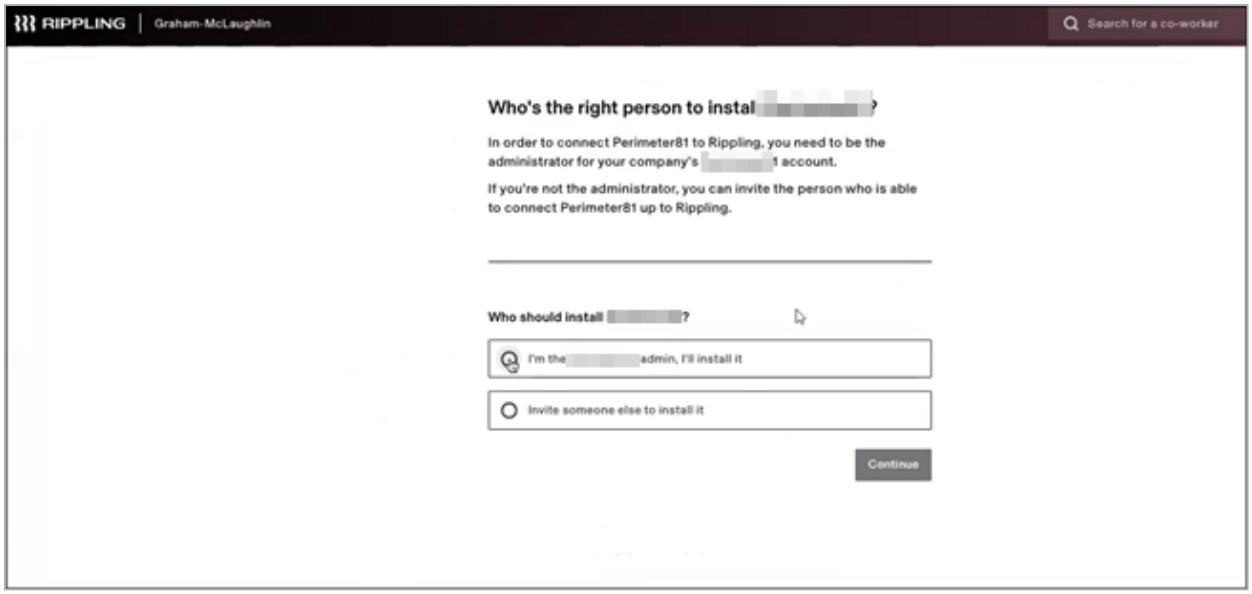
4. Click **Connect Existing Account**.



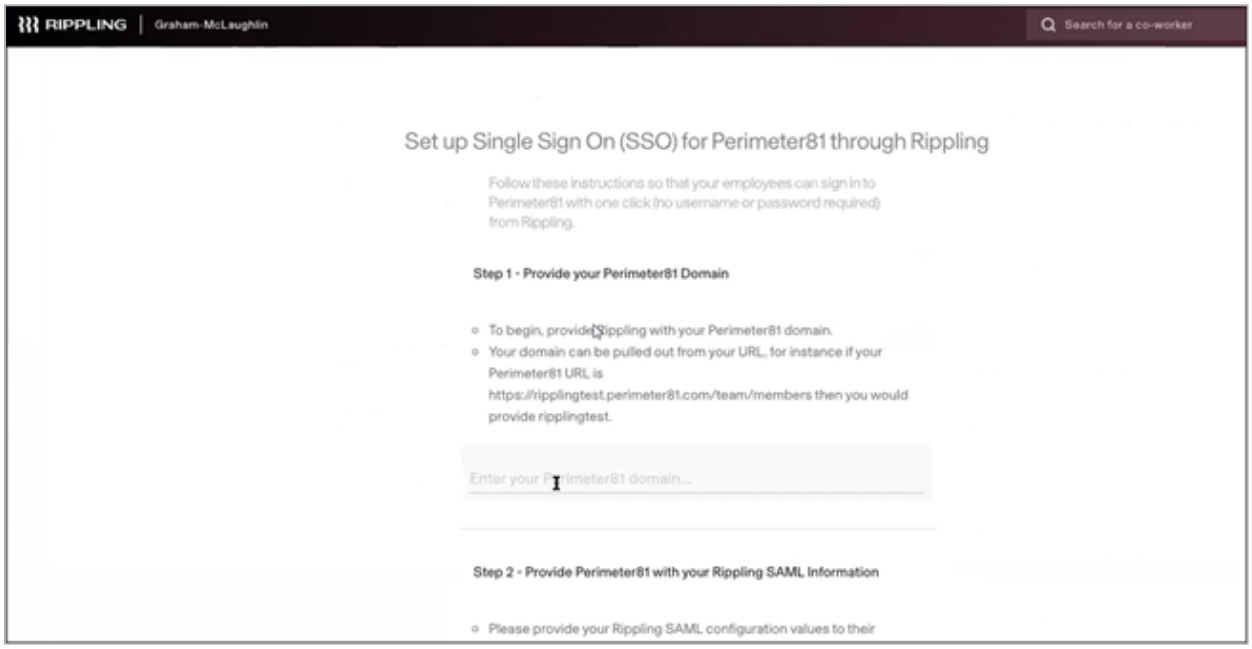
5. Click **Install**.



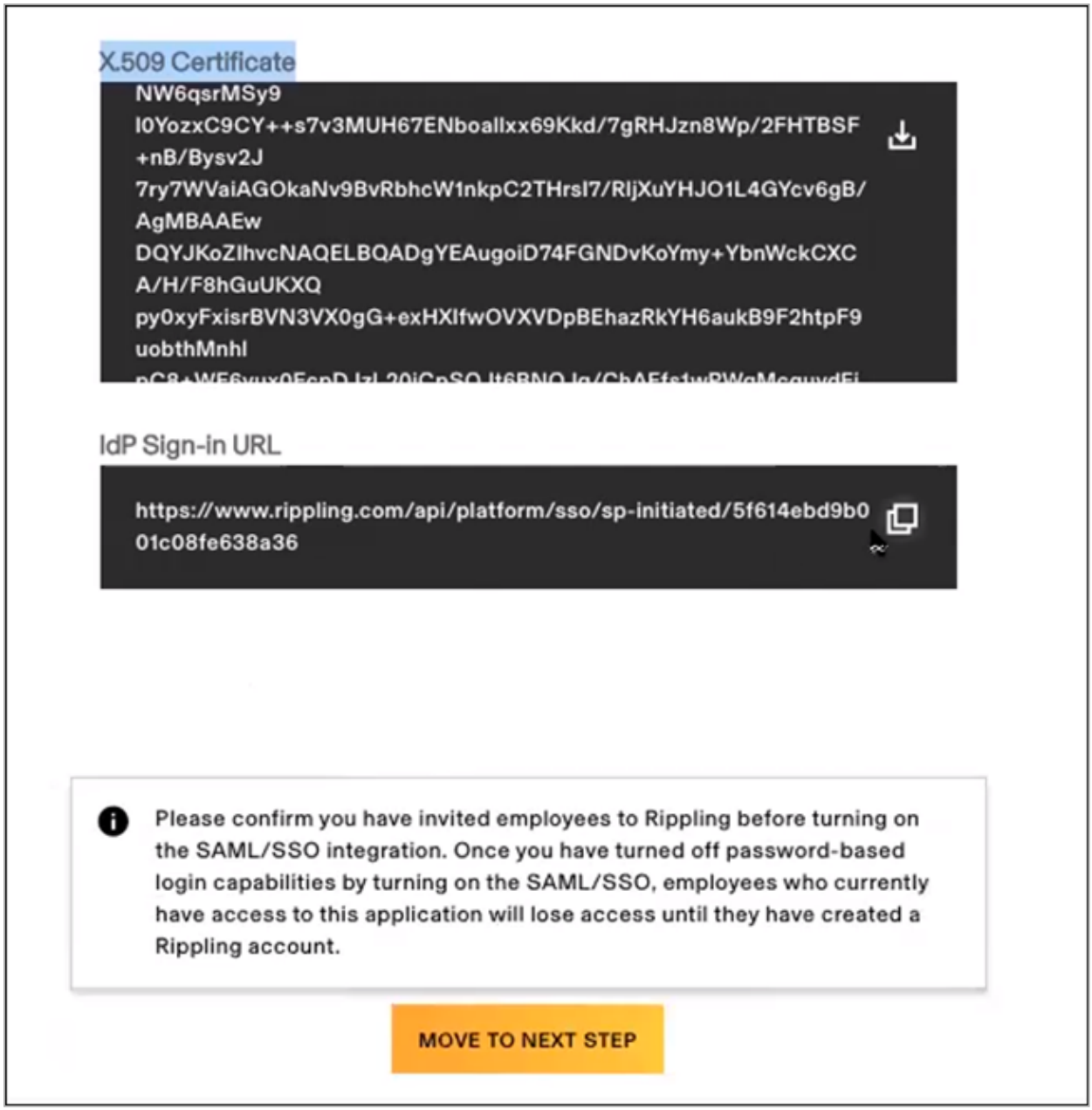
6. Select who should install Check Point SASE and click **Continue**.



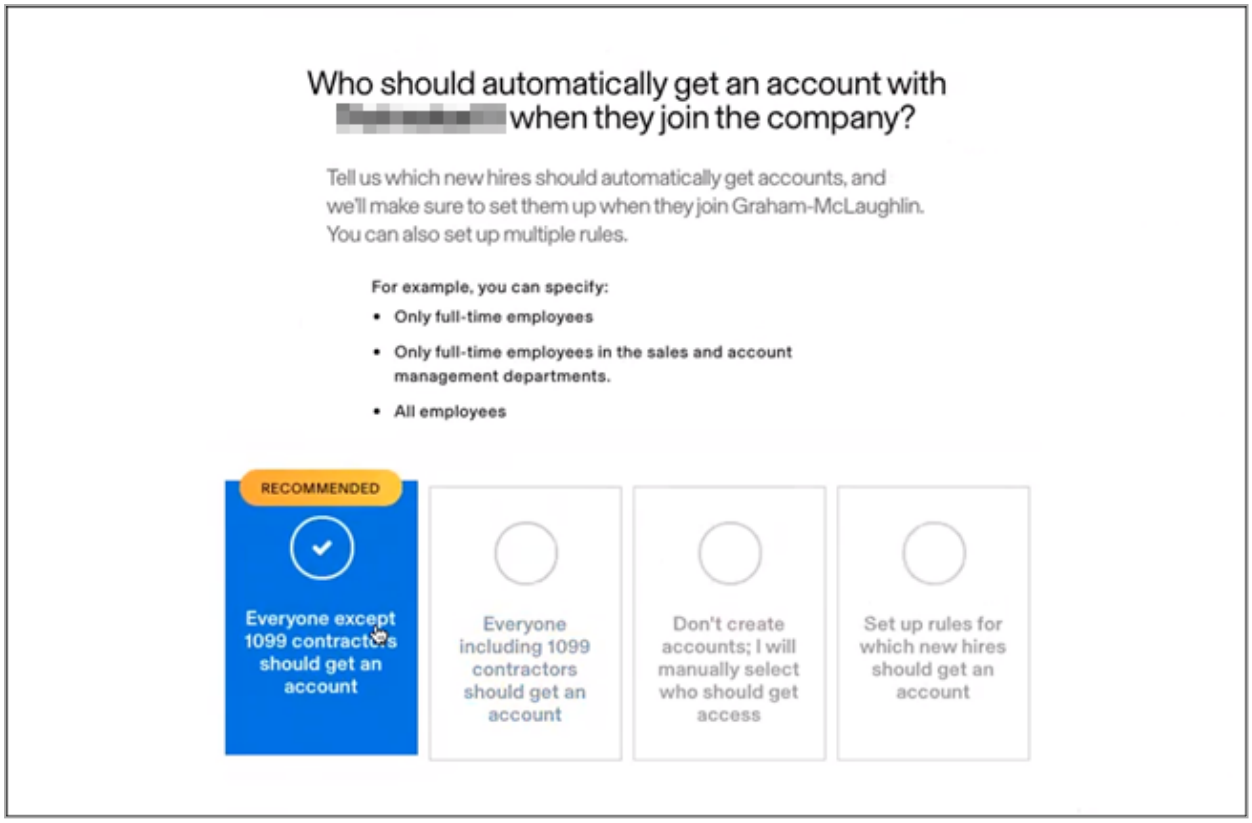
7. In **Step 1 - Provide your Check Point SASE Domain**, enter your Check Point SASE domain name.



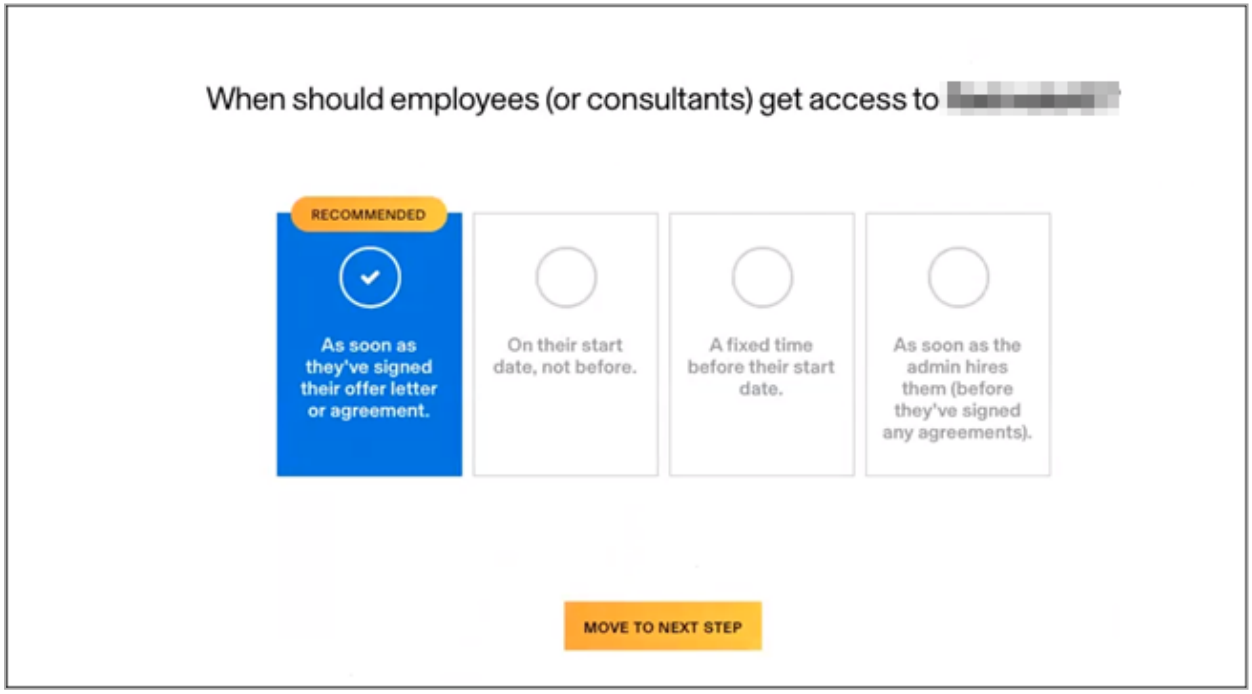
8. Copy or download the **X.509 Certificate**.



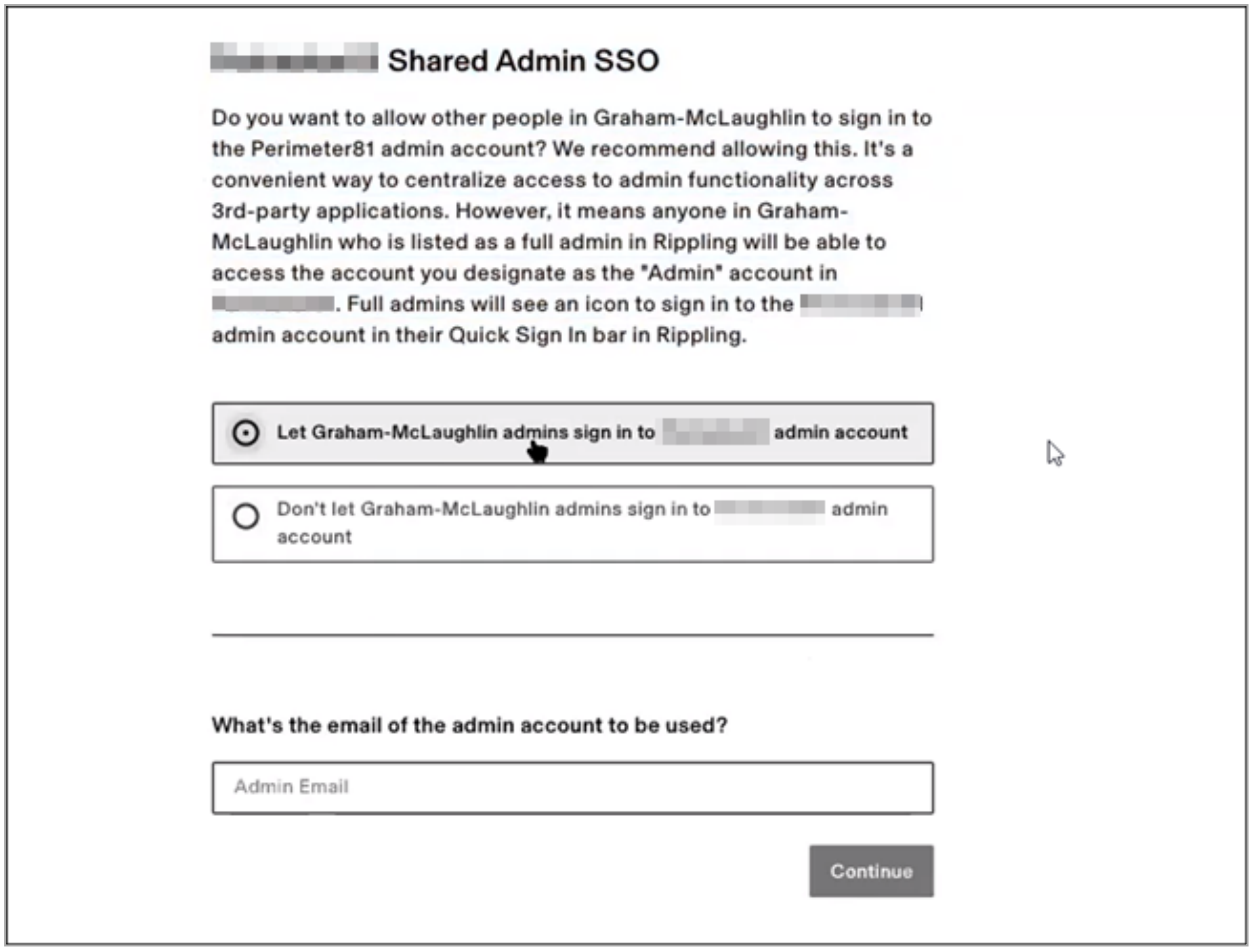
9. Copy the **IdP Sign-in URL** and click **Move to Next Step**.
10. Select who will get a Check Point SASE account when they join the company and click **Move to Next Step**.



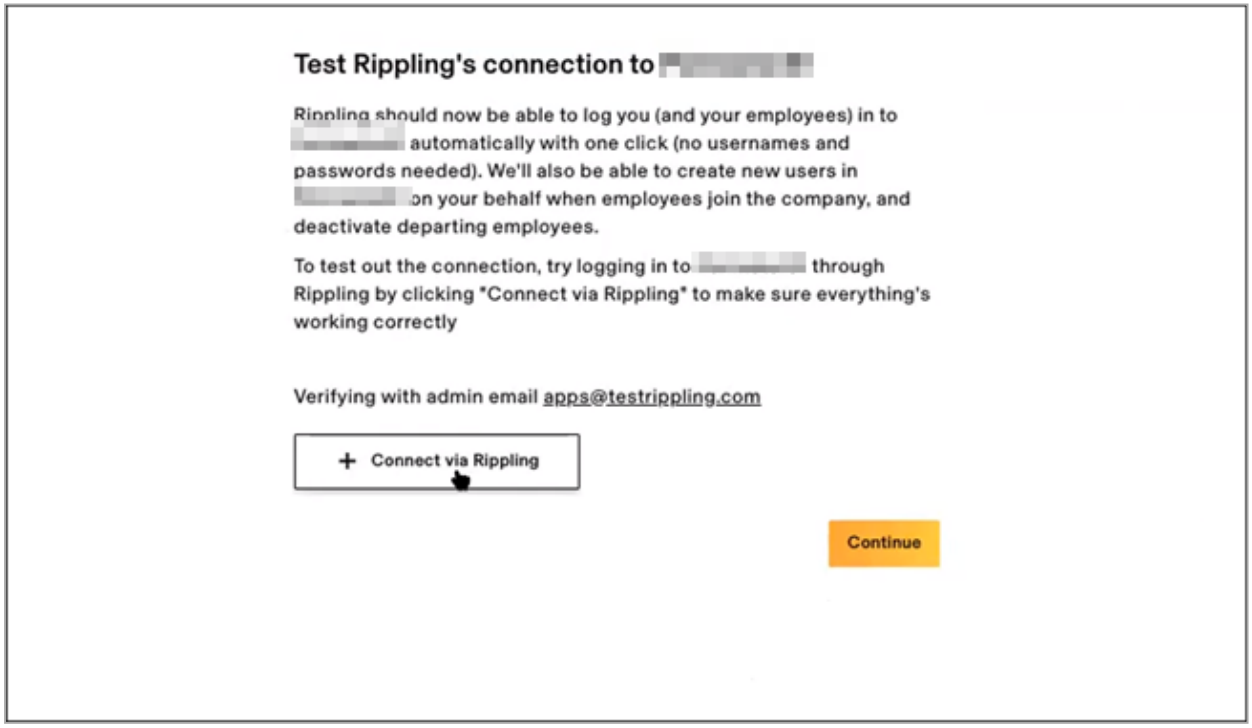
11. Select when employees or consultants should get access to Check Point SASE and click **Move to Next Step**.



12. Select if you want to allow other individuals to sign into the account and then click **Continue**.

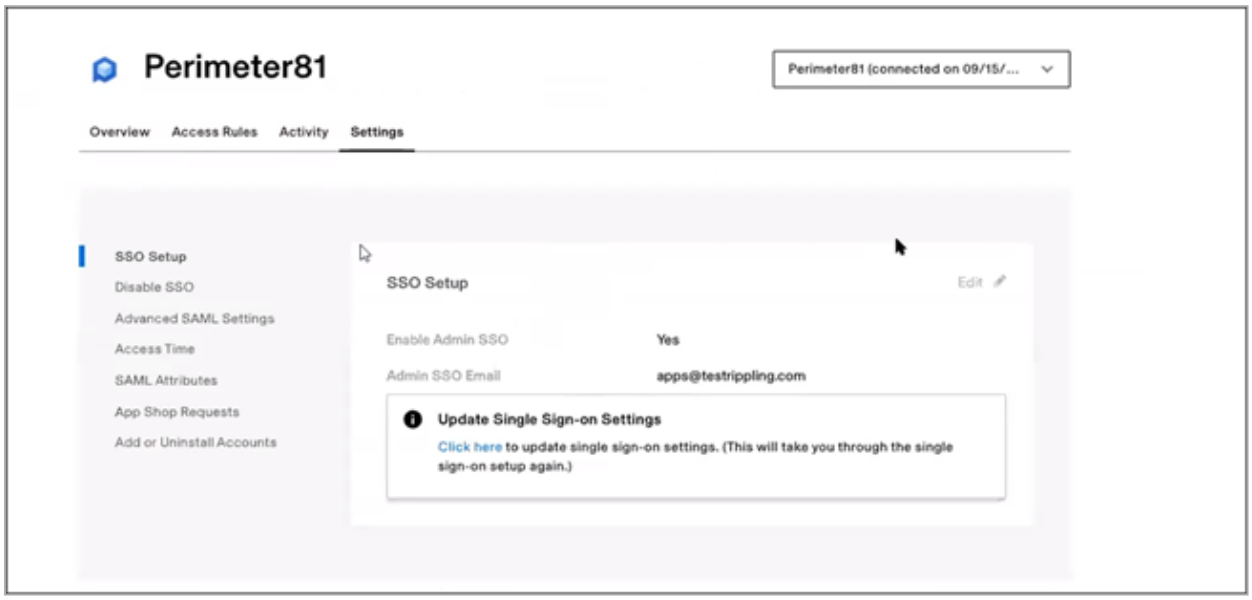


13. Click **Connect via Rippling** to test the connection and then click **Continue**.



14. Wait for the application to complete installation and then open the application.

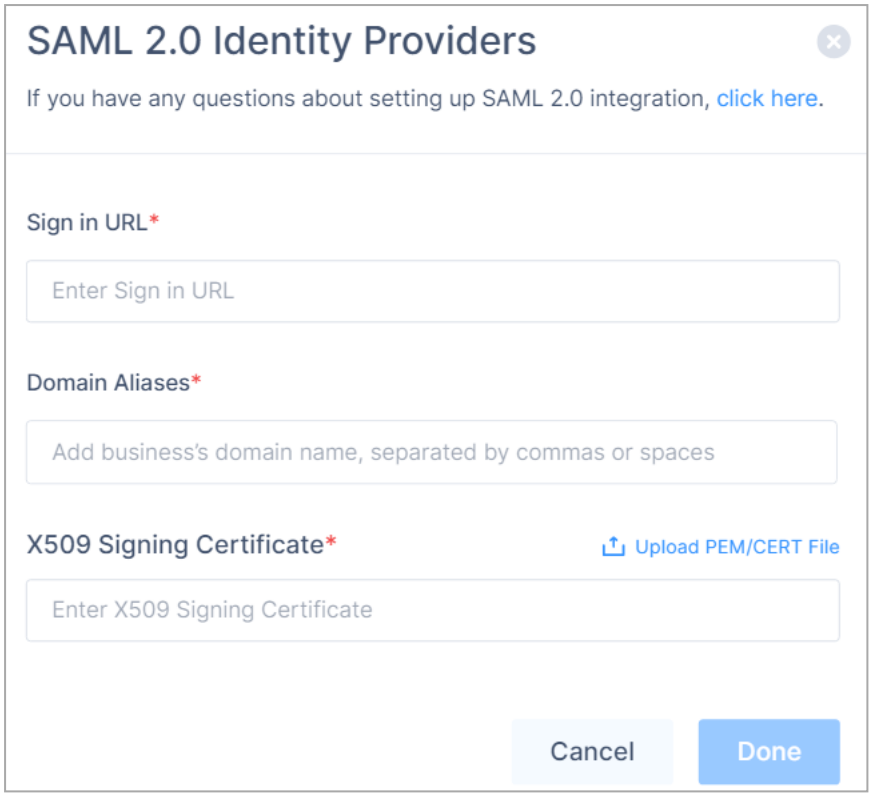
15. Go to the **Settings** tab and then enter the Check Point SASE information.



Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

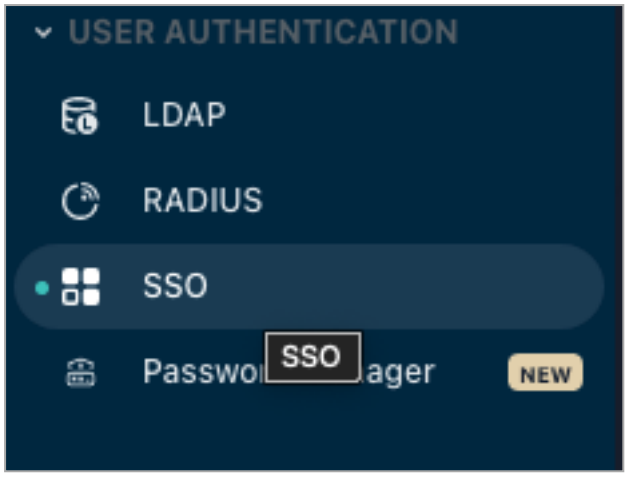
Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

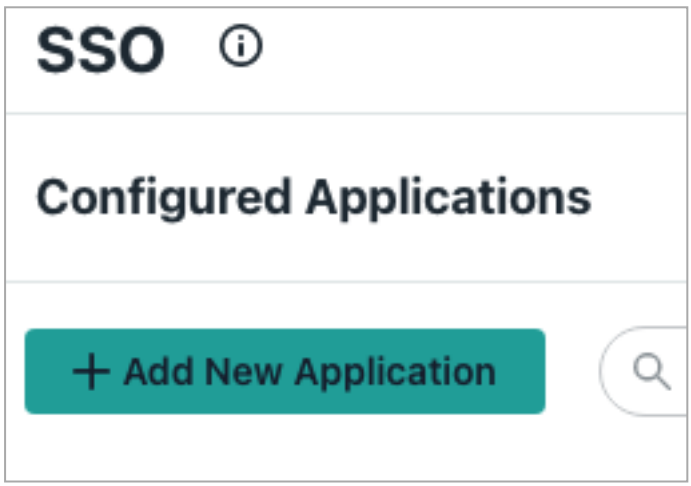
JumpCloud

Step 1 - Configure your JumpCloud Management Portal

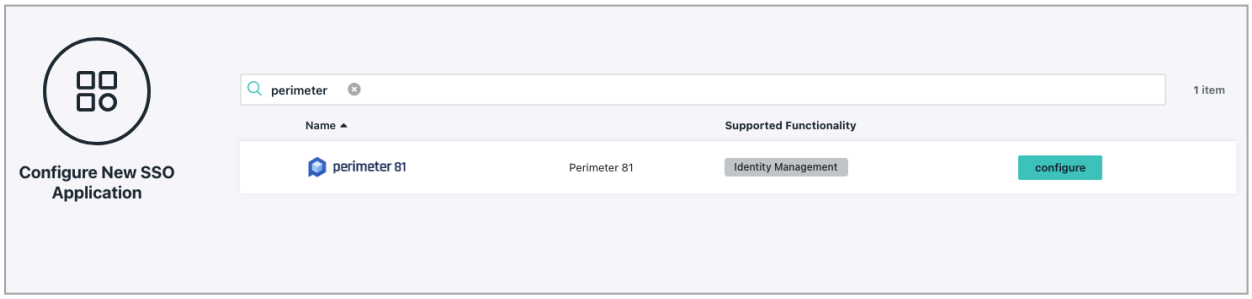
1. Log in to JumpCloud Management Portal.
2. From the main navigation panel, click **User Authentication** and select **SSO**.



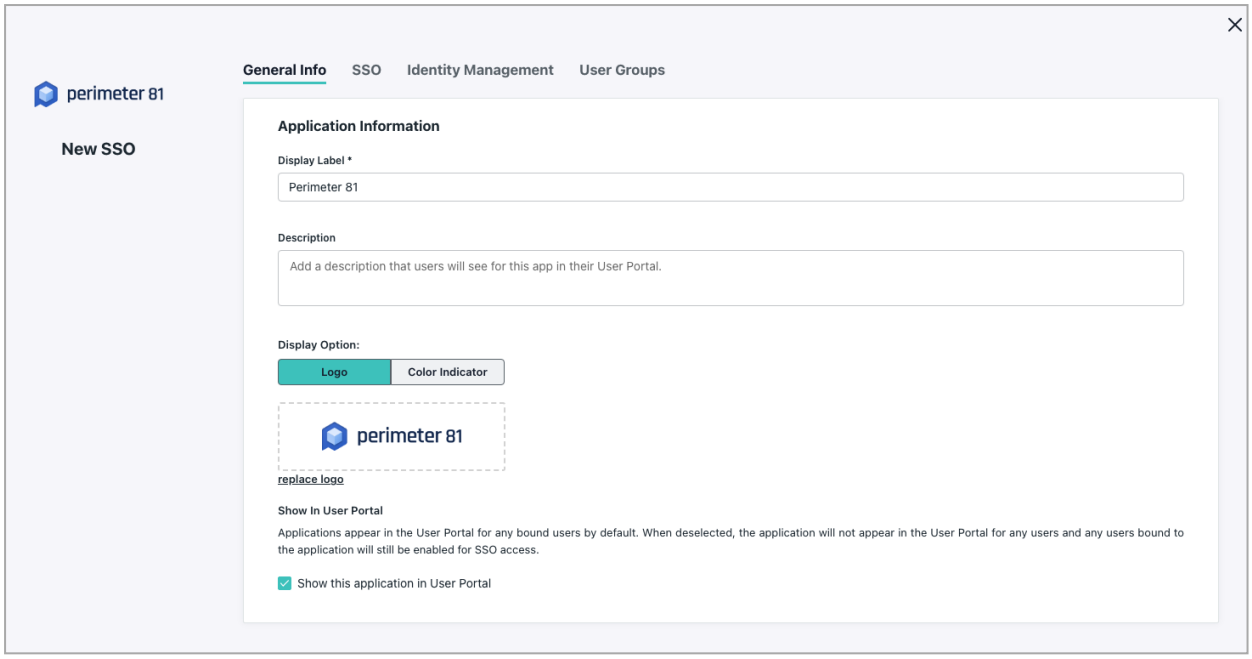
3. Click **Add New Application**.



4. Search for Check Point SASE application and click **Configure**.

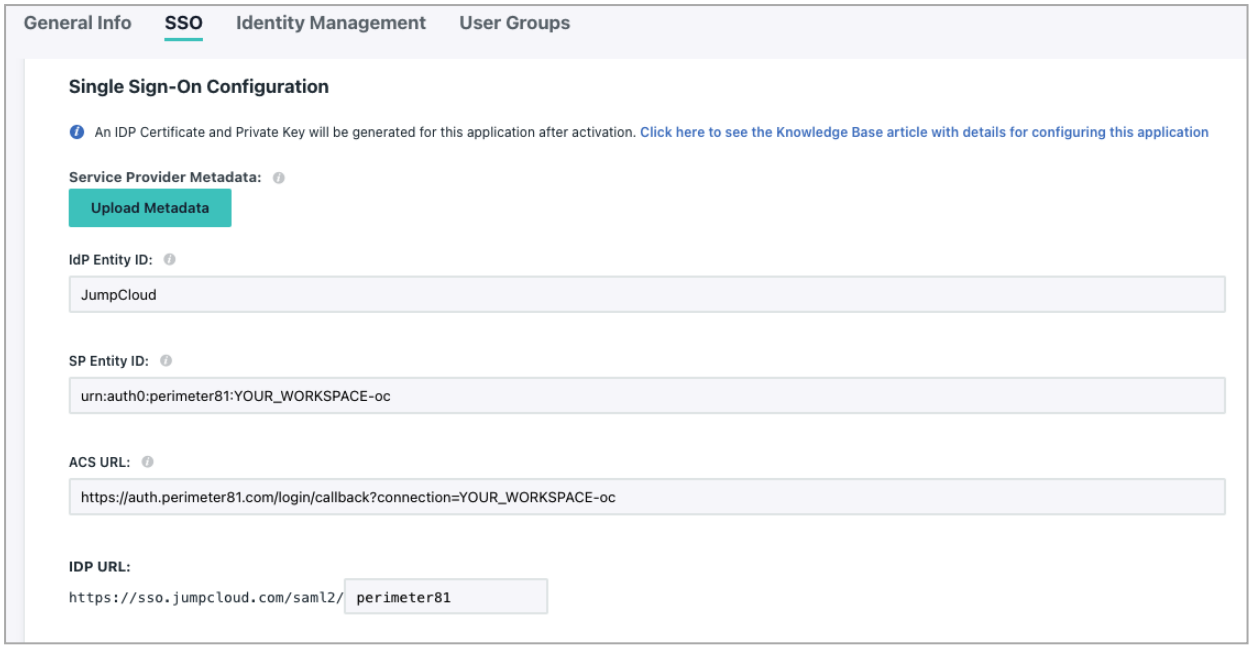


5. In the **General Info** tab, enter a name for the application in the **Display Label** field.

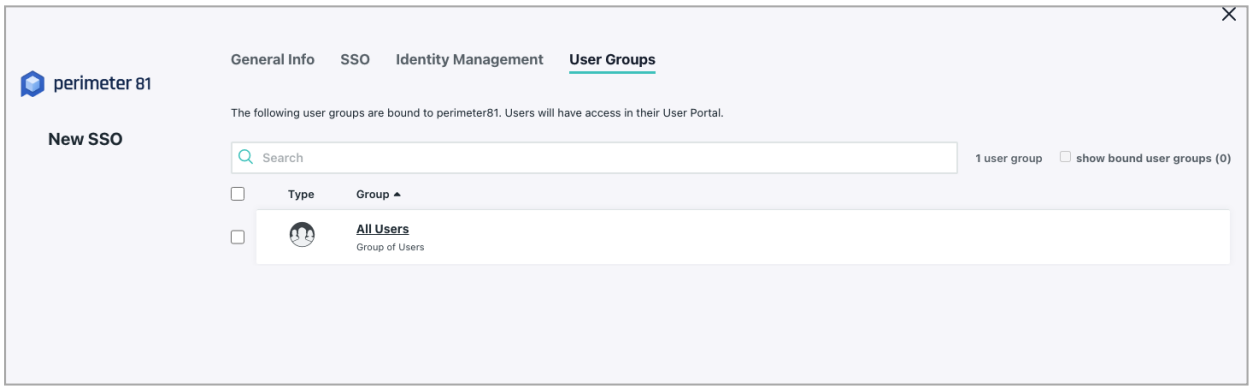


6. Go to the **SSO** tab and enter these values in the **Single Sign-On configuration** section:
   - **IDP Entity ID**: `https://{{WORKSPACE}}.perimeter81.com/`
   - **SP Entity ID**: US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`
   - **ACS URL**: US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
   - **IDP URL**: `https://sso.jumpcloud.com/saml2/{{required text}}`

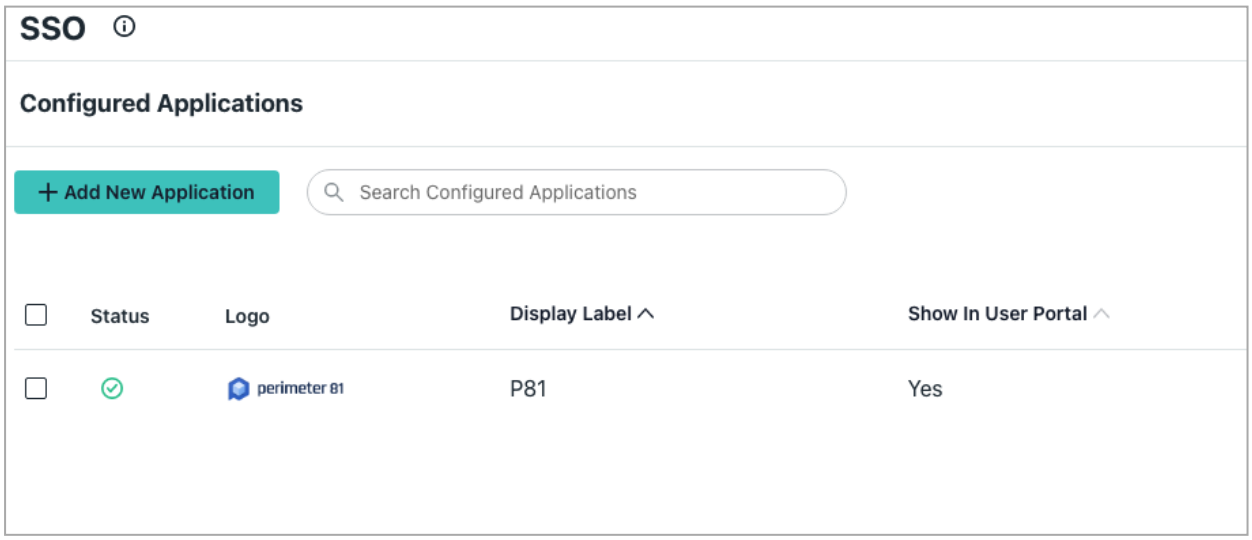
     For example, `https://sso.jumpcloud.com/saml2/perimeter81`.
   - Do not change the default values in the other fields.



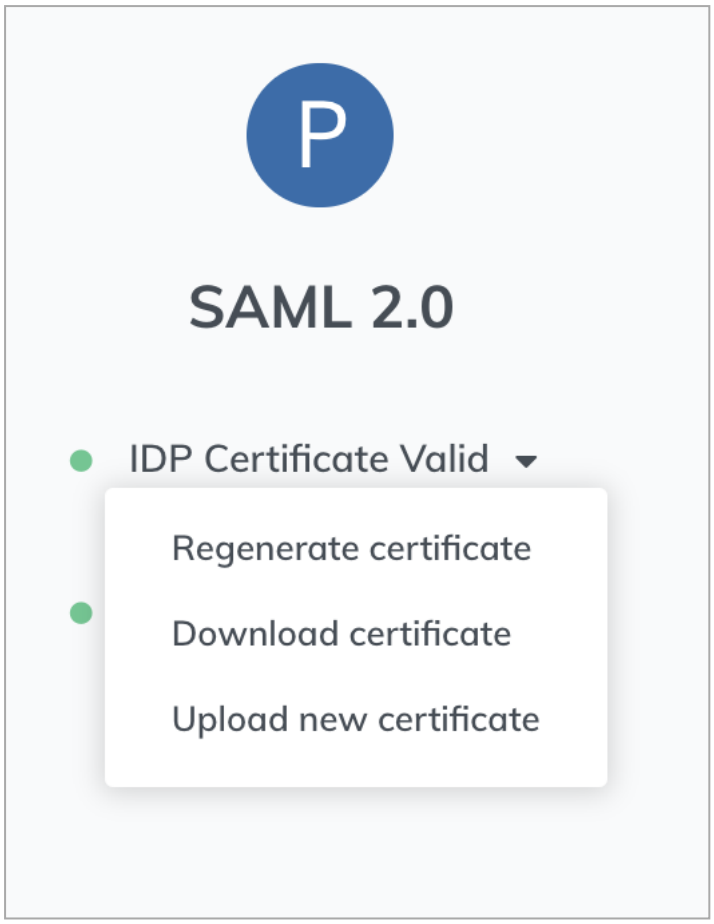
7. Go to the **User Groups** tab and verify that the required groups have the permissions.



8. Click **Activate**.
9. Click the newly created application.



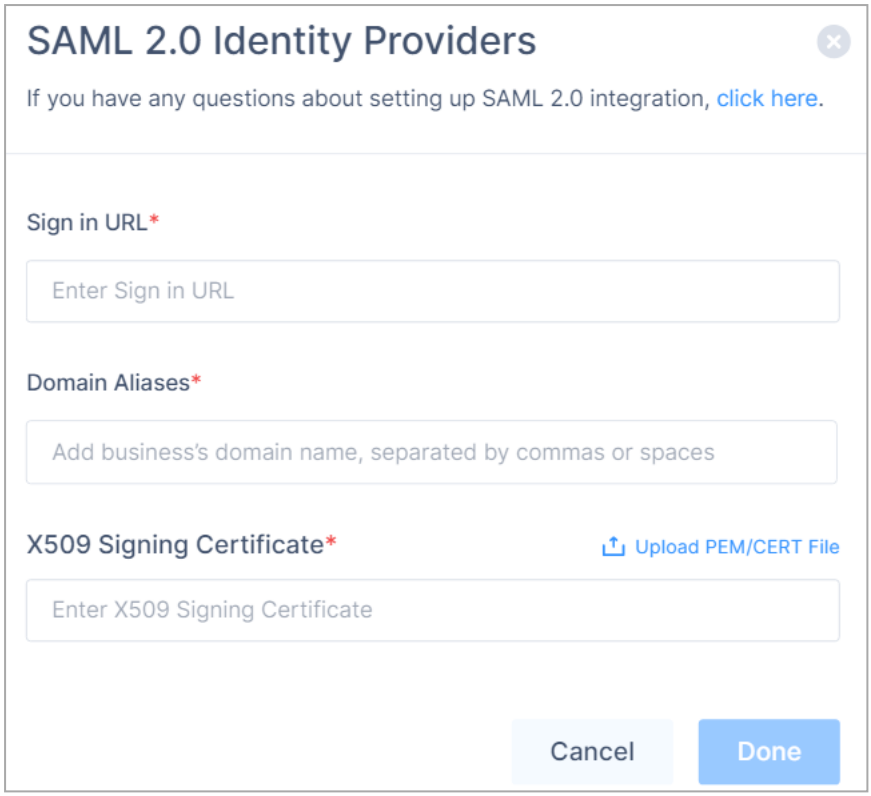
10. Click the **IDP Certificate Valid** drop-down and select **Download certificate**.



Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Okta with SAML

Supported Features

Integrating Okta with Check Point SASE using SAML protocol supports these features:

- SP-initiated SSO (only supported for the Web Client login)
- IdP-initiated SSO (only supported for the Web Client and Agent login)
- JIT (Just In Time) Provisioning

Prerequisites

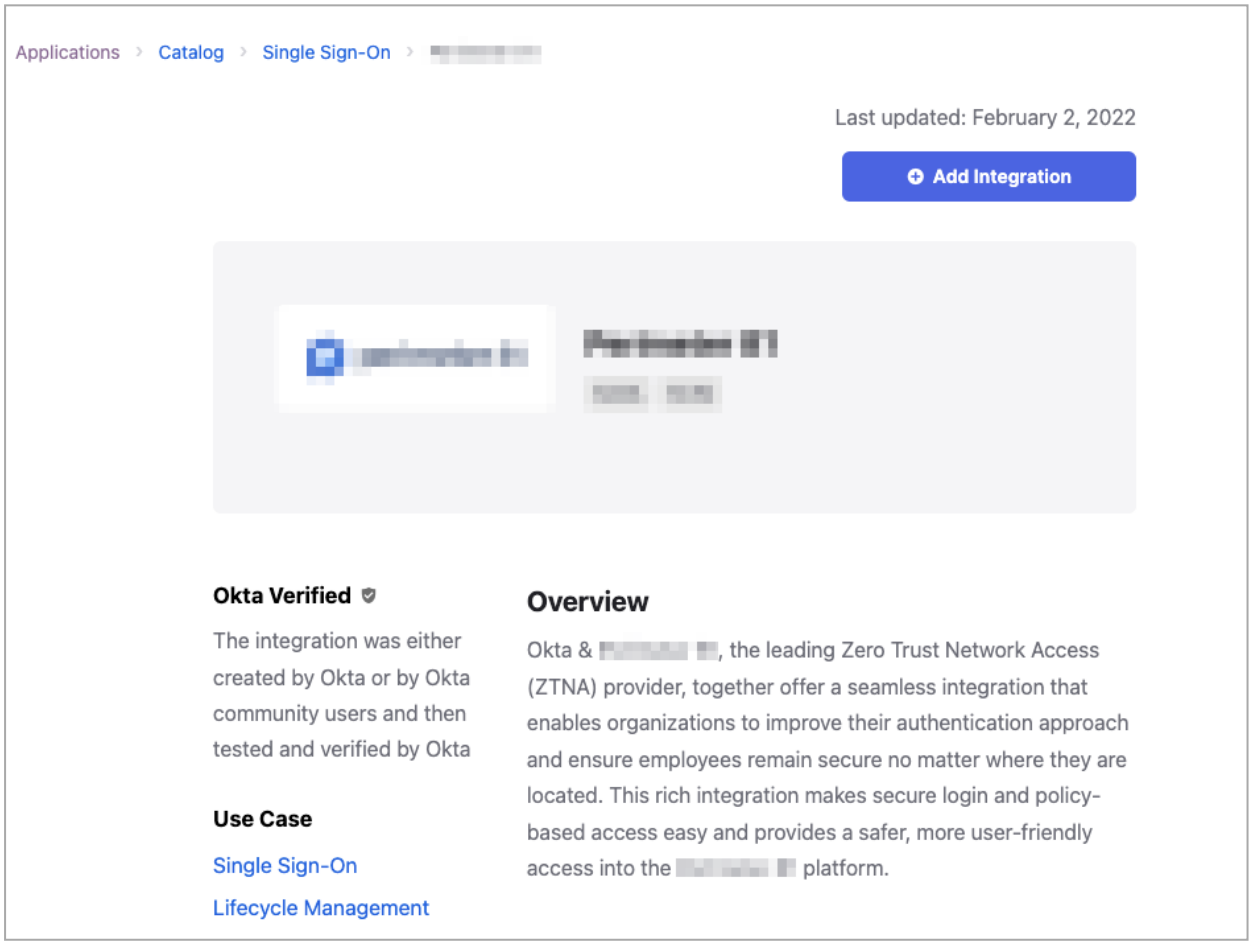
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

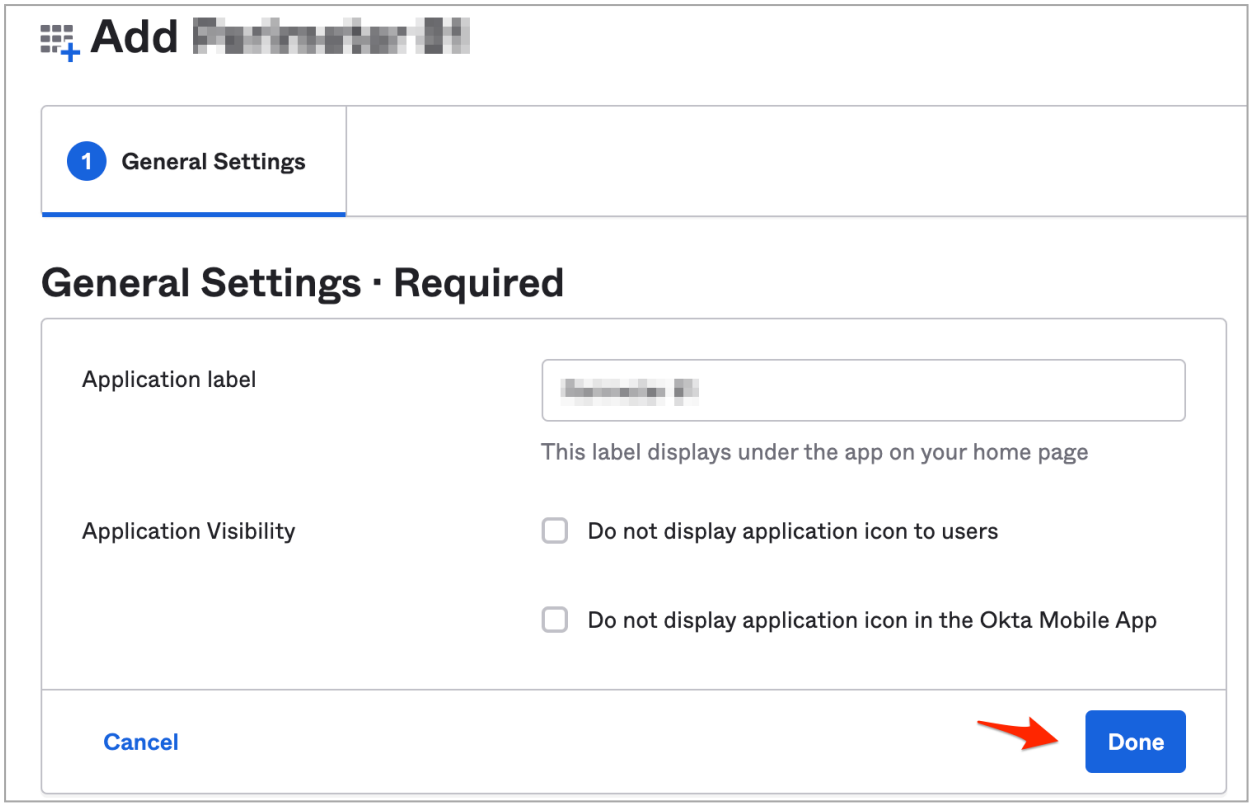
- Step 1 - Configure the Okta Management Portal
- Step 2 - Configure the Check Point SASE Administrator Portal
- Step 3 - Assign the App
- Step 4 - Verify SP-initiated SSO

Step 1 - Configure the Okta Management Portal

1. Log in to Okta Management Portal.
2. Go to **Applications**.
3. Click **Browse App Catalog** and search for Perimeter 81.
4. Click **Add Integration**.

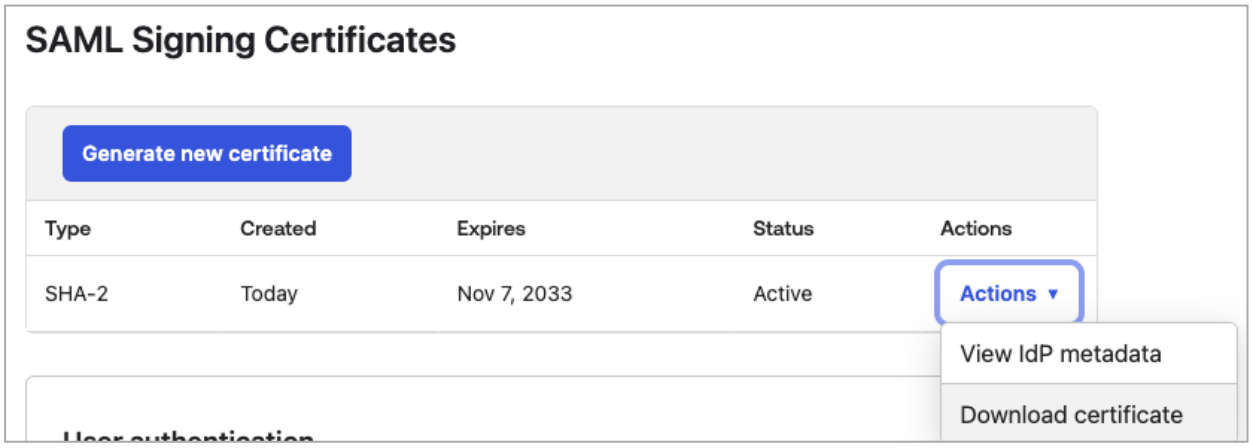


5. Click **Done**.

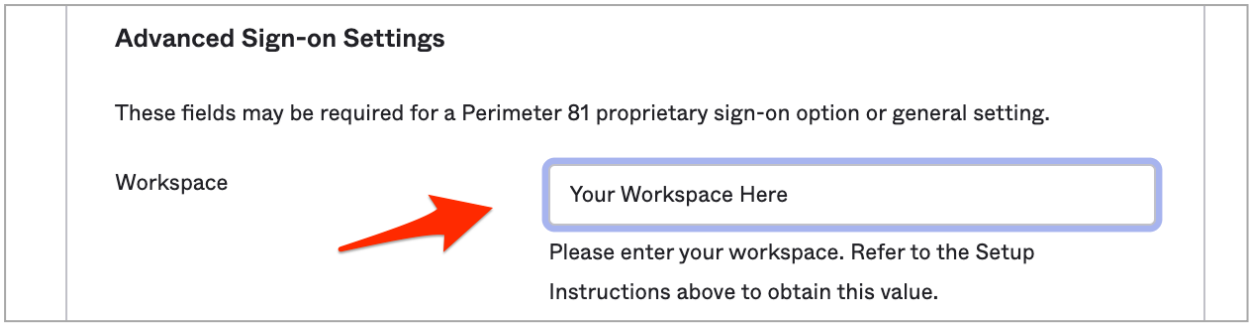


A Check Point SASE application is generated.

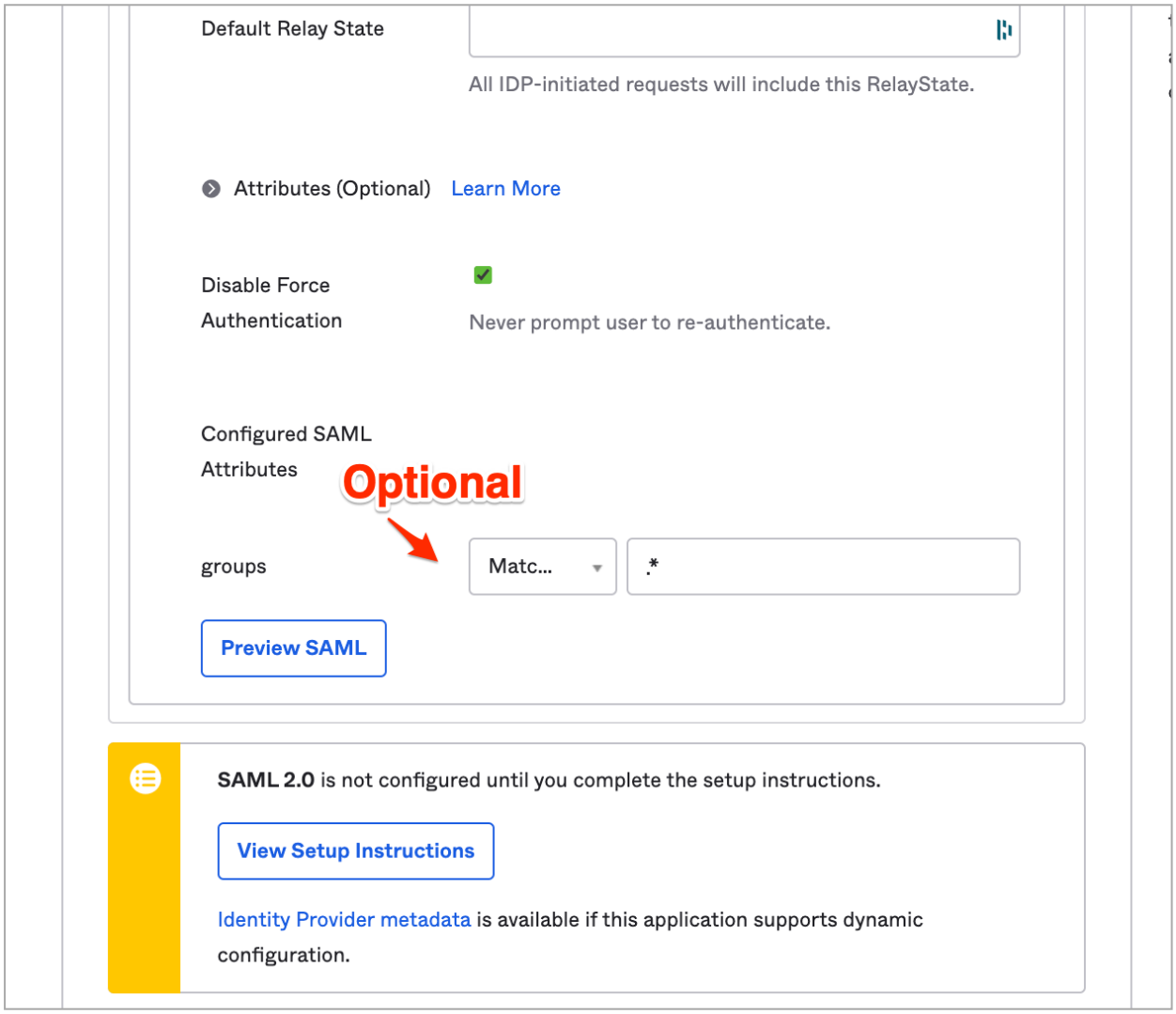
6. Go to the **Sign On** tab.
7. In the **SAML 2.0** section, click **More details** and then copy the **Sign on URL**.
8. In the **SAML Signing Certificates** section, click **Actions** and then select **Download certificate**.



9. On the **Sign On** page, go to **Settings** and click **Edit**.
10. In the **Workspace** field, enter your Check Point SASE workspace name.



11. (Optional) If you want the group membership of your Okta account to sync with Check Point SASE, make sure that the Groups has the **"Matches Regex" .*** syntax.



Note - You must create the group on Check Point SASE manually for this option to work.

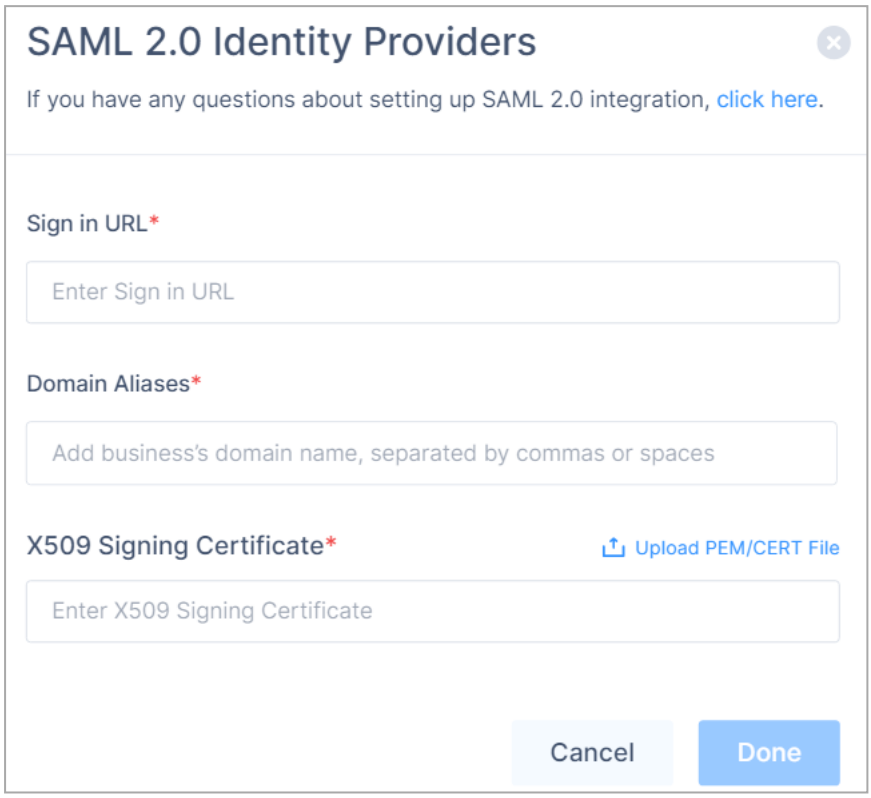
Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.

3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.

4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`

Identity Provider	Sign in URL
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

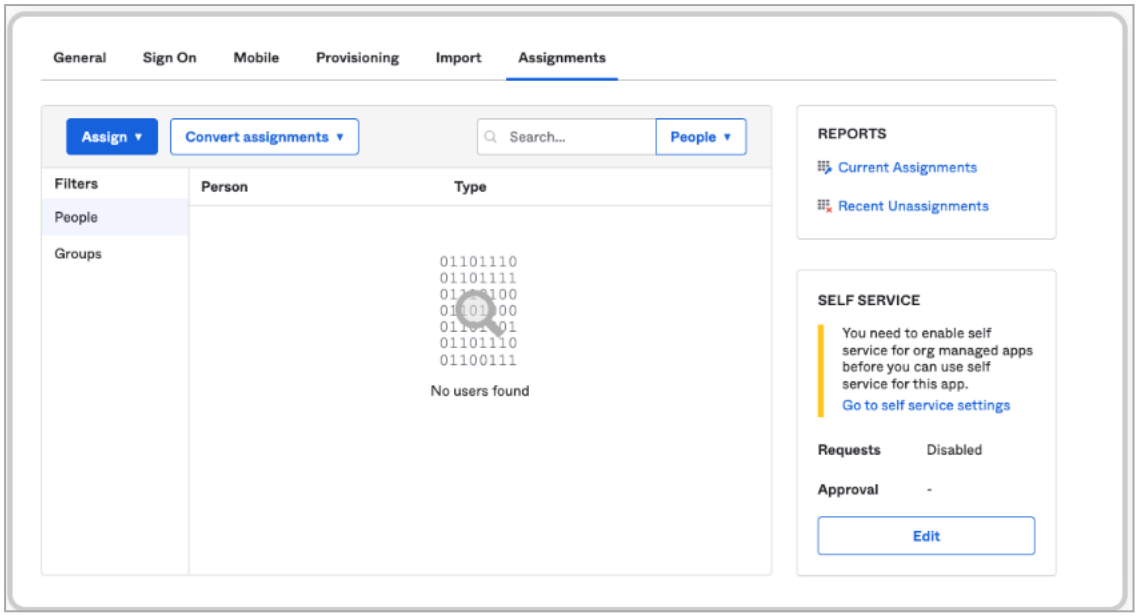
   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Step 3 - Assign the App

1. Log in to Okta Management Portal.
2. Go to **Applications** and select your SAML 2.0 Application.
3. Go to **Assignments** tab.



4. Assign the **People** or **Groups** you want to get synchronized with Check Point SASE.
5. Click **Save and Go Back** and then click **Done**.

Step 4 - Verify SP-initiated SSO

1. Log in to Check Point SASE workspace URL.
2. Click **Sign in with Okta**.
3. Verify you can successfully connect using your Okta credentials.

Supported SAML Attributes

Attribute Name	Value
given_name	user.firstName
family_name	user.lastName
email	user.email
groups	As configured in the app. **Note** - Local users not defined through Okta will not be automatically added or removed from any Okta-associated group to which they are assigned. You must manually add or remove them from the required groups.

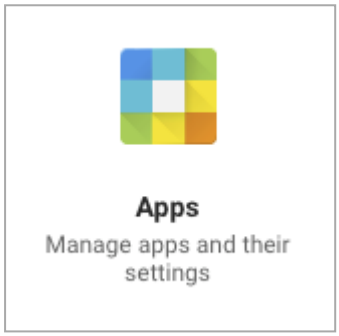
Google Applications with SAML 2.0

Prerequisites

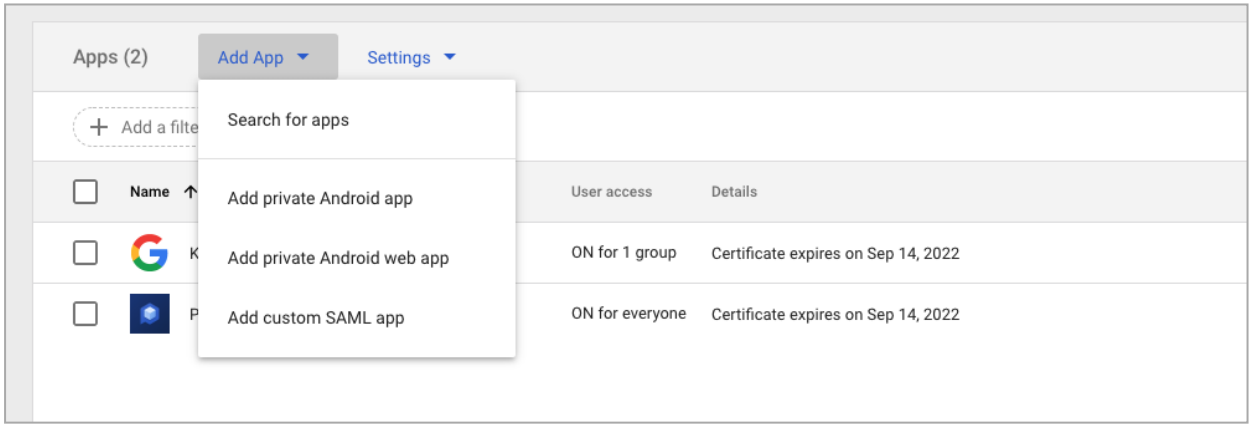
- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

Step 1 - Configuring the Application in the Google Admin Console

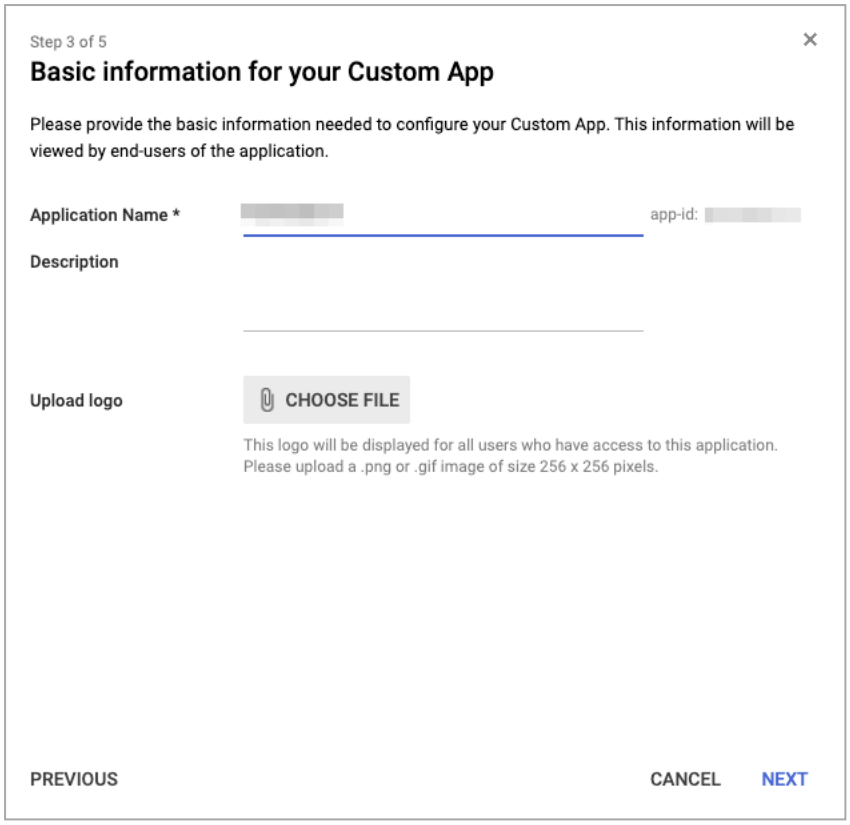
1. Log in to the Google Admin Console with a administrator account.
2. Go to **Apps**.



3. Click **Add App** and select **Add custom SAML app**.

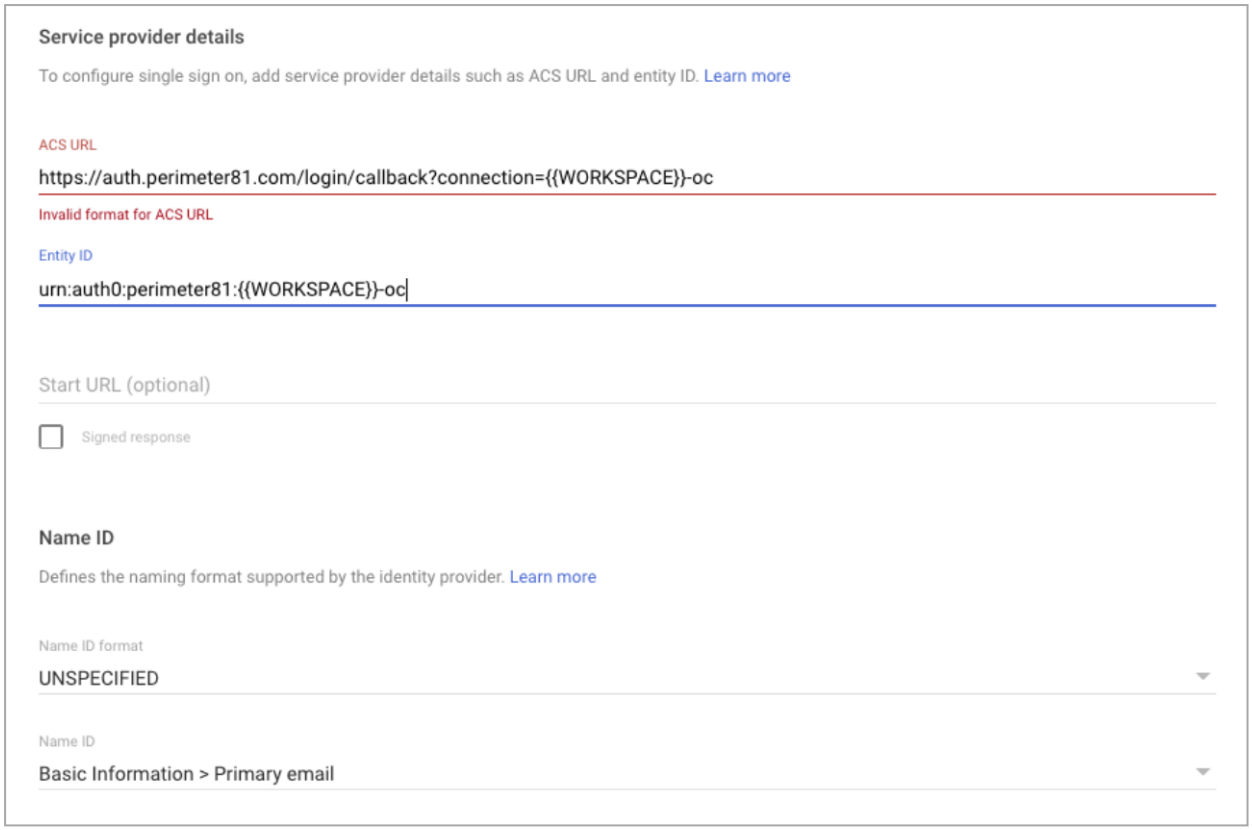


4. In the **Application Name** field, enter a name for the application.



5. (Optional) In the **Description** field, enter a description about the application.
6. (Optional) To add a logo to the application, click **Upload Logo** and select the file.
7. Click **Next**.
8. Copy the **SSO URL**.

9. Copy the certificate or click the download icon to download it.
10. Click **Next**.
11. In the **Service provider details** section:



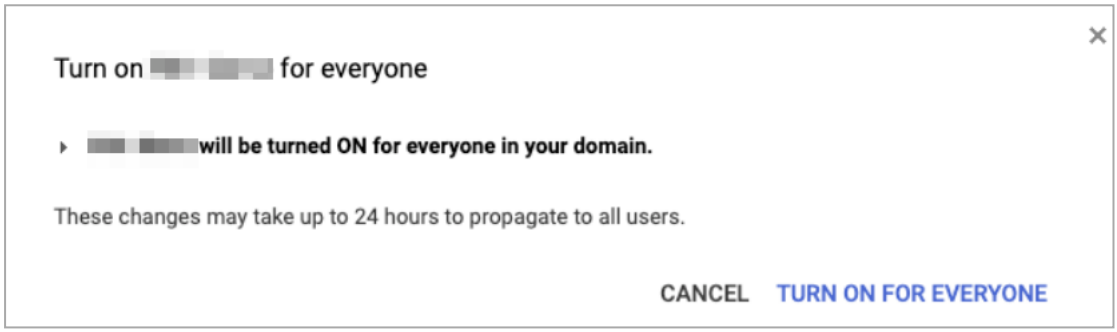
- **ACS URL** : Enter US-based platform: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`EU-based platform: `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`AU-based platform: `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`IN-based platform: `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
- **Entity ID** : Enter US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`
- **Name ID**: Select *Basic Information > Primary Email*
- **Name ID Format**: Select *UNSPECIFIED*

12. Click **Add mapping** and enter these attribute / value pairs in separate rows:

Attribute	value
Basic Information > Primary email	email
Basic Information > Last Name	family_name
Basic Information > First Name	given_name
Employee Details > Department	groups

The system creates the application.

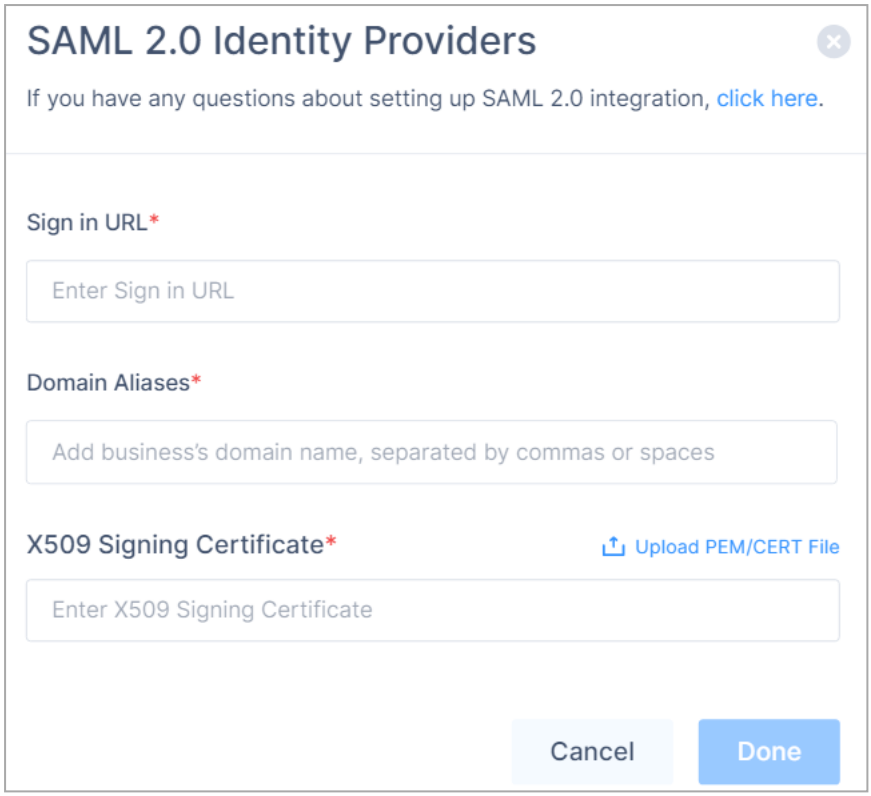
13. Click **Status** and select **Turn on for everyone**.



Step 2 - Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Google Services

Before opting for Google Services instead of the Google SAML application to log in with your Google Workspace account, evaluate the potential cost implications for using Google Services.

Prerequisites

- Administrator access to the Check Point SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Generate the Google Client ID and Client Secret" on the next page*
- *"Step 2 - Enable the Admin SDK Service" on page 1034*
- *"Step 3 - Configure the Check Point SASE Administrator Portal" on page 1034*

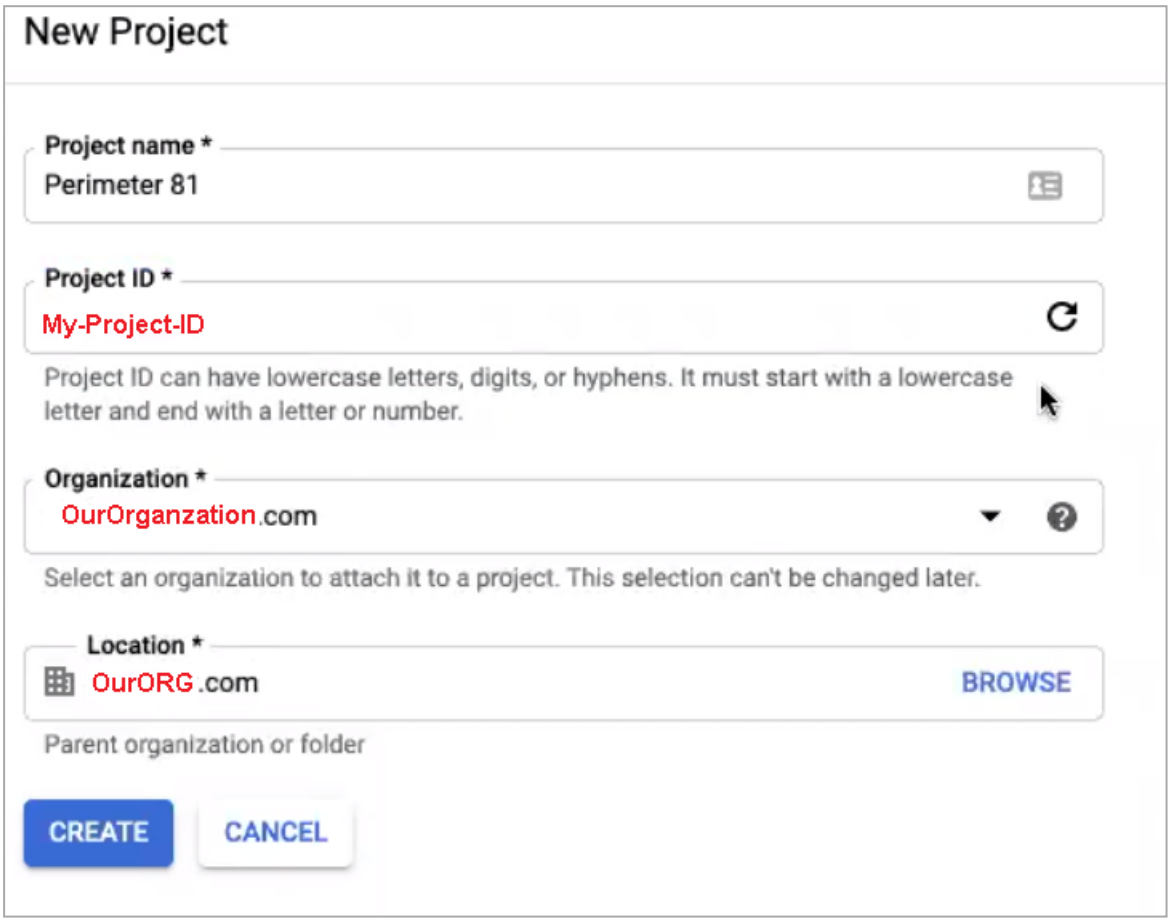
Step 1 - Generate the Google Client ID and Client Secret

1. Log in to the Google Admin Console.
2. Open the console left side menu and select **APIs & services**, and then select **Credentials**.
3. Select a project.
4. If you do not have a project defined on Google Cloud Platform:
   a. Click **Create**.

The **New Project** pop-up appears.

b. Enter these details:

- **Project Name**
- **Project ID**
- **Organization** - The organization to which the project should attach to.
- **Location** - Parent organization or folder where the project should be saved.



c. Click **Create**.

5. Go to **OAuth consent screen**, select **User Type** as **External** and then click **Create**.

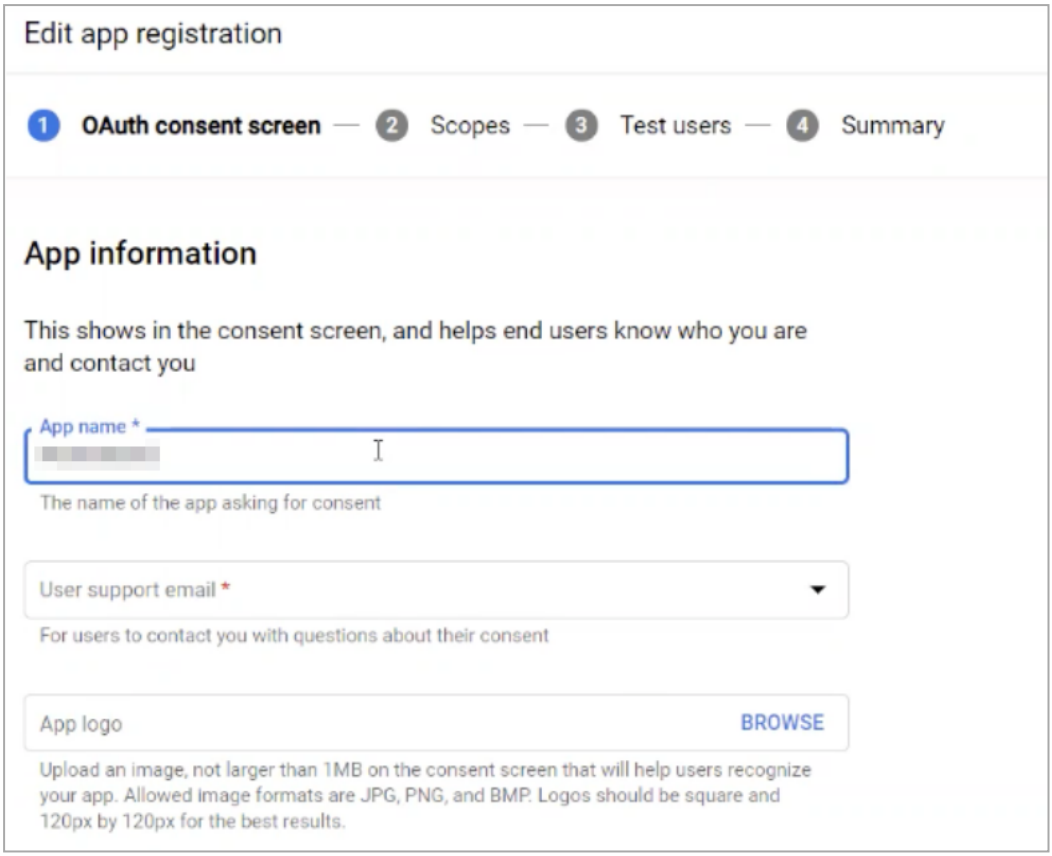
   The **Edit app registration** page appears. The information entered here will be used by the users to know who you are and contact you.

6. In the **OAuth consent screen** section, enter these values:

   a. Select the **Application Type** as **Public**.

   b. In the **Application Name** field, enter a name for the application.

c. In the **User support email** field, enter an email address. The users use this email address to contact for questions about the consent.



d. (Optional) To add a logo, in the **Add logo** field, click **Browse** and select the logo.

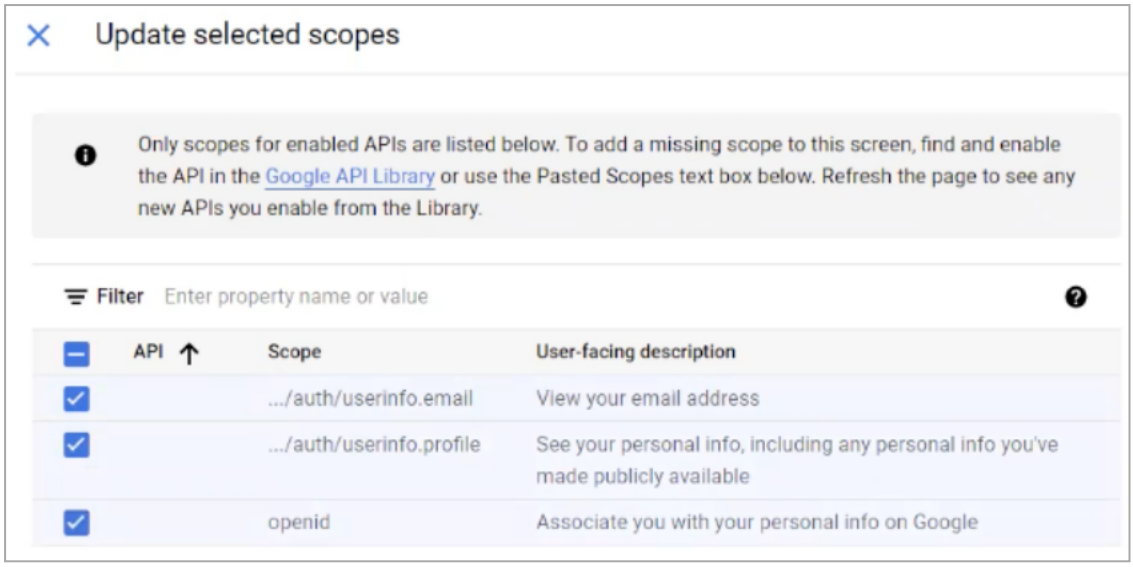
e. In the **Application Homepage link** field, enter your Check Point SASE workspace URL.

f. In the **Authorized domains** section, enter your domain name and click **Add Domain**.

g. In the **Developer contact information** field, enter your support email address.

h. Click **Save and Continue**.

7. In the **Scopes** section, select these options:



a. Click **Add or Remove Scopes**.

b. Select these scopes:

   i. userinfo.email

   ii. userinfo.profile

   iii. openid

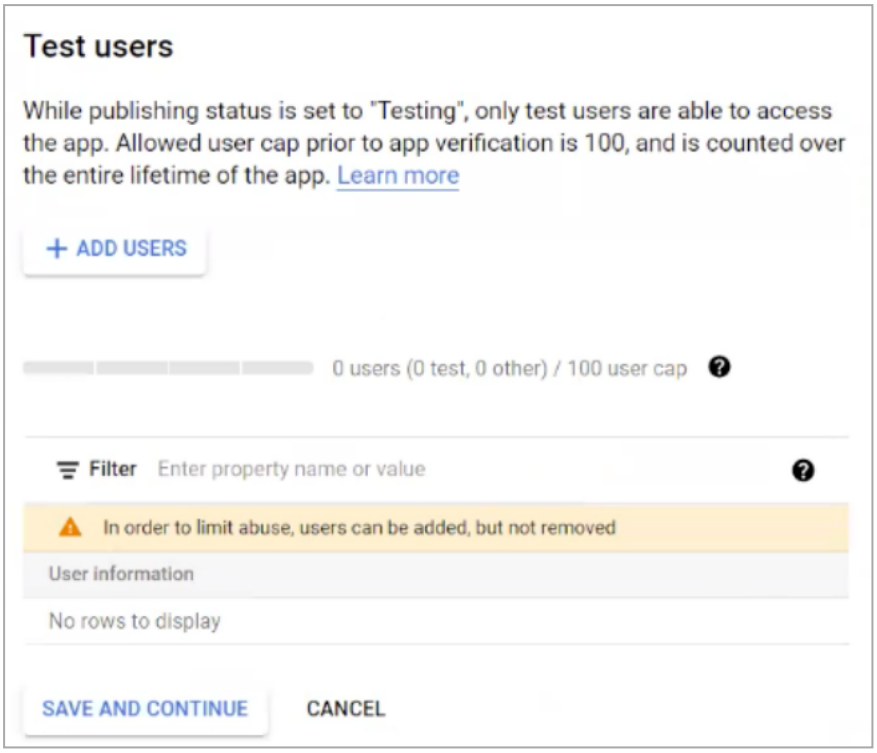
c. Click **Update** and then click **Save and Continue**.

   Note - To use Google Workspace groups, ensure required group authorization scopes are enabled. For more information, see the Google Workspace Admin SDK documentation.

8. (Optional) To test the users if they are able to access the application:

a. Click **Add Users**.

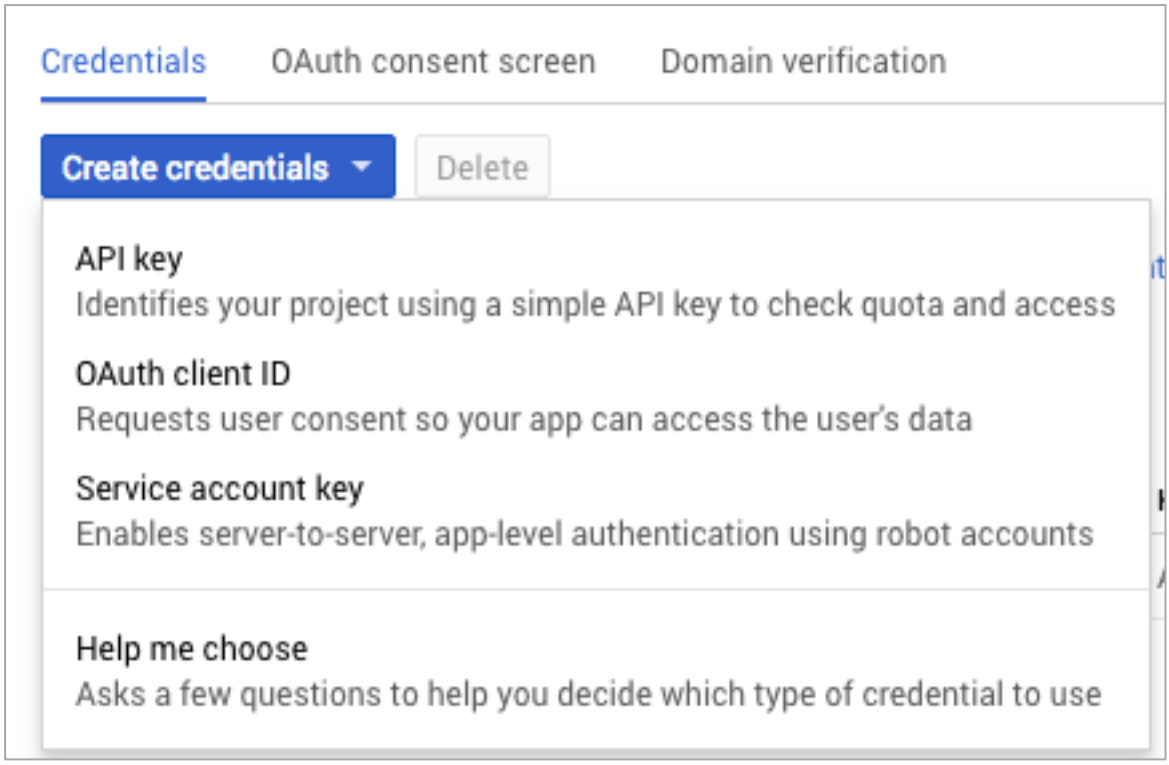
b. Enter the user email addresses.



9. To skip testing the users and continue, click **Save and Continue**.

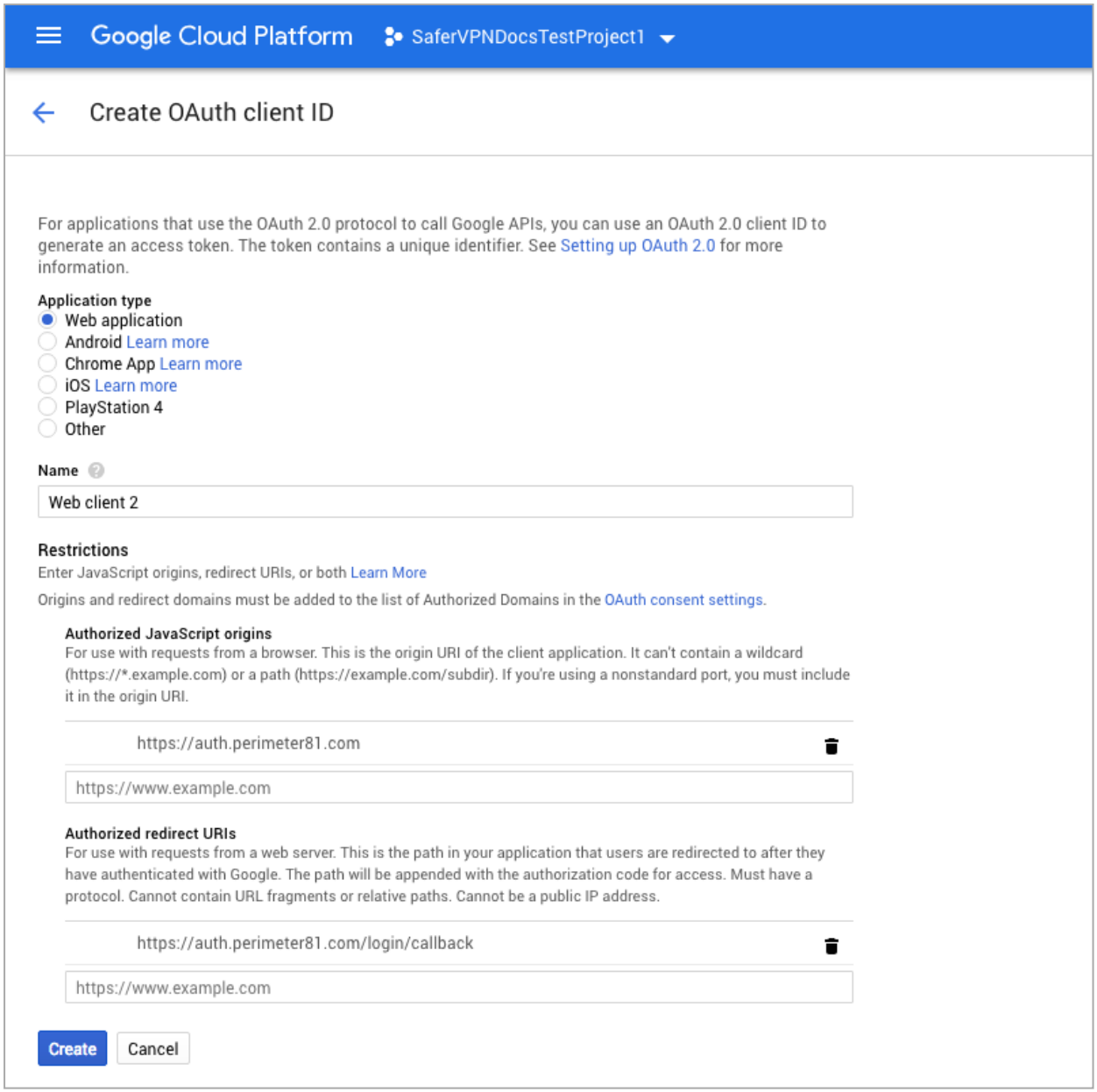
   Google creates your project and when the process completes, it prompts you to create credentials.

10. Click **Create credentials** and then select **OAuth client ID**.



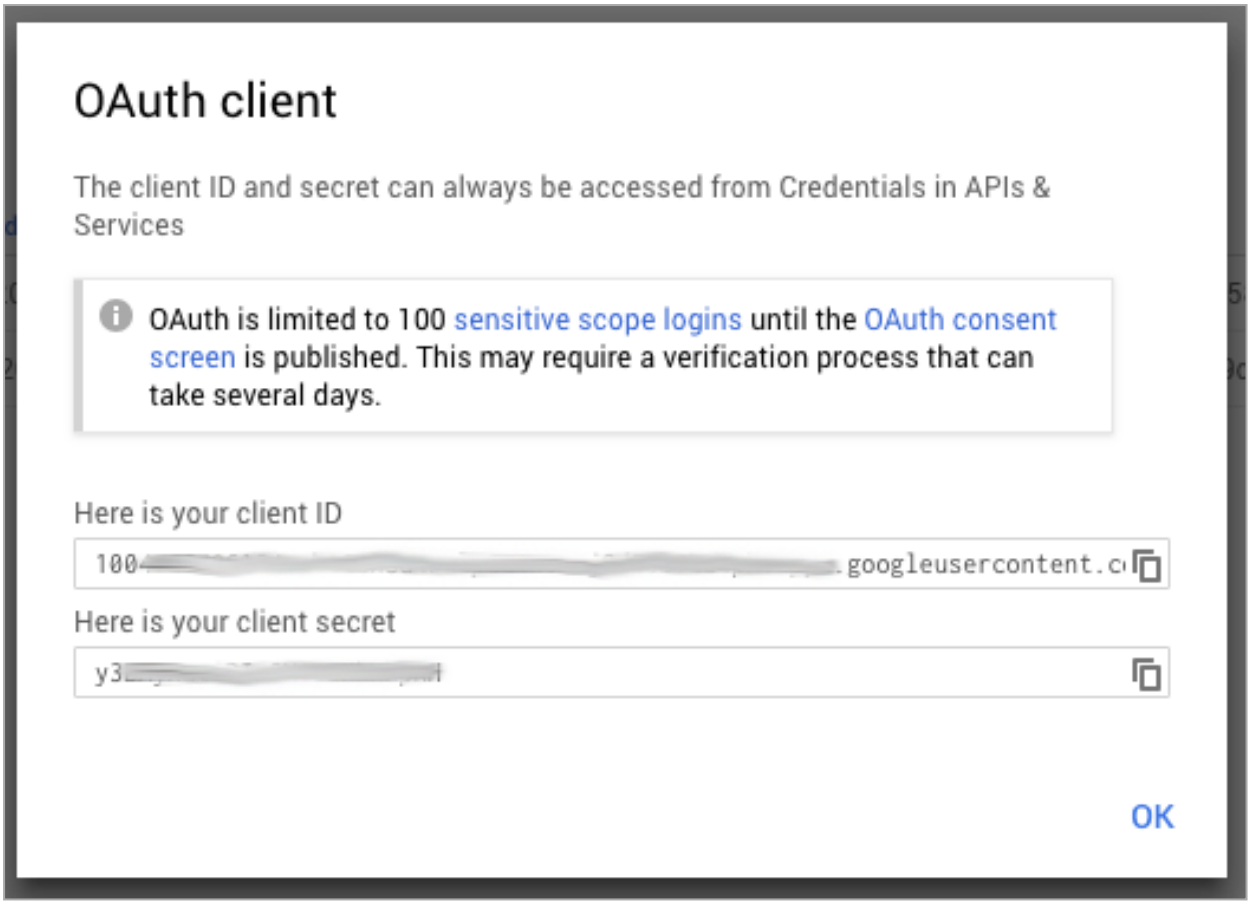
Google shows a **To create an OAuth client ID, you must first set a product name on the consent screen** warning.

11. Click **Configure consent** and enter a product name to appear for the users when they log in through Google.
12. Google prompts you to provide additional information about the newly-created app. Enter these details:



- In the **Application type**, select **Web application**.
- In the **Name** field, enter a name for the application.
- In the Restrictions section, enter these details:
  - **Authorized JavaScript origins**: https://auth.perimeter81.com
  - **Authorized redirect URI**: https://auth.perimeter81.com/login/callback
- Click **Create**.

13. If Google shows "unverified app" screen before showing the consent for your app, complete the OAuth Developer Verification.
14. Copy the **Client ID** and **Client Secret**.



Step 2 - Enable the Admin SDK Service

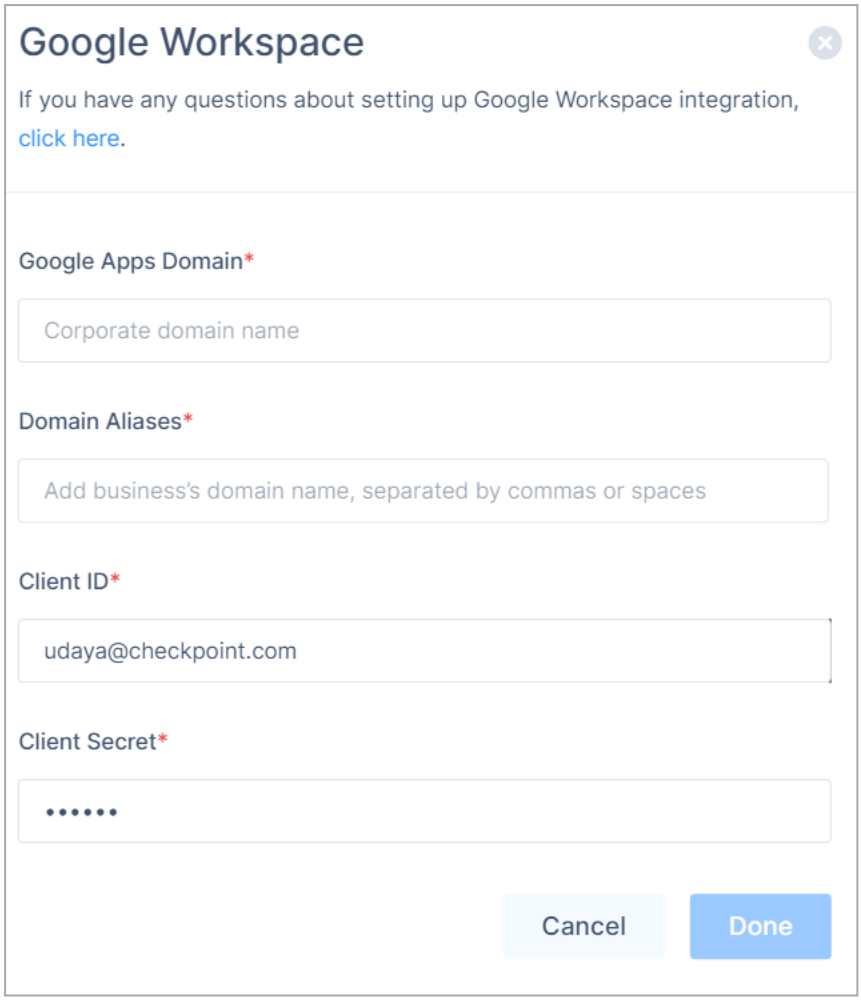
To connect to Google Suite enterprise domains, you need to enable the **Admin SDK** service. To do that:

1. Log in to the Google Admin Console with a administrator account.
2. From the console left side menu, select **APIs & services**, and then select **Library**.
3. Select **Admin SDK**.
4. On the **Admin SDK** page, select **Enable**.

Step 3 - Configure the Check Point SASE Administrator Portal

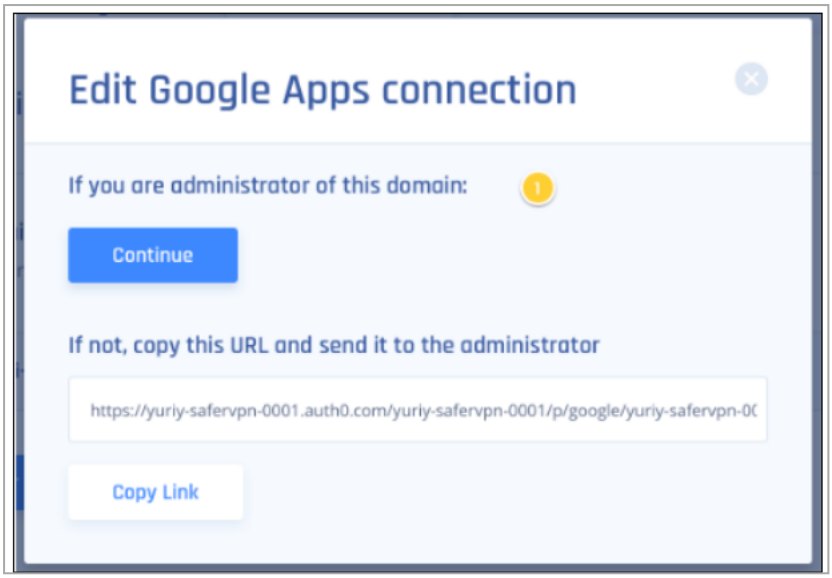
1. Log in to the Check Point SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **Google Workspace** and click **Continue**.
5. In the **Google Apps Domain** field, enter your corporate domain name.



6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **Client ID** field, enter the client ID.
8. In the **Client Secret** field, enter the client secret.
9. Click **Done**.

   The **Edit Google Apps connection** pop-up appears.



You must configure the application to use Google's Admin APIs. To do that, you must authenticate the application.

10. If you are an administrator in Google Workspace or you have the credentials of such a user, click **Continue** and authenticate the application.

    Best Practice - To authenticate, use a service user account with the sufficient permissions. If you authenticate with an administrator account and if that administrator leaves the organization, you must create a new **Client ID** and **Client Secret** and then re-authenticate with the new user.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

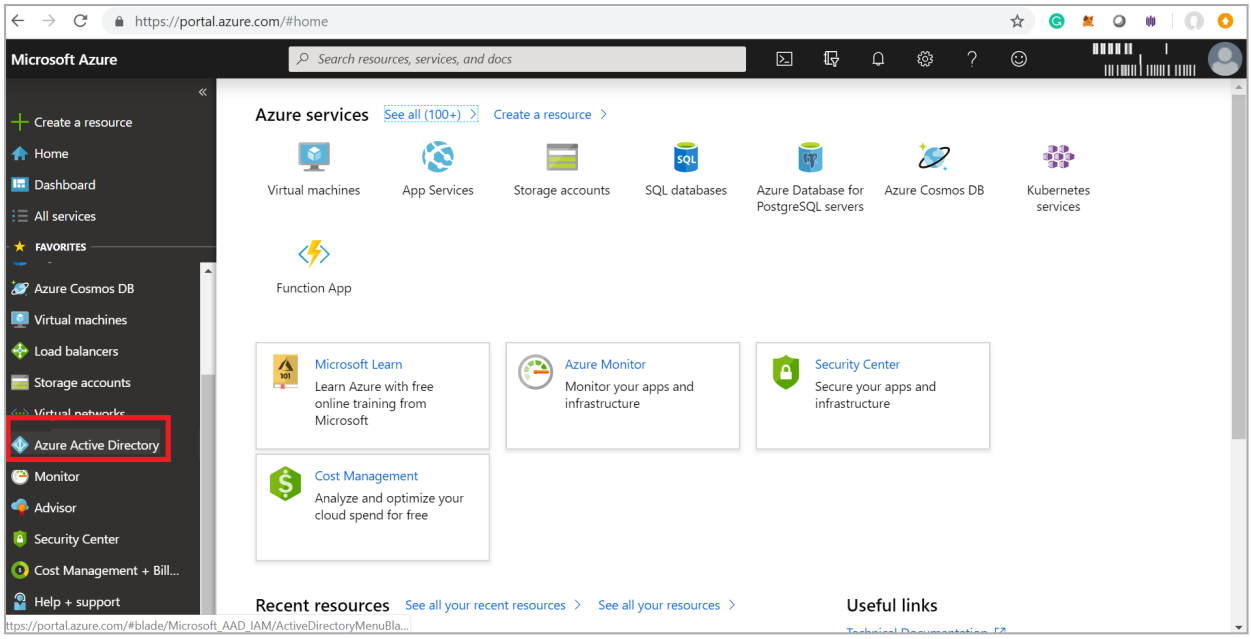
- Associates the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Microsoft Entra ID (formerly Azure AD) (SAML 2.0)

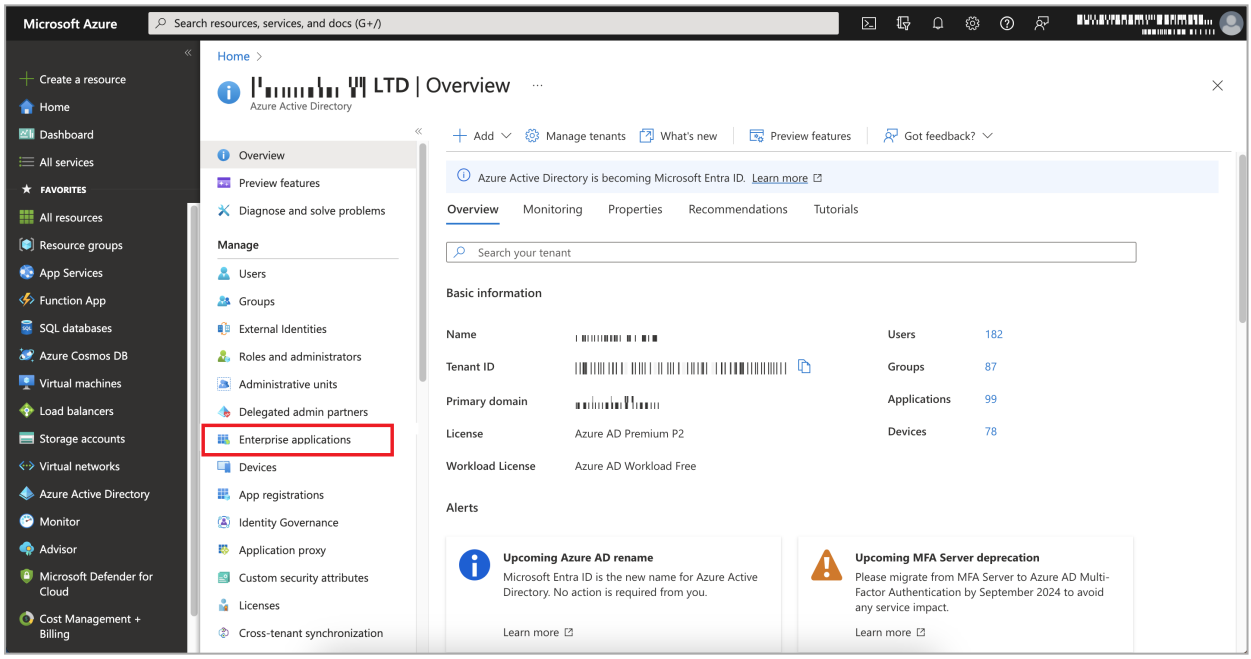
Check Point SASE allows you to authenticate securely by integrating Microsoft Entra ID (formerly Azure AD) with SAML 2.0.

Configure Microsoft Azure Portal

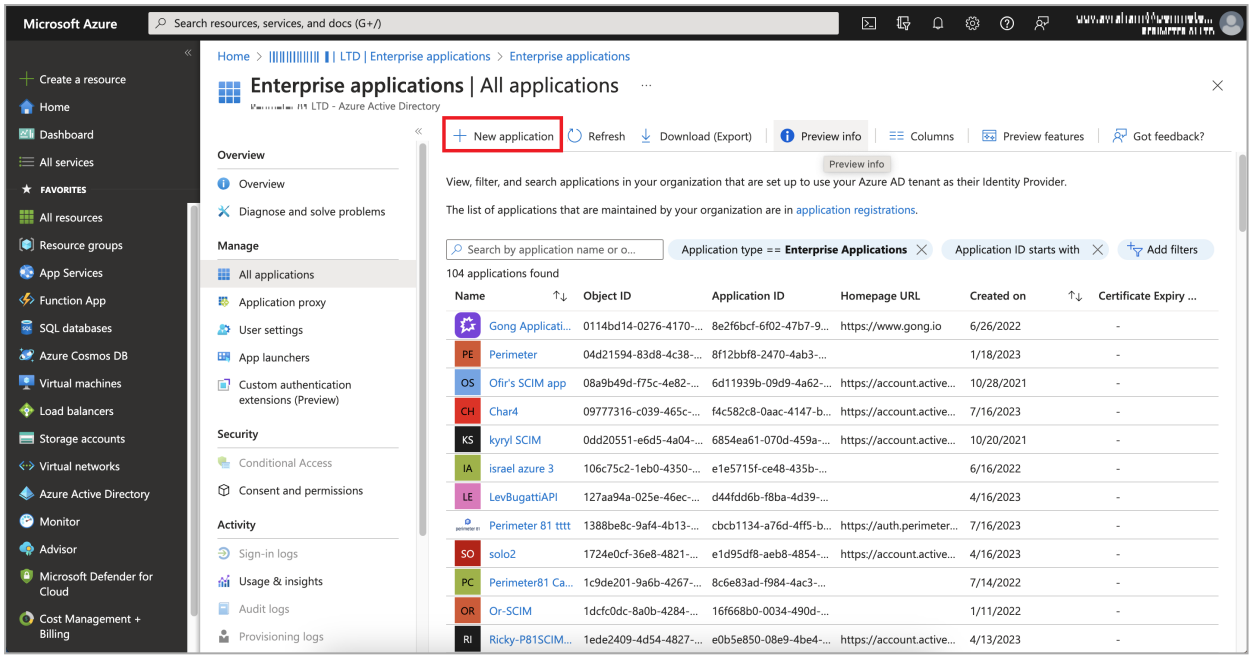
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



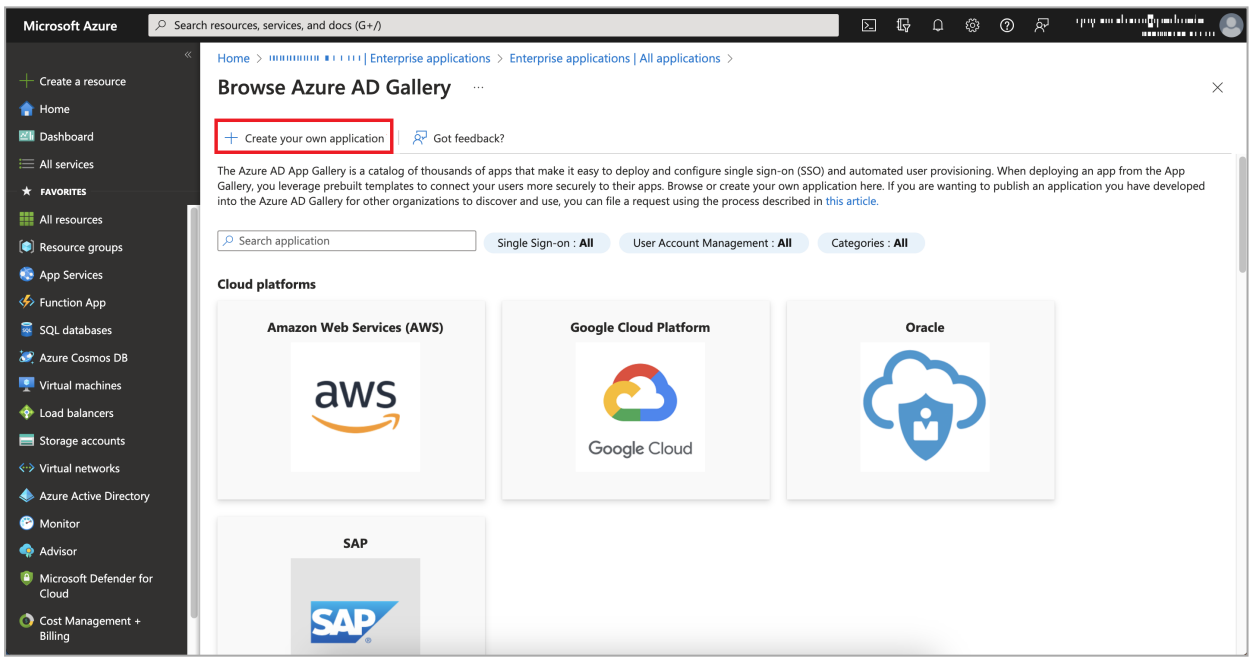
3. Go to **Manage** > **Enterprise applications**.



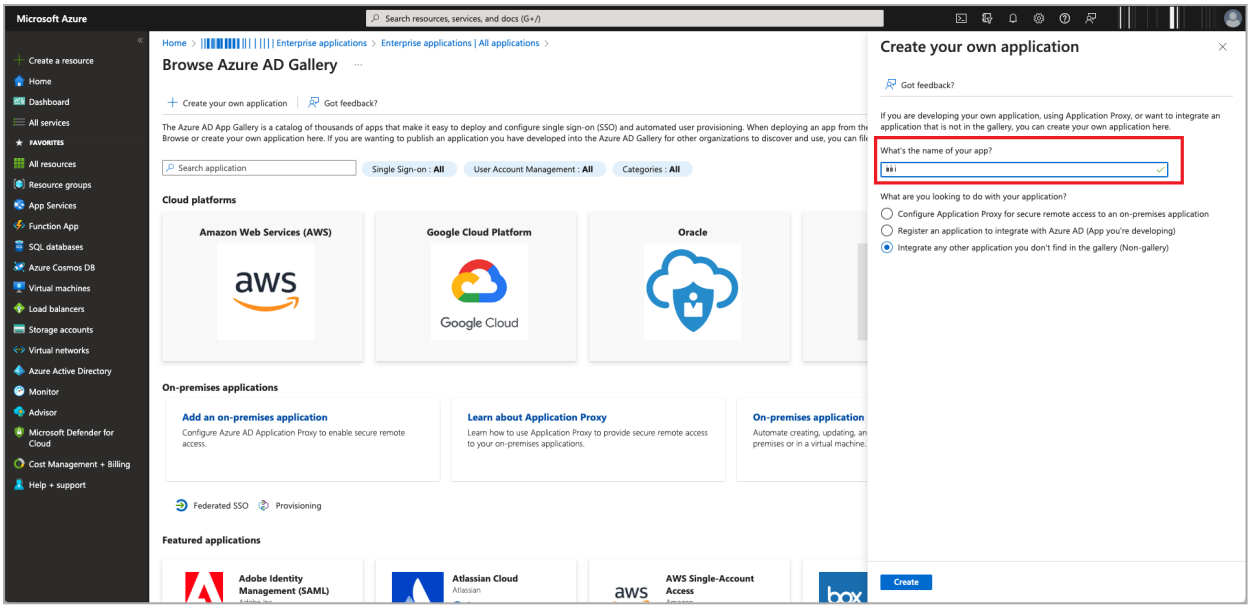
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.

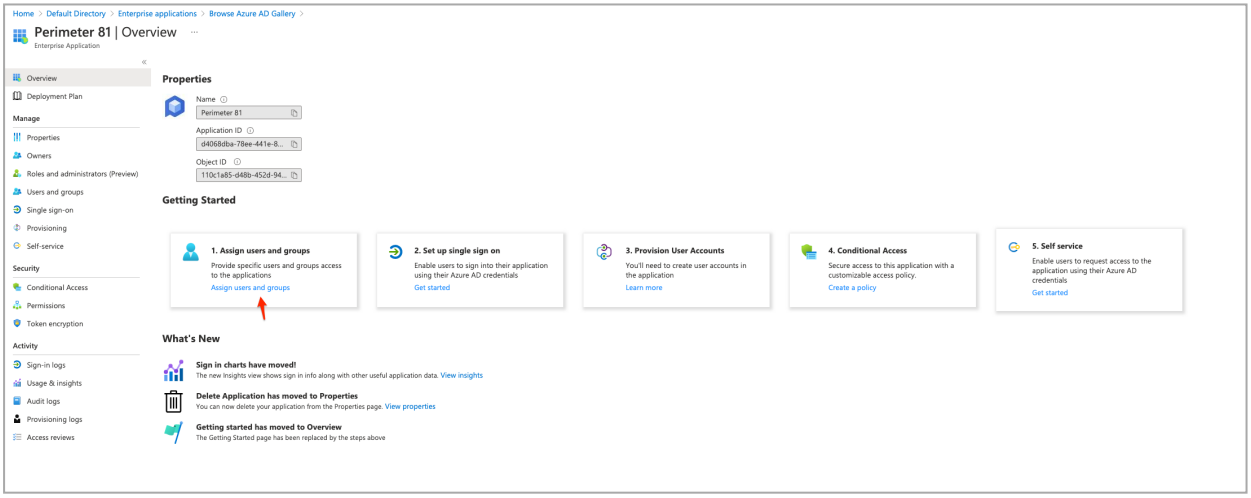


Note - Do not change the default setting.

7. Click **Create**.

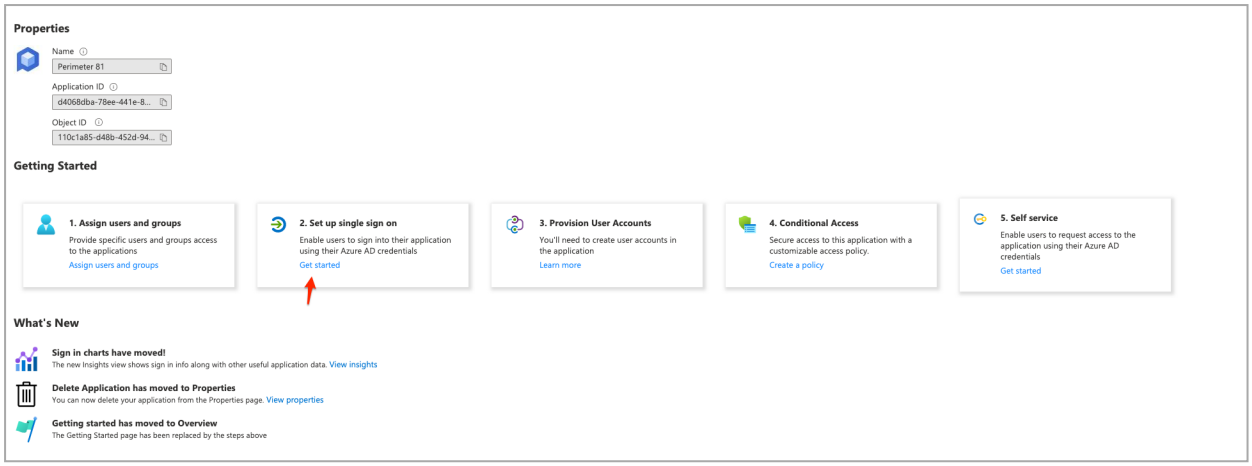
   The Microsoft Azure application is created.

8. Click **Assign users and groups** tile in the **Getting Started** section.

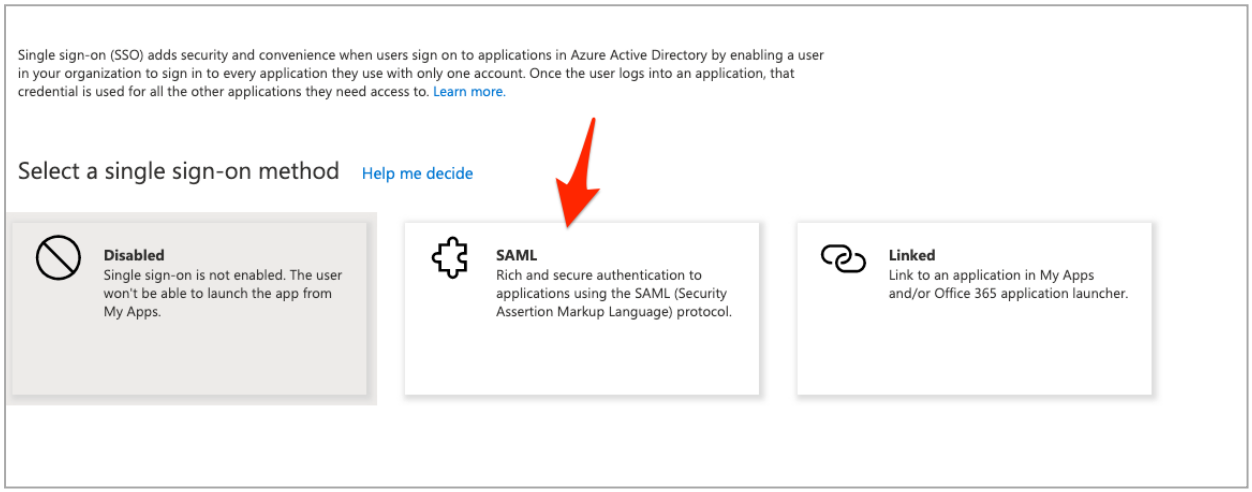


9. Search for and select the user and group that you want to assign to the application. If you are using Azure AD Free edition, you cannot add groups, add individual users instead.

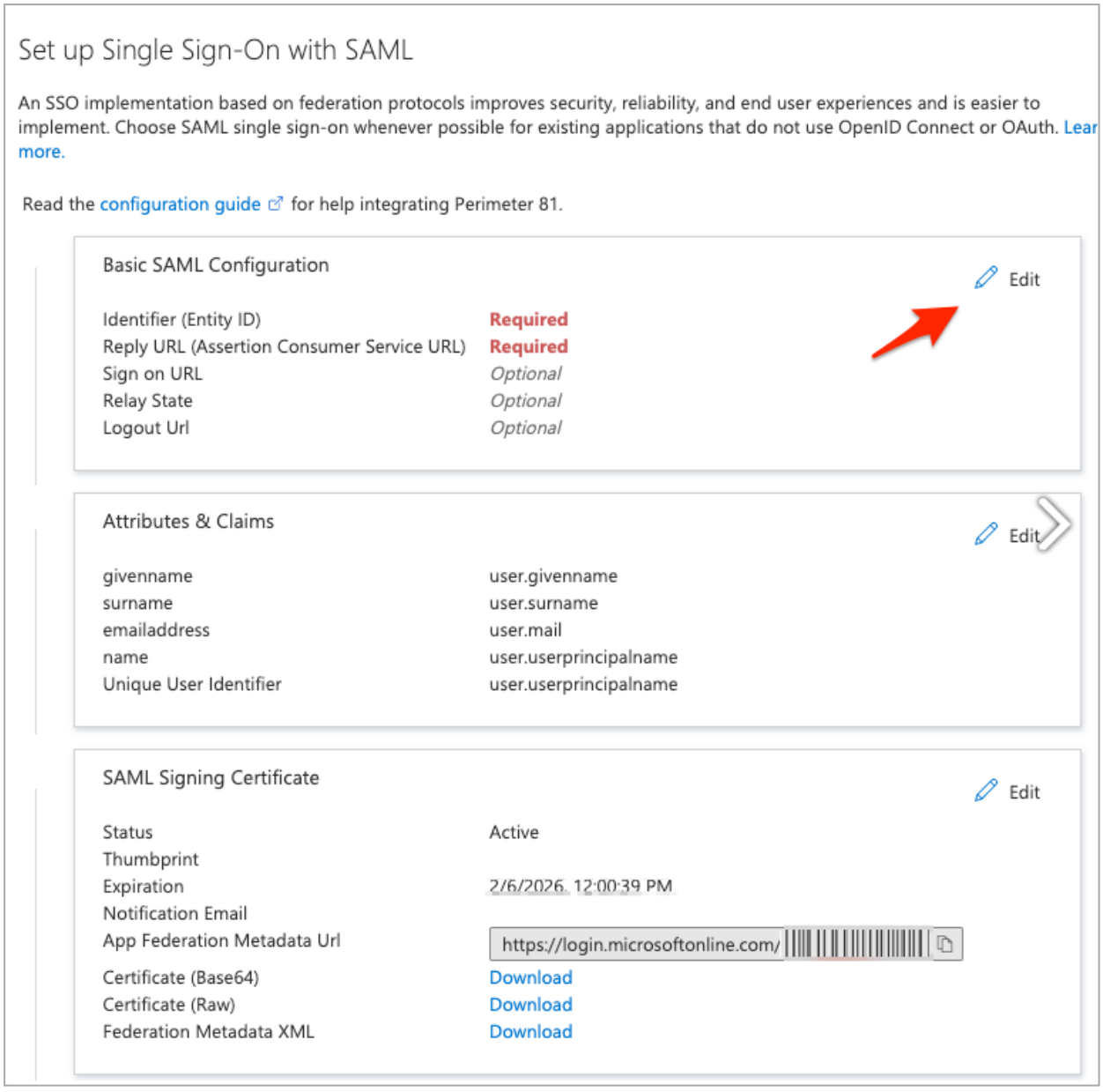
10. Click **Set up single sign on** to enable and configure single sign-on for your application.



The **Select a single sign-on method** window appears.



11. Click **SAML**.
12. Click **Edit** in the **Basic SAML Configuration** tile.



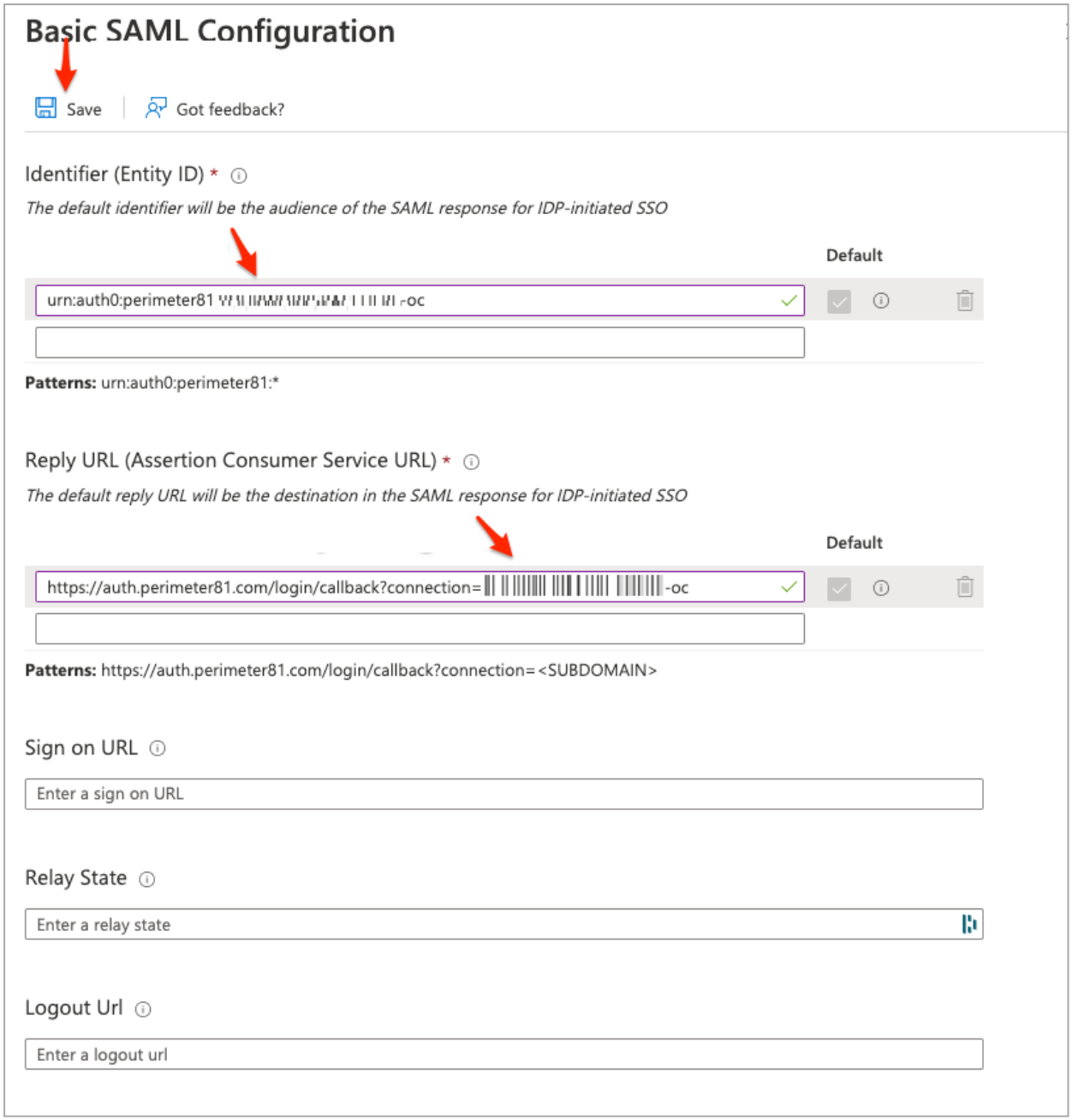
13. Enter these:

a. **Identifier**:

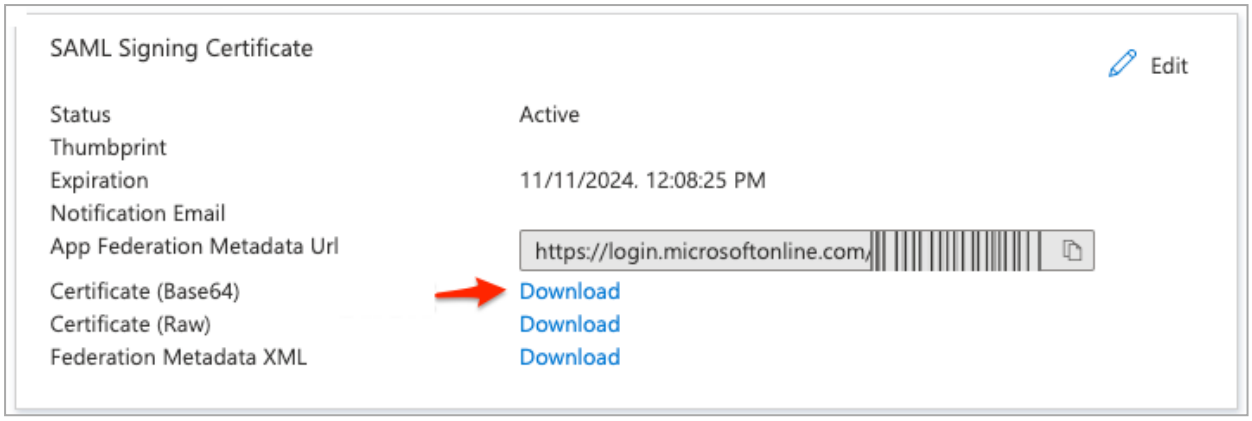
- For US data residency - US-based platform: `urn:auth0:perimeter81:{{WORKSPACE}}-oc`EU-based platform: `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`AU-based platform: `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`IN-based platform: `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc` For example: `acme.perimeter81.com` workspace should translate to `urn:auth0:perimeter81:acme-oc`
- For EU data residency - `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`
- For AU data residency - `urn:auth0:au-sase-checkpoint:{{WORKSPACE}}-oc`
- For IN data residency - `urn:auth0:in-sase-checkpoint:{{WORKSPACE}}-oc`
  where `{{WORKSPACE}}` refers to your SASE workspace name.

b. **Reply URL (Assertion Consumer Service URL)**:

- For US data residency - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
- For EU data residency - `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
- For AU data residency - `https://auth.au.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
- For IN data residency - `https://auth.in.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`
  where `{{WORKSPACE}}` refers to your SASE workspace name.

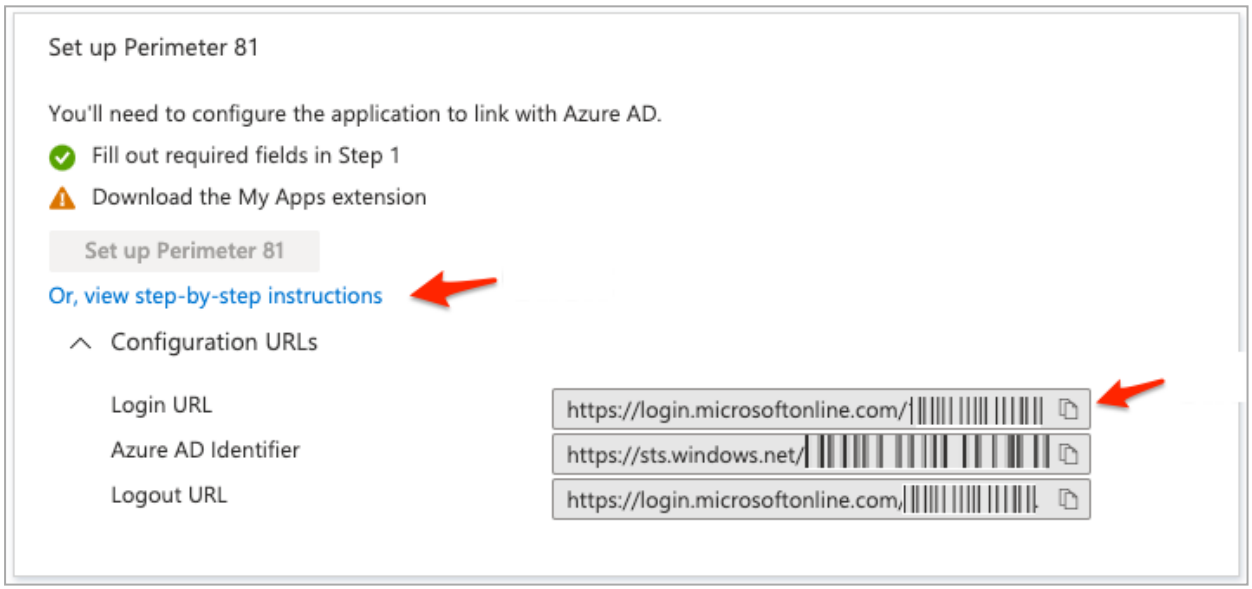


14. Click **Save**.
15. Back on the **SAML Signing Certificate** tile, go to the **Certificate (Base64)** file and click **Download**.



The Certificate (Base64) is downloaded. This certificate will be used for configuring the SAML settings for the application.

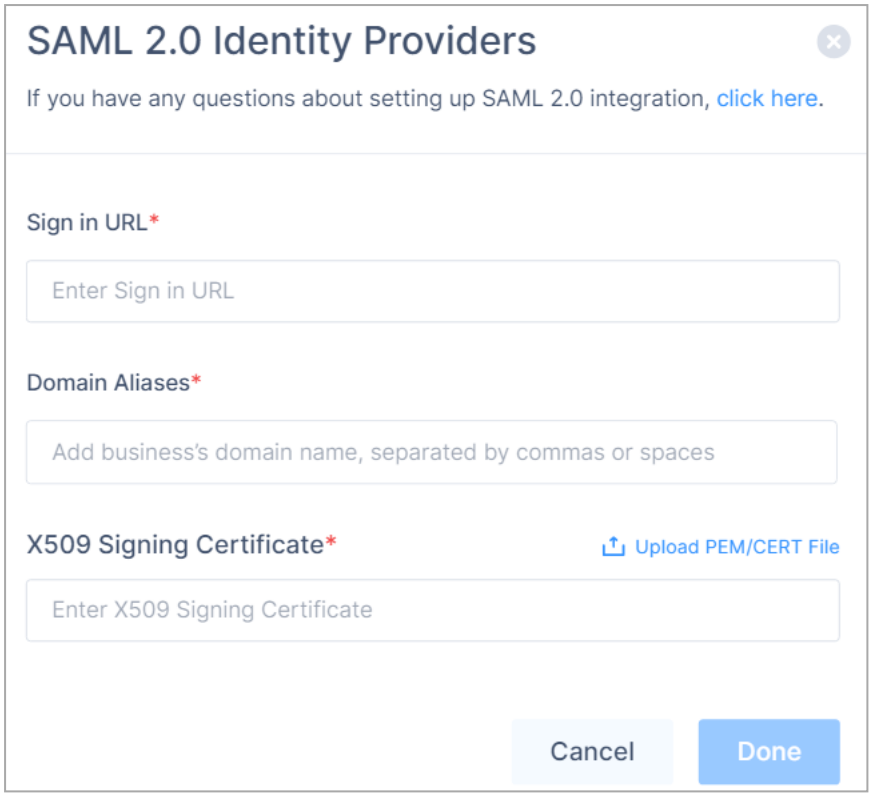
16. To copy your Login URL, go to the **Set up Check Point SASE** tile, expand **Or, view step-by-step instructions** and click .



Configure the Check Point SASE Administrator Portal

1. Log in to the SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Check Point SASE does this:

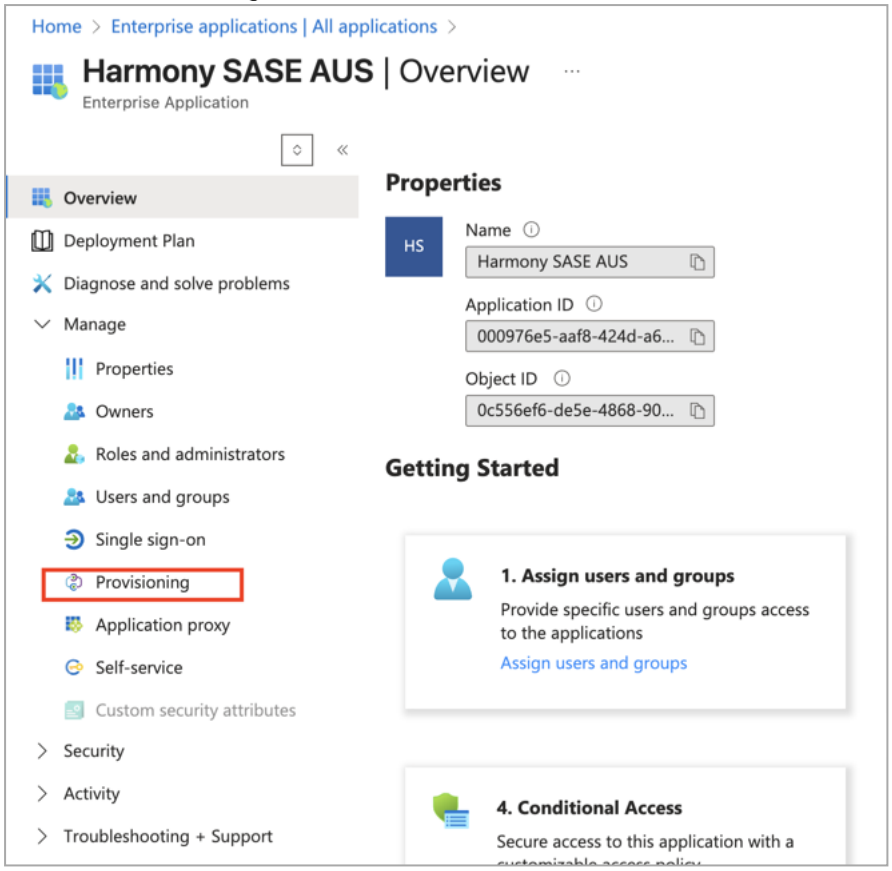
- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Preventing User Duplication in Microsoft Entra ID

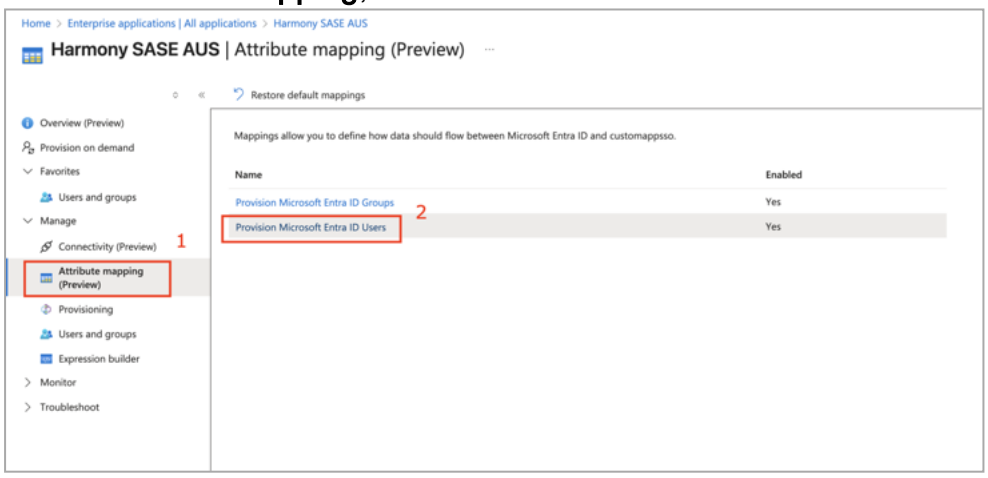
To avoid duplicate user accounts when integrating Microsoft Entra ID with SASE, configure SCIM attribute mappings:

1. Go to **Entra ID** > **Enterprise Applications** and select your Check Point SASE application.
2. Select the application name to open the configuration.

3. Click **Provisioning**.

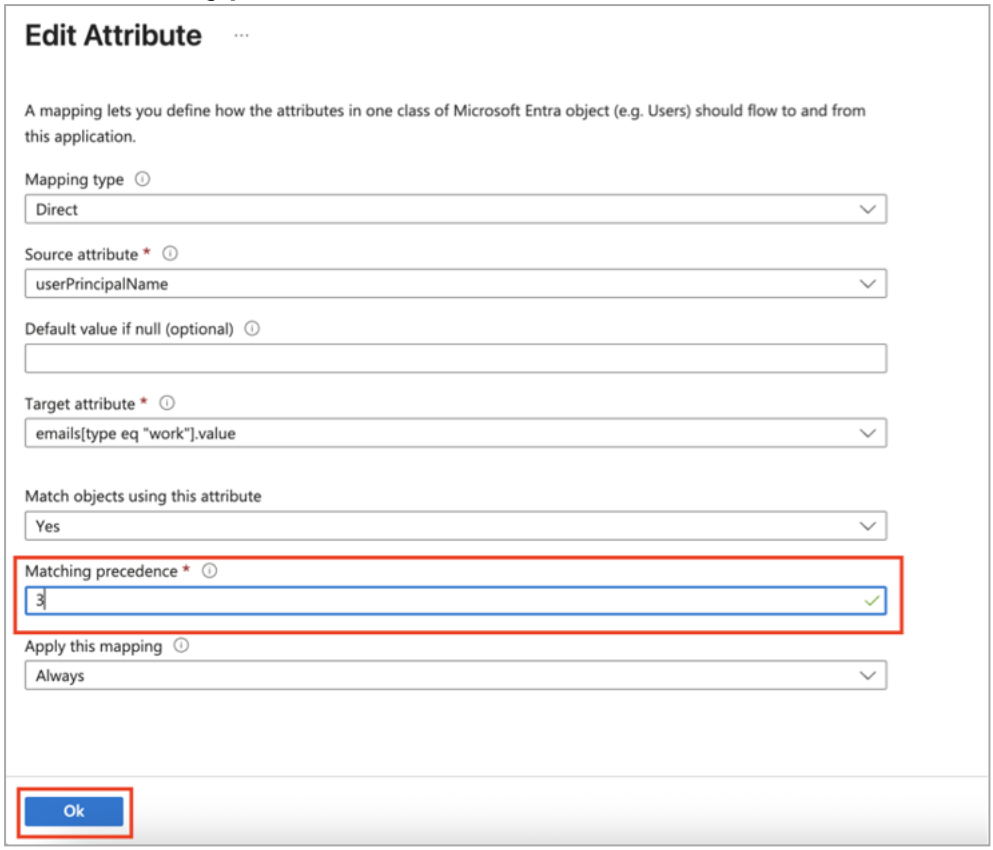


4. Under **Attribute mapping**, select **Provision Microsoft Entra ID Users**.



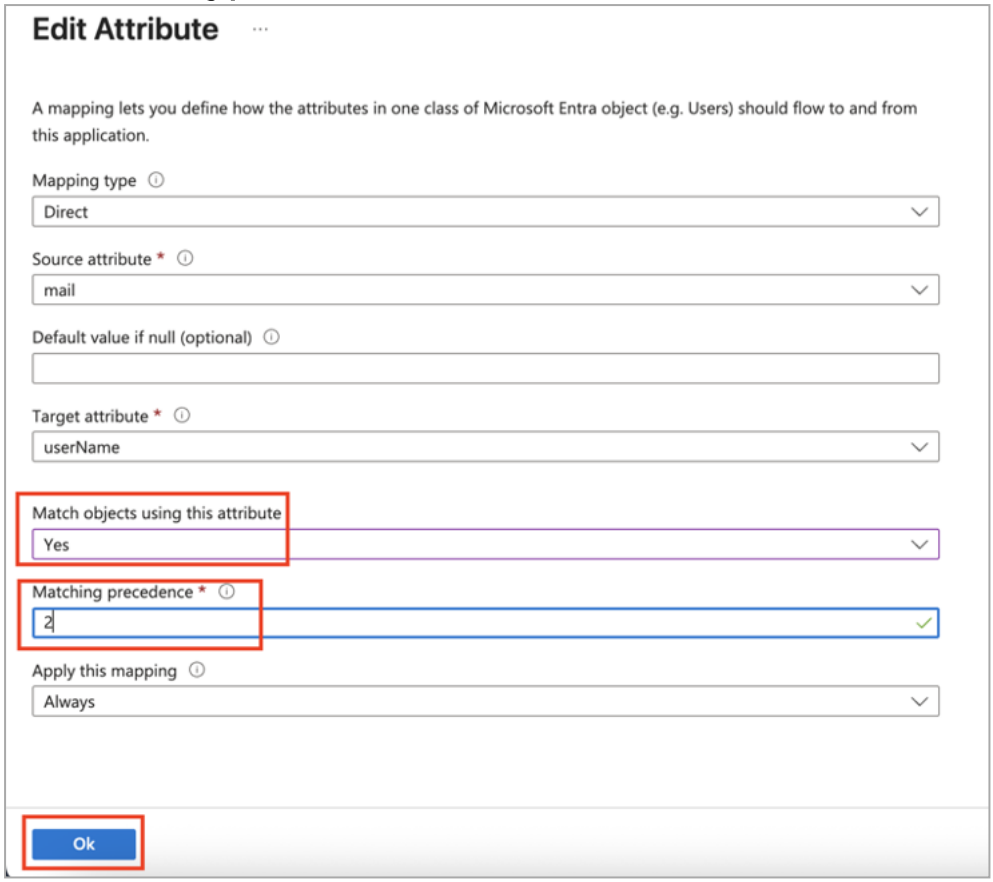
5. Locate the **emails[type eq "work"].value** attribute and click **Edit**.

6. From **Matching precedence** list, select **3**.



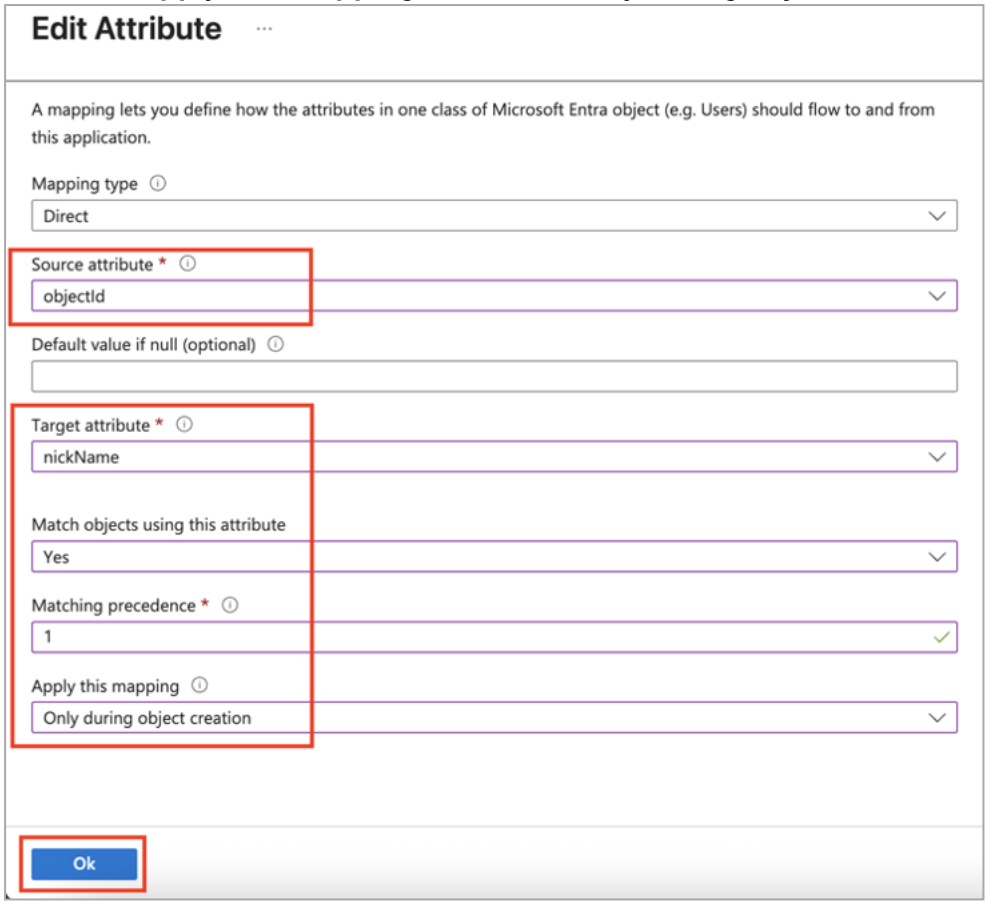
7. Click **OK**.
8. Go back to **Attribute Mappings** section and for **userName**, click **Edit**.
9. From the **Match objects using this attribute** list, select **Yes**.

10. From **Matching precedence** list, select **2**.

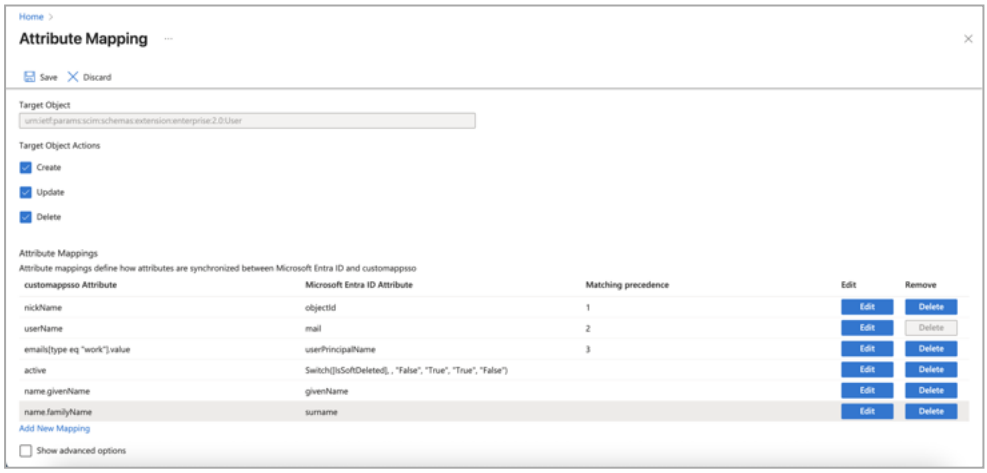


11. Click **OK**.
12. Go back to **Attribute Mappings** section and click **Add New Mapping**.
13. From the **Source attribute** list, select **objectId**.
14. From the **Target attribute** list, select **nickName**.
15. From the **Match objects using this attribute** list, select **Yes**.
16. From **Matching precedence** list, select **1**.

17. From the **Apply this mapping** list, select **Only during object creation**.



18. Click **Ok** and then click **Save**.

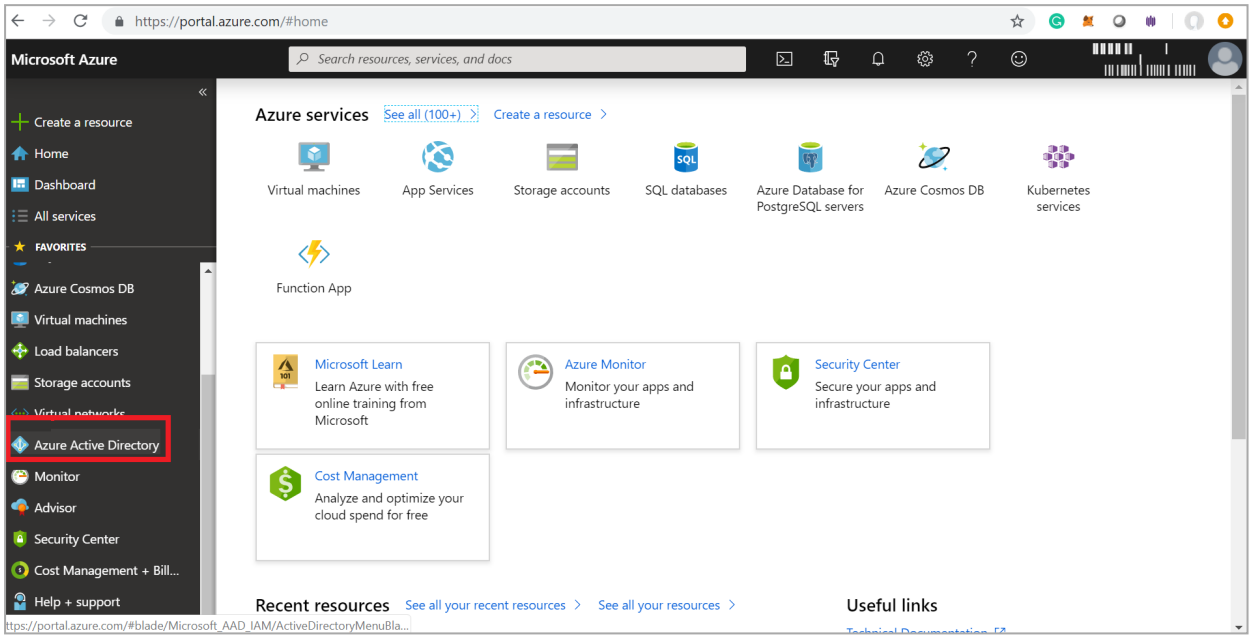


Microsoft Entra ID (formerly Azure AD) (Enterprise Application)

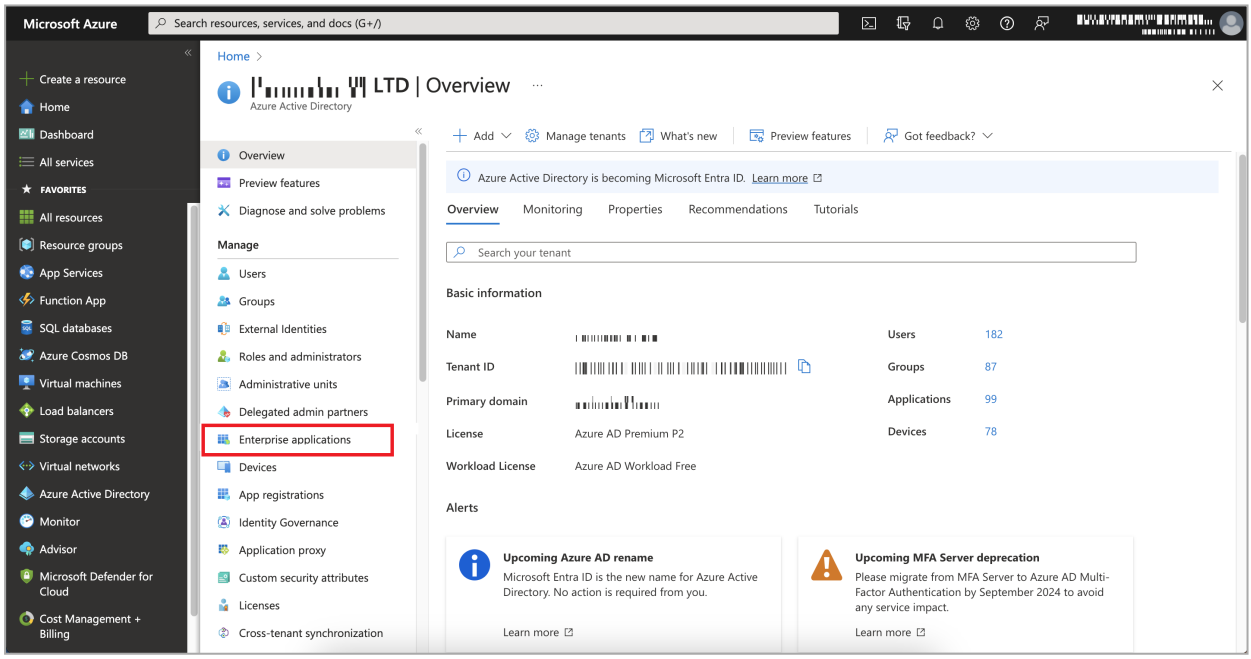
You can enable users to log in using a Microsoft Entra ID (formerly Azure AD) account, either from your computer or from the external directory.

Registering Application through the Microsoft Azure Portal

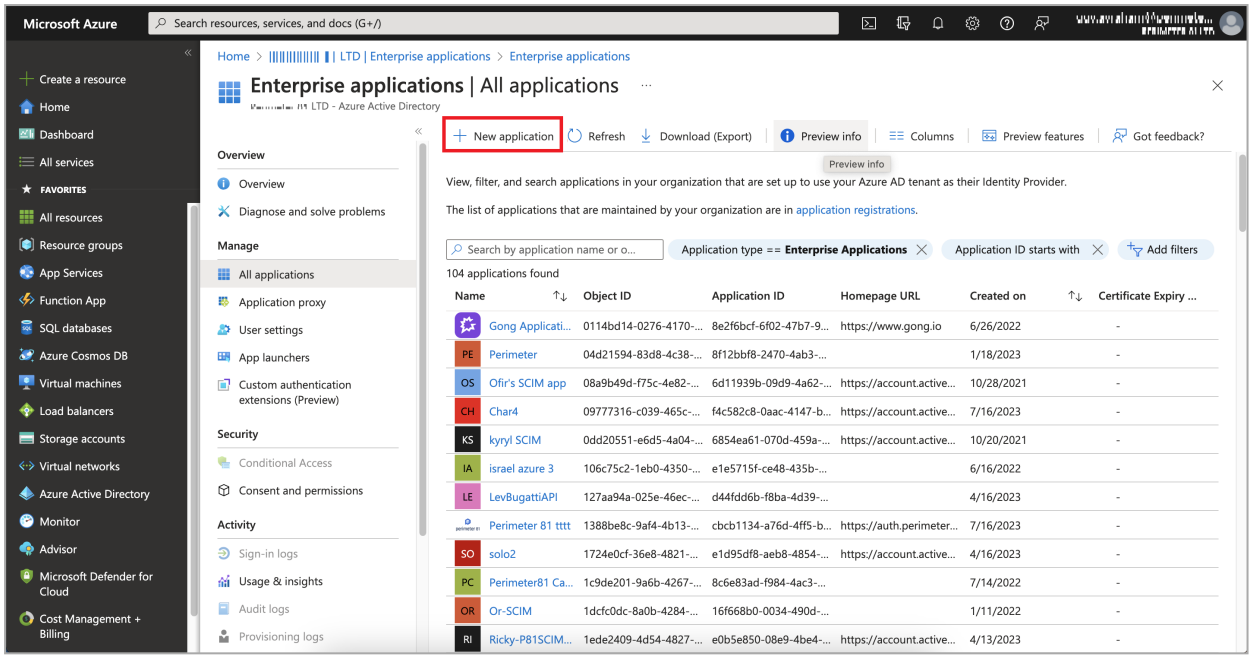
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



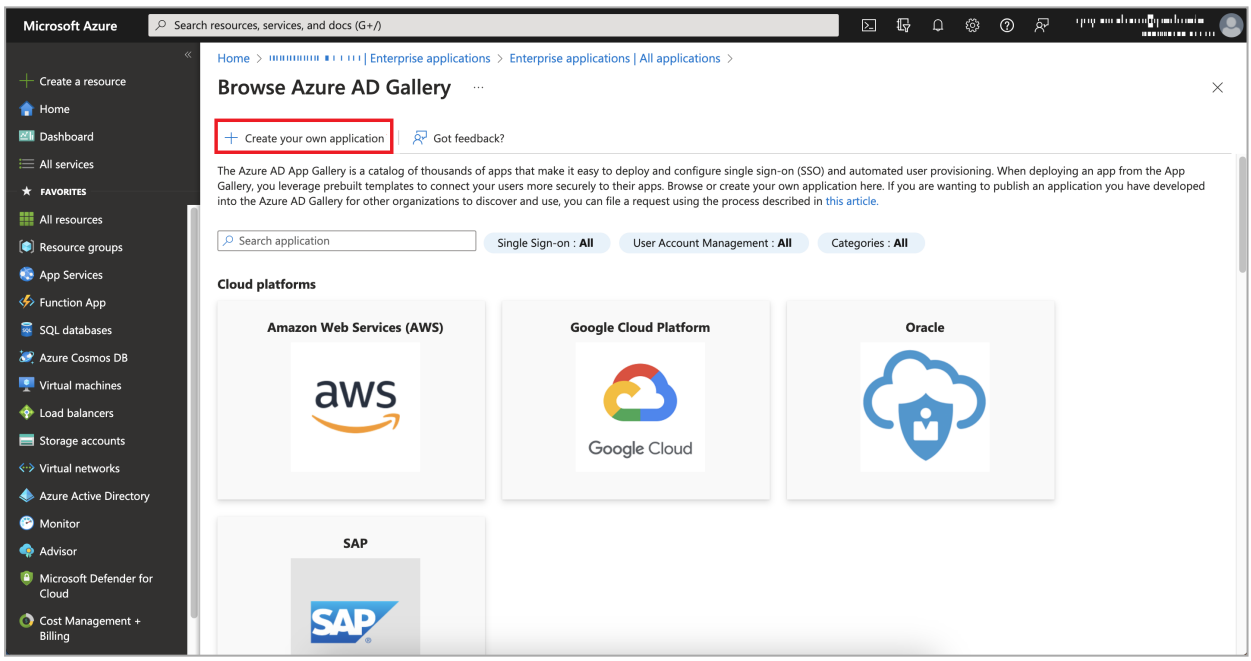
3. Go to **Manage** > **Enterprise applications**.



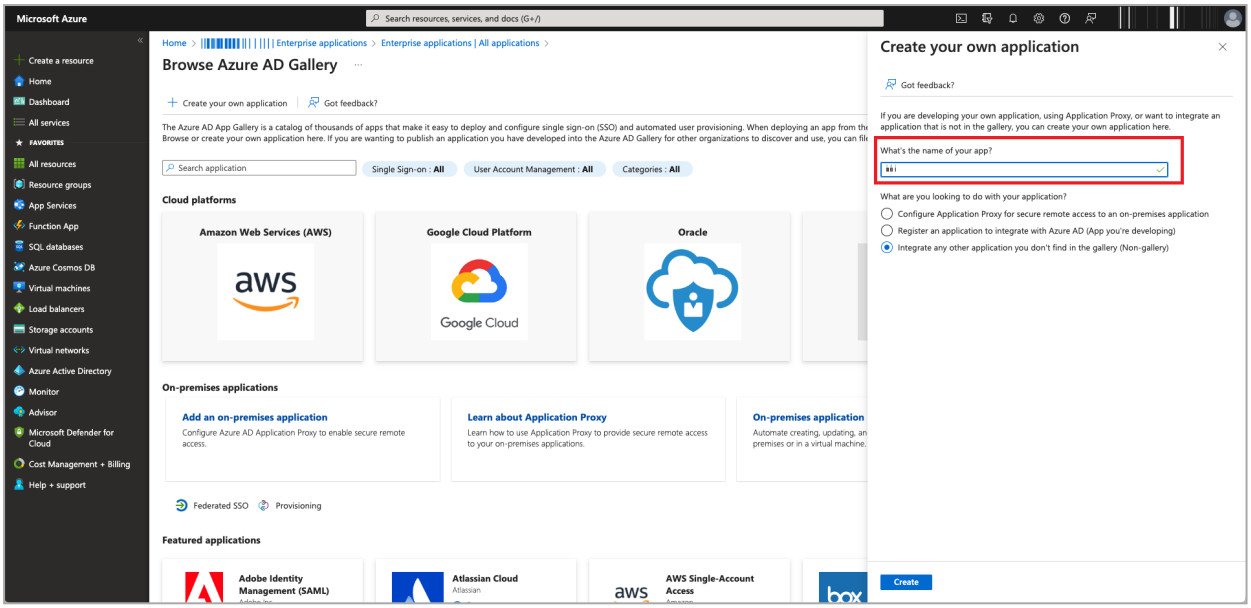
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.



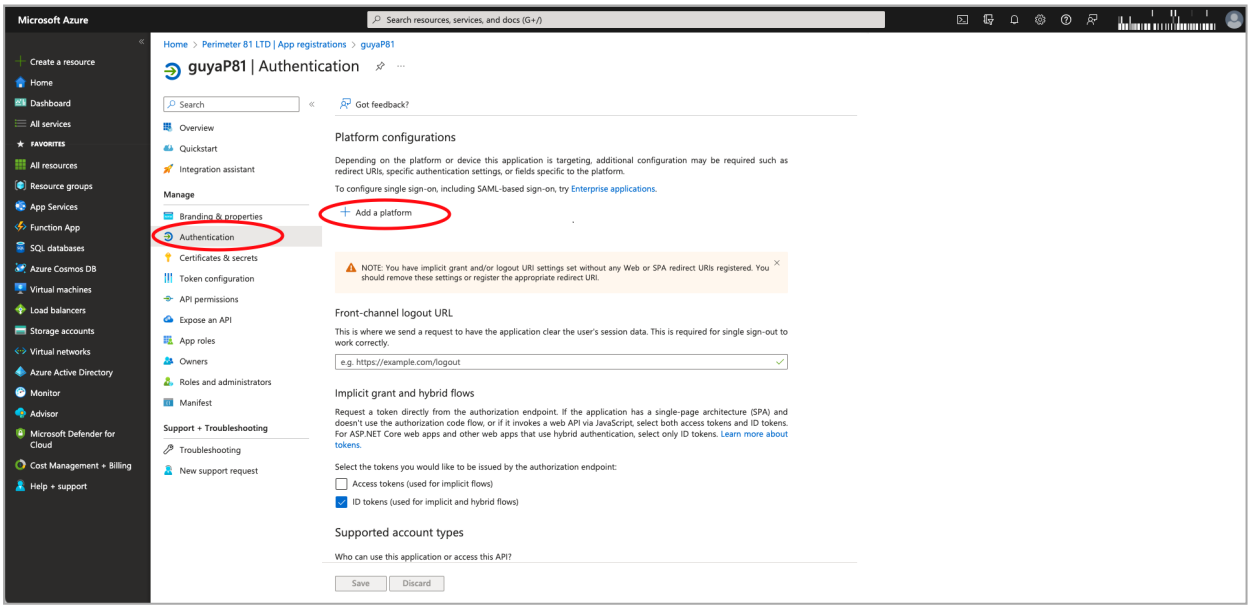
Note - Do not change the default setting.

7. Click **Create**.

   The Microsoft Azure application is created.

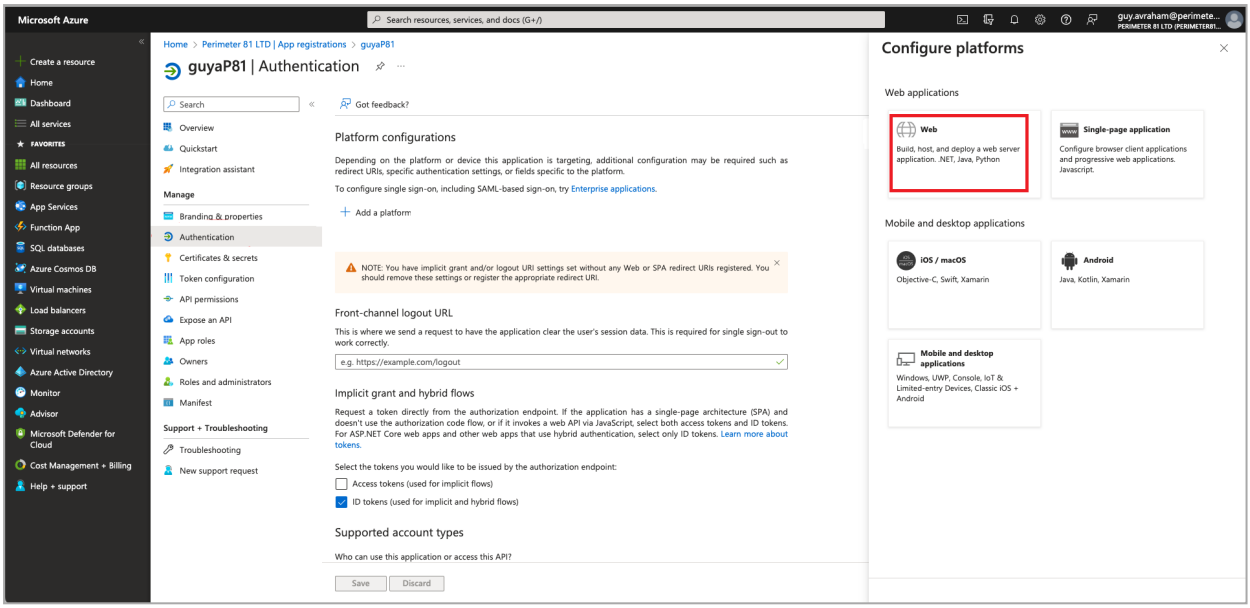
8. Browse to **App registrations**, locate and select your application.

9. Click **Manage** > **Authentication** > **Add a platform**.



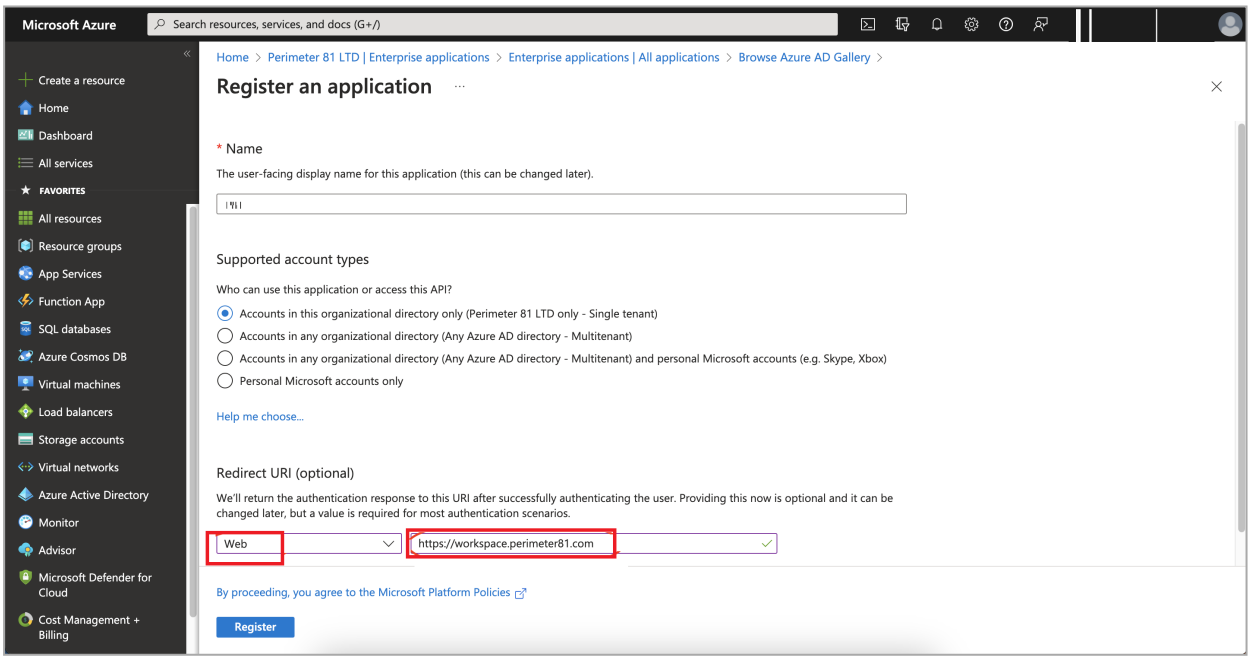
   The **Configure platforms** window appears.

10. Select **Web**.



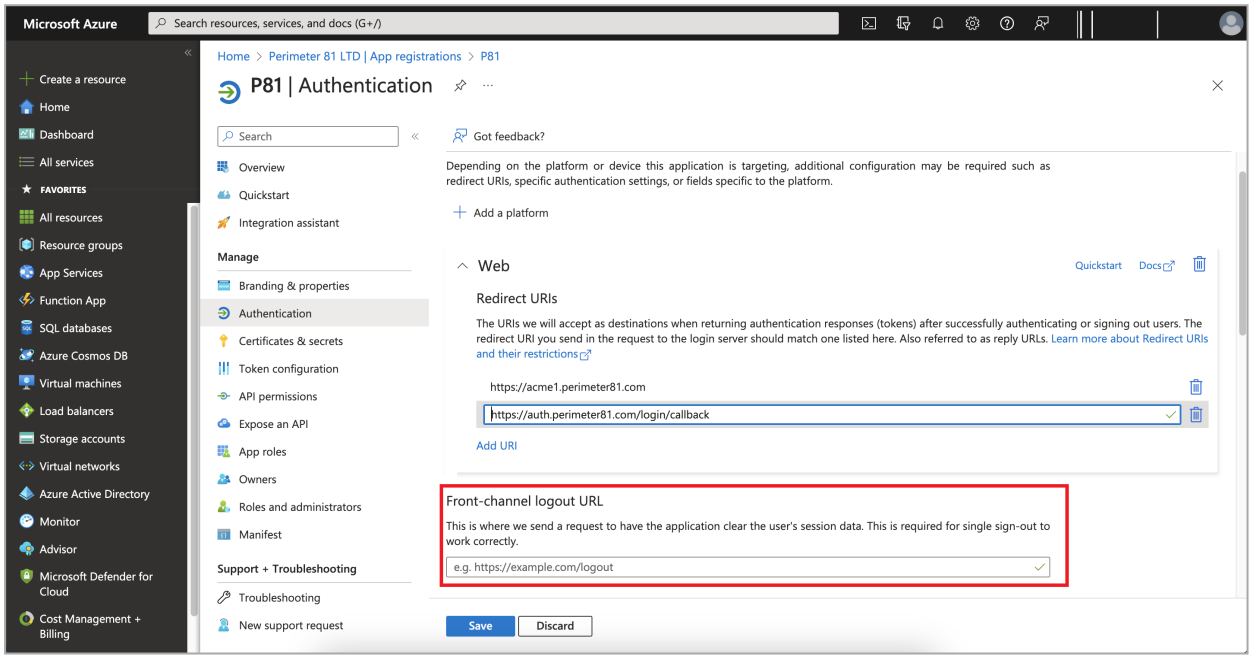
11. In the **Redirect URI (Optional)** field, select **Web** from the type of application list and enter the relevant URI where the access token is sent to:

    - For US data residency - `https://workspace.perimeter81.com`
    - For EU data residency - `https://workspace.eu.sase.checkpoint.com`
    - For AU data residency - `https://workspace.au.sase.checkpoint.com`
    - For IN data residency - `https://workspace.in.sase.checkpoint.com`

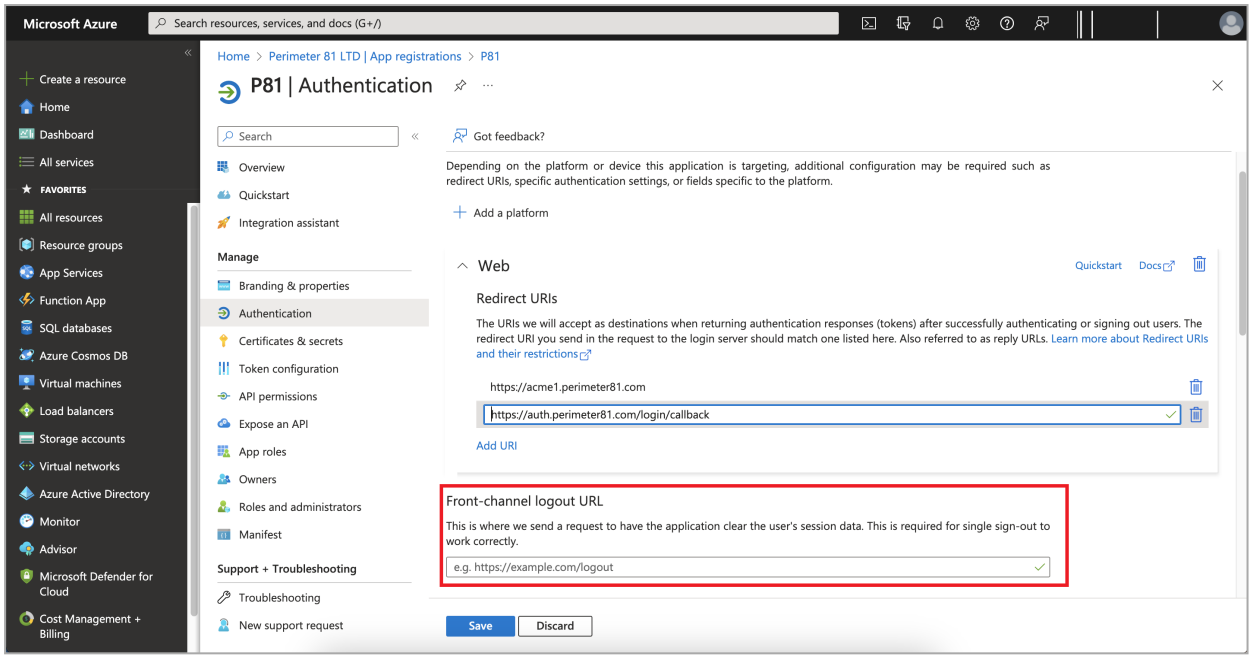


12. Click **Configure**.
13. In the **Redirect URIs** section, enter:

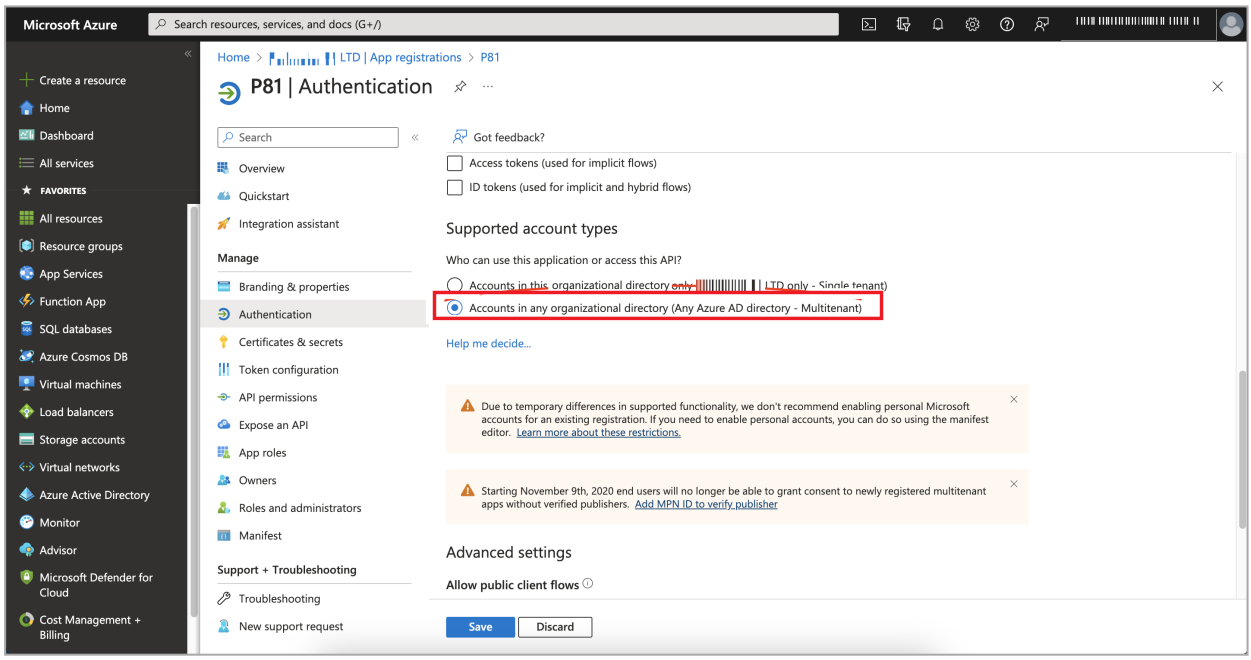
- For US data residency - `https://auth.perimeter81.com/login/callback`
- For EU data residency - `https://auth.eu.sase.checkpoint.com/login/callback`
- For AU data residency - `https://auth.au.sase.checkpoint.com/login/callback`
- For IN data residency - `https://auth.in.sase.checkpoint.com/login/callback`



14. In the **Front-channel logout URL** section, enter your workspace name:
    - For US data residency - `https://{{WORKSPACE}}.perimeter81.com`
    - For EU data residency - `https://{{WORKSPACE}}.eu.sase.checkpoint.com`
    - For AU data residency - `https://{{WORKSPACE}}.au.sase.checkpoint.com`
    - For IN data residency - `https://{{WORKSPACE}}.in.sase.checkpoint.com`
      where `{{WORKSPACE}}` refers to your Check Point SASE workspace name.



15. To allow access from external organizations, in the **Supported account types** section, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.



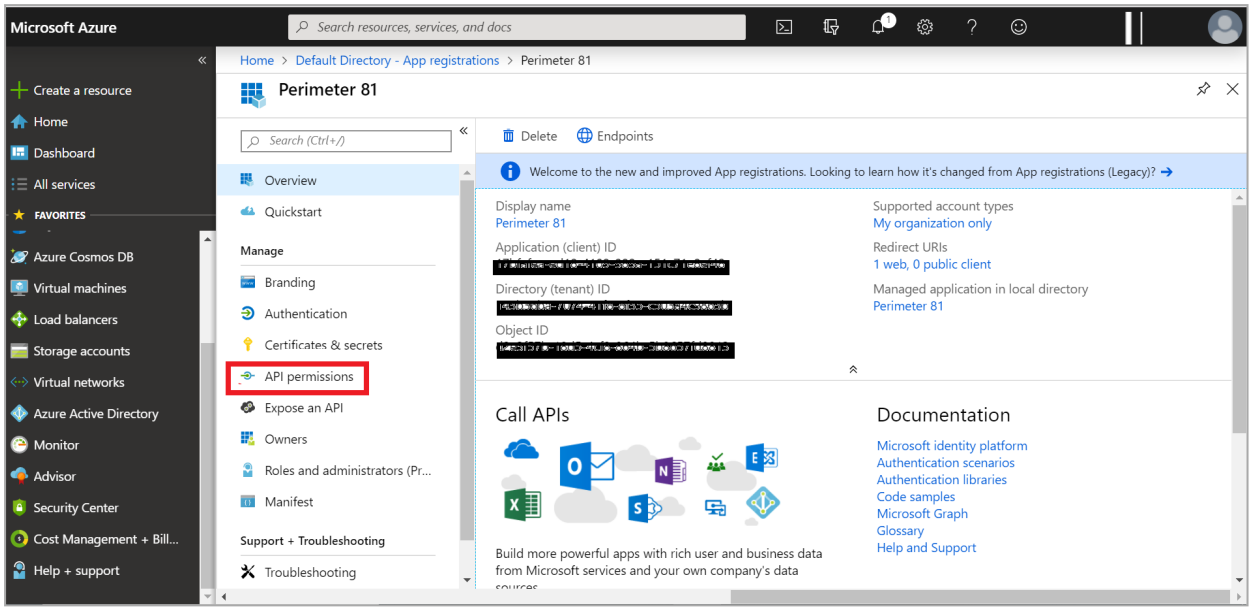
16. Click **Save**.

Configuring the Permissions for the Application

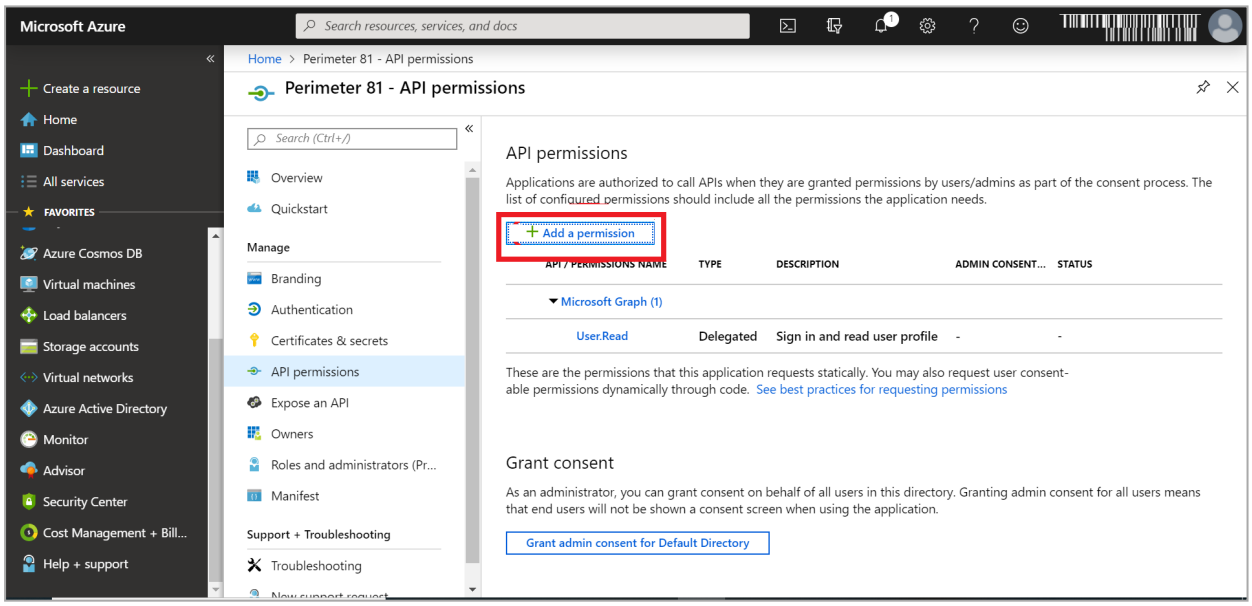
To configure the permissions for the application:

1. Log in to your Microsoft Azure Portal.
2. Click **Identity** > **Applications** > **App registrations** > **All applications**.

3. Select your application.
4. Click **Overview** > **Manage** > **API Permissions**.

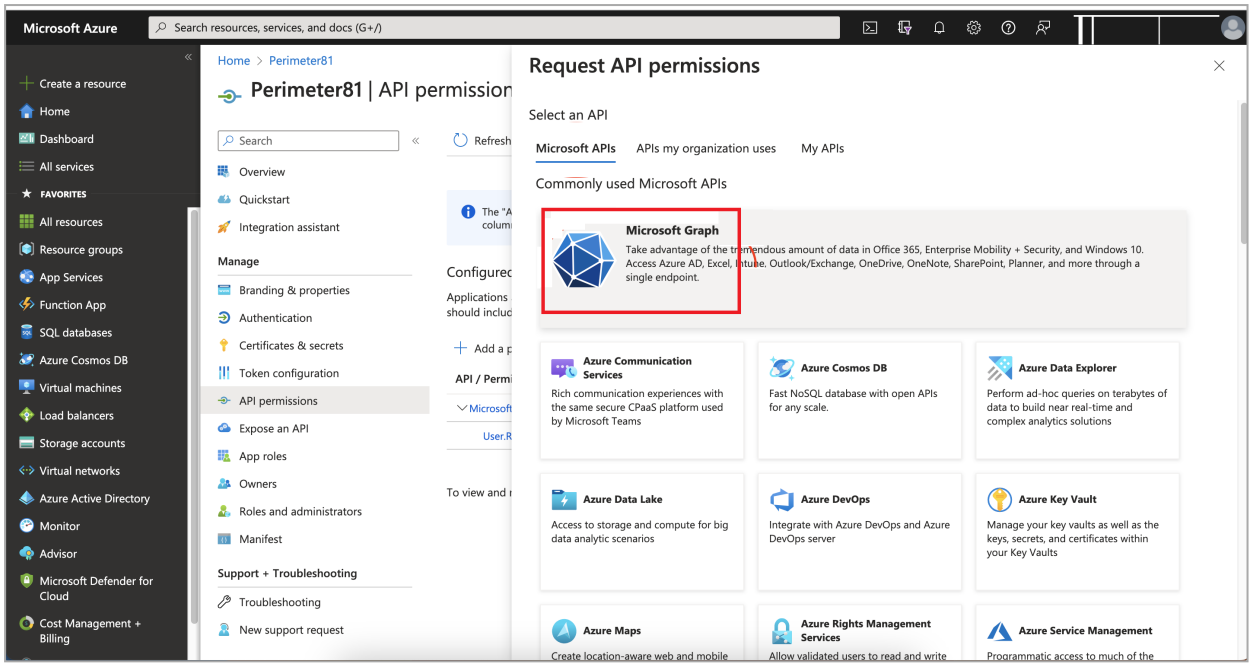


5. Click **Add a permission**.

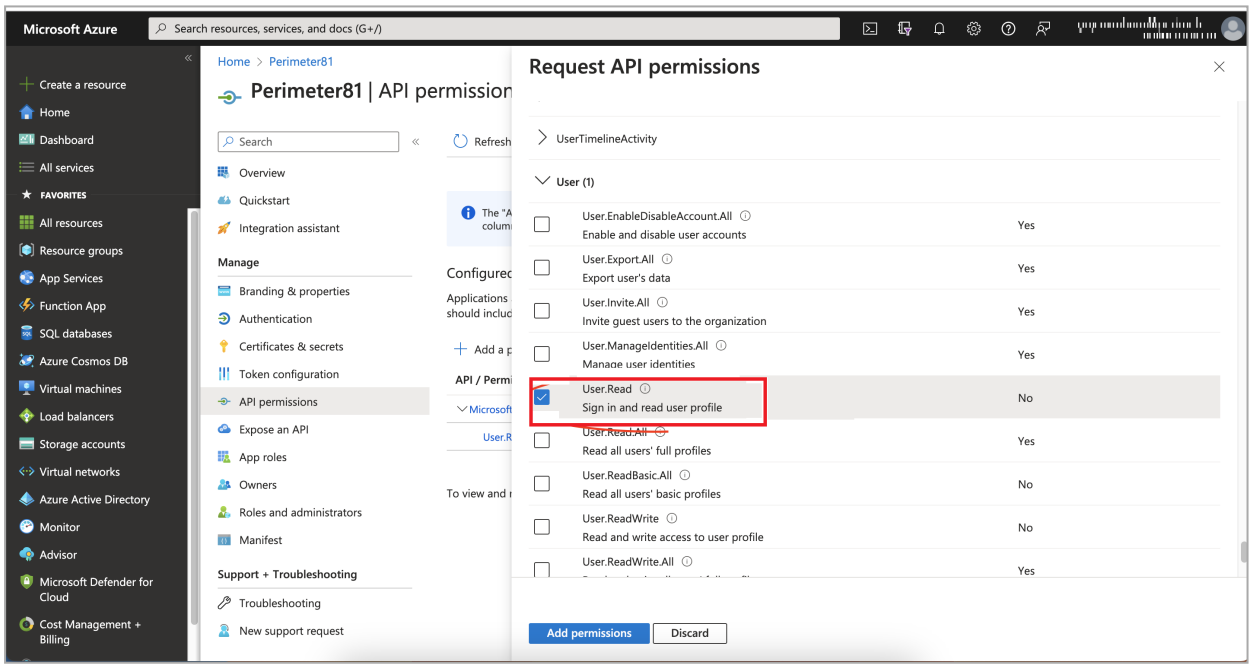


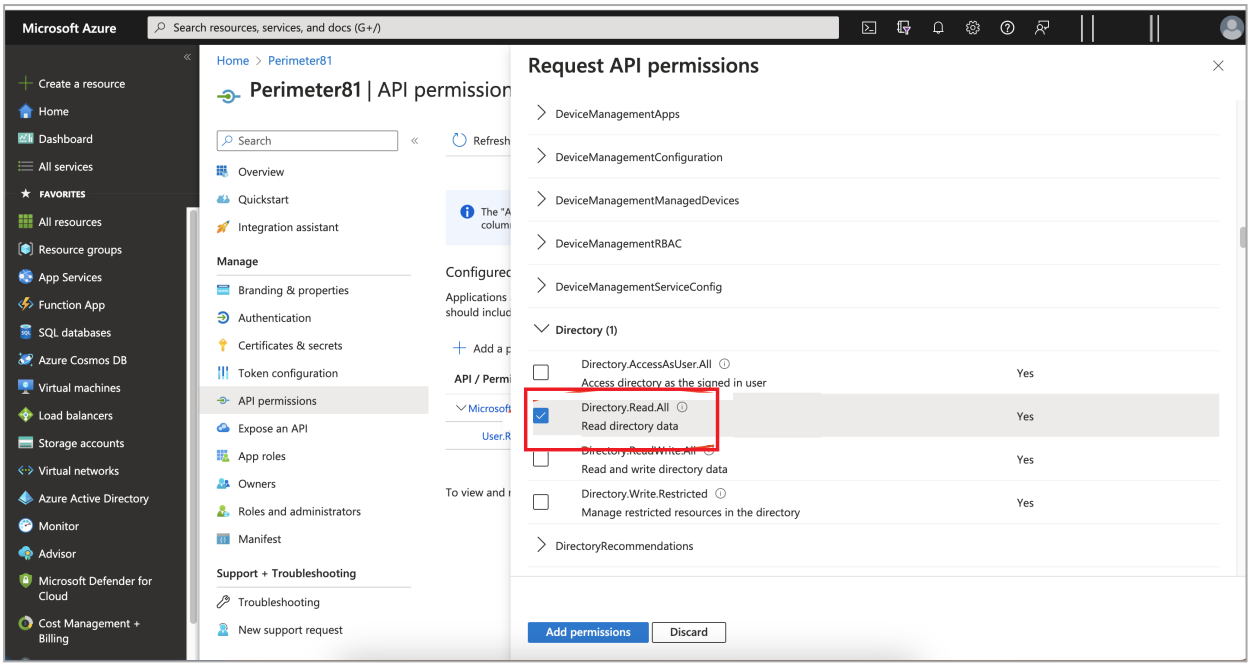
The **Request API permissions** page appears.

6. Click **Microsoft APIs** and select **Microsoft Graph** from the list of available APIs to change the access level.



7. Click **Delegated permissions**.
8. Select the **User.Read** and **Directory.Read.All** checkbox to modify the permissions so your application can read the directory..



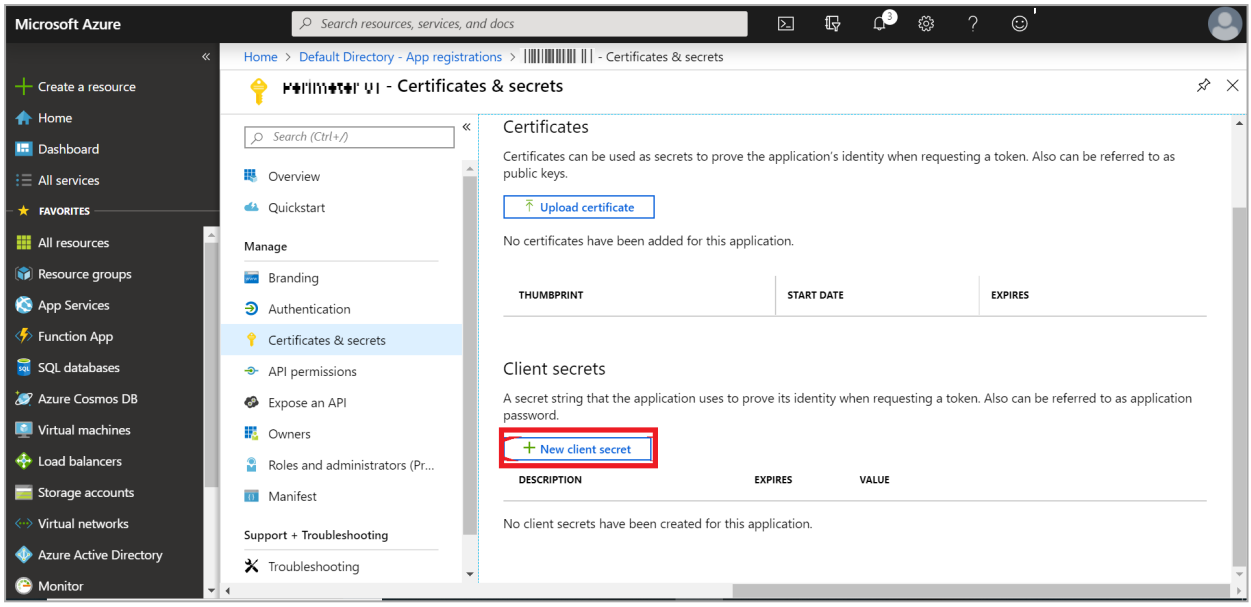


9. Click **Add permissions** > **Configured permissions** > **Grant admin consent** for approval of your app API permissions.
10. Click **Yes**.

    Your application gets the granted permissions.
11. To enable user group support, enable:
    a. **Application Permissions**: Read directory data.
    b. **Delegated permissions**: Access the directory as the signed in user.
12. Click **Save** to save the changes.
13. To remove the Windows Azure Active Directory API permission, see *"Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions" on page 1129*.

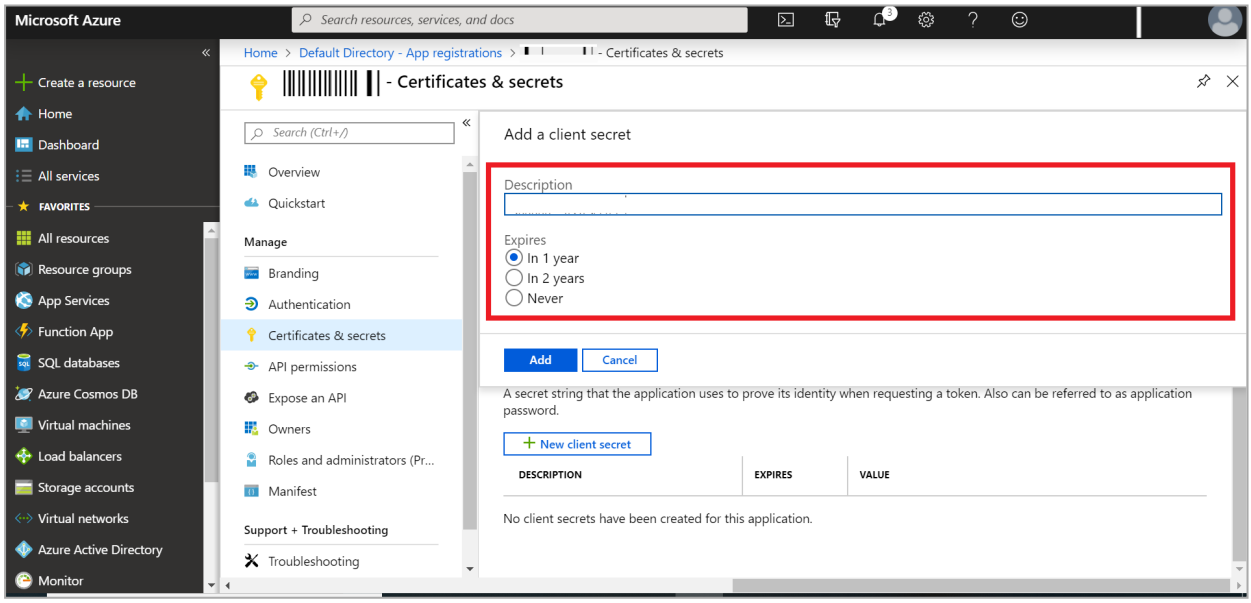
Configuring the Key

1. Log in to your Microsoft Azure Portal.
2. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
3. Browse to **App registrations**, locate and select your application.
4. Go to **Manage** > **Certificates & secrets**.
5. Click **New client secret**.



The **Add a Client secret** window appears.

6. In the **Description** filed, enter a name for the key.
7. In the **Expires** field, select the expiry:
   - **In 1 year**
   - **In 2 years**
   - **Never**



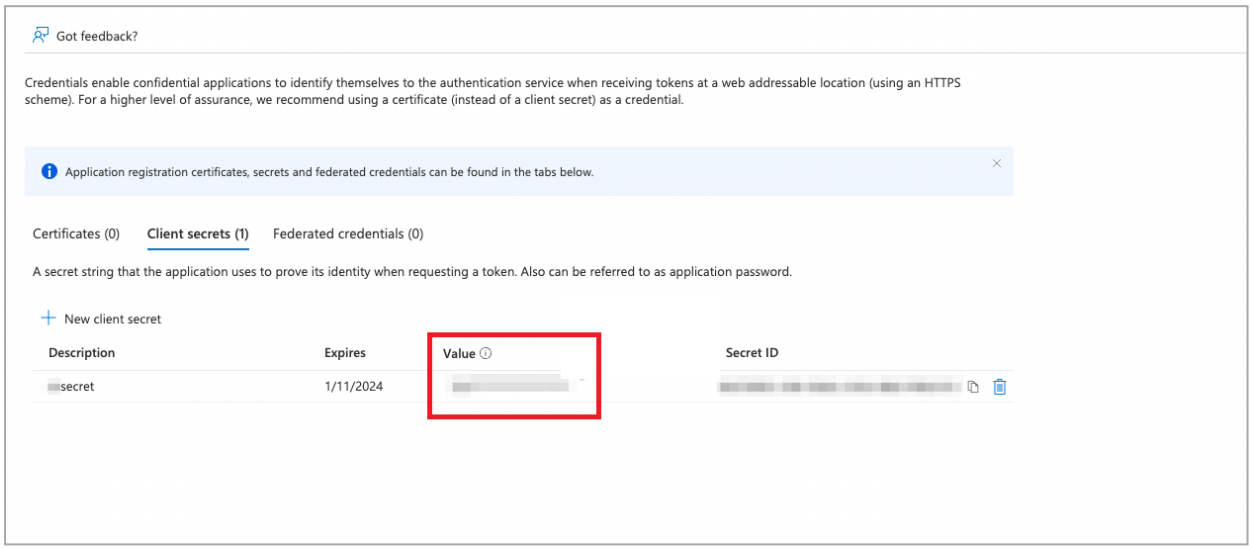
8. Click **Add**.

   The new key is added.

9. To get the secret value of the key, go to the **Client secrets** tab and copy the secret **Value**.

   This value is the **Client Secret** in SASE Admin console. .

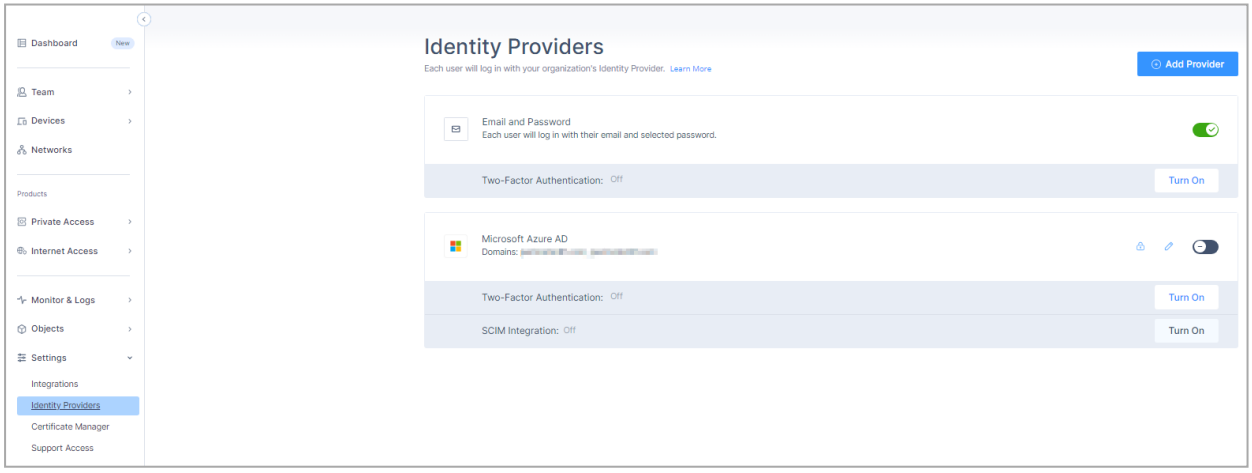
   Note - The Secret value of the key need to be copied before you close the screen. If not, you need to create a new key.



Configuring IDP Connection in SASE

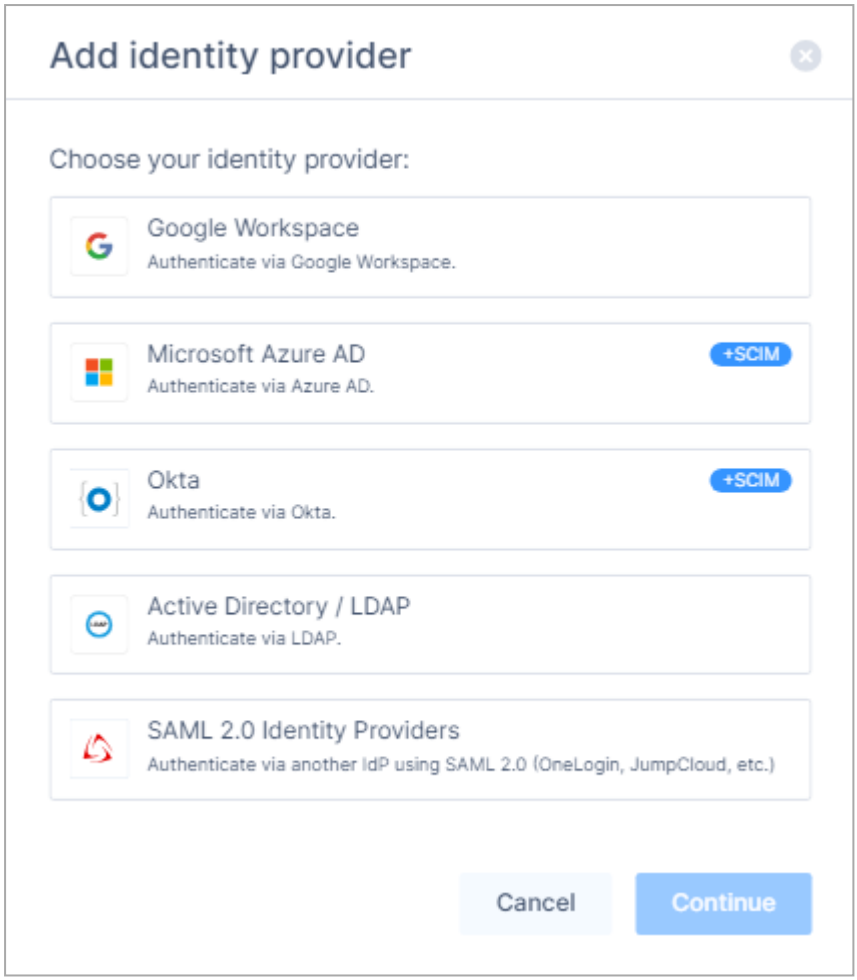
1. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.

   The **Identity Providers** page appears.



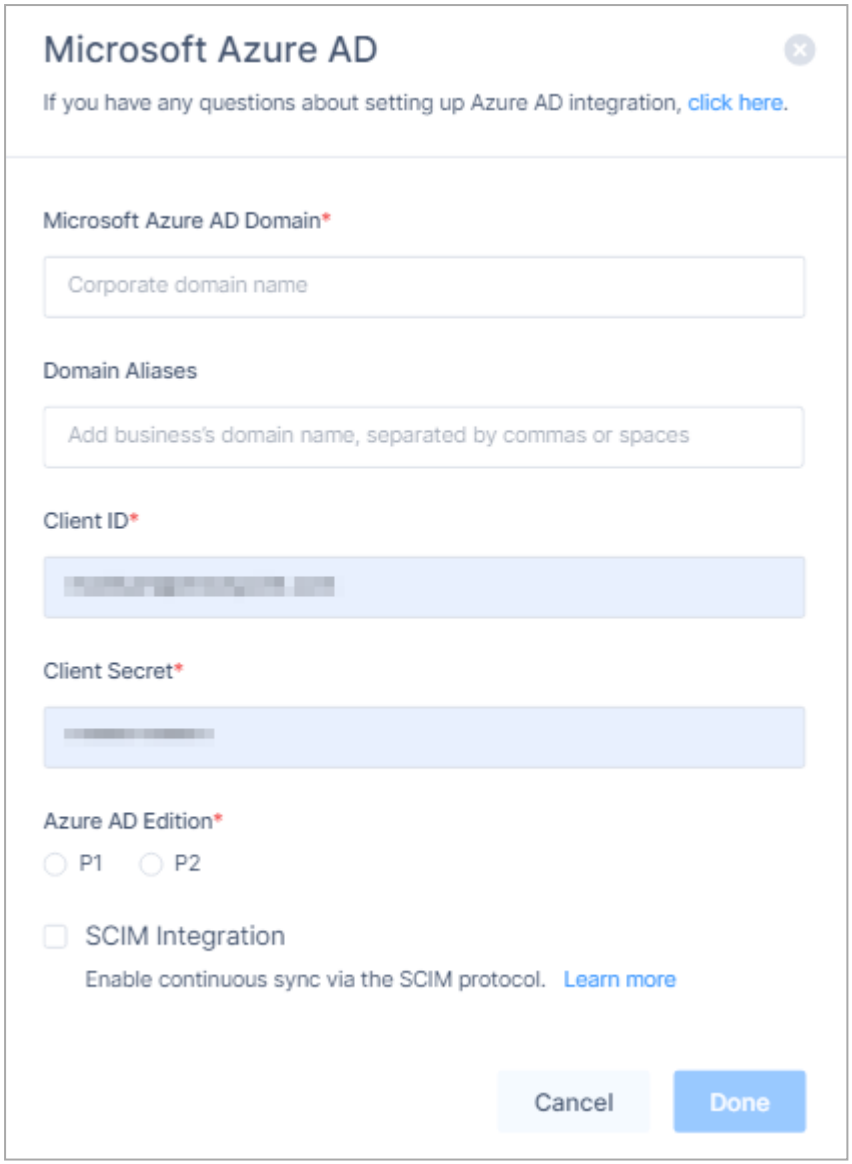
2. Click **Add Provider**.

   The **Add identity provider** window appears.



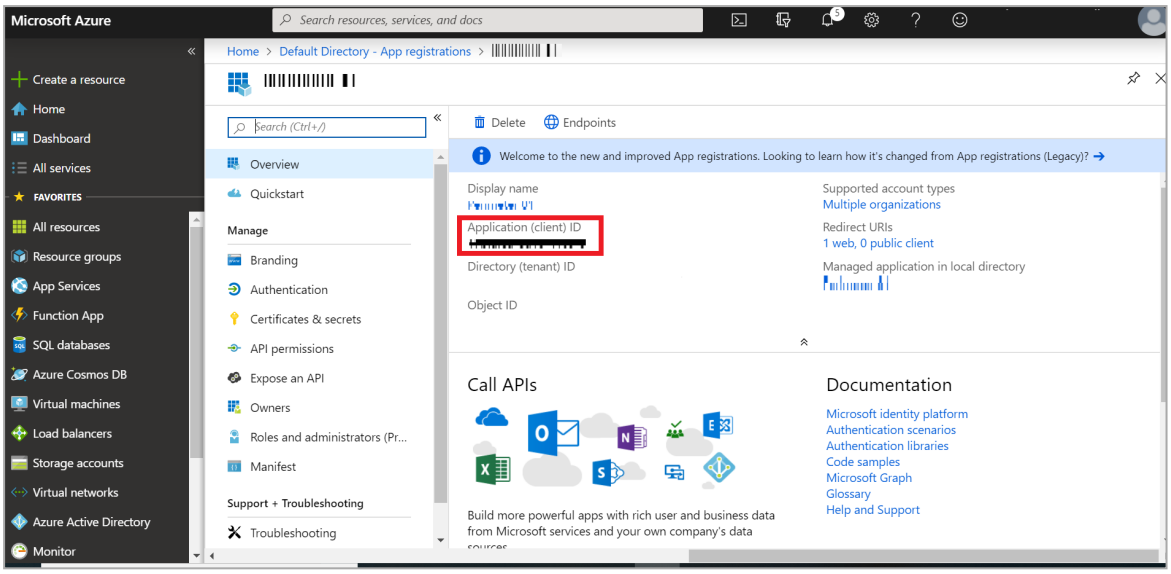
3. Select **Microsoft Azure AD**.
4. Click **Continue**.

   The **Microsoft Azure AD** page appears.



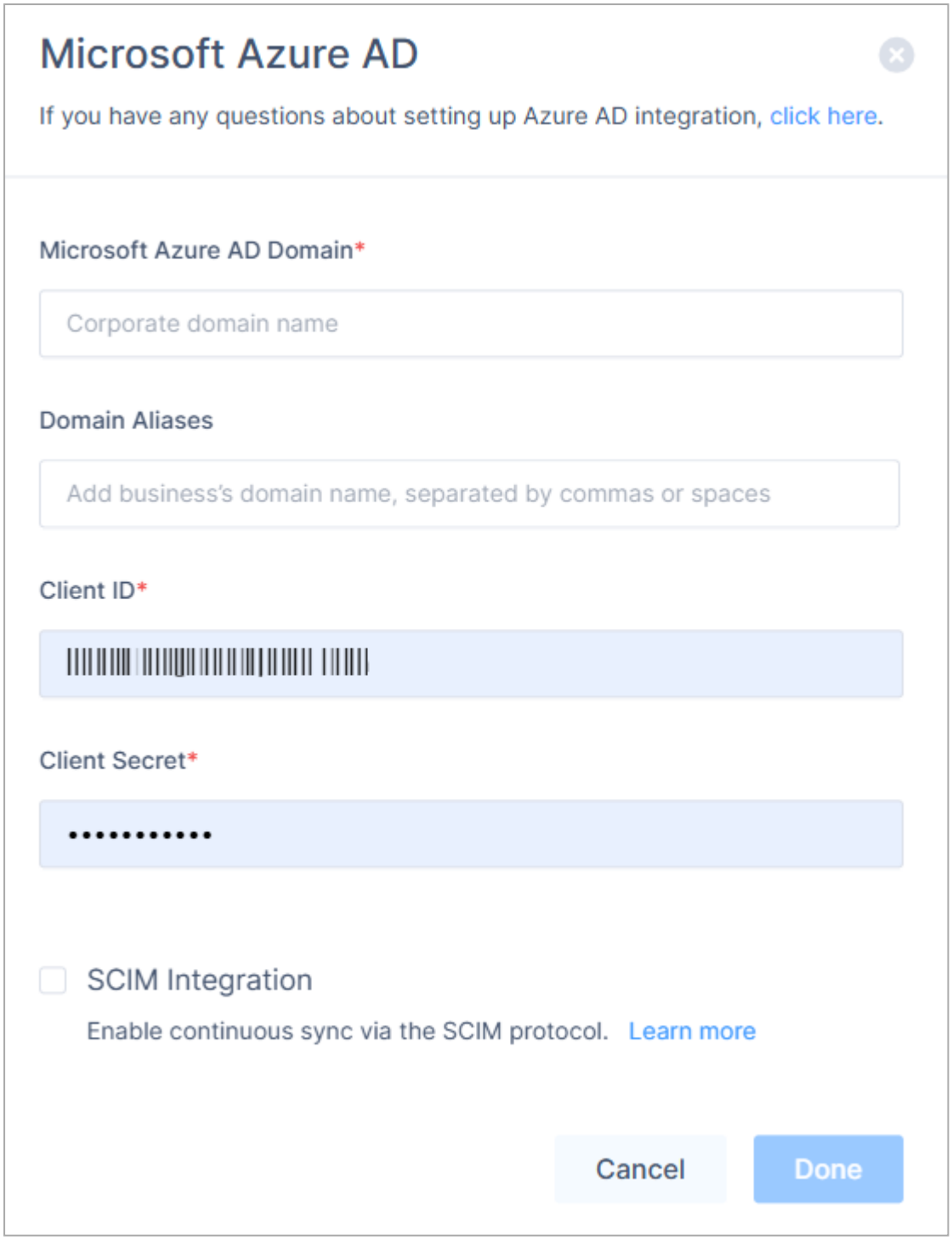
5. In the **Microsoft Azure AD Domain** field, enter the domain name.
6. In the **Domain Aliases** field, enter the email ID(s) separated by commas or spaces.
7. In the **Client ID** field, enter the **Application (client) ID** in Microsoft Azure AD:
   a. Log in to your Microsoft Azure Portal.
   b. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
   c. Browse to **App registrations**, locate and select your application.

d. Go to **Overview** > **Application (client) ID**.



e. Copy the **Application (cient) ID** value.

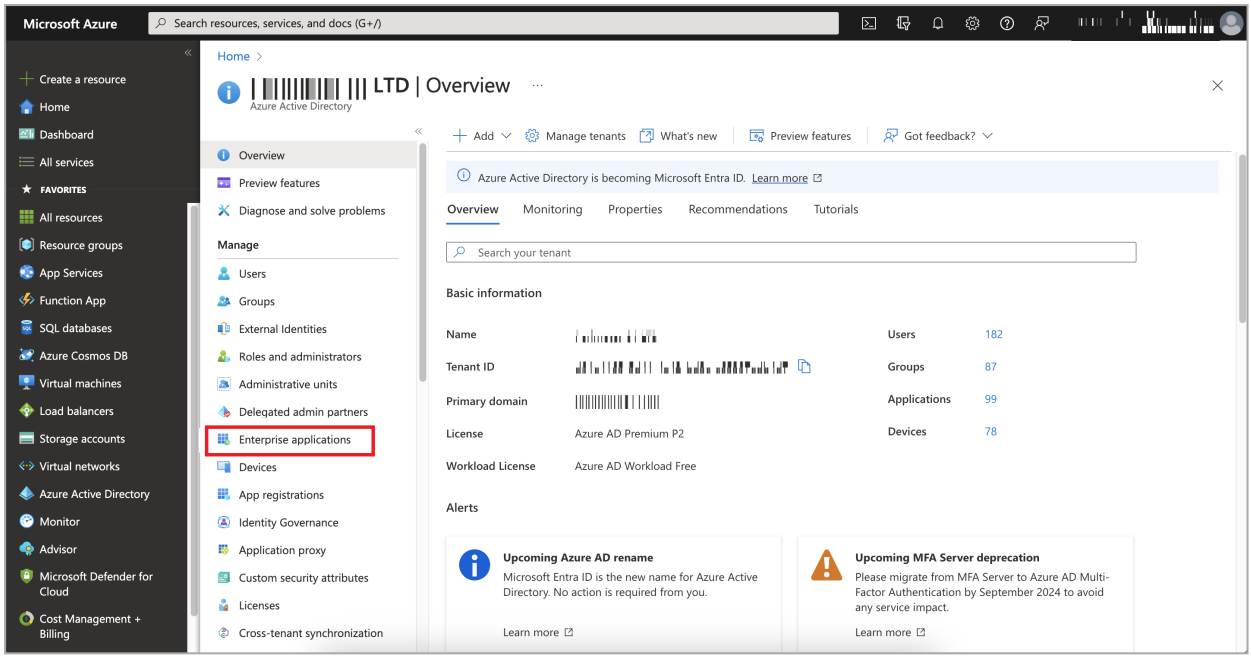
8. In the **Client Secret** field, enter the secret value. See step 9 in Configuring the Key.



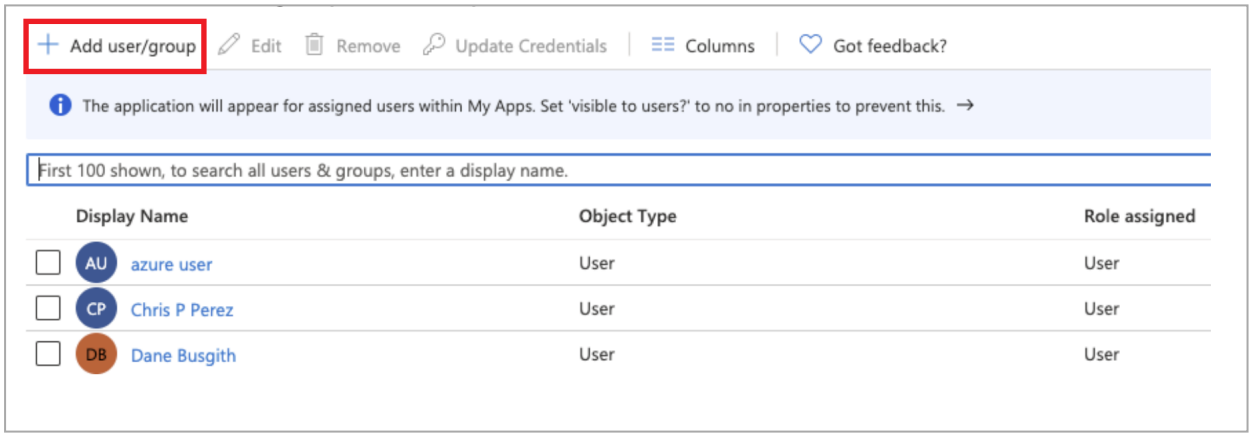
9. Select the **SCIM Integration** checkbox.
10. Click **Done**.

Assigning Users and Groups in Microsoft Azure

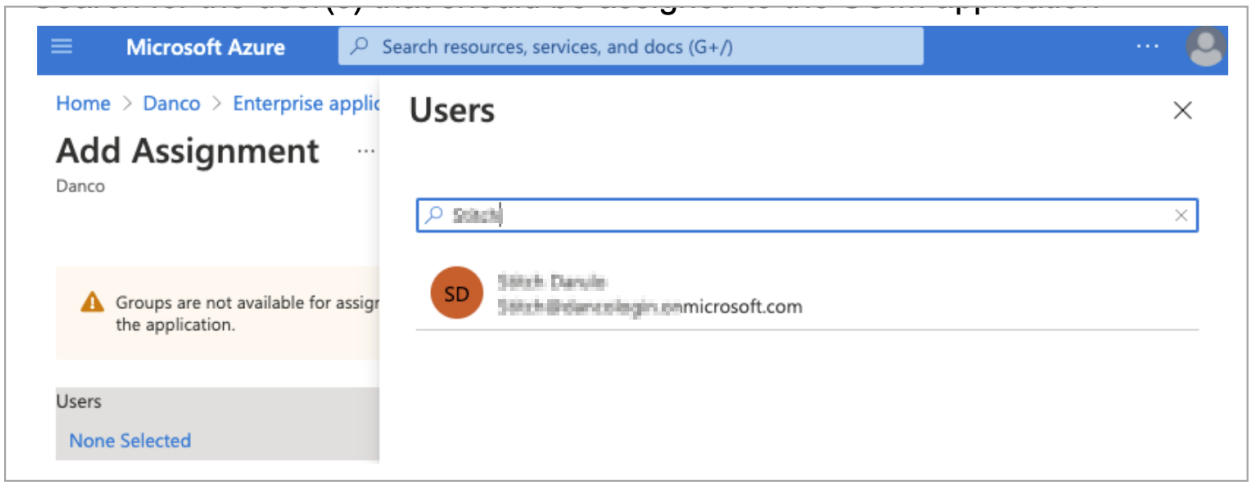
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.
3. Go to **Manage** > **Enterprise applications**.



4. Search and select your application.
5. Go to **Users and groups** and click **Add user/group**.



6. Click **None Selected** in **Users**.



7. Search and select the user(s) or group(s) you want to add to the application.

   Note - Special characters are not supported in groups.

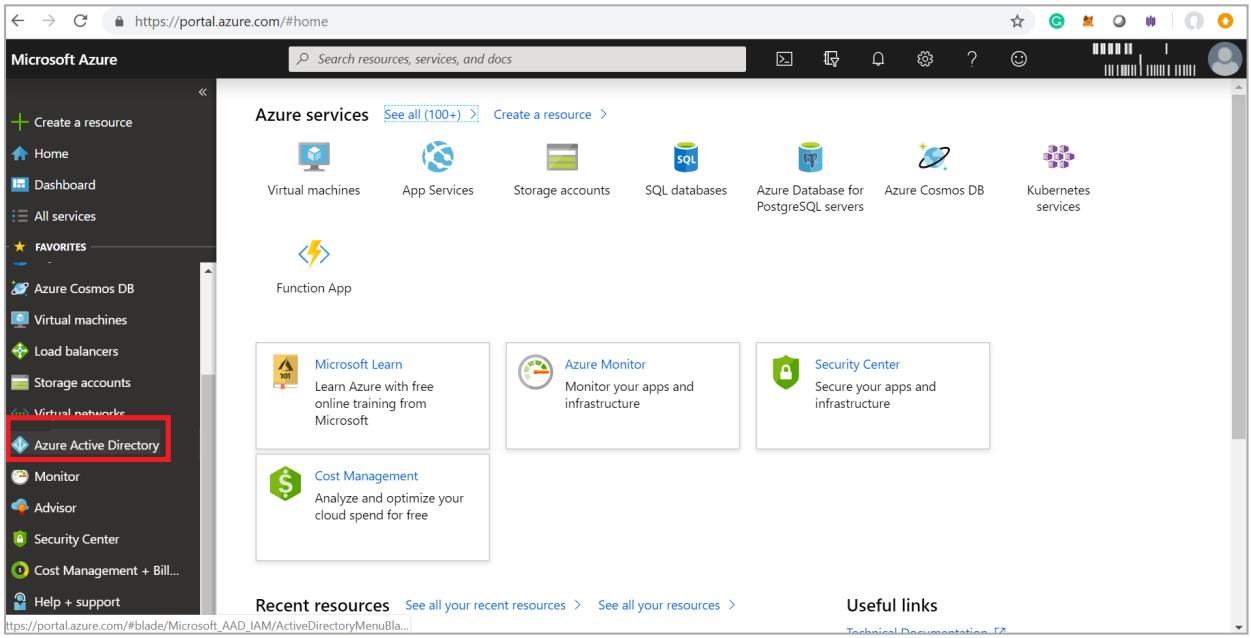
8. Click **Select**.
9. Click **Assign**.

Microsoft Entra ID (formerly Azure AD) (App Registration)

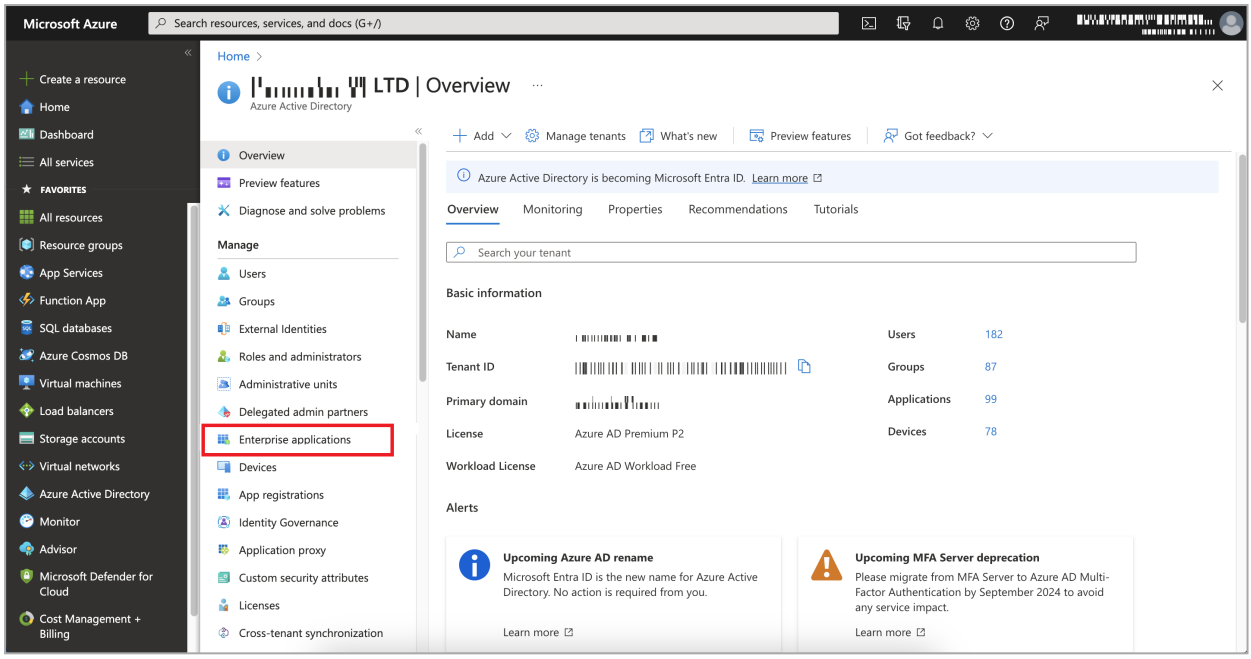
You can enable users to log in using a Microsoft Entra ID (formerly Azure AD) account, either from your computer or from the external directory.

Registering Application through the Microsoft Azure Portal

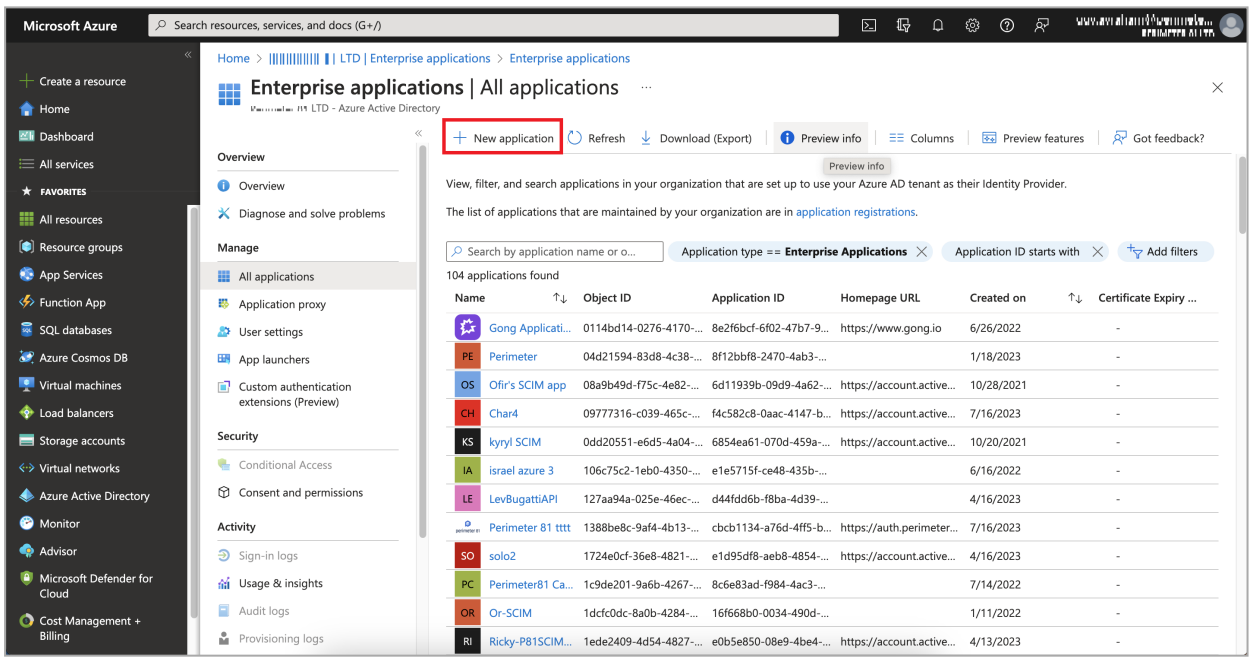
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



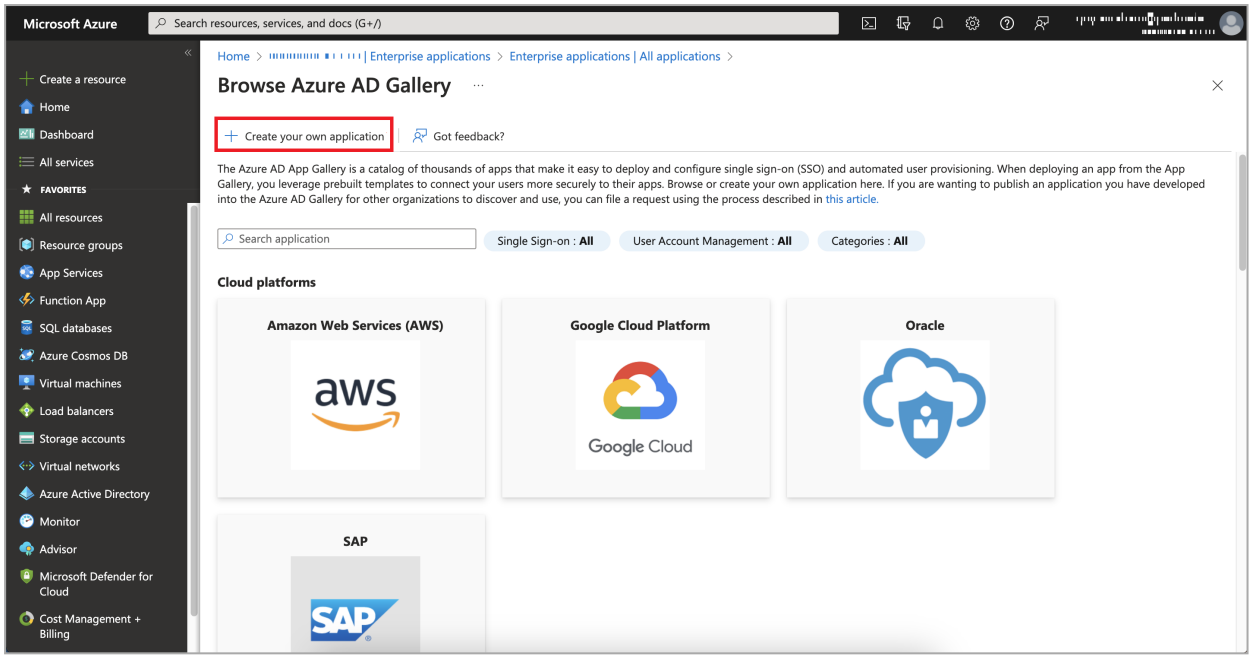
3. Go to **Manage** > **Enterprise applications**.



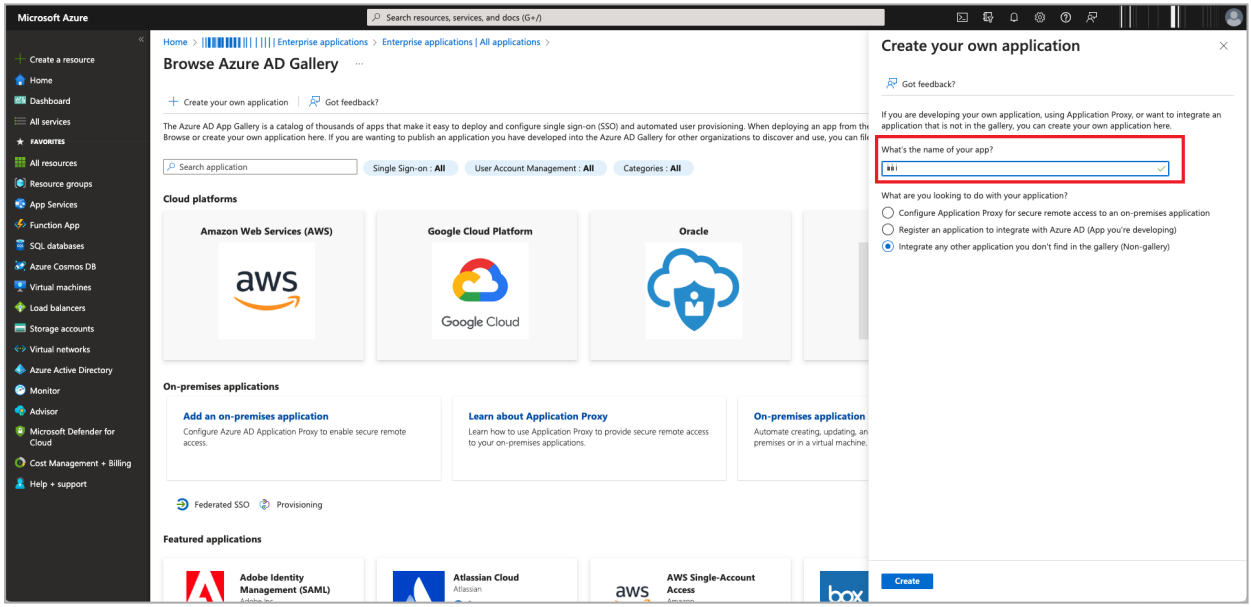
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.

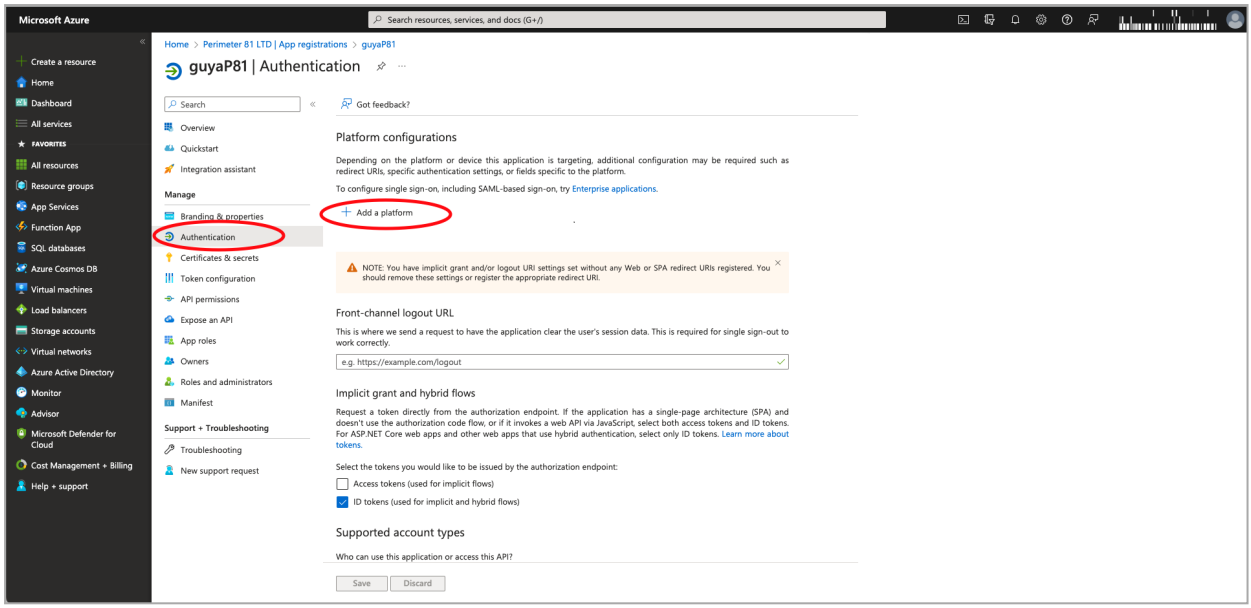


Note - Do not change the default setting.

7. Click **Create**.

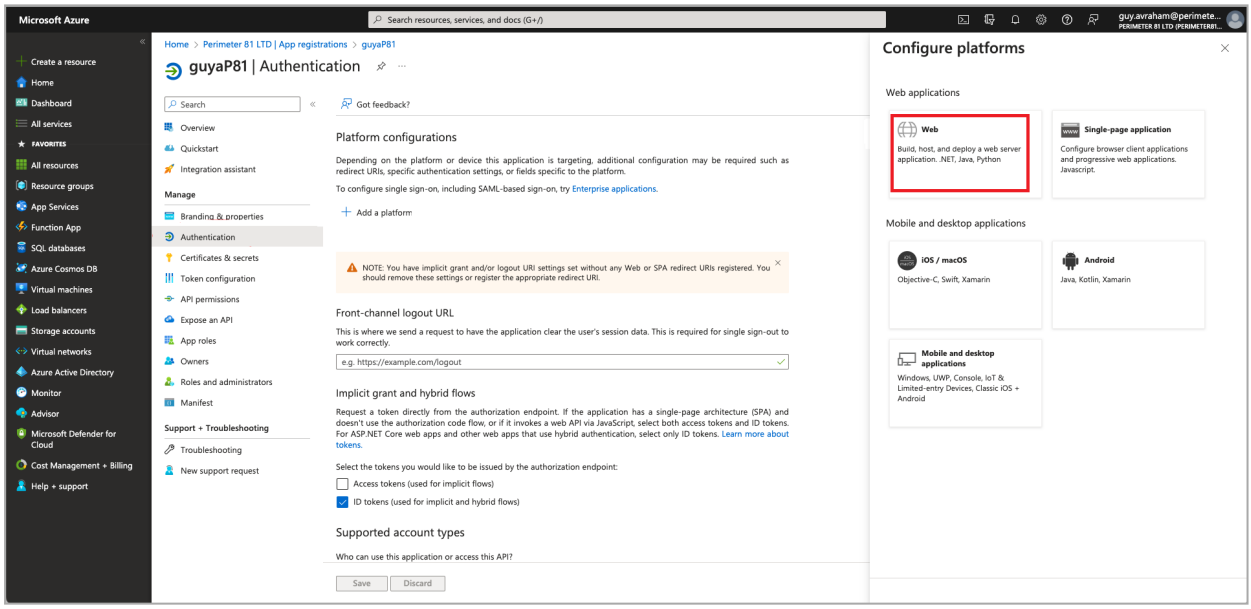
   The Microsoft Azure application is created.

8. Browse to **App registrations**, locate and select your application.
9. Click **Manage** > **Authentication** > **Add a platform**.



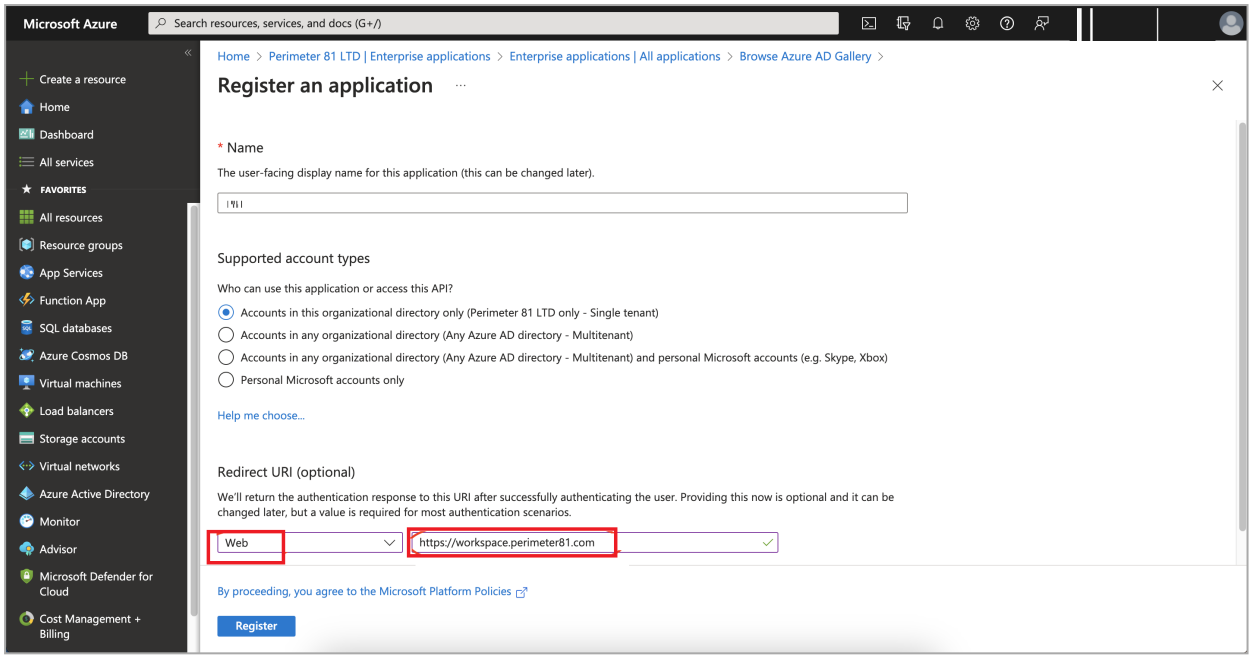
The **Configure platforms** window appears.

10. Select **Web**.

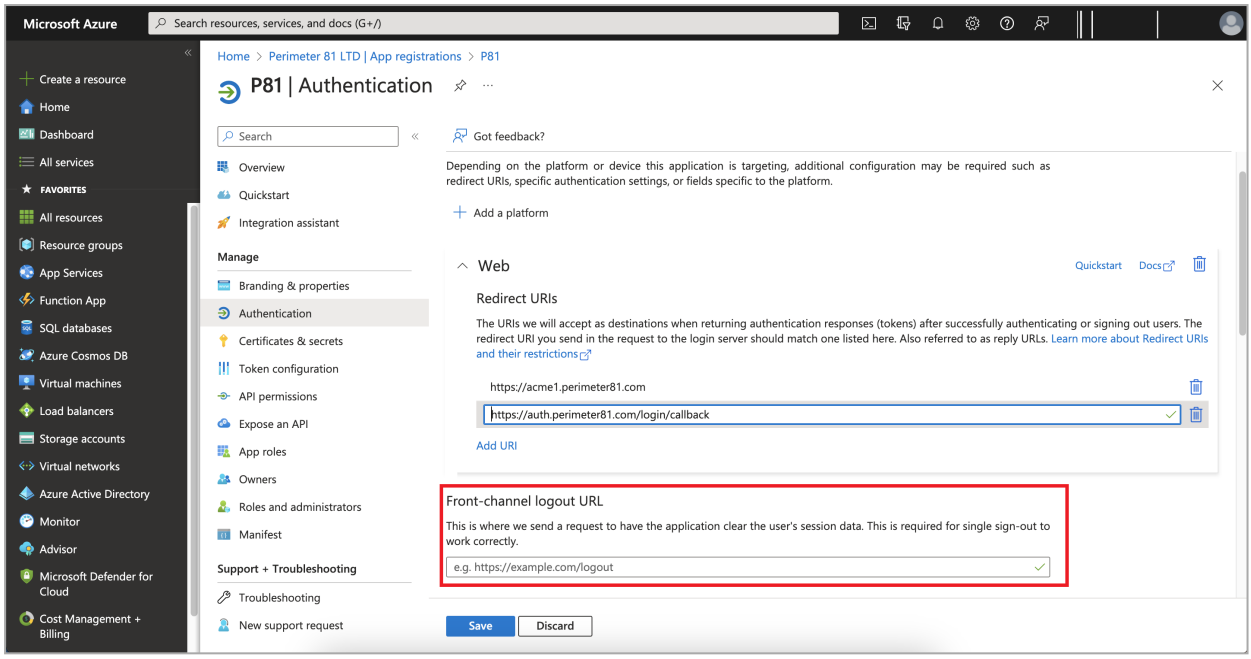


11. In the **Redirect URI (Optional)** field, select **Web** from the type of application list and enter the relevant URI where the access token is sent to:

    - For US data residency - `https://workspace.perimeter81.com`
    - For EU data residency - `https://workspace.eu.sase.checkpoint.com`
    - For AU data residency - `https://workspace.au.sase.checkpoint.com`
    - For IN data residency - `https://workspace.in.sase.checkpoint.com`

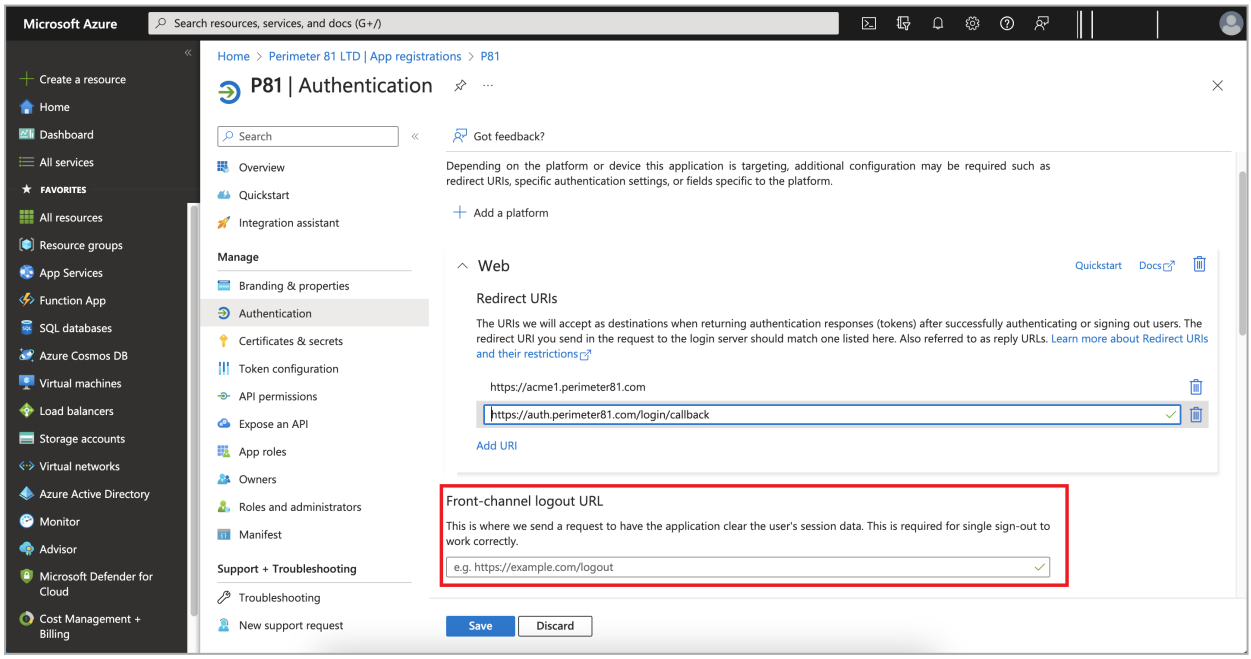


12. Click **Configure**.
13. In the **Redirect URIs** section, enter:
    - For US data residency - `https://auth.perimeter81.com/login/callback`
    - For EU data residency - `https://auth.eu.sase.checkpoint.com/login/callback`
    - For AU data residency - `https://auth.au.sase.checkpoint.com/login/callback`
    - For IN data residency - `https://auth.in.sase.checkpoint.com/login/callback`

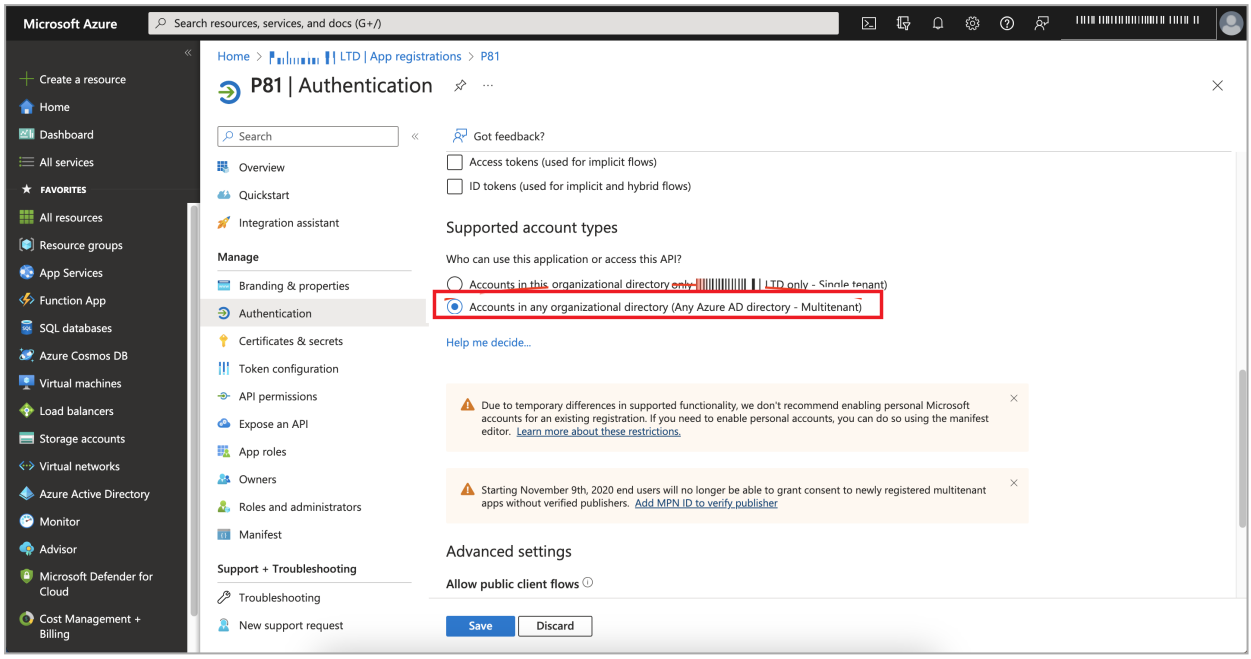


14. In the **Front-channel logout URL** section, enter your workspace name:

    - For US data residency - `https://{{WORKSPACE}}.perimeter81.com`
    - For EU data residency - `https://{{WORKSPACE}}.eu.sase.checkpoint.com`
    - For AU data residency - `https://{{WORKSPACE}}.au.sase.checkpoint.com`
    - For IN data residency - `https://{{WORKSPACE}}.in.sase.checkpoint.com`
      where `{{WORKSPACE}}` refers to your Check Point SASE workspace name.



15. To allow access from external organizations, in the **Supported account types** section, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.

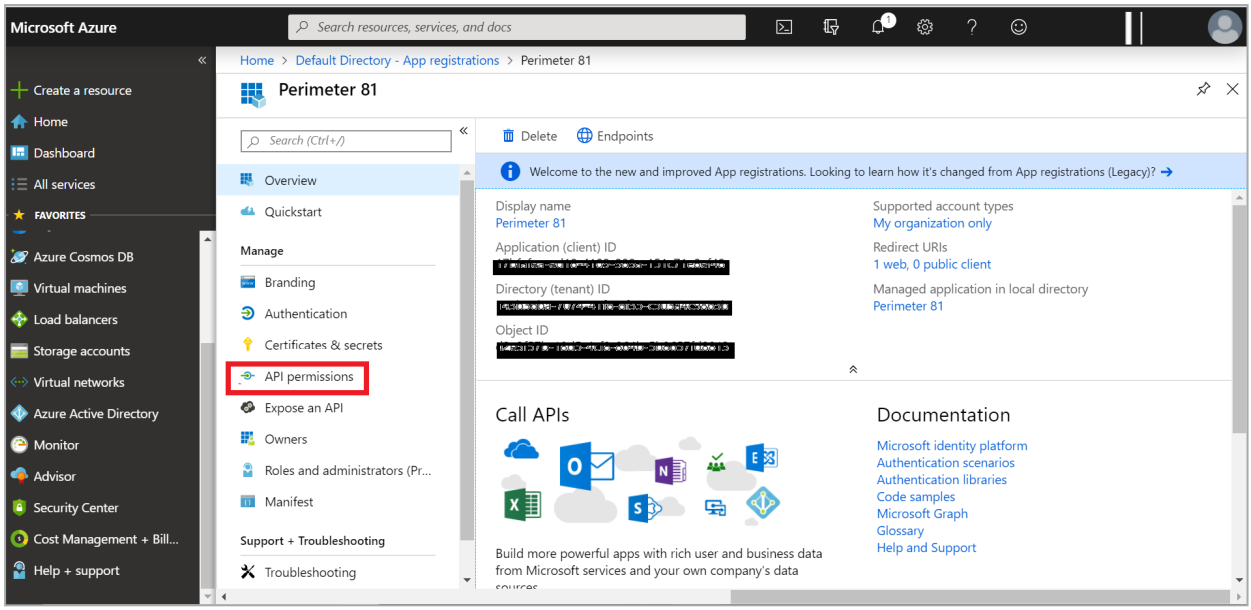


16. Click **Save**.

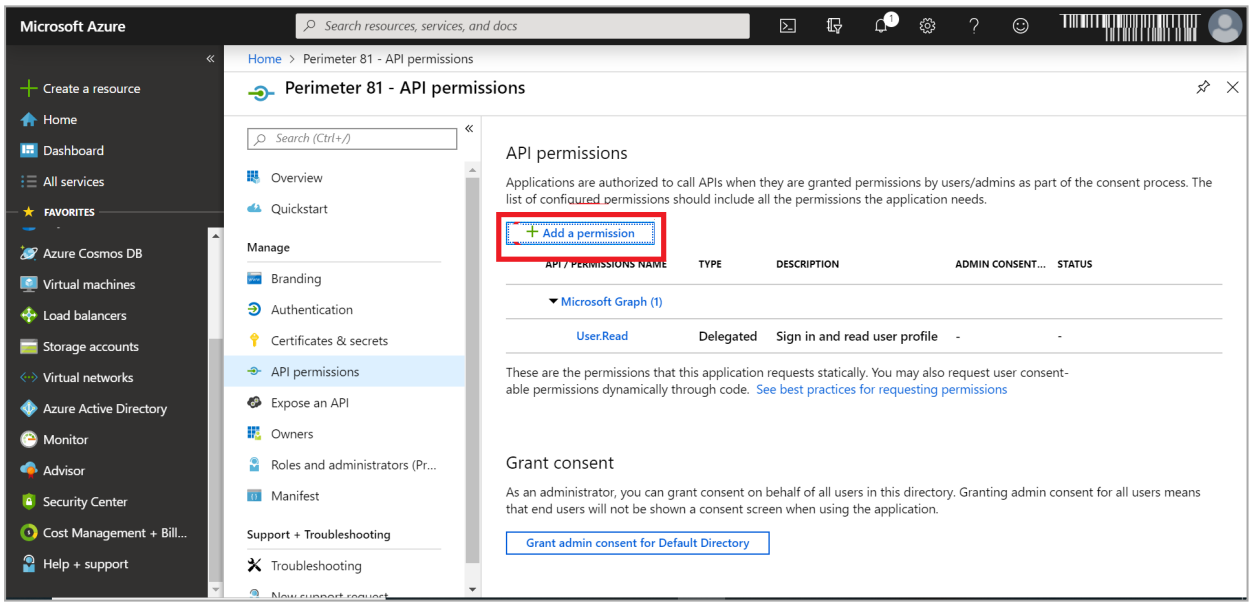
Configuring the Permissions for the Application

To configure the permissions for the application:

1. Log in to your Microsoft Azure Portal.
2. Click **Identity** > **Applications** > **App registrations** > **All applications**.
3. Select your application.
4. Click **Overview** > **Manage** > **API Permissions**.

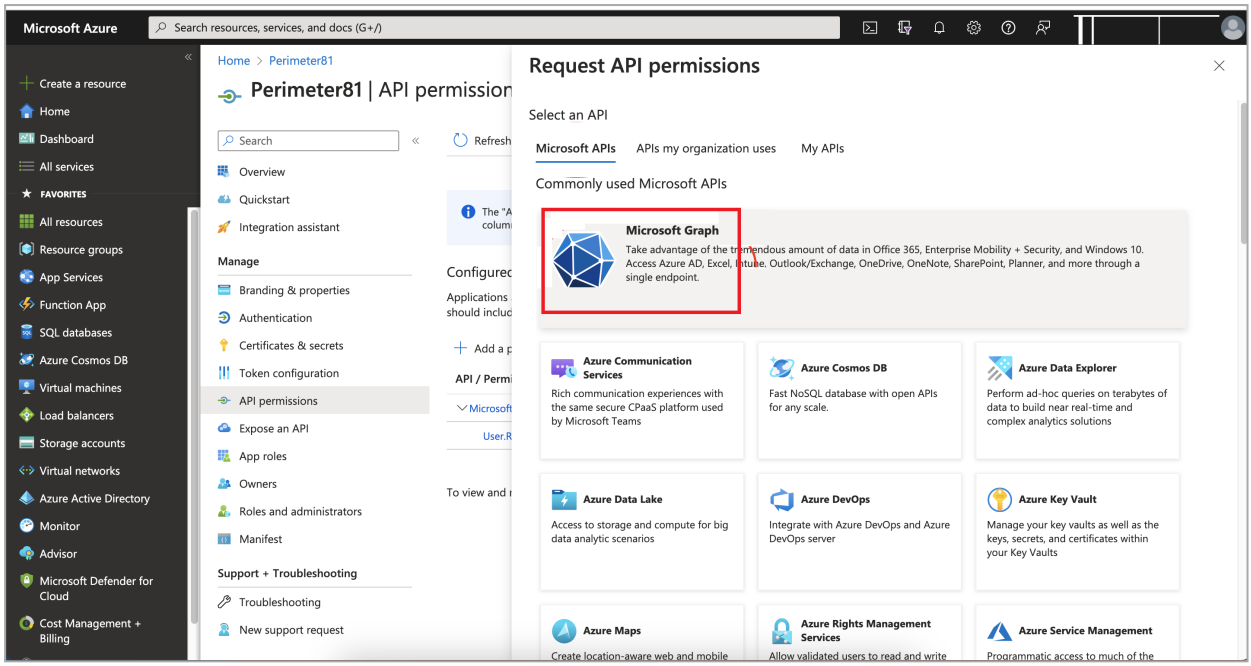


5. Click **Add a permission**.

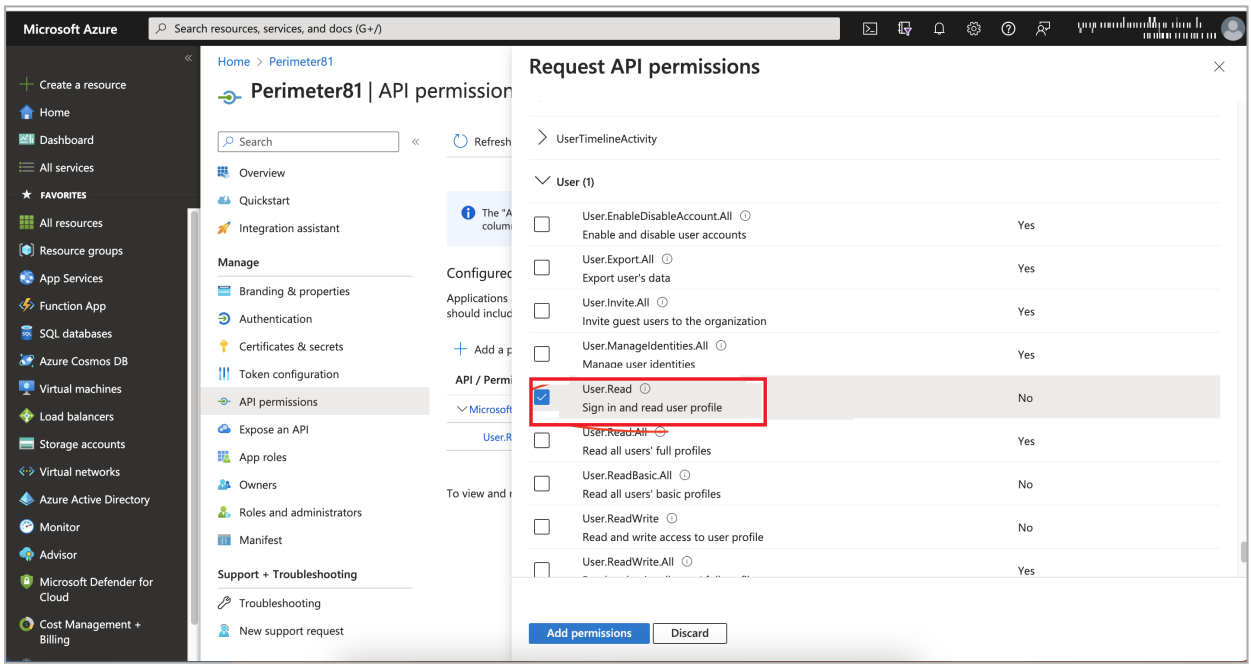


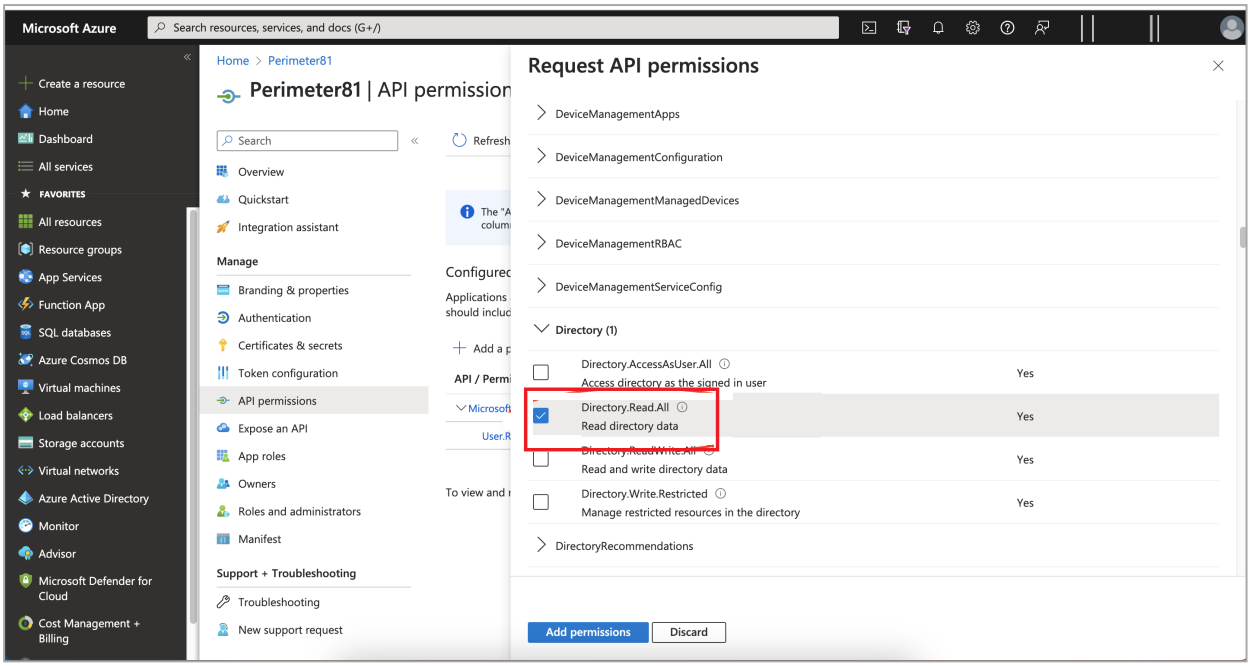
The **Request API permissions** page appears.

6. Click **Microsoft APIs** and select **Microsoft Graph** from the list of available APIs to change the access level.



7. Click **Delegated permissions**.
8. Select the **User.Read** and **Directory.Read.All** checkbox to modify the permissions so your application can read the directory..



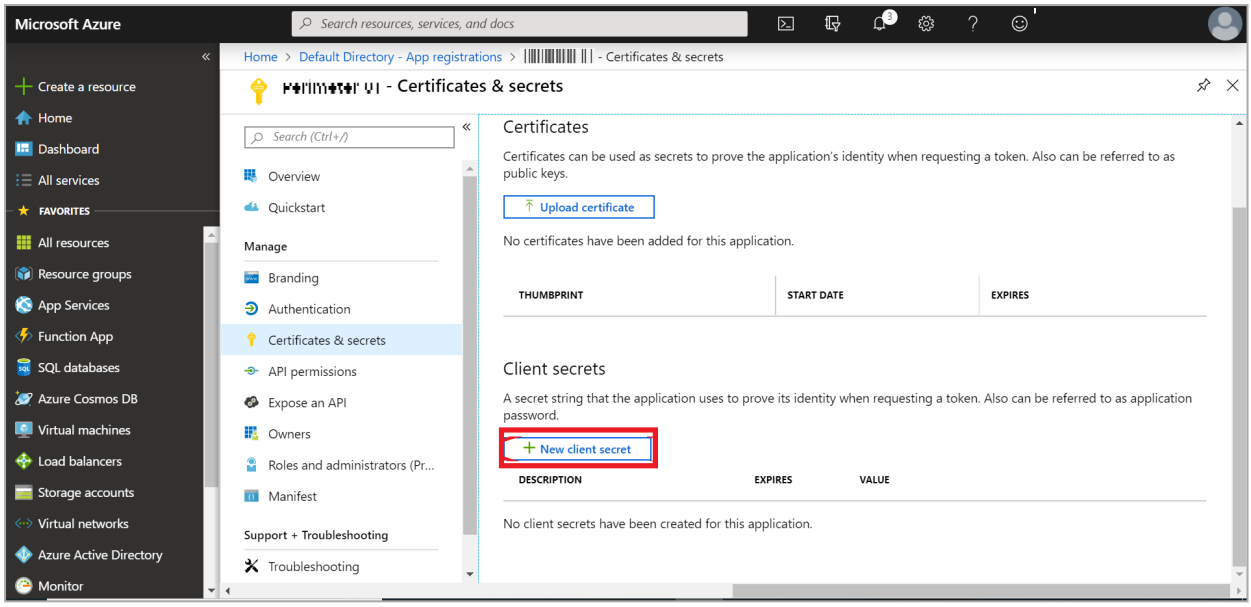


9. Click **Add permissions** > **Configured permissions** > **Grant admin consent** for approval of your app API permissions.
10. Click **Yes**.

    Your application gets the granted permissions.
11. To enable user group support, enable:
    a. **Application Permissions**: Read directory data.
    b. **Delegated permissions**: Access the directory as the signed in user.
12. Click **Save** to save the changes.
13. To remove the Windows Azure Active Directory API permission, see *"Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions" on page 1129*.

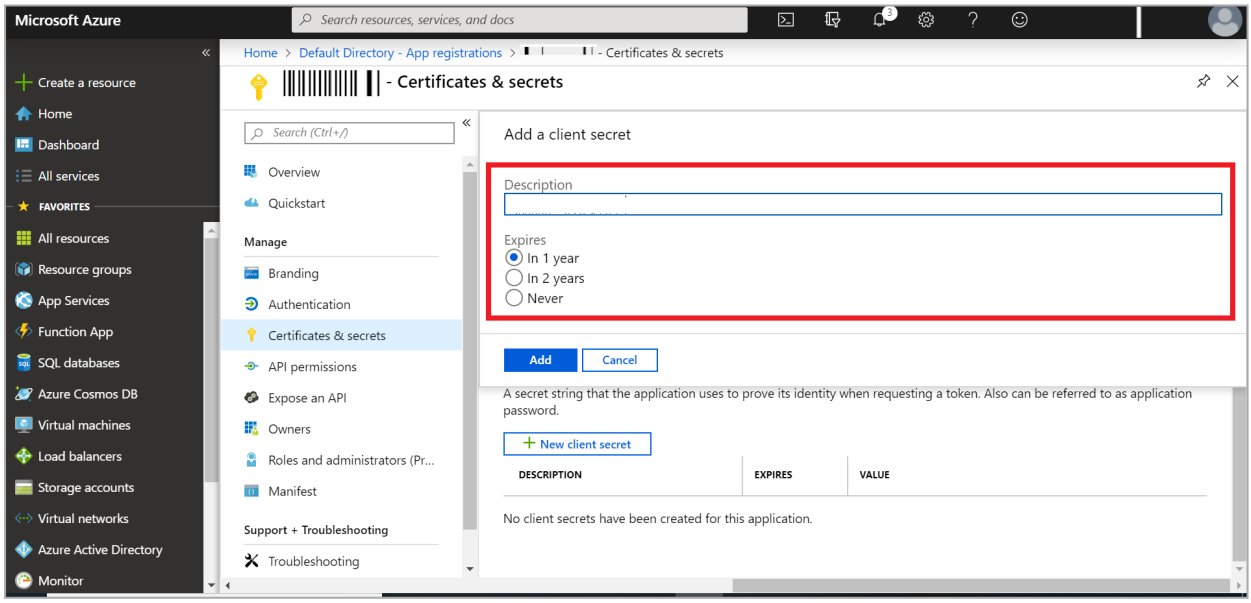
Configuring the Key

1. Log in to your Microsoft Azure Portal.
2. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
3. Browse to **App registrations**, locate and select your application.
4. Go to **Manage** > **Certificates & secrets**.
5. Click **New client secret**.



The **Add a Client secret** window appears.

6. In the **Description** filed, enter a name for the key.
7. In the **Expires** field, select the expiry:
   - **In 1 year**
   - **In 2 years**
   - **Never**



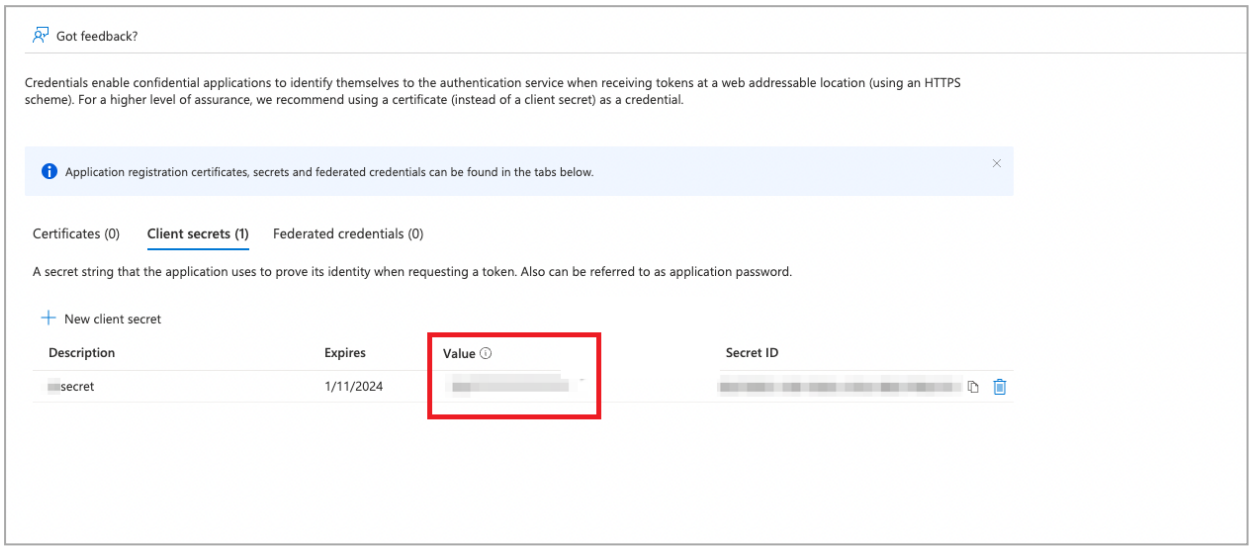
8. Click **Add**.

   The new key is added.

9. To get the secret value of the key, go to the **Client secrets** tab and copy the secret **Value**.

   This value is the **Client Secret** in SASE Admin console. .

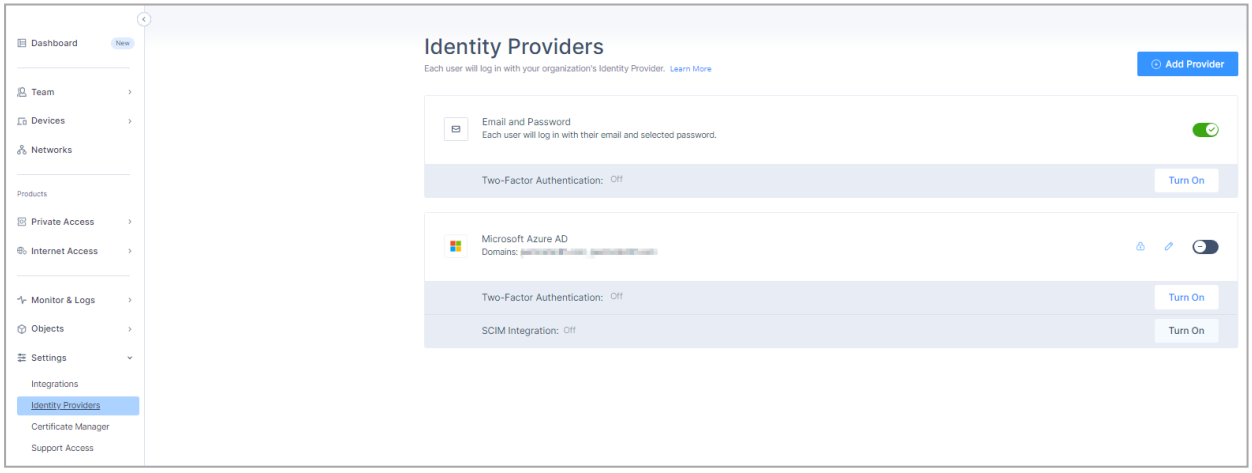
   Note - The Secret value of the key need to be copied before you close the screen. If not, you need to create a new key.



Configuring IDP Connection in SASE

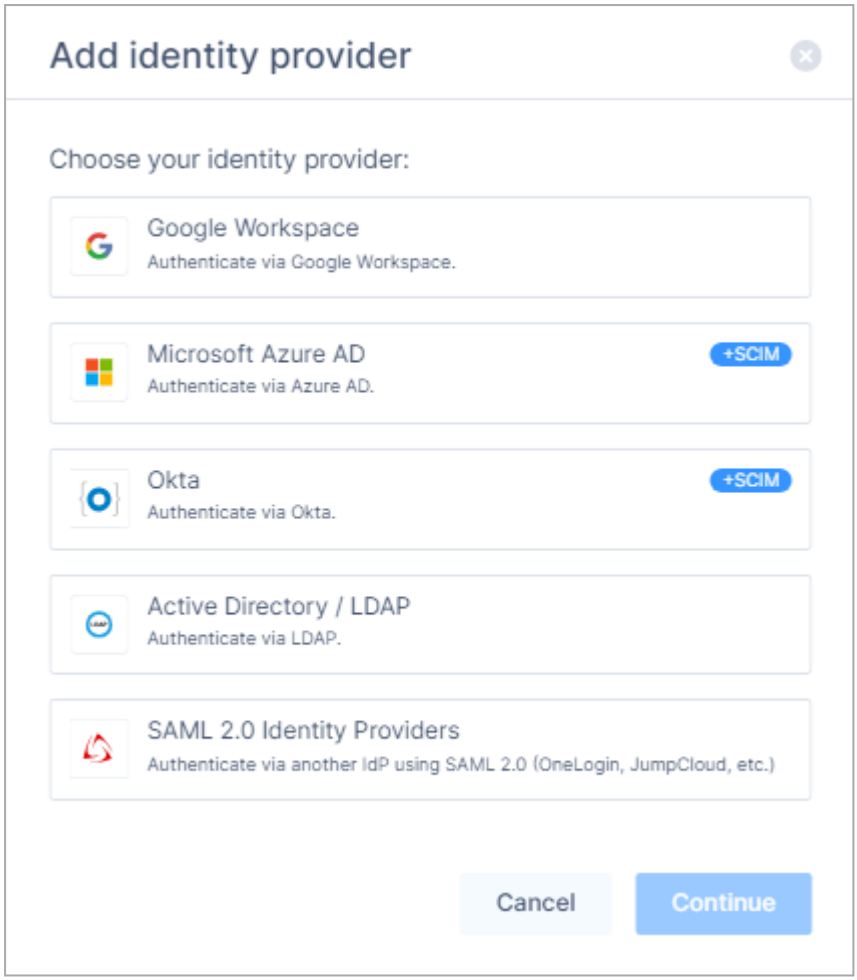
1. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.

   The **Identity Providers** page appears.



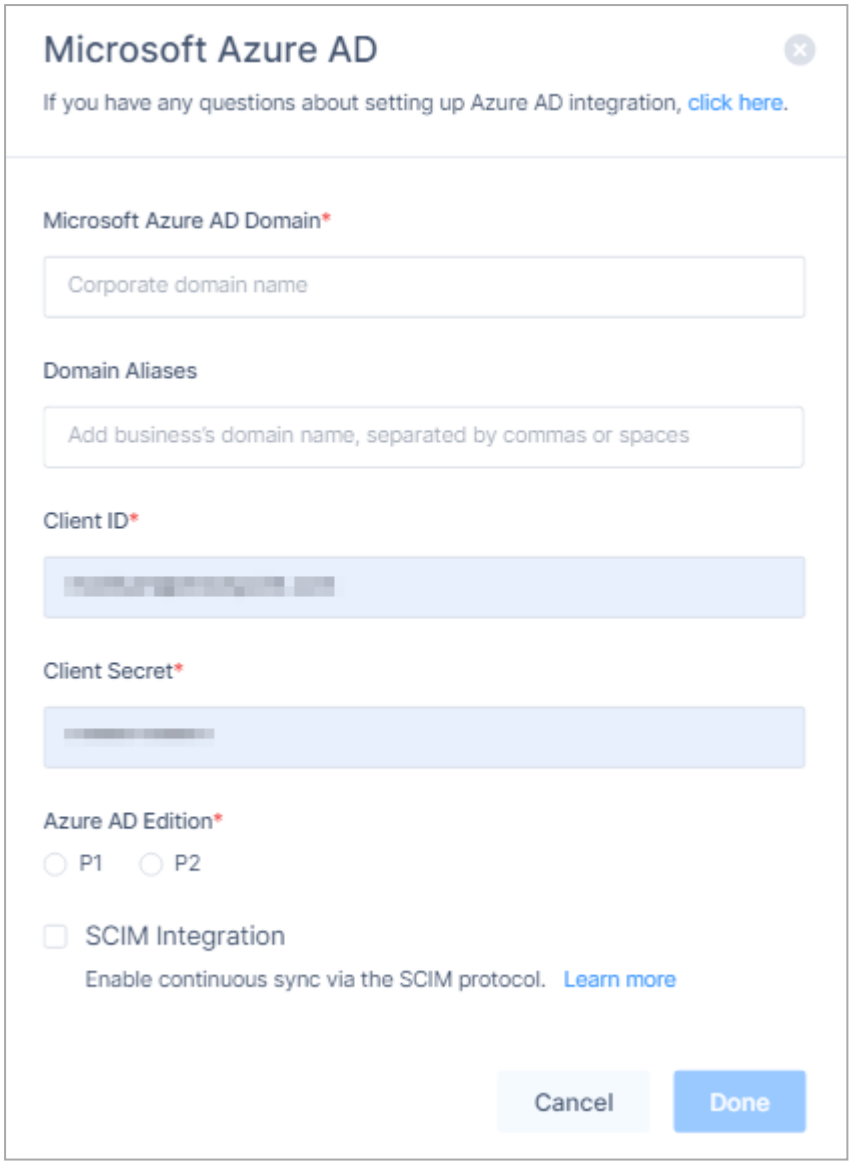
2. Click **Add Provider**.

   The **Add identity provider** window appears.



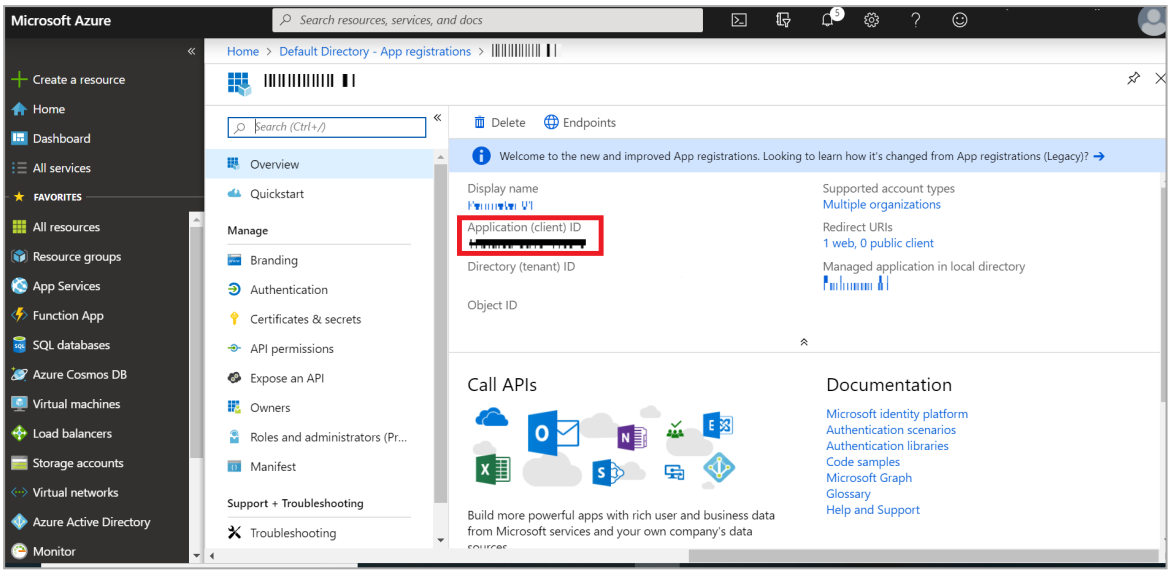
3. Select **Microsoft Azure AD**.
4. Click **Continue**.

   The **Microsoft Azure AD** page appears.



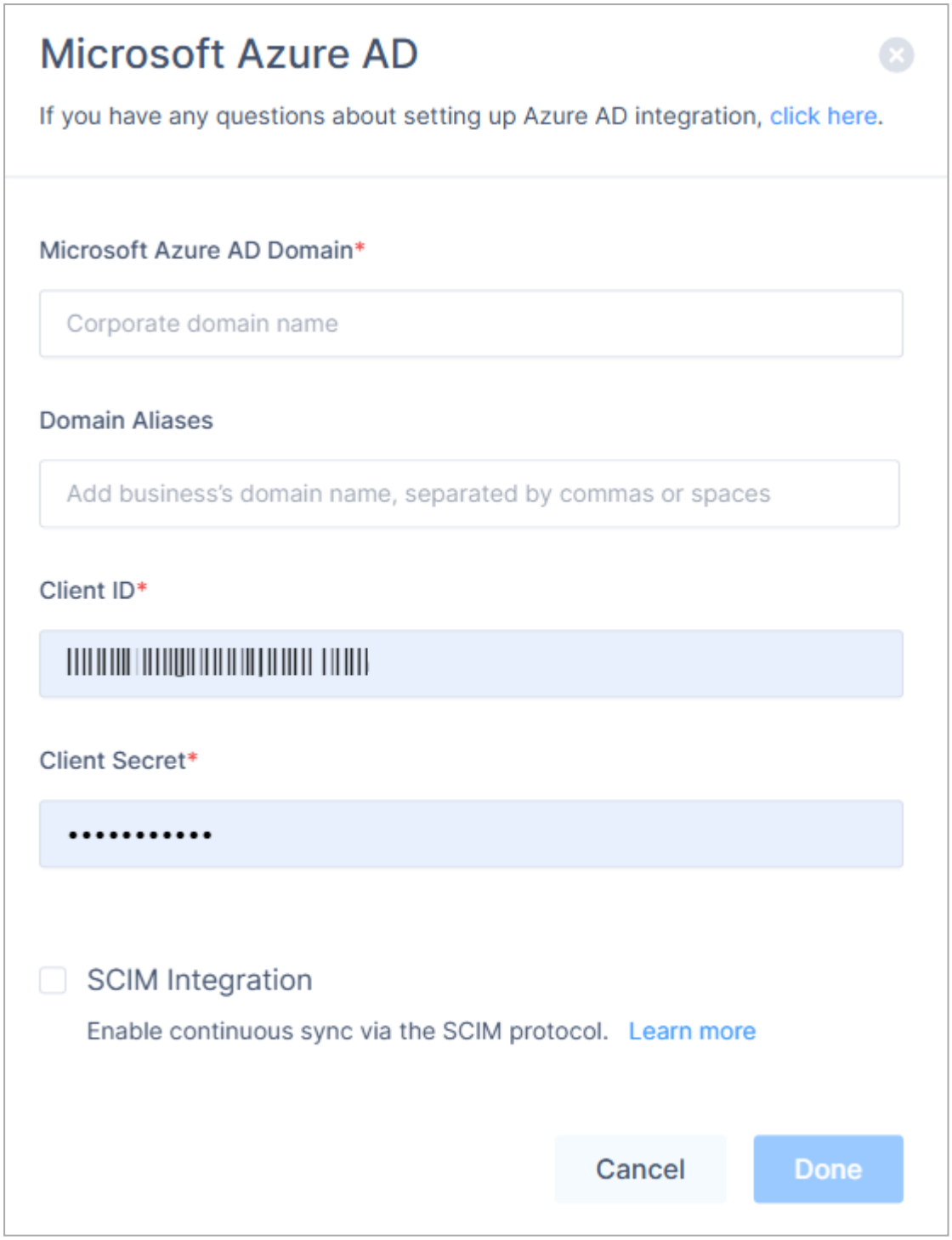
5. In the **Microsoft Azure AD Domain** field, enter the domain name.
6. In the **Domain Aliases** field, enter the email ID(s) separated by commas or spaces.
7. In the **Client ID** field, enter the **Application (client) ID** in Microsoft Azure AD:
   a. Log in to your Microsoft Azure Portal.
   b. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
   c. Browse to **App registrations**, locate and select your application.

d. Go to **Overview** > **Application (client) ID**.



e. Copy the **Application (cient) ID** value.

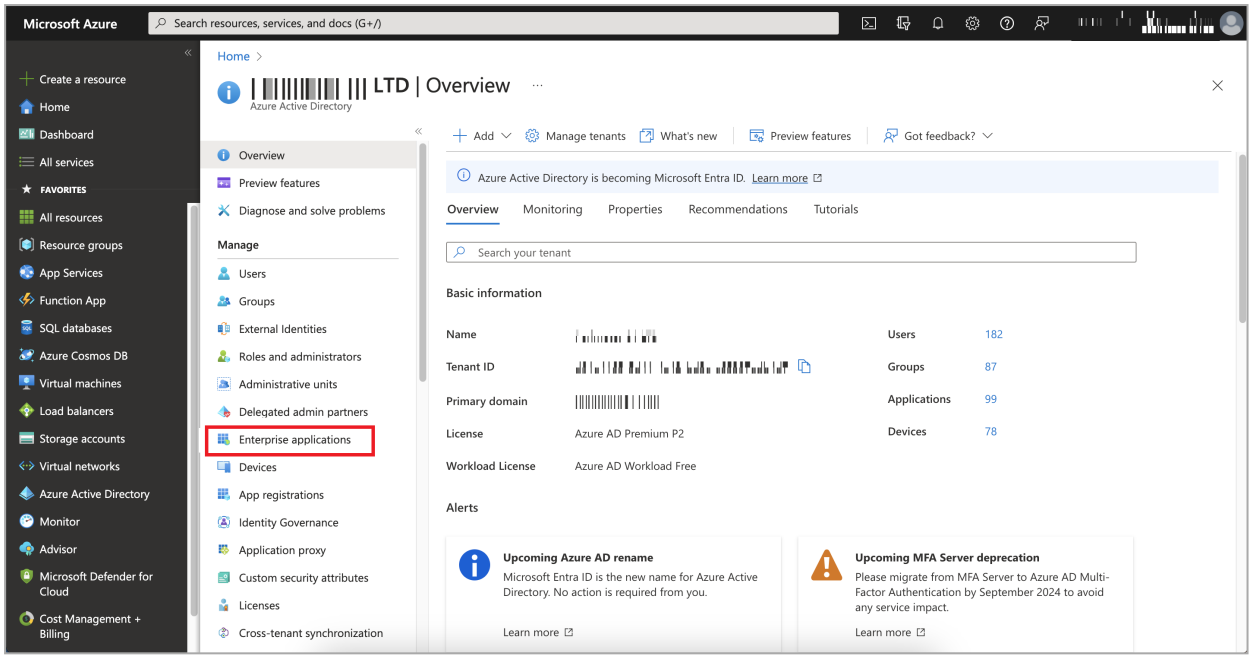
8. In the **Client Secret** field, enter the secret value. See step 9 in Configuring the Key.



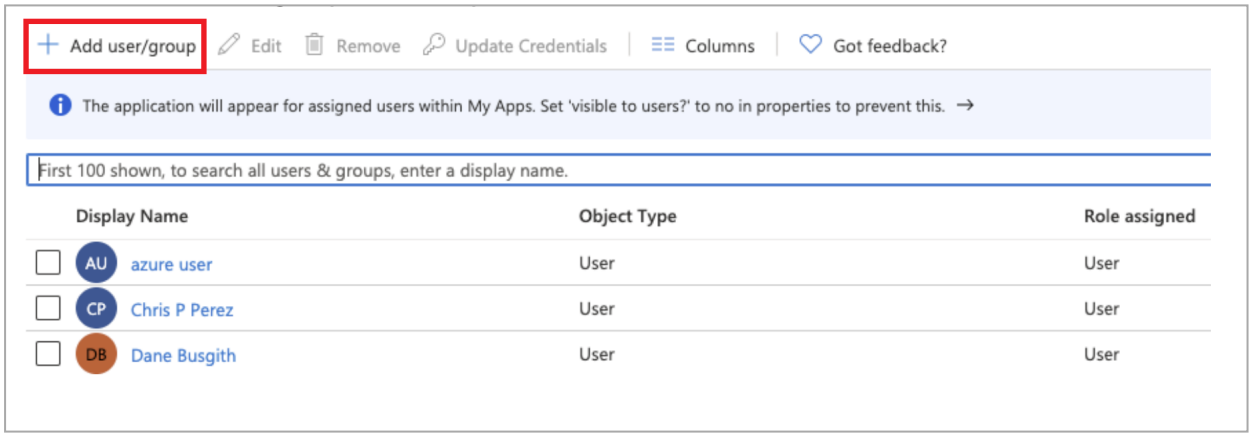
9. Select the **SCIM Integration** checkbox.
10. Click **Done**.

Assigning Users and Groups in Microsoft Azure

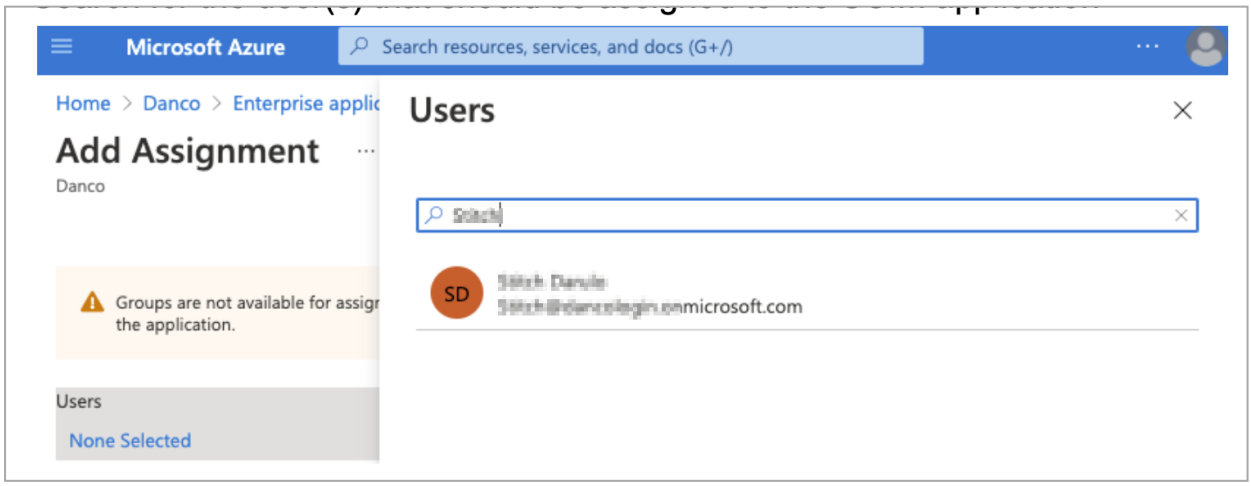
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.
3. Go to **Manage** > **Enterprise applications**.



4. Search and select your application.
5. Go to **Users and groups** and click **Add user/group**.



6. Click **None Selected** in **Users**.



7. Search and select the user(s) or group(s) you want to add to the application.

   Note - Special characters are not supported in groups.

8. Click **Select**.
9. Click **Assign**.

System for Cross-domain Identity Management (SCIM)

SCIM is an open standard that manage user identity information, enhances the automation of user provisioning and management.

When using SCIM, changes you make to users on the identity provider side are automatically synced to SASE Agent.

Examples:

- Deleting a user within your IDP, removes the user from the SASE console, freeing up the user's license.
- When a group is deleted in the identity provider, it remains in any policies or configurations where it was previously used. For more information, see *"Groups" on page 89*.
- When creating a new user within your IDP, and provisioning them through the SCIM integration, the user is automatically created in the SASE console.

SASE offers SCIM integration with these Identity Providers:

- *"Okta (SCIM)" below*
- *Azure Active Directory (SCIM)*

Okta (SCIM)

SASE integrates with Okta using SCIM, ensuring automatic user synchronization, profile updates, and streamlined deactivation when users are removed from the Okta SCIM Application.

Prerequisites

To integrate Okta and SASE, you must have:

- Administrator access to both Okta and SASE Administrator Portal.
- Active SASE Okta application configured for Single Sign-On.

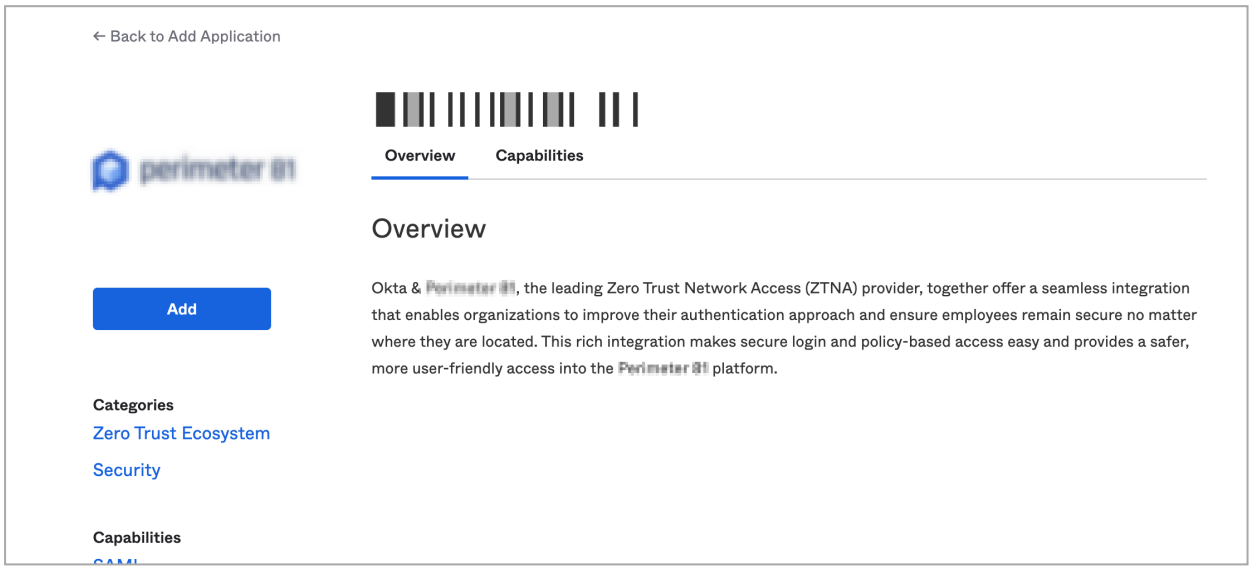
Note - SCIM based user provisioning is available to SASE Enterprise customers only.

Important -

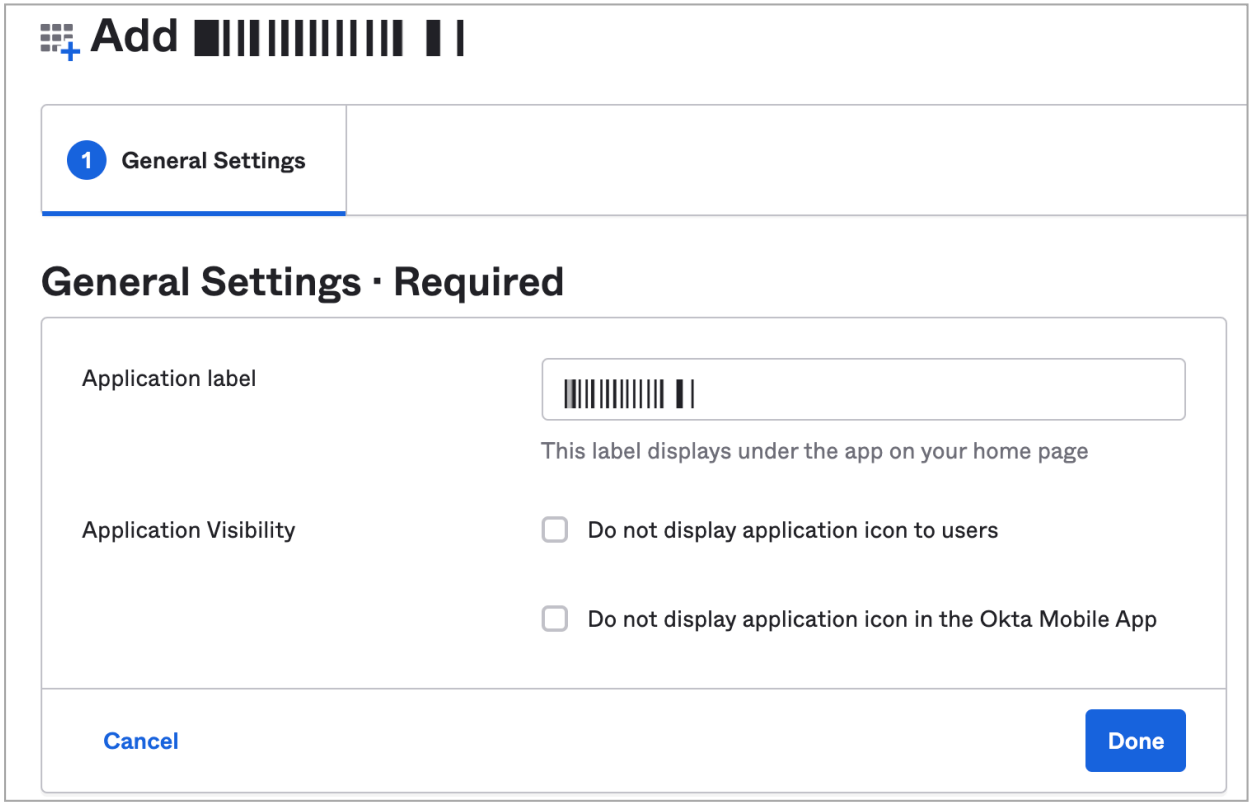
- If your account previously used a different Identity Provider (IdP), removing that IdP does not remove user-level IdP associations. Users provisioned through the previous IdP retain their former IdP linkage. If you enable Okta SCIM provisioning without first removing these users, they have dual IdP associations. This causes SCIM deactivation and sync failures.
- Before configuring Okta SCIM, remove all users provisioned through the previous IdP from the SASE console, then reprovision them through Okta. No bulk removal operation is available - remove users individually.

Enabling SCIM on Okta Management Portal

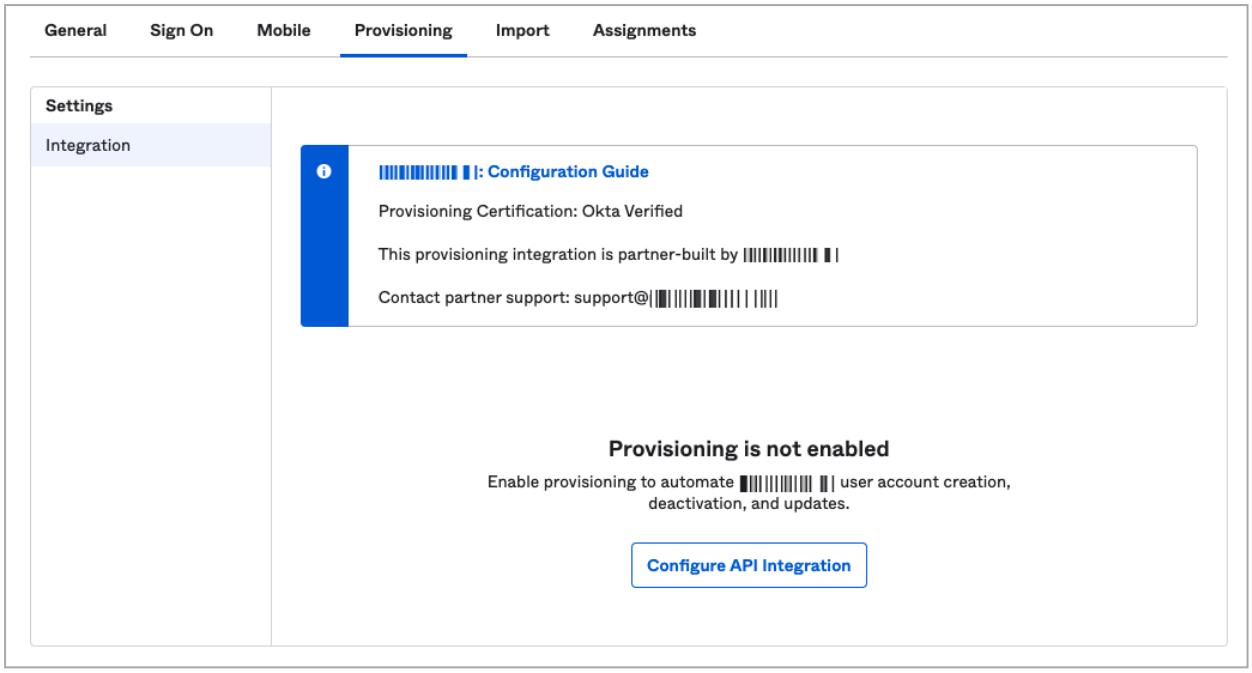
1. Log in to your Okta Management Portal.
2. Go to **Applications** > **Browse app Catalog**.
3. Search and select your application and click **Add**.



4. Click **Done**.

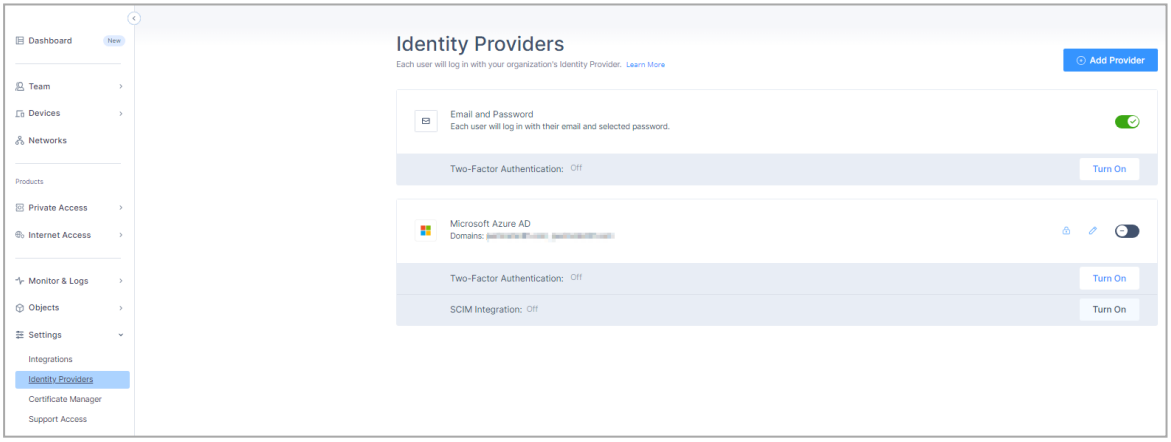


5. Go to the **Provisioning** tab and click **Configure API Integration**.

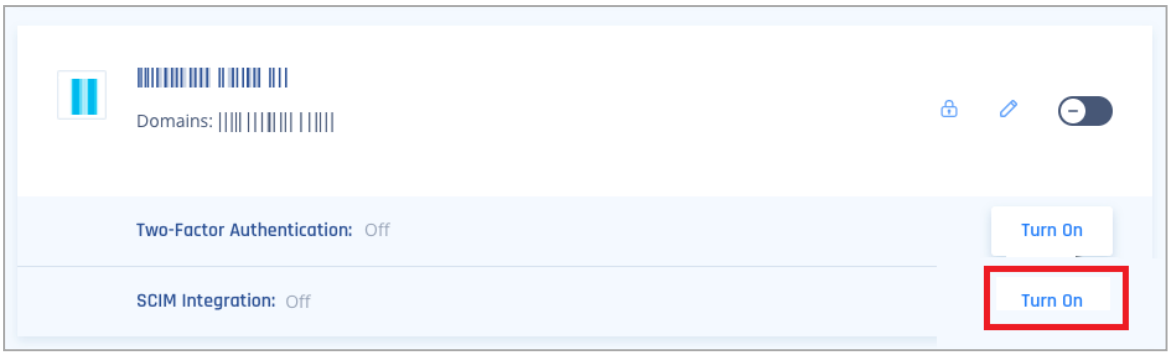


6. Select the **Enable API Integration** checkbox.
7. In the **API Token** field, enter the generated token. To get the generated token:
   a. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.

      The **Identity Providers** page appears.

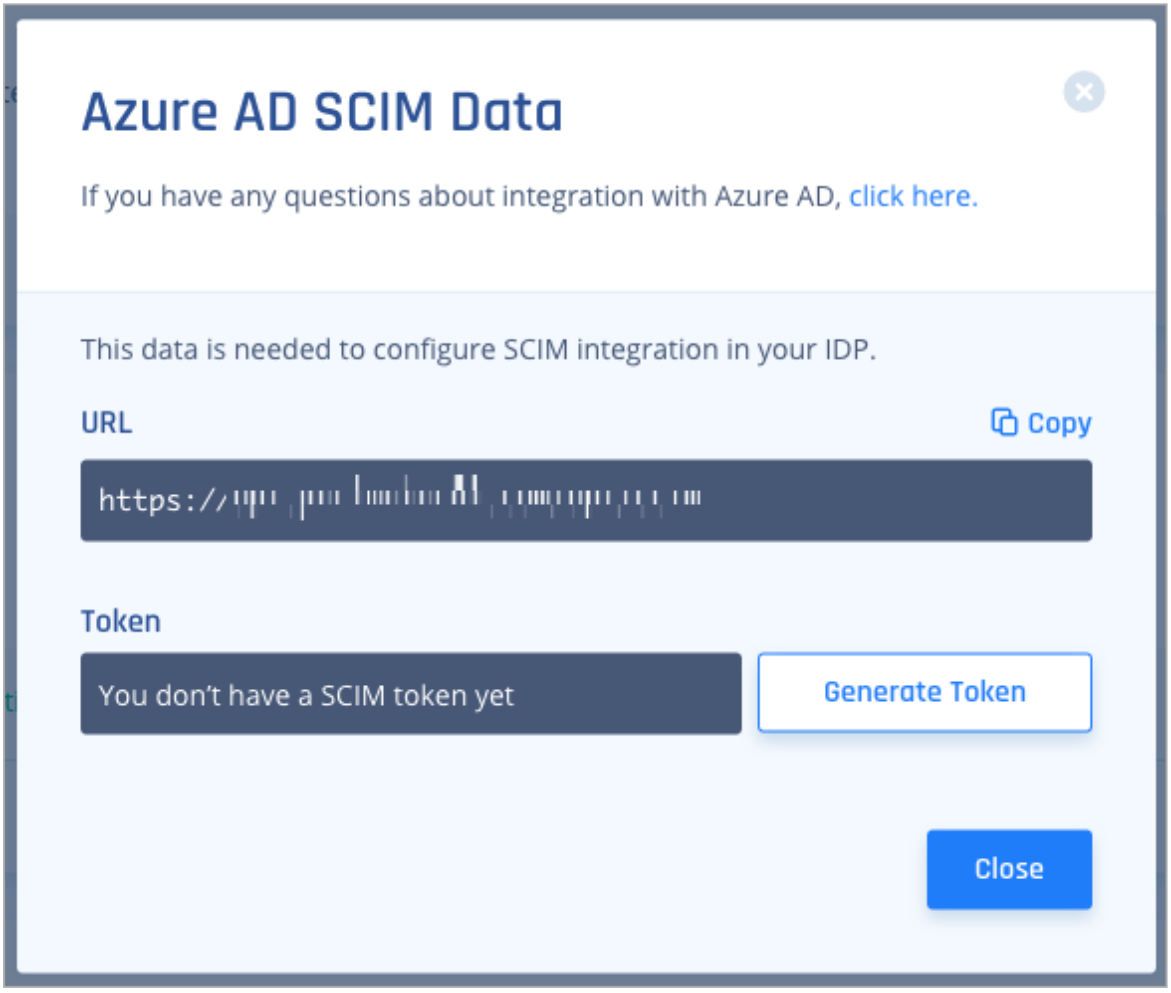


b. Click **Turn On** in the **SCIM Integration** section.



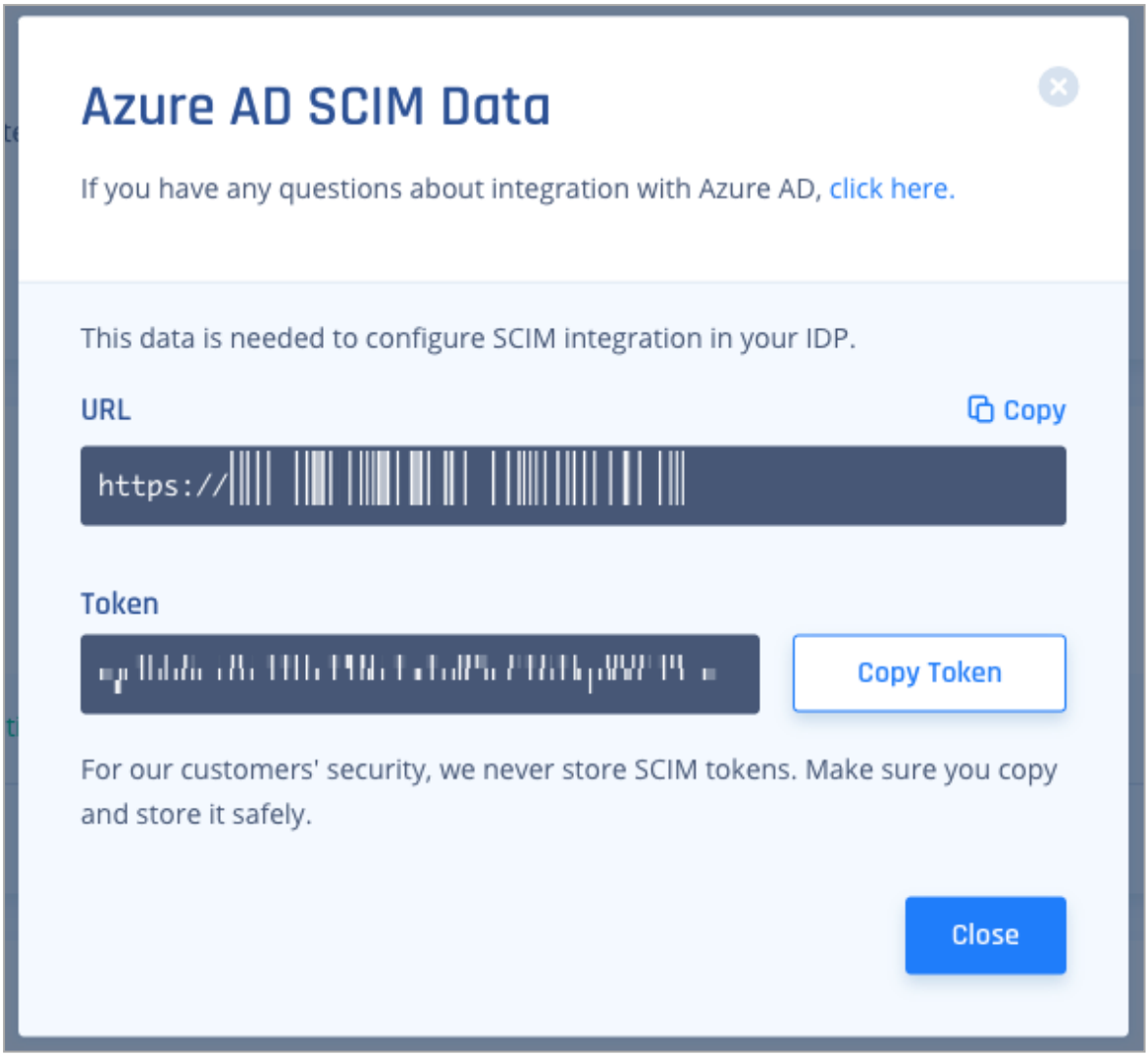
c. Click **Settings** in the **SCIM Integration** section.

d. Click **Generate Token**.



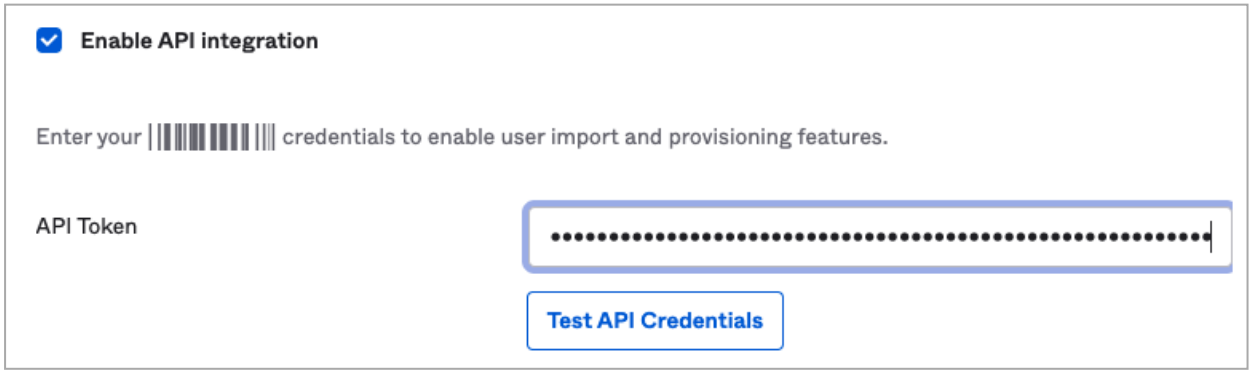
e. The secret token is generated.

f. Click **Copy Token**.



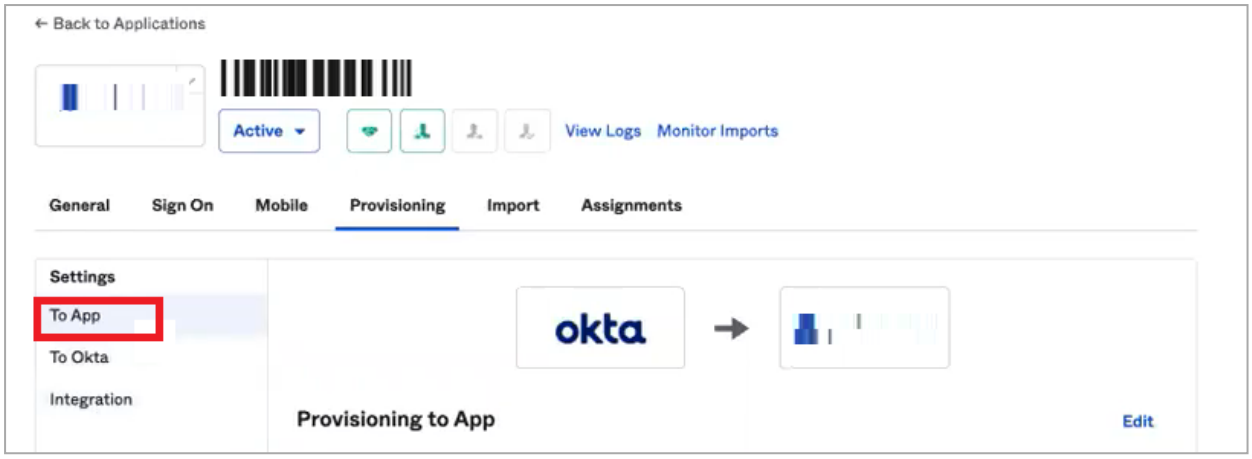
g. Click **Close**.

8. Click **Test API Credentials**.

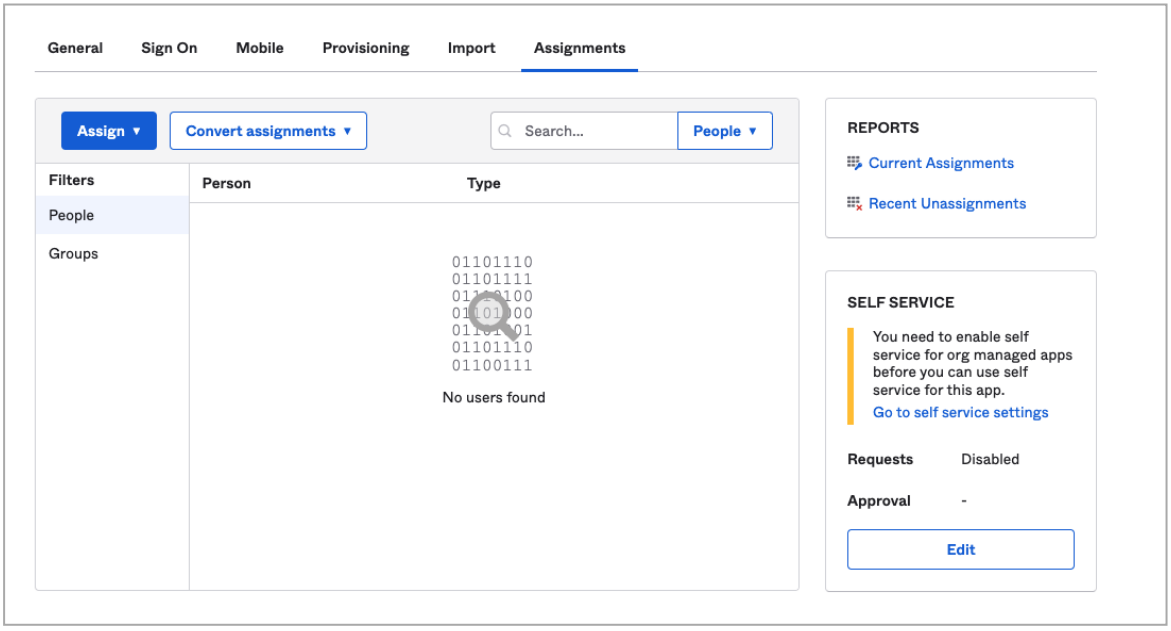


9. Click **Save**.

10. Go to **Settings** > **To App**.

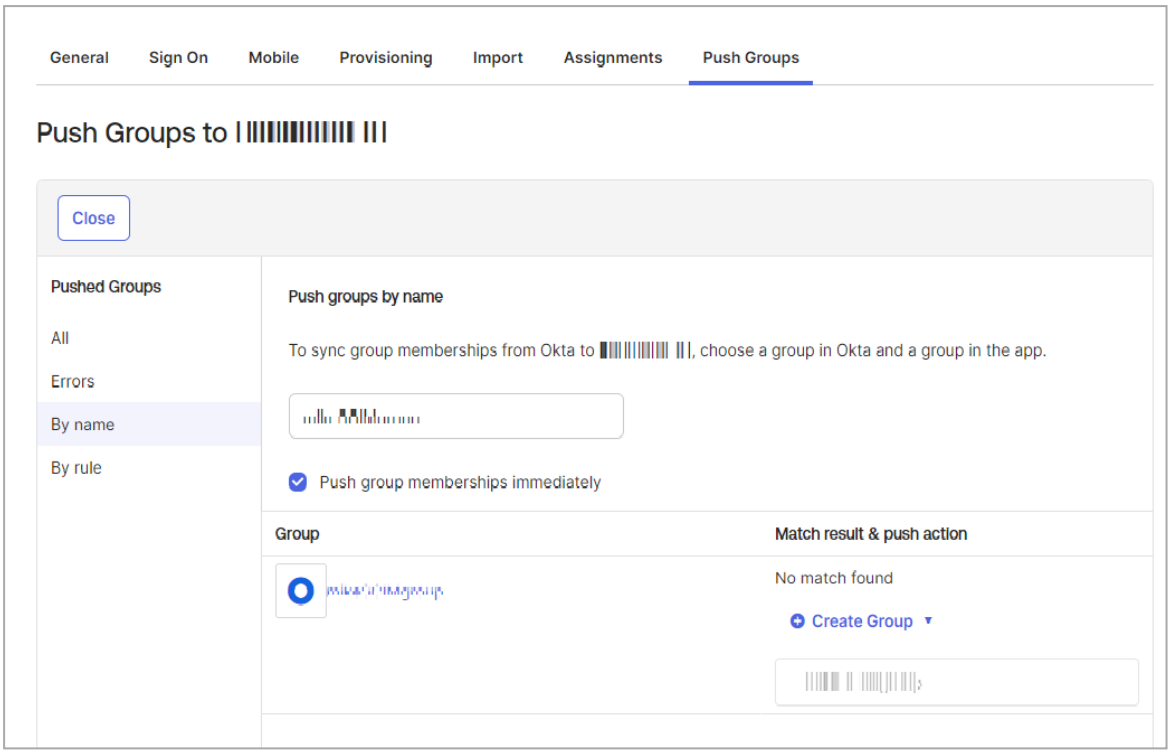


11. Click **Edit**.
12. Select the checkbox for:
    - **Create Users**
    - **Update User Attributes**
    - **Deactivate Users**
13. Click **Save**.
14. To provision users and groups:
    a. Go to **Applications** and select your SAML 2.0 application.
    b. Go to **Assignments** tab.



    c. Click **Assign**.
    d. Search and select the user name, email id, or group(s) name.

e. To push groups, click the **Push groups** tab and select **By name**.



f. In the **Push groups by name** field, enter the group name.

g. Select the **Push group memberships immediately** checkbox.

h. Click **Save and Go Back**.

i. Click **Done**.

These SAML attributes are supported:

Application Attribute	Identity Bridge Attribute or Literal Value
email	user.email
given_name	user.firstName
family_name	user.lastName
groups	Configured in the app UI. See Group Support section.

Microsoft Entra ID (formerly Azure Active Directory) (SCIM)

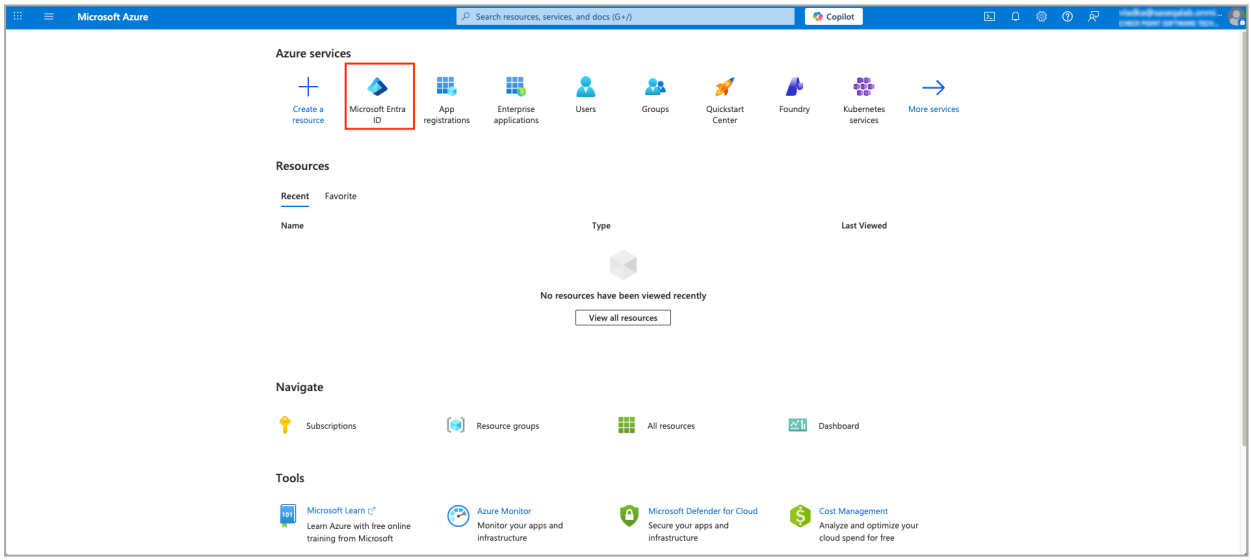
High-Level Procedure

- Part 1: Configure Entra ID
  - Step 1 - Creating an application in Entra ID
  - Step 2 - Configuring API Permissions
  - Step 3 - Configuring Secret Key for the Application
- Part 2: Configuring SASE IdP
- Part 3: Configuring SCIM

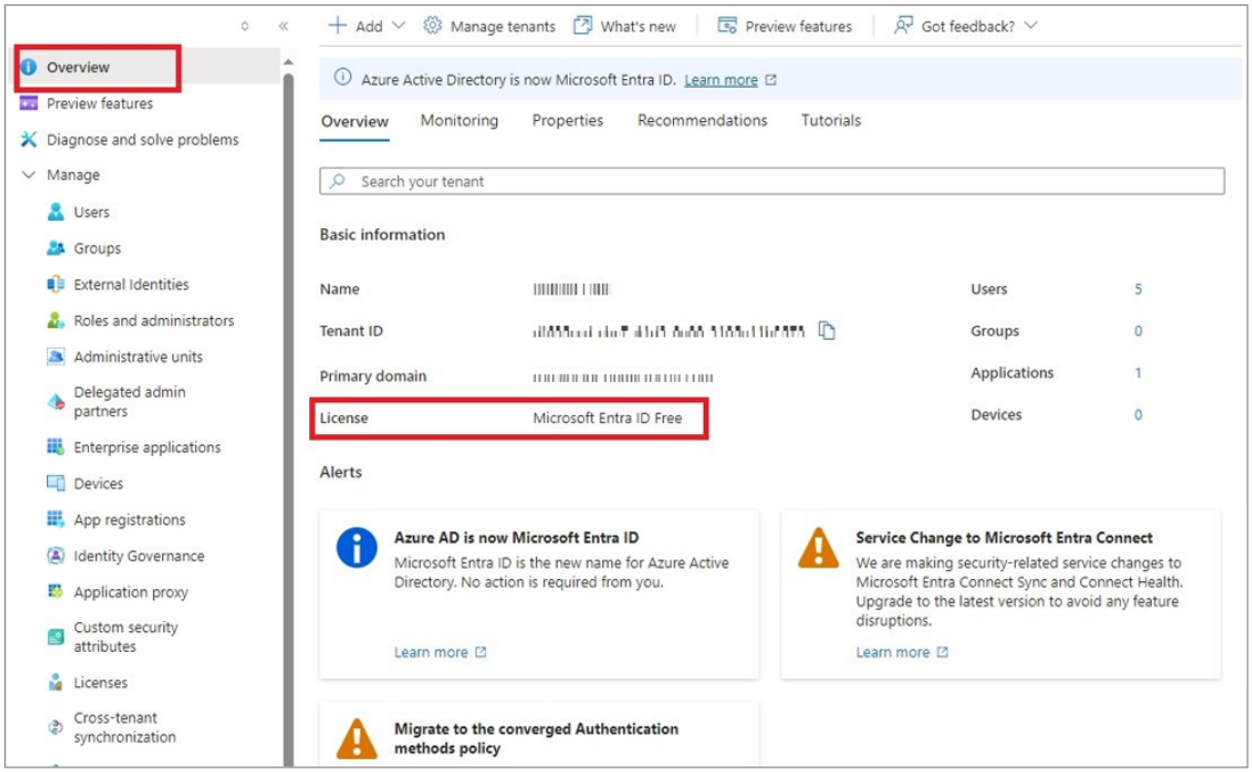
Part 1: Configure Entra ID

Step 1 - Creating an application in Entra ID

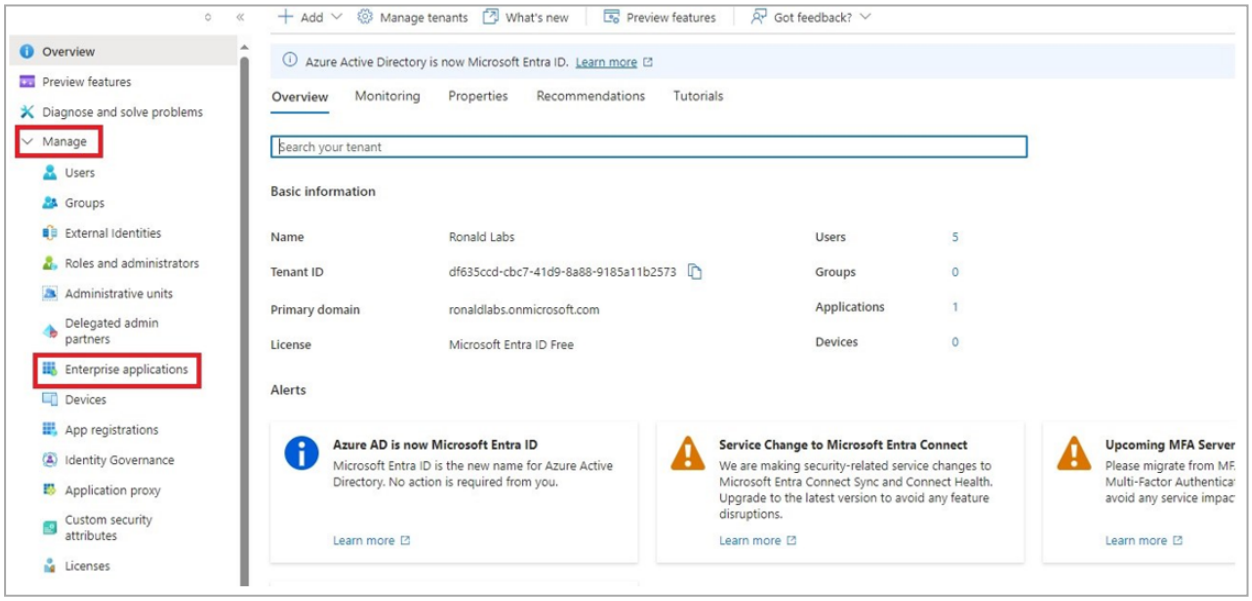
1. Access the Microsoft Azure Portal using administrator credentials.
2. From Azure services, click **Microsoft Entra ID**.



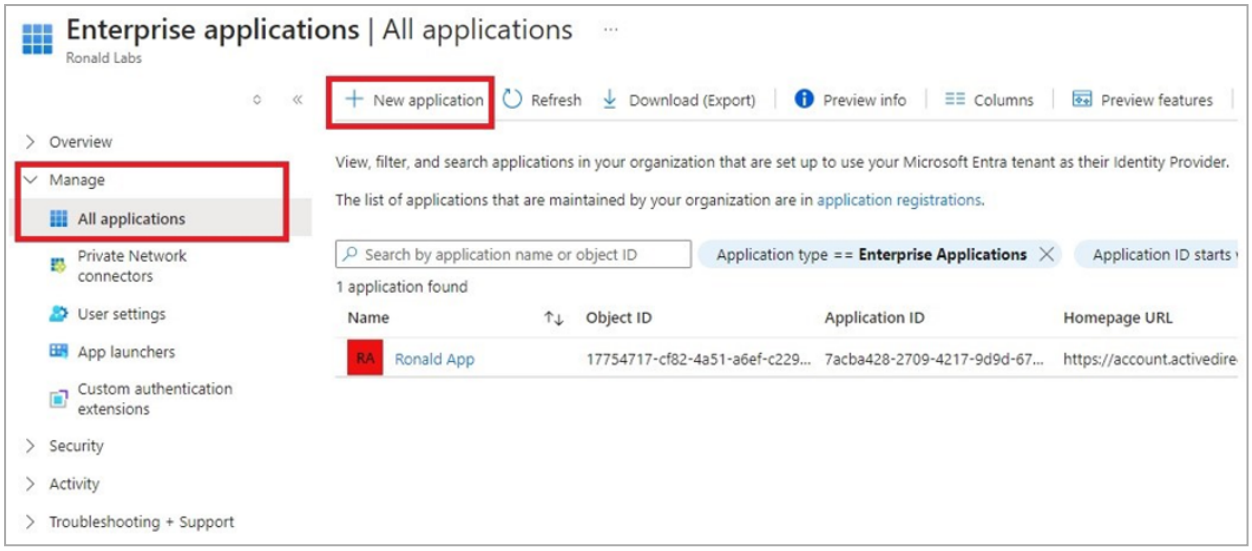
3. Click **Overview**.



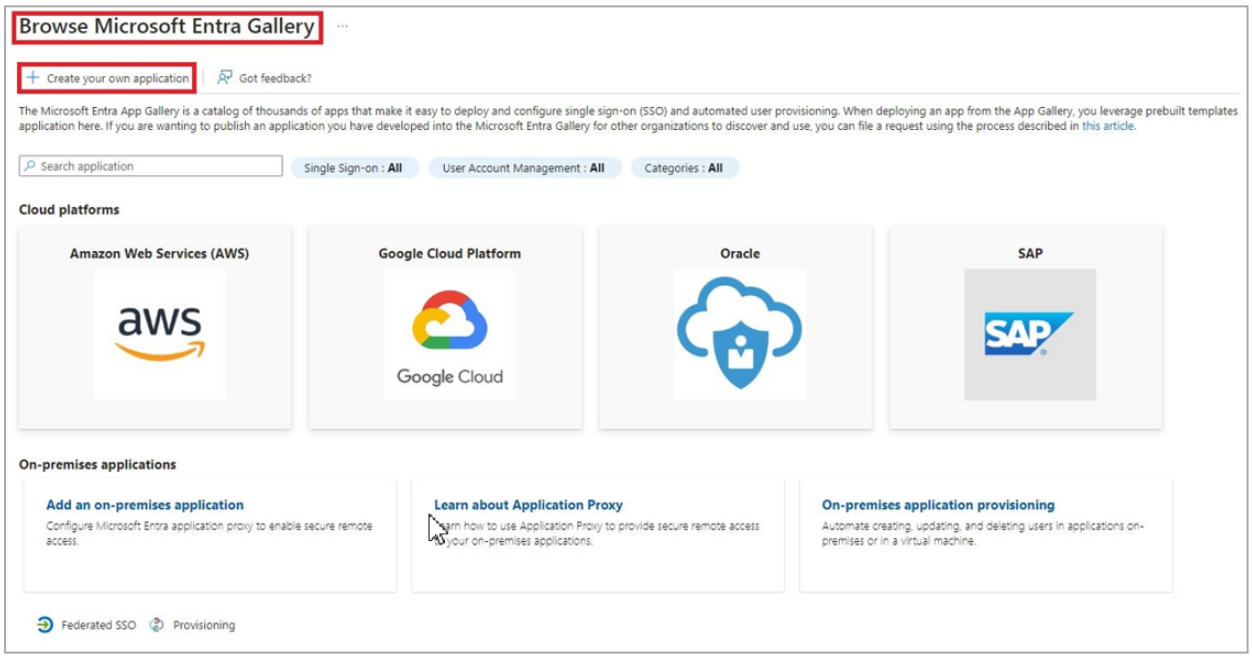
4. From the **Basic information** section, make a note of the **License**.
5. Go to **Manage** > **Enterprise applications**.



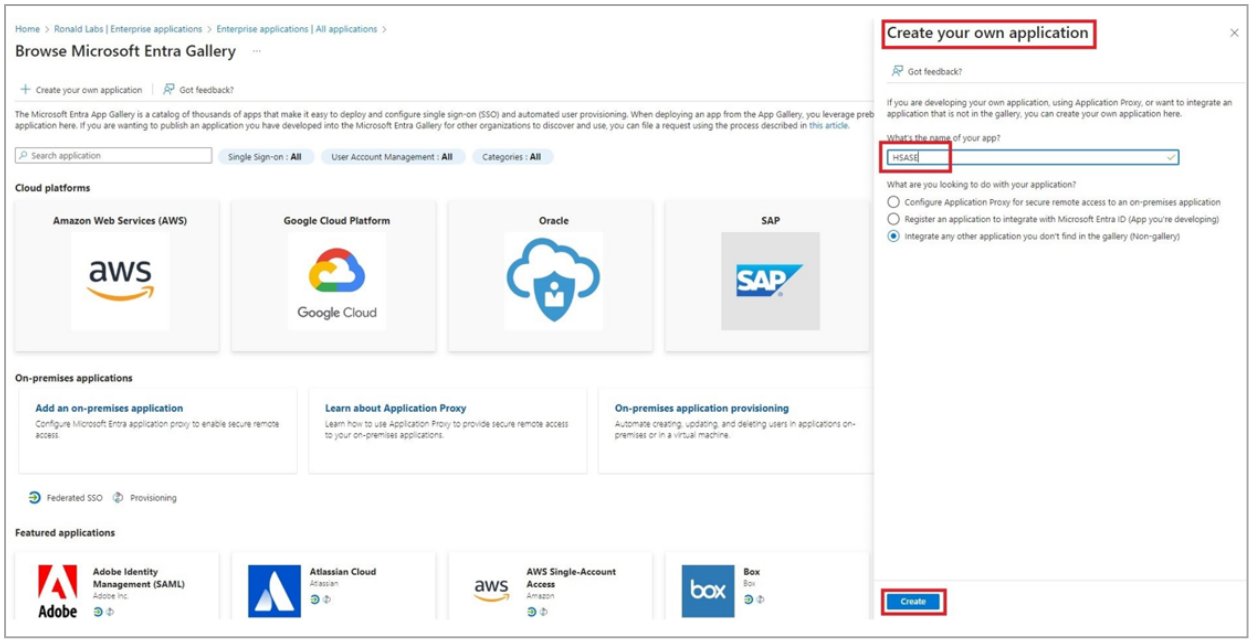
6. Go to **All applications**.
7. Click **New application**.



8. In the **Browse Microsoft Entra Gallery** page, click **Create your own application**.

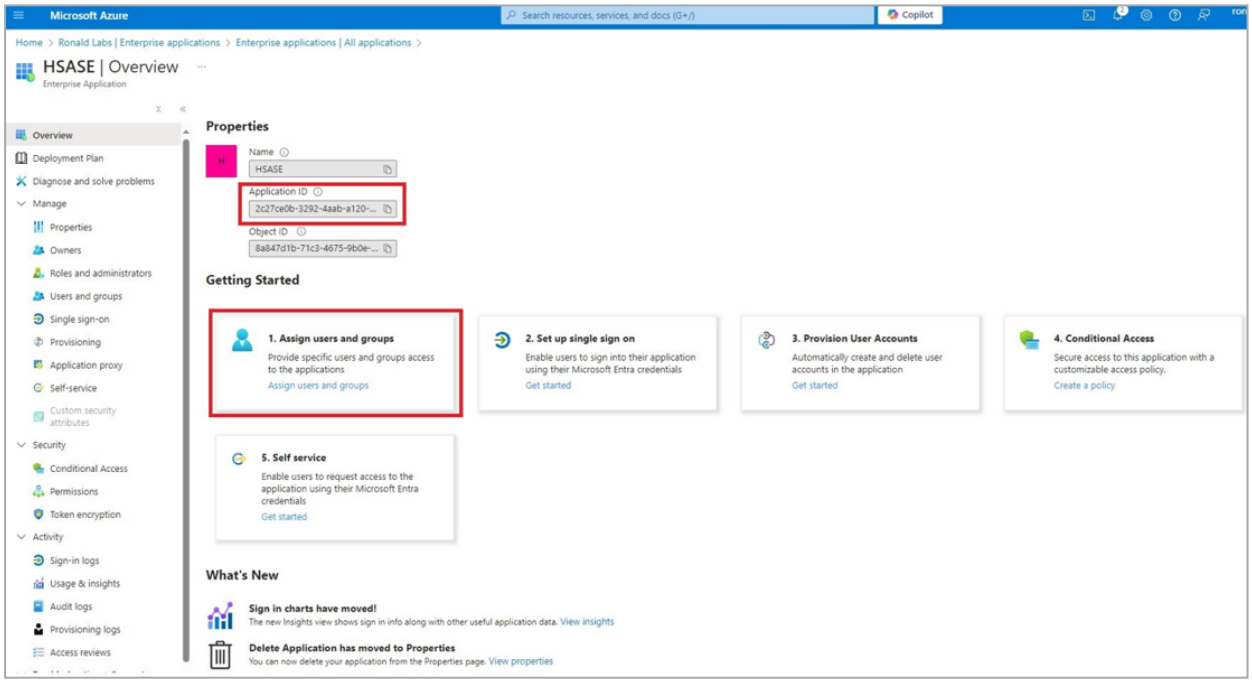


9. In the **Create your own application** panel that appears on the right, enter the application name (for example, SASE) and click **Create**.

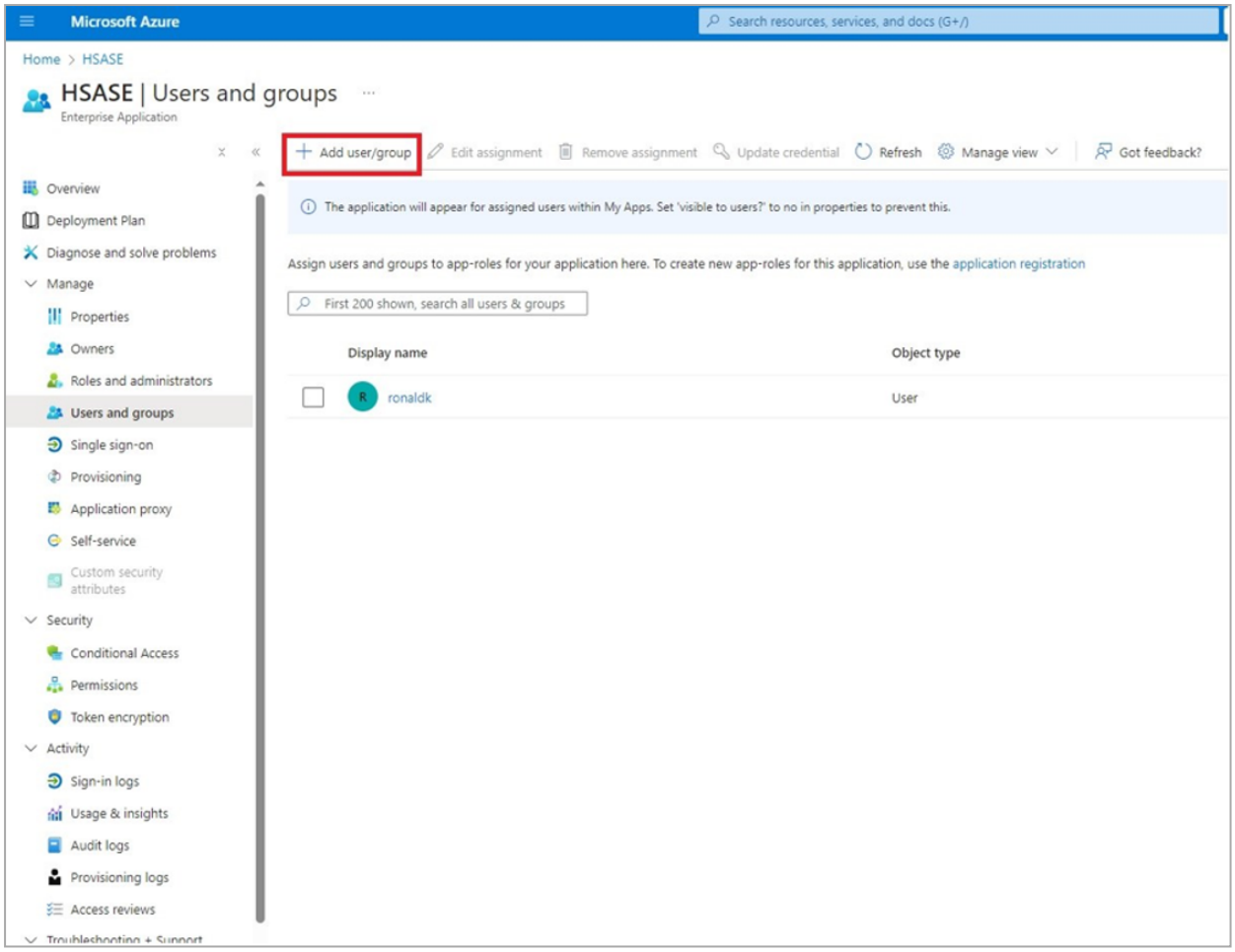


Once the application is created, the **Overview** page appears.

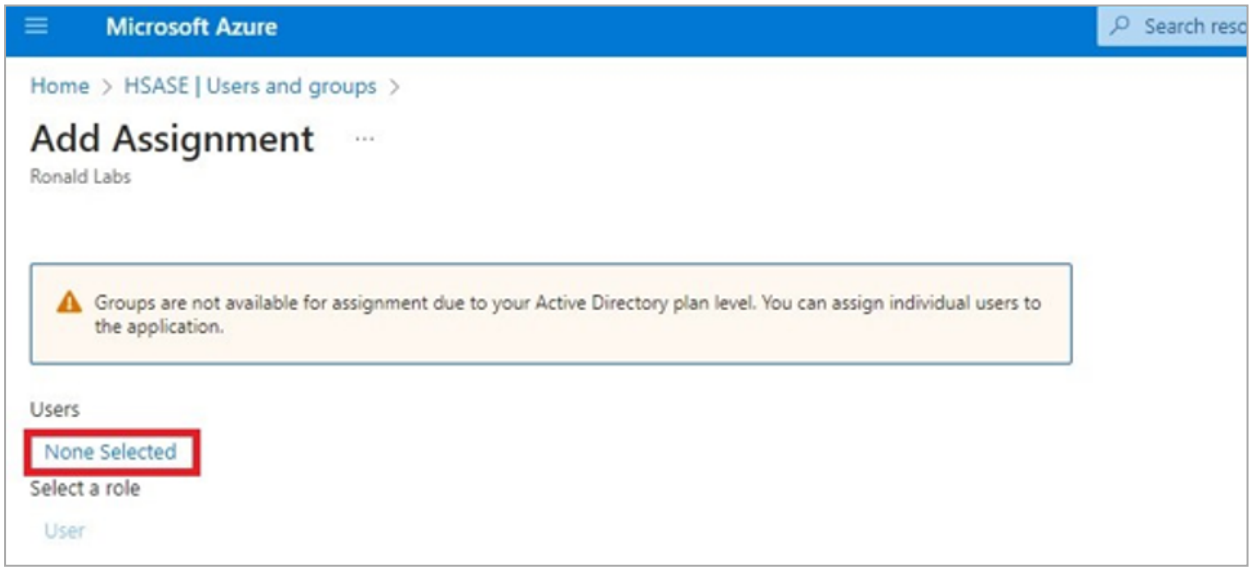
10. Click the icon next to **Application ID** to copy it.



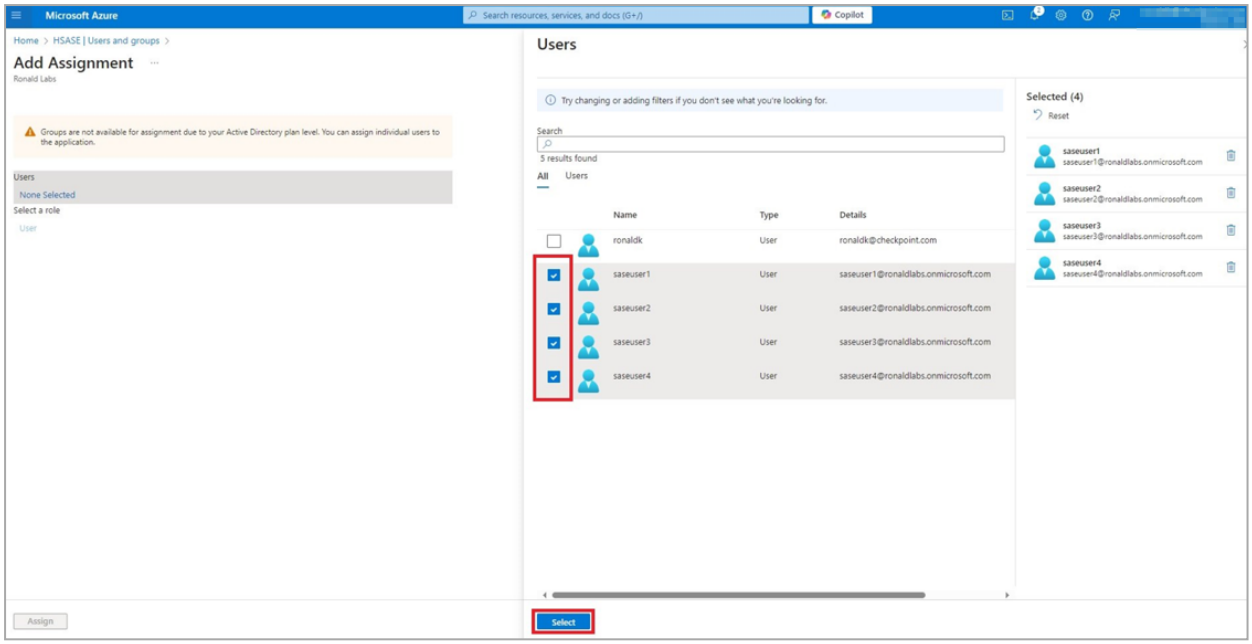
11. Click **Assign users and groups** and then click **Add user/group**.



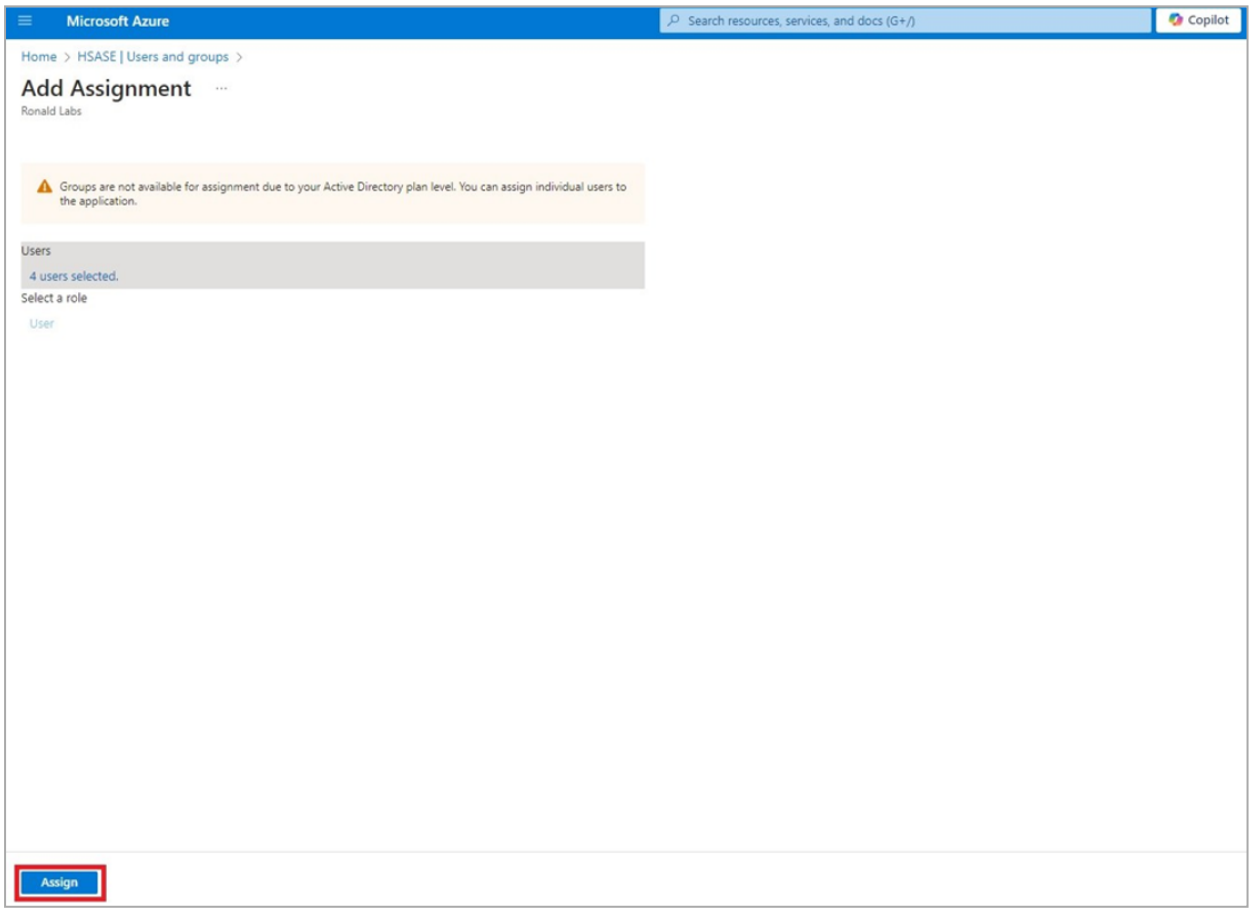
12. In the **Users** section, click **None Selected**.



13. Select the users and groups you want to add to the application and click **Select**.



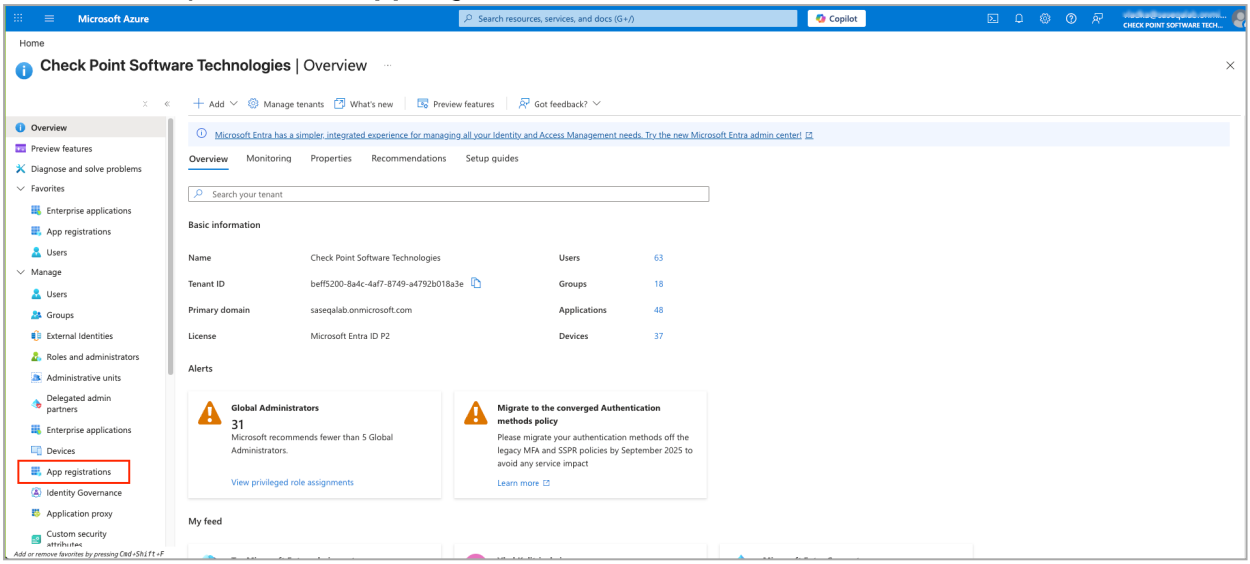
14. Click **Assign**.



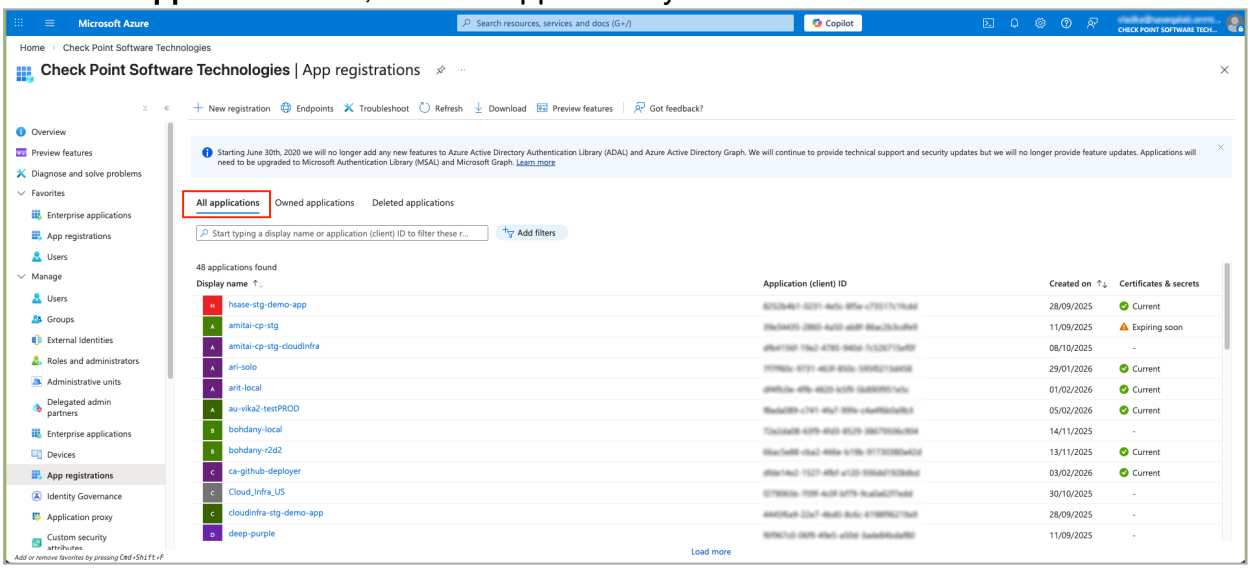
Once assigned, the Home page appears.

15. Click **Microsoft Entra ID**.

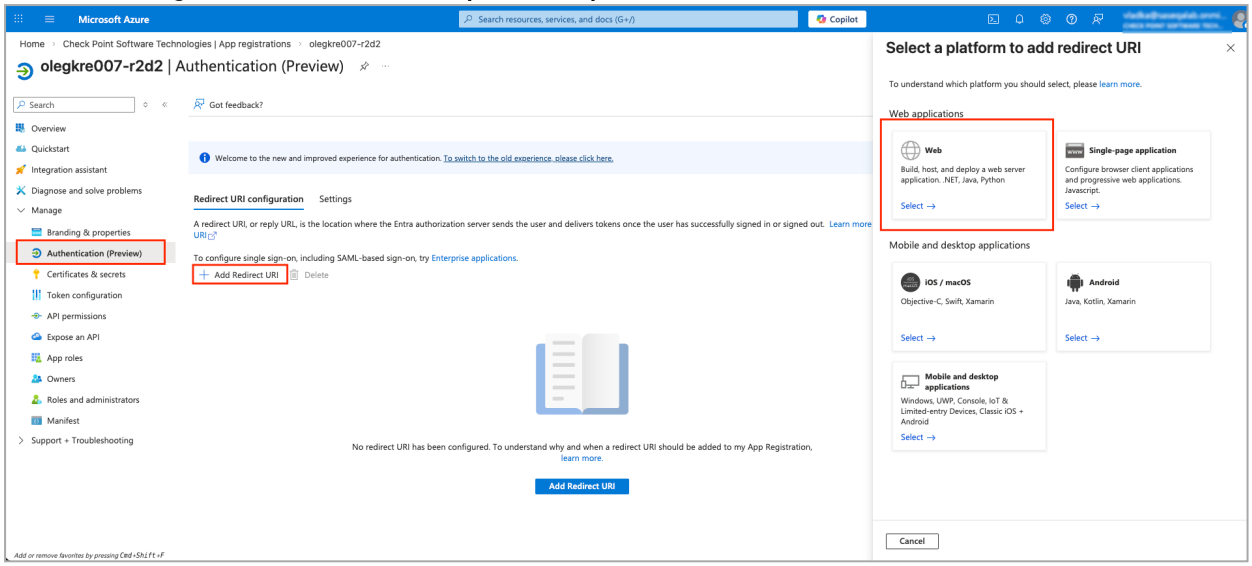
16. From the left panel, click **App registrations**.



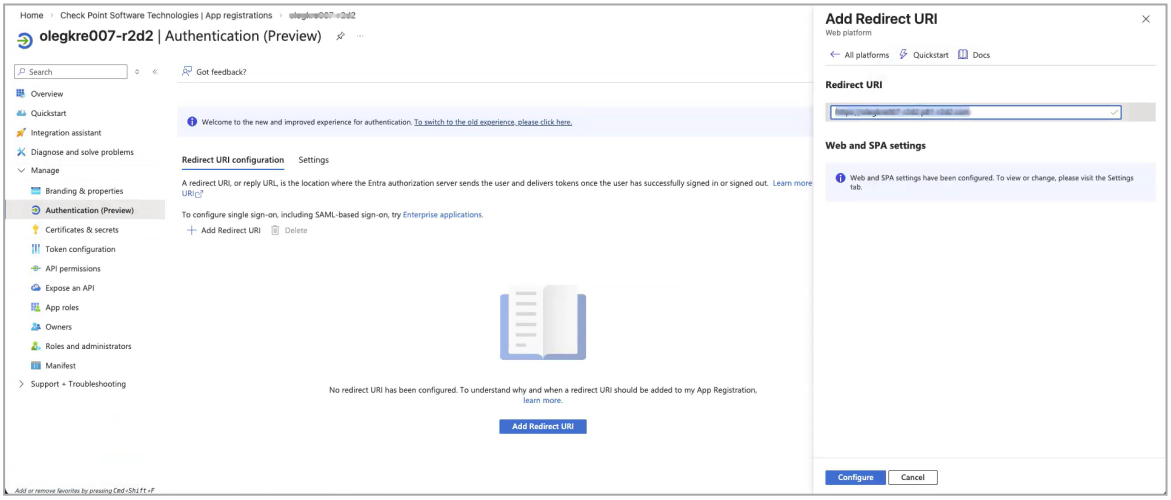
17. In the **All applications** tab, click the application you created.



18. Go to **Manage** > **Authentication (Preview)** and click **Add Redirect URI**.

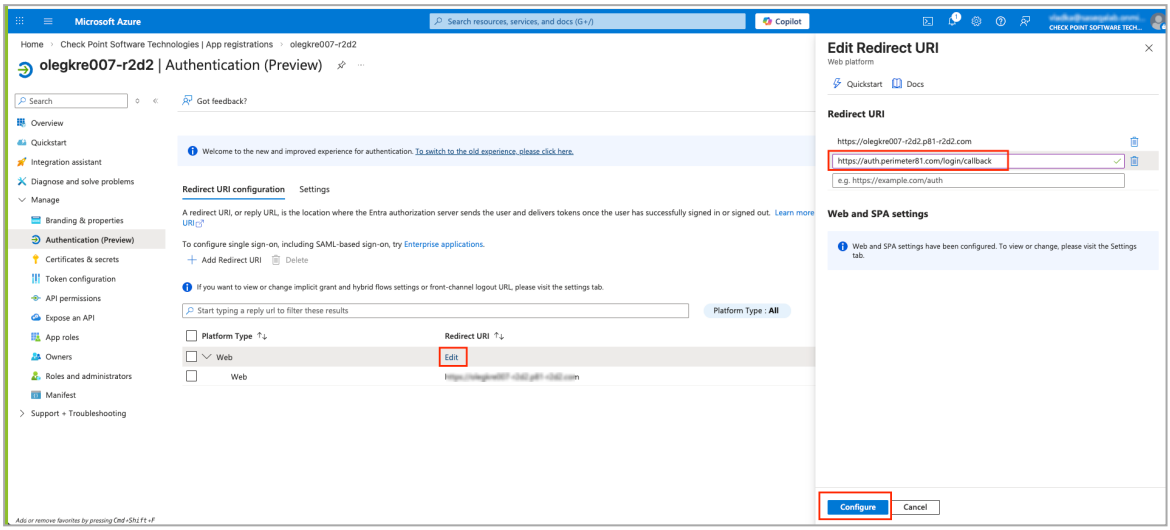


19. In the **Select a platform to add redirect URI** panel that appears on the right, select **Web**.
20. In the **Redirect URIs** field, enter your workspace name and click **Configure**:
    - For EU based platform - `https://workspace.eu.sase.checkpoint.com`
    - For US based platform - `https://workspace.perimeter81.com`
    - For AU based platform - `https://workspace.au.sase.checkpoint.com`
    - For IN based platform - `https://workspace.in.sase.checkpoint.com`

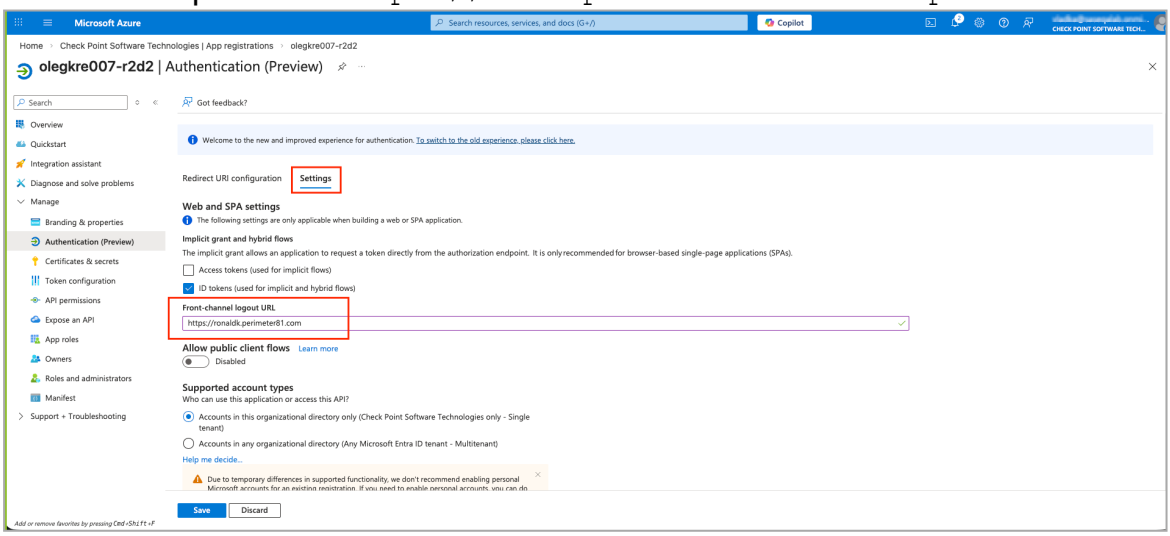


21. In the **Redirect URIs** section, click **Add URI** and add these:
    - For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback`
    - For US based platform - `https://auth.perimeter81.com/login/callback`

- For AU based platform - `https://auth.au.sase.checkpoint.com/login/callback`
- For IN based platform - `https://auth.in.sase.checkpoint.com/login/callback`



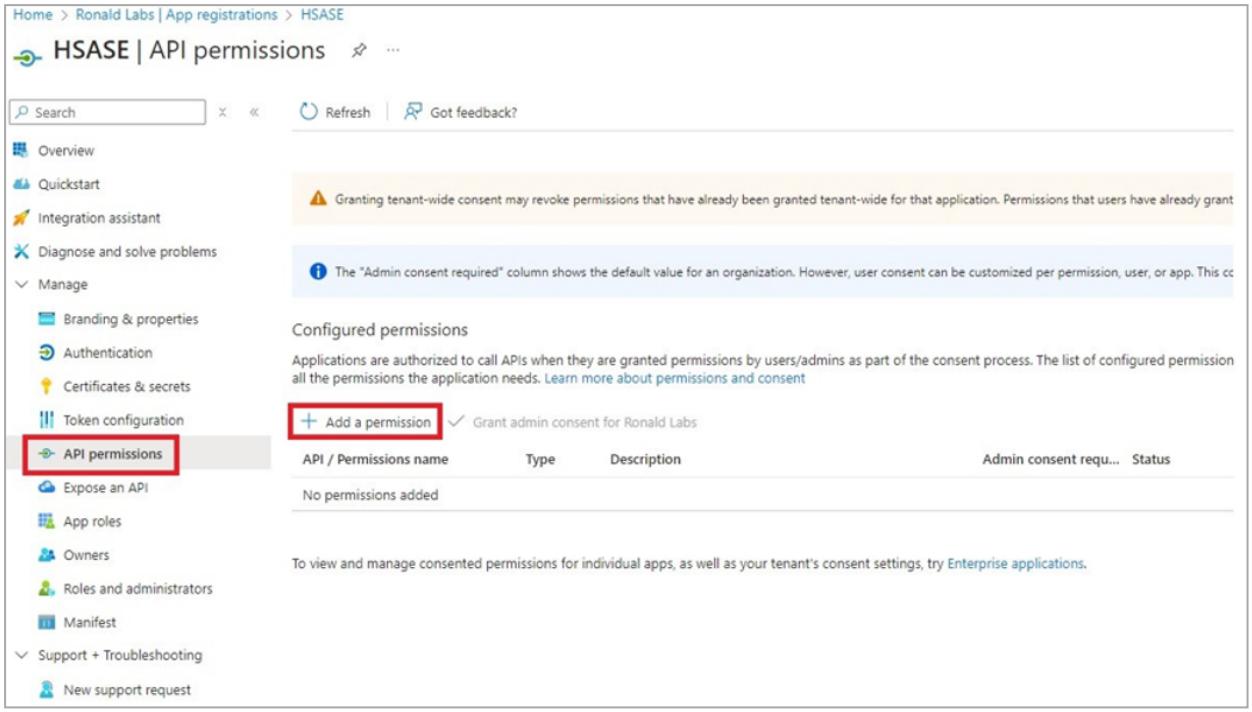
22. Click **Configure**
23. Click Settings. In the **Front-channel logout URL** section, enter your workspace name:
    - For EU based platform - `https://workspace.eu.sase.checkpoint.com`
    - For US based platform - `https://workspace.perimeter81.com`
    - For AU based platform - `https://workspace.au.sase.checkpoint.com`
    - For IN based platform - `https://workspace.in.sase.checkpoint.com`



24. In the **Supported account types** section, select the applicable option for supported account types and click **Save**.

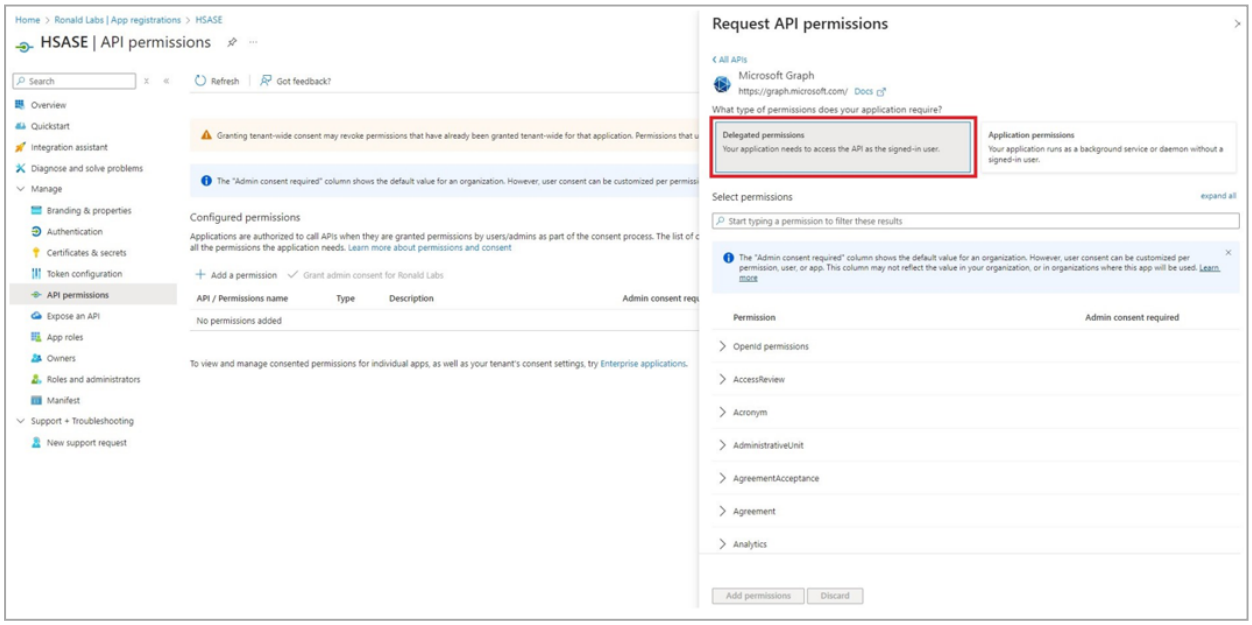
Step 2 - Configuring API Permissions

1. From the left panel, click **Manage** > **API permissions** and then click **Add a permission**.

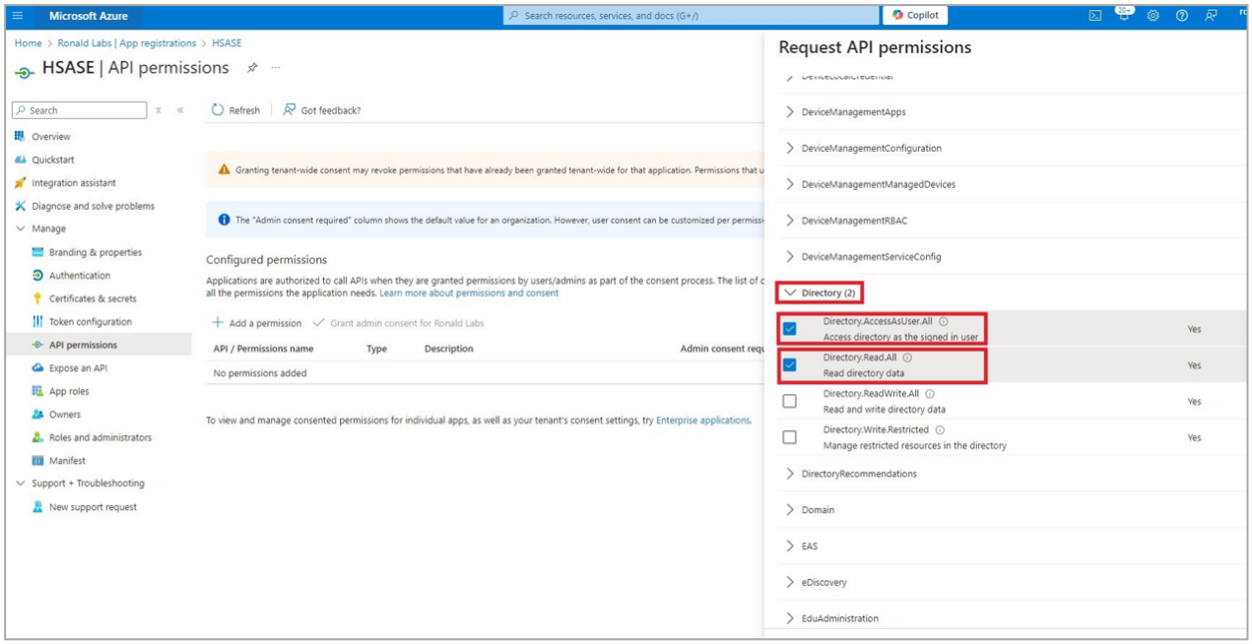


   The **Request API permissions** panel appears to the right.

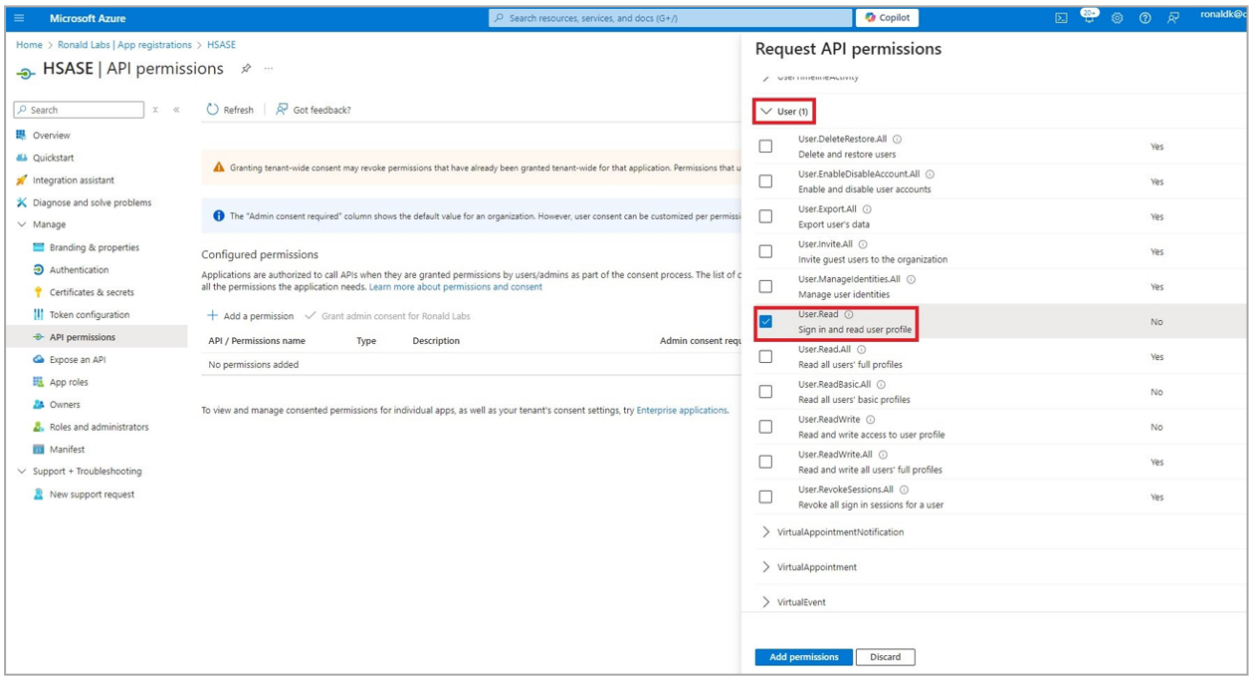
2. Select **Microsoft APIs** tab and then select **Microsoft Graph**.
3. Click **Delegated permissions**.



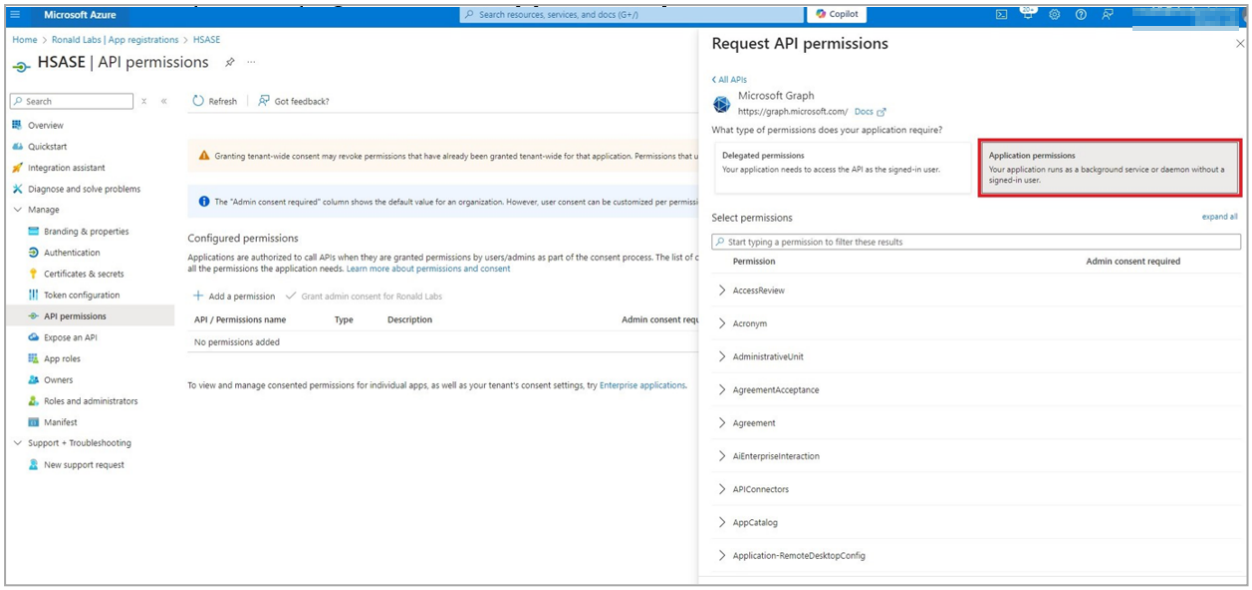
4. Click **Directory** to view the permissions and then select **Directory.Read.All**.



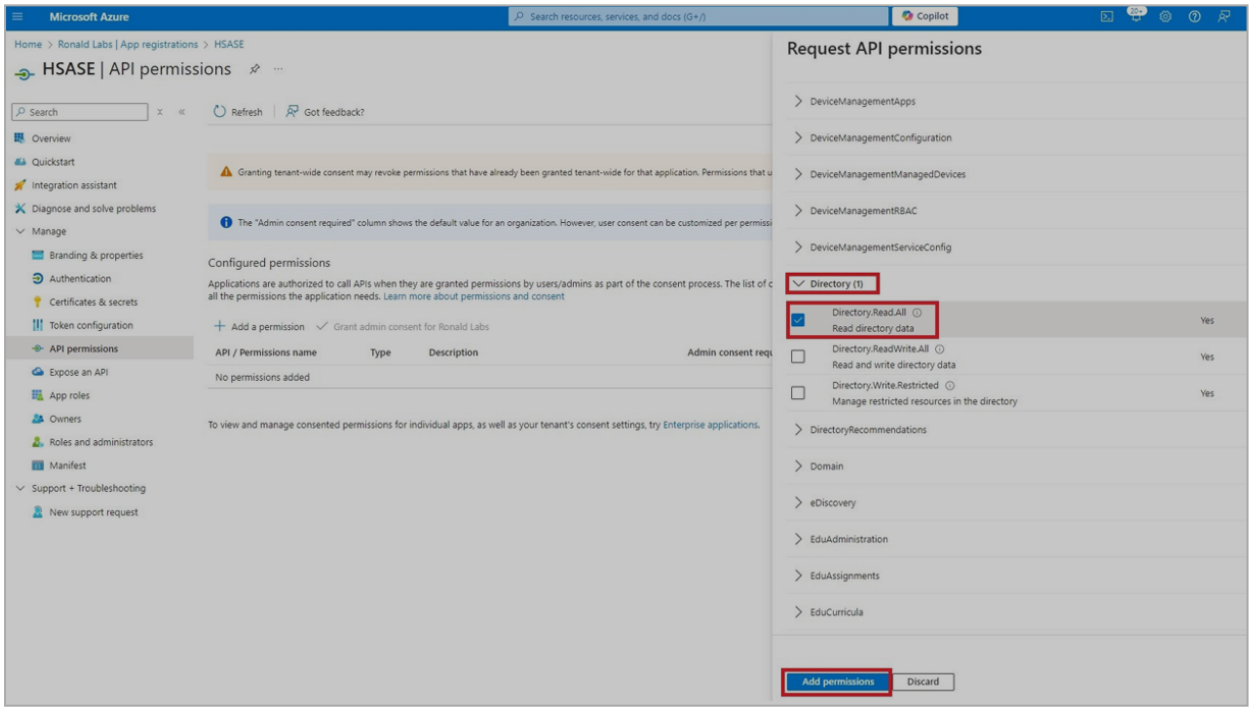
5. Click **User** to view the permissions and then select **User.Read**.



6. Scroll to the top of the page and click **Application permissions**.



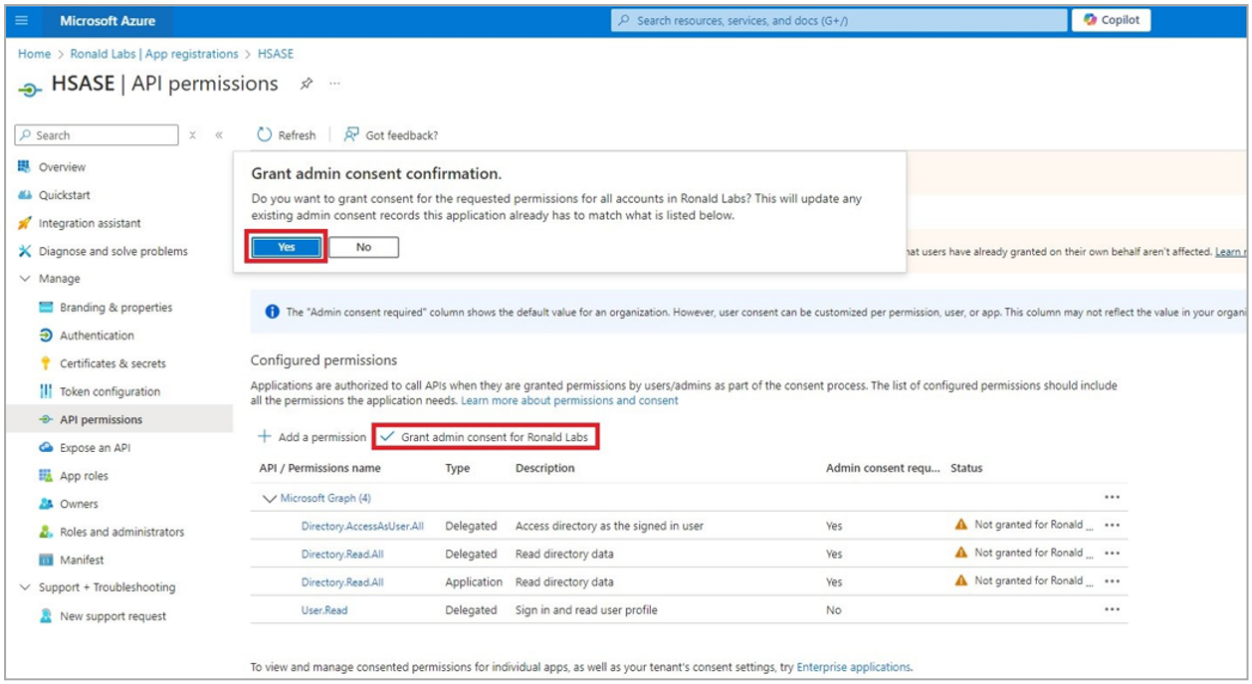
7. Click **Directory** to view the permissions and then select **Directory.Read.All**.
8. Click **Add permissions**.



9. Click **Grant admin**.

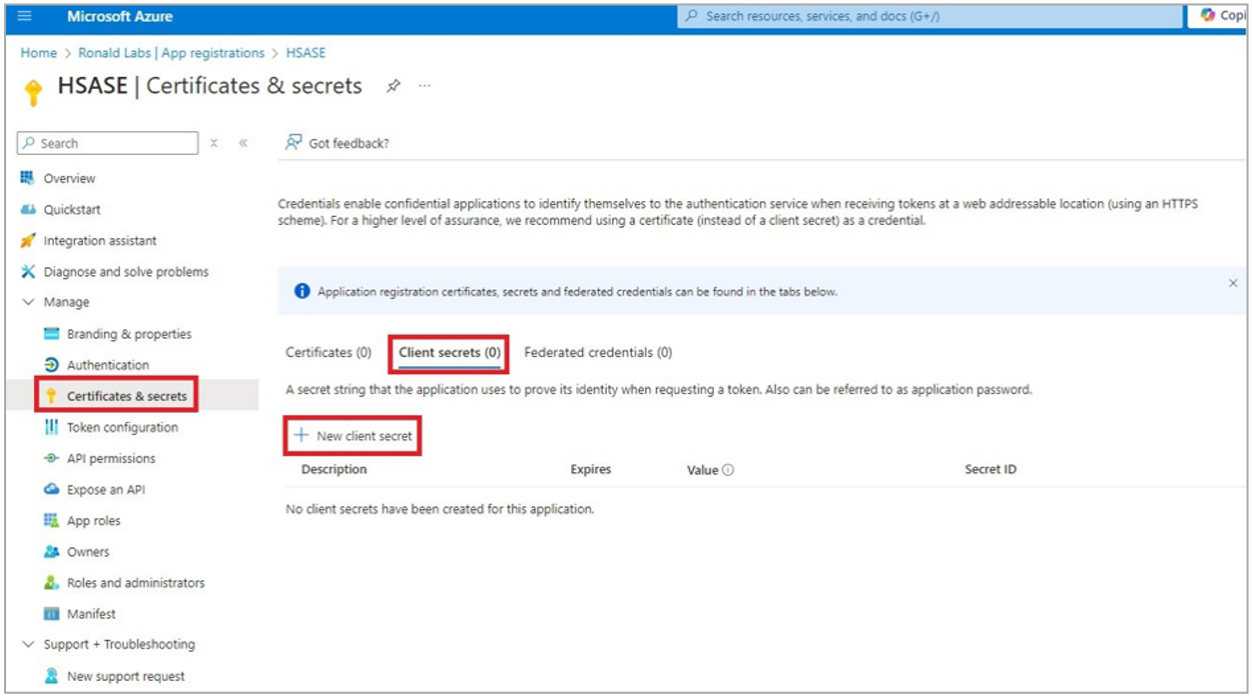
   The **Grant admin consent confirmation** window appears.

10. Click **Yes**.



Step 3 - Configuring Secret Key for the Application

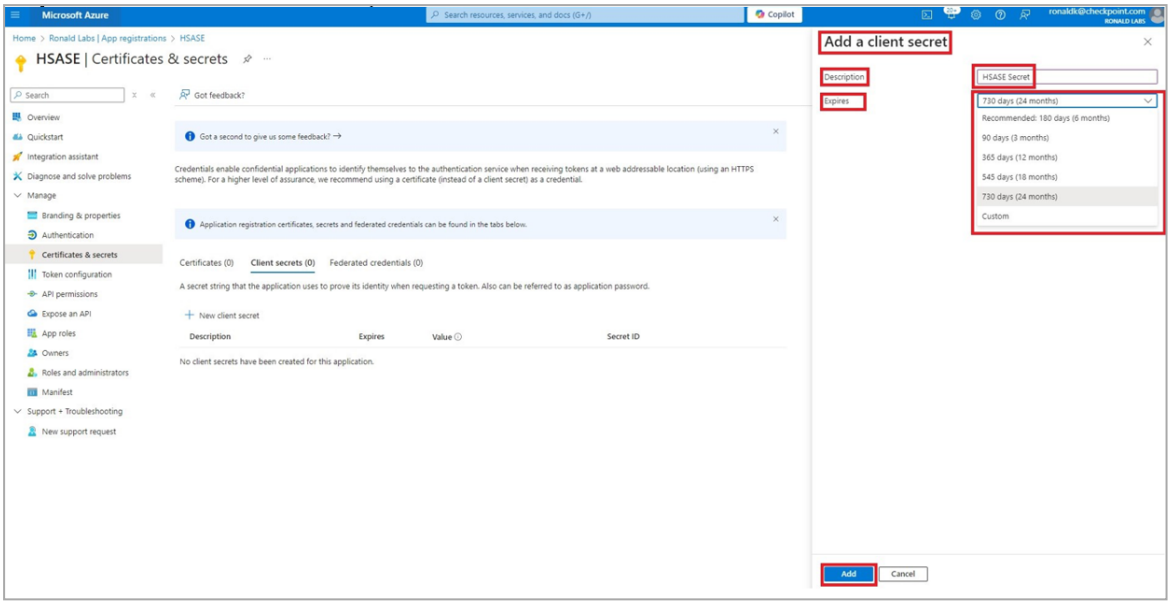
1. From the left panel, select **Certificates & secrets** and click the **Client secrets** tab.
2. Click **New client secret**.



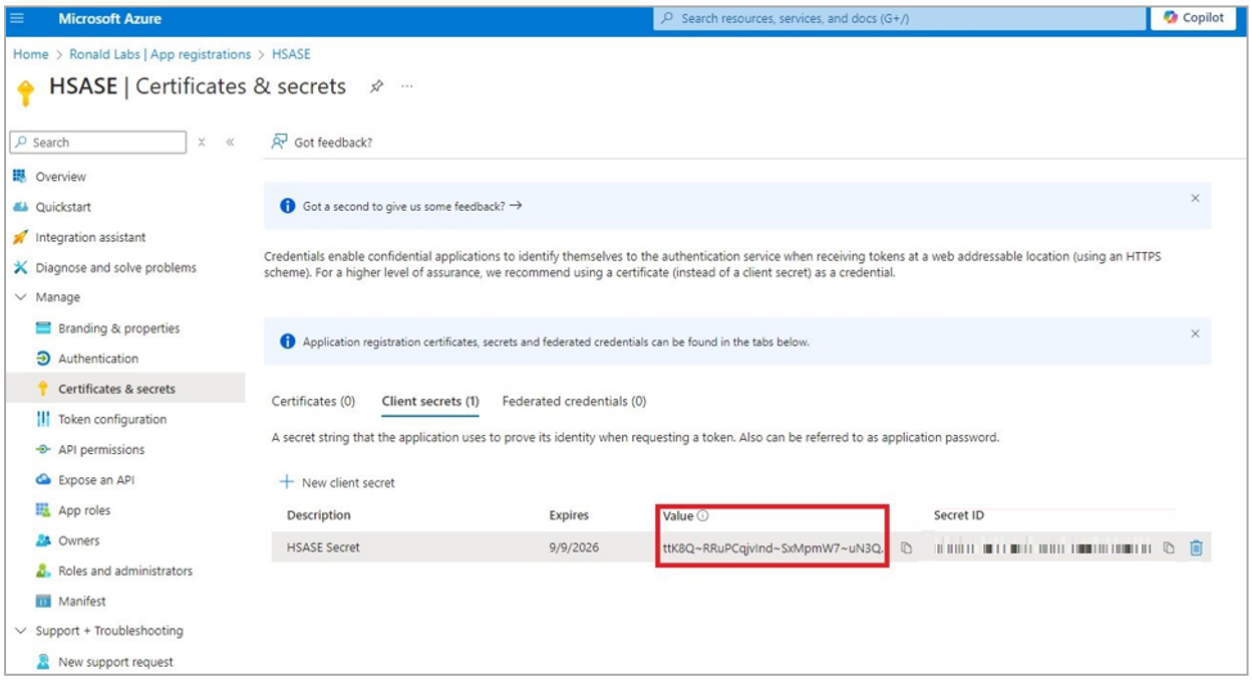
Note - You must use this client secret (password) as the Client Secret when connecting with the SASE IdP.

3. In the **Add a client secret** panel that appears on the right, specify these:

- **Description** - Enter a description.
- **Expires** - Select the secret expiration from the list.

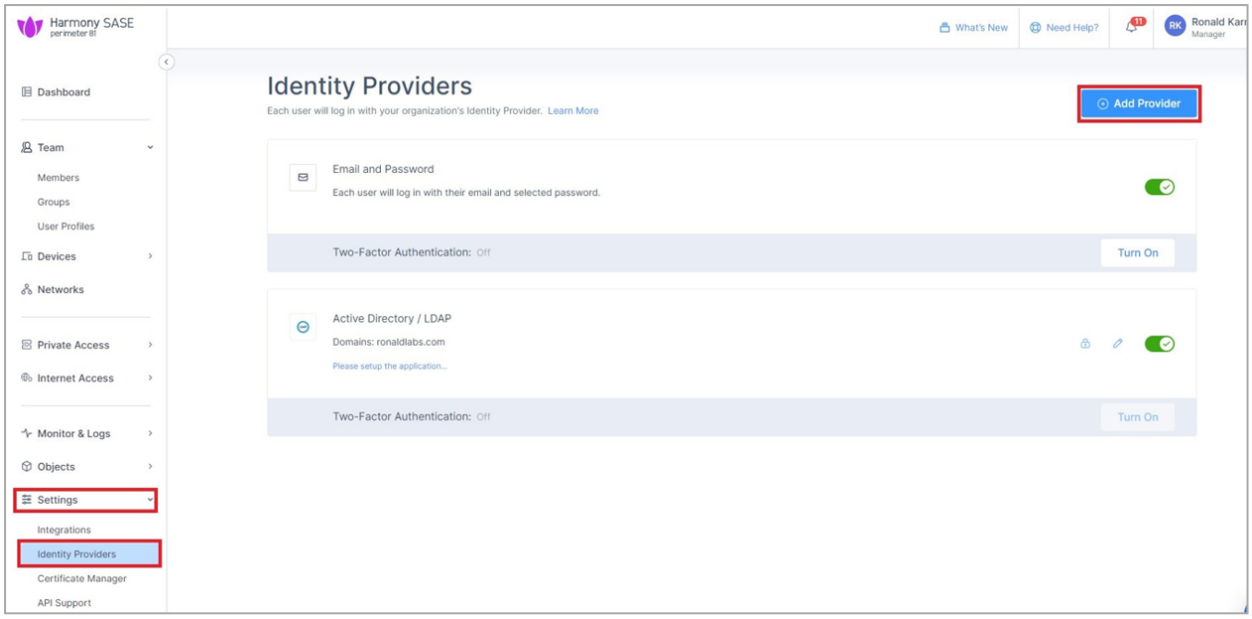


4. Click **Add**.
5. To copy the secret value, in the **Value** field, click .



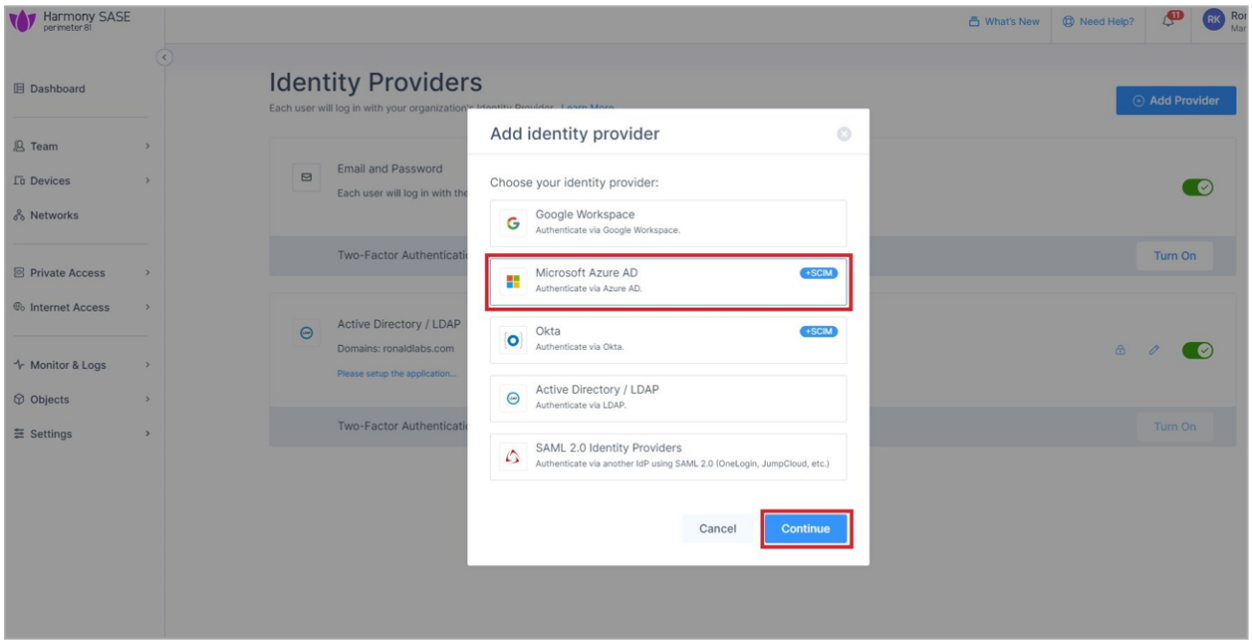
Part 2: Configuring SASE IDP

1. Access the SASE Administrator Portal.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.



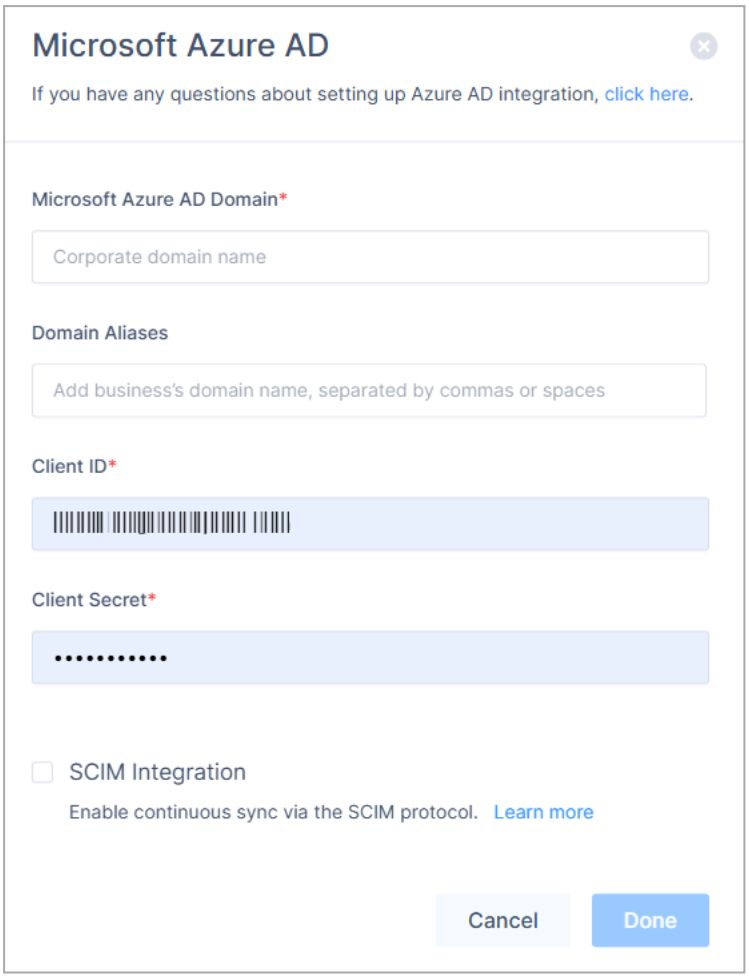
The **Add identity provider** window appears.

4. Select **Microsoft Azure AD** and click **Continue**.



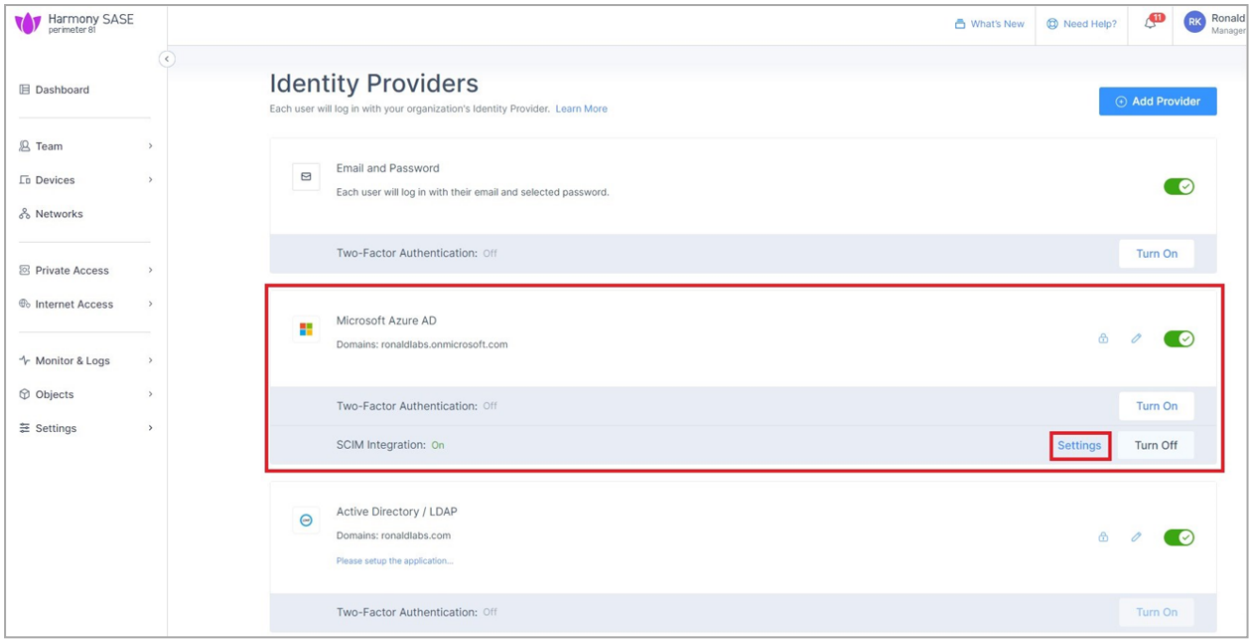
5. Enter these details:
   - **Microsoft Azure AD Domain**
   - (Optional) **Domain Aliases**
   - **Client ID**

- **Client Secret** (you copied while configuring the key)

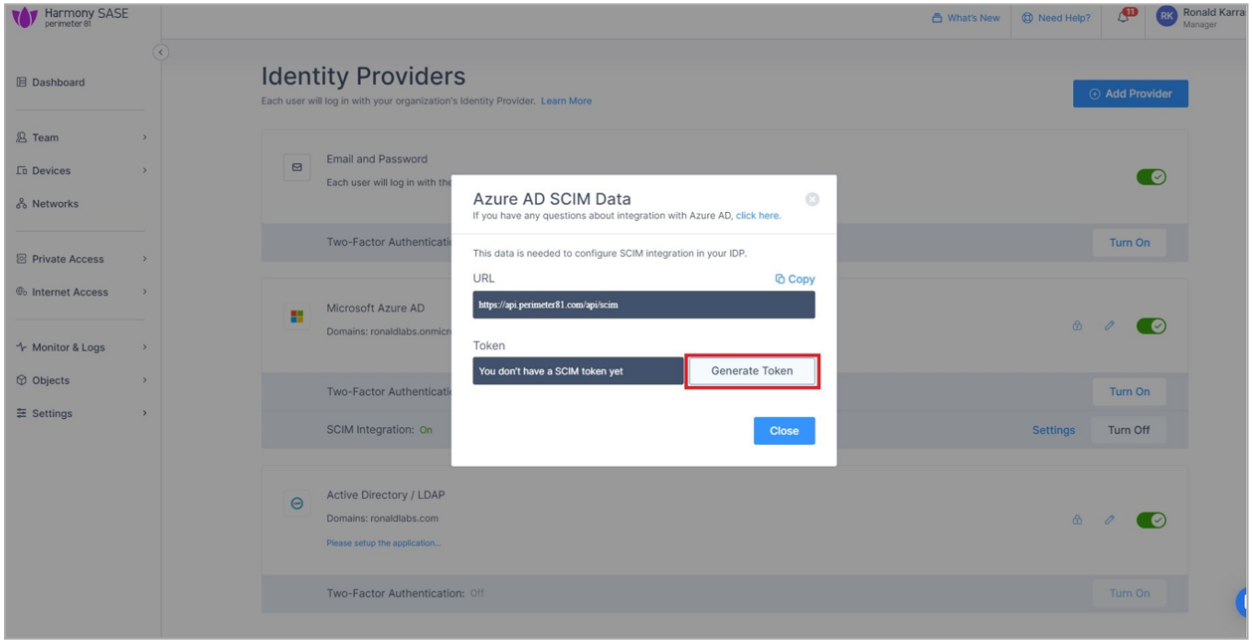


6. Select the **SCIM Integration** checkbox.
7. Click **Done**.

   The Azure AD gets created successfully.
8. In the **Microsoft Azure AD** section, click **Settings**.

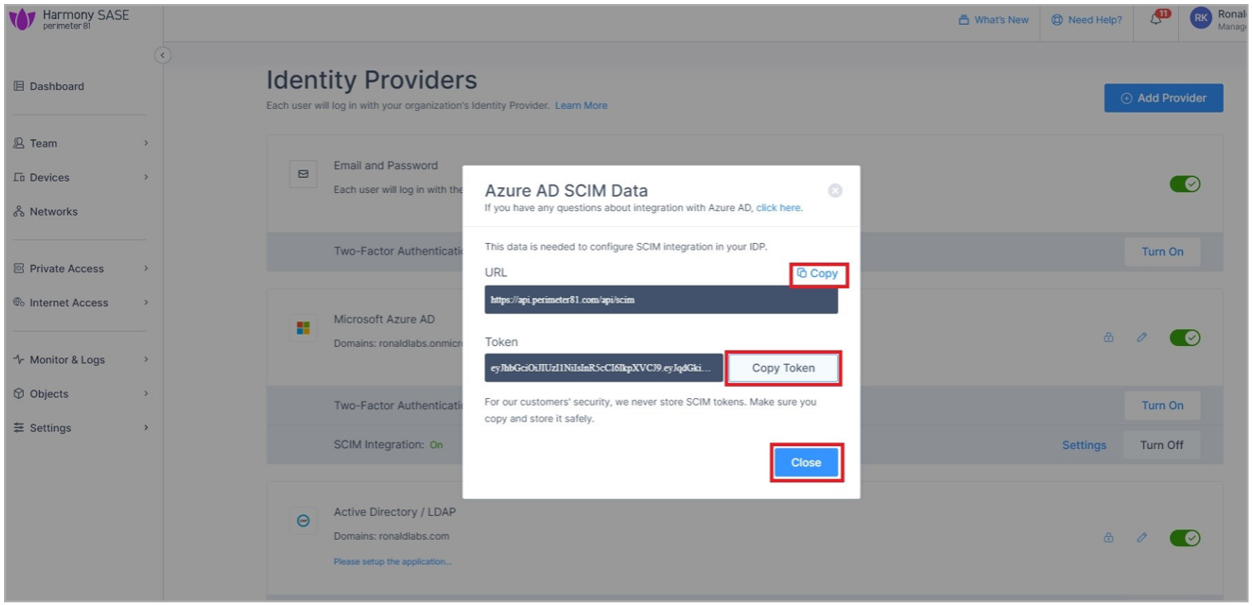


9. Click **Generate Token**.



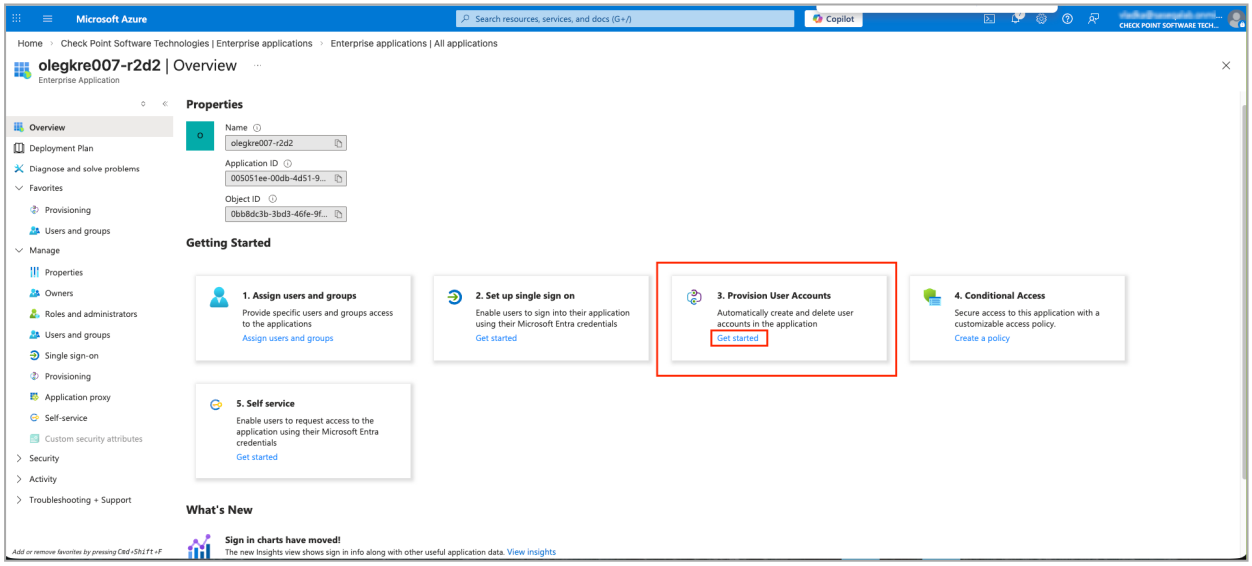
The **Azure AD SCIM Data** window appears.

10. Copy the URL and Token and then click **Close**.

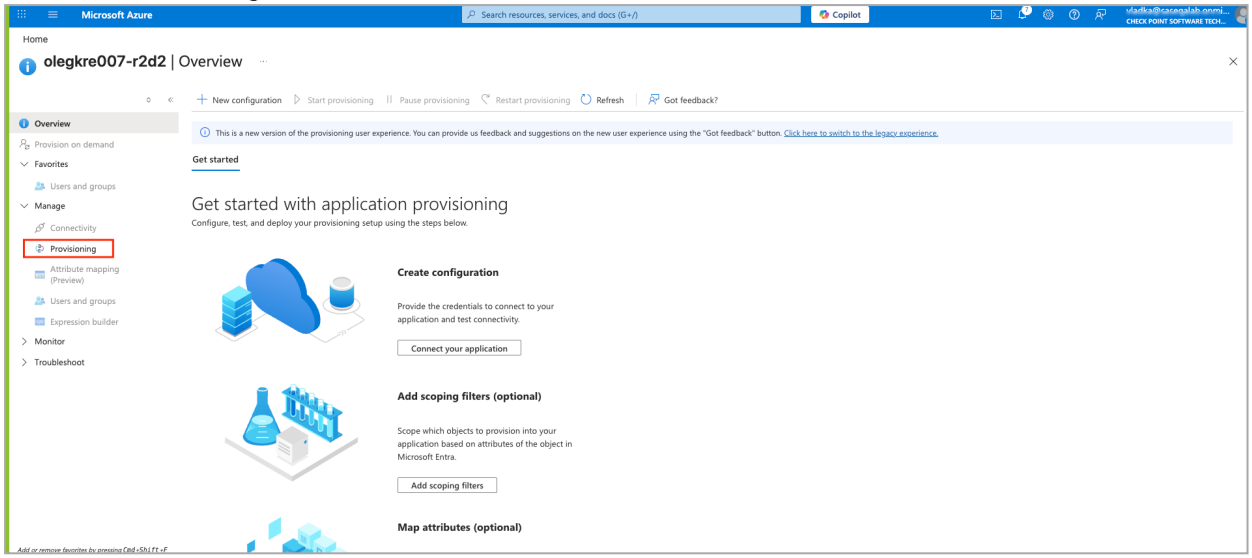


Part 3: Configuring SCIM

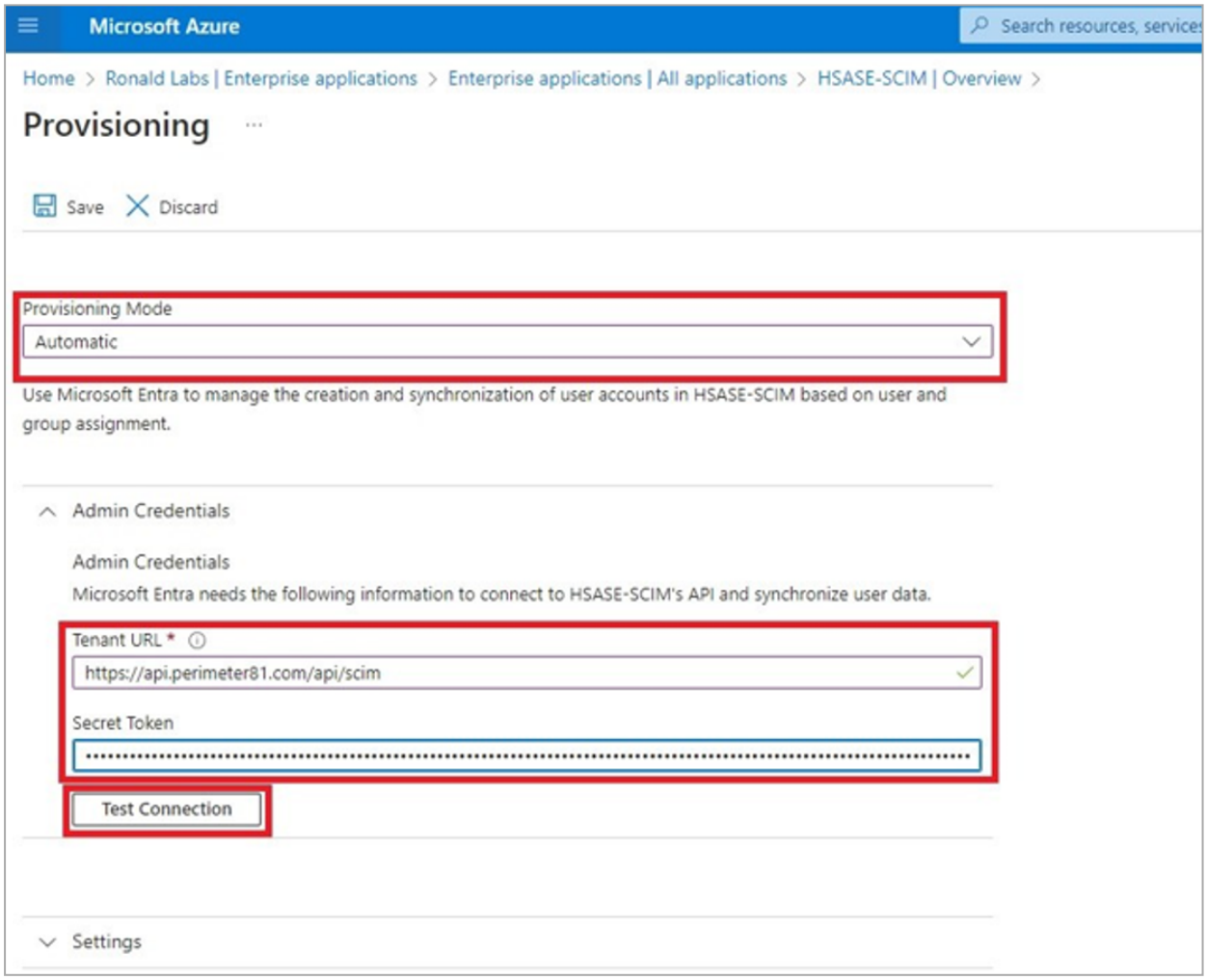
1. Access the Microsoft Azure Portal using administrator credentials.
2. Go to **Microsoft Entra ID** > **Enterprise Applications** and locate the application previously created in Step 1 - Creating an application in Entra ID.
3. Click the application name to open the configuration.
4. Click **Get Started** in the **Provision User Accounts** tile.



5. Click **Provisioning**.



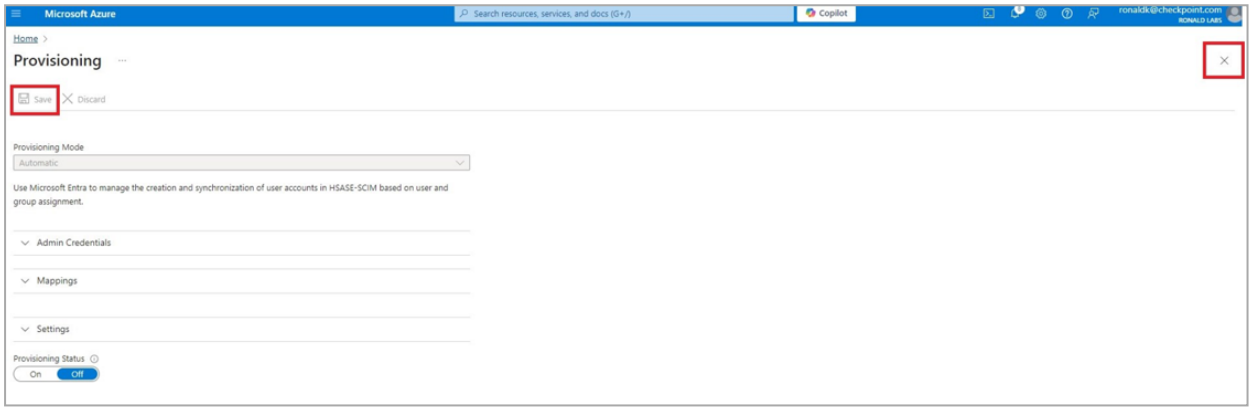
6. From the **Provisioning Mode** list, select **Automatic**.



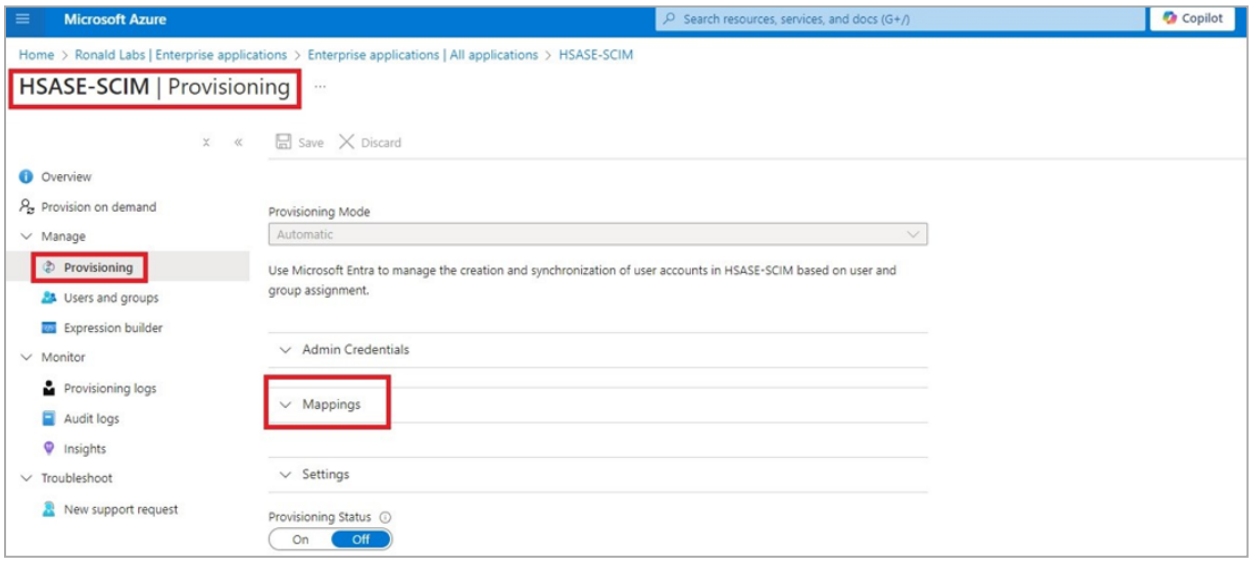
7. Expand **Admin Credentials**.
8. In the **Tenant URL** field, enter the SCIM URL.

- For US based platform - https://api.perimeter81.com/api/scim
- For EU based platform - https://api.eu.sase.checkpoint.com/api/scim
- For AU based platform - https://api.au.sase.checkpoint.com/api/scim
- For IN based platform - https://api.in.sase.checkpoint.com/api/scim

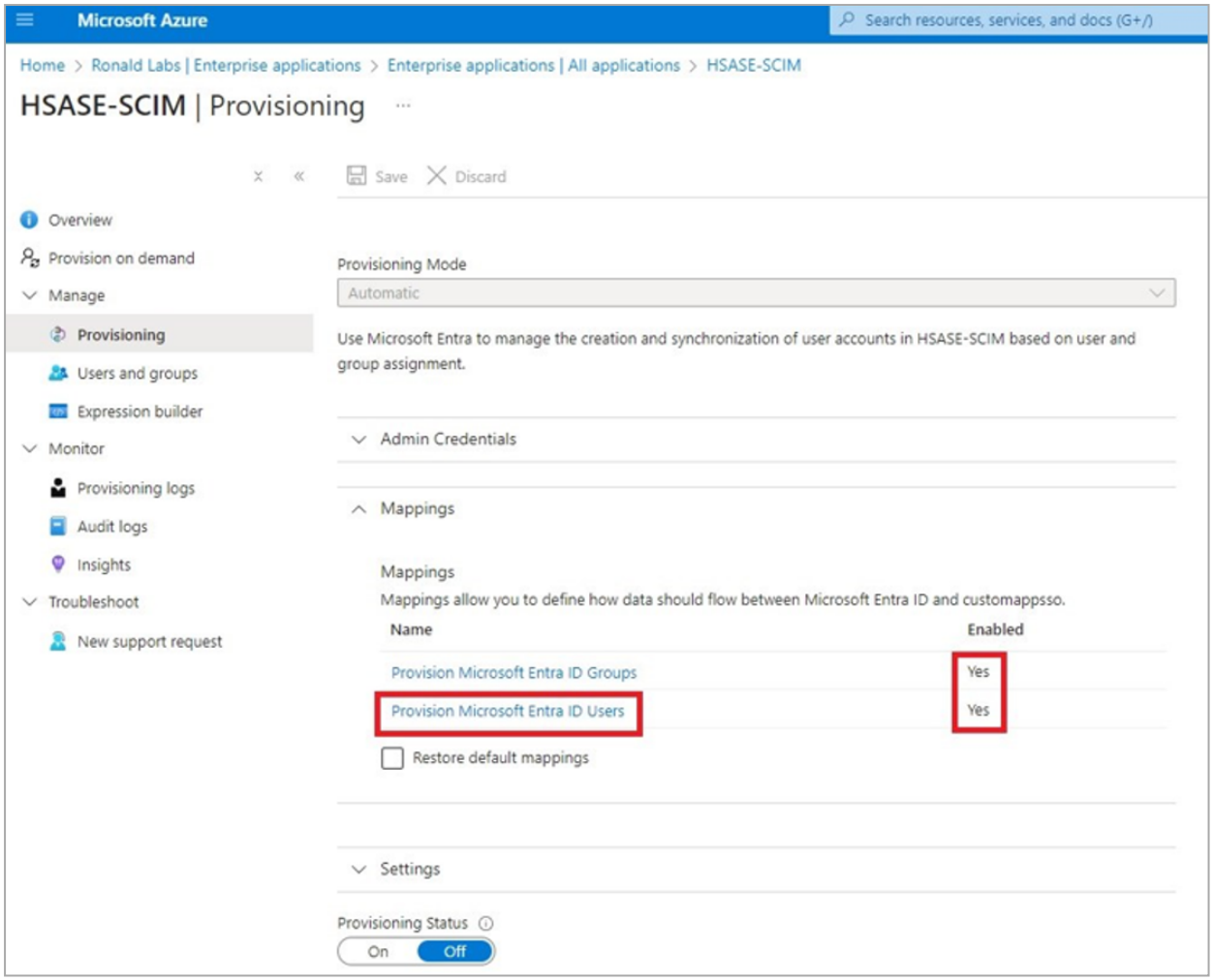
9. In the **Secret Token** field, paste the token you copied in Part 2: Configuring SASE IDP section **step 11**.
10. Click **Test Connection**.
11. Click **Save** at the top left corner.



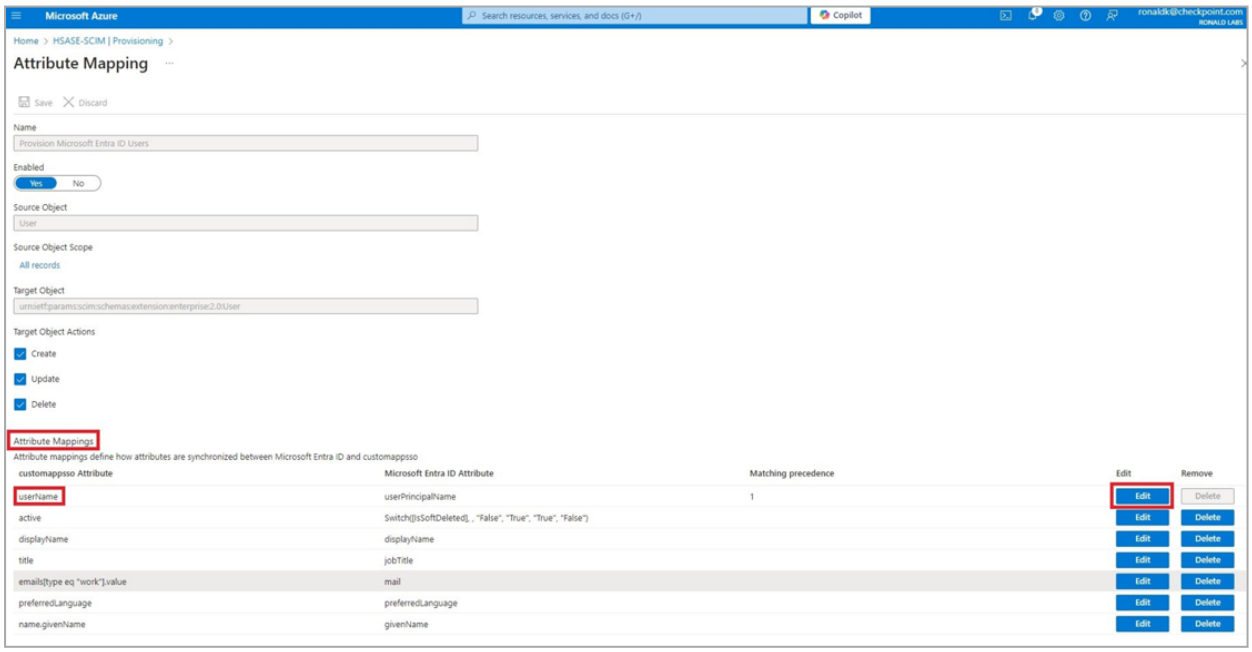
12. Expand **Mappings**.



13. Make sure that these options are enabled:
    a. **Provision Microsoft Entra ID Groups**
    b. **Provision Microsoft Entra ID Users**
14. Click **Provision Microsoft Entra ID Users**.

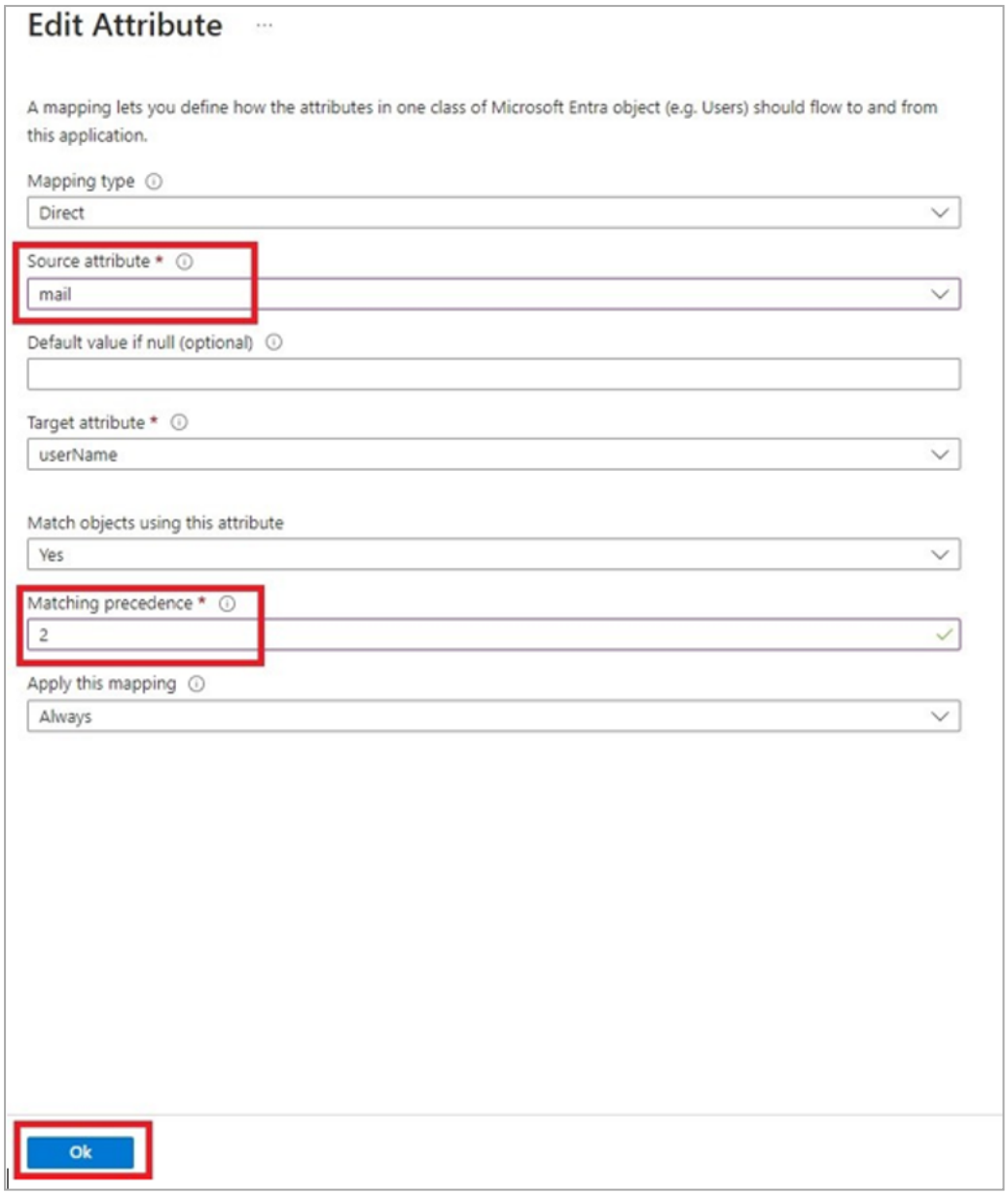


15. In the **Attribute Mappings** section, for **userName**, click **Edit**.



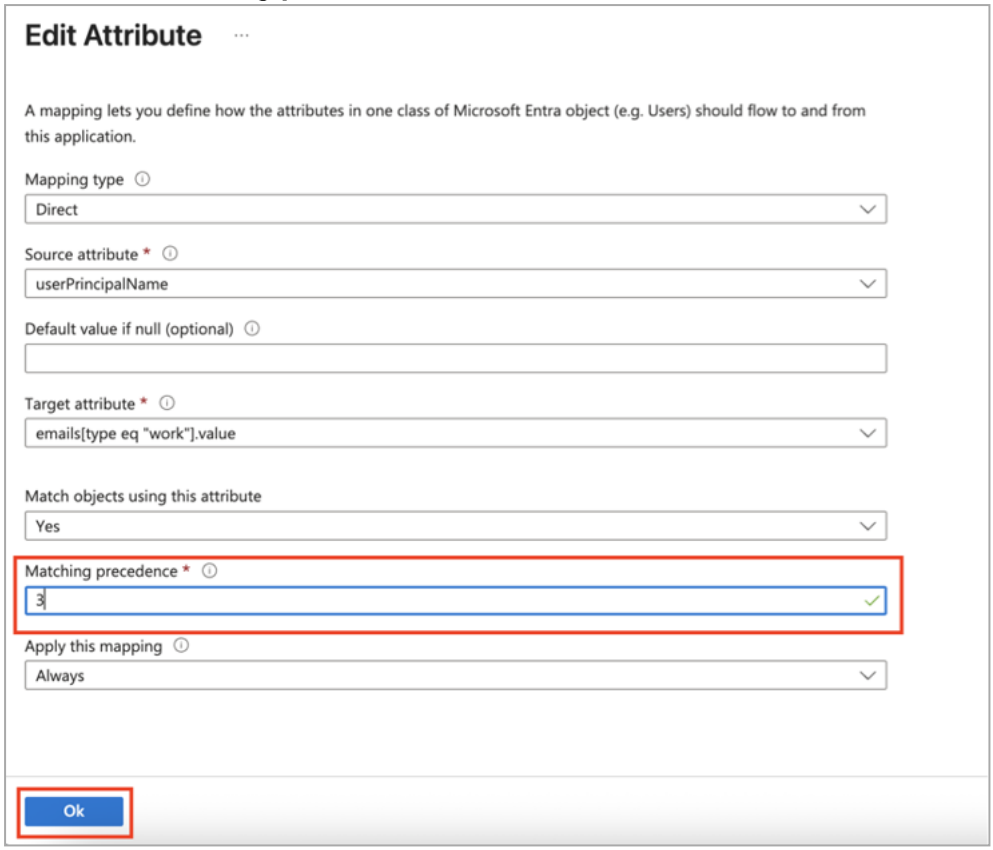
16. From the **Source attribute** list, select **mail**.

17. From the **Match precedence** list, select **2**.



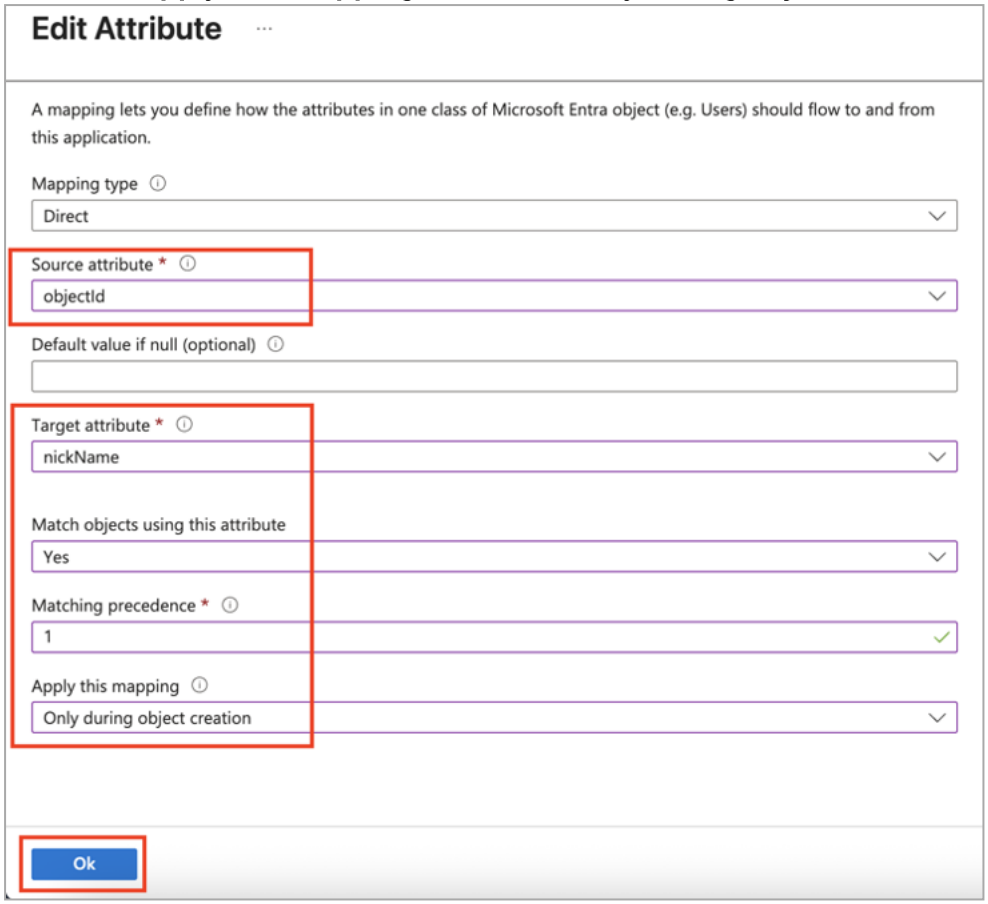
18. Click **OK**.
19. Locate the `emails[type eq "work"].value` attribute and click **Edit**.
20. From the **Source attribute** list, select **userPrincipalName**.
21. From the **Match objects using this attribute** list, select **Yes**.

22. From the **Matching precedence** list, select **3**.

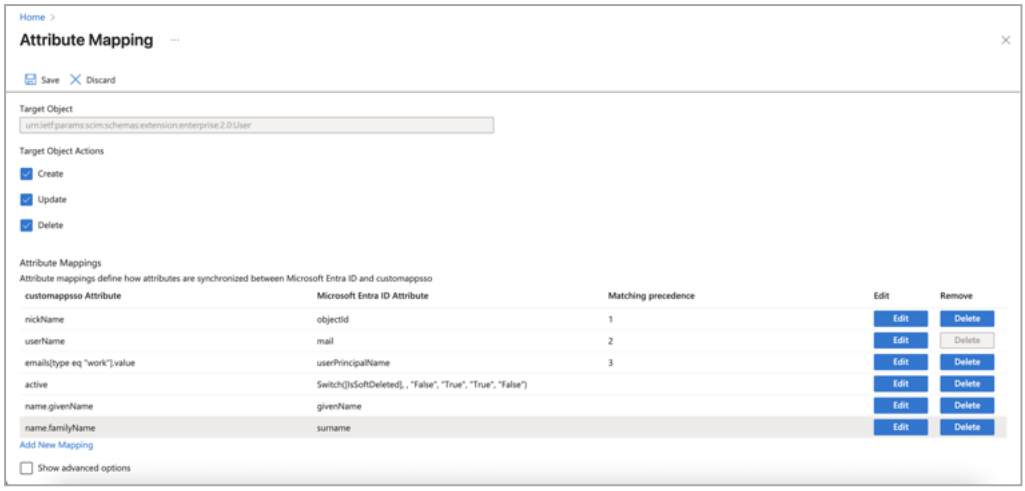


23. Click **OK**.
24. Go back to **Attribute Mappings** section and click **Add New Mapping**.
25. From the **Source attribute** list, select **objectId**.
26. From the **Target attribute** list, select **nickName**.
27. From the **Match objects using this attribute** list, select **Yes**.
28. From **Matching precedence** list, select **1**.

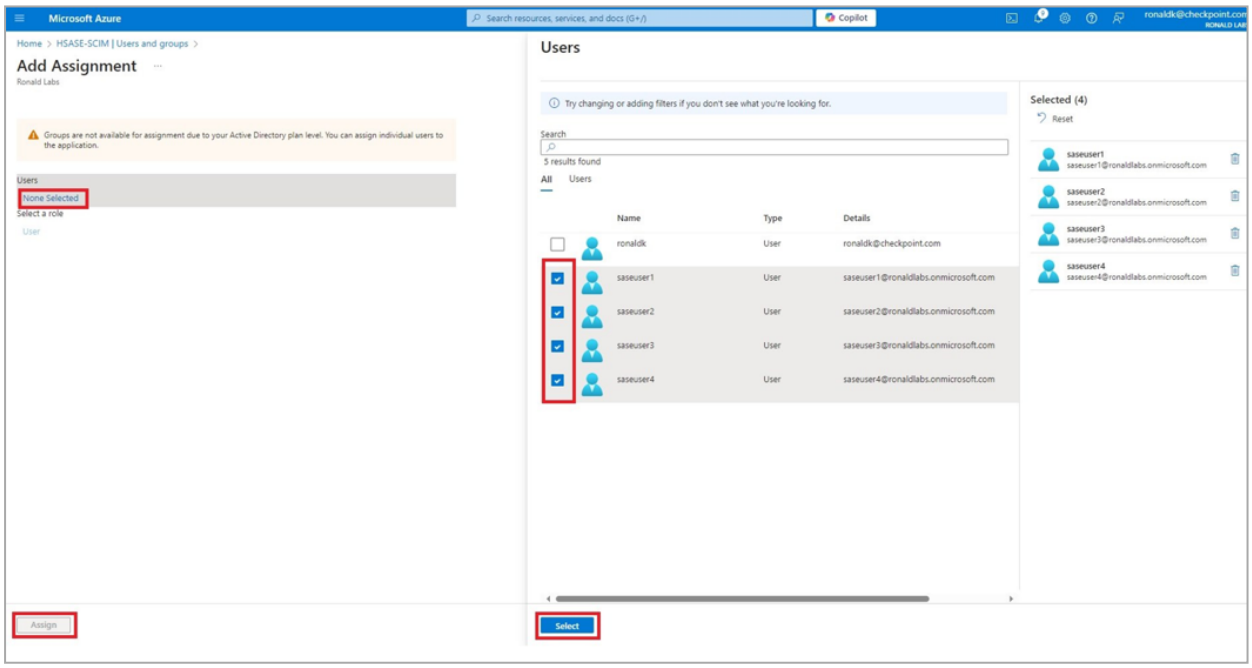
29. From the **Apply this mapping** list, select **Only during object creation**.



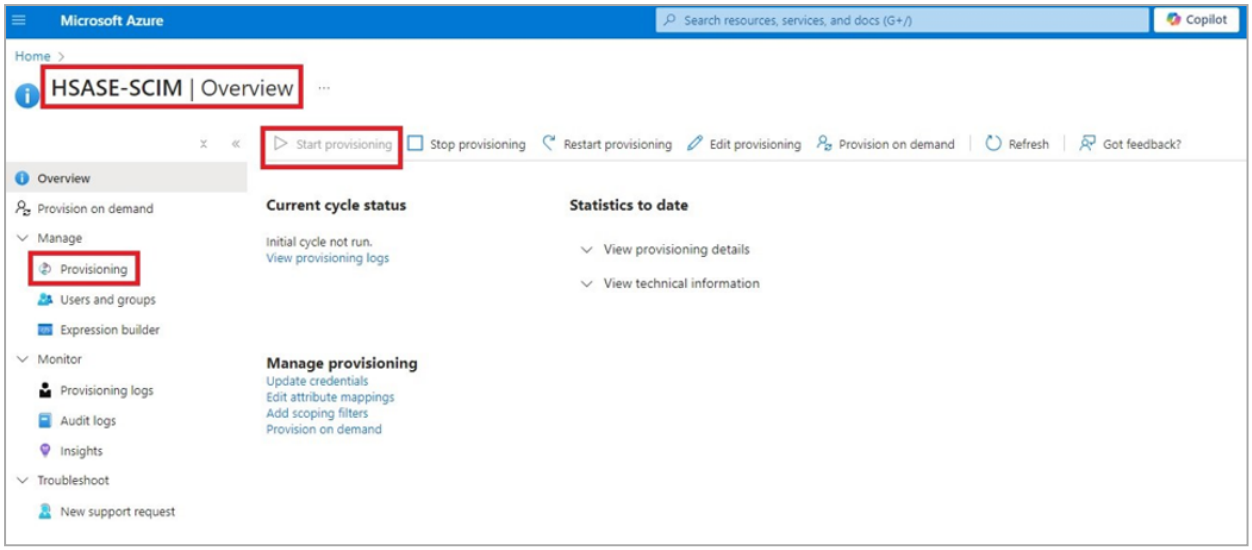
30. Click **OK**.
31. Retain these attributes and delete other attributes:
    - `nickName`
    - `emails[type eq "work"].value`
    - `userNamemail`
    - `active`
    - `name.givenName`
    - `name.familyNamesurname`



32. Click **Save**.
33. Go to SCIM Application and select **Users and groups**.
34. Click **Add users/group**.
35. In the **Users** section, click **None Selected**.
36. Select the user(s).
37. Click **Select** and then click **Assign**.

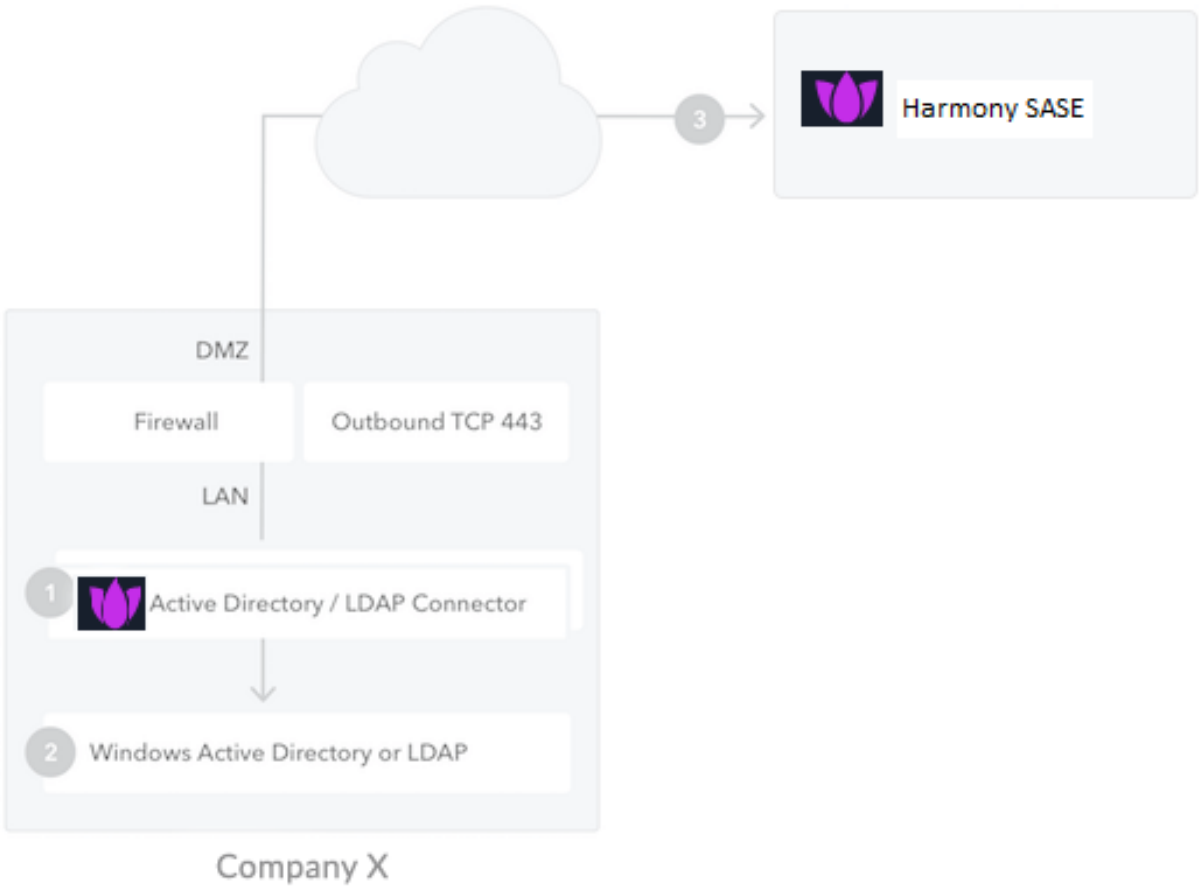


38. Go to the SCIM application.
39. Go to **Overview**.
40. Click **Start provisioning**.



On-Premises Active Directory

You can integrate SASE with Active Directory/LDAP through the Active Directory/LDAP connector installed on your network. The connector serves as a bridge between Active Directory and the SASE service.

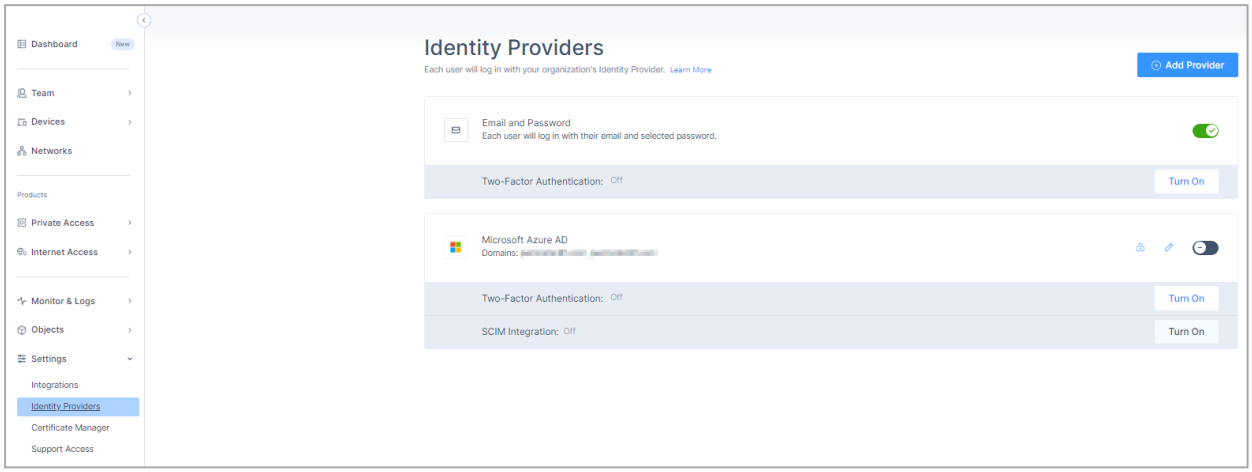


Note - For high availability and load balancing, install multiple connector instances. All connections are outbound to SASE, so firewall changes are generally unnecessary.

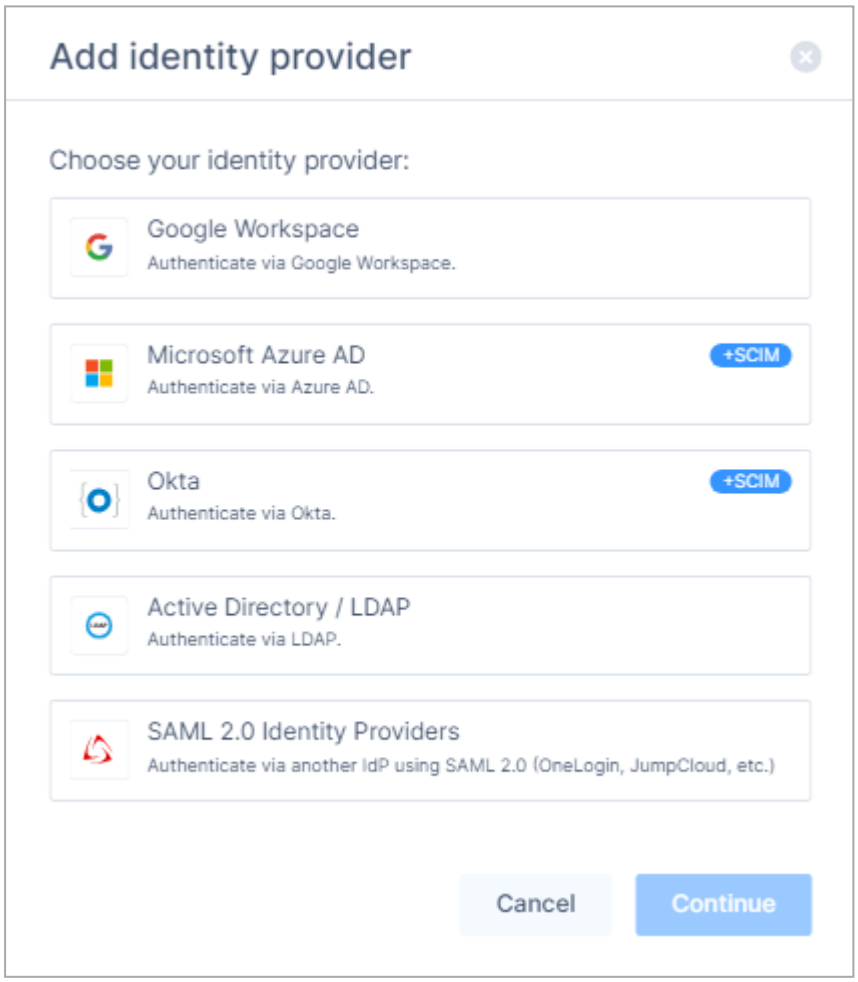
Enabling Active Directory/LDAP Connection

1. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.

   The **Identity Providers** page opens.

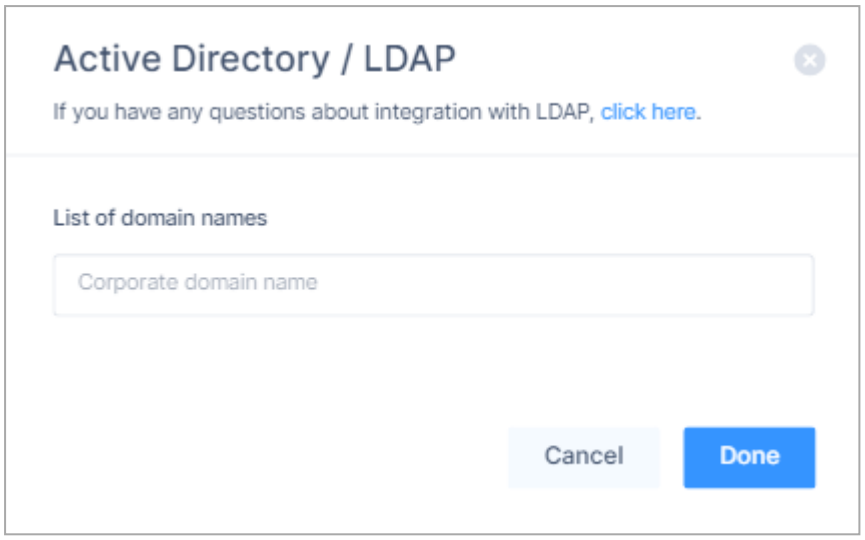


2. Click **Add Provider**.



3. Select **Active Directory / LDAP**.

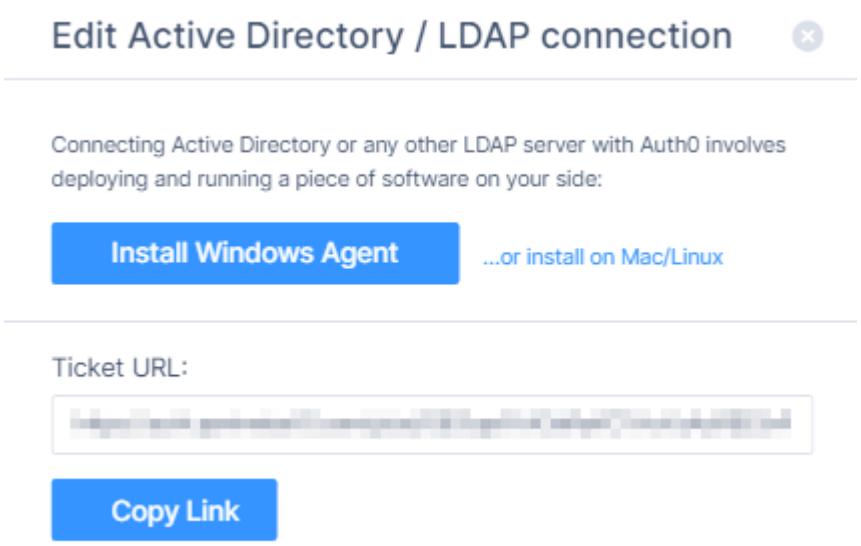
4. Click **Continue**.



5. In the **List of domain names** field, enter the domain name to allow log in to the Active Directory/LDAP connection. For example, `quantumsase.com`.
6. To find your domain name:
   a. Open **Control Panel** on your computer.
   b. Go to **System and Security** > **System** > **Advanced system settings**.

      The **System Properties** window appears.
   c. Go to the **Computer Name** tab to find your domain name.
7. Click **Done**.

   The **Edit Active Directory / LDAP connection** window appears.



8. To copy the **Ticket URL**, click **Copy Link**.

   This Ticket URL is required when you are linking to SASE.

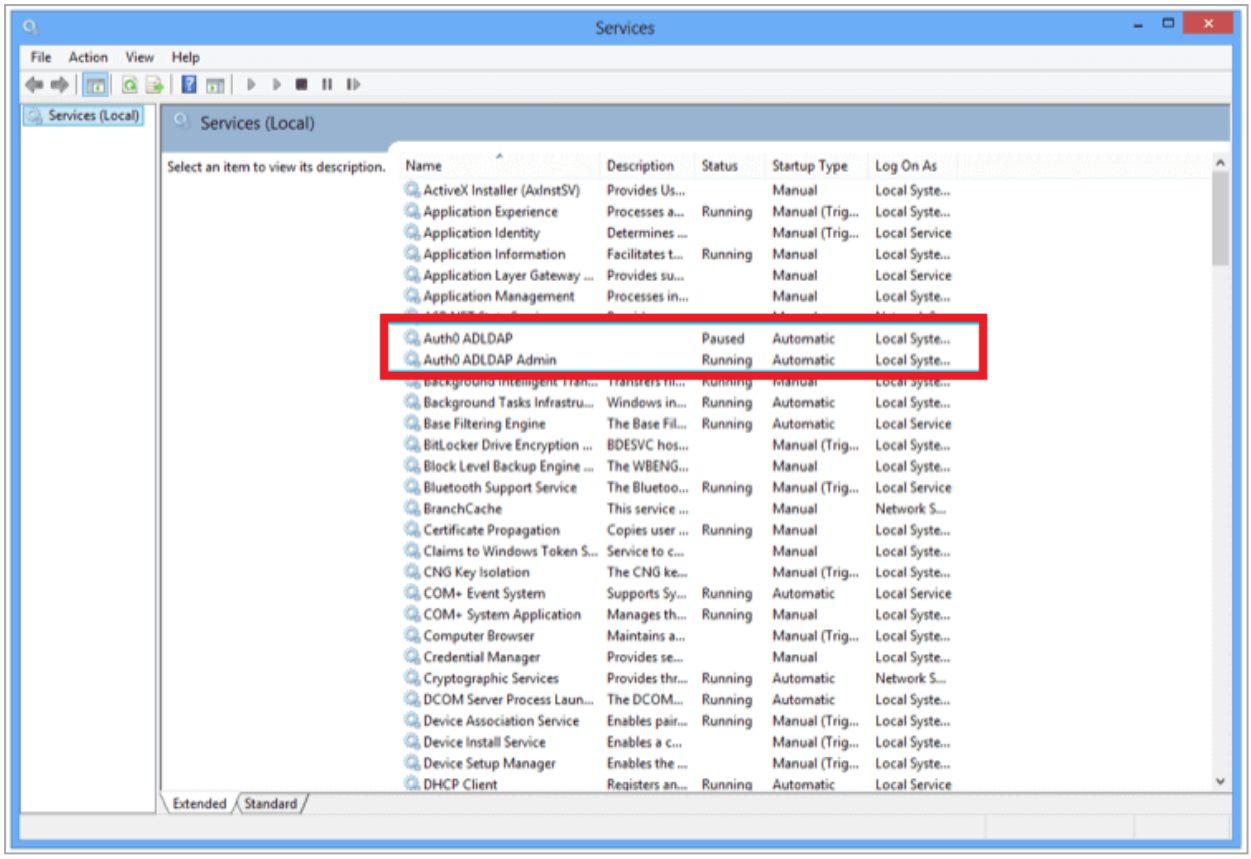
9. Click **Install Windows Agent** and follow the instruction to download the **Auth0 Active Directory/LDAP Connector for Windows** file, see Download the Installer.

   The MSI file downloads.

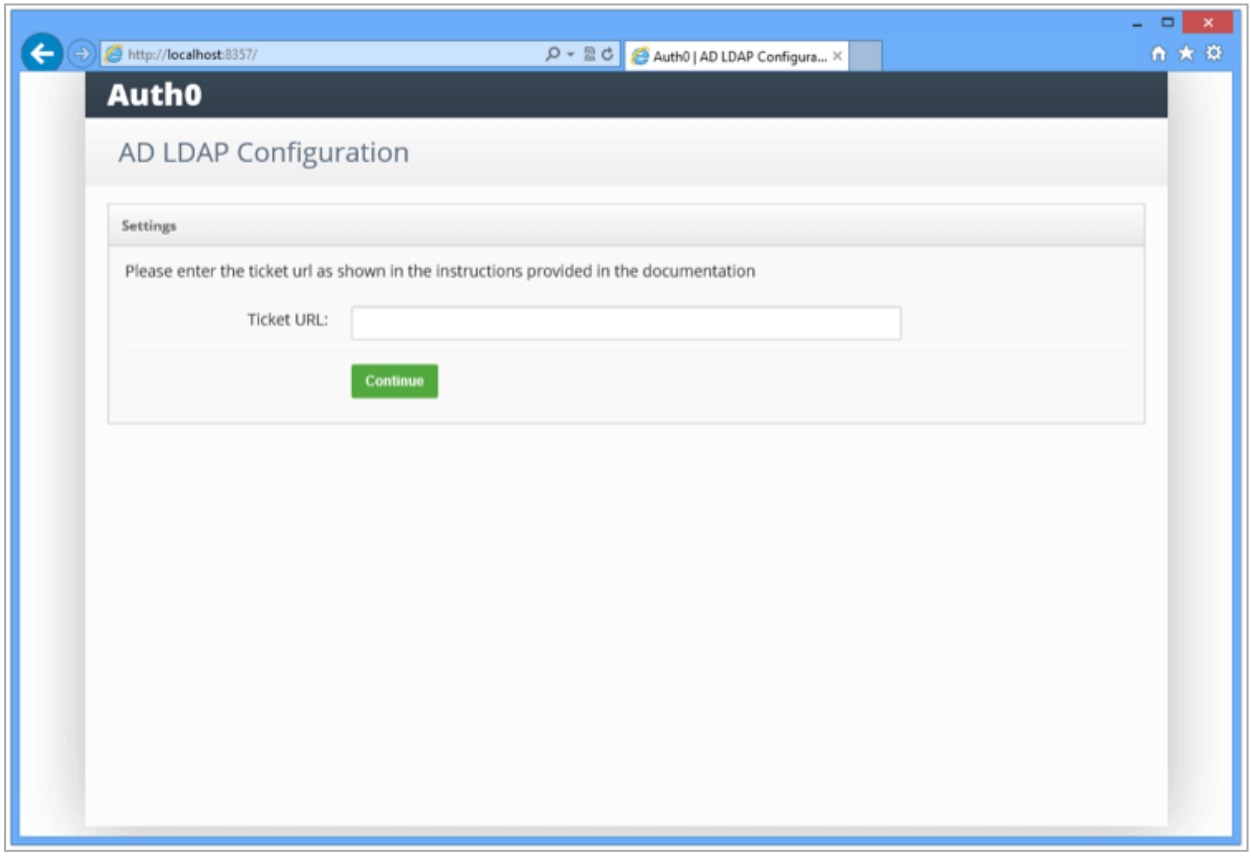
10. Locate the downloaded MSI file, run the installer, and follow the instructions.

Note - The connector can be installed on an existing server, even a Domain Controller. However, more often it is installed on virtual machines provisioned just for the connector.

The AD/LDAP connector is installed as a Windows Service.



The **Auth0** window appears once the installation is complete.

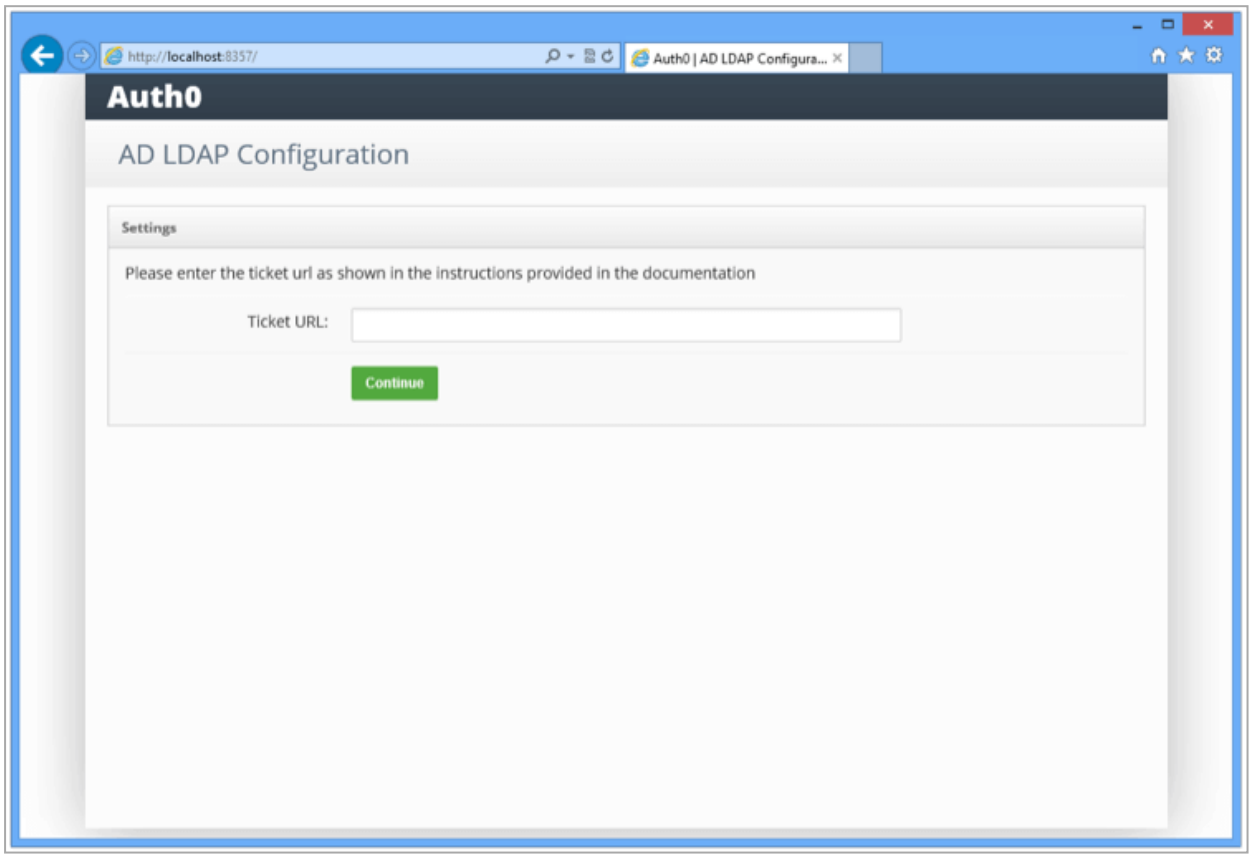


Link to SASE and LDAP

1. To link SASE:

   a. In the **Ticket URL** field, enter the URL. See step 8 in Enabling Active Directory/LDAP Connection.

   b. Click **Continue**.



Note - If you receive an **Unable to get local issuer certificate** error message, set an environment variable `NODE_TLS_REJECT_UNAUTHORIZED` with value `0` in your Windows system, and then restart the two Auth0 services. For more information, see Creating and Modifying Environment Variable in Windows.

2. To link LDAP, enter these:

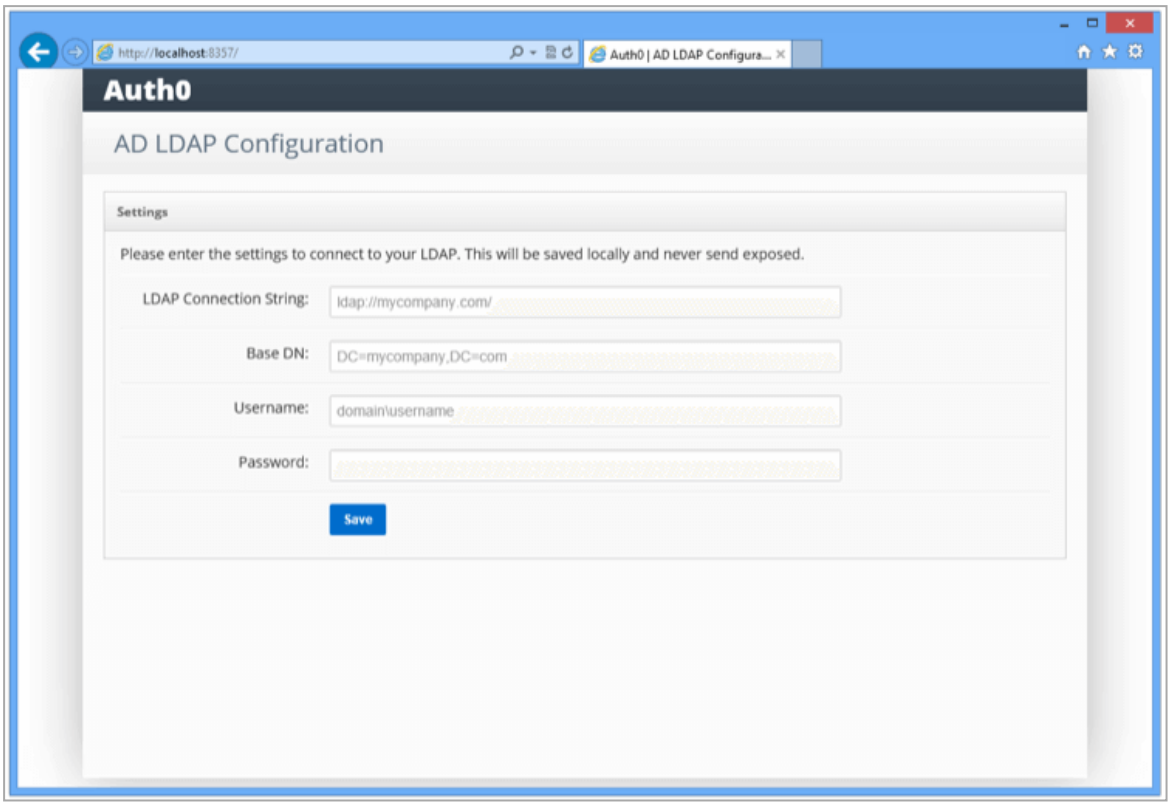
   a. **LDAP Connection String** - Domain name or IP address of your LDAP server. For example, `ldap://<my company>.com/`

      Note - Your LDAP server is the local domain controller where Active Directory is installed. The protocol can be either LDAP or LDAPS. To use LDAPS, make sure that the certificate is valid in the current server.

   b. **Base DN** - Base container for all the queries performed by the connector. For example, `dc=<my company>,dc=com`

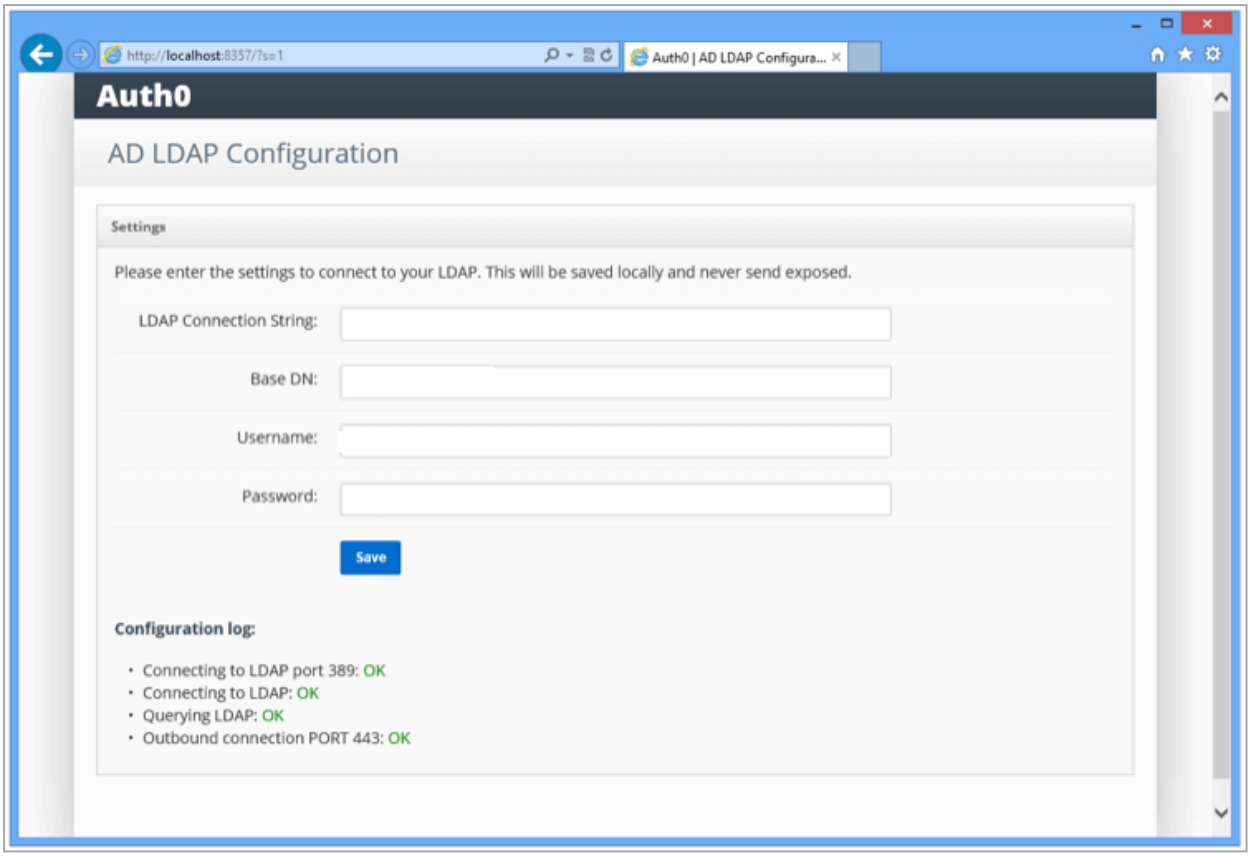
c. **Username** - Full name of the user with administrator rights to perform queries. For example, `cn=<domain name>,dc=<my company>,dc=com`

d. **Password** - Password of the user.



3. Click **Save**.

   The connector performs a series of tests. Make sure all tests result appear as **OK**.

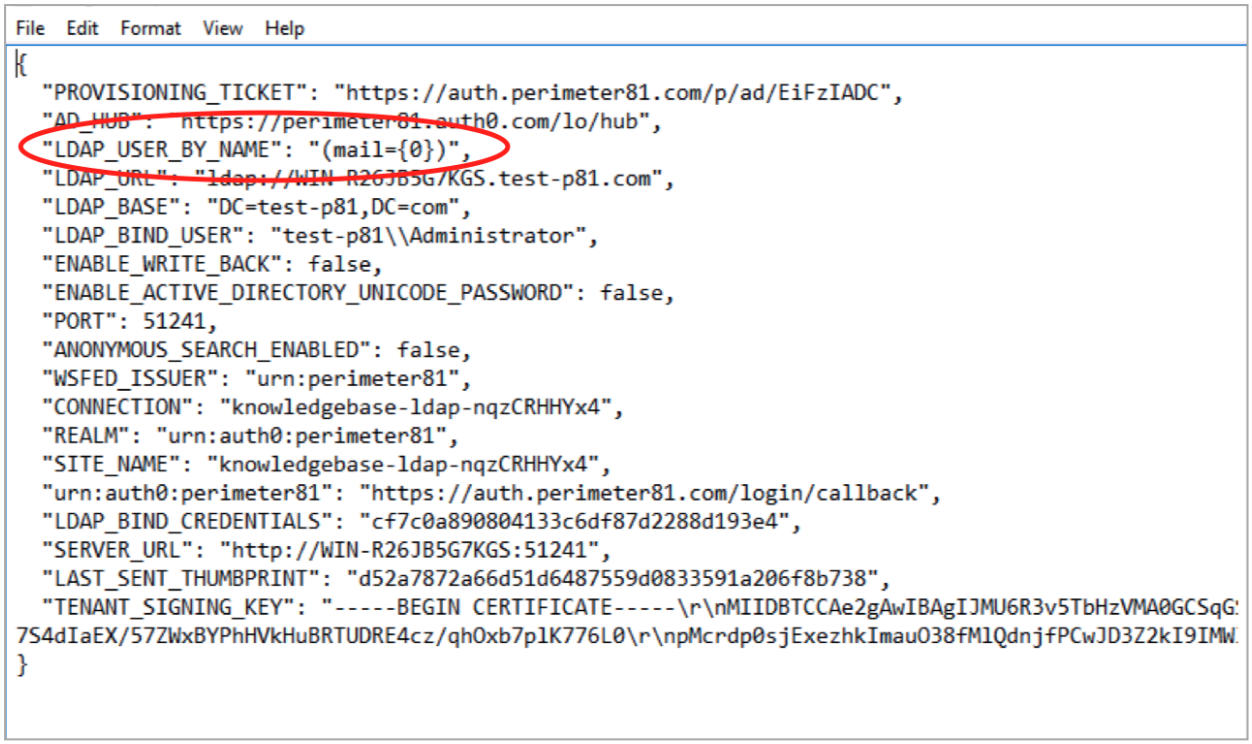


4. Find the AD/LDAP connector's config.json file in this location:

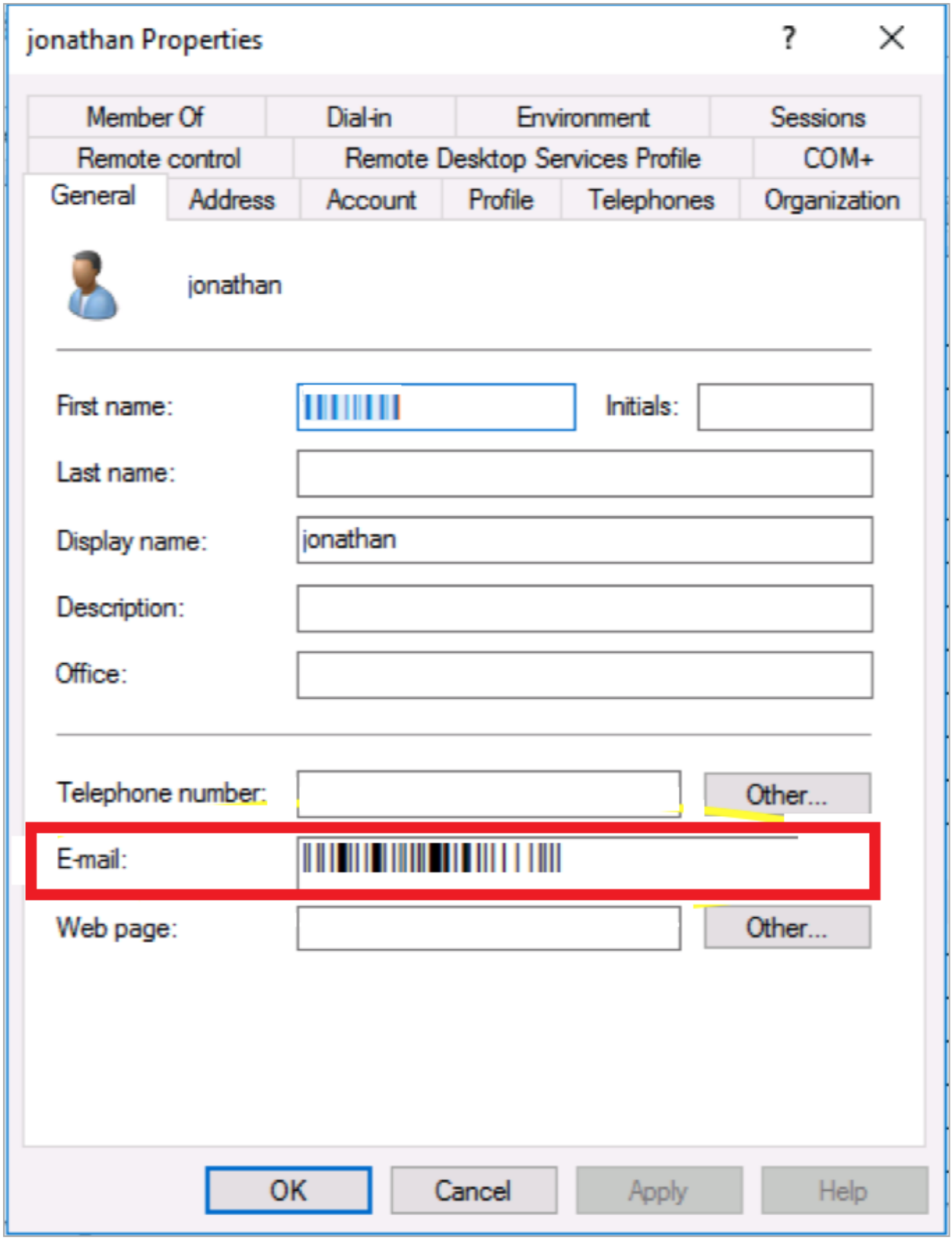
   C:\Program Files (x86)\Auth0\AD LDAP Connector

5. Open the config.json file in a text editor and add this after the second line:

   ```
   "LDAP_USER_BY_NAME": "(mail={0})",
   ```

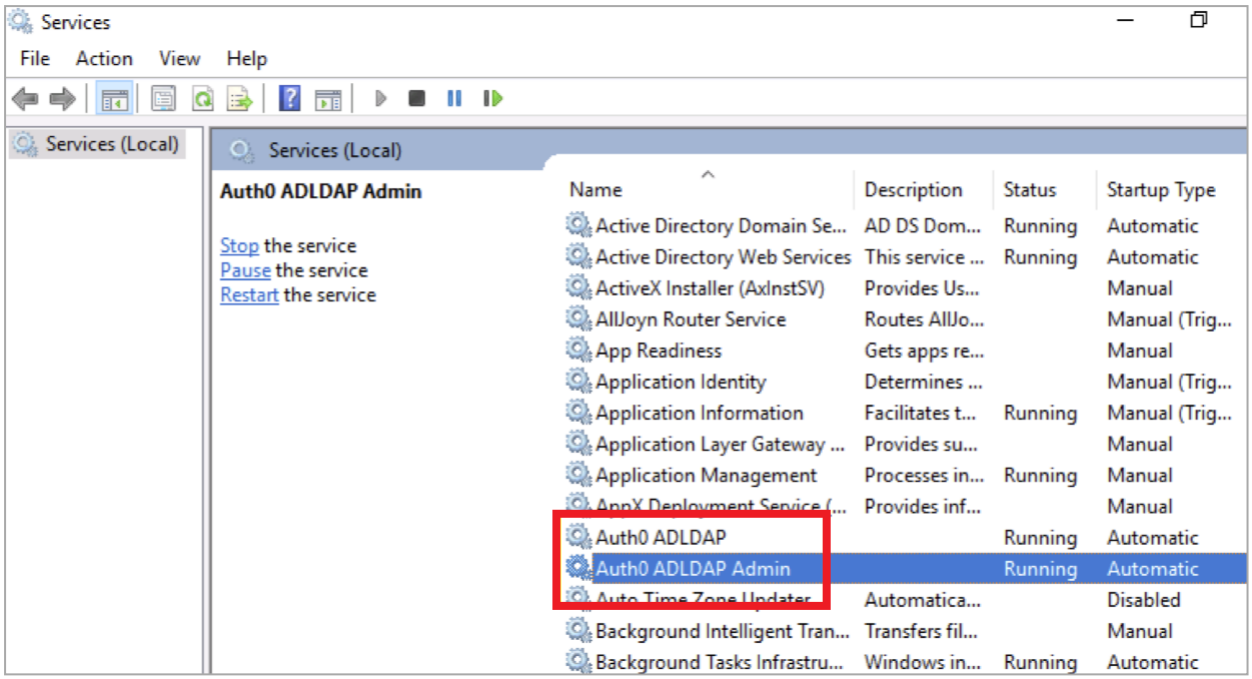


6. Go to **File** and then click **Save** to save the config.json file.
7. Go to **Properties** > **General**.



8. In the **First name** field, enter the user name.
9. In the **E-mail** field, enter the email id of the user.
10. Click **OK**.

11. Restart the AD/LDAP Connector service.



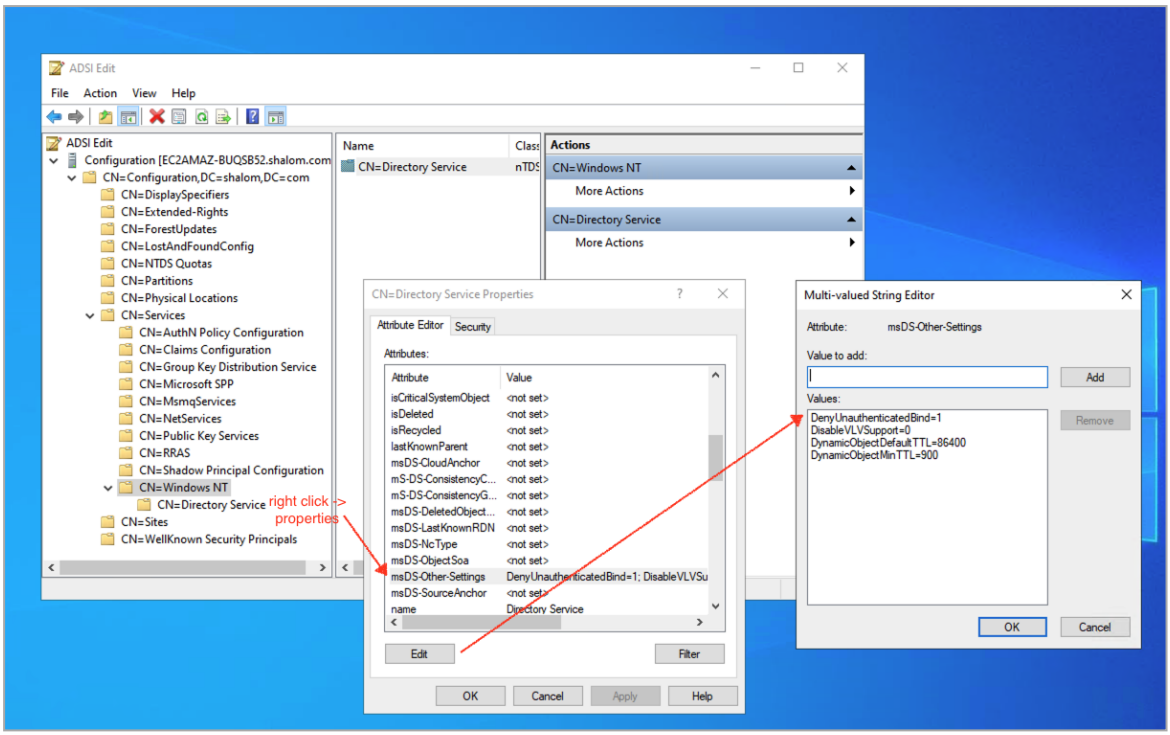
12. To prevent unauthenticated LDAP bind requests (unauthorized access to directory information and protecting sensitive data from potential exploitation):

    a. Open **ADSI Edit** (press `Win + R`, type `adsiedit.msc`, and press **Enter**).

    b. In **ADSI Edit**, right-click on **ADSI Edit** at the top of the left navigation pane and select **Connect to**.

    c. Under **Select a well known Naming Context**, select **Configuration**, and click **OK**.

d. In the left navigation pane, expand **Configuration** > **Services** > **Windows NT**.



e. Right-click **CN=Directory Service** and select **Properties**.

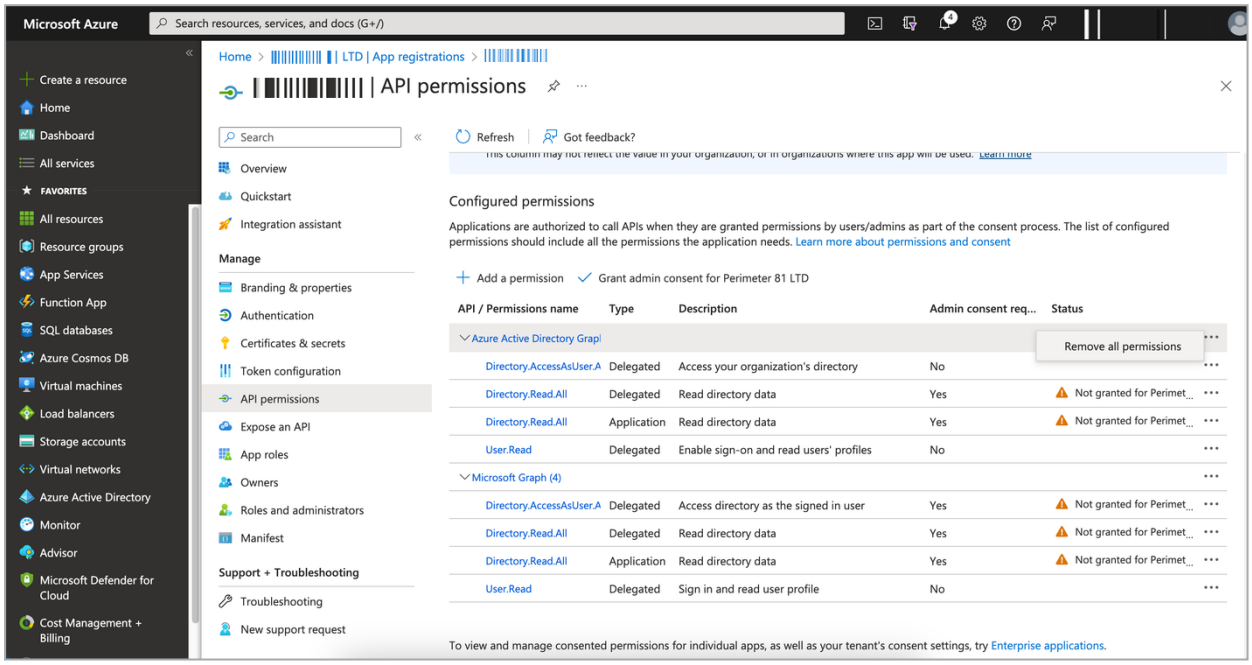
f. In the **Attributes Editor** list, scroll down and locate **msDS-Other-Settings**, and double-click it.

g. In the **Value to add** field, enter **DenyUnauthenticatedBind=1** and click **Add**.

h. Click **OK** to save your changes, then click **Apply** and **OK** to close Properties.

Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions

1. Configure the permissions for the application.
2. In the **Configured permissions** section, for **Azure Active Directory Graph**, scroll to the end of the row and click ⋮.
3. Click **Remove all permissions**.

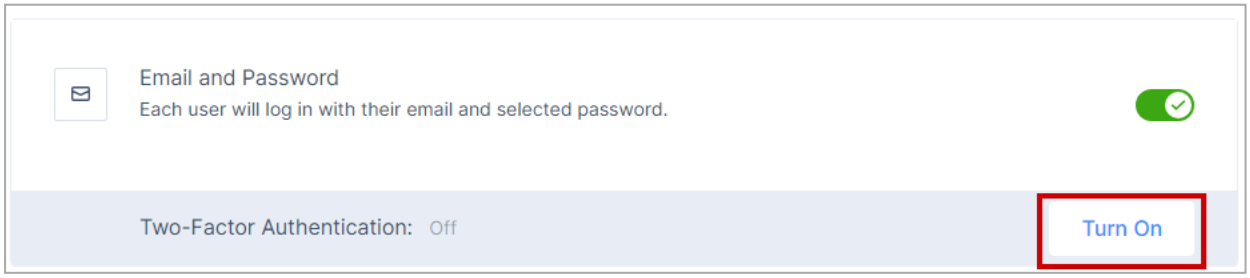


4. Click **Confirm**.

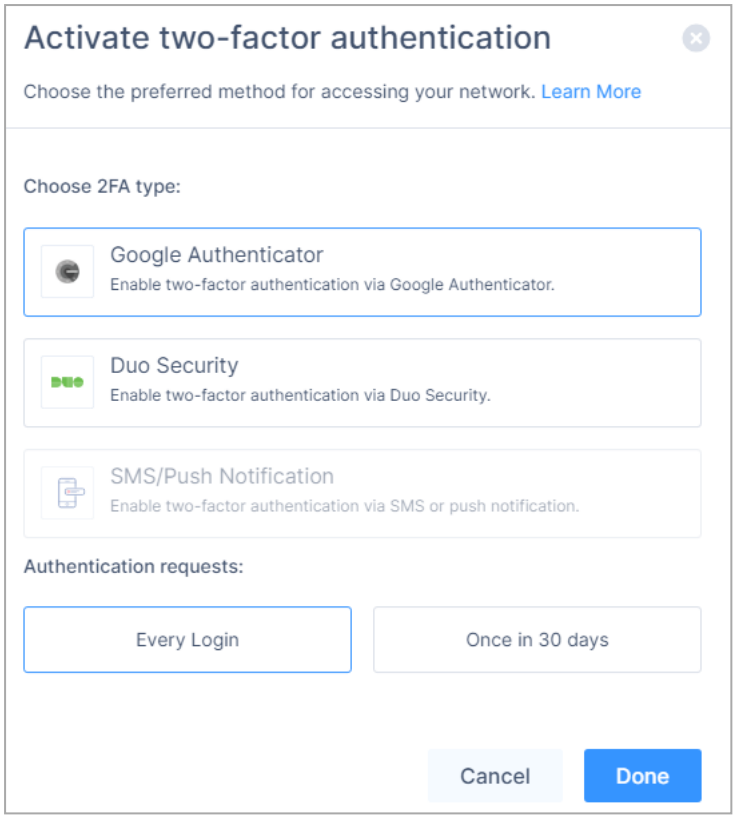
Two-Factor Authentication

Activating Two-Factor Authentication

1. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.
2. For the Identity Provider for which you want to activate 2FA, click **Turn On** for **Two-Factor Authentication**.



3. In the **Choose 2FA type** section, select the authentication type:



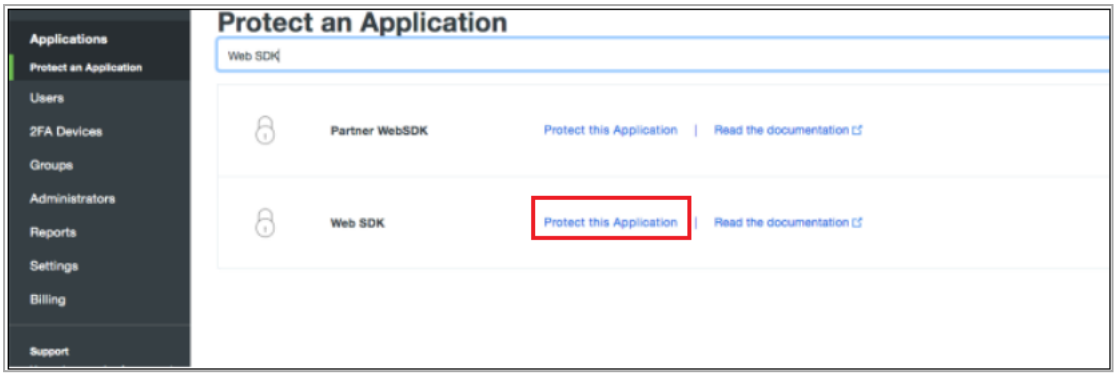
- Google Authenticator
- Duo Security
  - Enter the details in the **Integration key**, **API hostname**, and **Secret key** fields. See *"Configuring Duo Security for Two-Factor Authentication" below*.

4. In the **Authentication requests** section, select the frequency of authentication:
   - Every Login
   - Once in 30 days
5. Click **Done**.

Configuring Duo Security for Two-Factor Authentication

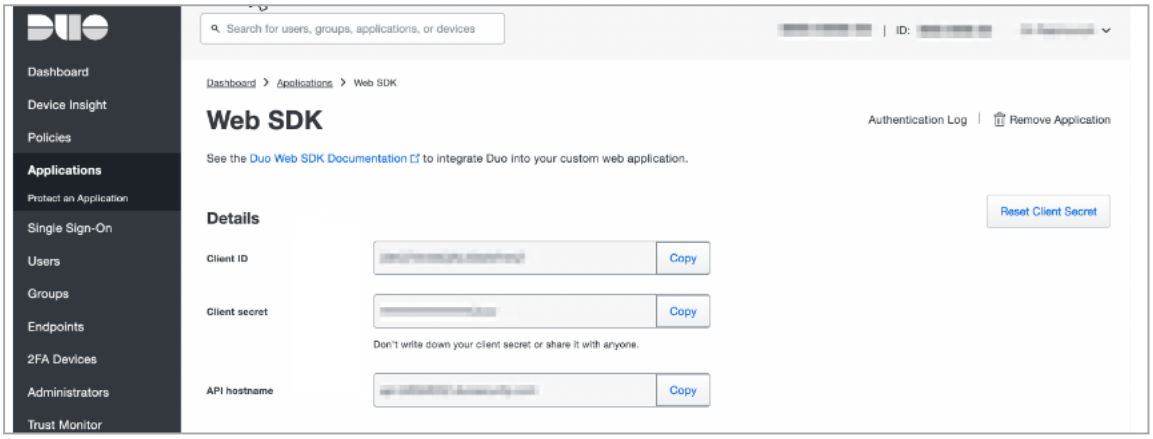
1. Log in to the Duo Security Management Portal.
2. Go to **Applications** and click **Protect an Application**.

3. Search for **Web SDK** and click **Protect this Application** for **Web SDK**.

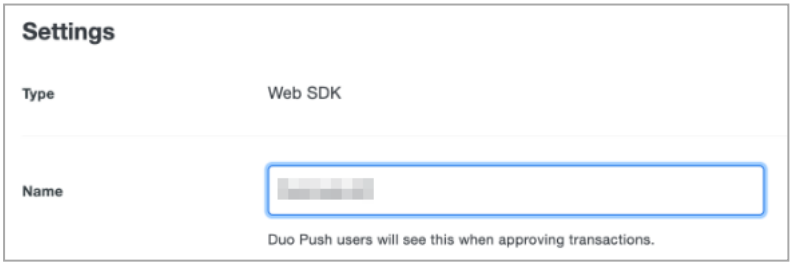


The system creates the application.

4. In the **Details** section, copy the **Client ID**, **Client secret**, and **API hostname**.

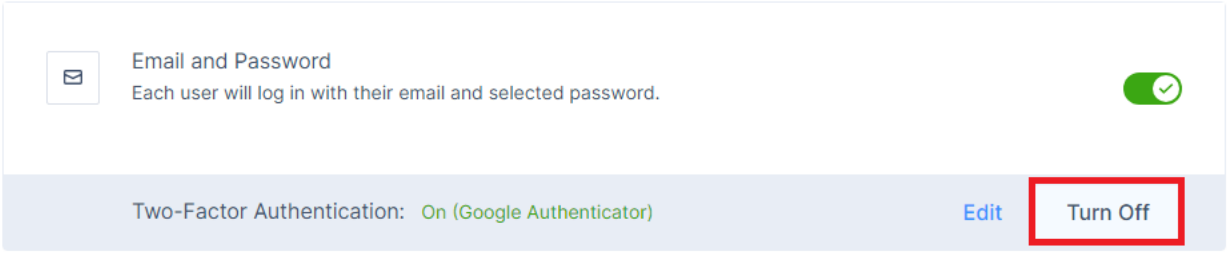


5. (Optional) Scroll down to **Settings** and in the **Name** field, change the name of the application.

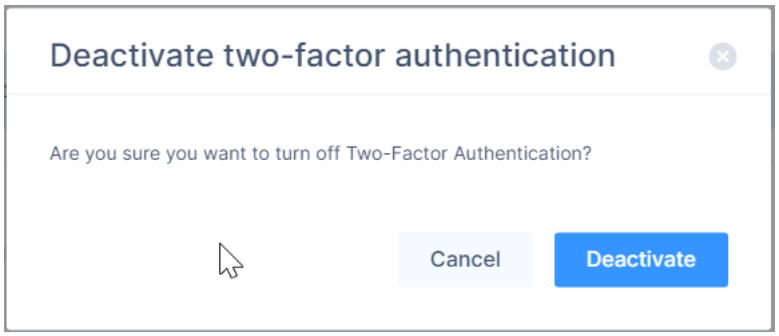


Deactivating Two-Factor Authentication

1. Access the SASE Administrator Portal and click **Settings** > **Identity Providers**.
2. For the Identity Provider for which you want to deactivate 2FA, click **Turn Off** for **Two-Factor Authentication**.



3. Click **Deactivate** in the confirmation pop-up that appears.



Certificate Manager

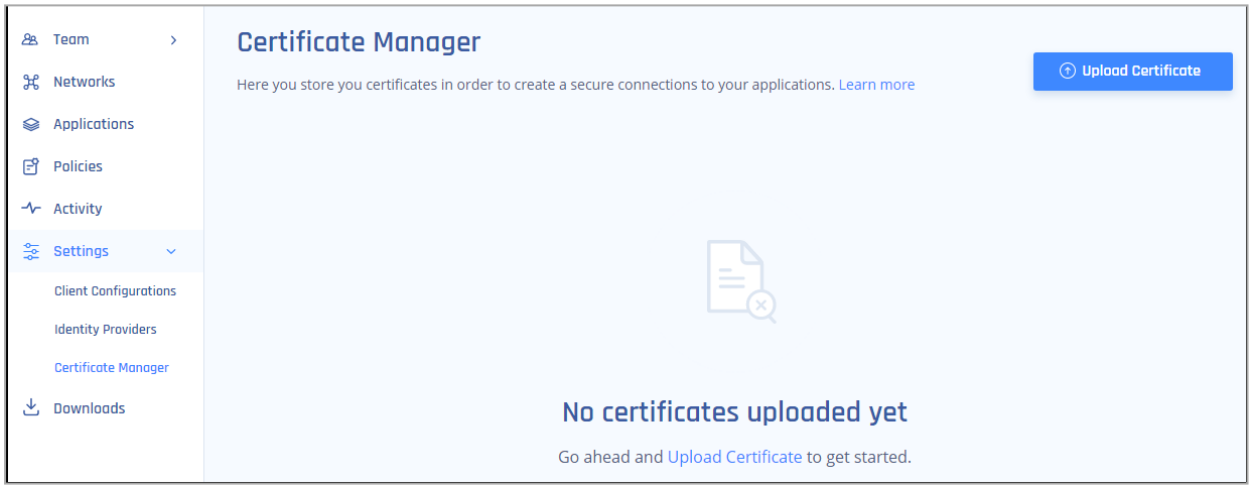
Certificate Manager allows to upload the application domain SSL certificate. This certificate is required to configure URL Alias for members to access the applications.

Note - If compatibility with GnuTLS is required, call openssl x509 on the exported CA certificate.
For more information, see GnuTLS certificate compatibility.

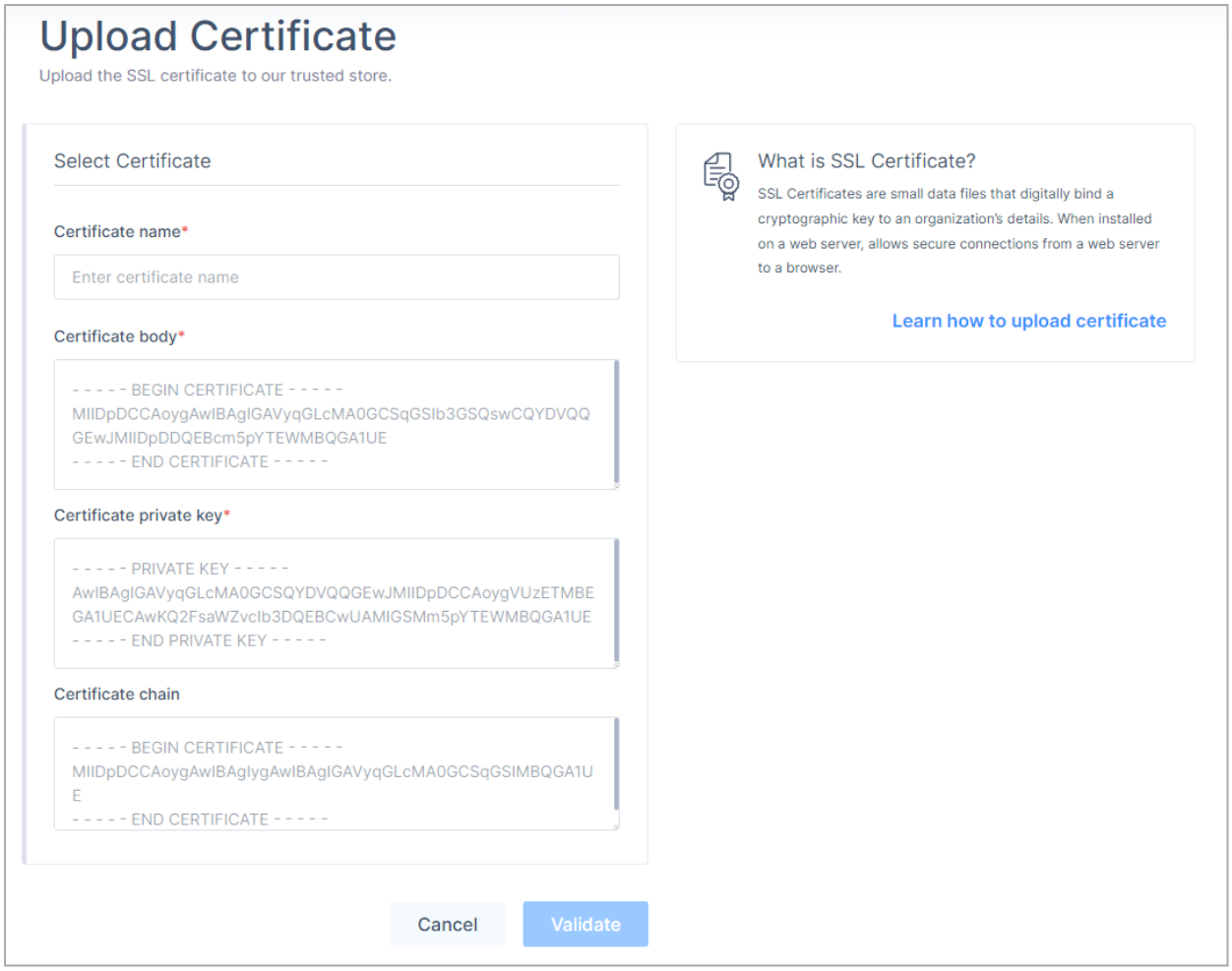
Uploading Domain SSL Certificates

Note - A domain-validated certificate (DV) is an X.509 digital certificate used for Transport Layer Security (TLS). The domain name of the applicant is validated by providing control over a DNS domain.

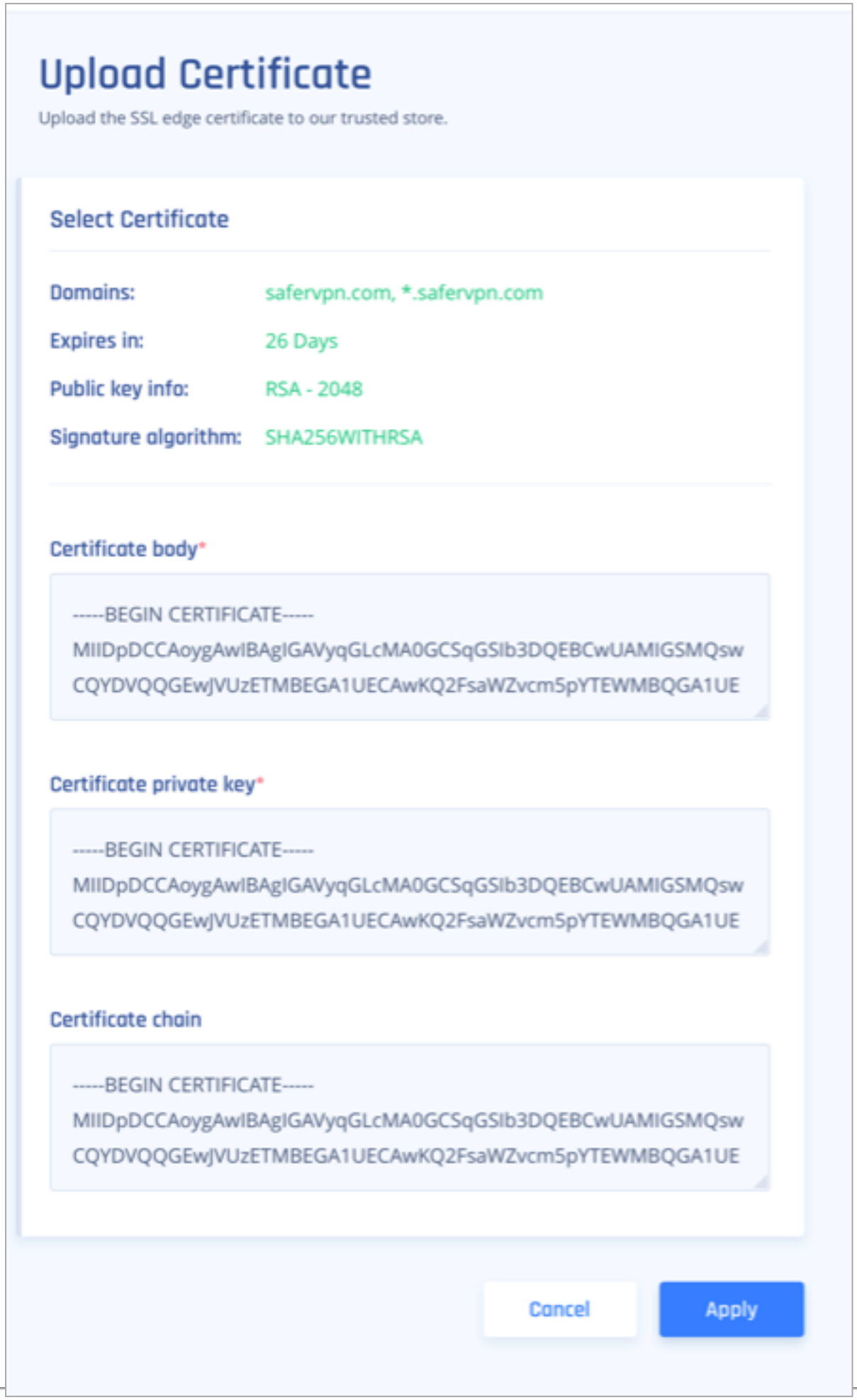
1. Access the Check Point SASE Administrator Portal and click **Settings** > **Certification Manager**.
2. Click **Upload Certificate**.



The **Upload Certificate** window appears.



3. Enter these:
    a. **Certificate name**
    b. **Certificate body**
    c. **Certificate private key**
    d. **Certificate chain**
4. Click **Validate** to ensure this certificate is correct.
5. Click **Apply**.


Upload Certificate
Upload the SSL edge certificate to our trusted store.
Select Certificate
Domains:
safervpn.com, *.safervpn.com
Expires in:
26 Days
Public key info:
RSA - 2048
Signature algorithm:
SHA256WITHRSA
Certificate body*
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Certificate private key*
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Certificate chain
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Cancel
Apply

URL Aliasing for Zero-Trust Applications on SASE

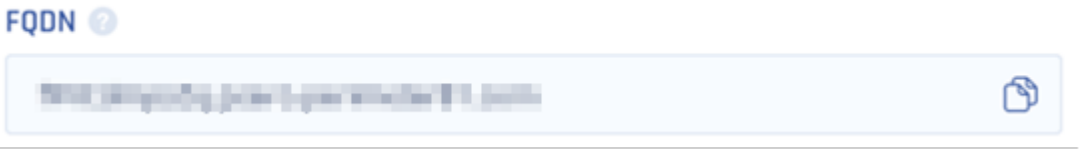
URL aliasing enables Zero-Trust Applications on the SASE platform to utilize a custom URL instead of the default FQDN assigned upon creation. This feature is essential for applications that establish connections from a trusted customer domain rather than the default Check Point Zero-Trust Application domain (pzero.perimeter81.com). It is used to authenticate the accessed resource through the company's domain and help troubleshoot security blocks, such as CORS issues when web servers require connections from a trusted Domain-Validated SSL certificate.

To define a URL Alias, do these:

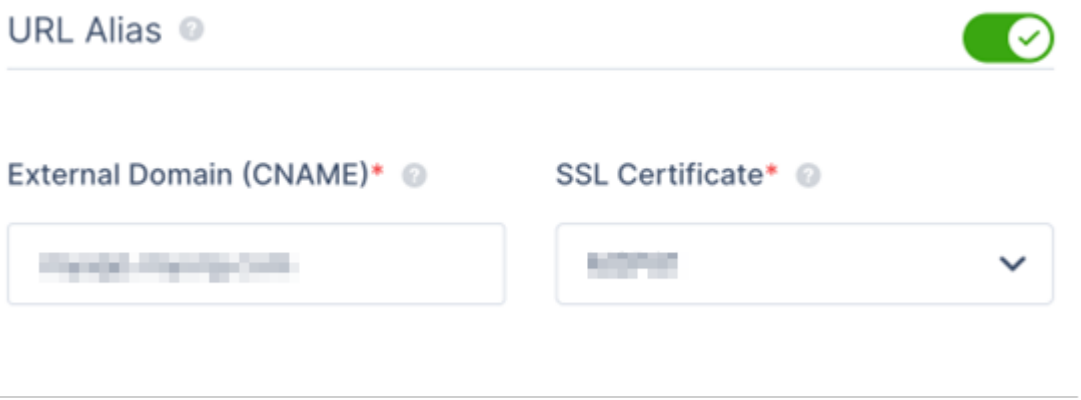
1. Access the SASE Administrator Portal.
2. Go to **Private Access** > **Applications**.
3. Find or set up the application you wish to alias.

   Note - The Zero Trust Application's FQDN is allocated in the SASE Administrator Portal only after you save your application's settings.

4. Once the application setting is saved, in the FQDN field, click to copy the FQDN.

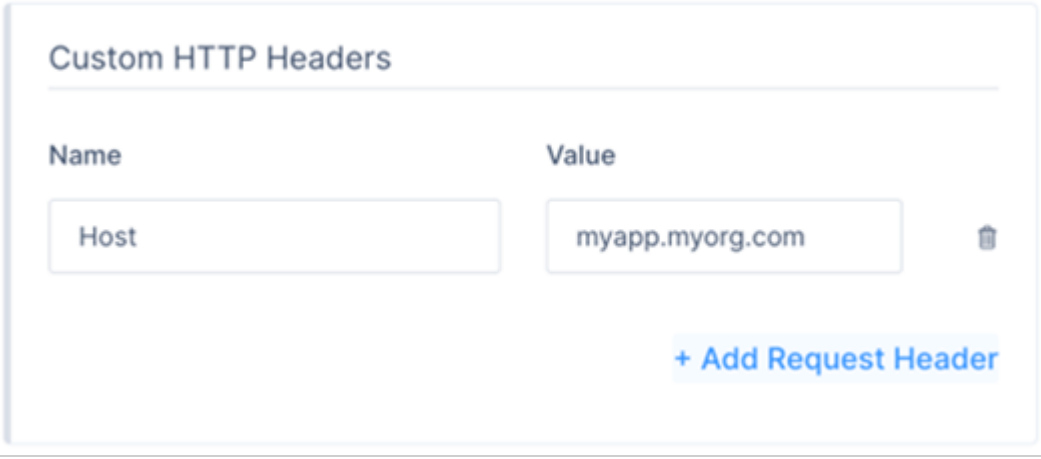


5. Go to your public DNS server (example: GoDaddy or Route53), define a **CNAME** record for a validated domain to point to the copied FQDN.
6. Go back to the SASE Administrator Portal, go to the **URL Alias** section, and turn on the **URL Alias** toggle button.
7. In the **External Domain (CNAME)** field, enter the CNAME associated with your domain.



Note - The value entered in the External Domain (CNAME) field must be resolvable through a public DNS server.

8. From the **SSL Certificate** list, select the certificate.
9. If your security mechanisms require the connection to originate from a specific host for successful webpage:
10. Go to the **Custom HTTP Headers** section.



11. In the **Name** field, enter Host.
12. In the **Value** field, enter the configured CNAME.

Support Access

The **Support Access** page allows you to assign Support Access role to Check Point SASE support engineer. This allows the Check Point SASE support engineer to temporarily access your tenant without credentials for troubleshooting purposes.

You can grant Support Access role to only one member or a group at a time.

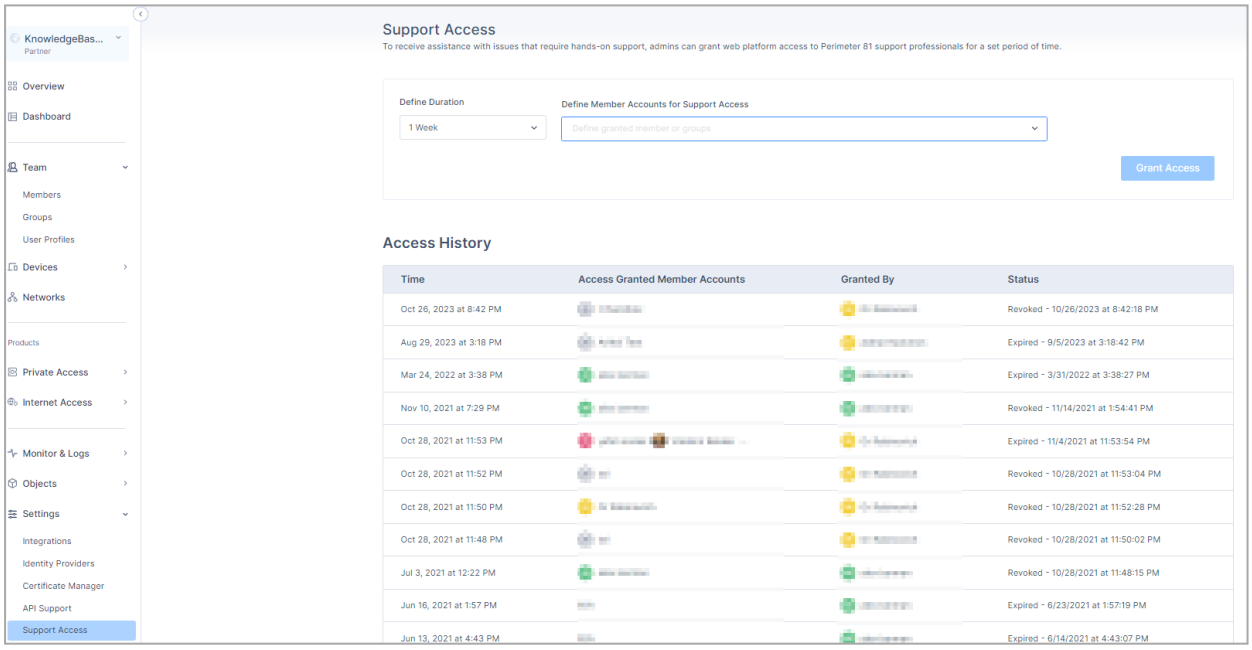
Notes -

- You do not require an additional user license to enable the Support Access role.
- When a Check Point SASE support engineer access your tenant, the system logs it in *"Member Activity" on page 895*.

Granting the Support Access Role

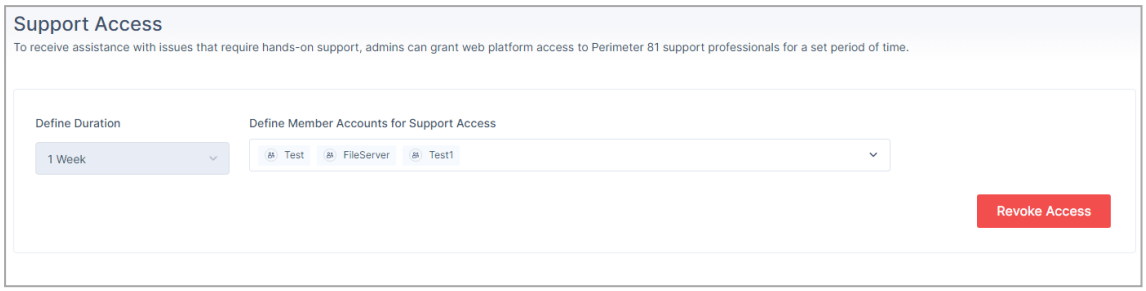
1. Access the Check Point SASE Administrator Portal and click **Settings** > **Support Access**.

   The **Support Access** page appears.



2. From the **Define Duration** list, select the time duration for which Support Access role is valid.
3. From the **Define Member Accounts for Support Access** list, select the member or member groups for the Support Access role.
4. Click **Grant Access**.

5. To revoke the current Support Access role, click **Revoke Access**.



Access History

The **Access History** table shows the history of members and groups with the Support Access role.

Item	Description
Time	Time when the Support Access role was granted, revoked or expired.
Access Granted Member Accounts	Members and member groups assigned with the Support Access role.
Granted By	Owner that granted the Support Access role.
Status	Status of the Support Access role. ■ Active ■ Revoked ■ Expired

Using Model Context Protocol (MCP) Server with SASE

Model Context Protocol (MCP) is an open-source standard that enables AI assistants to securely connect with external data sources and tools. By integrating MCP with Check Point SASE, you can query your infrastructure through natural conversation with AI.

Features

- Query SASE networks and their configurations.
- Retrieve and analyze gateway deployments across regions.
- List and inspect Zero Trust Architecture (ZTA) applications.
- Get all available Network regions.
- Get all the deployed Gateways, regions, and tunnels in the Network.

Supported Actions

MCP server provides to run these actions through your AI assistant:

- Network Management:
  - `list_networks` - Lists all SASE networks.
  - `get_network / find_network` - Fetches details for a specific network by ID.
- Gateway Management:
  - `get_gateway` - Provides gateway details for a specified network and gateway identifier.
- Region Management:
  - `list_network_regions` - Lists all available regions.
  - `get_region` - Retrieves detailed information for a specific region.
- Application Management:
  - `list_applications` - Lists all applications.
  - `get_application` - Retrieves detailed information for a specified application.

- `get_application_status` - Provides the deployment status of a specified application.

Note - Administrators can perform supported actions using free-text queries, not just predefined commands.

Security Guidelines

- API keys and credentials are never shared with the model.
- Only use client implementations you trust.
- Make sure that you only use models and providers that comply with your organization's policies for handling sensitive infrastructure data and Personally Identifiable Information.

SASE MCP Server Configuration

Prerequisites

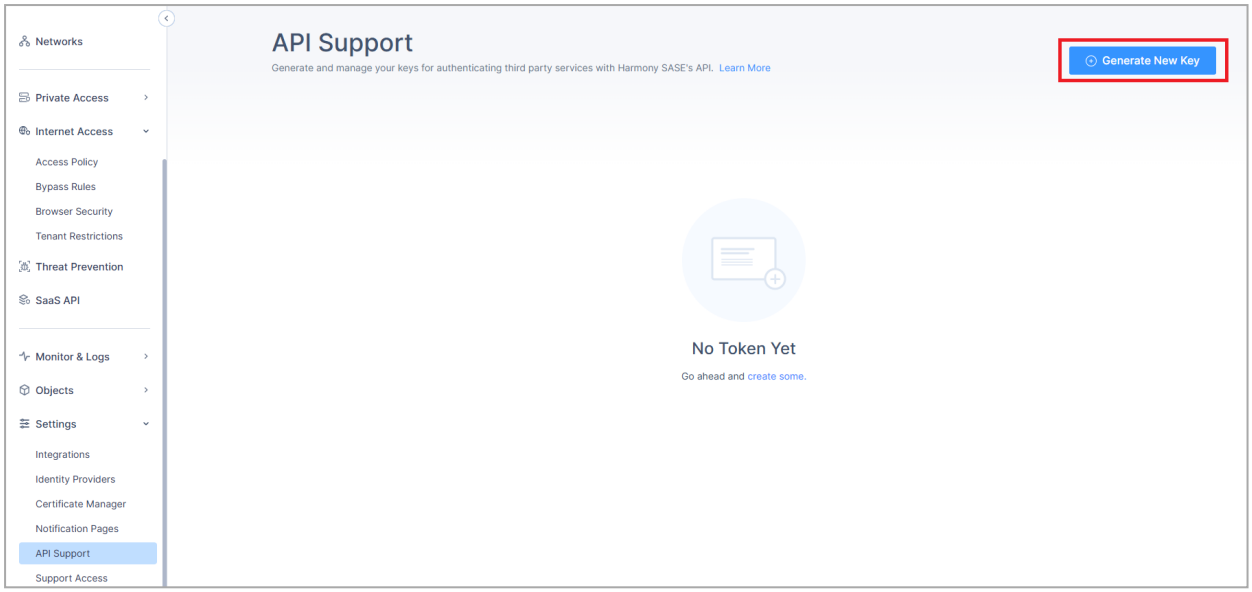
- Administrator access to the SASE Administrator Portal.
- API key generated from the SASE Administrator Portall.
- Node.js version 18 or higher.
- npm version 10 or higher.
- MCP compatible AI client. For example, Claude, Cursor, GitHub Copilot, and Windsurf.

High-Level Procedure

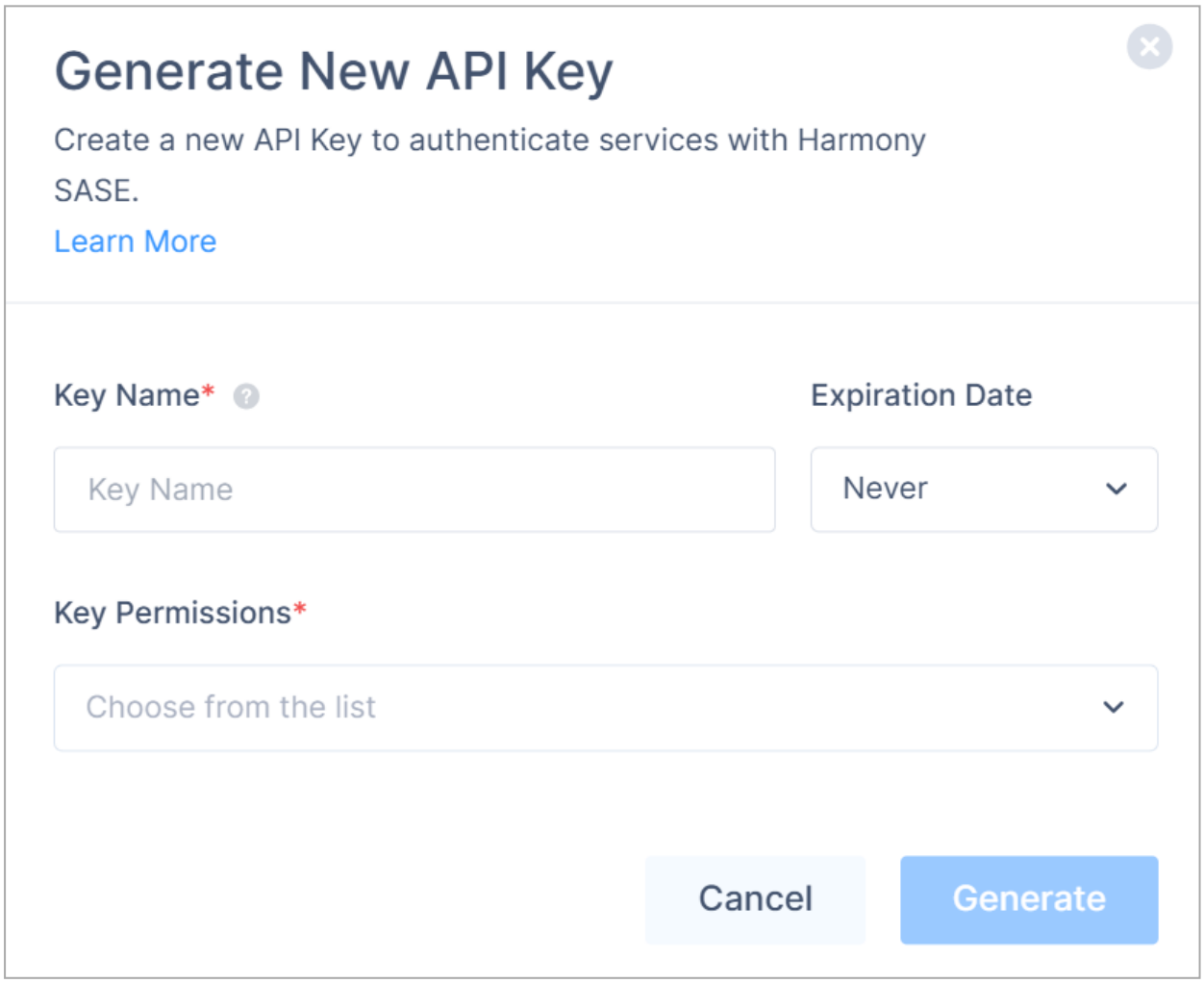
- Step 1 - Generate API Credentials
- Step 2 - Configure Bypass Rule for AI Tool Access
- Step 3 - Configure the AI Client
- Step 4 - Install and Access the SASE MCP Server

Step 1 - Generate API Credentials

1. Access the SASE Administrator Portal.
2. Go to **Settings** > **API Support**.
3. Click **Generate New Key**.



The **Generate New API Key** window appears.

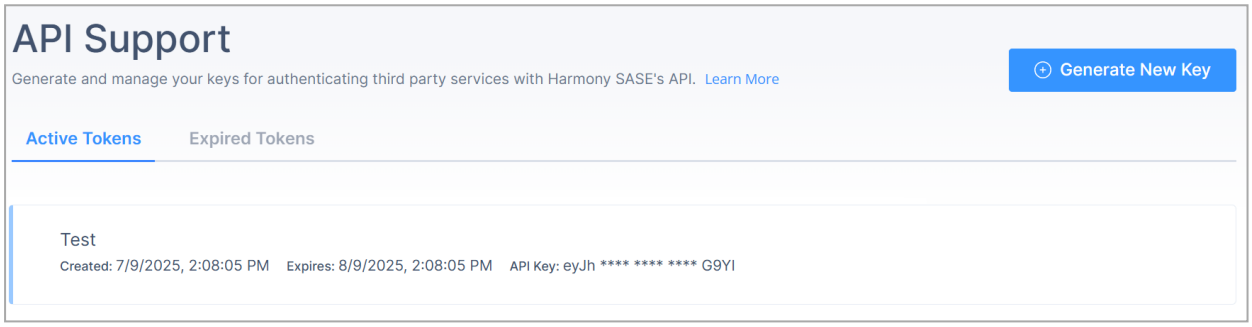


4. In the **Key Name** field, enter a name for the token.
5. From the **Expiration Date** list, select one of these:

- Never (Default)
- 1 Month
- 3 Month
- 6 Month
- 1 Year

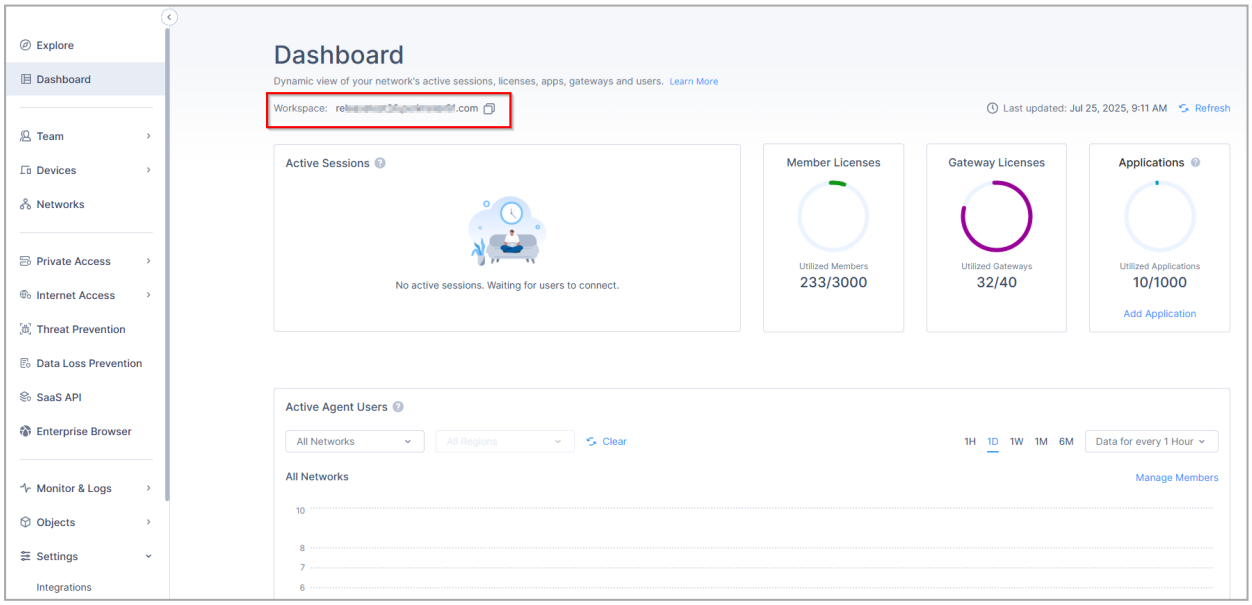
6. From the **Key Permissions** list, select the required permission(s).
7. Click **Generate**.

   The system generates the API Token.



8. To copy the API key, go to the **Active Tokens** tab, hover over the generated token, and click .
9. To copy your Management Host and Origin domain, click **Dashboard**, and in the **Workspace** field, click .

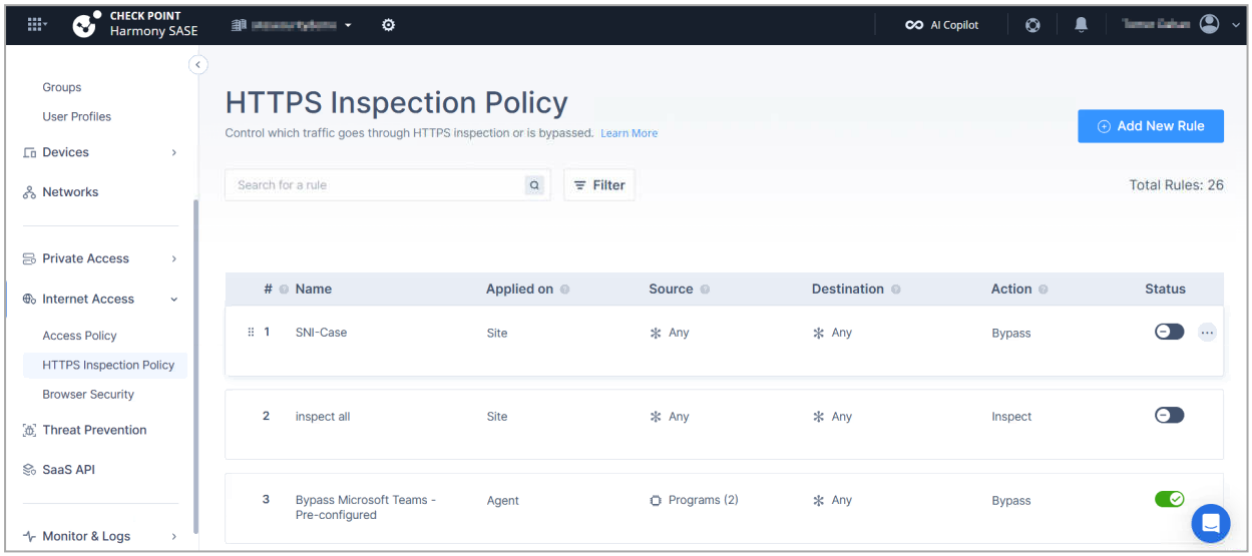
   The workspace name is your Management Host and Origin domain.



Note - Make a note of the API key, Management Host, and Origin domain. These values are required during Client configuration.

Step 2 - Configure Bypass Rule for the AI Client

1. Click **Internet Access** and go to **HTTPS Inspection Policy**.
2. Click **Add New Rule**.



A new rule appears in the table.

3. Specify these:
   a. Name
   b. Source
   c. Destination - For example, enter these:
      i. `*.claude.ai`
      ii. `*.anthropic.com`
      iii. *.api.anthropic.com

      For more information on adding a new rule, see *"Creating a Bypass Rule" on page 790*
4. Turn on the **Status** toggle button.
5. Click **Apply** at the bottom of the page.

6. Click **Apply**.

Step 3 - Configure the AI Client

Supported Client

- Claude Desktop
- GitHub Copilot
- Cursor
- Windsurf
- Any MCP compatible AI Client

Note - Due to the nature of SASE API calls and the variety of server tools, using this server may require a paid subscription to the AI client provider to support token limits and context window sizes.
For smaller models, you can reduce token usage by limiting the number of enabled tools in the client.

Management Host and Origin

Use these values according to your regions:

- For US regions:
  - MANAGEMENT_HOST: `https://api.perimeter81.com/api`
  - ORIGIN: `https://tenant.perimeter81.com`
- For Other Regions:
  - MANAGEMENT_HOST: `https://api.<region>.sase.checkpoint.com/api`
  - ORIGIN: `https://tenant.<region>.sase.checkpoint.com`

Replace, `<region>` with your SASE region (for example: eu, in, au, etc.).

Note - Using incorrect region values will result in authentication or connection failures.

Configuring Claude Desktop

1. For macOS:
   a. Open Terminal.
   b. Run this command to check if the *claude_desktop_config.json* file is available:

```
ls"$HOME/Library/Application Support/Claude/claude_desktop_
config.json"
```

   c. If the file is not available, create the file using this command:

```
touch "$HOME/Library/Application Support/Claude/claude_
desktop_config.json"
```

   d. To open the file in TextEdit, run:

```
open -e "$HOME/Library/Application Support/Claude/claude_
desktop_config.json"
```

   e. Add the below configuration to the JSON file:

```
{
  "mcpServers": {
    "harmony-sase": {
      "command": "npx",

      "args": ["@chkp/harmony-sase-mcp"],

      "env": {
        "API_KEY": "your-harmony-sase-api-key",

        "MANAGEMENT_HOST": "<MANAGEMENT_HOST>",

        "ORIGIN": "<ORIGIN>"
      }
    }
  }
}
```

Replace,

- `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
- `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

2. For Windows:
   a. Press **Win+R**.

      The **Run** window appears.

   b. From the **Open** list, select **cmd**.

   c. To open the configuration file, run:

```
code %APPDATA%\Claude\claude_desktop_config.json
```

   d. Add the below configuration to the JSON file:

```
{
  "mcpServers": {
    "harmony-sase": {
      "command": "npx",

      "args": ["@chkp/harmony-sase-mcp"],

      "env": {
         "API_KEY": "your-harmony-sase-api-key",

        "MANAGEMENT_HOST": "<MANAGEMENT_HOST>",

        "ORIGIN": "<ORIGIN>"
      }
    }
  }
}
```

   Replace,

   - `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
   - `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

Configuring Visual Studio (VS) Code

1. Open Visual Studio (VS) Code.
2. Open the Command Palette (Ctrl+Shift+P).

3. Search for **MCP: Open User Configuration**.
4. Edit the **mcp.json**.
5. Add these configuration:

```
"servers": {
    "harmony_sase": {
        "command": "npx",
        "args": [
            "@chkp/harmony-sase-mcp"
        ],
        "env": {
            "API_KEY": "<API_KEY>",
            "MANAGEMENT_HOST": "<MANAGEMENT_HOST>",
            "ORIGIN": "<ORIGIN>"
        },
        "type": "stdio"
    }
}
```

Replace,

- `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
- `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

6. Save the file and click **Start** to launch the server.

(Optional) To validate the configuration, open your AI assistant (for example, Copilot Chat in Visual Studio Code) and ask: List all SASE networks.

A successful response confirms the MCP server is configured correctly.

Configuring Windsurf

1. Open Windsurf.
2. Go to **Windsurf Settings**.
3. In the search bar, search for **mcp**.
4. Add the below configuration to the JSON file:

```
{
  "mcpServers": {
    "harmony-sase": {
      "command": "npx",

      "args": ["@chkp/harmony-sase-mcp"],

      "env": {
         "API_KEY": "your-harmony-sase-api-key",

        "MANAGEMENT_HOST": "<MANAGEMENT_HOST>",

        "ORIGIN": "<ORIGIN>"
      }
    }
  }
}
```

Replace,

- `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
- `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

Configuring Cursor

1. Open **Cursor**.
2. Go to **Settings** > **Cursor Settings** > **MCP**.
3. Click **Add new MSP server**.
4. Add the below configuration to the JSON file:

```
{
  "mcpServers": {
    "harmony-sase": {
      "command": "npx",

      "args": ["@chkp/harmony-sase-mcp"],

      "env": {
        "API_KEY": "your-harmony-sase-api-key",

        "MANAGEMENT_HOST": "<MANAGEMENT_HOST>",
```

```
        "ORIGIN": "<ORIGIN>"
      }
    }
  }
}
```

Replace,

- `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
- `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

Step 4 - Install and Access the SASE MCP Server

1. Install the MCP Server Tool Globally.
   a. Open Terminal or Command Prompt.
   b. Run:

   ```
   npm install -g @chkp/harmony-sase-mcp
   ```

2. To clone the repository, run:

   ```
   git clone <repository-url>
   cd mcp-servers/packages/harmony-sase
   ```

3. To install dependencies, run:

   ```
   npm install
   ```

4. To build the project, run:

   ```
   npm run build
   ```

5. Run the server locally:

```
node /path/to/packages/harmony-sase/dist/index.js
--api-key YOUR_API_KEY
--management-host <MANAGEMENT_HOST>
--origin <ORIGIN>
```

Replace,

- `your-checkpoint-sase-api-key` with your SASE API Key. See step **8** in Generating API Credentials.
- `<MANAGEMENT_HOST>` and `<ORIGIN>`. See, Management Host and Origin.

Note - You can also run the server locally for development using MCP Inspector or any compatible client.

Managing SASE MSSP Tenants in Check Point Portal

This topic describes how Managed Security Service Provider (MSSPs) onboard and manage customerSASE tenants using the Check Point Portal. In an MSSP environment, administrators manage user access centrally from the Infinity parent tenant and assign permissions to child SASE tenants through User Groups.

This section explains how to:

- Create a SASE-enabled child tenant
- Assign the SASE service and PAYG license
- Grant MSSP parent access
- Manage users and roles

For general Check Point Portal account management and user administration, see Infinity Portal MSSP Administration Guide.

Prerequisites

Before you begin, ensure Check Point Portal Parent account:

- Is configured as an MSSP account
- Is connected to a valid User Center account
- Has Pay-As-You-Go (PAYG) licensing enabled

> **Note** - If you need assistance configuring these prerequisites, contact *Check Point Support*.

Onboarding a SASE Child Tenant

Follow these steps to onboard a new customer tenant with SASE.

Create a Child Tenant

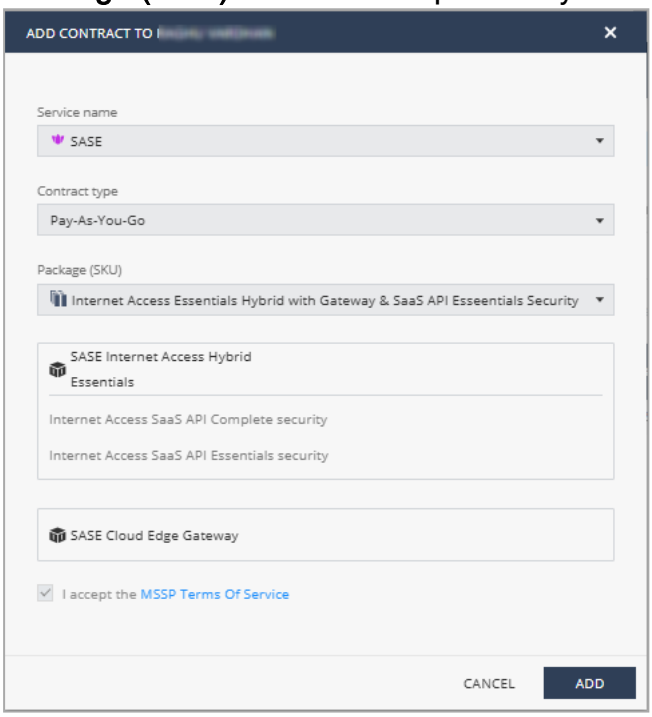
1. Sign in to Check Point Portal.
2. Create a new child tenant under the MSSP parent account.

The user who creates the child tenant becomes the Primary Admin for that tenant.

For information about how to create a child tenant, see Infinity Portal MSSP Administration Guide.

Add the SASE Service to the Child Tenant

1. Access to Check Point Portal, go to **Manage Accounts**.
2. Select the newly created child tenant.
3. Click **Add Contract**.
4. Add the SASE service:
   a. **Service name**: SASE
   b. **Contract type**: Pay-As-You-Go license.
   c. **Package (SKU)**: Select the required Pay-As-You-Go (PAYG) SKU.



The user who adds the SASE service must:

- Have Administrator permissions in the MSSP parent tenant.
- Have User Group Admin access to the child tenant.

Supported PAYG SKUs

- Internet Access
- Private Access
- Gateway

User Management

User management depends on where the user is defined.

For more information about user roles and management, see Infinity Portal MSSP Administration Guide.

MSSP Parent Users

Parent users receive access to child tenants through User Groups.

Users assigned administrative roles through User Groups automatically inherit access to permitted child tenants.

Supported Roles

- Primary Global Admin
- Global Admin
- SASE Admin
- User Manager
- Network Manager
- Security Manager

Notes -

- Each user can have only one SASE role.
- If a user belongs to multiple User Groups, ensure the groups do not assign conflicting SASE roles.

Not Supported

- Global Read-Only
- SASE Read-Only
- Multiple roles per user
- Custom roles
- Global User Admin role mapping to SASE roles

  Note - The Global User Admin (Infinity user manager role) does not map to any SASE role.

Grant Additional MSSP Parent Users Access to the Child Tenant

To grant additional MSSP parent users access to the child tenant:

1. In the MSSP parent tenant, open User Groups.
2. Edit or create a User Group.
3. Grant access to the required child tenant.
4. Assign the appropriate SASE role.

User Groups control how access is inherited from the parent tenant to child SASE tenants.

Note - The Read-Only roles, whether assigned through Global or service-specific roles, is not supported for SASE.

Child Tenant SASE Members

You can add members directly to the child tenant:

- Manually
- Through an integrated Identity Provider (IdP)

When a member signs in to SASE for the first time, the system adds the user as a SASE member and includes the user in license consumption.

Usage and Billing

Billing is based on usage reported by each child tenant.

- Usage data is reported daily.
- Reports reflect the previous day's usage.

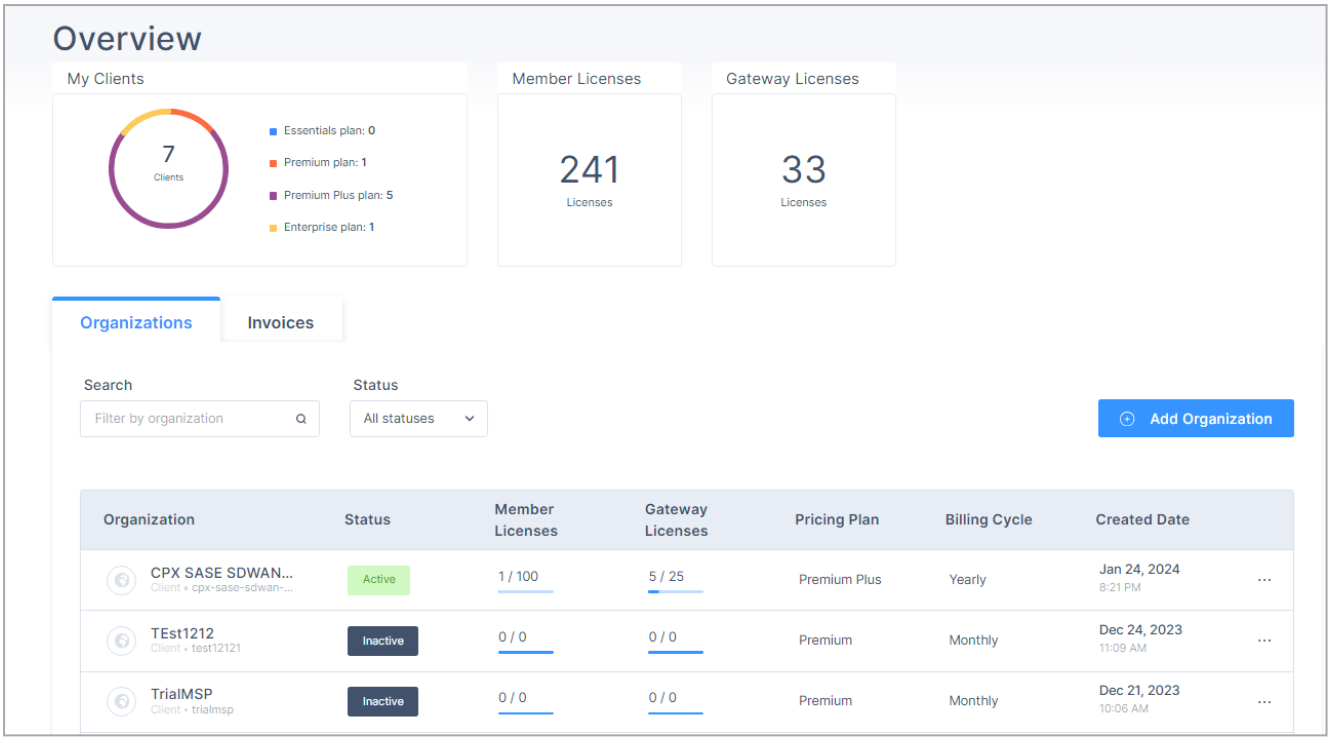
Overview

Note - This page is available only for the MSSP accounts in the Perimeter 81 workspace.

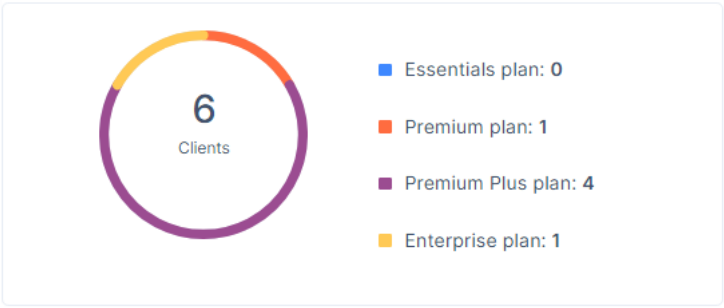
The **Overview** page allows you to view:

- *"My Clients" on the next page*
- *"Member Licenses" on the next page*
- *"Gateway Licenses" on page 1157*
- *"Organizations" on page 1157*
- *"Invoices" on page 1161*

To view the **Overview** page, access the **Check Point SASE** (Perimeter 81) Administrator Portal and click **Overview**.



My Clients



My Clients widget shows the number of clients and their subscription plans.

Member Licenses

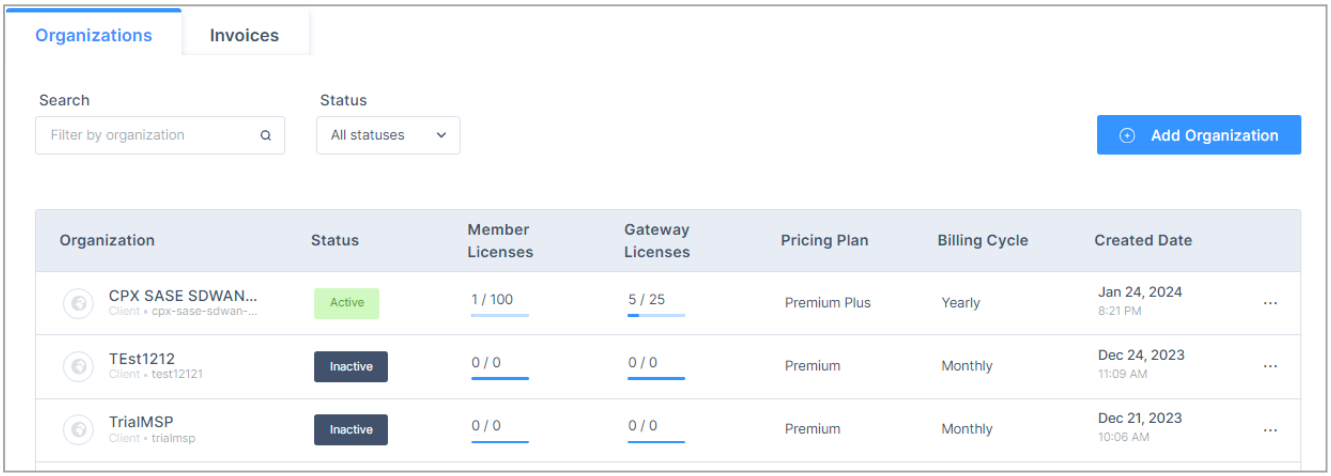
The **Member Licenses** widget shows the total number of purchased member licenses.

Gateway Licenses

The **Gateway Licenses** widget shows the total number of purchased gateway licenses.

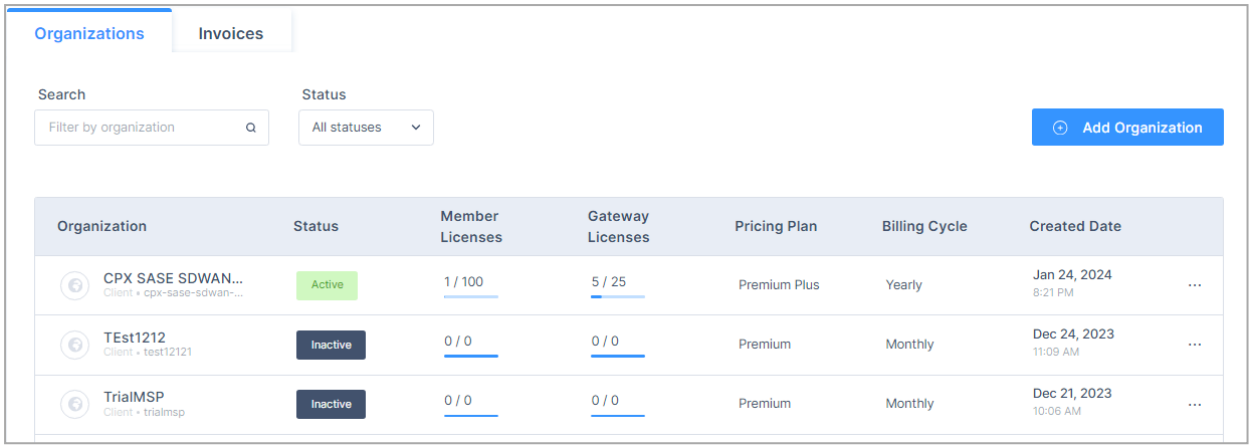
Organizations

The **Organizations** tab allows you to view and manage billing for the organizations.

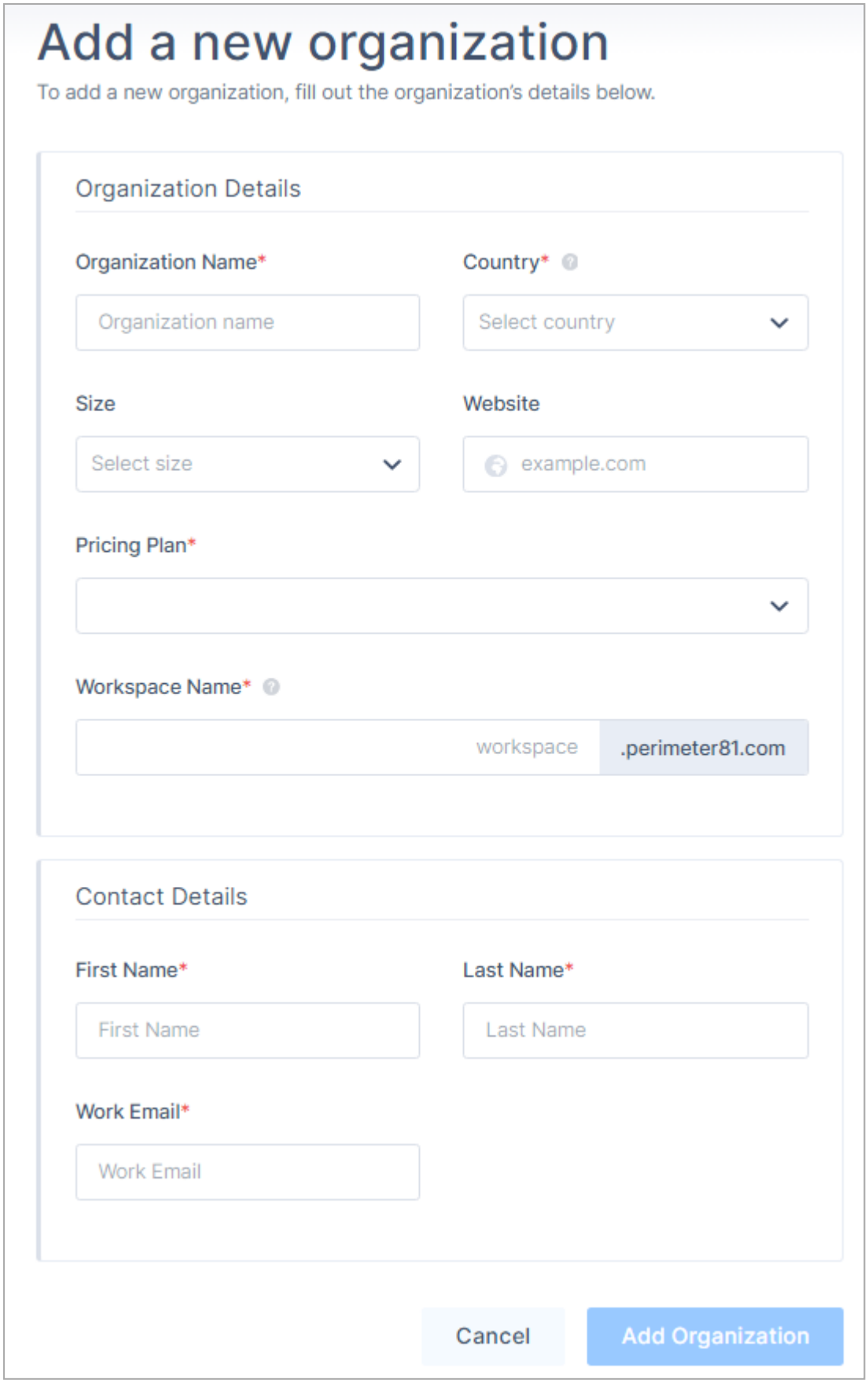


Adding an Organization

1. Access the **Check Point SASE** (Perimeter 81) Administrator Portal and go to **Overview** and then click the **Organizations** tab.
2. Click **Add Organization**.



The **Add a new organization** window appears.



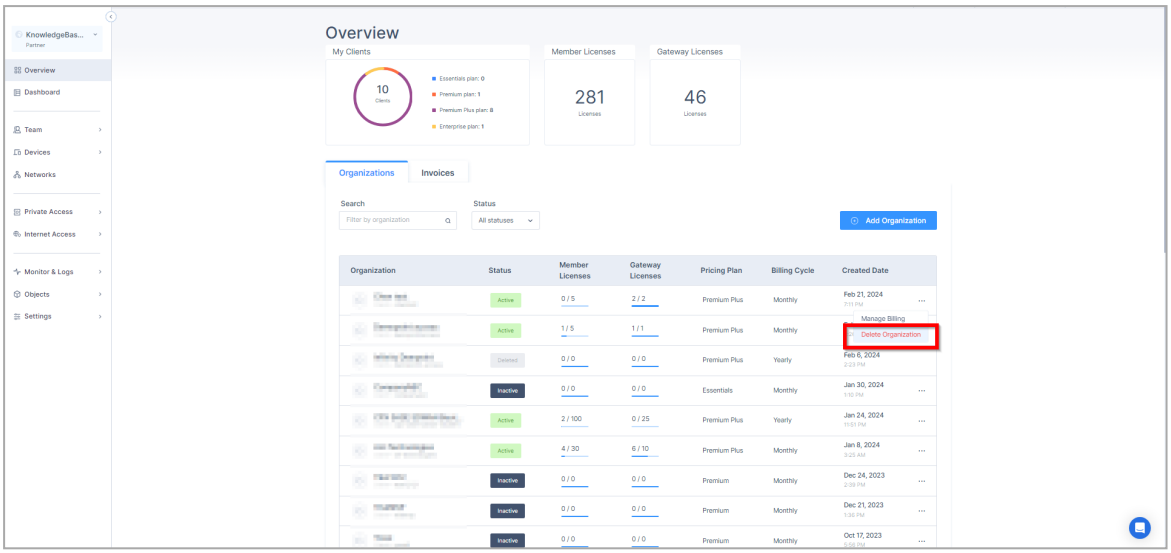
3. In the **Organization Details** section, specify these:

- **Organization Name**
- **Country**
- **Size**
- **Website** - Your organization's website address.
- **Pricing Plan**
- **Workspace Name**.

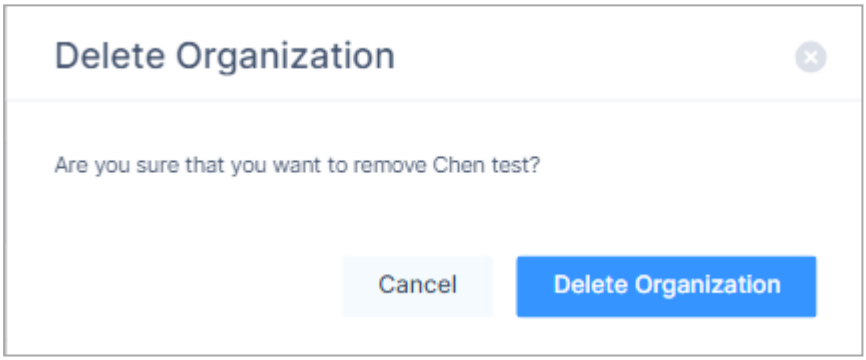
Note - You cannot change the workspace name after you create it.

4. In the **Contact Details** section, enter these:
   - **First Name**
   - **Last Name**
   - **Work Email**
5. Click **Add Organization**.
6. To delete an organization, scroll to the end of the row and click ··· .

a. Select **Delete Organization**.



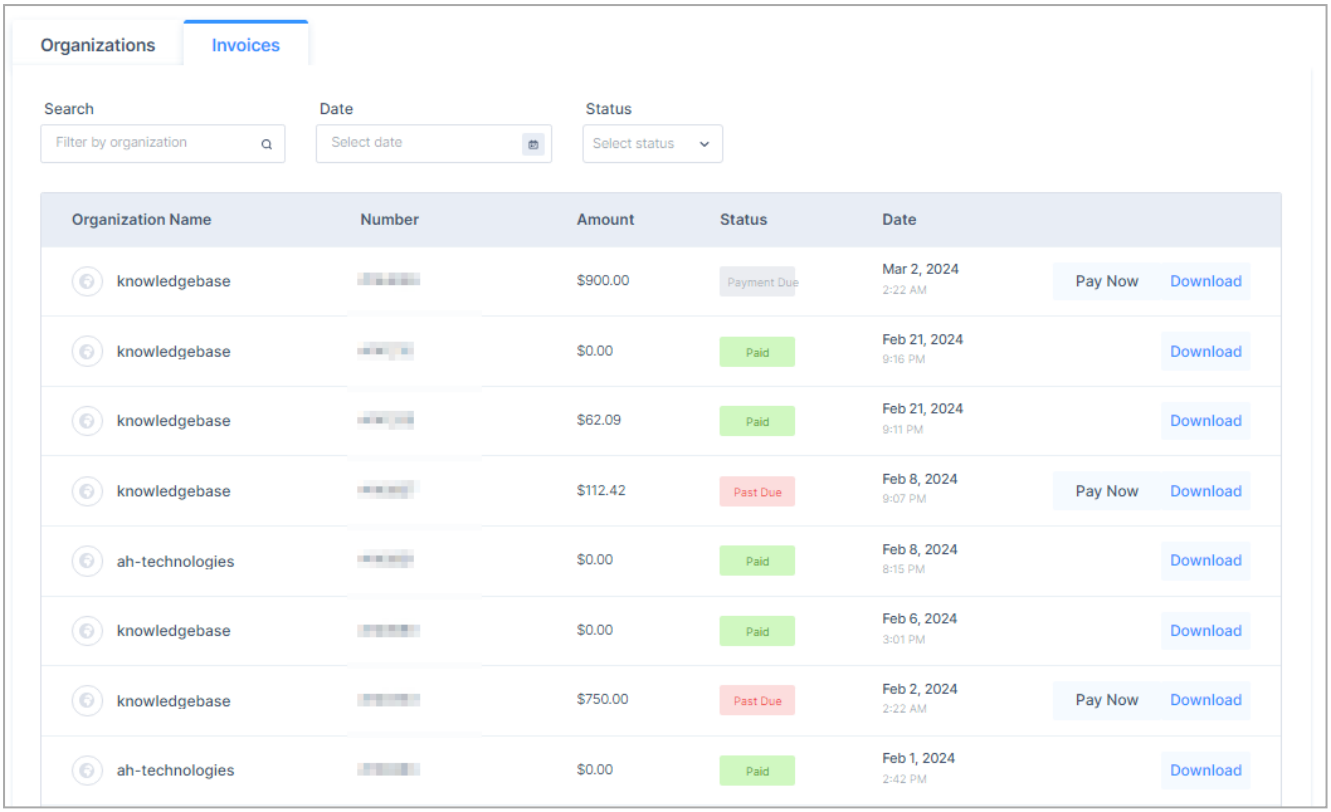
The **Delete Organization** window appears.



b. Click **Delete Organization**.

Invoices

The **Invoices** tab allows you to view, pay and download the invoices.

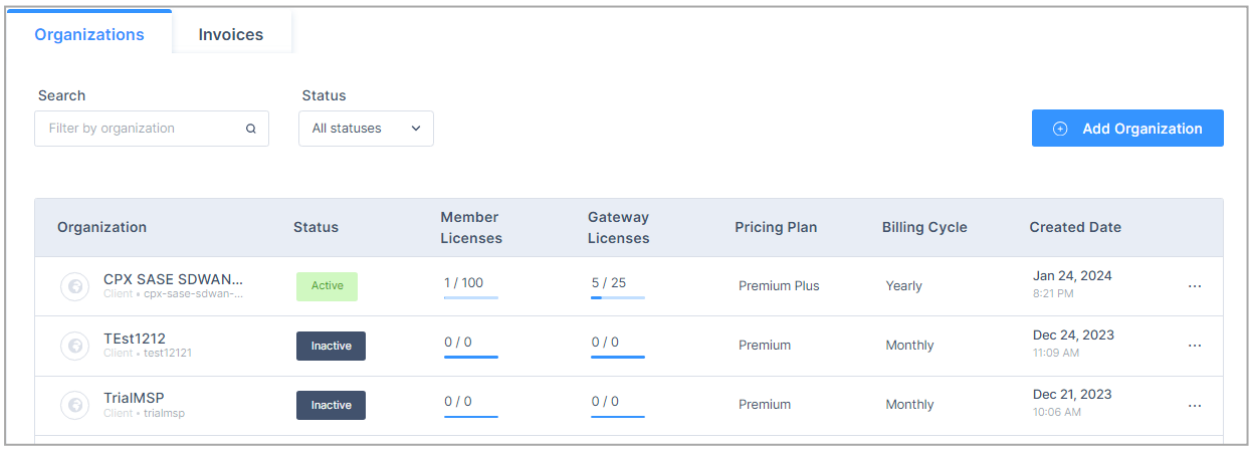


To pay an invoice, click **Pay Now**.

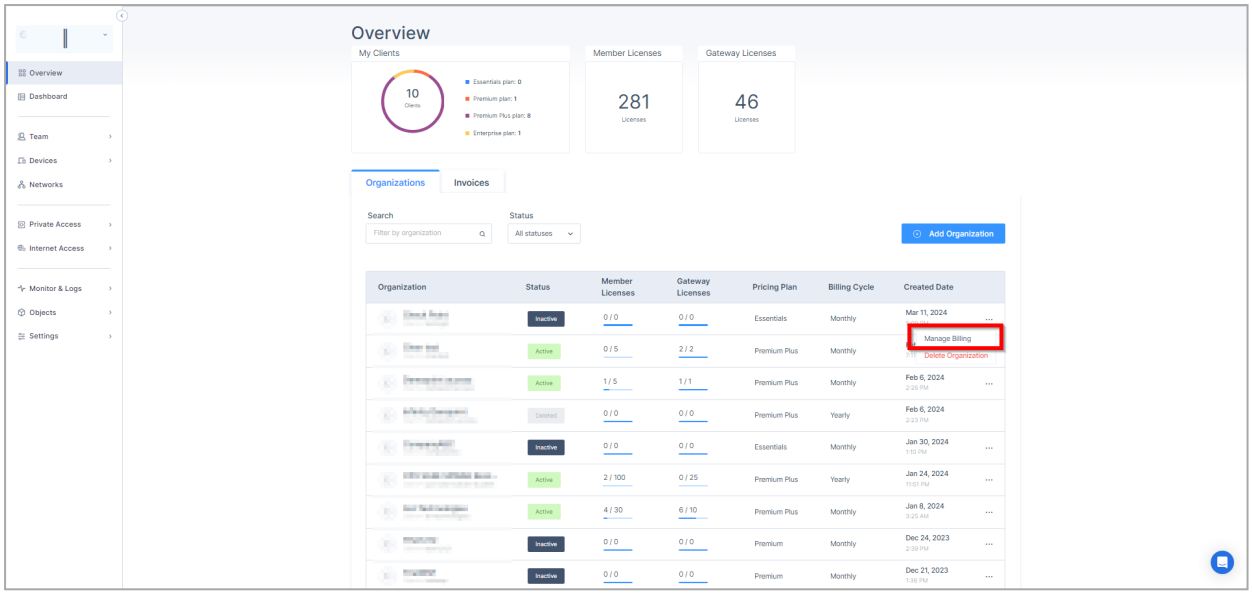
To download an invoice, click **Download**.

Managing Billing

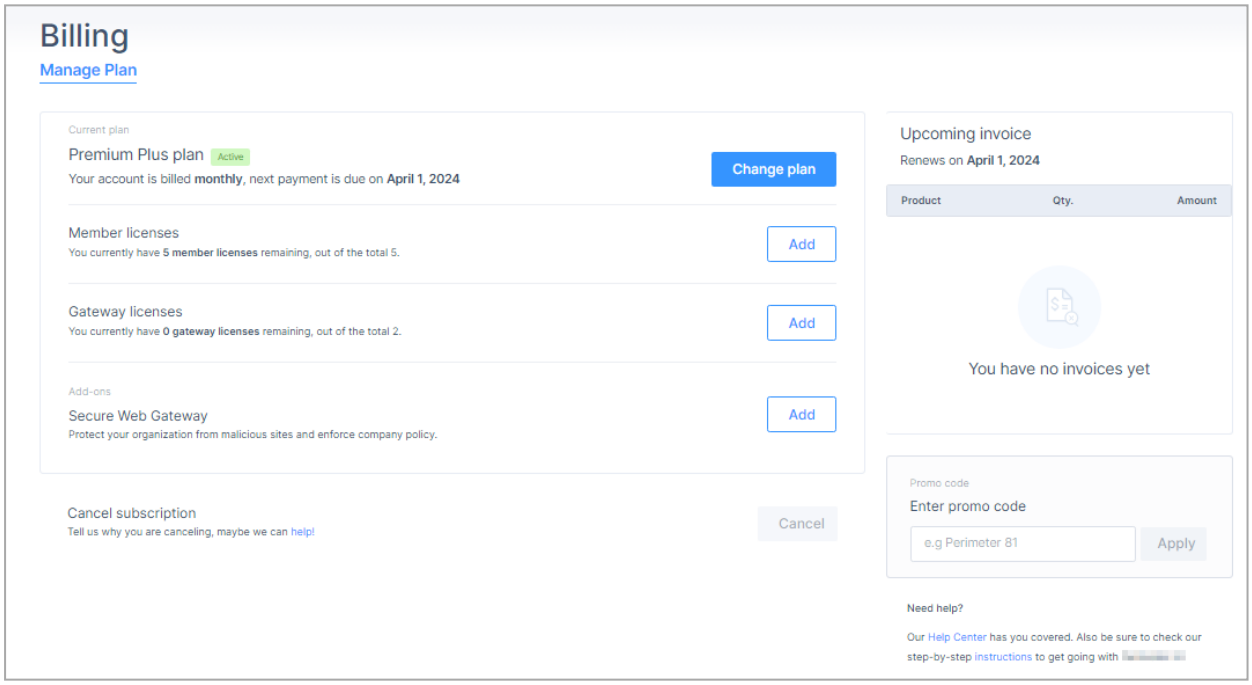
1. Access the **Check Point SASE** (Perimeter 81) Administrator Portal and go to **Overview** and click the **Organizations** tab.



2. Scroll to the end of the row and click ... and select **Manage Billing**.



The **Billing** page appears.



3. To change the subscription plan, see Updating the Subscription Plan.
4. To modify member license, see Modifying Member Licenses.
5. To add or remove the gateway license, see Modifying Gateway / Application Licenses.
6. To cancel the subscription, see Cancelling Subscription.

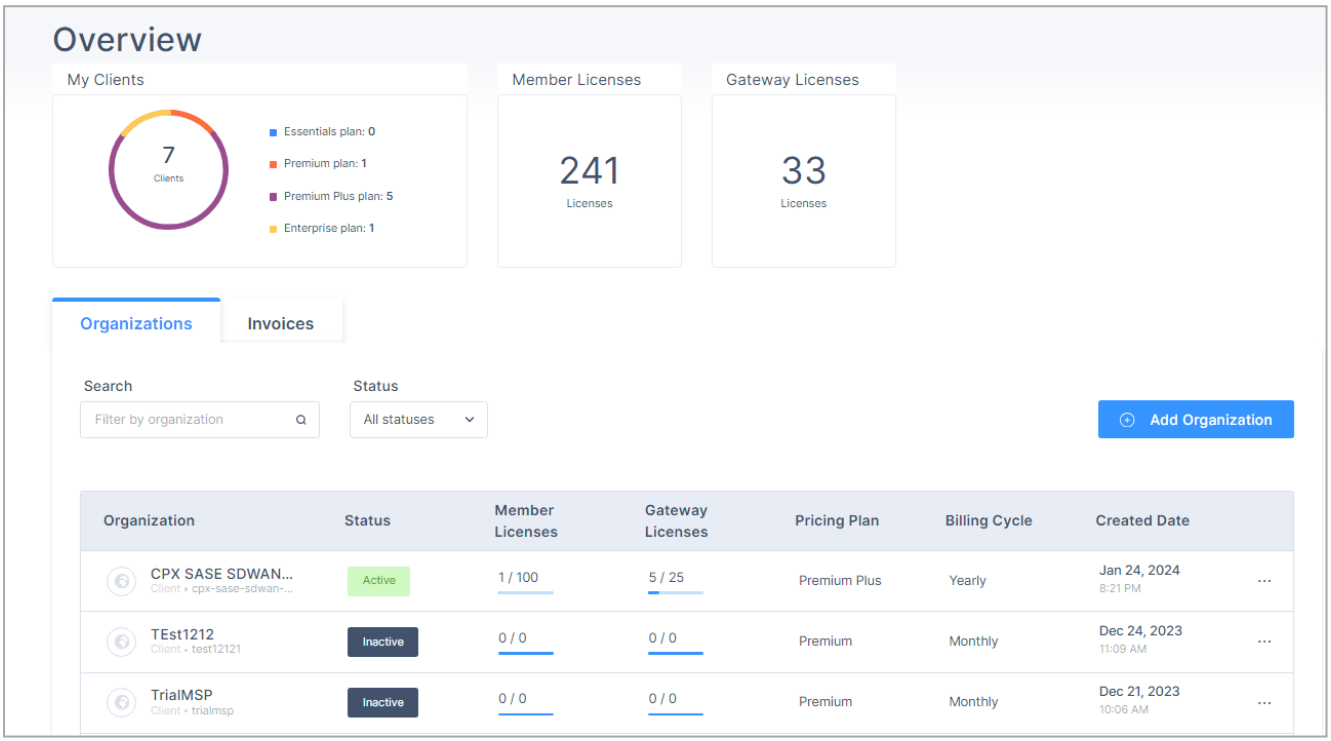
Overview

Note - This page is available only for the MSSP accounts in the Perimeter 81 workspace.

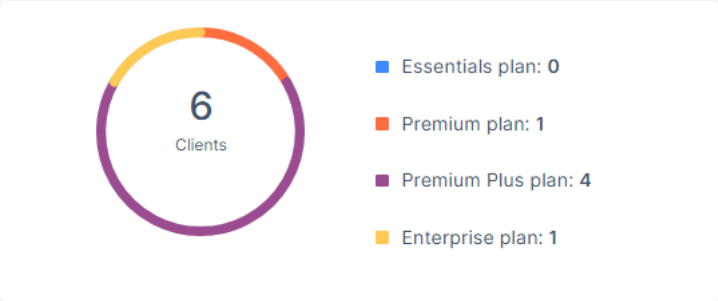
The **Overview** page allows you to view:

- *"My Clients" below*
- *"Member Licenses" below*
- *"Gateway Licenses" on the next page*
- *"Organizations" on the next page*
- *"Invoices" on page 1169*

To view the **Overview** page, access the **Check Point SASE** (Perimeter 81) Administrator Portal and click **Overview**.



My Clients



My Clients widget shows the number of clients and their subscription plans.

Member Licenses

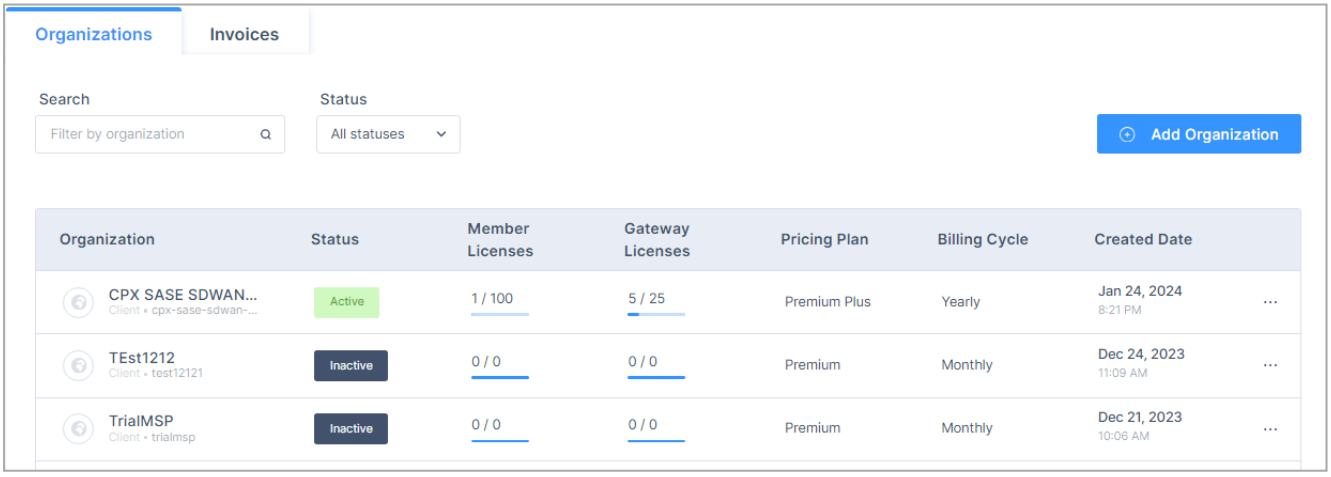
The **Member Licenses** widget shows the total number of purchased member licenses.

Gateway Licenses

The **Gateway Licenses** widget shows the total number of purchased gateway licenses.

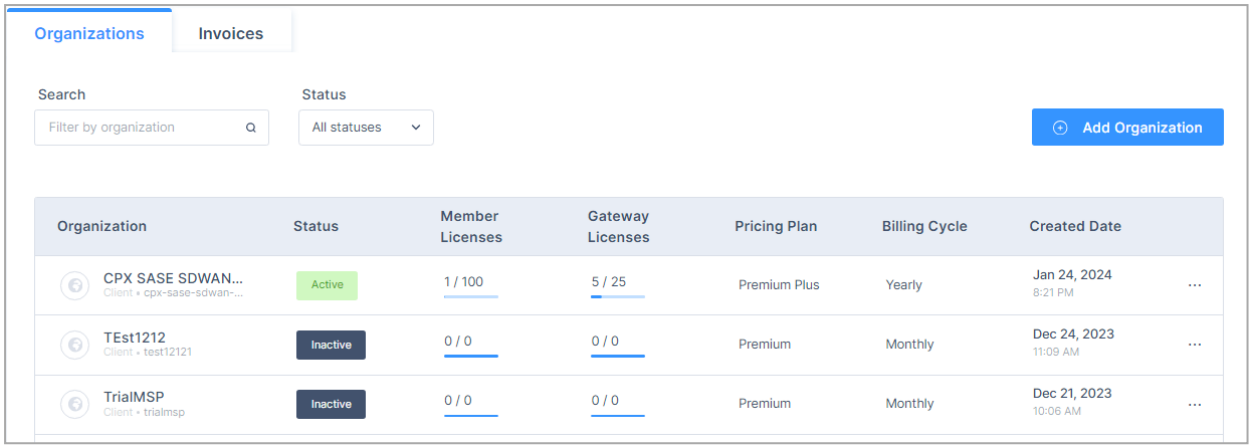
Organizations

The **Organizations** tab allows you to view and manage billing for the organizations.

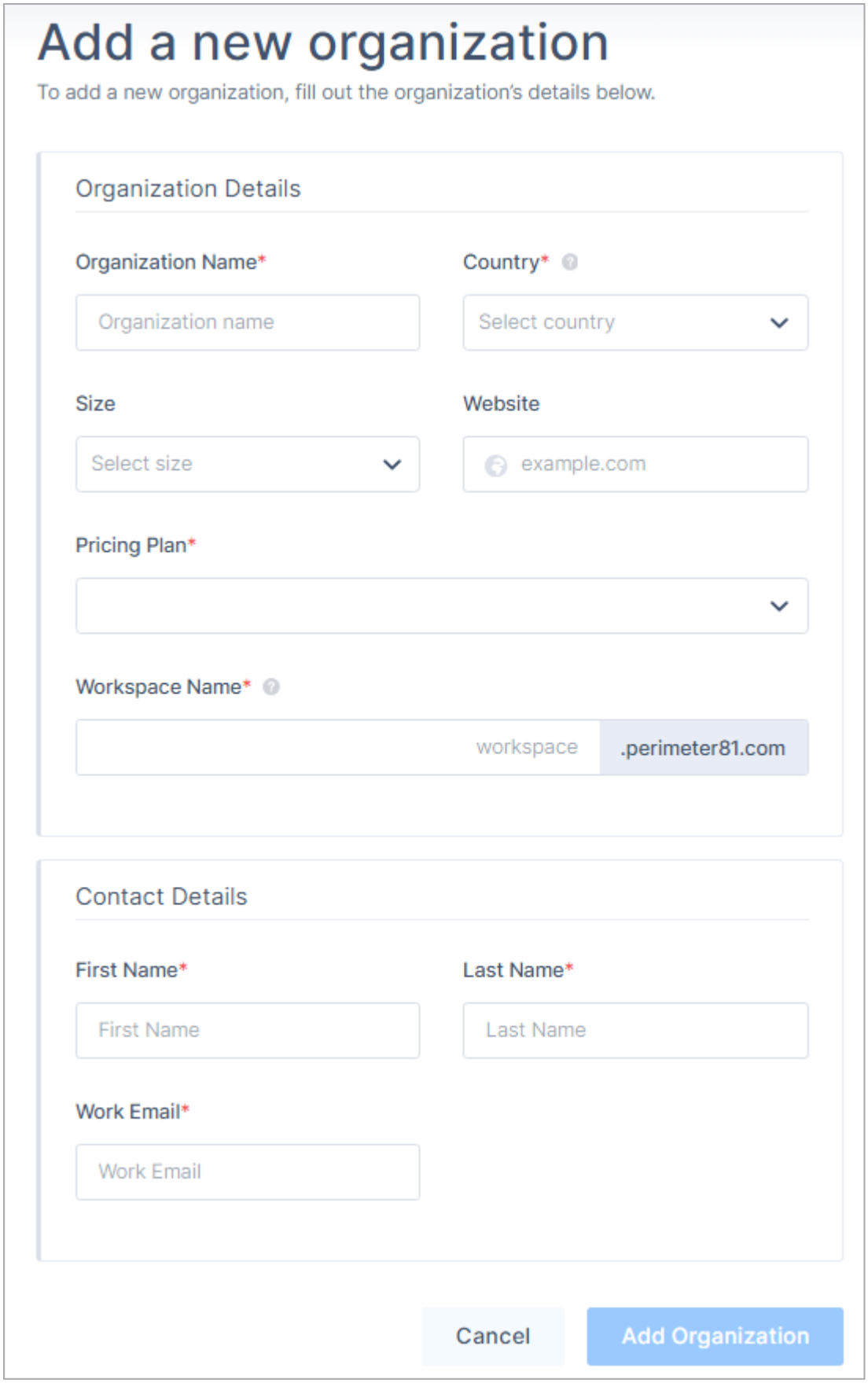


Adding an Organization

1. Access the **Check Point SASE** (Perimeter 81) Administrator Portal and go to **Overview** and then click the **Organizations** tab.
2. Click **Add Organization**.



The **Add a new organization** window appears.



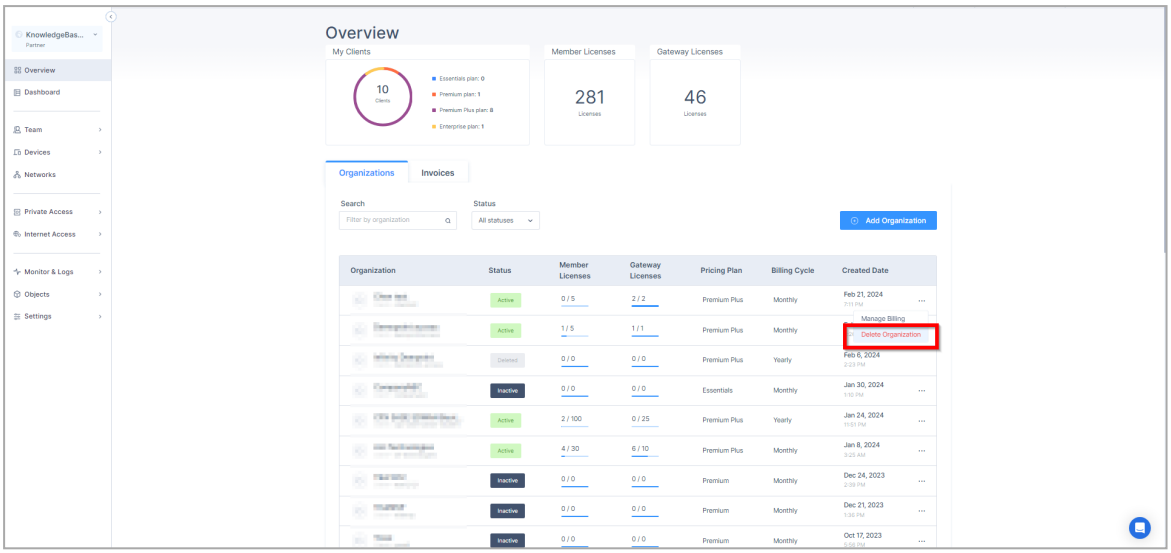
3. In the **Organization Details** section, specify these:

- **Organization Name**
- **Country**
- **Size**
- **Website** - Your organization's website address.
- **Pricing Plan**
- **Workspace Name**.

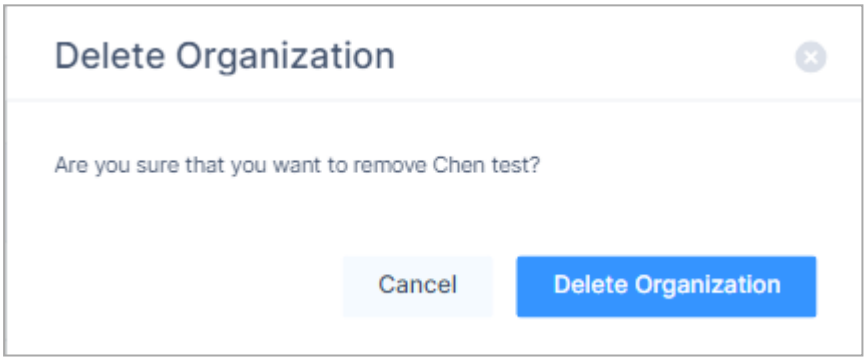
Note - You cannot change the workspace name after you create it.

4. In the **Contact Details** section, enter these:
   - **First Name**
   - **Last Name**
   - **Work Email**
5. Click **Add Organization**.
6. To delete an organization, scroll to the end of the row and click ··· .

a. Select **Delete Organization**.



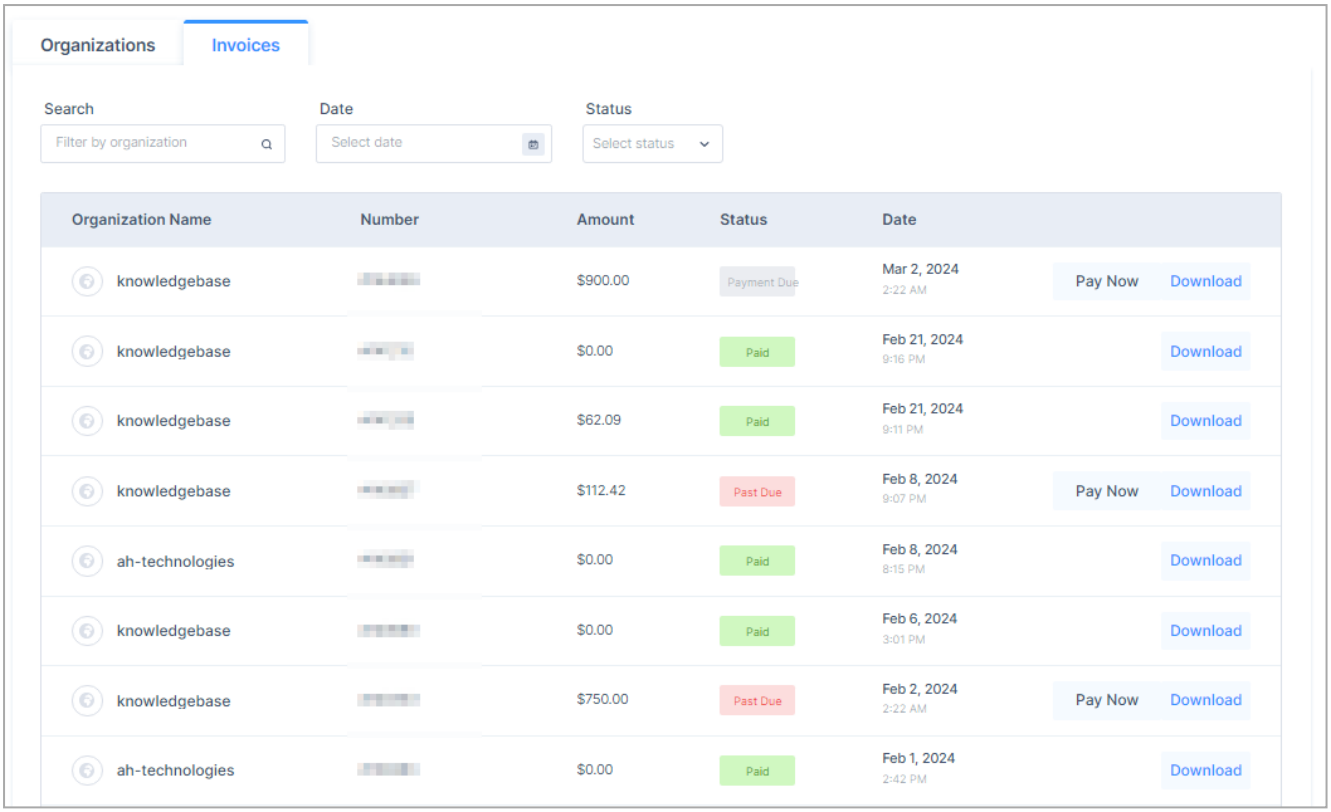
The **Delete Organization** window appears.



b. Click **Delete Organization**.

Invoices

The **Invoices** tab allows you to view, pay and download the invoices.

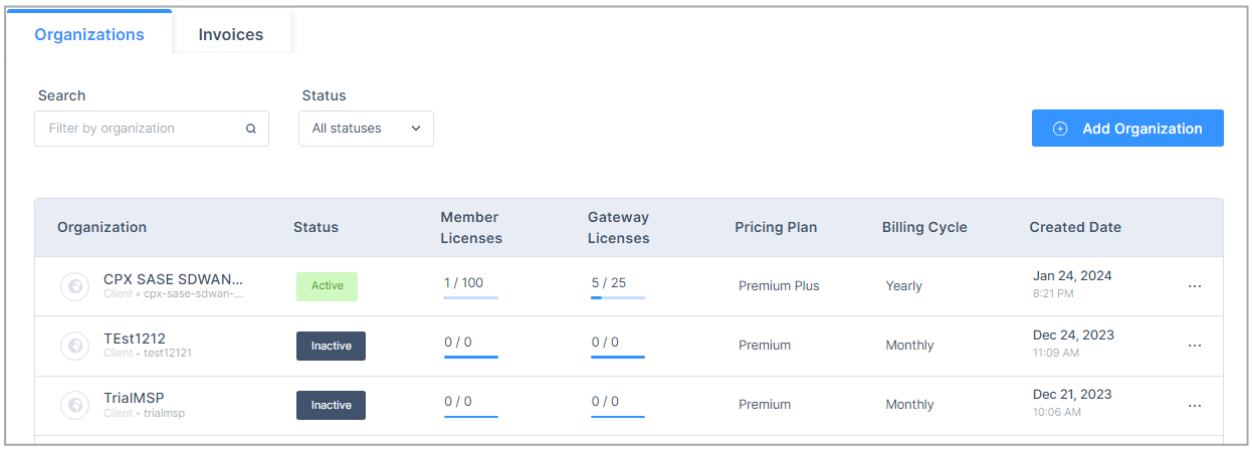


To pay an invoice, click **Pay Now**.

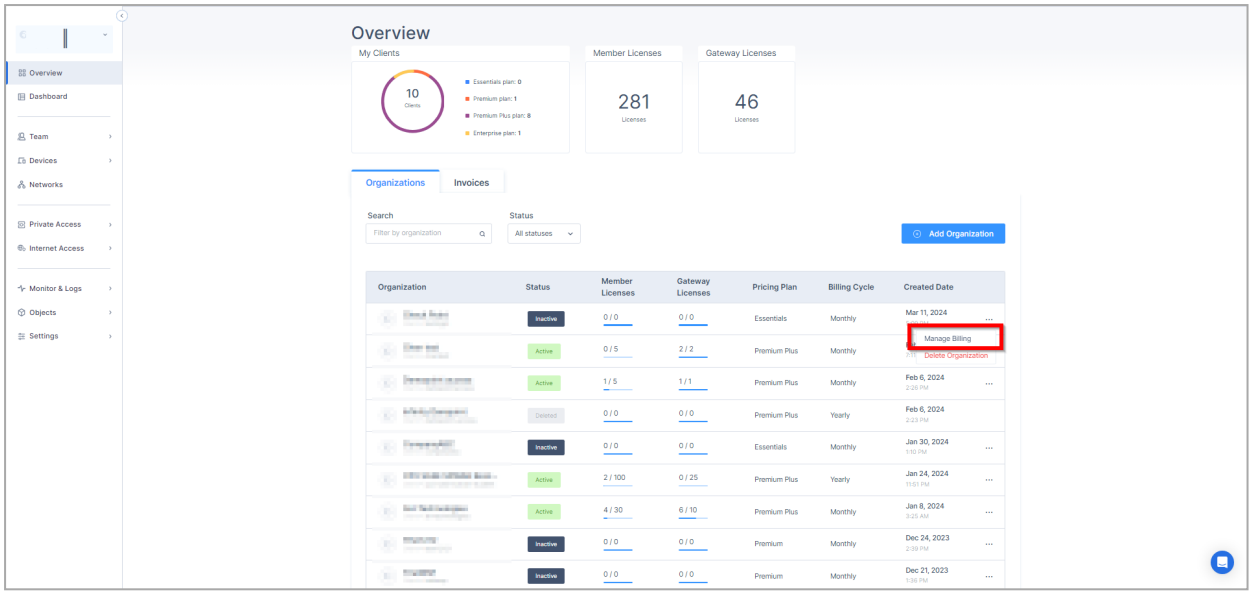
To download an invoice, click **Download**.

Managing Billing

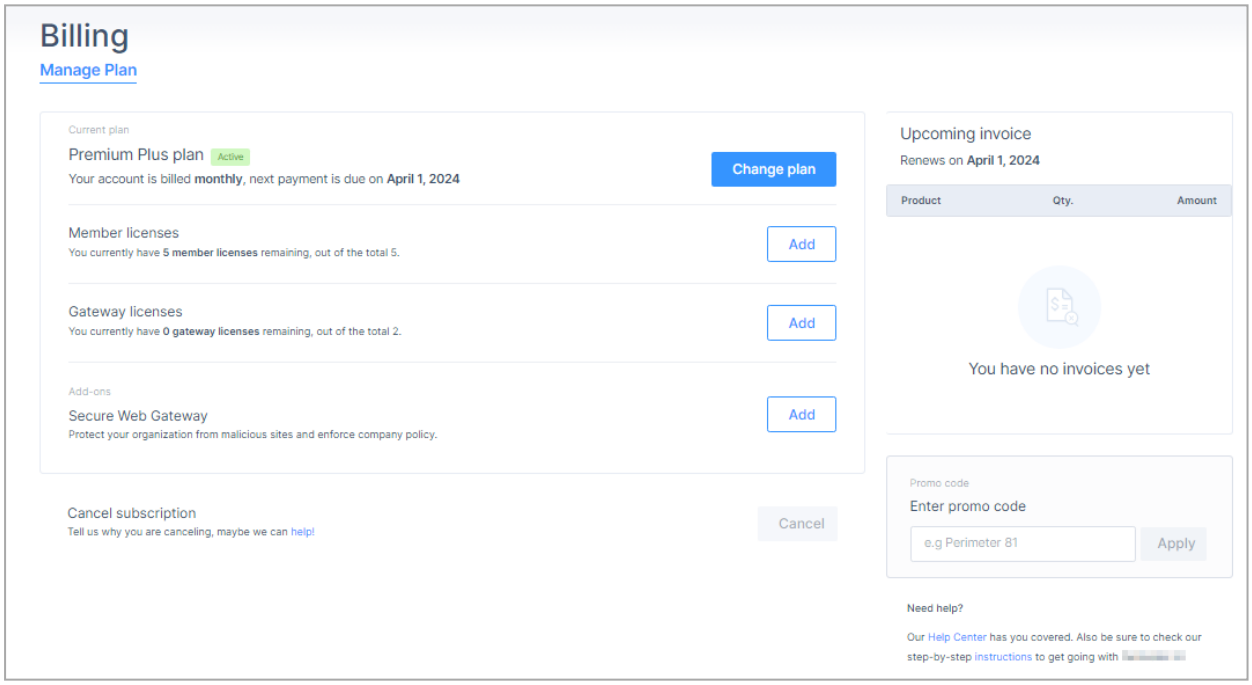
1. Access the **Check Point SASE** (Perimeter 81) Administrator Portal and go to **Overview** and click the **Organizations** tab.



2. Scroll to the end of the row and click ... and select **Manage Billing**.



The **Billing** page appears.



3. To change the subscription plan, see Updating the Subscription Plan.
4. To modify member license, see Modifying Member Licenses.
5. To add or remove the gateway license, see Modifying Gateway / Application Licenses.
6. To cancel the subscription, see Cancelling Subscription.

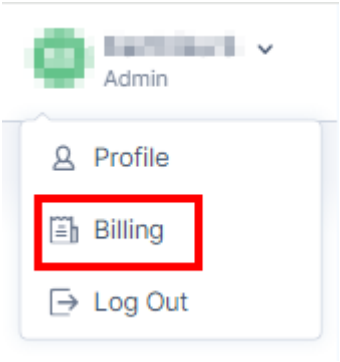
Billing

Note - This page is available only for the MSSP accounts in the Perimeter 81 workspace.

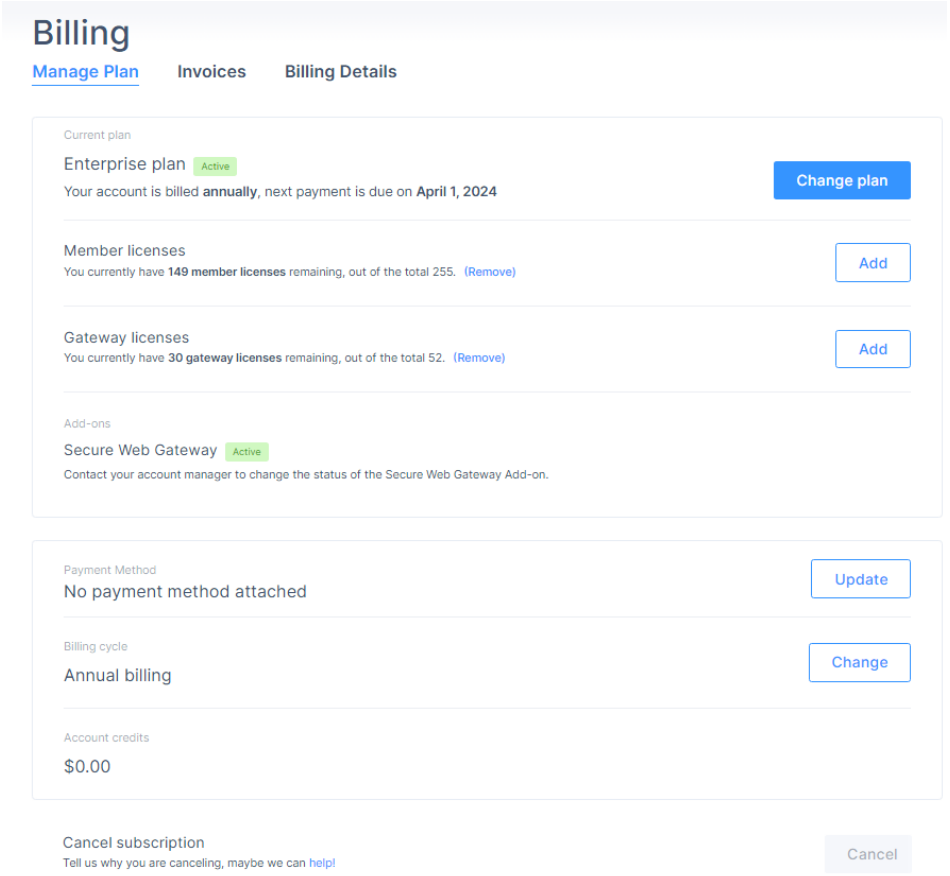
Billing allows you to manage your billing plan, pay invoices and update billing details.

To view Billing:

1. Access the Check Point SASE Administrator Portal.
2. In the top-right corner, click the username and then click **Billing**.



The **Billing** page appears. The **Manage Plan** tab is displayed by default.



Manage Plan

The **Manage Plan** tab allows you to manage your billing plan.

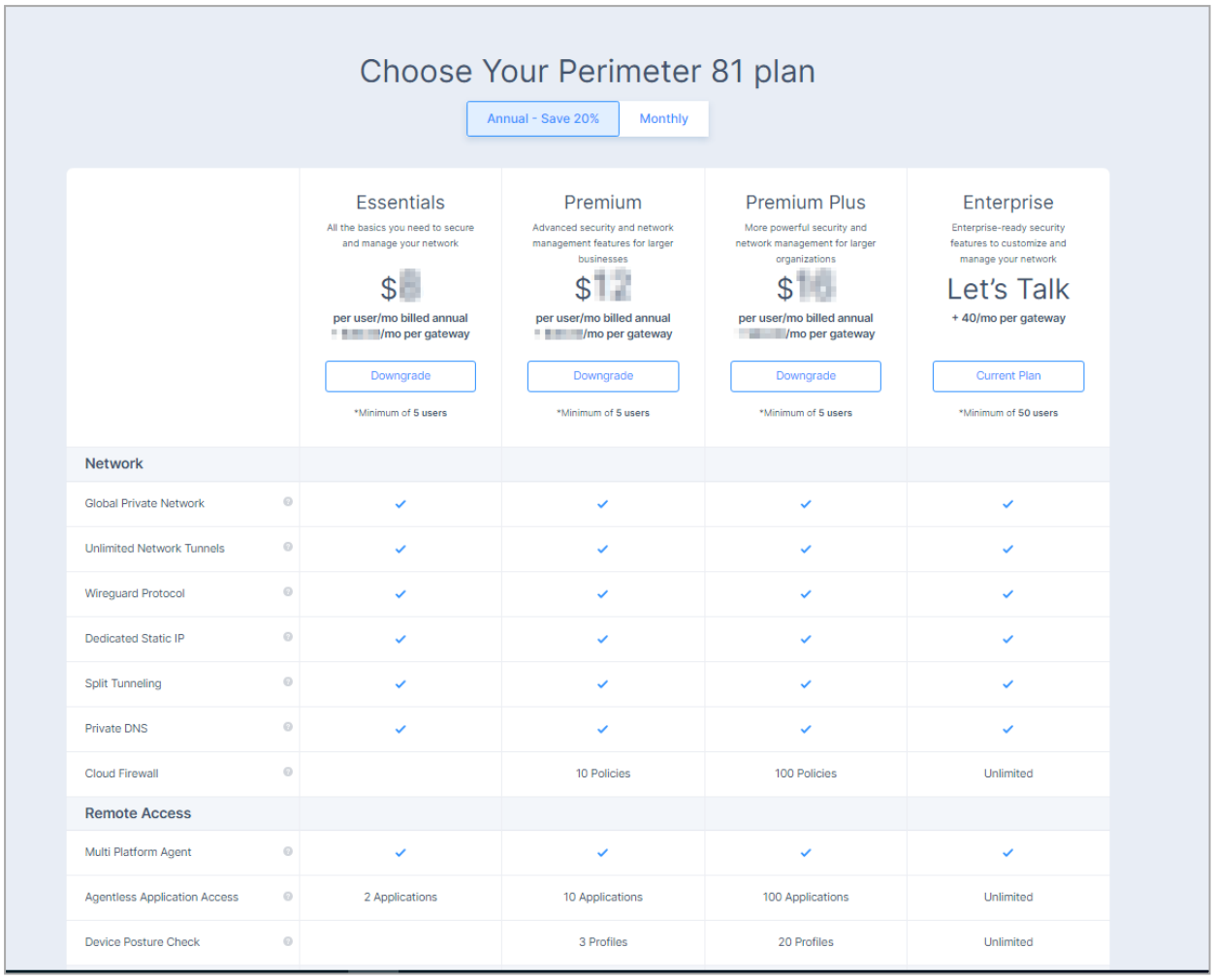
- Update your Subscription Plan
- Modify Member Licenses
- Modify Gateway / Application Licenses
- Add a payment method
- Cancel subscription

Updating the Subscription Plan

1. In the **Current plan** section, click **Change plan**.

The system displays the available plans.

Note - Default is the **Essentials** Plan.

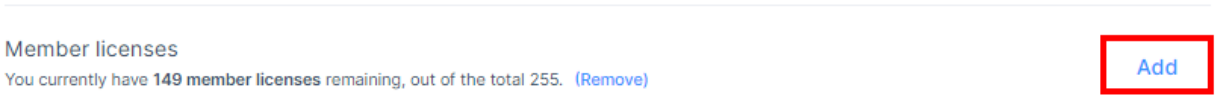


2. Select your billing cycle:
   - Annual
   - Monthly

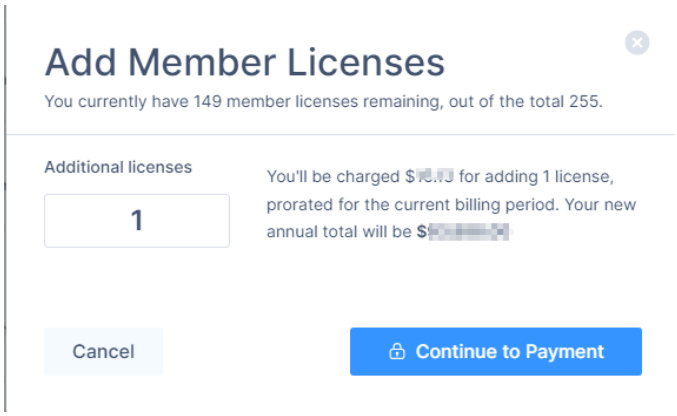
   Note - The billing cycle starts at the beginning of the month. If you purchase a subscription mid-month, you are charged a prorated amount.
     - Monthly billing - You are charged the full subscription amount on the 1st of the following month. For example, you purchased on 15 April, you are charged $5 on the same day, then $10 on 1 May and every following month.
     - Annual billing - You are charged the full subscription amount on the 1st of the purchased month. For example, you purchased on 15 April, you are charged $92 on the same day, then $100 on 1 April next year.
3. Select the plan you want to upgrade to.

Modifying Member Licenses

1. In the **Member licenses** section, click **Add**.

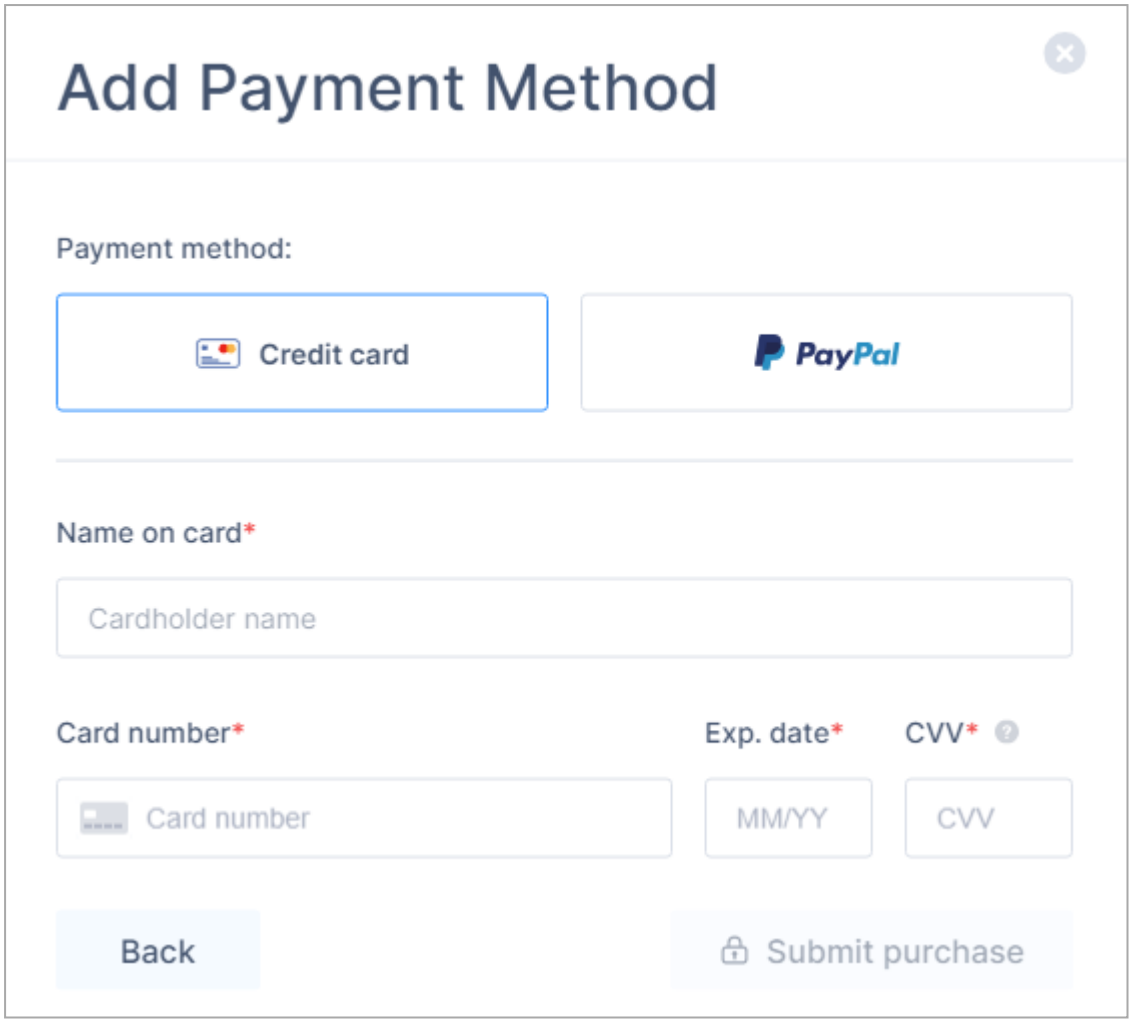


   The **Add Member Licenses** window appears.



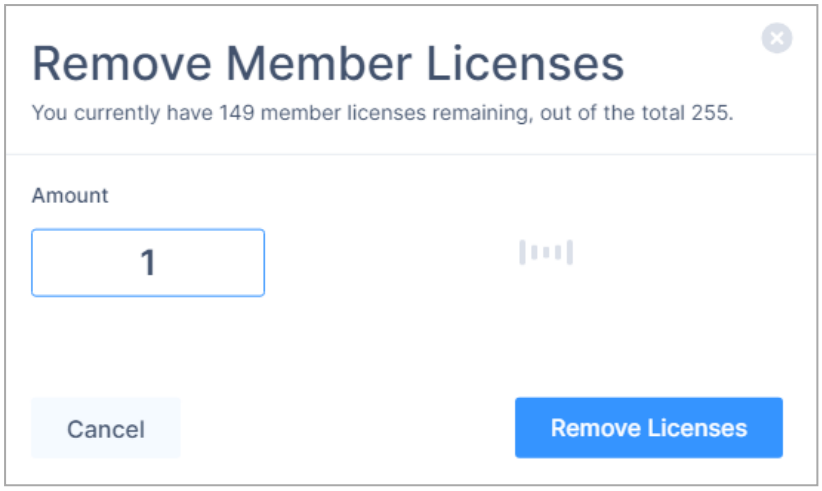
2. In the **Additional licenses** field, enter the number of member licenses.
3. Click **Continue to Payment**.

   The **Add Payment Method** window appears.



4. Select the payment method and enter the details.
5. Click **Submit purchase**.
6. To remove a member license, in the **Member licenses** section, click **Remove**.

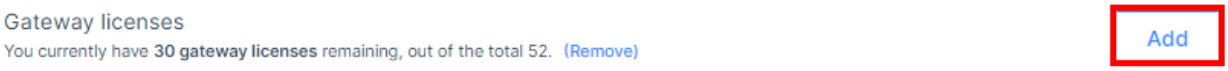
The **Remove Member Licenses** window appears.



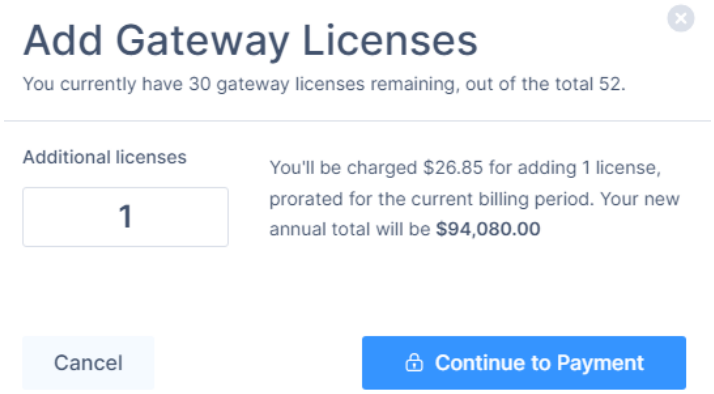
7. Enter the number of licenses to remove and click **Remove Licenses**.

Modifying Gateway / Application Licenses

1. To add a Gateway license, in the **Gateway licenses** section, click **Add**.

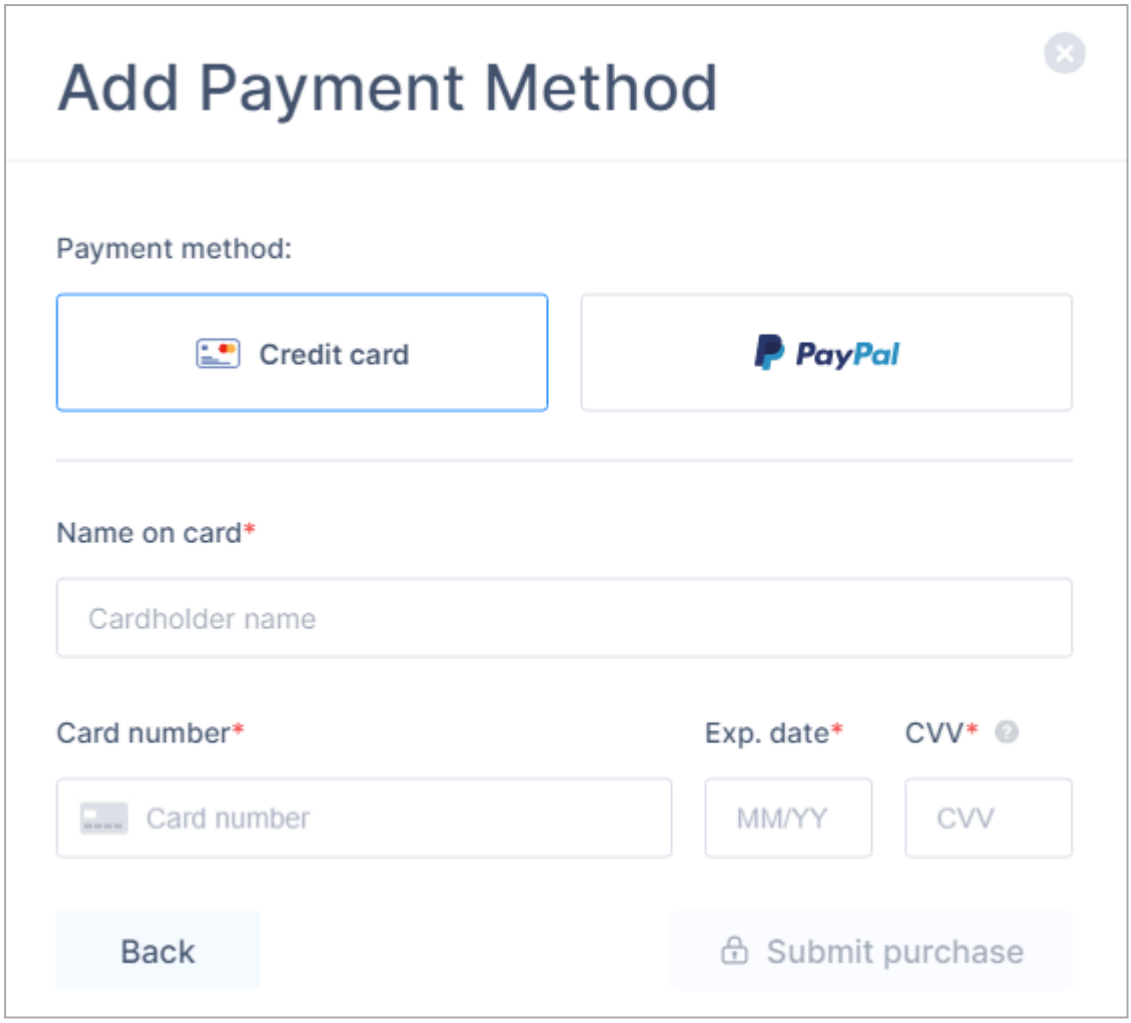


The **Add Gateway Licenses** window appears.



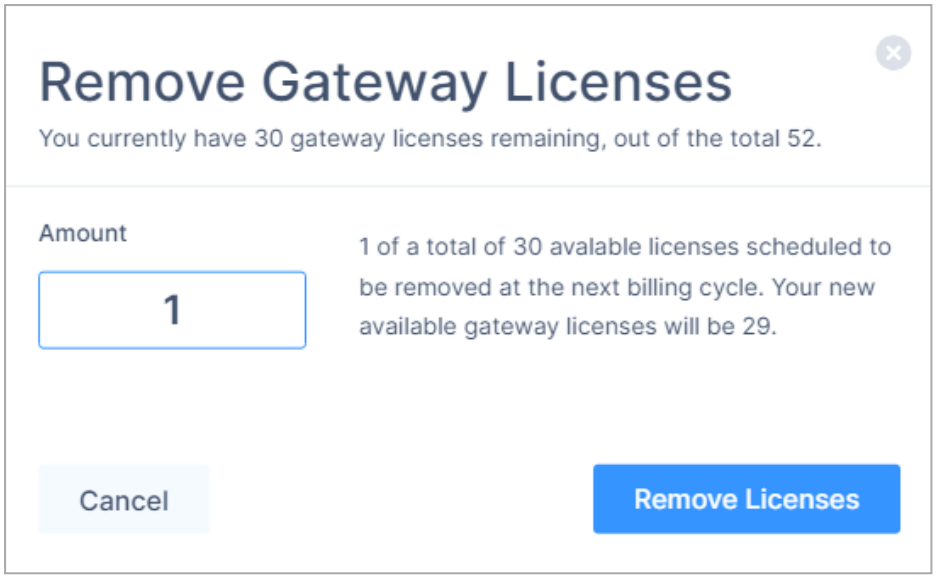
2. In the **Additional licenses** field, enter the number of gateway licenses.
3. Click **Continue to Payment**.

   The **Add Payment Method** window appears.



4. Select the payment method and enter the details.
5. Click **Submit purchase**.
6. To remove a Gateway license, in the **Gateway licenses** section, click **Remove**.

The **Remove Gateway Licenses** window appears.

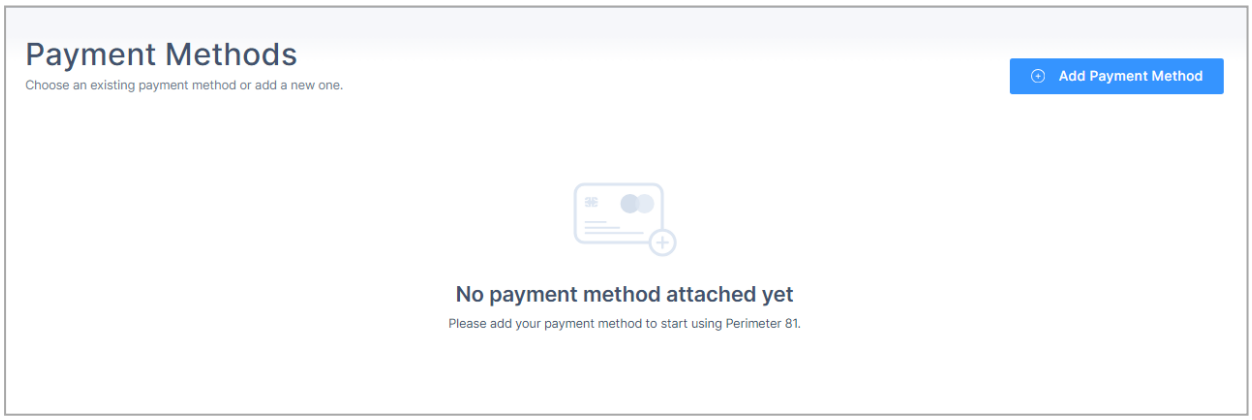


7. Enter the number of licenses to remove and click **Remove Licenses**.

Adding a Payment Method

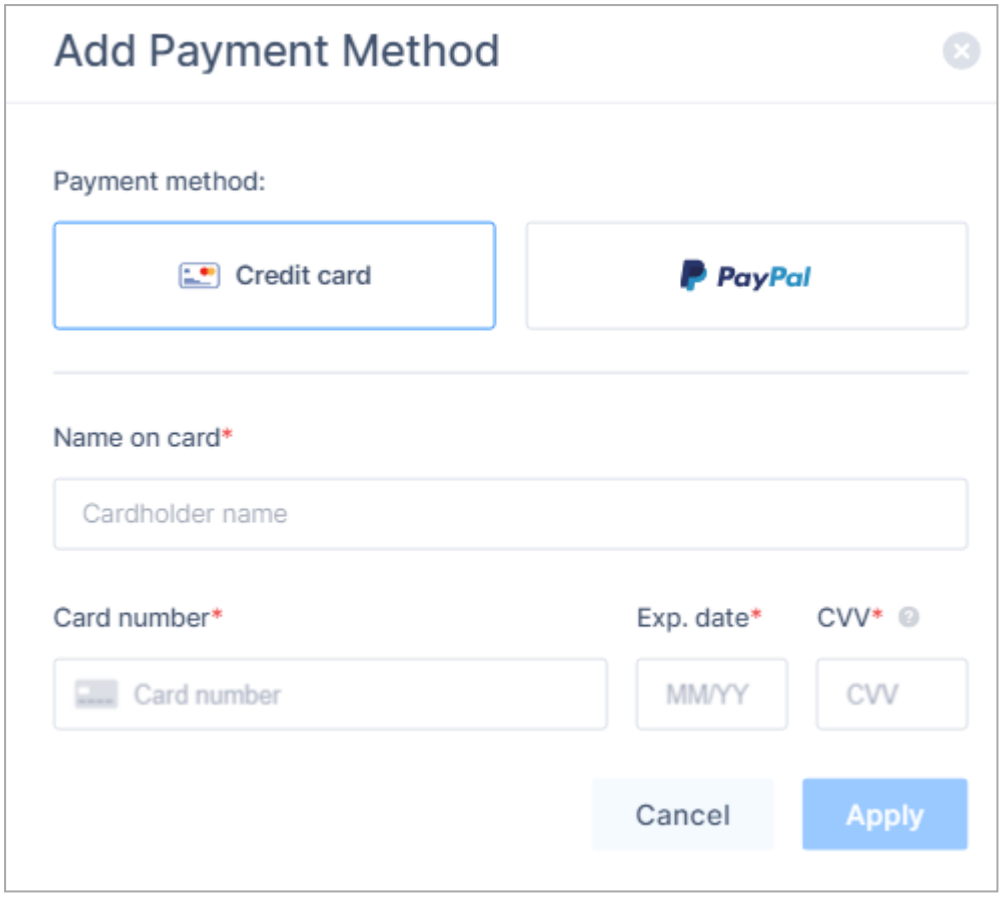
1. In the **Payment Method** section, click **Update**.

The **Payment Methods** page appears.



2. Click **Add Payment Method**.

   The **Add Payment Method** window appears.



3. Select the payment method and enter the details.
4. Click **Apply**.

   After the payment method is added, you receive a confirmation email.

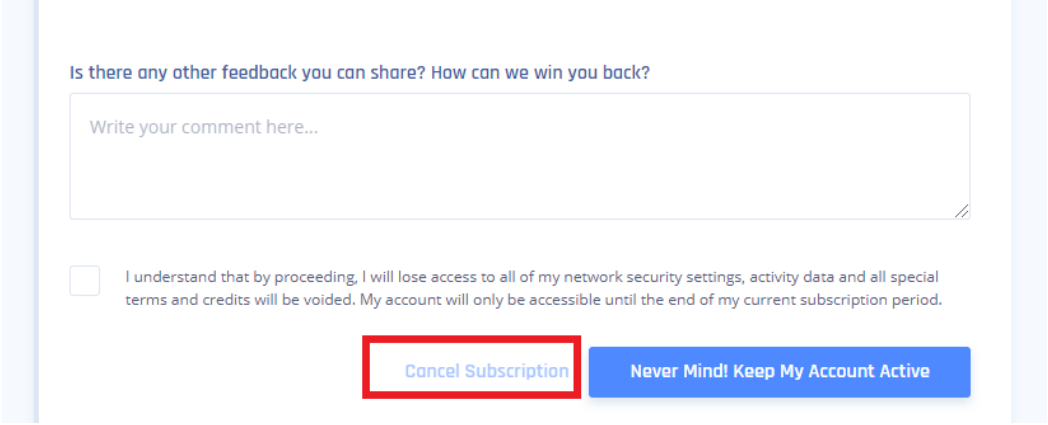
Cancelling Subscription

Notes -

- If you cancel the subscription within 30 days of activating your account, you get a full refund.
- After you cancel your subscription, your account is accessible only till the end of the current subscription period.

1. To cancel your account subscription, in the **Cancel subscription** section, click **Cancel**.

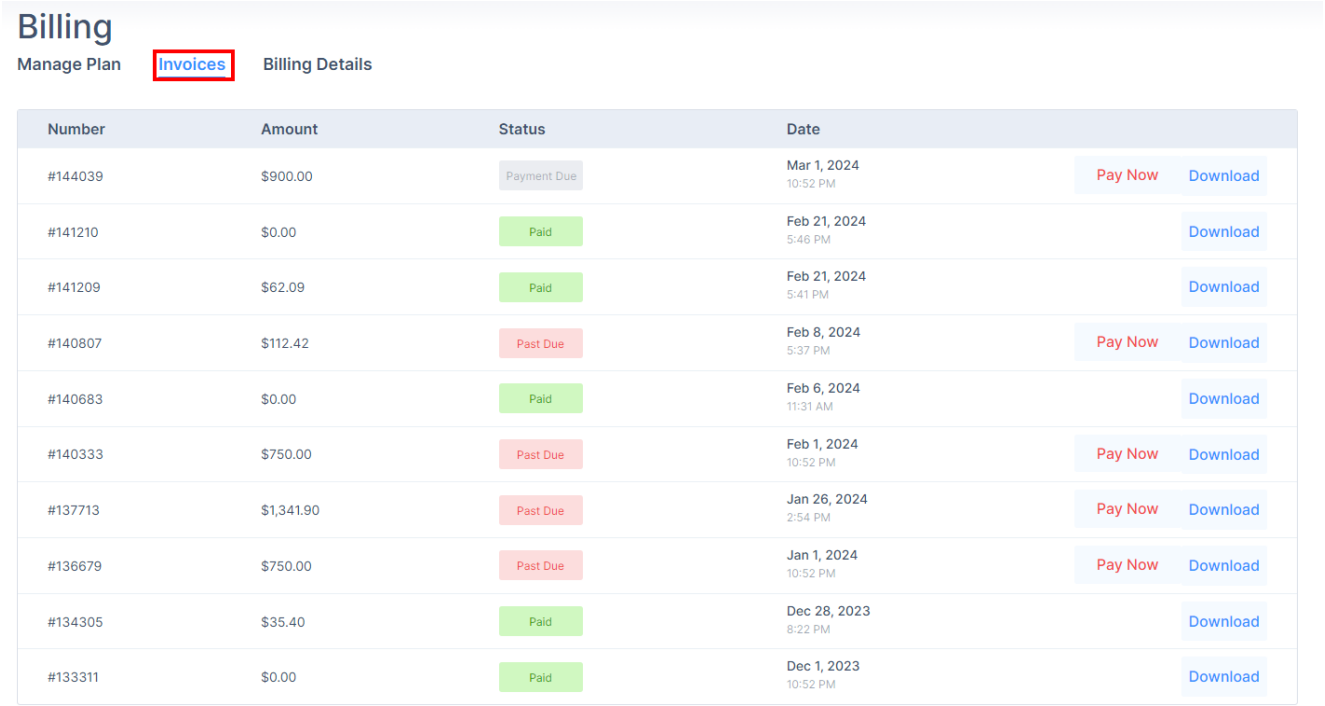
2. Enter a feedback (optional), select the checkbox and then click **Cancel Subscription**.



Invoices

The **Invoices** tab allows you to pay and download your invoices.

To view **Invoices**, access the **Billing** page and click the **Invoices** tab.



To pay an invoice, click **Pay Now**.

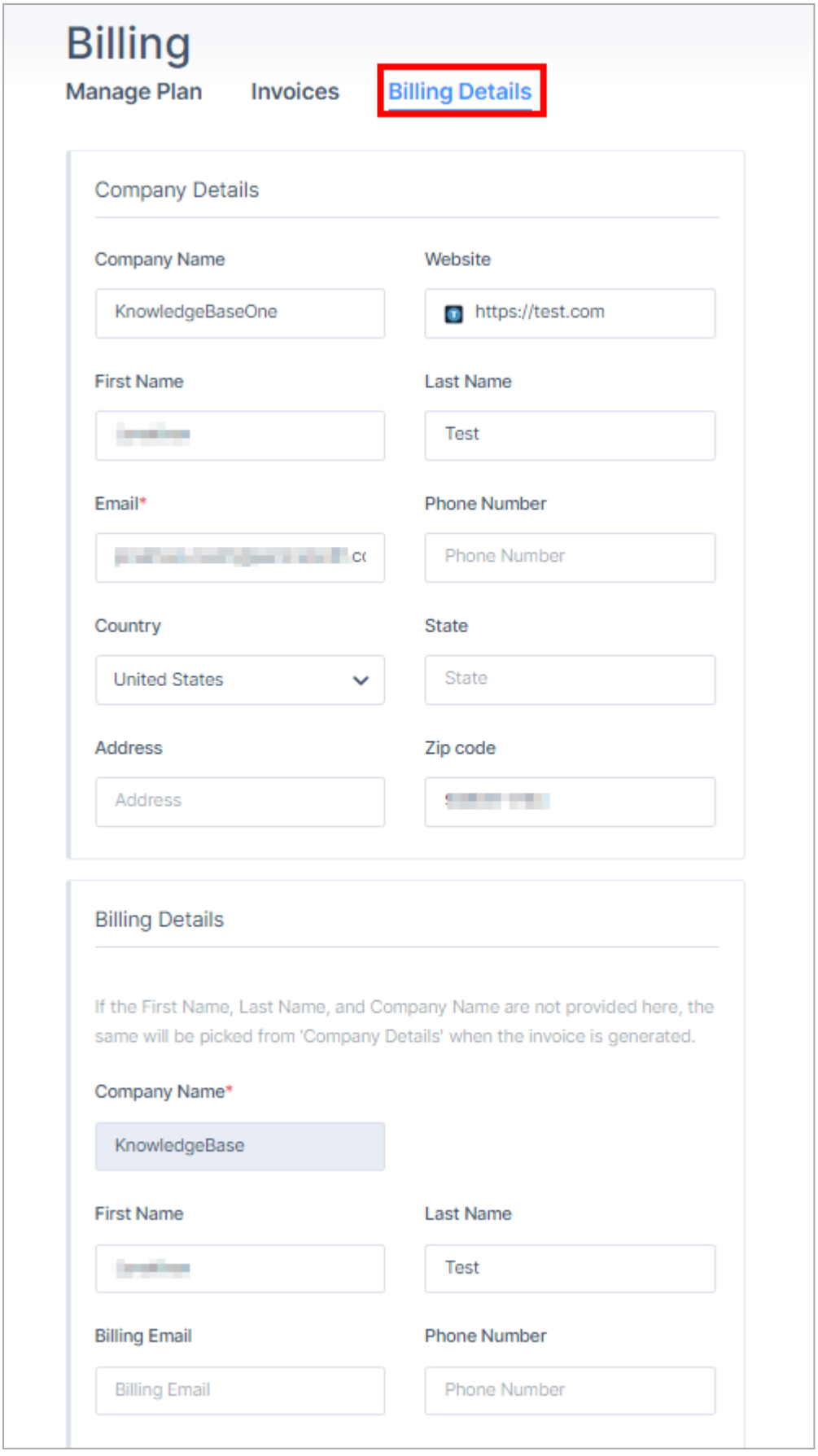
To download an invoice, click **Download**.

The system download the invoice in PDF format.

Billing Details

The **Billing Details** tab allows you to update the billing information for your organization.

To view **Billing Details**, access the **Billing** page and click the **Billing Details** tab.



To update the billing details, enter the required changes and click **Save**.

Managing SASE MSSP Tenants in Check Point Portal

This topic describes how Managed Security Service Provider (MSSPs) onboard and manage customerSASE tenants using the Check Point Portal. In an MSSP environment, administrators manage user access centrally from the Infinity parent tenant and assign permissions to child SASE tenants through User Groups.

This section explains how to:

- Create a SASE-enabled child tenant
- Assign the SASE service and PAYG license
- Grant MSSP parent access
- Manage users and roles

For general Check Point Portal account management and user administration, see Infinity Portal MSSP Administration Guide.

Prerequisites

Before you begin, ensure Check Point Portal Parent account:

- Is configured as an MSSP account
- Is connected to a valid User Center account
- Has Pay-As-You-Go (PAYG) licensing enabled

> **Note** - If you need assistance configuring these prerequisites, contact *Check Point Support*.

Onboarding a SASE Child Tenant

Follow these steps to onboard a new customer tenant with SASE.

Create a Child Tenant

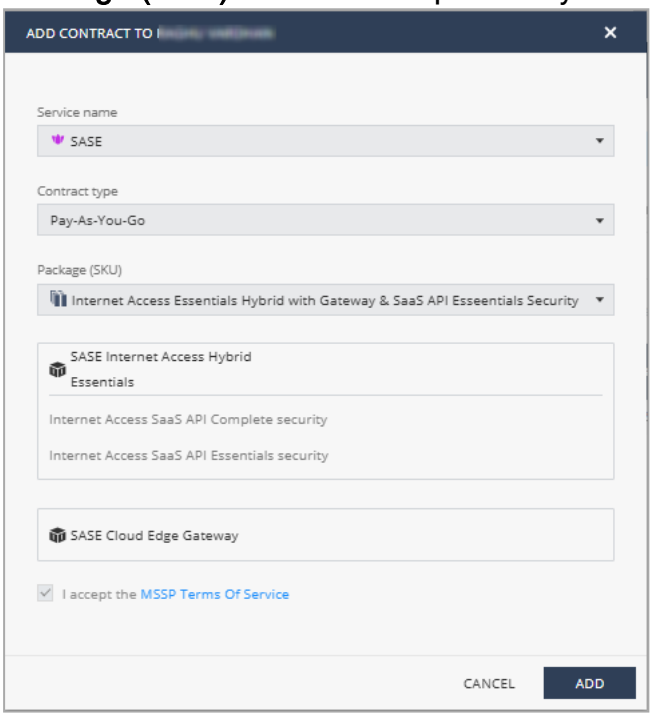
1. Sign in to Check Point Portal.
2. Create a new child tenant under the MSSP parent account.

The user who creates the child tenant becomes the Primary Admin for that tenant.

For information about how to create a child tenant, see Infinity Portal MSSP Administration Guide.

Add the SASE Service to the Child Tenant

1. Access to Check Point Portal, go to **Manage Accounts**.
2. Select the newly created child tenant.
3. Click **Add Contract**.
4. Add the SASE service:
   a. **Service name**: SASE
   b. **Contract type**: Pay-As-You-Go license.
   c. **Package (SKU)**: Select the required Pay-As-You-Go (PAYG) SKU.



The user who adds the SASE service must:

- Have Administrator permissions in the MSSP parent tenant.
- Have User Group Admin access to the child tenant.

Supported PAYG SKUs

- Internet Access
- Private Access
- Gateway

User Management

User management depends on where the user is defined.

For more information about user roles and management, see Infinity Portal MSSP Administration Guide.

MSSP Parent Users

Parent users receive access to child tenants through User Groups.

Users assigned administrative roles through User Groups automatically inherit access to permitted child tenants.

Supported Roles

- Primary Global Admin
- Global Admin
- SASE Admin
- User Manager
- Network Manager
- Security Manager

Notes -

- Each user can have only one SASE role.
- If a user belongs to multiple User Groups, ensure the groups do not assign conflicting SASE roles.

Not Supported

- Global Read-Only
- SASE Read-Only
- Multiple roles per user
- Custom roles
- Global User Admin role mapping to SASE roles

  Note - The Global User Admin (Infinity user manager role) does not map to any SASE role.

Grant Additional MSSP Parent Users Access to the Child Tenant

To grant additional MSSP parent users access to the child tenant:

1. In the MSSP parent tenant, open User Groups.
2. Edit or create a User Group.

3. Grant access to the required child tenant.
4. Assign the appropriate SASE role.

User Groups control how access is inherited from the parent tenant to child SASE tenants.

Note - The Read-Only roles, whether assigned through Global or service-specific roles, is not supported for SASE.

Child Tenant SASE Members

You can add members directly to the child tenant:

- Manually
- Through an integrated Identity Provider (IdP)

When a member signs in to SASE for the first time, the system adds the user as a SASE member and includes the user in license consumption.

Usage and Billing

Billing is based on usage reported by each child tenant.

- Usage data is reported daily.
- Reports reflect the previous day's usage.

How-To and Troubleshooting References

How-To References

- For SASE Frequently Asked Questions (FAQ), see sk182225.
- For information on how to segment networks, see *"Segmenting Networks" on page 239*.
- For information on how to upload tunnel configuration files, see *"Using the Configuration File for Tunnel Configuration" on page 538*.
- For information on how to securely connect sites and cloud resources using SASE, see *"Interconnectivity (Cloud-Agnostic)" on page 241*.
- For information on how to create Route 53 Inbound Endpoints, see sk182274.
- For information on how to manage member devices, see *"Managing Members" on page 79*.
- For information on certificate manager and how to upload application domain certificate, see *"Certificate Manager" on page 1133*.
- For information on how to whitelist resources, see sk182260.
- For integrating Google Cloud's Private Zone/Private DNS feature with SASE gateway, see *"Google Cloud DNS" on page 719*.
- For information on Google Cloud VPC Peering, *"Google Cloud VPC Peering" on page 718*.
- For information on how to change region and language for accurate Google search results, see sk182250.
- For information on how to change DNS settings in Windows and Mac, see sk182255.
- For information on how to remove the Wireguard Connector, see *"Removing the WireGuard Connector" on page 212*.
- For information on how to deactivate a gateway, see *"Deactivating a Gateway" on page 170*.

Troubleshooting References

- For troubleshooting common errors in IPsec Site-to-Site connection setup, see sk182243.

- For information on how to collect logs manually, see *"Collecting Logs Manually" on page 153*.
- For assigning Support Access role to Check Point SASE support engineer to temporarily access your tenant without credentials, see *"Support Access" on page 1138*
- For troubleshooting web application issues, generate the HTTP Archive (HAR) file. For more information, see sk182245.
- For troubleshooting connectivity issue with SASE Agent, see sk182251.

Release Notes

- SASE Administrator Portal
  - *"2026" on page 1190*
  - *"2025" on page 1197*
  - *"2024" on page 1212*
- SASE Agent
  - *"Android / Chromebook" on page 1245*
  - *"iOS" on page 1242*
  - *"Linux" on page 1238*
  - *"MacOS" on page 1229*
  - *"Windows" on page 1218*

Check Point SASE Administrator Portal

2026

March

Early Availability	■ **Web RDP – NLA Authentication Support** End users accessing Web RDP applications with NLA security mode are now prompted to enter RDP credentials directly in the browser. Supports both Standard and Enhanced Networks. Requires a new network or upgrade to the latest version. *Check Point SASE Administration Guide* ■ **Enhanced Network IPsec Redundancy** Admins can now create dynamic IPsec tunnels with multiple terminations in the same region, enabling active-active HA setups. Not supported with Quantum/Spark devices. Requires a new network or upgrade to the latest version. ■ **Block Websites with Invalid Certificates** Admins can enforce blocking of websites with expired, revoked, self-signed, or untrusted certificates, preventing end users from accessing potentially unsafe sites. **Minimum Agent Version:** Windows/macOS v12.6 ■ **Security Events Notification Control** Admins can now disable end-user security event notifications and enforce this setting across the organization. By default, users receive notifications and can toggle this setting individually until it is enforced. **Minimum Agent Version:** Windows/macOS v12.6 ■ **Updatable Objects Support for Internet Access** Updatable Objects, which are dynamically maintained and automatically updated objects managed by Check Point, are now supported in Internet Access policies. This extends Updatable Objects support beyond Split Tunneling (introduced February 2026). **Minimum Agent Version:** Windows/macOS v12.6

New Features	■ **Canada Data Residency** Check Point SASE now supports Canada as its fifth data residency region (joining US, EU, IN, and AU). Canadian organizations can process and store SASE data locally, including traffic inspection, session data, logs, metadata, and configuration. Full platform access includes Private Access (ZTNA), Internet Access (SWG), and SaaS Security. ■ **New Check Point SASE Point of Presence – Perth** Check Point SASE has expanded its regional coverage with a new Point of Presence (PoP) in Perth, Australia. ■ **SaaS + SASE Integration** Admins can now access a unified view of SaaS Security and SASE in a single location within the SASE platform, providing SaaS visibility and controls alongside Private Access and Internet Access. ■ **Unified Internet Access Policy with Quantum – General Availability (GA)** The unified Internet Access policy with Quantum is now generally available, enabling consistent web security policy enforcement across SASE and Check Point Quantum gateways from a single policy definition.

Enhancements	▪ **Enhanced Networks – Regional Expansion** Enhanced Networks are now available in Hong Kong, Istanbul, and Taipei. ▪ **Check Point SASE Rebranding** The platform has been rebranded from Check Point SASE to Check Point SASE, aligning with the broader Check Point Portal rebranding. ▪ **Tenant Restrictions – Failed Login Attempt Logging** Failed login attempts blocked by Tenant Restrictions rules are now logged, providing better visibility into unauthorized access attempts. **Minimum Agent Version:** 12.7 ▪ **HTTPS Inspection – Bypass Traffic Logging** Admins can now view logs for traffic excluded from HTTPS inspection, providing visibility into bypassed traffic. **Minimum Agent Version:** 12.7 ▪ **IOC – Infinity Portal Integration** IOC management is now supported through the Infinity Portal, enabling centralized handling of indicators of compromise across the SASE platform. **Minimum Agent Version:** 12.7 ▪ **Security Profiles – Full Threat Emulation Event Logging** Admins can now log all Threat Emulation verdicts, including non-malicious files, providing full visibility into file inspection outcomes. **Minimum Agent Version:** 12.7
Resolved Issues	N/A

February

Early Availability	■ **Updatable Objects Support in Split Tunneling** Split Tunneling rules can now reference **Updatable Objects**, which are dynamically maintained network objects that automatically update based on vendor-managed or predefined feeds. This enhancement eliminates manual IP address and FQDN maintenance and ensures that Split Tunneling policies remain accurate as vendor endpoints change. **Minimum Agent Version**: Windows: 12.5 For more information, see *"Updatable Objects" on page 923*. ■ **Pre-Login Authentication for Windows** Administrators can now enable a secure tunnel before OS login using second-device authentication. This enables seamless access to private organizational resources, such as Active Directory, when users work remotely or outside the corporate network. **Minimum Agent Version: Windows:** 12.5 For more information, see *"Pre-Login Tunnel Connection for Windows" on page 146*

New Features	■ **New Built-in Role – Security Manager** A new **Security Manager** built-in role is now available in Check Point SASE. This role enables organizations to delegate security operations and monitoring. It is available to both direct and MSSP customers. Users assigned with this role can: • Access Internet Access configuration • Define Data Loss Prevention (DLP) policies • Manage Objects configuration (Addresses and Custom URLs) • View and investigate Security Events For more information, see *"Member Roles and Permissions" on page 75*. ■ **New Check Point SASE Point of Presence – Hong Kong** Check Point SASE has expanded its regional coverage with a new Point of Presence (PoP) in Hong Kong. For more information, see *"Regions and Point-of-Presence" on page 157*. ■ **Public API Support for FQDN Object Type** Administrators can now manage Fully Qualified Domain Name (FQDN) address objects through the Public API. This enhancement enables: • Programmatic creation of FQDN objects • Retrieval of FQDN object configurations • Updates to existing FQDN objects • Deletion of FQDN objects For more information, see the API documentation. ■ **Tunnel Down Notification via Playblocks** Administrators can now configure automated notifications when a network tunnel goes down. Notifications can be delivered through: • Slack • Microsoft Teams • Email • SMS Supported capabilities include: • Immediate alerts when a tunnel state changes • Consolidated summary notifications at configurable intervals • Configurable silence windows to reduce alert noise • Exclusion of specific tunnels from monitoring Availability: Available for Infinity Portal tenants in US and EU regions.

Enhancements	**Tenant Restrictions – Domain Validation** Tenant Restriction rules now enforce the use of domain values in entries. This enhancement: ■ Prevents the use of invalid formats ■ Improves policy consistency ■ Reduces configuration errors ■ Strengthens enforcement accuracy For more information, see *"Tenant Restrictions" on page 817*.
Resolved Issues	N/A

January

Early Availability	■ **Firewall Logging Granularity** Administrators can now configure logging per firewall rule, enabling logs for both **Allowed** and **Blocked** rules. This provides deeper visibility and improved troubleshooting of firewall policies. **Notes:** • New customers automatically receive firewall logging granularity. • Existing customers without firewall logging enabled can now enable it with granularity. • Firewall logging is not supported for gateways created in the past with one CPU. • Firewall logging granularity requires coordination with support engineer for deployment.

New Features	■ **Granular Role Support for MSSP Parent Users – General Availability (GA)** The Check Point Portal now supports granular SASE service roles for MSSP Parent users, expanding beyond the previous admin-only model. MSSPs can assign roles directly or via Infinity User Groups, enabling least-privilege access and clearer separation of duties. Supported roles include: • Security Manager • Network Manager • User Manager • Admin ■ **Infinity Audits for SASE – General Availability (GA)** SASE now integrates with Infinity Audits, making member activity and administrator actions visible directly in the Infinity Portal. When Infinity Event Forwarding is enabled, these audit events are also exported to your SIEM alongside other security events. ■ **SCIM Sync User Duplication Prevention with Entra ID – General Availability (GA)** Enhanced SCIM mapping for Azure/Entra ID allows SASE to consistently identify users using the Entra ID unique identifier during provisioning and login. This ensures that changes to user attributes such as email or UPN do not result in duplicate user records. As a result, existing access and group memberships are preserved, providing more reliable SSO behavior and reducing operational overhead for teams managing Entra ID-based environments.
Enhancements	■ **Idle Member Automatic Sign-Out** Administrators can now automatically sign out users from idle or unattended devices, reducing exposure from inactive sessions and strengthening endpoint security. ■ **Device Posture Check – Certificate Issuer & Root CA Validation** Device Posture Check (DPC) now includes an additional validation for device certificates, verifying the certificate issuer, validity, and matching private key. This strengthens device trust and compliance posture. ■ **Agent Reset Button Control** Administrators can now control whether the **Reset Agent** button is visible to end users, helping prevent accidental resets and improving manageability in controlled environments.
Resolved Issues	N/A

2025

December

Early Availability	■ **SCIM Sync User Duplication Prevention with Entra ID** Enhanced SCIM mapping for Azure AD/Entra ID to prevent user duplication when connected via Entra ID identity provider. ■ **Infinity Integration with Quantum Services** **Identity and Trust** is now integrated with **Quantum Services**. This allows SASE to share identity information via Identity and Trust to Quantum Security Gateway to enable identity-based rules across SASE and Quantum services. ■ **SASE Audit Logs integrated with Infinity Audits** SASE audit logs are now part of, and integrated into **Infinity Platform Audits**. You can now export these logs via Infinity to SIEM systems. ■ **Internet Access Threat Prevention Security Profiles** Administrators can now define enforcement behavior and configure Threat Prevention blades (including Malware Protection, Anti-Bot, Threat Emulation) to match their security posture and operational needs. **Minimum agent version required**: • Windows: 12.3.0.10 • macOS: 12.3 ■ **Internet Access Threat Prevention Exceptions** Administrators can now define granular exceptions for specific URLs or files using SHA-256 identifiers. This capability reduces false positives while maintaining strong enforcement. **Minimum agent version required**: • Windows: 12.4 • macOS: 12.3

New Features	■ **New Role - Security Manager** A new **Security Manager** role is now available in the platform to support more granular role-based access control. Users with this role can: • Manage Internet Access configurations • Define Data Loss Prevention (DLP) policies • Monitor and investigate security events ■ **MSSP / Infinity – Granular Role Support for MSSP Parent Users** The Check Point Portal now supports additional SASE service roles for MSSP Parent users, enabling granular, role-based access beyond the previously Admin-only model. This enhances security and governance through least-privilege access and clearer separation of duties. With this release, MSSPs can assign the following SASE roles to their users, either directly or via Infinity User Groups: • Security Manager • Network Manager • User Manager • Admin ■ **New SASE Points of Presence (PoPs)** SASE expanded global coverage with new PoPs in: • Istanbul (Turkey) • Auckland (New Zealand) • Montréal (Canada) ■ **Enhanced Networks** Enhanced Networks is now available in US,EU, and AU data residencies and on-demand in India (IN). This feature provides: • Higher network scale • Improved resilience • Simplified networks and tunnels management For more information, see Enhanced Network. ■ **DLP Enhancements** Data Loss Prevention (DLP) now includes: • Data Type Manager – Browse built-in data types (such as PII and payment data) and create custom data types. **Minimum agent version required**: Windows and macOS: 11.7 • Services column in the DLP policy – Configure more granular DLP rules for web categories, custom URLs, applications. • Apply DLP policy on downloaded files. For more information, see Data Loss Prevention. ■ **Okta SCIM App – Regional Support Expansion**

	SASE's Okta application (SCIM integration) now supports **India (IN)** and **Australia (AU)** regions. Customers whose SASE tenant resides in these regions can connect their Okta IDP (with SCIM enabled) using the built-in Okta app. ■ **Web Categories – New Gen AI Category** A new **URL Filtering (URLF) Gen AI** web category is now available. This category: • Supports all policies that allow categories selection (Access, Bypass, DLP) • Provides visibility for generative-AI destinations
Enhancements	■ **Internet Access Rules – UX Improvements** Improvements to Internet Access policy management aimed at large enterprise rule sets, including: • Safer defaults to reduce new rule misconfiguration • Faster access to detailed rule view (quick access / one-click view) • Easier management of large selectors ■ **Trusted Networks – Certificate Validation Hardening** Trusted Networks configuration has been strengthened by removing the option to skip certificate validation, reducing risk from weak or misconfigured trust settings.
Resolved Issues	N/A

November

Early Availability	■ **Agent UI Controls** Administrators can now hide the **Reset Agent** button from end-users on SASE Windows and macOS agents.

New Features	■ **Operational Events – General Availability (GA)** Operational events and tunnel logs are now available across all regions in Events & AIOps, giving administrators unified visibility and faster troubleshooting for their SASE deployment. ■ **Tenant Restrictions – General Availability (GA)** Tenant Restrictions are now in GA, enabling organizations to limit access to approved SaaS tenants only. This feature prevents users from signing in to personal or untrusted tenants. The supported applications are: • Microsoft Office 365 • Google Workspace For more information, see Tenant Restrictions. ■ **Data Loss Prevention (DLP) for File Uploads – General Availability (GA)** DLP for file uploads is now in GA on all environments. Administrators can detect and block sensitive data being uploaded to cloud services, helping protect confidential information and support regulatory compliance. For more information, see Data Loss Prevention.
Enhancements	■ **Improved Split Tunnelling Resilience** When **Split Tunnelling** is enabled, network configuration changes now occur more smoothly, significantly reducing the chance of VPN interruptions during maintenance operations. **Note** - This feature is available on Windows and macOS agents, version 12.2 or higher. ■ **Scalability and Performance for Large Deployments** Multiple backend and UI optimizations improve performance and responsiveness in large environments, including: • Faster loading of route tables and network routes. • More efficient handling of tenants with very large firewall rule sets. These improvements help administrators manage complex environments with less waiting and fewer timeouts. ■ **Stronger Device Posture** • Device Posture Check - Added **Microsoft Defender** to the list of supported Endpoint Security products for macOS, improving device compliance validation options. ■ **Better Renewal Experience** The in-product renewal banner now appears **45** days before subscription renewal, giving administrators more time to plan renewals and avoid service disruption.
Resolved Issues	N/A

October

New Features	■ **Parent-MSP Access**: SASE now supports administrative access inheritance from a parent MSSP Infinity account to its child accounts through **User Groups**. **Note** - Currently supports **Admin** roles only, via **Global** or **Service-Specific** Roles. ■ Operational events and tunnel logs are now integrated to and available in Events & AIOps. ■ **Device Posture Check (DPC) Empty State Improvements**: Added an interactive **DPC** widget to the **Device Inventory** dashboard, offering quick links and guidance to help users enable Device Posture Check. ■ **Public API Support for Split Tunnelling**: Added support for managing split tunnelling configurations via Public API. ■ Desktop devices are now labeled as **Computer** to align with industry standards.
Enhancements	N/A
Resolved Issues	N/A

September

Early Availability	■ Operational events and tunnel logs are now integrated to and available in Events & AIOps. ■ A new Device Posture Check (DPC) feature offers full device certificate validation. Administrators can now verify authenticity, validity, and private key matching to strengthen overall device security and compliance. This feature requires Windows agent version 12.0.
New Features	■ **SaaS API** in SASE is now available in Australia and India. ■ Introduced **Tenant Restrictions** to control user access to approved Office 365 and Google Workspace tenants. For more information, see Tenant Restrictions.
Enhancements	■ Improved handling of disconnection issues during network configuration updates. ■ UI changes to support large-scale organizations.
Resolved Issues	N/A

August

Early Availability	■ **Data Loss Prevention (DLP) Support for File Uploads** Added Data Loss Prevention (DLP) support for file uploads to detect and block sensitive data exfiltration. ■ **Enhanced Application Control** Enhanced granularity in Application Control with new actions to block file uploads to Box and Google Drive.
New Features	N/A
Feature Enhancements	■ **Support for enterprise clients** Admins can now manage members in large groups, exceeding 500 users. ■ **Support for device isolation** *(Available for Windows and macOS devices with agent version 11.6 and higher)* Admins can now add an extra preventive security layer for devices by blocking all local network (LAN) traffic when the device is connected to the VPN. This isolates the device from nearby devices, reducing risks such as lateral movement or exposure to unsafe local traffic. Outbound communication to external resources and the public internet remains unaffected. For more information, see *"Device Isolation" on page 102*. ■ **Firewall logs location change** Firewall logs have moved to the new **Unified Logs/Security Events** page in **Events & AIOps**, which allows users to: • View logs across all Check Point products in a centralized location • Search, filter, and analyze events for faster threat detection and response • Automate workflows using Playblocks and Event Forwarding • Send automated notifications for SASE via email, SMS, Slack, and Microsoft Teams using Playblocks • Export events using Check Point Infinity's Event Forwarding
Resolved Issues	■ P81-72299 - Address issue where connection would drop after 1 hour due to session validation issues

July

Early Availability	■ **Check Point Enterprise Browser with Surf Security Integration** This release introduces **SSO connectivity** from SASE to the Surf Security admin platform, along with browser-level Zero Trust Access (ZTA) enforcement. Surf Security provides agentless protection for unmanaged devices, offering features such as session recording, screen capture prevention, and device posture checks. For more information, see: • Enterprise Browser • SASE_enterprise_browser_fov.pdf • SASE_enterprise_browser_wpr.pdf ■ **Internet Access - Tenant Restrictions** Added support for tenant restrictions in Office 365 and Google Workspace. This feature allows access only to organization-approved tenants, blocking personal and unauthorized corporate accounts to prevent data leakage and unapproved external collaboration. For more information, see Tenant Restrictions.
New Features	N/A
Feature Enhancements	■ Increased Active Directory (AD) domain support in Device Posture Check (DPC) from **2** to **10** domains. ■ Renamed the **Unified Logs** page to **Security Events**.

Resolved Issues	■ P81-67049 - Fixed an issue that allowed bypassing account activation via the 'Forgot Password' link ■ P81-70003 - Fixed allow rule not applying when followed by overlapping block rules ■ P81-70004 - Resolved sorting behavior on the applications page ■ P81-71453 - Resolved Unified log view filtering and pagination issues ■ P81-71936 - Resolved an issue where viewing request details in the Integration settings failed with an error when accessing older events ■ P81-72305 - Fixed errors when adding access policy rules with custom URLs ■ P81-72981 - Fixed an issue where logging was missing for allowed traffic under Internet Access allow rules ■ P81-73019 - Fixed an issue where users with admin or manager roles could not view the Access History section under Support Access ■ P81-74452 - Fixed issues with group-based settings failing for large groups in the Support Access page ■ P81-74768 - Resolved an issue where firewall filter for Members does not show results

June

New Features	■ New Point-of-Presence (PoP) in Taipei, expanding coverage and enhancing performance. For full list of cloud locations, see *"Regions and Point-of-Presence" on page 157*.
Feature Enhancements	■ Revised Members page - Added support for large-scale user management. ■ A new panel for user and group selection is now available on the right side of the interface, providing better support for large directories and an enhanced search experience. ■ You can now add up to **10** individual users per firewall rule. For larger groups, use user groups for easier management.
Resolved Issues	■ P81-70311 - Users removed from a group in Okta are now correctly unassigned from the corresponding group in SASE.

May

New Features	■ **Added New Data Residencies: Australia and India** SASE is now available in the Check Point Portal in two new data residencies, **Australia** and **India**, in addition to the existing US and EU options. This expansion supports customers with regional data residency requirements and broadens our global reach. See the blog post. ■ **New iOS Agent with Check Point Mobile Protect available on the App Store** The latest iOS agent is now live on the App Store and available from the **Downloads** page in SASE. The new version: • Integrates Mobile Security Protect security features with SASE Private Access connectivity. • Requires a Mobile Security Protect license. ■ **Internet Access – Allow Logs now available** Administrators can now view **Allow** logs for Internet Access policies, in addition to existing block and alert logs. This enhancement improves visibility of permitted user activity and helps with auditing and troubleshooting. Available on agent version 11.5 or above. **Note** - This feature may generate a high volume of logs. ■ **Internet Access Logs integrated with Events & AIOps and SIEM Export Support** • All security engines in Internet Access, such as URL Filtering, Anti-Virus, and Anti-Bot, now send logs to Infinity Events, providing centralized and real-time visibility across your SASE deployment. • You can now export logs to your SIEM solution via Syslog from Events & AIOps. This enables streamlined incident response, threat hunting, and compliance reporting by integrating SASE logs into your existing security workflows. **Note** - Configuration for SIEM export is available in the Check Point Portal. For more information, see the Infinity Portal Administration Guide. ■ **Agent Anti-Tampering** Anti-tampering is now supported (available on agent version 11.5 and above). Uninstalling the agent requires a code, preventing unauthorized removal. ■ **Internet Access Transparent Installation** A new transparent install capability allows Internet Access protection to be applied immediately upon agent installation, without requiring user login. This ensures instant security for internet traffic. For more information, see Transparent Internet Access Installation.

Feature Enhancements	■ **Trusted Networks Enhancement** Trusted networks can now be identified using an HTTPS server, providing more flexible and secure detection mechanisms. ■ **Unified Log View** SASE introduces a redesigned log screen that aligns with Events & AIOps, delivering a unified and consistent log experience across platforms to enhance visibility and simplify analysis.
Early Availability	**Improved security visibility by capturing only events blocked by firewall rules** Key features: ■ **Improved Visibility** - Only events that are blocked by firewall rules are logged, helping you quickly identify and troubleshoot unauthorized access attempts. ■ **Network-Level Control** - Logging can be enabled or disabled at the network level directly from the Firewall configuration page, allowing for granular logging based on specific network needs. ■ **Log Access** - You can view the logged events in: • SASE Unified Logs • Infinity Events page To enable firewall logs, contact *Check Point Support*.
Resolved Issues	N/A

April

New Features	■ Added API support for managing Zero Trust applications. For more information, refer to the API documentation. ■ Updated the default bypass rules in SASE to align with the standard configuration used in Check Point Quantum Security Gateway. See sk163595. ■ SASE network or user managers inherit their role from Check Point Check Point Portal. We now support service roles for network and user managers. ■ Firewall events are now presented in the Events & AIOps application in the Check Point Portal (Early Availability). This enables customers to consolidate logs from all Check Point Portal applications in a single location.

Feature Enhancements	■ SASE strengthens security for locally defined users by enabling two-factor authentication (2FA) by default for newly created tenants. ■ Group naming becomes more flexible now, allowing names to include special characters for groups synced via SCIM. ■ Firewall policy action names and images are aligned with Check Point's terminology and standards, using **Drop** and **Accept**, instead of Deny and Allow.
Resolved Issues	■ P81-64882 - Resolved an issue where enabling two-factor authentication (2FA) for Azure IDP disrupted the login flow. ■ P81-63630 - Firewall events log page fails from time to time. ■ P81-66970 - Admin user deletion is audited on the admin activity log. ■ P81-67091 - Resolved an issue affecting groups synchronized from Azure, where users were not being added to groups as expected, and existing group memberships were removed.

March

Early Availability Programs	Early availability programs for upcoming SASE enhancements: 1. **Agent 11.5 – Enhanced Security, Control, and Usability** The latest Agent 11.5 update introduces multiple improvements to security, policy enforcement, and user experience. **What's New**: ▪ **New Threat Prevention Policy** – Includes threat emulation, anti-bot, and malware protection, with the flexibility to enable or disable as needed. ▪ **Trusted Networks via HTTPS Server** – Define trusted networks based on an HTTPS server, enhancing security posture. ▪ **URL Filtering Log Support** – Enables logging for better visibility and analysis of URL filtering actions (Allow or Deny). ▪ **Application Control Enhancements** – Administrators can now regulate the use of SaaS applications, ensuring compliance and security by allowing, blocking, or restricting specific applications based on policies. This helps prevent unauthorized access, control bandwidth usage, and enforce corporate security guidelines. ▪ **Transparent Internet Access Installation** – This is a simplified deployment with seamless internet access configuration. For more information, see Deploying the Check Point SASE Agent. ▪ **Enhanced Anti-Tampering Protection** – Agent exit code protection now also applies to uninstallation, preventing unauthorized removal. ▪ These updates enhance security, visibility, and ease of management for administrators. 2. **Site Security** - Strengthening protection and policy enforcement for remote locations. 3. **Next-Generation Networking (NGN)** – Advancing network performance and security for modern enterprise needs. Admins can now gain early access to NGN capabilities and provide feedback before the general release. To participate, contact your Check Point representative. **What's New**: ▪ **Single Public IP per Region** – Simplifies management by eliminating the need to handle individual gateway IPs. ▪ **Enhanced IPSec Tunnels** – Supports up to eight parallel tunnel legs for improved redundancy, link aggregation, and streamlined IPSec configuration.

New Features	■ New Point-of-Presence (PoP) in Zurich, Switzerland, expanding coverage and enhancing performance. ■ SASE now features a redesigned log screen that matches the look and feel of Events & AIOps. This update provides a seamless and consistent experience across platforms, enhancing visibility and simplifying log analysis.
Feature Enhancements	N/A
Resolved Issues	■ P81-61595 - Learn More text was truncated when duplicating a custom URL.

February

New Features	■ New PoP in Brussels - Launched a new Point of Presence (PoP) in Brussels, Belgium, expanding coverage and enhancing performance.
Feature Enhancements	■ Hybrid-Split Tunneling Enhancement - Administrators are now guided to configure automatic split tunneling for optimal traffic routing. Existing configurations are migrated automatically with no impact on current networks. ■ Microsoft Outlook is now excluded by default from Internet Access bypass rules. ■ Administrators can now manage the multi-monitor settings for ZTA RDP applications. ■ Improved security warning when disabling 2FA for local users. Administrators can now see a clear notification highlighting the security risks before confirming the action.
Resolved Issues	■ P81-55537 - Bypassed URLs are now case-insensitive, ensuring consistent enforcement regardless of letter casing.

January

New Features	■ The new **Hybrid Split Tunneling** functionality automates tunneling of private traffic only, ensuring an optimized end-user experience along with full connectivity (Currently available in Early Availability) ■ Added two new predefined member roles, **Network Manager** and **User Manager**, for simplified management. These roles simplify permissions setup, enhance security, and improve access control. For more information, see Member Roles and Permissions. ■ Added the new **Explore Check Point SASE** page that helps customers discover and understand SASE features. It guides them to enhance their security posture, manage SASE effectively, and follow best practices with video guides and tips. ■ SaaS is now accessible through Check Point SASE, offering enhanced security for your SaaS applications. Make sure you have the appropriate license to fully utilize Check Point SaaS. For more information, refer to the Check Point SaaS solution brief (Currently available in Early Availability) ■ Wildcard support is now available for URL Filtering rules, offering greater flexibility and efficiency. Use the * wildcard to match multiple URLs with similar patterns (for example, **.example.com* covers all subdomains and paths under example.com). For more information, see the blog post.
Feature Enhancements	N/A
Resolved Issues	N/A

2024

December

New Features	■ Enhanced admin experience for managing groups – While assigning new members to a group, the **Assign new members** pane now supports improved search and scrolling, enabling easier navigation and management of groups with a large number of members. ■ The Internet Access policy is now distributed to end users more efficiently and at a larger scale, ensuring quicker updates and improved performance. ■ Introduced an enhanced **Get Started** wizard for Private Access Onboarding. ■ Admins can now view the workspace name from the main dashboard. For example, a workspace name is required for agent installation.
Feature Enhancements	N/A
Resolved Issues	■ P81-55727 - Retrieving custom properties for ZTA Dynamic RDP can end up with a timeout.

November

New Features	■ **IDP Okta integration supports EU region** - IDP Okta now supports tenants and workspaces configured in the EU region. For more information, see here. ■ **Customer Admin Role** - MSP admins can now create and manage granular access policies for child accounts.
Feature Enhancements	N/A
Resolved Issues	■ P81-50352 - Deleted user groups are now visually distinguished on the User Groups page. ■ P81-54824 - Positioning of addresses combo box and drop-down list is fixed, ensuring the appropriate controls' layout. ■ P81-55740 - Resolved an issue that caused a "Cross origin login not allowed" error, blocking platform access after sign-up.

October

New Features	■ **MSP Child Tenant Allocation** - Managed Service Providers (MSPs) can now manage access permissions for specific child tenants within their partner organization. This allows MSPs to control and allocate access for team members, ensuring that only authorized personnel can manage designated child tenants, enhancing security and streamlining tenant administration. ■ You can now avail a 30-day free trial of the complete SASE platform.
Feature Enhancements	N/A
Deprecations	■ Configuring members' image is now deprecated.
Resolved Issues	■ P81-51616 - Clicking on Device Name leads to the proper page, based on the tenants' licensing. ■ P81-52473 - Logging out when using Google SSO, logs out Google account entirely. ■ P81-52796 - Auto logout at 3am, doesn't work when session duration is set to 24 hours. ■ P81-54660 - Firewall logs not generated for rules created by API ■ P81-54685 - Disable Sign-out option not available ■ P81-51935 - ZTA application fails to load after gateway upgrade

September

New Features	■ **Native RDP support** - This feature enables users to connect to agentless applications through their native RDP client. It now offers improved performance, multi-monitor support, and clipboard and printing controls for a more seamless experience. ■ **Personal RDP for agentless application access** – Generates personalized RDP access based on the user's IDP attributes. It is available for beta customers. ■ **Copilot available for Check Point SASE** - Administrators can now consult the **Infinity AI Copilot** within the Infinity Portal for topics related to Check Point SASE. We have trained our LLM model on our SASE documentation and it currently supports queries on an array of Check Point SASE topics, including setup, configuration, features, best practices, and more. ■ Allow usage of single IP Address in Redundant IPSec tunnel.
Feature Enhancements	N/A

Resolved Issues	■ P81-51169 - Improved policy editing for a smoother user experience. ■ P81-51040 - Allow the admin to unblock a user when the user is signed in to multiple tenants. ■ P81-51187 - Active sessions now accurately display detailed user information for VPN-connected sessions, while addressing previous discrepancies.

August

New Features	■ Bundle of SASE with Browser Security is now GA. The service is available with a new SKU. ■ Enhanced session synchronization with the Check Point Portal.
Feature Enhancements	N/A
Resolved Issues	N/A

July

New Features	■ **MSPs Support**: • Support for PAYG plan for sub-tenants. • Support for MSPs with a large number of sub-tenants. ■ **Added new regions**: • New York 3, USA • London 3, UK • Sao Paulo 3, Brazil ■ Improved network operations infrastructure in APAC. ■ **Sign In** page now shows the data residency region in the Workspace drop-down list. ■ Updated the Wireguard connector script to support Ubuntu 24.04 LTS and future versions.
Feature Enhancements	N/A
Resolved Issues	■ P81-47263 - iPad agent is signed out the next day, in case it remained connected overnight ■ P81-48176 - SAML 2.0 IDP URL configuration now supports all valid domain extensions, allowing for broader customization

June

New Features	■ Added a new **Remove Device** action on the **Device Inventory** page, allowing Administrators to optimize device inventory by removing unused devices. ■ Partners can now create trial tenants for their customers with a 30-day free trial to evaluate SASE. When a partner creates a new trial workspace for a customer, select the **Premium+30 Day** trial plan. ■ Improved Gateway geographic location announcements (RFC 9092)
Feature Enhancements	N/A
Resolved Issues	■ P81-46499 - Active user sessions, accessible from the dashboard, now display the correct country under Session Origin. ■ P91-46780 - Device posture check (DPC) for Mac agents is compatible with Check Point's End Point process names.

May

New Features	A new **Browser Security** menu is now available (in Beta). It supports the new *Internet Security Essentials+* offering which includes the Browser Security browser extension.
Feature Enhancements	N/A
Resolved Issues	■ P81-42112 - Can't create a group where the name contains ":" ■ P81-46478 - Can't create a network with /22 subnet ■ P81-39418 - Can't update Configuration profile

April

New Features	SASE now supports EU data residency, using a separate new instance of the platform.
Feature Enhancements	■ Aligned Web Filtering category names to Check Point standard categories. ■ Added support for **Specific Service Roles** in the Check Point Check Point Portal, so users with a Read-Only role in the portal can be given an Admin role specifically for SASE. ■ Implemented minor UI fixes.
Resolved Issues	N/A

March

New Features	N/A
Feature Enhancements	■ Zero trust applications - Added an **Access for Members** button for admins to display the URL to be sent to users to allow access. ■ Further platform scalability improvements.
Resolved Issues	■ P81-38343 - Networks tab - 'undefined' error

February

New Features	■ SWG certificates for macOS can now be installed using MDM tools. This allows administrators to configure SWG (Internet Access) seamlessly for macOS devices using MDM tools without user intervention. The certificate can be generated and downloaded from the tenant **Downloads** page. **Check Point SASE** Agent for macOS version 10.4 and above supports this functionality.
Feature Enhancements	■ Two-Factor authentication improvements: • Added support for Duo Security Universal Prompt. • Changed verbiage to better reflect the support for different TOTPs such as Microsoft Authenticator and Google Authenticator. ■ IDP/SCIM Integration - Added support for syncing user names which include commas. ■ Web Activity page: • Log data in the table is now updated when changing selection in the widgets. • Improved display for deleted users. ■ Scalability improvements in the web platform to support large customers.
Resolved Issues	N/A

January

New Features	■ Rebranded to **Check Point SASE** and changed to the **Harmony** pillar in Check Point Infinity Portal.
Feature Enhancements	■ SCIM Group Sync for Okta is now available to all customers.
Resolved Issues	N/A

Check Point SASE Agent

- *"Windows" on page 1218*
- *"MacOS" on page 1229*
- *"Linux" on page 1238*
- *"iOS" on page 1242*
- *"Android / Chromebook" on page 1245*

Windows

12.7.4.14246

Release Date	20 April 2026
New Features	N/A
Enhancements	N/A
Resolved Issues	N/A
Updates	Updated Malware Protection engine components.
Status	Under gradual rollout to all customers.
Download Agent	Download

12.4.2.14245

Release Date	20 April 2026
New Features	N/A
Enhancements	N/A
Updates	Updated Malware Protection engine components.
Resolved Issues	N/A

12.7.3.13958

Release Date	16 April 2026
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-109788 - VPN reconnection triggered by unrelated network changes. ■ P81-114498 - High memory usage by the agent service.

12.7.0.13190

Release Date	23 March 2026

New Features	■ **Indicator of Compromise (IOC) - Infinity Portal Management** The agent now supports Indicator of Compromise (IOC) management through the Infinity Portal. This enables centralized IOC policy handling across the organization. *(Available in Early Availability mode)* ■ **ARM64 Agent Support - Private Access** The agent now supports ARM64 devices (Windows on ARM), enabling Private Access connectivity on ARM-based hardware.
Enhancements	■ **Split Disable Sign-Out and Block Uninstall into Two Separate Controls** **Disable Sign-Out** and **Block Uninstall** are now independent controls, each with its own dedicated code and prompt, giving administrators more granular control over endpoint restrictions. *(Available in Early Availability mode)* ■ **Tenant Restrictions - Failed Login Attempt Logs** Logs are now generated for failed login attempts, giving administrators better visibility into unauthorized access attempts. ■ **HTTPS Inspection Allow Logs** Administrators can now enable logs for traffic bypassed from HTTPS inspection, making it easier to track what is excluded from inspection policies. ■ **Security Profiles** • File types are now grouped under file handling, with no constraints on using the Strict and Optimized built-in profiles. • Administrators can now log all Threat Emulation verdicts, including non-malicious files, for full inspection visibility. ■ **Split Tunnel Subnet Exceptions by IP or CIDR (Include Mode)** Administrators can define exceptions for included subnets using specific IP addresses or CIDR ranges. This excludes selected traffic from the tunnel and provides more granular routing control. *(Available in Early Availability mode)* ■ **Trusted Network 'Connect Anyway' Confirmation Pop-up** When a user on a trusted environment tries to connect to a private network, a confirmation pop-up now appears, helping avoid unnecessary VPN connections.
Resolved Issues	N/A

12.6.0.12786

Release Date	02 March 2026

New Features	■ **Block Websites with Invalid Certificates** Administrators can now enforce blocking of websites with invalid certificates (Expired, Revoked, Self-Signed, Untrusted), strengthening endpoint security and preventing end users from accessing potentially unsafe sites. (Available in Early Availability mode)
Enhancements	■ **Security Events Pop-Up Notification Control** Administrators can now disable and enforce security event pop-up notifications across their organization. By default, end users continue to receive notifications and can toggle this setting from the agent settings screen. (Available in Early Availability mode) ■ **Updatable Objects Support for Internet Access** Updatable Objects, which are dynamically maintained network objects that automatically update based on vendor-managed feeds, are now supported in Internet Access policies. (Available in Early Availability mode)
Resolved Issues	■ P81-103116 – Users could access blocked websites even though the Internet Access security policy was set to block them. ■ P81-102365 – Trusted network detection did not disable Internet Access protection when configured to do so.

12.5.0.11894

Release Date	9 February 2026
New Features	N/A
Enhancements	**Pre-Login Tunnel Creation** Allows users to establish a secure tunnel before OS login using a second device authentication. This enables seamless access to private organizational resources, such as Active Directory, even when working remotely or outside the corporate network. *(Available in Early Availability mode)*
Resolved Issues	■ P81-100329 – Agent uninstall using management tools triggers the anti-tampering mechanism ■ P81-85868 – Trusted network misdetection when switching between networks

12.4.1.12192

Release Date	11 February 2026
New Features	N/A

Enhancements	N/A
Resolved Issues	▪ P81-102296 - Browser shows error empty response while connected to Private network

12.4.0.10709

Release Date	26 December 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-87690 – Incorrect route table rules applied when using the OpenVPN protocol in split tunnel mode ▪ P81-86385 – Agent could become unresponsive when a user attempts to connect during an upgrade ▪ P81-86357 – Device Posture Status was not reflected in the management platform ▪ P81-85716 – Check Point SASE agent deployment via MECM failure

12.3.0.10330

Release Date	10 December 2025
New Features	N/A
Enhancements	▪ **Threat Prevention Security Profiles** These profiles introduce flexible security enforcement. Administrators can now define enforcement behavior and configure key Threat Prevention blades—including Malware Protection, Anti-Bot, and Threat Emulation—to align with their security posture and operational needs *(Available in Early Availability mode)* ▪ **Data Loss Prevention (DLP) Enhancements** DLP now includes: • **Data Type Manager** for fine-tuning data types. • A new **Services** column in the DLP policy for applying rules based on URL categories, applications, and custom URLs. These enhancements provide greater granularity and more precise enforcement. ▪ **Threat Prevention Exceptions** Administrators can now define granular exceptions for specific URLs or files, using SHA-256 identifiers. This provides precise control to handle trusted resources and to reduce false positives.
Resolved Issues	N/A

12.2.0.9608

Release Date	18 November 2025
New Features	N/A
Enhancements	■ Admins can now hide the **Reset Agent** button in the agent UI, preventing end-users from resetting the agent themselves
Resolved Issues	■ P81-85870, P81-77546 – False DPC result causes users to automatically sign-out ■ P81-85866 – Traffic redirection causing allowed URL's to get blocked

12.1.0.9079

Release Date	21 October 2025
New Features	N/A
Enhancements	■ **Idle Device Detection and Automatic Sign-Out** - The SASE agent now detects unattended devices and disconnect those users from your private resources, thereby protecting the company resources.
Resolved Issues	■ P81-75516 – Wrong trusted web server detection leading to VPN disconnection

12.0.0.8750

Release Date	29 September 2025
New Features	N/A
Enhancements	■ **Multi-language Support** - The agent now supports multi-language mode and is fully localized in French. Users can set the language through: • User settings • Automatically by the OS language • Installation parameters ■ **Device Posture Check (DPC)** - A new DPC feature offers full device certificate validation. Administrators can now verify authenticity, validity, and private key matching to strengthen overall device security and compliance ■ **Granular DLP Policy Control** - Enhanced DLP policy granularity by adding a new dimension - **service**. It allows administrators to select web categories, URLs or applications *(Available in Early Availability mode)*

Resolved Issues	■ P81-72328 – Trusted network detected while connected to a regular network ■ P81-76823 – Failure to get URL reputation categorization

11.7.0.2606

Release Date	28 July 2025
New Features	N/A
Enhancements	■ Transparent Internet Access protection now supports deployment through Mobile Device Management (MDM) for domain users, even if you do not provide the user's email address. ■ Switch user event tracking and monitoring allows better security event tracking and accurate policy enforcement on shared devices. ■ Agent anti-tampering mechanism now also protects SASE agent processes and services from being terminated *(Available in Early Availability mode)* ■ Added Data Loss Prevention (DLP) support for file uploads to detect and block sensitive data exfiltration *(Available in Early Availability mode)* ■ Introduced Tenant Restrictions to control user access to approved Office 365 and Google Workspace tenants. This helps to prevent data leaks and shadow IT *(Available in Early Availability mode)* ■ Enhanced Application Control granularity with new actions to block file uploads to Box and Google Drive *(Available in Early Availability mode)*
Resolved Issues	■ P81-67078 – Similar Device ID causes fail in multiple devices sign-in ■ P81-67952 – Uninstallation code request pop-up not presented ■ P81-69474 – Resources connectivity issue when failing to disable IPv6

11.6.0.2555

Release Date	21 May 2025
New Features	N/A

Enhancements	■ A new option allows SASE agent's Internet Access protection to be disabled when the device is connected to a secured trusted network, to avoid duplicate traffic inspection. ■ Device isolation from Local Area Network (LAN) is now available as a new option to enhance device security. *(Available in Early Availability mode)* ■ Customization of Block/Warn pages is now available, allowing tailored messages for end-users.
Resolved Issues	■ P81-62620, P81-62633 – Private DNS resolve issues ■ P81-65145 – User can disconnect while always-on mode in enabled ■ P81-69416 – Split Tunnel FQDN entries resolve issues

11.5.0.2501

Release Date	27 March 2025
New Features	N/A
Enhancements	■ A new option is available to install the SASE agent, enabling Internet Access security to start working out of the box without user interaction. ■ The new Application control security engine allows managing and restricting applications on end-user protected devices. ■ URL Filtering **Allow** logs - SASE now collects and stores **Allowed** end-user browsing history in Admin portal. ■ The Agent anti-tampering feature now allows administrators to enforce an admin code requirement to uninstall the SASE agent. ■ URL Filtering, Malware Protection, Anti-Bot, and Threat Emulation logs are now available on Events & AIOps and in a new **Unified Log viewer** screen. These logs can also be exported to SIEM systems via Events & AIOps.
Resolved Issues	■ P81-56886, P81-61354 – Unable to access specific internal resources (DNS resolve error) ■ P81- 62195 – Agent connectivity problems with local Wi-Fi network

11.2.1.2378

Release Date	22 January 2025
New Features	N/A
Enhancements	■ New Anti-Bot security engine detects and prevents access to malicious URLs. ■ New Threat Emulation engine uses connected sandboxes to prevent multi-stage attacks at the earliest available stage.

Resolved Issues	■ P81-53008 – Long VPN connection time post device reboot ■ P81-53330 – DNS connectivity loss post network connection ■ P81-54570 – Some deny logs does not appear in management platform ■ P81-55316 – Trusted environment users are presented in platform as VPN connected users

11.1.0.2248

Release Date	12 November 2024
New Features	N/A
Enhancements	■ Enhanced Trusted Network capability, now supporting the use of an HTTPS server and a TLS certificate ■ Implemented a comprehensive update to our Malware protection engine
Resolved Issues	■ P81-47954 - Users experience BSOD ■ P81-51792 - Device status does not updates after sleep when connected to trusted router

11.0.11.2205

Release Date	16 October 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-54903 - User gets stuck in obtaining an IP address mode

11.0.10.2177

Release Date	30 September 2024
New Features	N/A
Enhancements	■ Added support for wildcards in URL filtering rules
Resolved Issues	■ Updated vulnerable library (CVE-2024-21907) ■ P81-48205 - Unable to remove configured default DNS

11.0.1.2083

Release Date	28 August 2024

New Features	N/A
Enhancements	N/A
Resolved Issues	■ Mitigation for OpenVPN vulnerability (CVE-2024-1305) ■ P81-50980 - Custom URL SWG allow rule mismatch

11.0.0.2050

Release Date	30 July 2024
New Features	N/A
Enhancements	■ Implemented a comprehensive update to our Web filtering security engine. ■ Rebranded the task bar icons. ■ Rebranded **Block**, **Warn**, and **Malware Protection** pages. ■ Renamed installation file from *Perimeter81_10.x.x.xxxx.msi/exe* to *HarmonySASE11.x.x.xxxx.msi/exe* ■ Bug fixes and stability improvements.
Resolved Issues	■ P81-36415 - Agent not opening channel ■ P81-38160 - Unexpected Timeout On Agent ■ P81-38285 - Stuck in Connecting State when on Trusted Routers ■ P81-42138 - Windows 10.5 Web activity doesn't log events when signed out ■ P81-42248 - Windows agent installer deploys with older .net8 version ■ P81-46702 - Windows agent connected to EU platform is not showing the GW IP but the native IP address ■ P81-47192 - SWG not blocking site

10.5.2.1979

Release Date	28 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-47112, P81-47119, P81-47205 - Latency issue with Citrix and RDP

10.5.1.1790

Release Date	20 May 2024

New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-37892 - Compatibility with N-Able Web protection ■ P81-38465 - Windows 11 machines BSOD with specific netio.sys with DRIVER_IRQL_NOT_LESS_OR_EQUAL ■ P81-39767 - SWG events initially not sent correctly after switching to a workspace in a different region

10.5.0.1760

Release Date	29 March 2024
New Features	Secure Web Gateway (which includes Web Filtering and Malware Protection) now stays active even when the user is signed out of the agent, using the most recently cached web filtering policy. The user interface has been updated to show that the SWG is enabled in this situation. If allowed by the admin, the SWG can be turned off by quitting the agent.
Enhancements	■ The agent supports the new European Data Residency instance of Check Point SASE, which will be launched in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ■ Improved, simplified connection logic and refactoring for speed. ■ Agent logging events have been moved to a new, robust and more scalable infrastructure. ■ Improvements to the Web Filtering category resolving mechanism. ■ .Net version updated to 8.0. ■ The agent is now signed with a Check Point certificate instead of a Perimeter 81 certificate.
Resolved Issues	■ P81-27360 - DNS resolution issue when using split tunneling + Custom DNS ■ P81-35882 - Latency in video calls (Zoom, Google Meet) ■ P81-36299 - Web Filtering rule with all categories is applied partially ■ P81-38526 - Memory used by agent grows over time

10.4.3.1672

Release Date	27 February 2024
New Features	N/A
Enhancements	N/A

Resolved Issues	P81-37301 - Compatibility issue with external DNS filtering tool

10.4.2.1645

Release Date	29 January 2024
New Features	N/A
Enhancements	The Perimeter 81 agent is now rebranded to Check Point - Harmony SASE.
Resolved Issues	N/A

MacOS

12.7.4.9577

Release Date	20 April 2026
New Features	N/A
Enhancements	N/A
Updates	Updated Malware Protection engine components.
Resolved Issues	N/A
Status	Under gradual rollout to all customers.
Download Agent	Download

12.7.3.9355

Release Date	16 April 2026
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-114498 – High memory usage by the agent service.

12.7.0.8565

Release Date	17 March 2026
New Features	▪ **Indicator of Compromise (IOC) - Infinity Portal Management** The agent now supports Indicator of Compromise (IOC) management through the Infinity Portal. This enables centralized IOC policy handling across the organization. *(Available in Early Availability mode)*

Enhancements	■ **Split Disable Sign-Out and Block Uninstall into Two Separate Controls** **Disable Sign-Out** and **Block Uninstall** are now independent controls, each with its own dedicated code and prompt, giving administrators more granular control over endpoint restrictions. *(Available in Early Availability mode)* ■ **Tenant Restrictions - Failed Login Attempt Logs** Logs are now generated for failed login attempts, giving administrators better visibility into unauthorized access attempts. ■ **HTTPS Inspection Allow Logs** Administrators can now enable logs for traffic bypassed from HTTPS inspection, making it easier to track what is excluded from inspection policies. ■ **Security Profiles** • File types are now grouped under file handling, with no constraints on using the Strict and Optimized built-in profiles. • Administrators can now log all Threat Emulation verdicts, including non-malicious files, for full inspection visibility. ■ **Split Tunnel Subnet Exceptions by IP or CIDR (Include Mode)** Administrators can define exceptions for included subnets using specific IP addresses or CIDR ranges. This excludes selected traffic from the tunnel and provides more granular routing control. *(Available in Early Availability mode)* ■ **Trusted Network 'Connect Anyway' Confirmation Pop-up** ■ When a user on a trusted environment tries to connect to a private network, a confirmation pop-up now appears, helping avoid unnecessary VPN connections.
Resolved Issues	■ P81-105963 - Unable to collect logs when the agent is in signed-out state. ■ P81-87418 - Keychain corruption affecting agent connection.

12.6.0.8419

Release Date	05 March 2026
New Features	■ **Block Websites with Invalid Certificates** Administrators can now enforce blocking of websites with invalid certificates (Expired, Revoked, Self-Signed, Untrusted), strengthening endpoint security and preventing end users from accessing potentially unsafe sites. *(Available in Early Availability mode)*

Enhancements	■ **Security Events Pop-Up Notification Control** Administrators can now disable and enforce security event pop-up notifications across their organization. By default, end users continue to receive notifications and can toggle this setting in the agent settings screen. *(Available in Early Availability mode)* ■ **Updatable Objects Support for Internet Access** Internet Access policies now support dynamically maintained network objects that automatically update based on vendor-managed feeds. *(Available in Early Availability mode)*
Resolved Issues	■ P81-103116 – Users could access blocked websites even though the Internet Access security policy was set to block them. ■ P81-102365 – Trusted network detection did not disable Internet Access protection when configured to do so.

12.5.1.8141

Release Date	13 February 2026
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-99418 - Agent takes a long time to open when DNS addresses are blocked on the local firewall. ■ P81-89899 - Agent fails to parse DNS packets, causing issues with Split Tunneling.

12.3.0.7524

Release Date	20 January 2026
New Features	N/A

Enhancements	■ **Threat Prevention Security Profiles** - These profiles introduce flexible security enforcement. Administrators can now define enforcement behavior and configure key Threat Prevention blades–including Malware Protection, Anti-Bot, and Threat Emulation–to align with their security posture and operational needs *(Available in Early Availability mode)* ■ **Data Loss Prevention (DLP) Enhancements** DLP now includes: • **Data Type Manager** for fine-tuning data types. • A new **Services** column in the DLP policy for applying rules based on URL categories, applications, and custom URLs. These enhancements provide greater granularity and more precise enforcement. ■ **Threat Prevention Exceptions** - Administrators can now define granular exceptions for specific URLs or files, using SHA-256 identifiers. This provides precise control to handle trusted resources and to reduce false positives.
Resolved Issues	■ P81-86793 - User couldn't connect to VPN although Always-on was enabled ■ P81-83839 - Agent failed routing Split-tunneled traffic correctly

12.2.0.6683

Release Date	19 November 2025
New Features	N/A
Enhancements	■ Admins can now hide the **Reset Agent** button in the agent UI, preventing end-users from resetting the agent themselves

12.1.0.6369

Release Date	29 October 2025
New Features	N/A
Enhancements	■ **Idle Device Detection and Automatic Sign-Out** - The SASE agent now detects unattended devices and disconnects those users from your private resources, thereby protecting company's resources. ■ Renamed application name from **Perimeter81.app** to **Check Point SASE.app**
Resolved Issues	■ P81- 81220 - Agent IA certificate installation requires admin’s credentials ■ P81-84212 - Frequent agent disconnections from the network

12.0.0.6063

Release Date	29 September 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-75099 - User cannot sign in to agent due to DPC failure

12.0.0.6019

Release Date	8 September 2025
New Features	N/A
Enhancements	■ Multi-language Support - The agent now supports multi-language mode and is fully localized in French. Users can set the language through: • User settings • Automatically by the OS language • Installation parameters ■ Device Posture Check (DPC) - A new DPC feature offers full device certificate validation. Administrators can now verify authenticity, validity, and private key matching to strengthen overall device security and compliance ■ Granular DLP Policy Control - Enhanced DLP policy granularity by adding a new dimension - **service**. It allows administrators to select web categories, URLs or applications *(Available in Early Availability mode)*
Resolved Issues	■ P81-77570 - Wrong Split-tunnel routes creation while using OpenVPN ■ P81-77781 - Agent fails to search system domains through, causing DNS to fail unless using FQDN

11.7.0.5477

Release Date	6 August 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-69837 – Split-tunnel traffic goes through VPN tunnel

11.7.0.5310

Release Date	4 August 2025
New Features	N/A
Enhancements	■ Added Data Loss Prevention (DLP) support for file uploads to detect and block sensitive data exfiltration (Available in Early Availability mode) ■ Introduced Tenant Restrictions to control user access to approved Microsoft Office 365 and Google Workspace tenants. This helps to prevent data leaks and shadow IT (Available in Early Availability mode) ■ Enhanced Application Control granularity with new actions to block file uploads to Box and Google Drive (Available in Early Availability mode) ■ Agent to Platform communications have transitioned to port 443, enabling user policy updates and usage monitoring even on restricted networks.
Resolved Issues	■ P81-64450 – Regional Private DNS suffix does not match Check Point SASE suffix ■ P81-71325 – FQDN entries are not working while using split-tunnel

11.6.1.4855

Release Date	10 June 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-70427 – Private access connection lost in changing network event

11.6.0.4498

Release Date	28 May 2025
New Features	N/A

Enhancements	■ A new option allows SASE agent's Internet Access protection to be disabled when the device is connected to a secured trusted network, to avoid duplicate traffic inspection. ■ Device isolation from Local Area Network (LAN) is now available as a new option to enhance device security. *(Available in Early Availability mode)* ■ Customization of Block/Warn pages is now available, allowing tailored messages for end-users.
Resolved Issues	■ P81-63994 – Automatic user sign-out triggers internet disconnection ■ P81-68913 – Split Tunnel FQDN entries resolve issues

11.5.0.4178

Release Date	1 April 2025
New Features	N/A
Enhancements	■ A new option is available to install the SASE agent, enabling Internet Access security to start working out of the box without user interaction. ■ The new Application control security engine allows managing and restricting applications on end-user protected devices. ■ URL Filtering **Allow** logs - SASE now collects and stores **Allowed** end-user browsing history in Admin portal. ■ The Agent anti-tampering feature now allows administrators to enforce an admin code requirement to uninstall the SASE agent. ■ URL Filtering, Malware Protection, Anti-Bot, and Threat Emulation logs are now available on **Events & AIOps** and in a new **Unified Log viewer** screen. These logs can also be exported to SIEM systems via Events & AIOps.
Resolved Issues	■ P81-52669, P81-62196 - Unable to access specific internal resources (DNS resolve error)

11.2.1.3411

Release Date	22 January 2025
New Features	N/A

Enhancements	■ Enhanced Trusted Network capability, now supporting the use of an HTTPS server and a TLS certificate. ■ Implemented a comprehensive update to the Malware protection engine. ■ New Anti-Bot security engine detects and prevents access to malicious URLs. ■ New Threat Emulation engine uses connected sandboxes to prevent multi-stage attacks at the earliest available stage.
Resolved Issues	■ P81 - 51175 – SWG not active after reboot ■ P81 - 54570 – Some deny logs do not appear in management platform

11.0.10.2696

Release Date	21 October 2024
New Features	N/A
Enhancements	■ Added support for wildcards in URL filtering rules ■ Renamed installation file from **Perimeter81_10.x.x.xxxx.pkg** to **Check Point_SASE_11.x.x.xxxx.pkg**
Resolved Issues	■ P81-51175 - Agent failed to start URL filtering after reboot ■ P81-50195 - Agent blocked downloads from IBM aspera ■ P81-37249 - User can't run FaceTime calls when URL filtering feature is enabled

11.0.1.2339

Release Date	28 August 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ Mitigation for OpenVPN vulnerability (CVE-2024-1305) ■ P81-50980 - Custom URL SWG allow rule mismatch

11.0.0.2227

Release Date	7 August 2024
New Features	N/A

Enhancements	■ Implemented a comprehensive update to our Web filtering security engine. ■ Rebranded the taskbar icons. ■ Rebranded **Block**, **Warn**, and **Malware Protection** pages.
Resolved Issues	■ P81-37479 - Quick access UI disappear ■ P81-37717 - Failed to connect to private access network ■ P81-38526 - Agent memory usage ■ P81-39300 - Agent frequent disconnects ■ P81-40851 - Can't remove Trusted Wi-Fi from Trusted network list ■ P81-46855 - Changing network requires device admin's permission ■ P81-46907 - Agent unexpected crashes

10.5.0.1476

Release Date	29 March 2024
New Features	Secure Web Gateway (which includes Web Filtering and Malware Protection) now stays active even when the user is signed out of the agent, using the most recently cached web filtering policy. The user interface has been updated to show that the SWG is enabled in this situation. If allowed by the admin, the SWG can be turned off by quitting the agent.
Enhancements	■ The agent supports the new European Data Residency instance of Check Point SASE, which will be launched in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ■ Agent logging events have been moved to a new, robust and more scalable infrastructure.
Resolved Issues	■ P81-37479 - UI is hidden on mouse cursor move when an application is running full-screen in the background ■ P81-37735 - Unable to connect to the agent when Mac has Homebrew installed

10.4.2.1198

Release Date	29 January 2024
New Features	N/A
Enhancements	The Perimeter 81 agent is now rebranded to Check Point SASE.
Resolved Issues	N/A

Linux

10.0.6.996

Release Date	20 April 2026
New Features	N/A
Enhancements	N/A
Updates	Updated Malware Protection engine component.
Resolved Issues	N/A
Download Agent	Download

10.0.5.962

Release Date	19 February 2026
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-93494 – The SWG certificate is now automatically installed in the Fedora Linux system trust store. P81-86379 – Split-tunnel rules are not respected when using the OpenVPN protocol.

10.0.4.947

Release Date	19 November 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-78129 - Users unable to connect to Private access

10.0.3.933

Release Date	30 June 2025
New Features	N/A
Enhancements	■ Implemented a remote sign-in mechanism that allows administrators to sign in Private Access (PA) users on Linux devices and terminals using Command Line Interface (CLI) commands.
Resolved Issues	N/A

10.0.2.915

Release Date	23 April 2025
New Features	N/A
Enhancements	■ The SASE application now stores support logs directly on the device.
Resolved Issues	■ P81-60958, P81-63177 - Private network connection in Split-tunnel mode leads to DNS resolve errors ■ P81-63178 - Internal routes access issues

10.0.1.885

Release Date	30 December 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-58390 - Login fail in ubuntu 20.04.6 ■ P81-59734 - Split tunnel include mode bug on private DNS

10.0.0.879

Release Date	04 December 2024
New Features	■ Support for split tunneling configuration by domains (FQDN)
Enhancements	N/A
Resolved Issues	N/A

9.0.1.843

Release Date	03 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-46506 - apt remove perimeter81 could delete /home/user folder when specific chars are used ■ P81-46999 - Errors when uninstalling from terminal

9.0.0.832

Release Date	24 April 2024
New Features	■ The Perimeter 81 agent is now rebranded to Check Point - SASE. This includes new logos and a new color scheme. ■ Secure Web Gateway (SWG) now includes Malware Protection. SWG users now have an additional layer of protection against malicious software, on top of the existing web filtering functionality. Malware Protection actively scans content before it reaches the user's browser, blocks multiple types of threats, and notifies the user. Admins can view logs of blocked malware in a new page under the **Monitor & Logs** section.
Enhancements	■ The agent supports the new European Data Residency instance of Check Point SASE, launched earlier in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ■ The agent now reports the exact Linux distribution (Ubuntu 23.04) in the **Device Inventory** page. Also, the agent version number now has a lin_ prefix to align the versioning with the other operating systems.
Resolved Issues	■ P81-37246 - Agent not displaying DPC failure notifications ■ P81-34266 - SWG bypass rule not being respected ■ P81-40066 - Issue connecting to shared networks with openVPN protocol ■ P81-41876 - RHEL & Fedora - issue connecting with split tunneling enabled

8.1.0.778

Release Date	23 November 2023
New Features	N/A
Enhancements	Deprecated IKEv2 protocol as a method of agent connection and removed it from the agent UI

Resolved Issues	■ P81-24634, P81-26185 - Agent is stuck while connecting ■ P81-26613 - Connection takes too long ■ P81-27881 - Agent disconnects and connects constantly ■ P81-27963 - Agent crashes after 8 hours ■ P81-28239 - Unable to connect to network until restarting helper service + crashes ■ P81-29403 - Agent is failing to launch on Fedora 38 ■ P81-28797 - When returning from sleep, agent does not reconnect to VPN ■ P81-34181 - Issue when updating UI to latest version on RHEL

iOS

8.4.1.5570

Release Date	12 August 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-55367 - Agent Public IP stuck on refreshing mode ■ P81-63047 - Network connection button disabled for no reason ■ P81-70203 - Device network change disconnects agent connection
Download Agent	Download

8.4.0.4488

Release Date	13 May 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-63047 - User is unable to connect to private networks

8.3.0.2600

Release Date	25 September 2024
New Features	N/A
Enhancements	■ New application icon
Resolved Issues	■ P81-48119 - App stuck in loading page

8.2.0.1934

Release Date	13 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-47262 - App stuck on splash screen

8.1.0.1831

Release Date	03 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-30654 - Agent keeps disconnecting and reconnecting ■ P81-46602 - OS version is displayed incorrectly in the Device Inventory page

8.0.0.1730

Release Date	12 May 2024
New Features	N/A
Enhancements	■ The agent is now rebranded to Check Point - Check Point SASE. ■ The agent supports the new European Data Residency instance of Check Point SASE. ■ The agent now blocks usage on jailbroken devices.
Resolved Issues	■ P81-30654 - Agent keeps disconnecting and reconnecting ■ P81-42234 - When typing the sign-out code, digits are not visible in dark mode ■ P81-42091 - Private DNS icon is not displayed in the agent

7.0.6.1

Release Date	01 August 2023
New Features	N/A
Enhancements	N/A

Resolved Issues	■ P81-14047 - Agent does not open on iPad ■ P81-12409 - AppStore crash reports ■ P81-7559 - Occasional disconnections during long sessions ■ P81-7245 - Wrong app version shown in Monitoring Dashboard ■ P81-5900 - Issue logging out users by the workspace admin ■ P81-3133 - 'Login error. Failed to establish SDP socket connection' when no Internet connection is available ■ P81-2676 - Automatic Wi-Fi Security doesn't work on unsecured networks ■ P81-2396 - Device Posture Check - the user isn't signed out when DPC failed (but still cannot connect) ■ P81-2359 - No autoconnect to the next network if existing network was deleted, while AlwaysOn is enabled ■ P81-1956 - VPN does not connect automatically when signing in ■ P81-1542 - Auto Reconnect value is set to OFF on every disconnect when changing networks

Android / Chromebook

8.2.0.3395

Release Date	2 November 2025
New Features	N/A
Enhancements	■ Android 15 support
Resolved Issues	■ P81-81556 – User gets 'device limit reached' message when trying to sign in
Download Agent	Download

8.1.3.3382

Release Date	7 August 2025
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-27822 – Chromebook fail to connect RDP ZTA ■ P81-64191 – Application freezes on launch

8.1.2.3355

Release Date	29 November 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	■ P81-47928 - Nonresponsive connect button during agent installation on Chromebook

8.1.0.3337

Release Date	25 September 2024
New Features	N/A
Enhancements	■ Android 14 support ■ New application icon
Resolved Issues	N/A

8.0.0.3276

Release Date	9 April 2024
New Features	N/A
Enhancements	■ The agent is now rebranded to Check Point - SASE. ■ The agent supports the new European Data Residency instance of SASE. ■ IKEv2 protocol deprecated as a method of agent connection - removed from agent UI.
Resolved Issues	■ P81-33813 - Users can't connect Agent using Android - Job Cancellation Exception ■ P81-34474 - Obfuscation of data

7.1.9.2577

Release Date	13 February 2024
New Features	N/A
Enhancements	■ Updated reconnection logic. ■ Improved logging. ■ When the user session expires (according to the session length set by the administrator), the agent automatically logs out during local night time, to avoid disconnections during the workday. This applies to session lengths of two days and higher. ■ Prevent usage on rooted devices.
Resolved Issues	■ P81-19677 - StackOverflowError in Sets.kt ■ P81-18833 - Failed to login with 'Too Many Open Sessions' error ■ P81-18608 - Agent does not present 'All the time' option in Location Permissions, causing disconnects when idle

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.