

Hybrid Mesh Network Security

01 October 2026

CHECK POINT SD-WAN

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2023 - 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.



Check Point Check Point SD-WAN Administration Guide

For more about this release, see the home 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.

Revision History

Date	Description
01 October 2026	Updated: ■ Early Availability Features are now offered only over the R82.20 release
13 September 2026	Updated (moved these features from Early Availability to General Availability in R82.20): ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* ■ *"SD-WAN in Layer 2" on page 281* ■ *"SD-WAN Overlay ECMP and Symmetric Overlay Return" on page 286* ■ *"SD-WAN Steering Enforcement when Selected Links are Down" on page 290* Removed these features as deprecated: ■ EA Feature: SD-WAN with a Traditional VSX Virtual System ■ EA Feature: SD-WAN with SmartLSM (SmartProvisioning)
07 September 2026	Updated: ■ *"SD-WAN Connection Type - "Overlay"" on page 200* ■ *"SD-WAN Limitations" on page 30* ■ *"Troubleshooting SD-WAN Installation" on page 321* ■ *"Step 3 - Configuration on Security Gateways" on page 83*
21 July 2026	Updated: ■ *"SD-WAN Limitations" on page 30*
16 July 2026	Updated: ■ *"SD-WAN Limitations" on page 30*
25 May 2026	Updated: ■ *"SD-WAN Limitations" on page 30*
14 May 2026	Added: ■ *"SD-WAN Steering Enforcement when Selected Links are Down" on page 290* ■ *"SD-WAN Overlay ECMP and Symmetric Overlay Return" on page 286*

Date	Description
27 April 2026	Updated: ■ Early Availability Features are now offered only over the R82.10 release
09 April 2026	Updated: ■ *"SD-WAN Symmetric Packet Return" on page 257*
18 March 2026	Updated: ■ *"SD-WAN NAT for ISP" on page 271*
25 February 2026	Updated: ■ *"Configuring a Maestro Security Group for SD-WAN" on page 113*
16 February 2026	Updated: ■ *"Configuring Steering Behavior" on page 171* ■ *"Troubleshooting SD-WAN "Overlay"" on page 340*
15 February 2026	Added: ■ *"EA Feature: IPv6 in SD-WAN" on page 309* Updated: ■ *"SD-WAN NAT for ISP" on page 271*
29 January 2026	Added: ■ *"SD-WAN Settings Profile" on page 296* Updated: ■ *"Configuring SD-WAN Policy" on page 160* ■ *"Troubleshooting SD-WAN Installation" on page 321*
21 January 2026	Updated: ■ *"Troubleshooting SD-WAN "Local Breakout Only"" on page 329*
21 January 2026	Added: ■ *"Troubleshooting traffic that does not match SD-WAN rules" on page 377*

Date	Description
24 December 2025	Updated: ■ *"Troubleshooting SD-WAN "Overlay"" on page 340* ■ *"Troubleshooting SD-WAN with Kernel Debug" on page 385*
15 December 2025	Updated: ■ *"Step 2 - Configuration on the On-Premises Management Server" on page 71*
12 December 2025	Updated: ■ *"Troubleshooting SD-WAN "Local Breakout Only"" on page 329*
27 October 2025	Updated: ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* - updated the title ■ *"SD-WAN Symmetric Packet Return" on page 257* ■ *"Troubleshooting SD-WAN Installation" on page 321* ■ *"Configuring Steering Behavior" on page 171*
28 September 2025	Updated: ■ EA Feature: SD-WAN with a Traditional VSX Virtual System - Virtual Systems do not support FEC
23 September 2025	Updated: ■ *"SD-WAN Service GUI" on page 42*
21 September 2025	Added: ■ *"SD-WAN in Layer 2" on page 281* Updated: ■ *"SD-WAN Limitations" on page 30* ■ *"Configuring Steering Behavior" on page 171*
09 September 2025	Updated: ■ *"Licensing the SD-WAN Product" on page 33*

Date	Description
17 July 2025	Added: ■ *"EA Feature: QoS in SD-WAN" on page 301* Updated: ■ *"WAN Link Mapping" on page 207* - the page design was changed
14 July 2025	Updated: ■ *"Step 2 - Configuration on the On-Premises Management Server" on page 71* ■ *"Step 2 - Configuration in Smart-1 Cloud" on page 121* ■ *"Step 3 - Configuration on Security Gateways" on page 83* ■ *"Step 3 - Configuration on Security Gateways" on page 130* ■ *"Configuring Steering Behavior" on page 171* - in Quality Check Methodology, added Multiple Target Probing (MTP) - previously, the Early Availability feature ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* - added the procedure forSpark Firewall Appliances
26 June 2025	Updated: ■ *"Step 2 - Configuration on the On-Premises Management Server" on page 71* ■ *"Step 2 - Configuration in Smart-1 Cloud" on page 121* ■ *"SD-WAN Service GUI" on page 42* - the widget was renamed from "Steering Objects" to "Steering Object Usage Breakdown" ■ *"SD-WAN Monitoring" on page 212* - the widget was renamed from "Steering Objects" to "Steering Object Usage Breakdown"

Date	Description
09 June 2025	Updated: ■ Changed the term from "Overlay - VPN" to "Overlay" ■ *"Step 3 - Configuration on Security Gateways" on page 83* "Part 2 - Configuration of SD-WAN interfaces on the Security Gateway" • Procedure for a Security Gateway that runs Gaia OS ◦ Improved the notes about the options **Directly accessible** and **Accessible via NAT** • Procedure for Spark Firewall Appliance that runs Gaia Embedded OS ◦ Updated the steps on the **Connection Monitoring** tab ■ *"Configuring Steering Behavior" on page 171* • Updated the notes for the field **Check interval** ■ *"SD-WAN Connection Type - "Overlay"" on page 200* ■ *"SD-WAN Configuration for DAIP Security Gateways" on page 220* ■ *"The "Monitor" View" on page 45* • Updated the titles of the tabs ■ *"Monitoring SD-WAN Status in Check Point Portal" on page 212* • Updated the titles of the tabs
04 June 2025	Updated: ■ *"Configuring a Maestro Security Group for SD-WAN" on page 113* (Early Availability Feature) ■ EA Feature: SD-WAN with a Traditional VSX Virtual System ■ EA Feature: SD-WAN with SmartLSM (SmartProvisioning) ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* ■ EA Feature: Quality Check Methodology - Multiple Targets for Probing
14 May 2025	Updated: ■ *"Configuring a Maestro Security Group for SD-WAN" on page 113* (Early Availability Feature) ■ EA Feature: SD-WAN with a Traditional VSX Virtual System ■ EA Feature: SD-WAN with SmartLSM (SmartProvisioning) ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* ■ EA Feature: Quality Check Methodology - Multiple Targets for Probing

Date	Description
13 May 2025	Added: ■ *"Configuring a Maestro Security Group for SD-WAN" on page 113* (Early Availability Feature) ■ EA Feature: SD-WAN with a Traditional VSX Virtual System ■ EA Feature: SD-WAN with SmartLSM (SmartProvisioning) ■ *"SLA-Based Prioritize Local Breakout in SD-WAN" on page 277* ■ EA Feature: Quality Check Methodology - Multiple Targets for Probing Updated: ■ *"SD-WAN DSCP" on page 275* ■ *"SD-WAN NAT for ISP" on page 271*
08 April 2025	Updated: ■ *"SD-WAN Limitations" on page 30* ■ *"SD-WAN Symmetric Packet Return" on page 257*
25 March 2025	Updated: ■ The Zone object "**Public Networks**" was renamed to "**SD-WAN Internet**" ■ The Zone object "**Private Networks**" was renamed to "**My VPN Domain & Peer VPN Domain**" ■ *"SD-WAN Service GUI" on page 42* ■ *"Licensing the SD-WAN Product" on page 33* - added information about an Evaluation License ■ *"Part 2 - Configure Object Sharing and Log Sharing" on page 72* ■ *"Configuring SD-WAN Policy" on page 160* ■ *"Troubleshooting SD-WAN "Overlay"" on page 340*
25 February 2025	Updated: ■ *"Part 2 - Configure Object Sharing and Log Sharing" on page 72* ■ *"Monitoring SD-WAN Status in Check Point Portal" on page 212*
28 January 2025	Added: ■ *"Route-Based VPN traffic that is routed towards a VTI is not encrypted and is sent in clear-text" on page 355* Updated: ■ *"SD-WAN FEC" on page 246*

Date	Description
12 January 2025	Updated: ■ *"SD-WAN NAT for ISP" on page 271*
01 January 2025	Updated: ■ *"CPView shows that the "Overlay" probing state is "DOWN"" on page 342*
30 December 2024	Updated: ■ *"SD-WAN DSCP" on page 275* - added the list of supported Security Gateways
24 December 2024	Updated: ■ *"Outbound Hide NAT" on page 55* ■ *"Additional Considerations" on page 62* ■ *"Step 3 - Configuration on Security Gateways" on page 83* ■ *"SD-WAN Connection Type - "Internet"" on page 188* ■ *"SD-WAN Connection Type - "Overlay"" on page 200* ■ *"Monitoring Overlay Tunnels in Check Point Portal" on page 214* ■ *"SD-WAN Best Practices" on page 235*
30 November 2024	Updated: ■ *"Troubleshooting SD-WAN "Overlay"" on page 340* - the scenario *"Expected VPN Transports to VPN Peers are missing from the list" on page 348*
19 November 2024	Updated: ■ *"Licensing the SD-WAN Product" on page 33* ■ *"SD-WAN Configuration for DAIP Security Gateways" on page 220* - moved some known limitations to the main SK article sk180605
13 November 2024	Updated: ■ *"Troubleshooting SD-WAN "Local Breakout Only"" on page 329* ■ *"Troubleshooting SD-WAN "Overlay"" on page 340*

Date	Description
11 November 2024	Added: ■ Moved all information from *sk181147: SD-WAN - Troubleshooting* to the chapter "*SD-WAN Troubleshooting*" Updated: ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ *"SD-WAN Connection (Steering Behavior) Types" on page 184* ■ *"Routing Preference "Backhaul Only"" on page 191* ■ *"Routing Preference "Prioritize Local Breakout"" on page 195* ■ *"SD-WAN Best Practices" on page 235* ■ *"SD-WAN Symmetric Packet Return" on page 257* ■ *"SD-WAN and Route-Based VPN" on page 266* ■ *"Troubleshooting SD-WAN "Overlay"" on page 340* ■ *"SD-WAN Configuration for DAIP Security Gateways" on page 220* - moved some known limitations to the main SK article sk180605
29 October 2024	Added: ■ *"SD-WAN NAT for ISP" on page 271* ■ *"SD-WAN DSCP" on page 275* Updated: ■ *"Configuring SD-WAN Policy" on page 160* ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ *"Routing Preference "Backhaul Only"" on page 191* ■ *"SD-WAN Best Practices" on page 235* ■ *"SD-WAN Symmetric Packet Return" on page 257* ■ *"SD-WAN and Route-Based VPN" on page 266*
12 September 2024	Added: ■ *"SD-WAN and Route-Based VPN" on page 266* Updated: ■ *"SD-WAN Terms" on page 35* ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ *"Configuring SD-WAN Policy" on page 160* ■ *"Configuring Steering Behavior" on page 171* ■ *"SD-WAN Symmetric Packet Return" on page 257*

Date	Description
26 August 2024	Updated: ■ *"SD-WAN Service GUI" on page 42* - updated the names of GUI elements ■ *"Configuring SD-WAN Policy" on page 160* - new Dynamic Objects ■ *"SD-WAN Symmetric Packet Return" on page 257* - minor textual corrections
23 August 2024	Added: ■ *"SD-WAN FEC" on page 246* ■ *"SD-WAN Symmetric Packet Return" on page 257* ■ *"SD-WAN Circuit ID" on page 248* Updated: ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ Workflow for an On-Premises Management Server: *"Step 3 - Configuration on Security Gateways" on page 83* - Part 4 - Configuration of the Security Gateway object in SmartConsole ■ Workflow for Smart-1 Cloud: *"Step 3 - Configuration on Security Gateways" on page 130* - Part 4 - Configuration of the Security Gateway object in SmartConsole ■ *"Configuring Steering Behavior" on page 171* - added "Selection Method" in "WAN Link Utilization" > "Link Aggregation" ■ *"Configuring Steering Behavior" on page 171* - added requirements for the HTTP probing protocol
12 August 2024	Updated: ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ *"Configuring Steering Behavior" on page 171* - added HTTP as the probing protocol

Date	Description
08 August 2024	Added: ■ *"Guidelines for Planning and Configuring SD-WAN" on page 49* ■ *"Licensing the SD-WAN Product" on page 33* Updated: ■ *"Getting Started with SD-WAN" on page 32* ■ *"SD-WAN Terms" on page 35* ■ Workflow for an On-Premises Management Server: • *"Step 2 - Configuration on the On-Premises Management Server" on page 71* • *"Step 3 - Configuration on Security Gateways" on page 83* ■ Workflow for Smart-1 Cloud: • *"Step 2 - Configuration in Smart-1 Cloud" on page 121* • *"Step 3 - Configuration on Security Gateways" on page 130* ■ *"Configuring SD-WAN Policy" on page 160* ■ *"Configuring Steering Behavior" on page 171* ■ *"SD-WAN Configuration for DAIP Security Gateways" on page 220* ■ *"WAN Link Mapping" on page 207* ■ *"Monitoring ISP Link Attributes in Check Point Portal" on page 214*
19 June 2024	Updated: ■ *"Introduction to SD-WAN" on page 24*
16 January 2024	Added: ■ *"SD-WAN Configuration for DAIP Security Gateways" on page 220*
23 December 2023	Added: ■ *"Upgrading an SD-WAN Security Gateway" on page 299*
05 October 2023	Updated: ■ Workflow for an On-Premises Management Server: *"Step 4 - SD-WAN Wizard" on page 111* ■ Workflow for Smart-1 Cloud: *"Step 4 - SD-WAN Wizard" on page 158*

Date	Description
07 September 2023	Updated: ■ The document structure to show the required steps for each workflow: • *"Workflow for an On-Premises Management Server" on page 67* • *"Workflow for Smart-1 Cloud" on page 118* ■ *"Getting Started with SD-WAN" on page 32* ■ *"SD-WAN Next Hop Probing on Cloud Firewall Gateways" on page 242*
05 July 2023	Added: ■ *"SD-WAN Connection Type - "Internet"" on page 188* The new connection type replaced these dedicated connection types: • Local Breakout • Backhaul Note - Check Point Portal migrated the previous connection types automatically. ■ Topic "SD-WAN Troubleshooting" Updated: ■ *"Introduction to SD-WAN" on page 24* ■ *"Configuring Steering Behavior" on page 171* ■ *"SD-WAN Connection (Steering Behavior) Types" on page 184* ■ *"The "Monitor" View" on page 45* - the "Logs" page - removed the limitation "Currently, this page shows the information only for the SD-WAN connection of type Local Breakout"
02 July 2023	Added: ■ *"SD-WAN GraphQL API" on page 298* Updated: ■ *"The "Support" View" on page 48* - added the "API" section ■ *"SD-WAN Configuration in Gaia Clish" on page 293* - corrected the syntax of "`next-hop`" in the "`add interface`" and "`set interface`" commands

Date	Description
01 June 2023	Updated: ■ Workflow for an On-Premises Management Server: *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Spark Firewall Appliances - added the note that VLAN interfaces are supported as SD-WAN interfaces ■ Workflow for Smart-1 Cloud: *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Spark Firewall Appliances - added the note that VLAN interfaces are supported as SD-WAN interfaces
30 May 2023	Updated: ■ *"Objects Supported in SD-WAN Policy" on page 169*
15 May 2023	Updated: ■ Workflow for an On-Premises Management Server: • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Security Gateways • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Spark Firewall Appliances ■ Workflow for Smart-1 Cloud: • *"Step 2 - Configuration in Smart-1 Cloud" on page 121* - procedure for Spark Firewall Appliances • *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Security Gateways
23 April 2023	Updated: ■ *"Getting Started with SD-WAN" on page 32* - added the note "See the **Limitations** section in sk180605" ■ Improved formatting in Workflow for an On-Premises Management Server: • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Security Gateways • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Spark Firewall Appliances ■ Improved formatting in Workflow for Smart-1 Cloud: • *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Security Gateways • *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Spark Firewall Appliances

Date	Description
20 April 2023	Updated: ■ Workflow for an On-Premises Management Server: *"Step 1 - Configuration in Check Point Portal" on page 68* - Part 2 Initial Configuration in Check Point Portal ■ Moved all limitations from this Administration Guide to the Home Page sk180605
17 March 2023	Added: ■ *"SD-WAN Best Practices" on page 235* Updated: ■ *"Introduction to SD-WAN" on page 24* ■ *"Getting Started with SD-WAN" on page 32* ■ *"SD-WAN Terms" on page 35* ■ *"SD-WAN Service GUI" on page 42* ■ Workflow for an On-Premises Management Server: • *"Step 1 - Configuration in Check Point Portal" on page 68* • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Security Gateways • *"Step 3 - Configuration on Security Gateways" on page 83* - procedure for Spark Firewall Appliances • *"Step 4 - SD-WAN Wizard" on page 111* ■ Workflow for Smart-1 Cloud" • *"Step 2 - Configuration in Smart-1 Cloud" on page 121* • *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Security Gateways • *"Step 3 - Configuration on Security Gateways" on page 130* - procedure for Spark Firewall Appliances • *"Step 4 - SD-WAN Wizard" on page 158* ■ *"Configuring SD-WAN Policy" on page 160* ■ *"SD-WAN Connection Type - "Overlay"" on page 200*
09 February 2023	First release of this document

Table of Contents

Introduction to SD-WAN ... *24*
SD-WAN Use Case ... *24*
Basic SD-WAN Action ... *24*
SD-WAN Policy ... *25*
Basic Workflow ... *29*
SD-WAN Limitations ... *30*
Getting Started with SD-WAN ... *32*
Licensing the SD-WAN Product ... *33*
Viewing the Current License for SD-WAN ... *33*
Associating the New License for SD-WAN ... *33*
Renewing the License for SD-WAN ... *33*
Evaluation License for SD-WAN ... *34*
SD-WAN Terms ... *35*
SD-WAN Service GUI ... *42*
The "Network" View ... *42*
The "Monitor" View ... *45*
The "Support" View ... *48*
The "Global Settings" View ... *48*
Guidelines for Planning and Configuring SD-WAN ... *49*
Public IP addresses that are not part of the Internet, but should be routed internally ... *50*
Inbound Non-Encrypted Traffic to Internal Servers ... *53*
Outbound Hide NAT ... *55*
Overlay ... *57*
VPN Community Settings ... *61*
Routes in Gaia / Gaia Embedded ... *62*
SD-WAN Interfaces in Gaia / Gaia Embedded ... *62*
Additional Considerations ... *62*

Workflow for an On-Premises Management Server ... 67
Step 1 - Configuration in Check Point Portal ... 68
Part 1 - Creating an Account in the Check Point Portal ... 68
Part 2 - Initial Configuration in Check Point Portal ... 70
What is Next? ... 70
Step 2 - Configuration on the On-Premises Management Server ... 71
Part 1 - Prerequisites for the Management Server ... 71
Part 2 - Configure Object Sharing and Log Sharing ... 72
What is Next? ... 82
Step 3 - Configuration on Security Gateways ... 83
Part 1 - Prerequisites for Security Gateways ... 83
Part 2 - Configuration of SD-WAN interfaces on the Security Gateway ... 84
Part 3 - Installation of the Nano-Agent on the Security Gateway ... 100
Part 4 - Configuration of the Security Gateway object in SmartConsole ... 104
Security Policy Installation Using SD-WAN Interface IP Addresses ... 105
Use Case ... 106
Updating SD-WAN Interface Information in the Security Management ... 106
Security Gateway Connectivity to Security Management ... 107
Part 5 - Configuration of VPN and Security Policy in SmartConsole ... 108
Part 6 - Configuration of Security Policy in SmartConsole ... 109
What is Next? ... 110
Step 4 - SD-WAN Wizard ... 111
Configuring a Maestro Security Group for SD-WAN ... 113
Supported Security Gateways ... 113
Prerequisites ... 113
Configuration ... 113
Workflow for Smart-1 Cloud ... 118
Step 1 - Configuration in Check Point Portal ... 118
Part 1 - Creating an Account in the Check Point Portal ... 118
Part 2 - Initial Configuration in Check Point Portal ... 120

What is Next? 120
Step 2 - Configuration in Smart-1 Cloud 121
Part 1 - Prerequisites for Smart-1 Cloud 121
Part 2 - Configure Configuration Sharing and Onboarding 123
What is Next? 129
Step 3 - Configuration on Security Gateways 130
Part 1 - Prerequisites for Security Gateways 130
Part 2 - Configuration of SD-WAN interfaces on the Security Gateway 131
Part 3 - Installation of the Nano-Agent on the Security Gateway 147
Part 4 - Configuration of the Security Gateway object in SmartConsole 151
Security Policy Installation Using SD-WAN Interface IP Addresses 152
Use Case 153
Updating SD-WAN Interface Information in the Security Management 153
Security Gateway Connectivity to Security Management 154
Part 5 - Configuration of VPN and Security Policy in SmartConsole 155
Part 6 - Configuration of Security Policy in SmartConsole 156
What is Next? 157
Step 4 - SD-WAN Wizard 158
Configuring SD-WAN Policy 160
Configuring SD-WAN Policy 160
Removing / Disabling SD-WAN Policy on the Security Gateway 162
Dynamic Objects in SD-WAN Policy 163
Objects Supported in SD-WAN Policy 169
Configuring Steering Behavior 171
SD-WAN Connection (Steering Behavior) Types 184
SD-WAN Connection Type - "Internet" 188
Routing Preference "Local Breakout Only" 188
Routing Preference "Backhaul Only" 191
Routing Preference "Prioritize Local Breakout" 195
SD-WAN Connection Type - "Overlay" 200

Diagram for "Overlay" ... 200
Use Case and Example for "Overlay" ... 201
Important Notes for "Overlay" ... 203
Traffic Flow in "Overlay" ... 206
Configuring Steering Candidates in "Overlay" ... 206
WAN Link Mapping ... **207**
SD-WAN Monitoring ... **212**
Monitoring SD-WAN Status in Check Point Portal ... 212
Monitoring ISP Link Attributes in Check Point Portal ... 214
Monitoring Overlay Tunnels in Check Point Portal ... 214
Monitoring SD-WAN Steering Events in Check Point Portal ... 215
Monitoring SD-WAN Traffic Logs in Check Point Portal ... 216
Monitoring SD-WAN Policy in Check Point Portal ... 217
Monitoring the Connected Security Gateways in Check Point Portal ... 218
Monitoring SD-WAN on the Security Gateway ... 219
SD-WAN Configuration for DAIP Security Gateways ... **220**
SD-WAN Requirements for DAIP Security Gateways ... 220
SD-WAN Support for DAIP Security Gateways ... 221
SD-WAN Known Limitations for DAIP Security Gateways ... 222
SD-WAN Configuration for DAIP Security Gateways ... 224
Part 1 - On a Security Gateway, configure the DAIP settings ... 224
Part 2 - In SmartConsole, configure the Security Gateway Object ... 227
Part 3 - In SmartConsole, configure the Access Control Policy ... 230
Part 4 - In Check Point Portal, configure the SD-WAN Policy ... 231
SD-WAN Troubleshooting for DAIP Security Gateways ... 233
SD-WAN Best Practices ... **235**
VPN - Link Selection ... 235
SD-WAN Policy - Rule Matching ... 236
SD-WAN Probing ... 238
Routes ... 245

SD-WAN Advanced Configuration ... *246*
SD-WAN FEC ... *246*
Introduction to FEC ... *246*
FEC Requirements ... *246*
FEC Configuration ... *246*
SD-WAN Circuit ID ... *248*
Overview ... *248*
How SD-WAN Uses the Circuit ID ... *250*
The Need to Override the Default the Circuit ID ... *251*
Configuring the Circuit ID ... *254*
SD-WAN Symmetric Packet Return ... *257*
Example SD-WAN Topology ... *257*
Traffic Flow Through an SD-WAN Security Gateway Without Symmetric Packet Return ... *258*
Traffic Flow Through an SD-WAN Security Gateway With Symmetric Packet Return *259*
SD-WAN and Route-Based VPN ... *266*
SD-WAN Rules and VTI Routing ... *266*
SD-WAN Policy Considerations for Route-Based VPN ... *267*
SD-WAN "Backhaul" and Route-Based VPN ... *268*
Considerations when the active default route is configured to the Center Gateway VTI ... *270*
SD-WAN NAT for ISP ... *271*
Introduction to NAT for each ISP ... *271*
Supported Security Gateways ... *271*
Configuring NAT for each ISP ... *271*
SD-WAN DSCP ... *275*
Introduction to DSCP ... *275*
Supported Security Gateways ... *275*
DSCP Classes ... *275*
DSCP Configuration ... *275*
SLA-Based Prioritize Local Breakout in SD-WAN ... *277*

SD-WAN in Layer 2 ... 281
Configuration ... 281
Step 1 - Configure the Next Hop ... 281
Step 2 - Configure Circuit ID Values ... 283
Step 3 - Configure WAN Link Mapping (only for Layer 2 peers) ... 285
CPView output ... 285
SD-WAN Overlay ECMP and Symmetric Overlay Return ... 286
Equal-Cost Multi-Path (ECMP) Routing for SD-WAN Overlay ... 286
Overview ... 286
Configuration ... 286
SD-WAN ECMP Behavior ... 287
Routing Behavior ... 287
Symmetric Return for Overlay Connections ... 288
Overview ... 288
Configuration ... 288
SD-WAN Steering Enforcement when Selected Links are Down ... 290
Overview ... 290
Behavior ... 290
SD-WAN Configuration in Gaia Clish ... 293
The "add" command ... 293
The "set" command ... 293
The "delete" command ... 293
The "show" command ... 294
Parameters for Gaia Clish Commands ... 295
SD-WAN Settings Profile ... 296
Overview ... 296
Configuration ... 296
SD-WAN GraphQL API ... 298
Upgrading an SD-WAN Security Gateway ... 299
Upgrading the Current Version ... 299

Clean Install of a New Version ... 300
Early Availability Features ... **301**
EA Feature: QoS in SD-WAN ... 301
Introduction to QoS in SD-WAN ... 301
Configuring QoS in SD-WAN ... 302
Example QoS Calculation ... 306
EA Feature: IPv6 in SD-WAN ... 309
Overview ... 309
Prerequisite ... 309
SD-WAN Behavior in IPv6 ... 309
IPv6 Support in SD-WAN Interfaces ... 310
Configuring SD-WAN Next Hop for IPv6 ... 310
Configuring "Accessible via NAT" ... 312
WAN Link Mapping ... 313
SD-WAN Policy Behavior with IPv6 ... 314
NAT per ISP with IPv6 ... 315
Monitoring and Statistics ... 316
Internal Architecture and Troubleshooting ... 317
SD-WAN Troubleshooting ... **321**
Troubleshooting SD-WAN Installation ... 321
Troubleshooting SD-WAN "Local Breakout Only" ... 329
Troubleshooting SD-WAN "Overlay" ... 340
Troubleshooting SD-WAN "Backhaul Only" / "Prioritize Local Breakout" ... 365
Troubleshooting SD-WAN in Check Point Portal ... 371
Troubleshooting traffic that does not match SD-WAN rules ... 377
Troubleshooting SD-WAN with Kernel Debug ... 385

Introduction to SD-WAN

With SD-WAN you can configure your Security Gateway / Cluster to steer traffic dynamically between the configured WAN Links based on the measured ISP link quality. This does *not* require dynamic routing configuration on your Security Gateway / Cluster.

With SD-WAN customers get the most efficient use of high-cost Wide Area Network connections and best user experience for consuming cloud-hosted services in branch offices.

The Security Gateway / Cluster sends different types of traffic through different Internet Service Providers (ISPs) based on application / identity and dynamic measurement of WAN Link characteristics.

The Security Gateway / Cluster applies the configured SD-WAN rules only if the Security Policy allows this traffic.

After you install the SD-WAN Policy, it becomes the main decision maker for traffic paths, traffic priorities, and so on for WAN connections. The SD-WAN policy makes these decisions based on the settings you configure in Check Point Portal.

For additional information, see sk180605.

SD-WAN Use Case

A Security Gateway is connected to two Internet Service Providers.

Traffic from the Zoom application goes to the Internet through ISP #1.

Traffic from the Outlook 365 application goes to the Internet through ISP #2.

Basic SD-WAN Action

You can use SD-WAN for:

- Local breakout – to control the steering and select the best path for outbound traffic to the Internet.
- Overlay – to control the best VPN path between VPN peers, for routing internal traffic between the organization sites, either from VPN Spokes to the Hub (Satellites to Center), or between VPN sites in a mesh topology.
- Backhaul - to route Internet traffic on VPN spoke sites through the Headquarters over the VPN tunnel. This connection uses the overlay-based connection from the Branch to the Center, and a Breakout-based connection from the Center to the Internet.

The Security Gateway uses the WAN Links you configured as SD-WAN interfaces, for Breakout (public SD-WAN interfaces) and for Overlay VPN (all SD-WAN interfaces).

SD-WAN Policy

The SD-WAN Policy contains these ordered rules:

1. **Classification of traffic:**
   - Source and Destination – IP address, Network address, User / Computer Identity.
   - Service or Application - `Zoom`, `Teams`, `https`, `ftp` (see *"Objects Supported in SD-WAN Policy" on page 169*).

     Note - The Security Gateway uses these heuristics to identify connections on the first packet:
     - DNS heuristic – The Security Gateway saves the DNS domains during the DNS query phase and associates the connection that follows with the applicable DNS domain.
     - SNI heuristic – The Security Gateway learns about HTTPS connections and applies the learned data to subsequent connections.
     - DPI heuristic – The Security Gateway applies Deep Packet Inspection to subsequent connections.

     As a result of these multiple heuristics, the Security Gateway might not detect the application on the first packet of its connection. For example, when two applications are hosted on the same server.

     Best Practice - Use Updatable Objects in the "**Destination**" column of the SD-WAN Policy. This allows matching of application connections on the first packet and most accurate traffic steering.

Example of an SD-WAN Policy

#	Name	Source	Destination	Services & Applications	Behavior
1	Teams	Net_ 192.168.20.0	`SD-WAN Internet`	`Microsoft Teams`	Aggregate
2	Zoom	Net_ 192.168.20.0	`Zoom Services`	`Any`	Prioritize_ WAN2
3	YouTube for Sales	SalesRole	`SD-WAN Internet`	`YouTube`	High_ Quality

- Rule #1 - For all traffic from the network 192.168.20.0/24 to the Internet, from the application with the signature of `Microsoft Teams`, apply the steering behavior "Aggregate".
- Rule #2 - For all traffic from the network 192.168.20.0/24 to IP addresses that are resolved from the Updatable object "`Zoom Services`", from any application, apply the steering behavior "Prioritize_WAN2".
- Rule #3 - For all traffic from users (IP addresses) determined by the Access Role "SalesRole" to the Internet, from the application with the signature of "`YouTube`", apply the steering behavior "High_Quality".

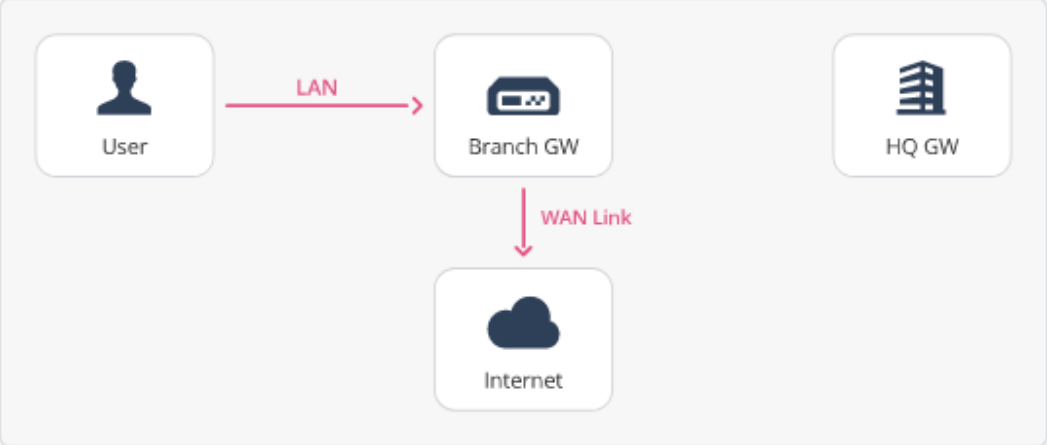
2. **Steering Behavior:**

   Steering tactics include a measurement target and a steering decision to select a WAN Link.

- Connection Type (Steering Behavior):
  - **"Internet" with "Local Breakout Only"**

    See *"Routing Preference "Local Breakout Only"" on page 188*.

    This connection type represents a direct WAN Link to the Internet.

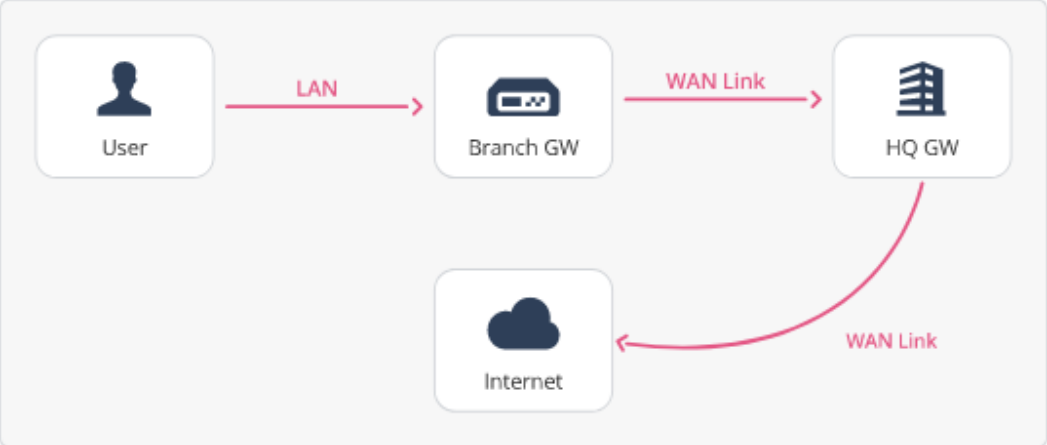
    

  - **"Internet" with "Backhaul Only"**

    See *"Routing Preference "Backhaul Only"" on page 191*.

    This connection sends traffic from VPN spoke sites to the Internet through the Central VPN hub site.

    This connection type enables the VPN spoke site to use the Public lines / Private lines to reach the Internet through the Headquarters.

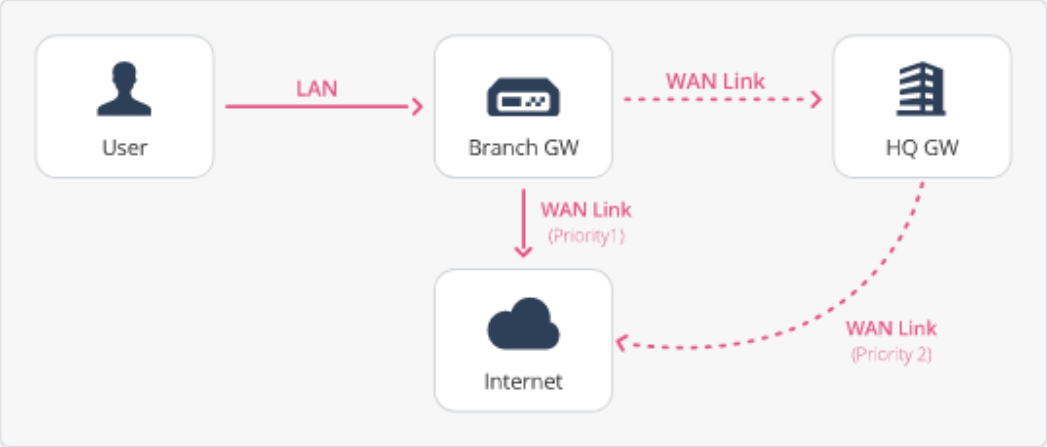
    

- **"Internet" with "Prioritize Local Breakout"**

  See *"Routing Preference "Prioritize Local Breakout"" on page 195*.

  This connection type gives priority to the direct WAN Link (not through the Headquarters) to send **all** traffic directly to the Internet.

  If **all** direct WAN Links to the Internet are down, the Security Gateway uses the direct WAN Link with encrypted traffic to the Headquarters to connect to the Internet.

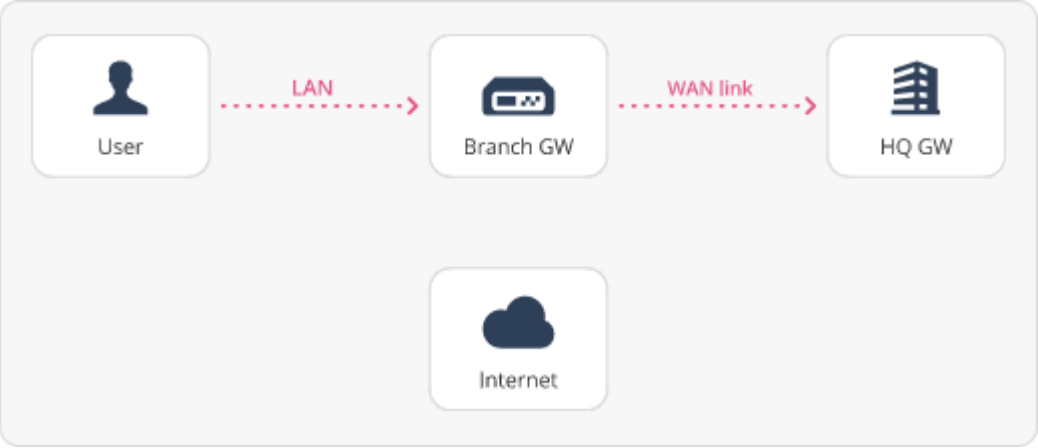


- **"Overlay"**

  See *"SD-WAN Connection Type - "Overlay"" on page 200*.

  This connection type represents a direct WAN Link with encrypted traffic to the Headquarters.

  The direct WAN Link with encrypted traffic to the Headquarters provides redundancy.



- Steering Criteria:
  - Select a better ISP Link based on Latency, Jitter, and Packet Loss.
  - Select a better ISP Link based on WAN Link utilization.

  You also configure the Quality Check methods to measure the ISP link quality.

Basic Workflow

To steer traffic with SD-WAN, you configure the required settings:

1. On the Security Gateway / each Cluster Member - The SD-WAN interfaces and the Nano-Agent.
2. In SmartConsole - The required objects and the connection to your account in Check Point Portal.

   In Smart-1 Cloud - The required objects.
3. In Check Point Portal - The required SD-WAN objects, WAN Link settings, and SD-WAN Policy.

SD-WAN Limitations

Limitations that are planned to be resolved:

See sk180605 > section "**Limitations**".

Limitations by design:

ID	Description
PMTR-115111	SD-WAN is not supported on Spark Firewall Appliances that use two SIM cards for one Cellular connection. In such a configuration, there are no two Internet Connections working at the same time, but rather a high availability of two Internet connections
PMTR-119509	SD-WAN is not supported on Standalone servers.
PMTR-105895	SD-WAN does not support ClusterXL in the Active-Active mode.
PMTR-105894	SD-WAN does not support ClusterXL in the Load Sharing Unicast mode. SD-WAN does not support ClusterXL in the Load Sharing Multicast mode.
PMTR-105215	SD-WAN does not support VPN "Overlay" with third-party VPN Peers (Check Point Firewall continues to use the existing Link Selection).

ID	Description
-	SD-WAN Overlay steering is supported only between VPN peers that meet **all** of these conditions: 1. Both VPN peers have SD-WAN enabled. 2. Both VPN peers are managed by the same Check Point Management Server. 3. Both VPN peers belong to the same Check Point Portal tenant. 4. Both VPN peers use the same SD-WAN management method (either from SmartConsole, or from Check Point Portal > SD-WAN App). If any of these conditions is not met, the VPN peers establish VPN tunnels according to the settings configured in SmartConsole > Security Gateway object > **IPSec VPN** section > **Enhanced Link Selection**/ **Link Selection** page.
PMTR-104985	SD-WAN does not support VPN Explicit Multiple Entry Point (MEP) configuration.
PMTR-109701	SD-WAN "Overlay" does not support configuring multiple Center gateways in a Star VPN Community with no satellites, when the "**Mesh center gateways**" option is enabled.
PMTR-104576	SD-WAN does not support VPN Permanent Tunnels.
PMTR-108281	SD-WAN does not support matching a "Local Breakout" rule to traffic in this scenario: 1. Traffic matches a Policy Based Routing (PBR) rule that applies to traffic from a local network to "Default", and the next hop in this rule is set to a VPN Tunnel Interface (VTI). 2. The priority of this PBR rule is lower than 100.

Getting Started with SD-WAN

Notes:

- We assume you are already familiar with the general configuration of Check Point on-premises Management Server and Security Gateways.
  See the *Security Management Administration Guide* for your version.
- To get familiar with the SD-WAN terms, see *"SD-WAN Terms" on page 35*.
- To get familiar with the SD-WAN GUI, see *"SD-WAN Service GUI" on page 42*.

Important - See the **Limitations** section in sk180605.

Getting Started Workflow:

1. Read sk180605 > section "**Limitations**".
2. Read *"Licensing the SD-WAN Product" on page 33*.
3. Read *"Guidelines for Planning and Configuring SD-WAN" on page 49*.
4. Follow the applicable deployment workflow:
   - *"Workflow for an On-Premises Management Server" on page 67*
   - *"Workflow for Smart-1 Cloud" on page 118*
5. Configure custom settings:
   a. *"Configuring SD-WAN Policy" on page 160*.
   b. *"Configuring Steering Behavior" on page 171*.
   c. *"WAN Link Mapping" on page 207*.
   d. *"SD-WAN Advanced Configuration" on page 246*.
6. Monitor your SD-WAN environment.

   Follow *"SD-WAN Monitoring" on page 212*.

Licensing the SD-WAN Product

Viewing the Current License for SD-WAN

1. Log in to *Check Point Portal*.
2. From the top toolbar, after the tenant name, click  and click **Services & Contracts**.

   This page shows all current subscriptions and services that are associated with your account.

Associating the New License for SD-WAN

1. You must follow these steps to associate the purchased SD-WAN subscriptions with your Check Point Portal Account:
   a. If you already have a *Check Point User Center* Account, then skip this step.

      Create a Check Point User Center Account and purchase SD-WAN subscriptions.

      Note - After you purchase SD-WAN licenses for your Security Gateways, Check Point updates your User Center Account with your new service subscriptions.

   b. Link your User Center Account with your Check Point Portal Account.

   c. Activate the SD-WAN service in Check Point Portal.

   For instructions, see the *Check Point Portal Administration Guide > Services & Contracts*.
2. In your User Center Account, you must associate the purchased SD-WAN SKU subscription with the specific Security Gateway.

Renewing the License for SD-WAN

If you renewed an SD-WAN subscription, it is necessary to synchronize your updated User Center Account with your Check Point Portal Account:

1. Log in to *Check Point Portal*.
2. From the top toolbar, after the tenant name, click  and click **Services & Contracts**.
3. In the top right corner, click the **Manage Accounts** link.

   The **Manage Accounts** window opens.
4. In the table row for the account, click **SYNC**.

Evaluation License for SD-WAN

You can request an evaluation license for the SD-WAN service in your active *Check Point User Center* account.

Check Point will then update your account with a 30-day evaluation license.

After this 30-day period, you will need to purchase a software license to continue using the product.

Warning - If you use the SD-WAN product without an active SD-WAN contract activated for you Check Point Portal Tenant, the log sharing for SD-WAN logs is not allowed. As a result, you are at risk of critical data loss.

1. Go to https://usercenter.checkpoint.com/ucapps/prodeval.
2. In the section **1 of 2 - Select Evaluation Product**:
   a. On the right side, select the radio button **OTHER EVALUTION OPTIONS**.
   b. Click **Select a product**.
   c. Search for **SD-WAN** and select **SD-WAN Evaluation**.
   d. In the bottom right corner, click **Select**.
   e. In the bottom right corner, click **Next**.
3. In the section **2 of 2 - Provide Evaluation Info**:
   a. In the **User Center Account** field, select the applicable account.
   b. In the **Evaluation Product will be used by** section, select the applicable option.
   c. In the **Purpose of Evaluation** section, select the applicable option.
   d. Select **I confirm and acknowledge that ...**.
   e. In the bottom right corner, click **Get Evaluation**.
4. Wait for the page to show the configuration and the evaluation steps.

SD-WAN Terms

Assets

Objects you configured on the on-premises Management Server or in Smart-1 Cloud.

These are objects of such types as **Security Gateway**, **Cluster**, **Host**, **Network**, **Service**, **Group**, **Address Range**, **Security Zone**, **Dynamic Object**, and so on.

Note - You can use these objects in the **Source** and the **Destination** columns of SD-WAN rules.

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Assets**.

Zones

Objects you configure in Check Point Portal. These objects are collections of assets.

The available Zones are:

- **SD-WAN Internet**
- **My VPN Domain & Peer VPN Domain**
- **Any**

Notes:

- You can use these objects in the **Source** and the **Destination** columns of SD-WAN rules.
- Object that represents the Internet:
  - If you do not use the SD-WAN Wizard, then to represent the entire Internet, you must manually create a **Zone** object called **SD-WAN Internet** (the object name is case-sensitive).
  - The SD-WAN Wizard creates this object automatically, if you configure the "Local Breakout".
- Object that represents all private networks:
  - If you do not use the SD-WAN Wizard, then to represent all private networks, you must manually create a **Zone** object called **My VPN Domain & Peer VPN Domain** (the object name is case-sensitive).
  - The SD-WAN Wizard creates this object automatically.
- In each **Zone** object (on the **General** tab), you must configure a logical query to match your assets:
  1. Click the left bar with three vertical dots to delete the query, or to create logical group of several queries ("`AND`", "`OR`").
  2. In the first field, select the applicable asset field.
  3. Click the middle bar with two vertical dots to select the match operation ("`Equals`", "`Not Equals`", "`In List`", "`Not In List`", "`Key Exists`").
  4. In the last field, enter the value to match.
- The SD-WAN Wizard creates the zone object "**My VPN Domain & Peer VPN Domain**" that matches these IP addresses:
  - from 10.0.0.0 to 10.255.255.255 (Class A)
  - from 172.16.0.0 to 172.31.255.255 (Class B)
  - from 192.168.0.0 to 192.168.255.255 (Class C)
- The SD-WAN Wizard creates the zone object "**SD-WAN Internet**" that matches these IP addresses:
  - from 0.0.0.0 to 9.255.255.255
  - from 11.0.0.0 to 126.255.255.255
  - from 127.0.1.0 to 172.15.255.255
  - from 172.32.0.0 to 192.167.255.255
  - from 192.169.0.0 to 255.255.255.255

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Zones**.

Applications

Predefined objects that exist in Check Point Portal.

These objects represent different applications that generate traffic (for example, Zoom, Gmail, Facebook).

Check Point updates the list of these applications in Check Point Portal.

Security Gateways get the updated identifications of these applications.

Services

A combination of predefined objects and user-defined objects (configured in SmartConsole).

These objects represent traffic over different protocols and ports.

WAN Links

Objects you configure in Check Point Portal.

These objects represent the Security Gateway's links to Internet Service Providers (ISPs).

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **SD-WAN Policy**.
3. From the top toolbar, click **WAN Link Mapping**.
4. From the top toolbar, click **Manage WAN Links**.

WAN Link Mapping

Configuration in Check Point Portal that controls the mapping of a WAN Link to a Security Gateway's interface based on the interface name, or a user-defined interface tag.

See *"WAN Link Mapping" on page 207*.

Note - An interface tag is an alternative name you can assign to an interface.
Example:
There are two SD-WAN Security Gateway peers that connect to the same two Internet Service Providers (ISPs).

- SD-WAN Security Gateway #1:
  - The interface `eth1` connects to ISP #1
  - The interface `eth2` connects to ISP #2
- SD-WAN Security Gateway #2:
  - The interface `eth3` connects to ISP #1
  - The interface `eth4` connects to ISP #2

To make it easier to configure and understand WAN Link Mapping, you can configure these interface tags:

- SD-WAN Security Gateway #1:
  - The interface `eth1` connects to ISP #1 - tag "`ISP1`"
  - The interface `eth2` connects to ISP #2 - tag "`ISP2`"
- SD-WAN Security Gateway #2:
  - The interface `eth3` connects to ISP #1 - tag "`ISP1`"
  - The interface `eth4` connects to ISP #2 - tag "`ISP2`"

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **SD-WAN Policy**.
3. From the top toolbar, click **WAN Link Mapping**.

Steering (Steering Behavior)

Configuration in Check Point Portal that controls how a Security Gateway must steer traffic based on:

- Applicable Internet Service Providers (ISPs)
- Latency, Jitter, Packet Loss of ISP Links
- WAN Link Utilization

See *"Configuring Steering Behavior" on page 171*.

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **SD-WAN Policy**.
3. From the top toolbar, click **Manage Objects**.

SD-WAN Policy

Set of steering rules that control how the Security Gateway steers the traffic for different applications and services to the Internet or Headquarters.

If a Security Gateway cannot find a match in this ordered policy, then:

- For connections that should not be encrypted, then Security Gateway uses the Gaia Operating System routing to forward the traffic.
- For connections that have be encrypted, then Security Gateway cannot use all available WAN Links to forward the traffic.

See *"Configuring SD-WAN Policy" on page 160*.

Important - SD-WAN Policy applies only if the Anti-Spoofing, the HTTPS Inspection Policy, the Access Control Policy, and Threat Prevention Policy allow the traffic.

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **SD-WAN Policy**.

Profiles

These are the available profile types:

- **Quantum Profile**

  This profile type uses a token to connect the Nano-Agent on the Security Gateway to Check Point Portal.

  Notes:
  - You can connect a Security Gateway only to one "**Quantum Profile**".
  - Make sure to configure the applicable maximum number of agents in the profile's "**Advanced**" settings.
  - The SD-WAN service creates this profile when you connect your Management Server to Check Point Portal.
    In addition, the SD-WAN Wizard makes sure this profile exists in the SD-WAN service.

  Best Practice - Connect all SD-WAN Security Gateways to the SD-WAN service in Check Point Portal with the same token (to make the policy configuration easier).

- **SD-WAN Profile**

  This is a logical profile type.

  This profile type contains a collection of manually selected Security Gateways. You can use this profile in the **Enforcement** column of each SD-WAN Policy rule.

  Note - You can connect a Security Gateway to more than one "**SD-WAN Profile**".

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Profiles**.

Profile Token

A profile of the type **Quantum Profile** uses an authentication token to identity an SD-WAN Security Gateway that connects to the SD-WAN service in Check Point Portal.

This token is a pre-shared secret.

You can always revoke the current token in a profile and generate a new token:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Profiles**.
3. Click the profile of the type **Quantum Profile**.
4. Click the tab **General**.
5. In the middle pane, refer to the section **Authentication**.
6. On the right side of the field **Token**, click .
7. Click **Yes** to confirm.

You can always delete Agents from the Tenant:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Agents**.
3. Select the applicable Agent.
4. From the top toolbar, click **Delete**.

Agents

A small software package (component) that runs on the Security Gateway.

This Nano-Agent is responsible for:

- Installing and enforcing the SD-WAN Policy
- Sending the logs for policy enforcement (success or failure) to Check Point Portal
- Sending the SD-WAN Link Swap events to Check Point Portal
- Sending the metrics for SD-WAN Links to Check Point Portal

To get there:

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Agents**.

SD-WAN Service GUI

This section provides a brief description of the views and pages available in *Check Point Portal* > **SD-WAN** Service.

The "Network" View

Page	Description
Getting Started	Contains the SD-WAN Wizard: ■ To create a new asset ■ To create a new profile ■ To open the **Monitor** view
Assets	Contains the objects you configured in SmartConsole on the on-premises Management Server or Smart-1 Cloud. These are objects of such types as **Security Gateway**, **Cluster**, **Host**, **Network**, **Service**, **Group**, **Address Range**, **Security Zone**, **Dynamic Object**, and so on. **Notes:** ■ You can use these objects in the **Source** and the **Destination** columns of SD-WAN rules. ■ From the top toolbar, you can: • Clone a selected object • Delete a selected object • Search for objects • Change the object view between List and Tiles • Enable the multi-select view (to select more than one object) • Refresh the list of objects ■ To see more information in the Tile view, click an Asset object and see the **Attributes** and **General** tabs. ■ To see more information in the List view, click a table row and see the **Attributes** and **General** tabs below the summary table.

Page	Description
Zones	Contains the objects you configure in Check Point Portal. These objects are collections of assets. **Notes:** ■ You can use these objects in the **Source** and the **Destination** columns of SD-WAN rules. ■ The **Zone** object that represents the entire Internet. ■ In each **Zone** object, you must configure a query (on the **General** tab). ■ From the top toolbar, you can: • Create a new object • Search for objects • Change the object view between List and Tiles • Enable the multi-select view (to select more than one object) • Refresh the list of objects ■ To see more information in the Tile view, click a Zone object and see the **General** tab. ■ To see more information in the List view, click a table row and see the **General** tab below the summary table.
SD-WAN Policy	Contains the configured rules for steering the traffic. See *"Configuring SD-WAN Policy" on page 160*. **Notes:** ■ You configure these columns: • **Name** • **Source** • **Destination** • **Services & Applications** • **Behavior** • **Enforcement** ■ From the top toolbar, you can: • Create a new rule • Delete a selected rule • Enable the multi-select view (to select more than one rule) • **Manage Objects** - WAN Links, NAT, QoS • Search in rules
WAN Link Mapping	Contains the mapping between WAN Links and Internet Service Providers. See *"WAN Link Mapping" on page 207*.

Page	Description
Profiles	Contains the summary of configured profiles for Nano-Agents on Security Gateways. In the List view, the summary table shows these columns: ■ **Profile** ■ **Status** ■ **Authentication** ■ **Connected agents** ■ **Outdated agents** **Notes:** ■ From the top toolbar, you can: • Create a new profile • Delete a selected profile • Search in profiles • Change the object view between List and Tiles ■ To see more information in the Tile view, click a Profile and see the **General** and **Advanced** tabs. ■ To see more information in the List view, click a table row and see the **General** and **Advanced** tabs below the summary table.
Agents	Contains the summary with Nano-Agents on Security Gateways. From the top toolbar, you can control how to show the data: ■ **Feed View** Shows only the Hostname of the Security Gateway and the assigned Profile. ■ **Grid View** Shows all available data. The top summary table shows basic information. The bottom pane **General** shows more details for the row you clicked in the top summary table.
	Notes: ■ To change the top table view between **SD-WAN** and **General**, right-click the table **header** and click the applicable view. ■ From the top toolbar, you can: • Select the type of agents to show (connected, disconnected, or both) • Delete a selected agent • Delete all agents • Search in agents • Change the object view between Feed View and Grid View

The "Monitor" View

See *"SD-WAN Monitoring" on page 212*.

Page	Description
Dashboard	The **General** tab shows a dashboard with widgets: ■ **Gateways** ■ **Overlay Tunnels** (*)(**) ■ **Steering Hits** (*) ■ **Link Swaps** (**) ■ **Overall SLA** (**) ■ **Top Applications** ■ **Top Users** The **Live Monitoring** tab shows real time information for Security Gateways and Steering Behaviors: ■ **Link Swaps** ■ **Gateway Details** (*) The **Overlay Tunnels Monitoring** tab shows real time information for Security Gateways and Overlay tunnels: ■ **Overlay Tunnels** ■ **Gateways by Overlay Tunnels status** (*)(**) ■ **Gateways with unstable Overlay Tunnels** (*) Notes: ■ (*) For more information, hover the mouse cursor over the icon. ■ (**) For more information, click the **View Details** link in the widget header. See: ■ *"Monitoring SD-WAN Status in Check Point Portal" on page 212*. ■ *"Monitoring ISP Link Attributes in Check Point Portal" on page 214*.

Page	Description
Events	Shows the steering events (examples: "`Link Swap`", "`SD-WAN Policy Failure`", "`SD-WAN Policy Success`"). See *"Monitoring SD-WAN Steering Events in Check Point Portal" on page 215*. You can: ■ Select a time period ■ Search in events (with special queries) ■ See the event statistics ■ Double-click an event record to see more details ■ Enable the automatic refresh ■ Refresh manually ■ Change the order of columns in this view (right-click any column header > click **Columns Profile Editor**)
Logs	Shows the logs from the SD-WAN rules and the Steering objects. See *"Monitoring SD-WAN Traffic Logs in Check Point Portal" on page 216*. You can: ■ Select a time period ■ Search in logs (with special queries) ■ See the log statistics ■ Double-click a log record to see more details ■ Enable the automatic refresh ■ Refresh manually ■ Export the logs to a file (CSV or JSON) ■ Change the order of columns in this view (right-click any column header > click **Columns Profile Editor**) **Important:** ■ For the on-premises Management Server, you must enable the **Log Sharing** in SmartConsole (see *"Optional: Enable Log Sharing:" on page 80*). ■ In Smart-1 Cloud, the **Log Sharing** is enabled by default.

Page	Description
Notifications	Shows the notifications from Nano-Agents and Security Gateways (examples: "`Agent/Gateway on host XXX software update succeeded. Agent is running latest software.`", "`Agent/Gateway on host XXX software update failed. Agent is running previous software.`"). You can: ■ Select a time period ■ Search in notifications (with special queries) ■ Double-click a notification record to see more details ■ See the notification statistics ■ Enable the automatic refresh ■ Refresh manually ■ Export the notifications to a file (CSV, JSON, or PDF) ■ Change the order of columns in this view (right-click any column header > click **Columns Profile Editor**)
Audit Logs	Shows the audit logs (examples: "`Publish Changes`", "`Enforce Policy`", "`Add WAN Link Mapping Rule`", "`Update SD-WAN Rule`"). You can: ■ Select a time period ■ Search in audit logs (with special queries) ■ Double-click an audit log record to see more details ■ See the audit log statistics ■ Enable the automatic refresh ■ Refresh manually ■ Change the order of columns in this view (right-click any column header > click **Columns Profile Editor**) ■ Export the audit logs to a file (CSV, JSON, or PDF)

The "Support" View

Page	Description
Contact Us	Shows: ■ The ways to contact Check Point Support. ■ Support Authorization settings.
Documentation	Shows: ■ The link to this SD-WAN Administration Guide. ■ Explanation about the Management API (GraphQL API).
System	You can discard unpublished changes in all active sessions. This operation is useful if an administrator is not available to complete the current session and leaves some objects locked. If objects remain locked, other administrators cannot change the configuration.
API	Provides an interface for GraphQL API. See *"SD-WAN GraphQL API" on page 298*.

The "Global Settings" View

From the top toolbar, on the right of the tenant name, click the gear wheel icon .

Provides access to your tenant global settings.

See the *Check Point Portal Administration Guide* > "*Global Settings*".

Guidelines for Planning and Configuring SD-WAN

Before you configure your Security Gateway for SD-WAN, review the planning and configuration guidelines below.

In addition, refer to *"SD-WAN Best Practices" on page 235*.

Public IP addresses that are not part of the Internet, but should be routed internally

Do you have traffic going to destinations with public IP addresses that are not part of the Internet, but should be routed internally (examples: DMZ, LAN, VoIP, Inbound NAT Pools, networks on a remote site behind MPLS or VPN)?

Guidelines

Example topology:

A DMZ network behind the Security Gateway must use a public IP address.

If **yes**, then follow the applicable scenario.

Scenario 1

If all these conditions occur:

1. Your Security Gateway runs:
   - R82.10 and higher
   - R82 Jumbo Hotfix Accumulator Take 14 and higher
   - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
   - Spark Firewall R81.10.15 and higher
2. You **use** public IP addresses in your internal networks.
3. These "internal" public IP addresses **are**:
   - Part of the VPN Domain, or
   - Part of the local networks that are connected directly to the Security Gateway.

Then it is not necessary to configure a bypass rule anymore in the SD-WAN Policy.

Use these Dynamic Objects in your SD-WAN Policy:

- **My VPN Domain** - in the "Overlay" rules
- **Peer VPN Domain** - in the "Overlay" rules
- **SD-WAN Internet** - in the "Local Breakout" rules

Explanations:

- The Dynamic Objects **My VPN Domain** and **Peer VPN Domain** will include public subnets inside the VPN Encryption Domain for overlay rules.
- The Dynamic Object **SD-WAN Internet** will exclude public IP addresses that are part of the VPN Encryption Domain, or belong to the Security Gateway interfaces.

  Currently, the Dynamic Object **SD-WAN Internet** does not exclude public subnets that are routed to a different next hop on the Security Gateway and are not connected directly to the Security Gateway.
- For more information about these Dynamic Objects, see *"Dynamic Objects in SD-WAN Policy" on page 163*.

Scenario 2

If all these conditions occur:

1. Your Security Gateway runs:
   - R82.10 and higher
   - R82 Jumbo Hotfix Accumulator Take 14 and higher
   - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
   - Spark Firewall R81.10.15 and higher
2. You **use** public IP addresses in your internal networks.
3. These "internal" public IP addresses are **not** part of the VPN Domain.
4. These "internal" public IP addresses are **not** part of the local networks that are connected directly to the Security Gateway.

Then:

1. In SmartConsole, create a simple **Network Group** object that contains all such "internal" public IP addresses (for example, call it "**Public_IPs_Group**") and install the Access Control policy.
2. In Check Point Portal, configure this bypass rule at the top of the SD-WAN Policy (see *"Configuring SD-WAN Policy" on page 160*):

#	Name	Source	Destination	Services & Applications	Behavior
1	Routing for "internal" public IPs	`Any`	`Public_IPs_Group`	`Any`	`Default overlay`

Scenario 3

If your Security Gateway runs:

- R81.20 Jumbo Hotfix Accumulator Take 76 and lower
- Spark Firewall from R81.10.05 to R81.10.10

Then:

1. In SmartConsole, create a simple **Network Group** object that contains all such "internal" public IP addresses (for example, call it "**Public_IPs_Group**") and install the Access Control policy.
2. In Check Point Portal, configure this bypass rule at the top of the SD-WAN Policy (see *"Configuring SD-WAN Policy" on page 160*):

#	Name	Source	Destination	Services & Applications	Behavior
1	Routing for "internal" public IPs	`Any`	`Public_ IPs_Group`	`Any`	`Default overlay`

Inbound Non-Encrypted Traffic to Internal Servers

Do you have inbound non-encrypted traffic from the Internet to published resources behind the Security Gateway?

Guidelines

Note - If the destination IP address of the inbound traffic is a public IP address, then follow the guidelines in *"Public IP addresses that are not part of the Internet, but should be routed internally" on page 50*.

If **yes**, then do you have an internal / DMZ server that has to be accessible from the Internet over multiple ISP links?

- If **yes**, then:

  - If the server has to be accessible only through one ISP link at a time (ISP links that provide an Active / Backup access):

    These are the possible workarounds:

    1. Configure your default routes with probing, with the desired priority, in this way:

       a. The inbound traffic has to arrive to the internal server at its public IP address that belongs to the main ISP link (best priority).

       b. If the inbound connection through the main ISP link fails, then the inbound traffic has to arrive to the internal server at its public IP address that belongs to the next ISP link (next in priority). See an example configuration of static routes in sk156812.

    2. Use Policy Based Routing (PBR) for the internal server only, with the above default routes with probing.

    The lower the route priority number, the higher the route precedence.

- If the server has to be accessible over different ISP links that provide a parallel access:

  1. The Security Gateway must run:

     - R82.10 and higher
     - R82 Jumbo Hotfix Accumulator Take 14 and higher
     - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
     - Spark Firewall R81.10.15 and higher

  2. Configure the Symmetric Packet Return as described in *"SD-WAN Symmetric Packet Return" on page 257*.

- If **no**, then:

  As a possible workaround, use Policy Based Routing (PBR) rules on the Security Gateway that configure a different next hop to Internet for each internal server. For outbound redundancy, you can configure multiple next hops with probing.

  - In the PBR rules, in the **Action** section, select the option **Table** (Gaia Portal shows the value **Main Table**).
  - Use the PBR rule priority lower than 100, so it takes precedence over SD-WAN rules.

These are the possible workarounds for inbound traffic to the Security Gateway itself (Remote Access VPN, Mobile Access, and so on):

- Use the workarounds from the sub-section *"If the server has to be accessible only through one ISP link at a time (ISP links that provide an Active / Backup access):" on the previous page* with different default route priorities.
- Wait for the symmetric return feature to support connections to the Local Security Gateway.

Outbound Hide NAT

Do you have Hide NAT configuration behind a specific IP address for outbound traffic from your internal networks?

Guidelines

Important - Currently, SD-WAN does **not** support ISP Link Redundancy for outbound traffic from internal networks in these cases:

- "**Hide behind IP address**" is configured in the Network object
- A Manual Static NAT rule is configured for the outbound traffic

If **yes**, then:

Do you need redundancy for this outbound NAT traffic between your ISP links?

- If **yes**, then:

  Can you change the outbound Hide NAT configuration to "**Hide behind the gateway**"?

  - If **yes**, then:

    In SmartConsole do these steps:

    1. In the applicable objects change your Hide NAT configuration to "**Hide behind the gateway**".
    2. In the NAT policy, delete the Manual NAT rules.
    3. Install the Access Control policy.

  - If **no**, then:

    See *"SD-WAN NAT for ISP" on page 271*.

- If **no**, then:

  In Check Point Portal, create this rule at the top of the SD-WAN Policy (see *"Configuring SD-WAN Policy" on page 160*):

#	Name	Source	Destination	Services & Applications	Behavior
1	Outbound Hide NAT	Network object with the real IP address	`SD-WAN Internet`	`Any`	Use a Steering Behavior object that uses **only** the ISP link that is related to the NAT IP address (go to **Steering Candidates** > **Specific WAN Links**)

Do you have Manual Hide NAT rules that hide traffic from internal networks behind the Security Gateway object?

Guidelines

If **yes**, then:

Replace all these Manual Hide NAT rules with the Automatic NAT configuration:

1. Edit the corresponding Network objects > click the **NAT** page > select "**Hide behind the gateway**" > click **OK**.
2. In the NAT policy, delete these Manual Hide NAT rules.
3. Install the Access Control policy.

By design, Manual NAT rules with the Security Gateway object selected in the "**Translated source**" column, use only the main IP address of the Security Gateway object for Hide NAT and do not use the corresponding Security Gateway's outgoing interface.

Overlay

Note - This section applies only to Security Gateways in a Site to Site VPN configuration with each other.

Do you have any public IP address used in your VPN Encryption Domain?

Guidelines

If **yes**, then:

- If your Security Gateway runs:
  - R82.10 and higher
  - R82 Jumbo Hotfix Accumulator Take 14 and higher
  - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
  - Spark Firewall R81.10.15 and higher

  Then make sure to add the applicable Dynamic Object **My VPN Domain** or **Peer VPN Domain** to the SD-WAN Policy rules that use the Steering Behavior of type "Overlay".

  The Dynamic Objects **My VPN Domain** and **Peer VPN Domain** will include public subnets inside the VPN Encryption Domain for overlay rules.

  For more information about these Dynamic Objects, see *"Dynamic Objects in SD-WAN Policy" on page 163*.

  Alternatively, make sure to add the public subnets to the SD-WAN Policy rules that use the Steering Behavior of type "Overlay".

- If your Security Gateway runs:
  - R81.20 Jumbo Hotfix Accumulator Take 76 and lower
  - Spark Firewall from R81.10.05 to R81.10.10

  Then make sure to add the public subnets to the SD-WAN Policy rules that use the Steering Behavior of type "Overlay".

Does the Security Gateway use a Dynamic IP address (either private or public) for an IPSec VPN Overlay tunnel?

Guidelines

If **yes**, then:

You must configure the Security Gateway object as an object with "Dynamic Address" (DAIP).

The DAIP configuration has limitations.

See *"SD-WAN Configuration for DAIP Security Gateways" on page 220*.

Do you have private WAN lines?

Guidelines

If **yes**, then:

- Is your MPLS router connected directly to your core switch, and not directly to the Security Gateway?

  To use MPLS connection as an SD-WAN interface, the MPLS router / line has to be connected directly to the Check Point Security Gateway at a Layer 3 level.

- Do you have Point-to-Point / Layer 2 connectivity between some peer VPN Gateways?

  Roadmap - Support for Point-to-Point / Layer 2 connectivity is on the roadmap.

  Workaround: Connect a separate Layer 3 device between the VPN Peers and use it as the next hop for the peer VPN Gateways.

- Do you need to send the SD-WAN Overlay traffic over a private line as non-encrypted (clear text)?

  This feature is **not** supported.

Do you need to use Dynamic Routing / Route-Based VPN (VTI) between Security Gateways?

Guidelines

If **yes**, then:

Support for Route-Based VPN with Dynamic Routing is available in.

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator Take 14 and higher
- R81.20 Jumbo Hotfix Accumulator Take 79 and higher
- Spark Firewall R81.10.15 and higher

Workaround:

For peer VPN Gateways that must use Route-Based VPN, enable SD-WAN only on one of the two peer VPN Gateways.

For additional information, see *"SD-WAN and Route-Based VPN" on page 266*.

Do you have multiple Data Centers that work as Primary/Backup and have an overlapping VPN Encryption Domain?

Guidelines

If **yes**, then:

Roadmap - Support for Explicit MEP feature is on the roadmap.

Workarounds:

1. Use Implicit MEP with Source NAT.

   See the *Site to Site VPN Administration Guide* for your version.
2. Separate your subnets between the Data Centers, so there are no overlaps.
3. User Route-Based VPN with Dynamic Routing.

   Available in:

   - R82.10 and higher
   - R82 Jumbo Hotfix Accumulator Take 14 and higher
   - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
   - Spark Firewall R81.10.15 and higher

VPN Community Settings

Guidelines

If **yes**, then:

1. Edit the VPN Community object.
2. In a VPN Community of type Star:
   a. In the left panel, click **MEP**.
   b. Clear the checkbox **Enable center gateways as MEP**.
      SD-WAN does **not** support Explicit MEP (Known Limitation PMTR-104985).
   c. If this VPN Community contains two or more Center Gateways,
      then either **all** or **none** of the Center Gateways must have SD-WAN enabled
      if on the **VPN Routing page**, you selected one of these options:
      - **To center and to other satellites through center**
      - **To center, or through the center to other satellites, to internet and other VPN targets**
3. In a VPN Community of type Star or Mesh:
   a. In the left panel, click **Tunnel Management**.
   b. If you selected **Set Permanent Tunnels**, and SD-WAN is enabled on the Security Gateways, then clear the checkbox **Enable Route Injection Mechanism (RIM)**.
      SD-WAN does **not** support RIM (Known Limitation PMTR-104984).
4. Click **OK**.
5. Install the Access Control policy.

Important - After you enable and configure SD-WAN on all Security Gateways in the VPN Community of type Star or Mesh:

1. Edit the VPN Community object.
2. In the left panel, click **Tunnel Management**.
3. Clear the checkbox **Set Permanent Tunnels**.
   SD-WAN does **not** support Permanent Tunnels (Known Limitation PMTR-104576).
4. Click **OK**.
5. Install the Access Control policy.

Routes in Gaia / Gaia Embedded

Guidelines

- For each ISP link, configure a default route with the required next hop. These default routes must have different priorities.
- Configure static routes for remote site networks to use the MPLS next hop, if it exists.

SD-WAN Interfaces in Gaia / Gaia Embedded

Guidelines

To configure each SD-WAN interface, get the required information:

- IP address and subnet mask for the SD-WAN interface.
- IP address of the next hop.
- NAT IP address, if the SD-WAN interface connects to the Internet through a NAT device.

Additional Considerations

Do you need to use SD-WAN in a Cloud environment?

Guidelines

If **yes**, then:

You can configure SD-WAN only on Cloud Firewall Security Gateways in cloud environments.

Roadmap - Support for SD-WAN in Geo Cluster / Cross AZ Cluster is on the roadmap.

Do you need SD-WAN for a Maestro Security Group or a VSX Gateway?

Guidelines

If **yes**, then:

Roadmap - Support for SD-WAN in a Maestro Security Group and a VSX Gateway is on the roadmap.

Workaround:

Put a dedicated supported Security Gateway between the Maestro Security Group and VSX Gateway and the Internet and configure SD-WAN on that dedicated Security Gateway.

Does your Security Gateway have to use a next hop device that does not respond to ICMP Probing (common in cloud environments)?

Guidelines

If **yes**, then:

- If your Security Gateway runs:
  - R82.10 and higher
  - R82 Jumbo Hotfix Accumulator Take 14 and higher
  - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
  - Spark Firewall R81.10.15 and higher

  Then the ARP Next-Hop Prober feature (enabled by default) should resolve this issue. By default, the Security Gateway performs the nexthop probing using the ARP prober. If the ARP prober fails or does not get a response, then the Security Gateway falls back to using the ICMP Probing.

  If the issue continues, then configure the parameter "`sdw_nexthop_probe_enabled = 0`" as described in *"SD-WAN Next Hop Probing on Cloud Firewall Gateways" on page 242*.

- If your Security Gateway runs:
  - R81.20 Jumbo Hotfix Accumulator Take 76 and lower
  - Spark Firewall Appliance R81.10.10 and lower

  Then configure the parameter "`sdw_nexthop_probe_enabled = 0`" as described in *"SD-WAN Next Hop Probing on Cloud Firewall Gateways" on page 242*.

Do you have ISP Redundancy enabled in the Security Gateway object in SmartConsole?

Guidelines

If **yes**, then:

You **must** disable ISP Redundancy in the Security Gateway object in SmartConsole (section **Other** > page **ISP Redundancy**) and install the Access Control policy.

SD-WAN cannot work with ISP Redundancy enabled.

Migration from ISP Redundancy to SD-WAN:

- **Do you use ISP Redundancy for inbound traffic?**

  If **yes**, then:

  - If the connections should be symmetric (request and reply arrive on the same ISP link), then follow *"Inbound Non-Encrypted Traffic to Internal Servers" on page 53*.
  - If you have Manual Proxy ARP configured on the Security Gateway (sk30197), then before you disable ISP Redundancy:
    1. In SmartConsole, click **Menu** > **Global properties**.
    2. In the left panel, click **NAT**.
    3. Select **Merge manual proxy ARP configuration**.
    4. Click **OK**.

  Roadmap - Support for DNS Proxy in SD-WAN is on the roadmap

- **Do you use ISP Redundancy for outbound traffic?**

  If **yes**, then:

  - If you use ISP Redundancy in the Primary/Backup mode, then in the applicable SD-WAN Policy rule, you can use the Steering Behavior object that is configured with "**Manual order of WAN Links**".
  - If you use ISP Redundancy in the Load Sharing mode, then in the applicable SD-WAN Policy rule, you can use the Steering Behavior object that is configured with "**Link Aggregation**".

  Note - SD-WAN does **not** support ISP Weight for Load Sharing.

- **Do you use ISP Redundancy for VPN traffic?**

  If **yes**, then after you disable ISP Redundancy:

  1. Edit the Security Gateway object.
  2. In the left panel, click **IPSec VPN** > click **Link Selection**.
  3. Configure the applicable settings.

     If a peer VPN Gateway does **not** have SD-WAN enabled, then select **Use probing. Link redundancy mode** and select the applicable mode.

     If you do not use link redundancy, then configure a single link.

     Refer to the *Site to Site VPN Administration Guide* for your version.
  4. Click **OK**.
  5. Install the Access Control policy.

  Note - If all peer VPN Gateways have SD-WAN enabled, then the settings on the **Link Selection** page do not apply.

Do you have Policy Based Routing (PBR) rules configured on the Security Gateway?

Guidelines

If **yes**, then:

- For PBR rules that match traffic based on the Access Control rules:
  1. Delete these PBR rules on the Security Gateway.
  2. Configure the applicable rules in SD-WAN Policy.
- For PBR rules that match traffic based on the Source IP address, Destination IP address, Port number, and so on:
  - If possible, delete these PBR rules on the Security Gateway and configure the applicable rules in SD-WAN Policy.
  - If it is not possible to delete the PBR rules, then make sure these PBR rules do not conflict with SD-WAN Policy rules.

  Notes:
  - PBR rules with priority lower than 100 take precedence over SD-WAN Policy rules.
  - SD-WAN Policy rules that use the Steering Behavior object of type "Local Breakout" take precedence over PBR rule with priority greater than 100.

Workflow for an On-Premises Management Server

This section describes the deployment procedure with an On-Premises Management Server.

For other deployment procedures see:

- *"Workflow for Smart-1 Cloud" on page 118*

Step 1 - Configuration in Check Point Portal

This is a step in the On-Premises Management Deployment.

Check Point Portal is a web-based component in which you configure SD-WAN Policy (rules).

Part 1 - Creating an Account in the Check Point Portal

Procedure

1. Create an account in the Check Point Portal:

   For more information, see the *Check Point Portal Administration Guide* > "*Getting Started*".

   a. In a web browser, go to:

      https://portal.checkpoint.com/create-account

b. Enter this information:

   i. In the **Company Name** field, enter the desired name for your account.

      Note - Account name cannot include special characters (`! @ # $ % ^ & *` or other special characters).

   ii. In the **First Name** and **Last Name** field, enter your name.

   iii. In the **Email** field, enter your company email.

   iv. In the **Phone** field, select your country and enter your contact phone number.

   v. In the **Select Country** field, select the applicable country.

   vi. In the **Select Data Residency** field, select the applicable region.

      The **Available Region** window opens and shows available services based on region.

      To see services available for a specific region, click a region's name.

      A green check mark next to the service name indicates an available service for that region.

      Best Practice - If you require a service that is not in your selected region, then we recommend that you select a region with the necessary services. We do **not** recommend the migration of an account from region to region.

   vii. In the **Customer** field, select the applicable type that describes this account.

      It is possible to change the account type after the account is created.

c. **Optional:** Select **Subscribe to Check Point Product News**.

d. Select **I accept the Check Point Portal terms of service and the Privacy Policy**.

e. In the CAPTCHA section, select **I'am not a robot**.

f. Click **Next**.

The Check Point Portal sends you an email with activation instructions.

2. Log in to the Check Point Portal:
   a. Go to *Check Point Portal*.
   b. Make sure you log in with the same email used to create the account.
   c. Below the account name, select a **Region**.
   d. Click **Next**.

Part 2 - Initial Configuration in Check Point Portal

Procedure

1. In the Check Point Portal, in the top left corner, click the **Menu** button.
2. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. Read the **Check Point Portal terms of service** and **Privacy Policy**.
4. Select **I accept the Check Point Portal terms of services and the Privacy Policy** and click the **TRY NOW** button.
5. Wait for several minutes for the **SD-WAN** service to become available in your account.

   Wait for several minutes for the SD-WAN views to appear (see *"SD-WAN Service GUI" on page 42*).

What is Next?

Follow *"Step 2 - Configuration on the On-Premises Management Server" on page 71*

Step 2 - Configuration on the On-Premises Management Server

This is a step in the On-Premises Management Deployment.

Part 1 - Prerequisites for the Management Server

Prerequisites

1. The Management Server must be up and running **one** of these versions:
   - R82:
     - sk181127 - Check Point R82
     - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.
   - R81.20:
     - sk173903 - Check Point R81.20
     - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.
2. The Management Server must connect to the Internet.
3. If you configured Manual Proxy ARP (sk30197) and Manual NAT rules, then you must follow these steps in SmartConsole:
   a. Click **Menu** > **Global properties**.
   b. In the left tree, click **NAT - Network Address Translation**.
   c. Select **Automatic ARP configuration**.
   d. Select **Merge manual proxy ARP configuration**.
   e. Click **OK**.

Important - Create the Security Gateway objects in SmartConsole only after you configure the applicable interfaces on the Security Gateways. This makes sure the Security Gateway objects automatically get the correct interface topology.

Part 2 - Configure Object Sharing and Log Sharing

It is necessary to enable Object Sharing on the on-premises Management Server to use the configured objects in Check Point Portal.

It is necessary to enable Log Sharing on the on-premises Management Server if you want to see the applicable logs in Check Point Portal.

The procedure below is based on the Management Server that meets the requirements in sk180557 for automatic on-boarding of supported Security Gateways.

Procedure

1. You must register in Check Point Portal.

   See *"Step 1 - Configuration in Check Point Portal" on page 68*.

2. Connect to the command line on the Management Server.
3. Log in to the Expert mode.
4. Connect to the Management Server in one of these ways:
   - With the Desktop SmartConsole connect to:

     ```
     IP Address of your Management Server
     ```

   - With a web browser, open Web SmartConsole at this URL:

     ```
     https://<IP Address of your Management
     Server>/smartconsole
     ```

5. Enable the Upload Consent:

   You must enable the "Upload Information" consent flag (see sk175504):

   a. In SmartConsole top left corner, click the **Menu** button.

   b. Click **Global properties**.

   c. From the left tree, click **Data Access Control**.

   d. Select **Help Check Point improve the products by sending anonymous information**.

   e. Click **OK**.

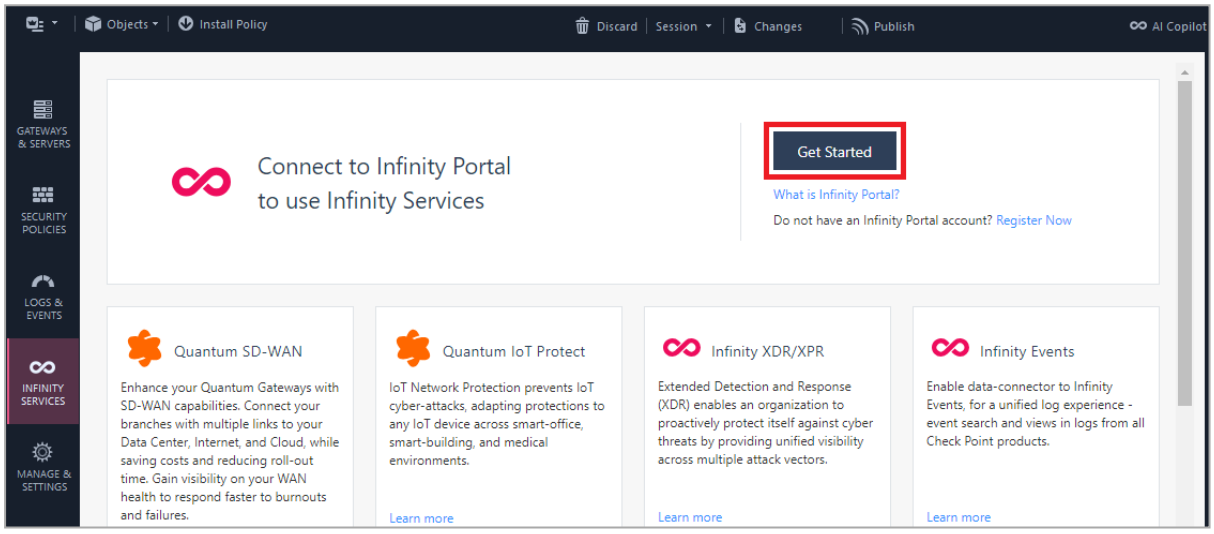
   f. Install the Access Control Policy.

6. From the left navigation panel, click **Infinity Services**.

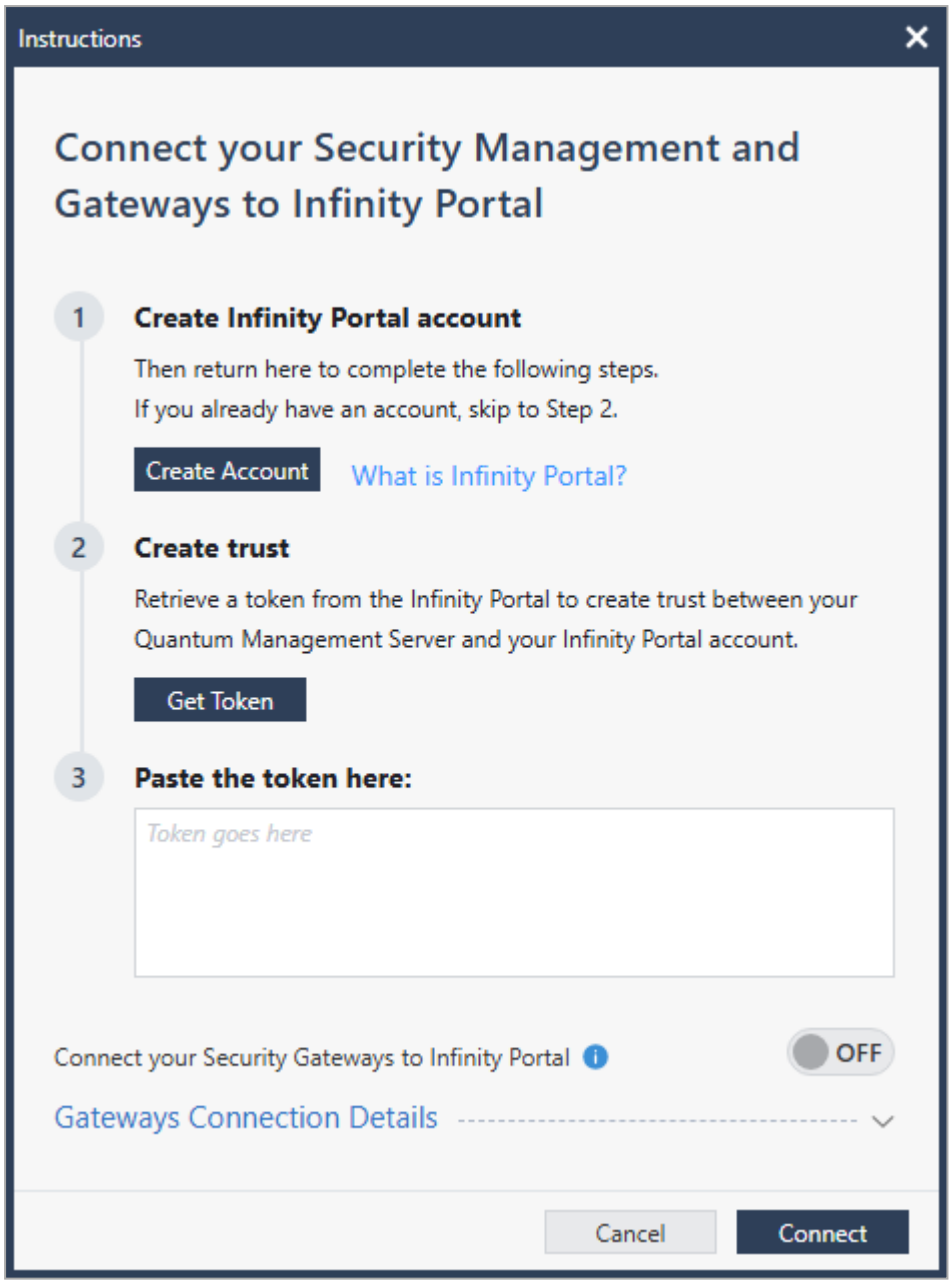


7. Click the **Get Started** button.

   Example:



8. The **Instructions** window opens.

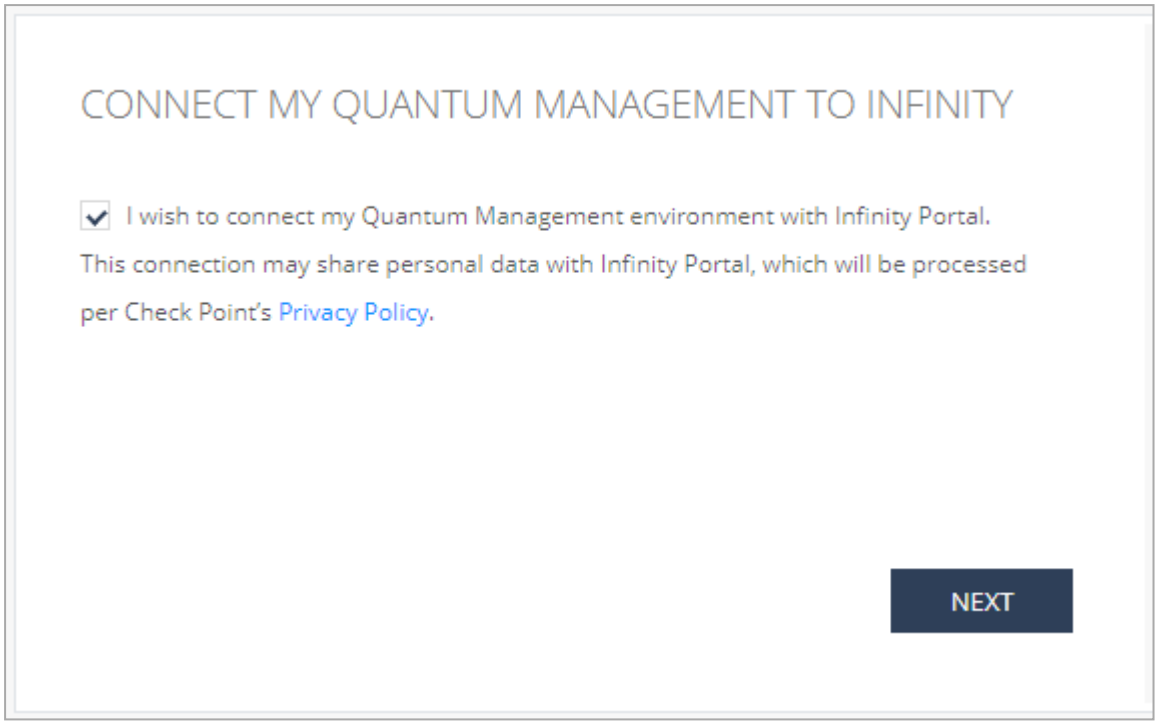


9. Click **Get Token**.

   Web browser opens Check Point Portal Login page. Log in.

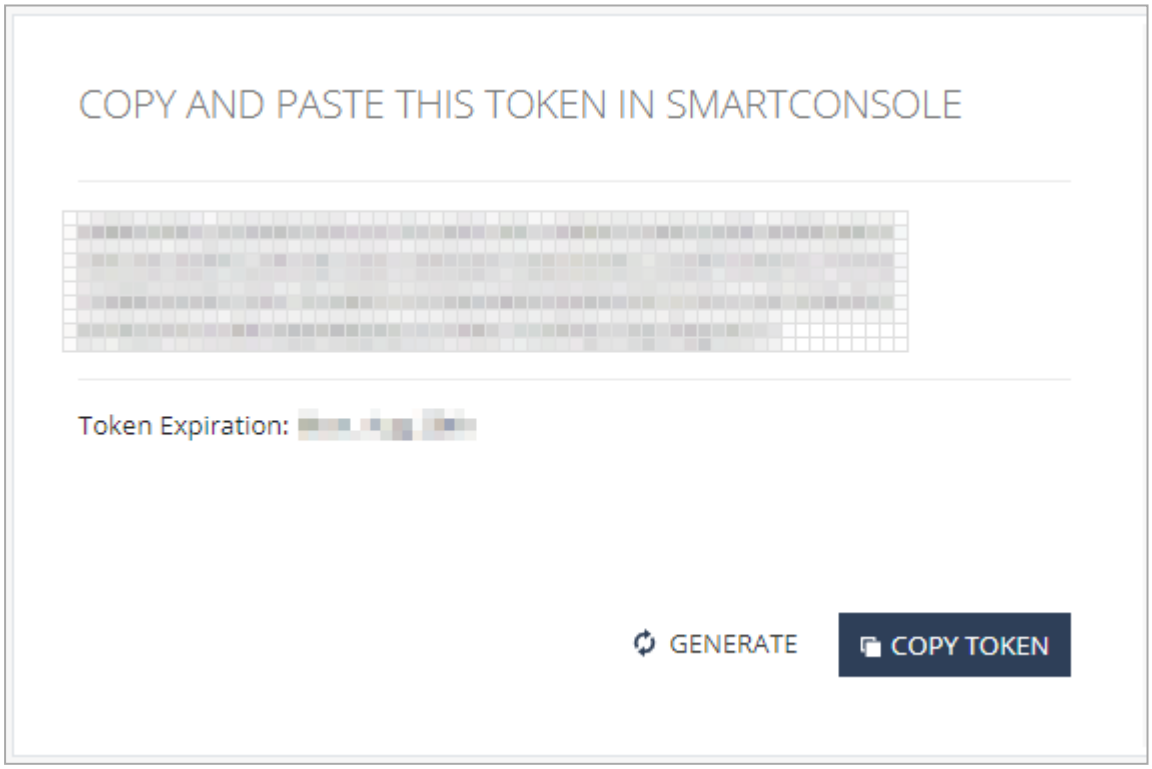
10. Select the applicable account, if you have more than one account, and click **Next**.

11. Select **I wish to connect my Self-hosted Security Management environment and Security Gateways to the Infinity Portal** and click **Next**.

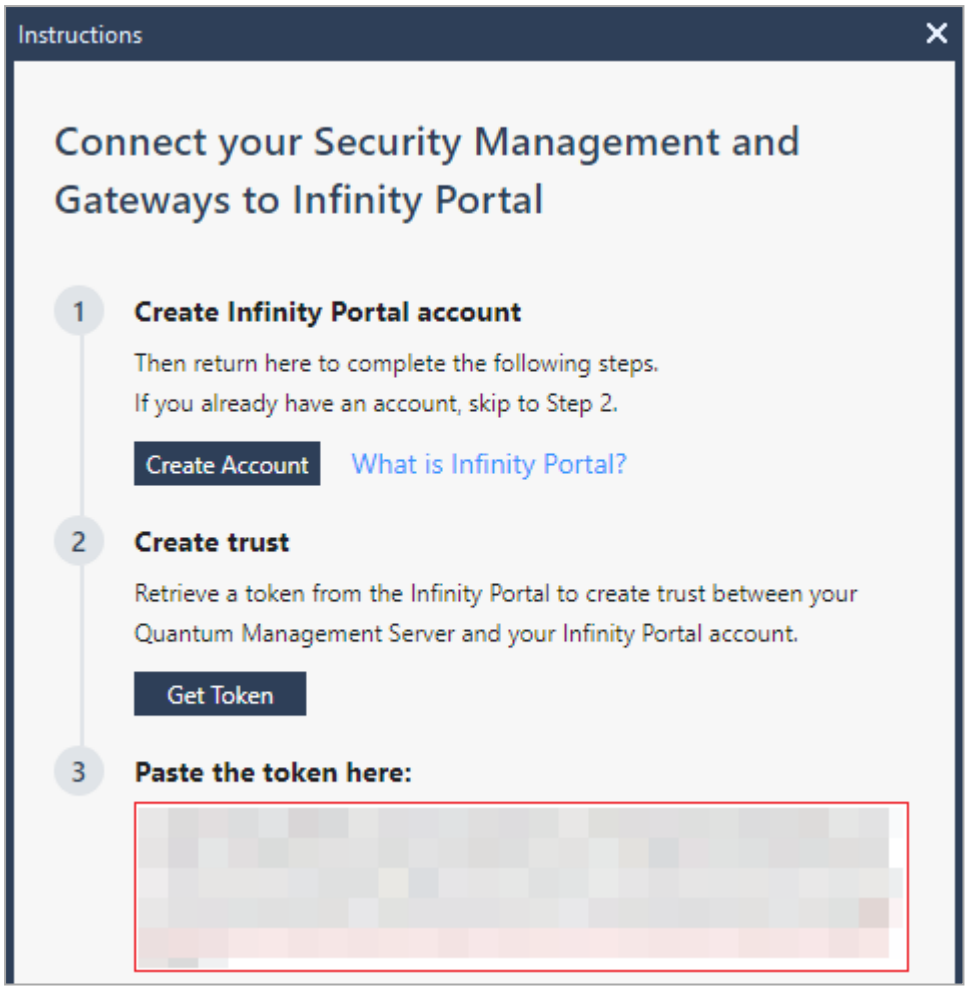


12. The page shows the required token.

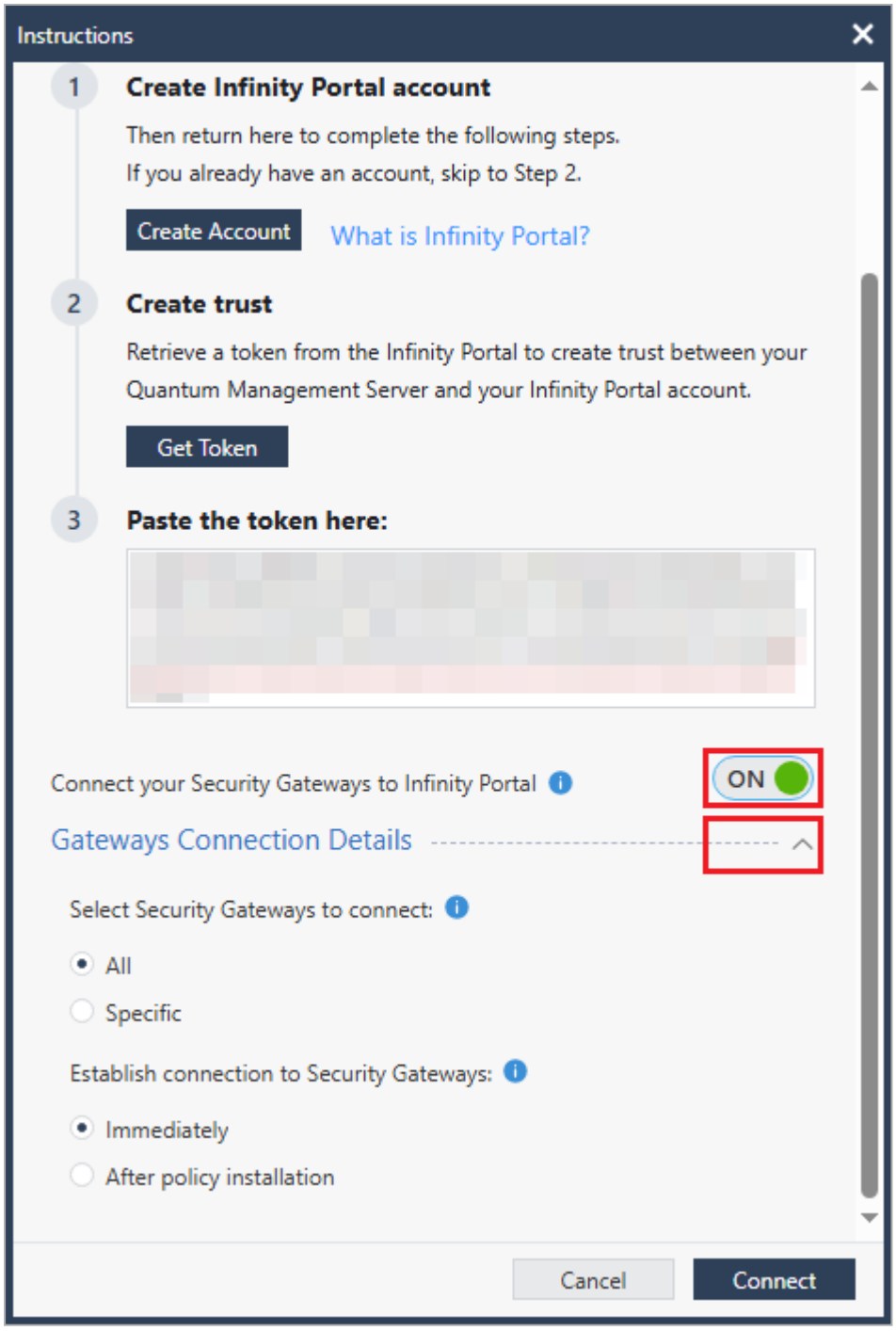
    Click **Copy Token**.



13. In SmartConsole, paste the token.



14. Enable the automatic onboarding of Security Gateways:
    a. Move the toggle **Connect your Security Gateways to Infinity Portal** from **OFF** to **ON**.
    b. Expand the section **Gateways Connection Details**.



15. In the section **Select Security Gateways to connect**, select which supported Security Gateways to onboard:

    For more information, click the **(i)** icon and see sk180557.

    - **All**

      All supported Security Gateways establish connection with Check Point Portal.

- **Specific**

  Only the selected supported Security Gateways establish connection with Check Point Portal.

Note - You can always change this setting later in SmartConsole > **Infinity Services** view > in the bottom right corner, on the right of **Gateways Connector**, click **Edit**.

16. In the section **Establish connection to Security Gateways**, select when to onboard the supported Security Gateways:

    For more information, click the **(i)** icon and see sk180557.

    - **Immediately**

      This is the default. Supported SD-WAN Security Gateways try to establish an immediate connection with Check Point Portal and then during every subsequent policy installation.

    - **After policy installation**

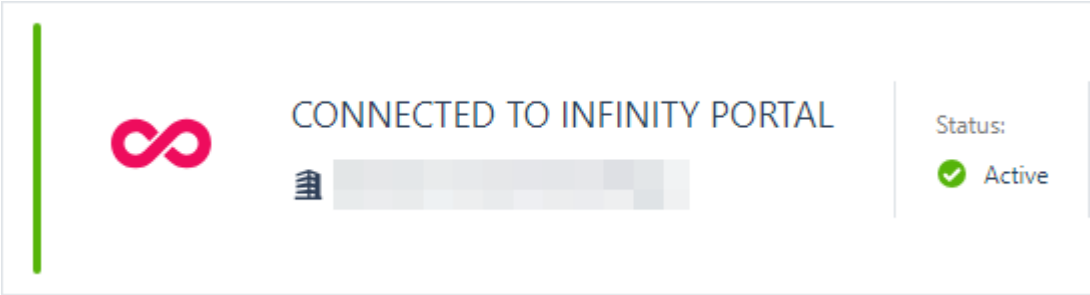
      Supported SD-WAN Security Gateways try to establish a connection with Check Point Portal only after you complete this procedure and install the Access Control policy.

    Note - You can always change this setting later in SmartConsole > **Infinity Services** view > in the bottom right corner, on the right of **Gateways Connector**, click **Edit**.

17. At the bottom, click **Connect**.

18. SmartConsole must show **Connected to Check Point Portal** and **Status: Active**.

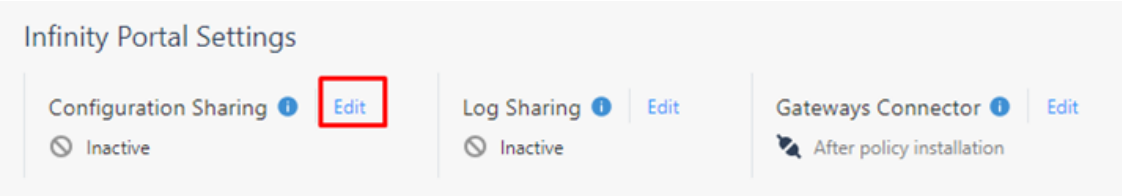
    Example:

19. Enable **Configuration Sharing**:

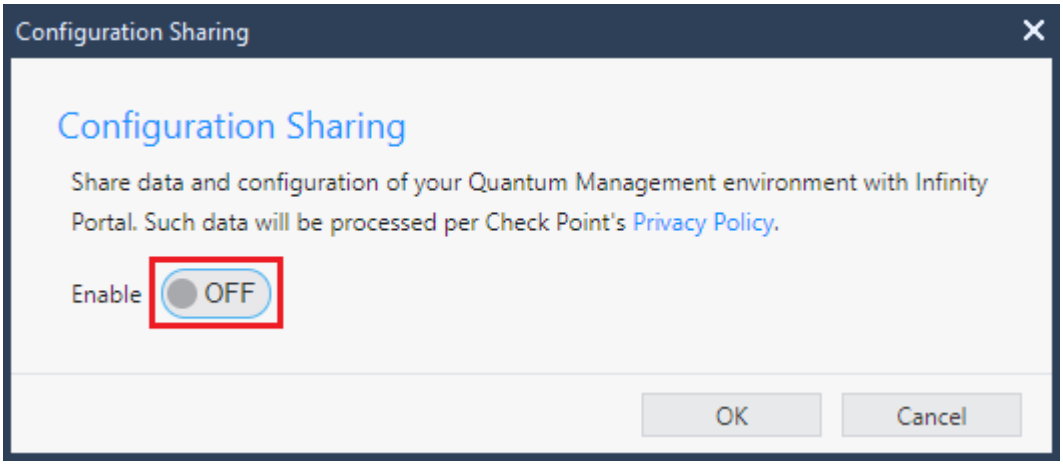
a. In SmartConsole, in the bottom left section **Infinity Portal Settings**, on the right of **Configuration Sharing**, click **Edit**.

Example:

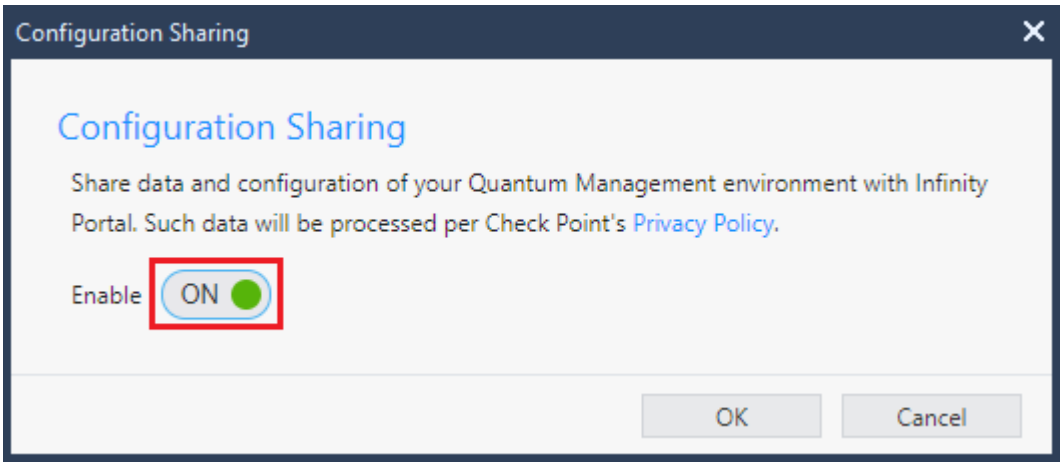


b. The **Configuration Sharing** window opens.

c. Near the **Enable** option, click the **OFF** button.



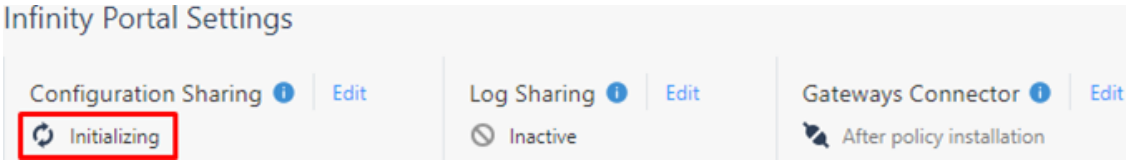
It must change to **ON**.



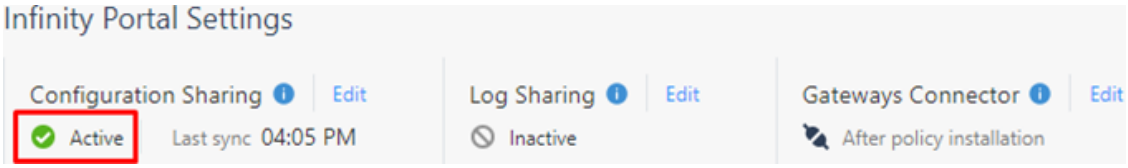
Click **OK**.

d. The configuration sharing starts, and after some time its status changes from **Initializing** to **Active**.

Example:



Example:



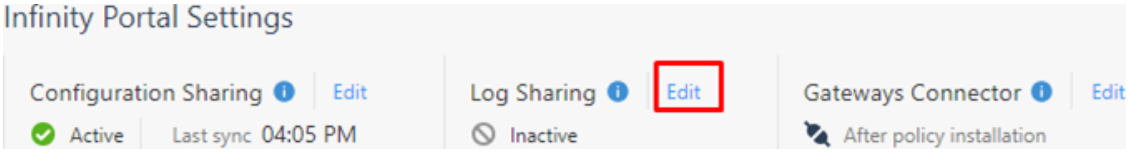
From this point, objects configured in SmartConsole on the on-premises Management Server appear in Check Point Portal as assets.

20. **Optional:** Enable **Log Sharing**:

Note - This configuration is required if you want to see the logs in Check Point Portal.

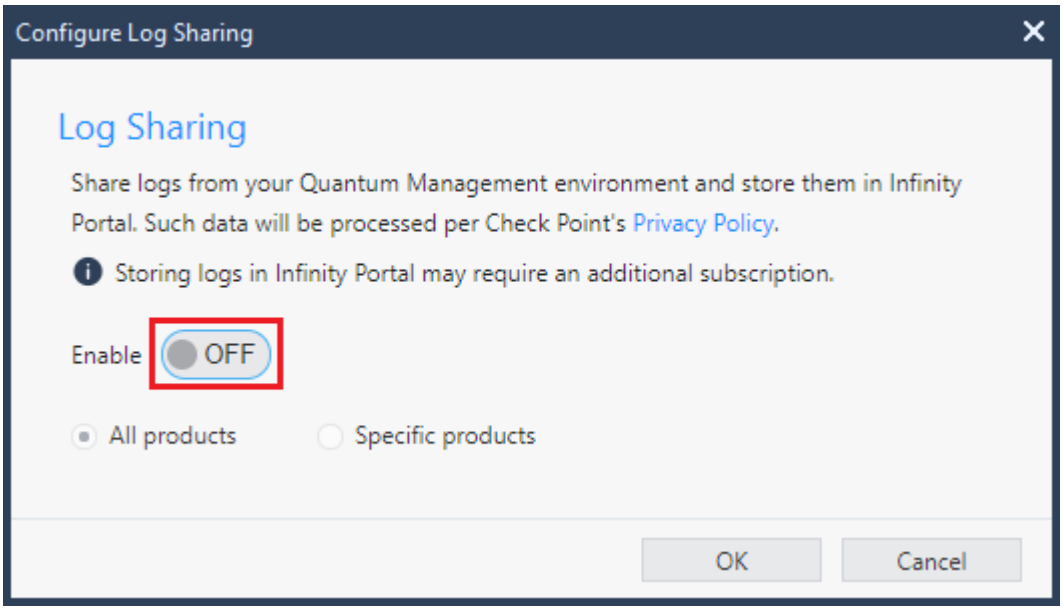
a. In SmartConsole, in the bottom left section **Infinity Portal Settings**, on the right of **Log Sharing**, click **Edit**.

Example:

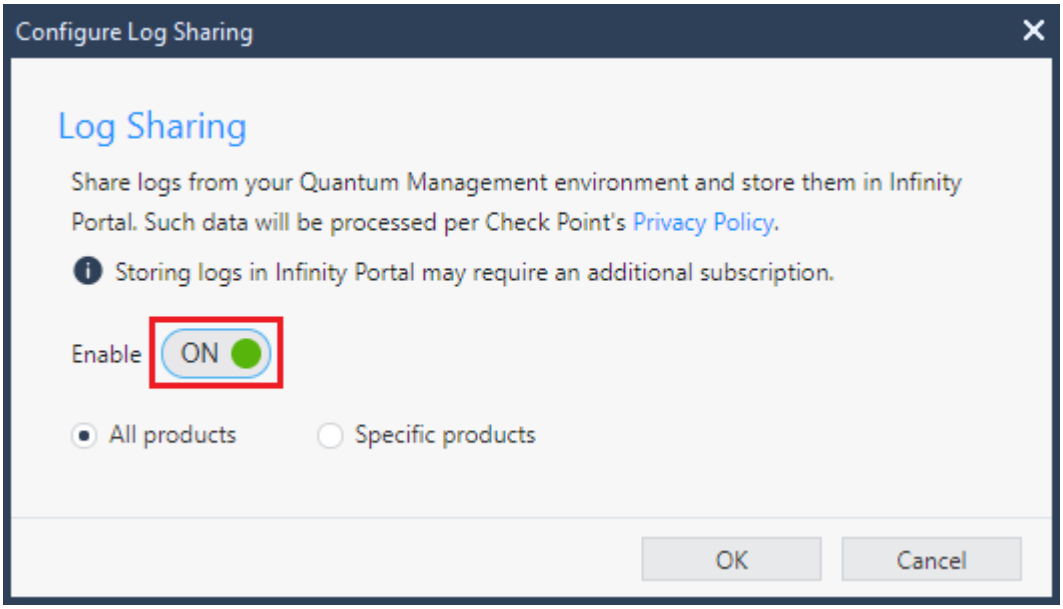


b. The **Configure Log Sharing** window opens.

c. Near the **Enable** option, click the **OFF** button.



It must change to **ON**.



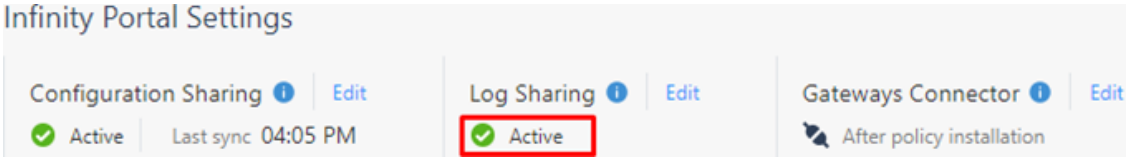
Notes:

- To share logs from all products, select **All products**.
- To share logs only from specific products, select **Specific products** and select the required products.
  - For full SD-WAN visibility, we recommend selecting these products:
    - **SD-WAN**
    - **Application Control**
    - **URL Filtering**
    - **Firewall** (required to see logs about "Overlay" - see *"SD-WAN Connection Type - "Overlay"" on page 200*)
  - To minimize log output, you can select only the **SD-WAN** product.
    Note that in this case, log-based widgets in the SD-WAN **Monitor** view (such as **Top Applications**) may display partial data or no data at all.

Click **OK**.

d. The log sharing starts, and its status changes to **Active**.

Example:



What is Next?

Follow *"Step 3 - Configuration on Security Gateways" on page 83*

Step 3 - Configuration on Security Gateways

This is a step in the On-Premises Management Deployment.

Part 1 - Prerequisites for Security Gateways

Prerequisites

1. The required version of the Security Gateway / Cluster must be up and running.

Platform	Instructions
Security Gateways that run Gaia OS	a. Download the required image from sk180605. b. Follow the *Installation and Upgrade Guide* for your version. c. Install the applicable Jumbo Hotfix Accumulator.
Spark Firewall Appliances that run Gaia Embedded OS	a. R81.10.05 and higher (we recommend R81.10.17). Refer to the corresponding Home Page SK article in sk179615. b. Centrally Managed.

Note - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.

2. The Security Gateway / Spark Firewall Appliance / Cluster Members must connect to the Internet.

Part 2 - Configuration of SD-WAN interfaces on the Security Gateway

Procedure for a Security Gateway that runs Gaia OS

Note - For a Maestro Security Group, see *"Configuring a Maestro Security Group for SD-WAN" on page 113*.

1. Configure the SD-WAN interfaces on the Security Gateway / each Cluster Member.

   You can configure the required SD-WAN interfaces in Gaia Portal or Gaia Clish.

   Notes:
   - This configuration also applies to VLAN interfaces.
     If you configure SD-WAN on a VLAN interface, then it is **not** supported to configure SD-WAN on the parent physical interface.
   - This configuration also applies to clusters, in which the IP addresses of Cluster Members and the Cluster Virtual IP address belong on different subnets.

   Configuration of a Security Gateway in Gaia Portal

   a. Connect to Gaia Portal.

   b. From the left tree, click **Network Interfaces**.

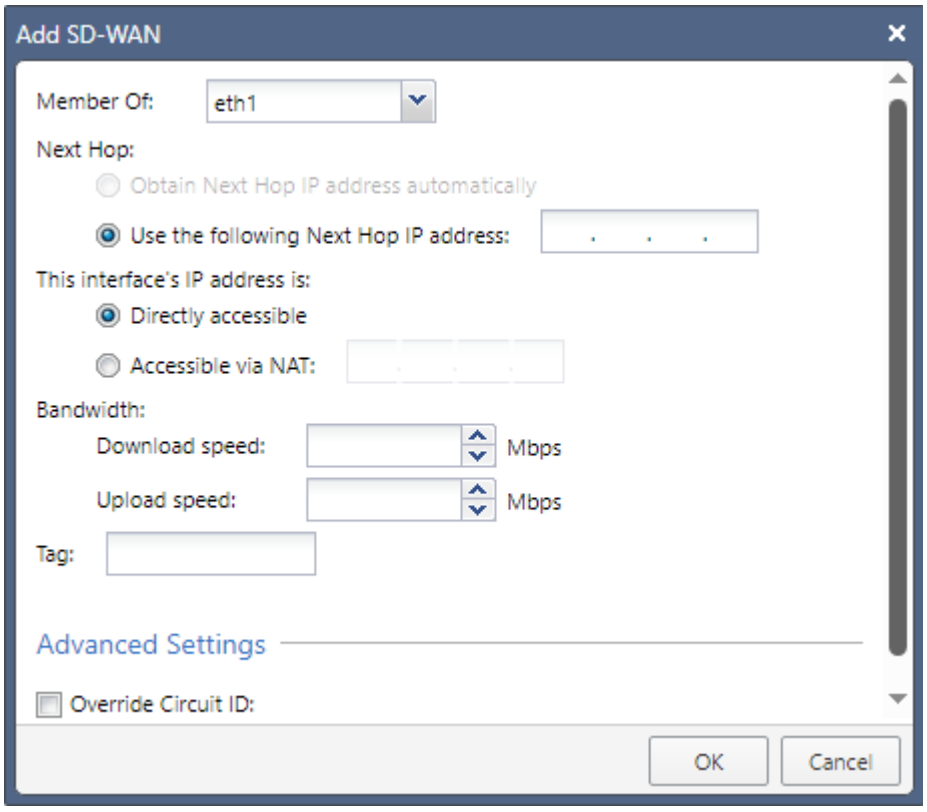
   c. Configure the applicable interfaces that you plan to use for SD-WAN.

      Enable the interfaces and configure the IPv4 address.

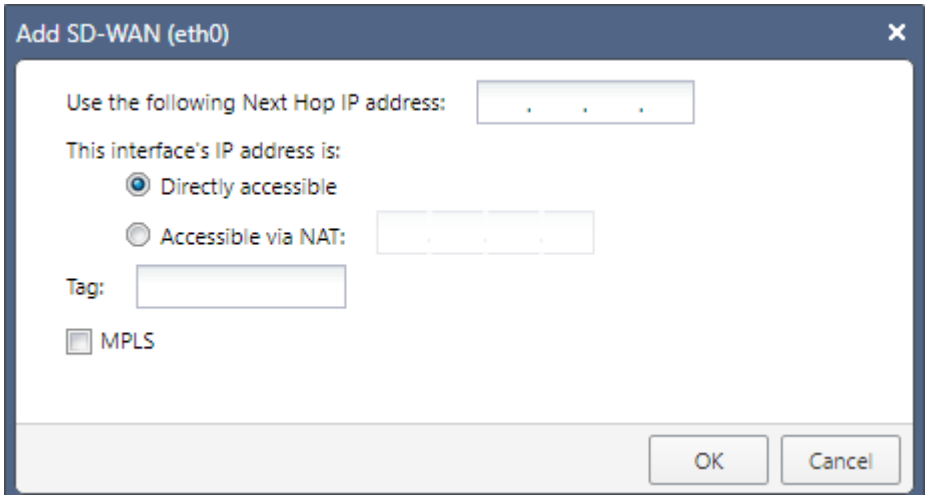
      See the *Gaia Administration Guide* for your version > "*Network Management*" > "*Network Interfaces*" > "*Physical Interfaces*".

   d. In the section **SD-WAN Interfaces**, click **Add**.

Example from R81.20 Jumbo Hotfix Accumulator, Take 79 and higher:



Example from R81.20:



e. Select the applicable interface that connects to the applicable ISP.

f. In the section **Next Hop**, configure the applicable next hop IP Address for the ISP, to which this interface connects.

In the field **Use the following Next Hop IP address**, enter the applicable IP address.

Note - This section title "**Next Hop**" is available in these Security Gateway versions:

- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

g. In the section **This interface's IP address is**, configure how SD-WAN rules get the IP address of this interface:

- **Directly accessible**

  Specifies that this interface has a public IP address, to which peers can connect directly.

  This applies to the interface with an IP address that is configured statically or by a DHCP server.

  Note - You must select this option if an ISP assigns an IP address dynamically (for example, when a Security Gateway connects to the Internet through a modem).
  For additional information, see *"SD-WAN Configuration for DAIP Security Gateways" on page 220*.

- **Accessible via NAT**

  Specifies that an external device or an ISP applies Static NAT on the IP address of this interface.

  Enter the applicable static IP address after this external NAT, as the peers receive it.

  Notes:
  - This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*).
    This option configures the IP address that VPN peers must use to negotiate the Site to Site VPN tunnel with this Security Gateway.
  - You do not need to configure NAT rules in SmartConsole for this external NAT.

Summary:

Option in Gaia Portal	When to Select
Directly accessible	SD-WAN interface with a Static IP address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with a Static IP address) --- (no NAT device) ---

Option in Gaia Portal	When to Select
	SD-WAN interface with a Dynamically Assigned IP Address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with DAIP) --- (no NAT device) ---
	SD-WAN interface with a Static IP address that is located behind a Dynamic NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns an IP address dynamically] ---
Accessible via NAT	This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*). SD-WAN interface with a Static IP address that is located behind a Static NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns a static IP address] ---

h. **Optional:** In the section **Bandwidth**, configure the applicable limits for the **Download speed** and **Upload speed**.

Note - This section is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

You can use these limits in the SD-WAN Steering Behavior objects. See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

i. **Optional:** In the **Tag** field, enter a desired interface tag. Example: `ISP1`

See the description and the example in *"WAN Link Mapping" on page 38*.

j. Select **MPLS**, if this interface connects to to a Private Link (for example, MPLS).

Note - This checkbox is available only in these Security Gateway versions:
- R81.20 Jumbo Hotfix Accumulator, Take 76 and lower.
- R81.20 without the Jumbo Hotfix Accumulator.

k. **Optional:** In the section **Advanced Settings**:

Note - This section is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

i. Select **Override Circuit ID**.

See *"SD-WAN Circuit ID" on page 248*.

ii. Enter a value between 0 and 255.

Important:
- The value 0 is the default for Public WAN Links.
- The value 1 is the default for Private WAN Links.

l. Click **OK**.

Configuration of a Security Gateway in Gaia Clish

For more information, see *"SD-WAN Configuration in Gaia Clish" on page 293*.

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in.

c. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

d. Configure the applicable interfaces that you plan to use for SD-WAN.

Enable the interfaces and configure the IPv4 address.

See the *Gaia Administration Guide* for your version > "*Network Management*" > "*Network Interfaces*" > "*Physical Interfaces*".

e. Configure the applicable next hop IP Address for the ISP, to which this interface connects:

```
set interface <Name of Interface> sdwan next-hop <IP Address of ISP Next Hop>
```

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1
```

f. Configure how SD-WAN rules get the IP address of this interface:

- If this interface has a public IP address, to which peers can connect directly, do not configure anything.

  This applies to the interface with an IP address that is configured statically or by a DHCP server.

  Notes:
  - In Gaia Portal, this corresponds to the option "**Directly accessible**".
  - You must select this option if an ISP assigns an IP address dynamically (for example, when a Security Gateway connects to the Internet through a modem). For additional information, see *"SD-WAN Configuration for DAIP Security Gateways" on page 220*.

- If an external device or an ISP applies NAT on the IP address of this interface, then configure the applicable IP address after this external NAT, as the peers receive it:

  ```
  set interface <Name of Interface> sdwan next-hop
  <IP Address> nat <IP Address after External NAT>
  ```

  Example:

  ```
  set interface eth1 sdwan next-hop 192.168.20.1
  nat 172.30.40.5
  ```

  Notes:
  - In Gaia Portal, this corresponds to the option "**Accessible via NAT**".
  - This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*).
    This option configures the IP address that VPN peers must use to negotiate the Site to Site VPN tunnel with this Security Gateway.
  - You do not need to configure NAT rules in SmartConsole for this external NAT.

Summary:

Option in Gaia Clish	When to Configure
Directly accessible	SD-WAN interface with a Static IP address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with a Static IP address) --- (no NAT device) ---
	SD-WAN interface with a Dynamically Assigned IP Address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with DAIP) --- (no NAT device) ---
	SD-WAN interface with a Static IP address that is located behind a Dynamic NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns an IP address dynamically] ---

Option in Gaia Clish	When to Configure
Accessible via NAT	This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*). SD-WAN interface with a Static IP address that is located behind a Static NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns a static IP address] ----

g. If this interface connects to a Private Link (for example, MPLS):

```
set interface <Name of Interface> sdwan next-hop <IP Address> is_mpls true
```

Note - This command is available only in these Security Gateway versions:
- R81.20 Jumbo Hotfix Accumulator, Take 76 and lower.
- R81.20 without the Jumbo Hotfix Accumulator.

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1 is_mpls true
```

h. **Optional:** Configure a desired interface tag:

See the description and the example in *"WAN Link Mapping" on page 38*.

```
set interface <Name of Interface> sdwan next-hop <IP Address> tag "<Tag Name>"
```

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1 tag "ISP1"
```

i. **Optional:** Configure the download speed limit (in Mbps):

```
set interface <Name of Interface> sdwan download-speed
<1 - 1000000>
```

Note - This command is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

Example:

```
set interface eth1 sdwan download-speed 500000>
```

j. **Optional:** Configure the upload speed limit (in Mbps):

```
set interface <Name of Interface> sdwan upload-speed
<1 - 1000000>
```

Note - This command is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

You can use these limits in the SD-WAN Steering Behavior objects.
See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

Example:

```
set interface eth1 sdwan upload-speed <1 - 100000>
```

k. Examine the SD-WAN configuration on the interface:

```
show interface <Name of Interface> sdwan
```

l. Save the configuration:

```
save config
```

2. Configure the applicable default routes on the Security Gateway / each Cluster Member.

   The Security Gateway / Cluster Member uses these default routes:

   - For traffic that does not match the configured SD-WAN rules.
   - For traffic that the Security Gateway / Cluster Member creates (for example, to connect to Check Point cloud).

   See the *Gaia Administration Guide* for your version > "*Network Management*" > "*IPv4 Static Routes*".

Important:

- For each Internet Service Provider (ISP), you must configure one default route with unique priority.
  The reasons for this configuration are:
  - A legacy ISP backup that is based on the link availability, if the SD-WAN service does down on the Security Gateway / Cluster Member.
  - The Security Gateway / Cluster Member sends its traffic (local connections) to the Internet based on the operating system routing table and not based on SD-WAN Policy rules.
  - The Security Gateway / Cluster Member must have an active route to the destination of the packet to process it. This applies to both cleartext traffic and VPN traffic.
    If only one ISP has a default route, and it goes down, then all overlay connections are lost and do not fail over.
    This does not apply in Local Breakout, because its mechanism has its routing table that does not depend on the operating system routing.
- The Security Gateway / Cluster Member cannot have different ISP default routes with the same priority.
  When the Security Gateway / Cluster Member cannot use an ISP default route with the lowest priority (for example, cannot reach the ISP), it uses another ISP default route with the next higher priority.
- It is **not** mandatory to configure static routes to branches, if they are part of the "Overlay" because the VPN clean up rule in the SD-WAN Policy is always matched.
- If the Security Gateway / Cluster Member has a private line, such as MPLS, which is part of the overlay, then it is a best practice to configure such routes that send traffic for all the overlay destination networks to the MPLS next hop. In this case, even if all ISP links are down, and no active default route exist in the operating system kernel, the specific route on the MPLS makes sure that the "Overlay" traffic continues to work over the MPLS SD-WAN interface. Without an active route to the destination, the packet is lost in the routing table, before the VPN encryption takes place.

Procedure for a Spark Firewall Appliance that runs Gaia Embedded OS

1. Configure the SD-WAN interfaces on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

   Note - This configuration also applies to VLAN interfaces.
   If you configure SD-WAN on a VLAN interface, then it is **not** supported to configure SD-WAN on the parent physical interface.

   You configure these SD-WAN interfaces in the WebUI, or Gaia Clish.

Configuration of a Spark Firewall Appliance in the WebUI

See *R82.00.X Spark Firewall Appliances Centrally Managed Administration Guide*

See the *R82.00.X Spark Firewall Appliances Centrally Managed Administration Guide* > "*Managing the Device*" > "*Configuring Internet Connectivity*".

a. Connect to the WebUI.

b. From the left tree, click **Device**.

c. In the middle pane, expand the section **Network** and click **Internet**.

d. Configure two Internet connections - one for each ISP:

   i. Click **Add an Internet connection**.

      The **New Internet Connection** window opens.

   ii. On the **Configuration** tab:

      i. In the **Connection name**, enter the applicable name for this connection.

      ii. In the **Interface** field, select the applicable interface.

      iii. In the **Connection type** field, select the applicable type.

   iii. On the **Connection Monitoring** tab:

      i. Select **Automatically detect loss of connectivity to the default gateway**.

      ii. Select **Monitor connection state by sending probe packets to one or more servers on the Internet**.

      Local connections (originating from the Spark Firewall Appliance) use the main routing table and are not affected by SD-WAN Local Breakout routing.

   iv. On the **Advanced** tab:

      Configure the applicable options based on the connection type.

      In firmware versions R81.10.15 and higher:

      i. Expand the section **SD-WAN Settings**.

      ii. **Optional:** Configure the applicable limits for the **Download speed** and **Upload speed**.

      Note - You can use these limits in the SD-WAN Steering Behavior objects.
      See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

      iii. **Optional:** Select **Override circuit ID**.

      See *"SD-WAN Circuit ID" on page 248*.

      Enter a value between 0 and 255.

   v. Click **Save**.

Configuration of a Spark Firewall Appliance in Gaia Clish - R81.10.10 and higher

Important - The Spark Firewall Appliances configure the SD-WAN next hop based on the Internet configuration.

a. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

b. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

c. Configure two Internet connections - one for each ISP.

Use this command:

```
add internet-connection name "<Name of Connection>"
interface <Name of Interface>
```

See the *R82.00.X Spark Firewall Appliances CLI Reference Guide* > "*Configuring the Internet Connections*" > "*Adding Internet Connections*".

Example:

```
add internet-connection name Internet2 interface DMZ
type static ipv4-address 192.168.223.5 subnet-mask
255.255.255.0 default-gw 192.168.223.4
```

Configuration of a Spark Firewall Appliance in CLI - only R81.10.05, R81.10.07, and R81.10.08

Important - The Spark Firewall Appliances configure the SD-WAN next hop based on the Internet configuration.

a. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

b. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

c. Configure two Internet connections - one for each ISP.

Use this command:

```
add internet-connection name "<Name of Connection>"
interface <Name of Interface> <options>
```

See the *R82.00.X Spark Firewall Appliances CLI Reference Guide* > "*Configuring the Internet Connections*" > "*Adding Internet Connections*".

Example:

```
add internet-connection name Internet2 interface DMZ
type static ipv4-address 192.168.223.5 subnet-mask
255.255.255.0 default-gw 192.168.223.4
```

Part 3 - Installation of the Nano-Agent on the Security Gateway

The Nano-Agent connects the Security Gateway / each Cluster Member to Check Point Portal, and enable the automatic installation and update of the SD-WAN policy from Check Point Portal.

There are two possible onboarding options - automatic (recommended) and manual.

Procedure for automatic onboarding of supported Security Gateways

Note - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.

1. In SmartConsole, make sure the Management Server is connected to Check Point Portal and automatic onboarding is enabled.
    a. From the left navigation panel, click **Infinity Services**.
    b. At the top, SmartConsole must show **Connected to Check Point Portal** and **Status: Active**.
    c. In the bottom right corner, on the right of **Gateways Connector**, click **Edit**.
    d. The option **Connection between your Security Gateways and Infinity Portal is enabled** must show **ON**.
2. In Check Point Portal, check if the Security Gateway is already connected:
    a. In Check Point Portal, in the top left corner, click the **Menu** button.
    b. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
    c. From the left navigation panel, click **Network**.

d. In the middle section, click **Agents**.

Possible next steps:

- If your Security Gateway appears on this page, then skip to "**Part 4 - Configuration of the Security Gateway object in SmartConsole**" below.
- If your Security Gateway does **not** appear on this page, then in SmartConsole, connect this Security Gateway:
  i. In the bottom right corner, on the right of **Gateways Connector**, click **Edit**.
  ii. In the section **Select Security Gateways to connect**, select **Specific** and select this Security Gateway.
  iii. In the section **Establish connection to Security Gateways**, select **Immediately**.
  iv. At the bottom, click **OK**.
  v. Wait for several minutes.
  vi. In Check Point Portal, check the **Agents** page again.

Procedure for manual onboarding of a Security Gateway

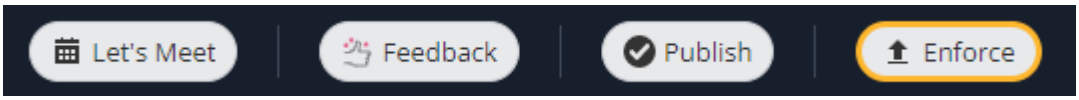
Note - For a Maestro Security Group, see *"Configuring a Maestro Security Group for SD-WAN" on page 113*.

1. Get the Authentication Token from the Quantum Profile in SD-WAN Application.
   a. In the Check Point Portal, in the top left corner, click the **Menu** button.
   b. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
   c. In the middle section, click **Profiles**.
   d. Click **Quantum Profile** to open it.

   Note - The SD-WAN Application creates this Quantum Profile automatically in these cases:
   - You connect your on-premises Management Server to Check Point Portal and configure Object Sharing.
     See *"Workflow for an On-Premises Management Server" on page 67*.
   - You enable the Smart-1 Cloud Application and configure Object Sharing.
     See *"Workflow for Smart-1 Cloud" on page 118*.

e. From the top of the page, click the **Enforce** button.

Note - Although you did not configure the SD-WAN Policy yet, this step is necessary.

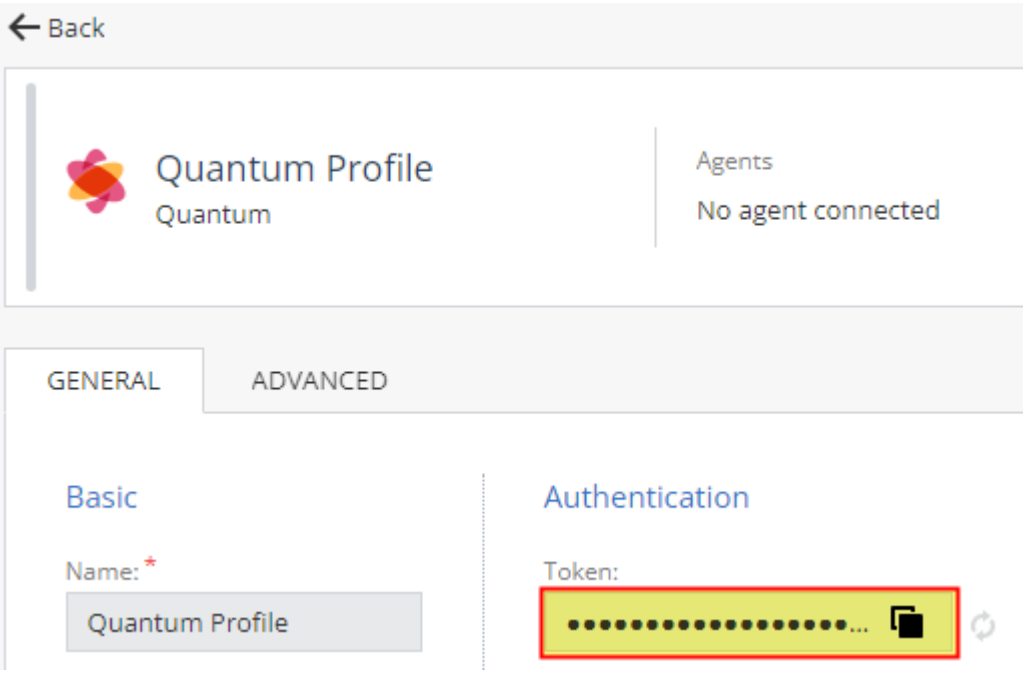


In the popup window that opens, click **Publish & Enforce Policy**.

f. In the middle pane, in the section **Authentication**, the field **Token** must be populated (dots appear instead the actual token value).

This means the service generated the required token.

Example:



g. Save your token:

i. In the section **Authentication**, in the field **Token**, click the **Copy** icon on the right.

ii. Save this string.

You use this token to install the Nano-Agent.

Best Practice - Connect all SD-WAN Security Gateways to Check Point Portal with the same token (to make the policy configuration easier).

2. Connect to the command line on the Security Gateway / each Cluster Member.

3. Log in.
4. If your default shell is Gaia Clish, go to the Expert mode:

   ```
   expert
   ```

5. Install the Nano-Agent:

   ```
   nano-egg --install --token <Authentication Token you copied earlier from your Quantum Profile>
   ```

Important:

- You can examine the connection from the Security Gateway / each Cluster Member to Check Point Portal only after you configure and enforce the SD-WAN Policy in Check Point Portal.
- It is necessary to uninstall the current Nano-Agent and install it again in these cases:
  - If you uninstalled the last installed Take of the Jumbo Hotfix Accumulator to revert to a previous installed Take.
  - If you uninstalled the last installed Major version.
  - If you reverted Gaia OS to one of the previous snapshots.

Part 4 - Configuration of the Security Gateway object in SmartConsole

Procedure

1. Connect with SmartConsole to the Security Management Server / Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new / configure the existing object for the Security Gateway / Cluster in SmartConsole.
4. On the **General Properties** page (of the Security Gateway / Cluster object), you must enable and configure these Software Blades:
   a. **Application Control**
   b. **URL Filtering**
   c. **IPSec VPN** (if this Security Gateway / Cluster must participate in VPN - see *"SD-WAN Connection (Steering Behavior) Types" on page 184*).

   Note - Installation of an Access Control Policy fails on a Security Gateway / Cluster Member when a Nano-Agent is installed, but the Application Control and URL Filtering Software Blades are not enabled.

   See the:
   - *Security Management Administration Guide* for your version.
   - *Spark Firewall Appliances Centrally Managed Administration Guide* for your version.
   - *Site to Site VPN Administration Guide* for your version.
5. On the **Network Management** page:

   (In the Spark Firewall object, this page is called **Topology**.)
   a. Write down the topology configuration of each existing interface.
   b. From the top toolbar, click **Get Interfaces** and click **Get Interfaces With Topology**.
   c. Accept the imported topology.
   d. Make sure for the SD-WAN interfaces, the **Network Type** column shows **External**.

   Important - The names of SD-WAN interfaces on the **Network Management** (**Topology**) page must be the same as the names of these interfaces on the Security Gateway / each Cluster Member.

6. Configure the **SD-WAN** interfaces - Topology and Anti-Spoofing:
    a. On the **Network Management** page (in the Spark Firewall object, this page is called **Topology**), select the SD-WAN interface and click **Edit**.
    b. In the **Topology** section, click **Modify**.
    c. In the **Leads To** section:
        - Make sure to select **Internet (External)**.
    d. In the **Anti-Spoofing** section:
        i. Select **Perform Anti-Spoofing based on interface topology**.
        ii. Select the applicable **Anti-Spoofing action**.
        iii. **Optional:** Select **Don't check packets from** and select the applicable Network, Network Group, or Address Range object.
        iv. Select the applicable **Spoof Tracking** option.
    e. Click **OK** to close the **Topology Settings** window.
    f. Click **OK** to close the **Interface** window.
7. Make sure the ISP Redundancy configuration is **disabled** in the **Other** section > on the **ISP Redundancy** page.

    Note - SD-WAN does **not** support the ISP Redundancy configuration. You **must** disable ISP Redundancy in the Security Gateway object in SmartConsole.
8. Click **OK** to close the Security Gateway / Cluster properties window.

Security Policy Installation Using SD-WAN Interface IP Addresses

Starting from R82, Security Management can use SD-WAN interface IP addresses to establish Security Policy installation connectivity.

When Security Policy installation to a Security Gateway fails because the primary management IP address is unreachable, Security Management attempts to establish a TCP connection to the Security Gateway through the IP addresses of its SD-WAN interfaces.

Security Management tries the SD-WAN interface IP addresses in order. If a TCP connection cannot be established through the first SD-WAN interface IP address, Security Management tries the next SD-WAN interface IP address in the list. This process continues until a TCP connection is successfully established or all available SD-WAN interface IP addresses have been tried.

Use Case

In environments where a Security Gateway is connected to multiple ISPs, one or more ISP links might become unavailable.

If the Security Gateway's primary management IP address belongs to an unavailable ISP link, Security Management might be unable to establish the initial TCP connection through that address.

When SD-WAN interfaces are configured on the Security Gateway, Security Management can attempt Security Policy installation through the other SD-WAN interface IP addresses.

If routing is configured correctly on the Security Gateway, the kernel routing table might update the default route to use an available ISP link. In this case, if Security Management establishes a TCP connection through the IP address of an available SD-WAN interface, Security Policy installation traffic can flow symmetrically over that ISP path.

In some environments, traffic from Security Management might enter the Security Gateway through one SD-WAN interface and return through another SD-WAN interface. This traffic flow can also succeed if the ISP path supports asymmetric routing and does not block the traffic.

Updating SD-WAN Interface Information in the Security Management

Security Management learns the SD-WAN interface configuration when the administrator selects **Get Interfaces** in the Security Gateway object under **Network Management > Topology**. The retrieved interface information is saved in the Security Management database.

To enable Security Management to use SD-WAN interface IP addresses for Security Policy installation connectivity, select **Get Interfaces** after SD-WAN interfaces are configured on the Security Gateway.

This action is required only once after the SD-WAN interfaces are configured. The information is saved in the Security Management database and used for future Security Policy installations.

If you add additional SD-WAN interfaces later, select **Get Interfaces** again to update the saved interface information.

Important:

- Security Management attempts Security Policy installation only through the SD-WAN interface IP addresses configured in the Security Security Gateway object.
- If an SD-WAN interface is located behind a NAT device, Security Management does not initiate the connection to the translated NAT IP address. Security Management attempts the connection only to the actual SD-WAN interface IP address configured in the Security Gateway object.
- This capability applies only to policy installation from Security Management to Security Gateways. It does not apply to Security Gateway monitoring.

Security Gateway Connectivity to Security Management

In some scenarios, the Security Gateway initiates connections to the Security Management Server. For example, the Security Gateway may connect to the Security Management Server to fetch policy, retrieve CRLs, and send logs.

To allow the Security Gateway to use all available external interfaces when connecting to Security Management, configure a valid route to Security Management through each relevant path.

For example, if Security Management is reachable through the Internet, configure either a route to the Security Management Server or a default route through each relevant ISP next hop, with different priorities. If Security Management is reachable only through an MPLS network or another private network, configure the required route through the relevant MPLS or private-network path.

It is recommended to enable next-hop monitoring, such as **Ping on** or **IP Reachability Detection**, for each route so that routes remain active only when the relevant path is reachable.

With this routing configuration, if the active path goes down, the Security Gateway can fail over to the next available route and continue to reach Security Management.

Part 5 - Configuration of VPN and Security Policy in SmartConsole

Procedure

If this Security Gateway / Cluster must participate in VPN (see *"SD-WAN Connection (Steering Behavior) Types" on page 184*), configure the applicable VPN Community of type **Star**:

1. You must configure the Headquarters Security Gateways that work as Center VPN Gateways.

   Configure the applicable Encryption Domain.

2. You must configure the Branch Security Gateways that work as Satellite VPN Gateways:

   a. Configure the applicable Encryption Domain.

   b. Configure the correct Link Selection.

      See *"VPN - Link Selection" on page 235*.

   The correct configuration makes sure you do not lose all VPN connectivity in these scenarios:

   - The main IP address of the Security Gateway object is not one of the link selections.
   - SD-WAN Policy is not loaded.

3. On the **VPN Routing** page of the VPN Community object, select the required setting:

   - If you configure only an SD-WAN Connection Type "**Overlay**" (without "**Backhaul**"), then select **To center only** or **To center and to other satellites through center**.
   - If you configure an SD-WAN Connection Type "**Backhaul**", then select **To center or through the center to other satellites, to Internet and other VPN targets**.

Note - SD-WAN does **not** support Permanent Tunnels.

See the:

- *Site to Site VPN Administration Guide* for your version.
- *Security Management Administration Guide* for your version.

Part 6 - Configuration of Security Policy in SmartConsole

Procedure

See the *Security Management Administration Guide* for your version.

1. Configure the applicable Access Control rules.

   Important:

   a. You must add an explicit rule to allow the service "`echo-request`" between the Security Gateways that participate in this VPN Community.
      - This explicit rule is necessary for the WAN Link probing.
      - The position of this explicit rule must be above all rules that may drop this traffic.

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On

SD-WAN probing	Security Gateways that participate in this VPN Community	Security Gateways that participate in this VPN Community	`Any`
			
			or
			
			Object of the applicable VPN Community
				`echo-request`	`Accept`	`Log`
						
						or
						
						`None`
							`Policy Targets`
							
							or
							
							Security Gateways that participate in this VPN Community

   b. If you selected **Accept ICMP requests** in SmartConsole > **Menu** button > **Global properties** > **FireWall** page, then you must:
      i. Select **Last** or **Before Last** for this option on the **FireWall** page.
      ii. Configure an explicit rule to allow ICMP requests between the Security Gateways - this probing traffic must be encrypted, which requires an explicit rule.

   For more information, see *"SD-WAN Best Practices" on page 235* > sections about ICMP Probing.

2. Configure the applicable NAT rules to hide internal networks behind this Security

Gateway / Cluster.

Important - If you configure an SD-WAN Connection Type "**Overlay**", then it is best to avoid NAT on traffic between internal networks when you configure "Hide NAT".
Do **one** of these, based on your requirements:

- Add an explicit Manual NAT rule (above all Automatic NAT rules) to forbid NAT for traffic between the applicable Source and Destination networks:
  a. In the **Original** columns, select the applicable Source and Destination networks.
  b. In the **Translated** columns, remove all objects so that these cells show "`=Original`".

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Internal networks behind this Security Gateway / Cluster	Internal networks behind this Security Gateway / Cluster	`Any`	`=Original`	`=Original`	`=Original`	`Policy Targets` or Object of this Security Gateway / Cluster	Overlay - disable NAT between internal networks
Automatic Generated Rules							

- In the properties of the VPN Community object > on the **Advanced** page, select **Disable NAT inside the VPN Community**.

3. Install the Access Control Policy on the Security Gateway / Cluster.

What is Next?

Follow *"Step 4 - SD-WAN Wizard" on page 111*.

Step 4 - SD-WAN Wizard

This is a step in the On-Premises Management Deployment.

Important:

- If you do **not** use the SD-WAN Wizard, then you must configure the required settings manually.
- The SD-WAN Wizard creates the required default rules only when you run it for the **first** time.

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle panel, click **Getting Started**.
5. In the **Configure SD-WAN** section, click **Open Wizard**.
6. In Step **(1) Environment**, click **Next**.

   To see more information, hover the mouse cursor over the icon.
7. In Step **(2) Uses Cases**:
   a. **Optional:** Select **Use only Internet use cases, but no Overlay VPN use cases**.

      This disables several use cases.

      To see more information, hover the mouse cursor over the icon.
   b. Click the predefined practices you want to disable (or enable again).
   c. Click **Next**.
8. In Step **(3) Quantum Gateways**:
   a. Select the connected Security Gateways you want to use.

      To see more information, hover the mouse cursor over the icon in the **Required** column.
   b. Click **Next**.

9. In Step **(4) WAN Link Mapping**:
    a. If you already have WAN Links configured on your Security Gateways, you can map them to specific interfaces.

       To see more information, hover the mouse cursor over the ⓘ icon in the column headers.

    b. Click **Next**.
10. In Step **(5) Summary**:
    a. Select the applicable option:
       - **I will publish the changes manually later**
       - **Publish the change now, and I will enforce the policy manually later**
       - **Publish and Enforce the policy now**

    b. Click **Done**.
11. Wait for the SD-WAN Wizard to create the required objects and the SD-WAN Policy.
12. If needed, change the object settings, add new objects, change the SD-WAN Policy rules.

    See:
    - *"Configuring SD-WAN Policy" on page 160*.
    - *"Configuring Steering Behavior" on page 171*.
    - *"WAN Link Mapping" on page 207*.
13. From the top toolbar, click **Publish** to save the changes.
14. From the top toolbar, click **Enforce** to apply the changes.

    The orange frame on this button means there are changes that are not enforced.

    In the popup window that opens, click **Publish & Enforce Policy**.
15. See *"SD-WAN Monitoring" on page 212*.

Configuring a Maestro Security Group for SD-WAN

Supported Security Gateways

- R82.10 and higher

Prerequisites

For information about Maestro, see the:

- *Maestro Getting Started Guide*
- *Scalable Platforms Administration Guide* for your version (R82 and higher).
- *Maestro Administration Guide* for your version (R81.20 and lower).

Configuration

Follow *"Step 3 - Configuration on Security Gateways" on page 83* with these changes:

- **Part 2 - Configuration of SD-WAN interfaces on the Security Gateway** >

  Procedure for a Security Gateway that runs Gaia OS

  You must configure the required interface settings in one of these ways:

  - In Gaia Portal on the Security Group.
  - In Gaia gClish on the Security Group.

- **Part 3 - Installation of the Nano-Agent on the Security Gateway** >

  Procedure for manual onboarding of a Security Gateway

  You must install the Nano-Agent on all Security Group Members:

  1. Get the Authentication Token you copied earlier from your Quantum Profile in Check Point Portal.
  2. Connect to the command line on the Security Group.
  3. Log in.
  4. If your default shell is Gaia gClish, go to the Expert mode:

     ```
     expert
     ```

5. Install the Nano-Agent on all Security Group Members:

```
nano-egg --install --token <Authentication Token you copied earlier from your Quantum Profile> --run-all-members
```

6. Examine the status of the required Nano-Services:

```
g_allc cpnano -s
```

The section "`Service settings`" in the output must show "`Status: Running`" for these services:

- `Check Point Orchestration Nano Service`
- `Check Point Messaging Proxy Nano Service`
- `Check Point SDWan Nano Service`
- `Check Point Cpview Metric Provider Nano Service`
- `Check Point SD-WAN Logger Nano Service`

7. In Check Point Portal > **SD-WAN**, navigate to the **Network** view > **Agents** page.

   This page must show each Security Group Member.

   Example:

Host	Name	IP Address	Quantum version	Hardware	SD-WAN applicable	SD-WAN active	Policy version	Profiles
MySG-s01-01	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile
MySG-s01-02	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile
MySG-s01-03	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile
MySG-s02-01	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile
MySG-s02-02	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile
MySG-s02-03	Maestro	192.168.6.76	R82	Maestro	✓	✓	Multiple versions	Quantum Profile, SD-WAN Profile

Notes:

- Do **not** install the Nano-Agent on Maestro Orchestrators.
- If you add a new Security Group Member later, then you must manually install the Nano-Agent on that new Security Group Member:
  1. Get the ID of the new Security Group Member in this Security Group.
  2. Connect to the command line on the new Security Group Member using the "`member`" command on the Orchestrator or on the Security Group.
  3. Log in to the Expert mode.
  4. Install the Nano-Agent on the new Security Group Member:

     ```
     nano-egg --install --token <Authentication Token
     you copied earlier from your Quantum Profile>
     ```

  5. Examine the status of the required Nano-Services:

     ```
     cpnano -s
     ```

- Check Point Portal > **SD-WAN** shows:
  - The **Network** view > **Agents** page shows only the object of each Security Group Member.
  - All other sections and fields show only the Security Group object.
- The Security Group selects the Security Group Member that runs the SD-WAN probing to run the Maestro task called "**SDWAN**". This Security Group Member is considered the "**SDWAN Task Owner (STO)**".
  Run this command on the Security Group to see which Security Group Member runs which Maestro task:

  ```
  asg stat -i tasks
  ```

- In a normal state, all Security Group Members must run the same SD-WAN Policy (with the same "`Policy ID`" values).
  If the Policy ID on a Security Group Member (Local Policy) differs from the Policy ID on the STO Security Group Member (Global Policy), then the non-STO Security Group Member begins to perform its own SD-WAN probing.
  The non-STO Security Group Member stops performing its own SD-WAN probing only when its Policy ID (Local Policy) is the same as the Policy ID on the STO Security Group Member.
  Run this command to see the SD-WAN policy:
  - To see the outputs that differ between Security Group Members (the policy installation time may differ by several seconds):

    ```
    g_allc cpsdwan stat
    ```

  - To see the complete outputs from each Security Group Member:

    ```
    g_all cpsdwan stat
    ```

- To see the probing status in CPView:
  1. Run on the Security Group:

     ```
     cpview
     ```

2. From the top, click **Advanced** > **SDWAN** > **Probing**.
   The row **Gateway Probing State** shows one of these:
   - `SD-WAN Task owner`
     This Security Group Member is the STO - responsible for the Global probing for the entire Security Group.
   - `Active probing member`
     This Security Group Member is not the STO, but it is currently performing the probing.
     Probably because its SD-WAN Policy ID is different than that of the STO.
   - `Active non probing member`
     This Security Group Member is not the STO, but an active Security Group Member that is not performing the probing.
     This is a normal state, when all Security Group Members have the same SD-WAN Policy ID.
   - `Standby on active site`
     This Security Group Member is currently in the Standby mode and does not handle traffic in general.
   - `Standby site member`
     This Security Group Member is currently a member of a Standby Site.

Workflow for Smart-1 Cloud

This section describes the deployment procedure with Smart-1 Cloud.

For other deployment procedures see:

- *"Workflow for an On-Premises Management Server" on page 67*

Step 1 - Configuration in Check Point Portal

This is a step in the Smart-1 Cloud Deployment.

Check Point Portal is a web-based component in which you configure SD-WAN Policy (rules).

Part 1 - Creating an Account in the Check Point Portal

Procedure

1. Create an account in the Check Point Portal:

   For more information, see the *Check Point Portal Administration Guide* > "*Getting Started*".

   a. In a web browser, go to:

      https://portal.checkpoint.com/create-account

b. Enter this information:

   i. In the **Company Name** field, enter the desired name for your account.

      Note - Account name cannot include special characters (`! @ # $ % ^ & *` or other special characters).

   ii. In the **First Name** and **Last Name** field, enter your name.

   iii. In the **Email** field, enter your company email.

   iv. In the **Phone** field, select your country and enter your contact phone number.

   v. In the **Select Country** field, select the applicable country.

   vi. In the **Select Data Residency** field, select the applicable region.

      The **Available Region** window opens and shows available services based on region.

      To see services available for a specific region, click a region's name.

      A green check mark next to the service name indicates an available service for that region.

      Best Practice - If you require a service that is not in your selected region, then we recommend that you select a region with the necessary services. We do **not** recommend the migration of an account from region to region.

   vii. In the **Customer** field, select the applicable type that describes this account.

      It is possible to change the account type after the account is created.

c. **Optional:** Select **Subscribe to Check Point Product News**.

d. Select **I accept the Check Point Portal terms of service and the Privacy Policy**.

e. In the CAPTCHA section, select **I'am not a robot**.

f. Click **Next**.

The Check Point Portal sends you an email with activation instructions.

2. Log in to the Check Point Portal:
   a. Go to *Check Point Portal*.
   b. Make sure you log in with the same email used to create the account.
   c. Below the account name, select a **Region**.
   d. Click **Next**.

Part 2 - Initial Configuration in Check Point Portal

Procedure

1. In the Check Point Portal, in the top left corner, click the **Menu** button.
2. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. Read the **Check Point Portal terms of service** and **Privacy Policy**.
4. Select **I accept the Check Point Portal terms of services and the Privacy Policy** and click the **TRY NOW** button.
5. Wait for several minutes for the **SD-WAN** service to become available in your account.

   Wait for several minutes for the SD-WAN views to appear (see *"SD-WAN Service GUI" on page 42*).

What is Next?

Follow *"Step 2 - Configuration in Smart-1 Cloud" on page 121*

Step 2 - Configuration in Smart-1 Cloud

This is a step in the Smart-1 Cloud Deployment.

Part 1 - Prerequisites for Smart-1 Cloud

Prerequisites

1. Register to the Check Point Portal.

   In the *Check Point Portal Administration Guide*, see the chapter "Getting Started":

   a. Follow the section "**How to Create an Account**".

   b. Follow the section "**How to Log in to your Account**".

2. Enable the Smart-1 Cloud Application:

   a. On the Check Point Portal top left corner, click the Menu button.

   b. In the **Hybrid Mesh Network Security** column, click **Management & Smart-1 Cloud**.

   c. Approve the service terms and privacy policy and check the box:

   ```
   I accept the Infinity Portal terms of service and the
   privacy policy
   ```

   d. Click **Try Now**.

   e. The Check Point Portal sends an email to your email account with confirmation of your Smart-1 Cloud registration.

   f. After you approve your registration, the Smart-1 Cloud page automatically refreshes, and you can start to use the application.

3. Create and Deploy a New Smart-1 Cloud:
   a. Click **Get Started**.
   b. Enter the required information to configure the service:

Field	Description
Service Identifier	The service identifier that you enter is used as a prefix for the unique identifier generated by the application.
Desired Log Retention Period	▪ The desired retention period to keep the logs. ▪ Logs are deleted after the defined period. ▪ If the available storage space cannot maintain the desired log retention period, Smart-1 Cloud sends a notification to your email. When the storage is full, Smart-1 Cloud deletes old logs.

   c. Click **Create**.

      The **Preparing Account** window opens.

      It takes 1-2 minutes to create a new service.

      After the process is complete, an email is sent to your account.
4. In your User Center Account, add your Smart-1 Cloud Account.

   As a result, Smart-1 Cloud can fetch all licenses and contracts automatically.
5. If you configured Manual Proxy ARP (sk30197) and Manual NAT rules, then you must follow these steps in SmartConsole:
   a. Click **Menu** > **Global properties**.
   b. In the left tree, click **NAT - Network Address Translation**.
   c. Select **Automatic ARP configuration**.
   d. Select **Merge manual proxy ARP configuration**.
   e. Click **OK**.

Part 2 - Configure Configuration Sharing and Onboarding

Procedure

1. Connect with the Desktop SmartConsole to Smart-1 Cloud:
   a. Download the SmartConsole package from one of these places in the Smart-1 Cloud Application:
      - From the left navigation panel, click the **Welcome** view.

        In the **Service Management** column, click **Download SmartConsole for Windows**.

        The **Settings** view > **SmartConsole** page opens.
      - From the left navigation panel, click the **Settings** view > **SmartConsole** page.

   b. Select the desired package:
      - **SmartConsole Installation**
      - **SmartConsole Portable** (for more information, refer to sk116158)

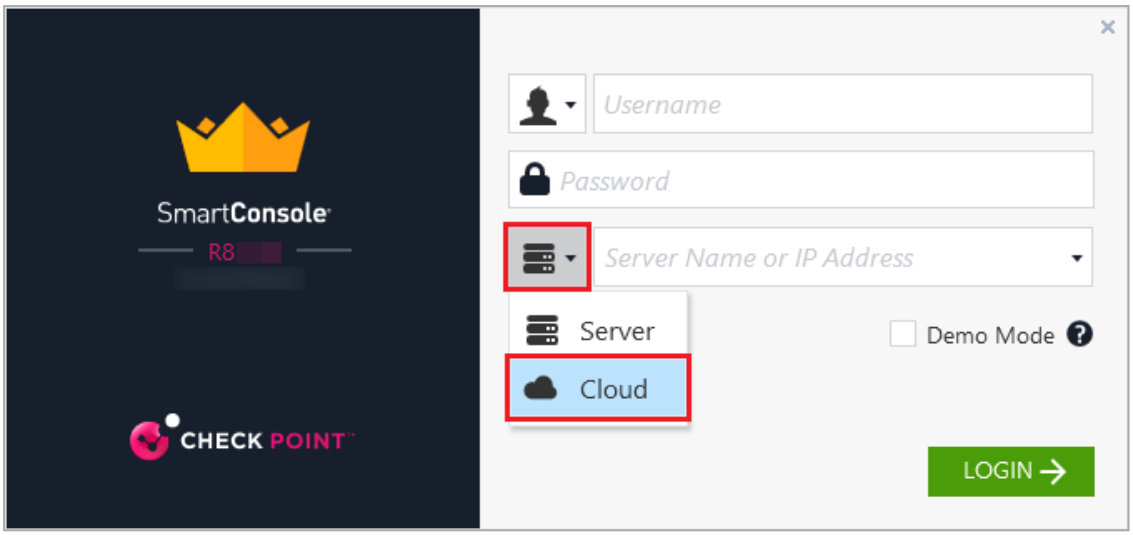
   c. Install SmartConsole:
      - If you downloaded the EXE file, double-click it and follow the instructions on the screen.
      - If you downloaded the ZIP file, extract it (refer to sk116158).

   d. Open SmartConsole.

      See the R82 SmartConsole Online Help for information about how to use SmartConsole.

      To open the relevant help page for a SmartConsole screen, press the **F1** key.

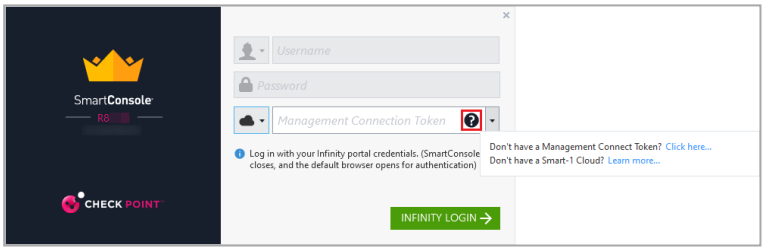
e. From the server drop-down list, select **Cloud**.



f. Enter the **Management Connection Token**.

Note

- You can hover over the help icon to see the applicable links:



- Get the token on the **Settings** view > **SmartConsole** page.
  Click the **"Copy to clipboard"** icon.

g. Click **Infinity Login**.

h. SmartConsole closes, and the default browser opens for authentication.

i. Enter your Check Point Portal administrator credentials.

j. Click **Sign in** and let the browser open Check Point SmartConsole.

k. SmartConsole portal opens for you to start work.

2. From the left navigation panel, click **Infinity Services**.

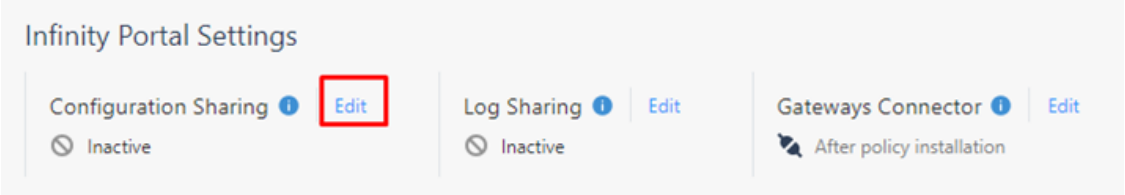


3. Enable **Configuration Sharing**:

   Note - **Log Sharing** is enabled automatically, although not indicated in SmartConsole.

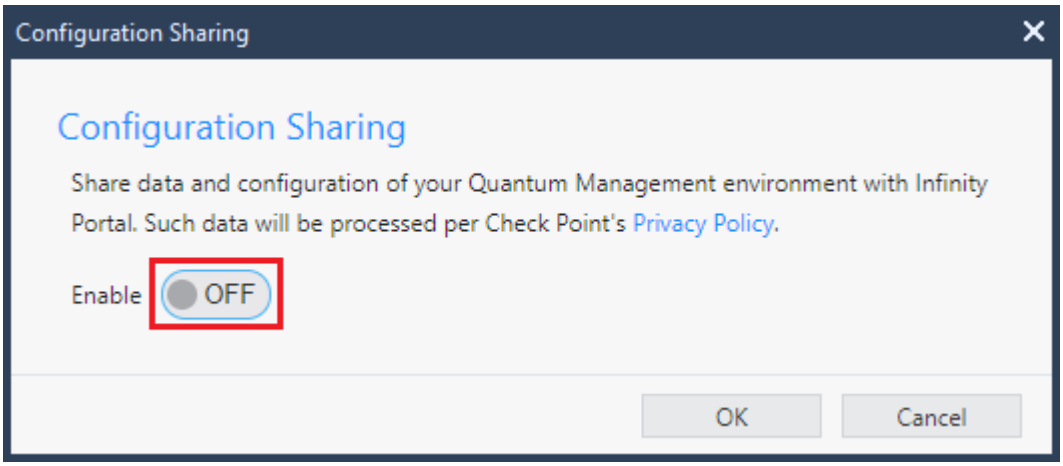
   a. In SmartConsole, in the bottom left section **Infinity Portal Settings**, on the right of **Configuration Sharing**, click **Edit**.

      Example:

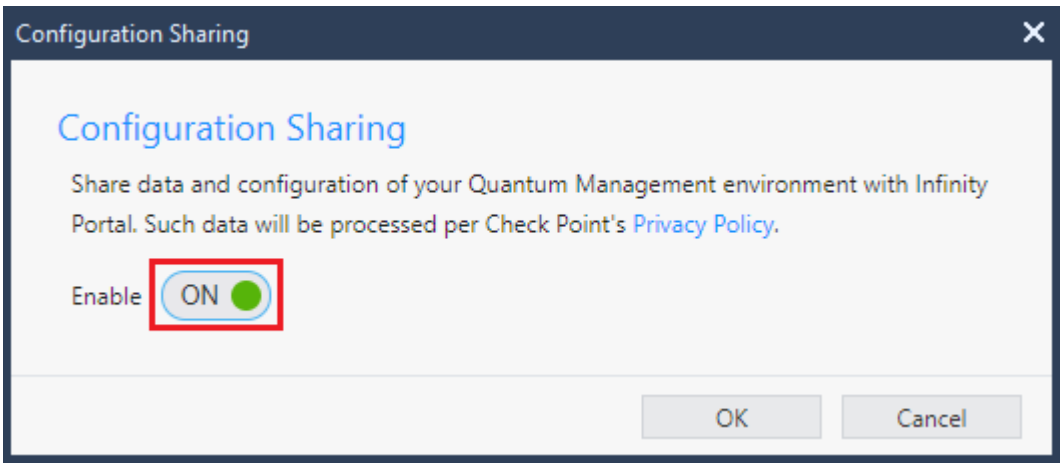


   b. The **Configuration Sharing** window opens.

c. Near the **Enable** option, click the **OFF** button.



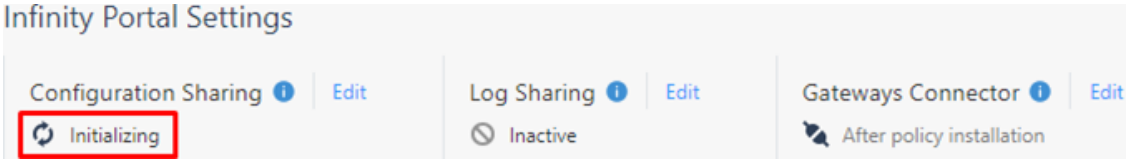
It must change to **ON**.

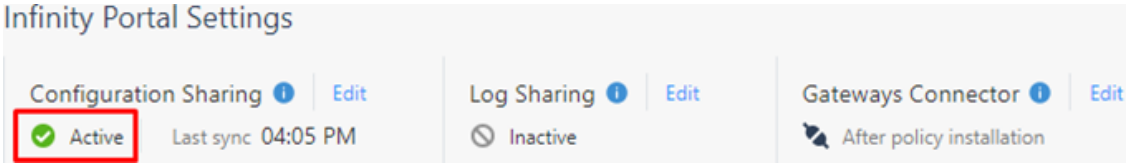


Click **OK**.

d. The configuration sharing starts, and after some time its status changes from **Initializing** to **Active**.

Example:

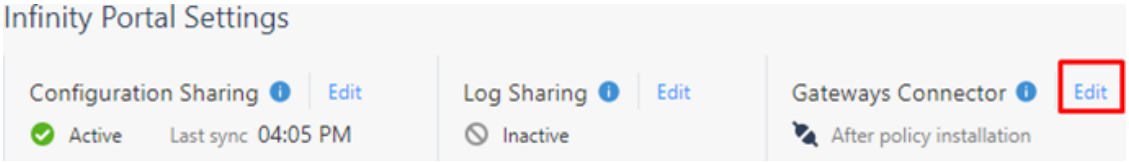




From this point, objects configured in SmartConsole on the on-premises Management Server appear in Check Point Portal as assets.

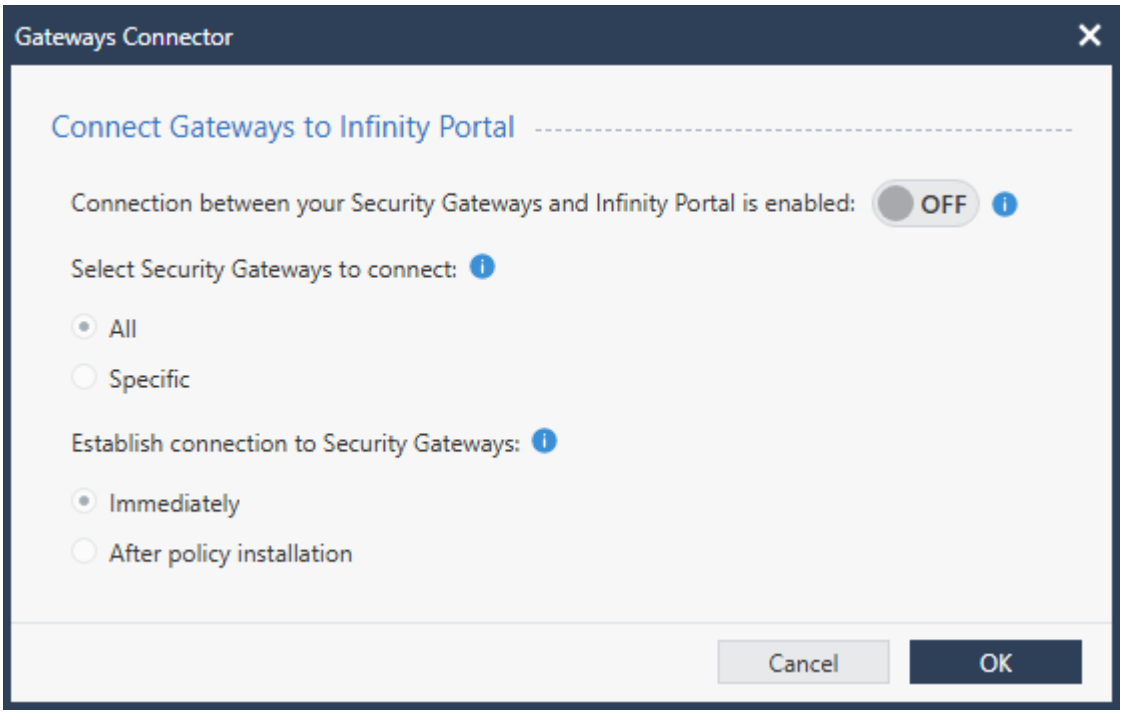
4. Configure how to onboard the supported SD-WAN Security Gateways:

   a. In the bottom left section **Infinity Portal Settings**, on the right of **Gateways Connector**, click **Edit**.

   b. The **Gateways Connector** window opens.

c. Select which supported SD-WAN Security Gateways to onboard and when:



i. Move the toggle **Connection between your Security Gateways and Infinity Portal isenabled** from **OFF** to **ON**.

ii. In the section **Select Security Gateways to connect**, select which supported Security Gateways to onboard:

For more information, click the **(i)** icon and see sk180557.

- **All**

  All supported Security Gateways establish connection with Check Point Portal.

- **Specific**

  Only the selected supported Security Gateways establish connection with Check Point Portal.

iii. In the section **Establish connection to Security Gateways**, select when to onboard the supported Security Gateways:

For more information, click the **(i)** icon and see sk180557.

- **Immediately**

  This is the default. Supported SD-WAN Security Gateways try to establish an immediate connection with Check Point Portal and then during every subsequent policy installation.

- **After policy installation**

  Supported SD-WAN Security Gateways try to establish a connection with Check Point Portal only after you complete this procedure and install the Access Control policy.

Note - You can always change this setting later in SmartConsole > **Infinity Services** view > in the bottom right corner, on the right of **Gateways Connector**, click **Edit**.

iv. At the bottom, click **OK**.

What is Next?

Follow *"Step 3 - Configuration on Security Gateways" on page 130*.

Important - Connect the Security Gateways to Smart-1 Cloud only after you configure the Security Gateways for SD-WAN. This makes sure the Security Gateway objects automatically get the correct interface topology.
To connect a Security Gateway to Smart-1 Cloud, follow the *Smart-1 Cloud Administration Guide* > Chapter "*Connecting Gateways and Clusters*".

Step 3 - Configuration on Security Gateways

This is a step in the Smart-1 Cloud Deployment.

Part 1 - Prerequisites for Security Gateways

Prerequisites

1. The required version of the Security Gateway / Cluster must be up and running.

Platform	Instructions
Security Gateways that run Gaia OS	a. Download the required image from sk180605. b. Follow the *Installation and Upgrade Guide* for your version. c. Install the applicable Jumbo Hotfix Accumulator.
Spark Firewall Appliances that run Gaia Embedded OS	a. R81.10.05 and higher (we recommend R81.10.17). Refer to the corresponding Home Page SK article in sk179615. b. Centrally Managed.

Note - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.

2. The Security Gateway / Spark Firewall Appliance / Cluster Members must connect to the Internet.

Part 2 - Configuration of SD-WAN interfaces on the Security Gateway

Procedure for a Security Gateway that runs Gaia OS

Note - For a Maestro Security Group, see *"Configuring a Maestro Security Group for SD-WAN" on page 113*.

1. Configure the SD-WAN interfaces on the Security Gateway / each Cluster Member.

   You can configure the required SD-WAN interfaces in Gaia Portal or Gaia Clish.

   Notes:
   - This configuration also applies to VLAN interfaces.
     If you configure SD-WAN on a VLAN interface, then it is **not** supported to configure SD-WAN on the parent physical interface.
   - This configuration also applies to clusters, in which the IP addresses of Cluster Members and the Cluster Virtual IP address belong on different subnets.

   #### Configuration of a Security Gateway in Gaia Portal

   a. Connect to Gaia Portal.

   b. From the left tree, click **Network Interfaces**.

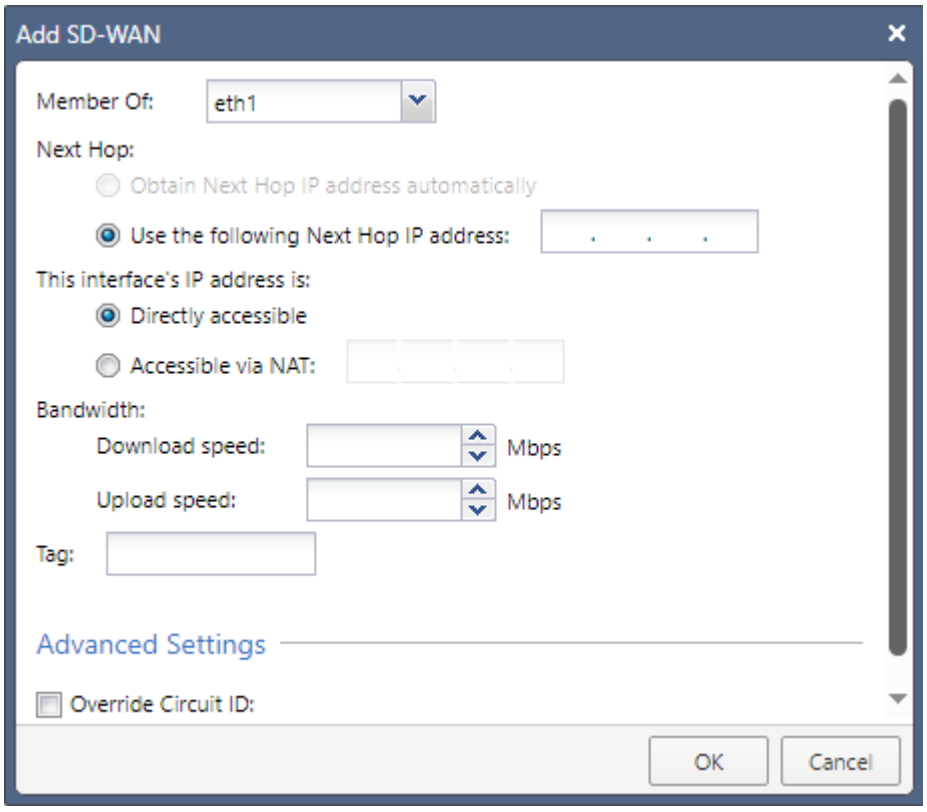
   c. Configure the applicable interfaces that you plan to use for SD-WAN.

      Enable the interfaces and configure the IPv4 address.

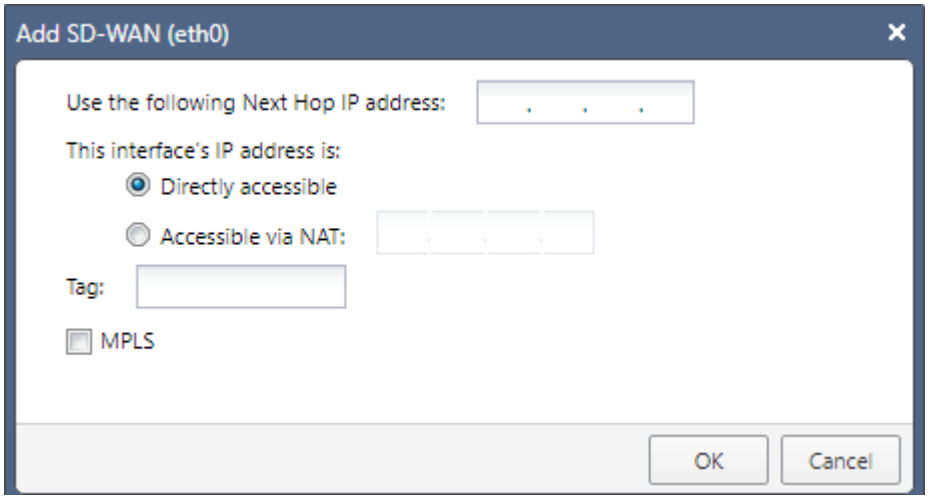
      See the *Gaia Administration Guide* for your version > "*Network Management*" > "*Network Interfaces*" > "*Physical Interfaces*".

   d. In the section **SD-WAN Interfaces**, click **Add**.

Example from R81.20 Jumbo Hotfix Accumulator, Take 79 and higher:



Example from R81.20:



e. Select the applicable interface that connects to the applicable ISP.

f. In the section **Next Hop**, configure the applicable next hop IP Address for the ISP, to which this interface connects.

In the field **Use the following Next Hop IP address**, enter the applicable IP address.

Note - This section title "**Next Hop**" is available in these Security Gateway versions:

- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

g. In the section **This interface's IP address is**, configure how SD-WAN rules get the IP address of this interface:

- **Directly accessible**

  Specifies that this interface has a public IP address, to which peers can connect directly.

  This applies to the interface with an IP address that is configured statically or by a DHCP server.

  Note - You must select this option if an ISP assigns an IP address dynamically (for example, when a Security Gateway connects to the Internet through a modem).
  For additional information, see *"SD-WAN Configuration for DAIP Security Gateways" on page 220*.

- **Accessible via NAT**

  Specifies that an external device or an ISP applies Static NAT on the IP address of this interface.

  Enter the applicable static IP address after this external NAT, as the peers receive it.

  Notes:
  - This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*).
    This option configures the IP address that VPN peers must use to negotiate the Site to Site VPN tunnel with this Security Gateway.
  - You do not need to configure NAT rules in SmartConsole for this external NAT.

Summary:

Option in Gaia Portal	When to Select
Directly accessible	SD-WAN interface with a Static IP address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with a Static IP address) --- (no NAT device) ---

Option in Gaia Portal	When to Select
	SD-WAN interface with a Dynamically Assigned IP Address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with DAIP) --- (no NAT device) ---
	SD-WAN interface with a Static IP address that is located behind a Dynamic NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns an IP address dynamically] ---
Accessible via NAT	This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*). SD-WAN interface with a Static IP address that is located behind a Static NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns a static IP address] ---

h. **Optional:** In the section **Bandwidth**, configure the applicable limits for the **Download speed** and **Upload speed**.

Note - This section is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

You can use these limits in the SD-WAN Steering Behavior objects. See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

i. **Optional:** In the **Tag** field, enter a desired interface tag. Example: `ISP1`

See the description and the example in *"WAN Link Mapping" on page 38*.

j. Select **MPLS**, if this interface connects to to a Private Link (for example, MPLS).

Note - This checkbox is available only in these Security Gateway versions:
- R81.20 Jumbo Hotfix Accumulator, Take 76 and lower.
- R81.20 without the Jumbo Hotfix Accumulator.

k. **Optional:** In the section **Advanced Settings**:

Note - This section is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

i. Select **Override Circuit ID**.

See *"SD-WAN Circuit ID" on page 248*.

ii. Enter a value between 0 and 255.

Important:
- The value 0 is the default for Public WAN Links.
- The value 1 is the default for Private WAN Links.

l. Click **OK**.

Configuration of a Security Gateway in Gaia Clish

For more information, see *"SD-WAN Configuration in Gaia Clish" on page 293*.

a. Connect to the command line on the Security Gateway / each Cluster Member.

b. Log in.

c. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

d. Configure the applicable interfaces that you plan to use for SD-WAN.

Enable the interfaces and configure the IPv4 address.

See the *Gaia Administration Guide* for your version > "*Network Management*" > "*Network Interfaces*" > "*Physical Interfaces*".

e. Configure the applicable next hop IP Address for the ISP, to which this interface connects:

```
set interface <Name of Interface> sdwan next-hop <IP Address of ISP Next Hop>
```

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1
```

f. Configure how SD-WAN rules get the IP address of this interface:

- If this interface has a public IP address, to which peers can connect directly, do not configure anything.

  This applies to the interface with an IP address that is configured statically or by a DHCP server.

  Notes:
  - In Gaia Portal, this corresponds to the option "**Directly accessible**".
  - You must select this option if an ISP assigns an IP address dynamically (for example, when a Security Gateway connects to the Internet through a modem). For additional information, see *"SD-WAN Configuration for DAIP Security Gateways" on page 220*.

- If an external device or an ISP applies NAT on the IP address of this interface, then configure the applicable IP address after this external NAT, as the peers receive it:

  ```
  set interface <Name of Interface> sdwan next-hop
  <IP Address> nat <IP Address after External NAT>
  ```

  Example:

  ```
  set interface eth1 sdwan next-hop 192.168.20.1
  nat 172.30.40.5
  ```

  Notes:
  - In Gaia Portal, this corresponds to the option "**Accessible via NAT**".
  - This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*).
    This option configures the IP address that VPN peers must use to negotiate the Site to Site VPN tunnel with this Security Gateway.
  - You do not need to configure NAT rules in SmartConsole for this external NAT.

Summary:

Option in Gaia Clish	When to Configure
Directly accessible	SD-WAN interface with a Static IP address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with a Static IP address) --- (no NAT device) ---
	SD-WAN interface with a Dynamically Assigned IP Address that connects to your network directly (without a NAT device): [Security Gateway] (SD-WAN interface with DAIP) --- (no NAT device) ---
	SD-WAN interface with a Static IP address that is located behind a Dynamic NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns an IP address dynamically] ---

Option in Gaia Clish	When to Configure
Accessible via NAT	This option applies only to the "Overlay" configuration (see *"SD-WAN Connection Type - "Overlay"" on page 200*). SD-WAN interface with a Static IP address that is located behind a Static NAT device: [Security Gateway] (SD-WAN interface with a Static IP address) --- [NAT device that assigns a static IP address] ----

g. If this interface connects to a Private Link (for example, MPLS):

```
set interface <Name of Interface> sdwan next-hop <IP Address> is_mpls true
```

Note - This command is available only in these Security Gateway versions:
- R81.20 Jumbo Hotfix Accumulator, Take 76 and lower.
- R81.20 without the Jumbo Hotfix Accumulator.

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1 is_mpls true
```

h. **Optional:** Configure a desired interface tag:

See the description and the example in *"WAN Link Mapping" on page 38*.

```
set interface <Name of Interface> sdwan next-hop <IP Address> tag "<Tag Name>"
```

Example:

```
set interface eth1 sdwan next-hop 192.168.20.1 tag "ISP1"
```

i. **Optional:** Configure the download speed limit (in Mbps):

```
set interface <Name of Interface> sdwan download-speed
<1 - 1000000>
```

Note - This command is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

Example:

```
set interface eth1 sdwan download-speed 500000>
```

j. **Optional:** Configure the upload speed limit (in Mbps):

```
set interface <Name of Interface> sdwan upload-speed
<1 - 1000000>
```

Note - This command is available only in these Security Gateway versions:
- R82 and higher.
- R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464).

You can use these limits in the SD-WAN Steering Behavior objects.
See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

Example:

```
set interface eth1 sdwan upload-speed <1 - 100000>
```

k. Examine the SD-WAN configuration on the interface:

```
show interface <Name of Interface> sdwan
```

l. Save the configuration:

```
save config
```

2. Configure the applicable default routes on the Security Gateway / each Cluster Member.

   The Security Gateway / Cluster Member uses these default routes:

   - For traffic that does not match the configured SD-WAN rules.
   - For traffic that the Security Gateway / Cluster Member creates (for example, to connect to Check Point cloud).

   See the *Gaia Administration Guide* for your version > "*Network Management*" > "*IPv4 Static Routes*".

Important:

- For each Internet Service Provider (ISP), you must configure one default route with unique priority.
  The reasons for this configuration are:
  - A legacy ISP backup that is based on the link availability, if the SD-WAN service does down on the Security Gateway / Cluster Member.
  - The Security Gateway / Cluster Member sends its traffic (local connections) to the Internet based on the operating system routing table and not based on SD-WAN Policy rules.
  - The Security Gateway / Cluster Member must have an active route to the destination of the packet to process it. This applies to both cleartext traffic and VPN traffic.
    If only one ISP has a default route, and it goes down, then all overlay connections are lost and do not fail over.
    This does not apply in Local Breakout, because its mechanism has its routing table that does not depend on the operating system routing.
- The Security Gateway / Cluster Member cannot have different ISP default routes with the same priority.
  When the Security Gateway / Cluster Member cannot use an ISP default route with the lowest priority (for example, cannot reach the ISP), it uses another ISP default route with the next higher priority.
- It is **not** mandatory to configure static routes to branches, if they are part of the "Overlay" because the VPN clean up rule in the SD-WAN Policy is always matched.
- If the Security Gateway / Cluster Member has a private line, such as MPLS, which is part of the overlay, then it is a best practice to configure such routes that send traffic for all the overlay destination networks to the MPLS next hop. In this case, even if all ISP links are down, and no active default route exist in the operating system kernel, the specific route on the MPLS makes sure that the "Overlay" traffic continues to work over the MPLS SD-WAN interface. Without an active route to the destination, the packet is lost in the routing table, before the VPN encryption takes place.

Procedure for a Spark Firewall Appliance that runs Gaia Embedded OS

1. Configure the SD-WAN interfaces on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

   Note - This configuration also applies to VLAN interfaces.
   If you configure SD-WAN on a VLAN interface, then it is **not** supported to configure SD-WAN on the parent physical interface.

   You configure these SD-WAN interfaces in the WebUI, or Gaia Clish.

Configuration of a Spark Firewall Appliance in the WebUI

See *R82.00.X Spark Firewall Appliances Centrally Managed Administration Guide*

See the *R82.00.X Spark Firewall Appliances Centrally Managed Administration Guide* > "*Managing the Device*" > "*Configuring Internet Connectivity*".

a. Connect to the WebUI.

b. From the left tree, click **Device**.

c. In the middle pane, expand the section **Network** and click **Internet**.

d. Configure two Internet connections - one for each ISP:

   i. Click **Add an Internet connection**.

      The **New Internet Connection** window opens.

   ii. On the **Configuration** tab:

      i. In the **Connection name**, enter the applicable name for this connection.

      ii. In the **Interface** field, select the applicable interface.

      iii. In the **Connection type** field, select the applicable type.

   iii. On the **Connection Monitoring** tab:

      i. Select **Automatically detect loss of connectivity to the default gateway**.

      ii. Select **Monitor connection state by sending probe packets to one or more servers on the Internet**.

      Local connections (originating from the Spark Firewall Appliance) use the main routing table and are not affected by SD-WAN Local Breakout routing.

   iv. On the **Advanced** tab:

      Configure the applicable options based on the connection type.

      In firmware versions R81.10.15 and higher:

      i. Expand the section **SD-WAN Settings**.

      ii. **Optional:** Configure the applicable limits for the **Download speed** and **Upload speed**.

      Note - You can use these limits in the SD-WAN Steering Behavior objects.
      See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**.

      iii. **Optional:** Select **Override circuit ID**.

      See *"SD-WAN Circuit ID" on page 248*.

      Enter a value between 0 and 255.

   v. Click **Save**.

Configuration of a Spark Firewall Appliance in Gaia Clish - R81.10.10 and higher

Important - The Spark Firewall Appliances configure the SD-WAN next hop based on the Internet configuration.

a. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

b. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

c. Configure two Internet connections - one for each ISP.

Use this command:

```
add internet-connection name "<Name of Connection>"
interface <Name of Interface>
```

See the *R82.00.X Spark Firewall Appliances CLI Reference Guide* > "*Configuring the Internet Connections*" > "*Adding Internet Connections*".

Example:

```
add internet-connection name Internet2 interface DMZ
type static ipv4-address 192.168.223.5 subnet-mask
255.255.255.0 default-gw 192.168.223.4
```

Configuration of a Spark Firewall Appliance in CLI - only R81.10.05, R81.10.07, and R81.10.08

Important - The Spark Firewall Appliances configure the SD-WAN next hop based on the Internet configuration.

a. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

b. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

c. Configure two Internet connections - one for each ISP.

Use this command:

```
add internet-connection name "<Name of Connection>"
interface <Name of Interface> <options>
```

See the *R82.00.X Spark Firewall Appliances CLI Reference Guide* > "*Configuring the Internet Connections*" > "*Adding Internet Connections*".

Example:

```
add internet-connection name Internet2 interface DMZ
type static ipv4-address 192.168.223.5 subnet-mask
255.255.255.0 default-gw 192.168.223.4
```

Part 3 - Installation of the Nano-Agent on the Security Gateway

The Nano-Agent connects the Security Gateway / each Cluster Member to Check Point Portal, and enable the automatic installation and update of the SD-WAN policy from Check Point Portal.

There are two possible onboarding options - automatic (recommended) and manual.

Procedure for automatic onboarding of supported Security Gateways

Note - For automatic on-boarding of supported SD-WAN Security Gateways, see the requirements in sk180557.

1. In SmartConsole, make sure the Management Server is connected to Check Point Portal and automatic onboarding is enabled.
    a. From the left navigation panel, click **Infinity Services**.
    b. At the top, SmartConsole must show **Connected to Check Point Portal** and **Status: Active**.
    c. In the bottom right corner, on the right of **Gateways Connector**, click **Edit**.
    d. The option **Connection between your Security Gateways and Infinity Portal is enabled** must show **ON**.
2. In Check Point Portal, check if the Security Gateway is already connected:
    a. In Check Point Portal, in the top left corner, click the **Menu** button.
    b. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
    c. From the left navigation panel, click **Network**.

d. In the middle section, click **Agents**.

Possible next steps:

- If your Security Gateway appears on this page, then skip to "**Part 4 - Configuration of the Security Gateway object in SmartConsole**" below.
- If your Security Gateway does **not** appear on this page, then in SmartConsole, connect this Security Gateway:
  i. In the bottom right corner, on the right of **Gateways Connector**, click **Edit**.
  ii. In the section **Select Security Gateways to connect**, select **Specific** and select this Security Gateway.
  iii. In the section **Establish connection to Security Gateways**, select **Immediately**.
  iv. At the bottom, click **OK**.
  v. Wait for several minutes.
  vi. In Check Point Portal, check the **Agents** page again.

Procedure for manual onboarding of a Security Gateway

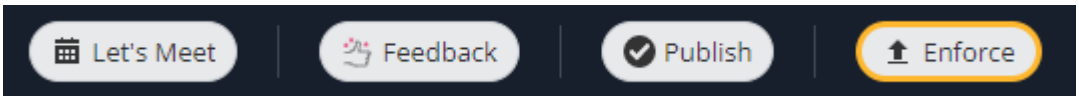
Note - For a Maestro Security Group, see *"Configuring a Maestro Security Group for SD-WAN" on page 113*.

1. Get the Authentication Token from the Quantum Profile in SD-WAN Application.
   a. In the Check Point Portal, in the top left corner, click the **Menu** button.
   b. From the drop-down list, in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
   c. In the middle section, click **Profiles**.
   d. Click **Quantum Profile** to open it.

   Note - The SD-WAN Application creates this Quantum Profile automatically in these cases:
   - You connect your on-premises Management Server to Check Point Portal and configure Object Sharing.
     See *"Workflow for an On-Premises Management Server" on page 67*.
   - You enable the Smart-1 Cloud Application and configure Object Sharing.
     See *"Workflow for Smart-1 Cloud" on page 118*.

e. From the top of the page, click the **Enforce** button.

Note - Although you did not configure the SD-WAN Policy yet, this step is necessary.

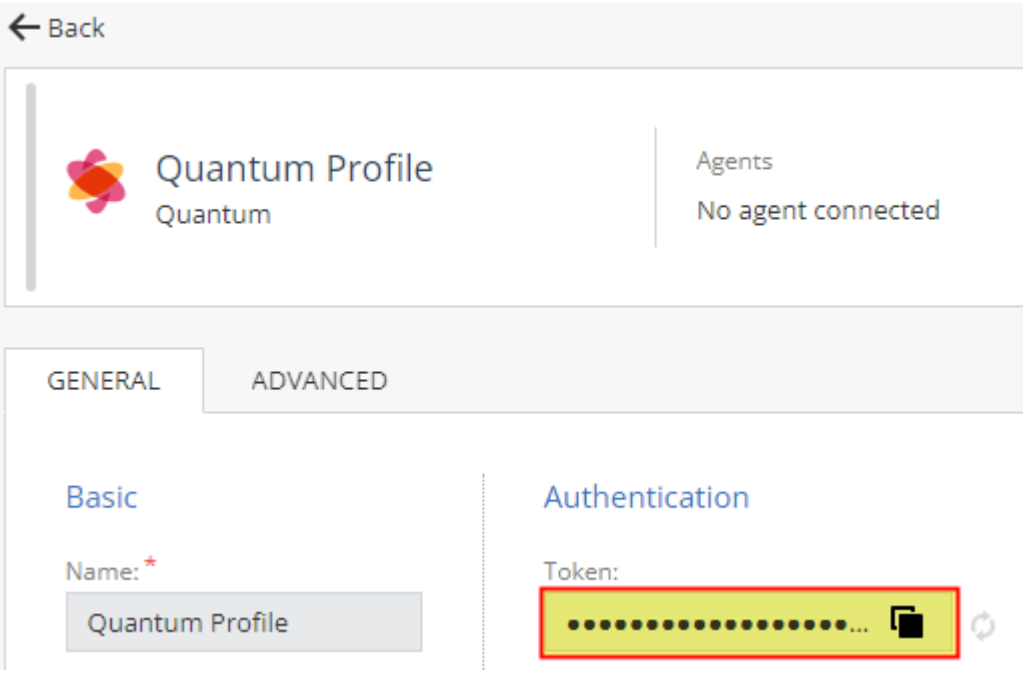


In the popup window that opens, click **Publish & Enforce Policy**.

f. In the middle pane, in the section **Authentication**, the field **Token** must be populated (dots appear instead the actual token value).

This means the service generated the required token.

Example:



g. Save your token:

i. In the section **Authentication**, in the field **Token**, click the **Copy** icon on the right.

ii. Save this string.

You use this token to install the Nano-Agent.

Best Practice - Connect all SD-WAN Security Gateways to Check Point Portal with the same token (to make the policy configuration easier).

2. Connect to the command line on the Security Gateway / each Cluster Member.

3. Log in.
4. If your default shell is Gaia Clish, go to the Expert mode:

   ```
   expert
   ```

5. Install the Nano-Agent:

   ```
   nano-egg --install --token <Authentication Token you copied earlier from your Quantum Profile>
   ```

Important:

- You can examine the connection from the Security Gateway / each Cluster Member to Check Point Portal only after you configure and enforce the SD-WAN Policy in Check Point Portal.
- It is necessary to uninstall the current Nano-Agent and install it again in these cases:
  - If you uninstalled the last installed Take of the Jumbo Hotfix Accumulator to revert to a previous installed Take.
  - If you uninstalled the last installed Major version.
  - If you reverted Gaia OS to one of the previous snapshots.

Part 4 - Configuration of the Security Gateway object in SmartConsole

Procedure

1. Connect with SmartConsole to the Security Management Server / Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Create a new / configure the existing object for the Security Gateway / Cluster in SmartConsole.
4. On the **General Properties** page (of the Security Gateway / Cluster object), you must enable and configure these Software Blades:
   a. **Application Control**
   b. **URL Filtering**
   c. **IPSec VPN** (if this Security Gateway / Cluster must participate in VPN - see *"SD-WAN Connection (Steering Behavior) Types" on page 184*).

   Note - Installation of an Access Control Policy fails on a Security Gateway / Cluster Member when a Nano-Agent is installed, but the Application Control and URL Filtering Software Blades are not enabled.

   See the:
   - *Security Management Administration Guide* for your version.
   - *Spark Firewall Appliances Centrally Managed Administration Guide* for your version.
   - *Site to Site VPN Administration Guide* for your version.
5. On the **Network Management** page:

   (In the Spark Firewall object, this page is called **Topology**.)
   a. Write down the topology configuration of each existing interface.
   b. From the top toolbar, click **Get Interfaces** and click **Get Interfaces With Topology**.
   c. Accept the imported topology.
   d. Make sure for the SD-WAN interfaces, the **Network Type** column shows **External**.

   Important - The names of SD-WAN interfaces on the **Network Management** (**Topology**) page must be the same as the names of these interfaces on the Security Gateway / each Cluster Member.

6. Configure the **SD-WAN** interfaces - Topology and Anti-Spoofing:
    a. On the **Network Management** page (in the Spark Firewall object, this page is called **Topology**), select the SD-WAN interface and click **Edit**.
    b. In the **Topology** section, click **Modify**.
    c. In the **Leads To** section:
        - Make sure to select **Internet (External)**.
    d. In the **Anti-Spoofing** section:
        i. Select **Perform Anti-Spoofing based on interface topology**.
        ii. Select the applicable **Anti-Spoofing action**.
        iii. **Optional:** Select **Don't check packets from** and select the applicable Network, Network Group, or Address Range object.
        iv. Select the applicable **Spoof Tracking** option.
    e. Click **OK** to close the **Topology Settings** window.
    f. Click **OK** to close the **Interface** window.
7. Make sure the ISP Redundancy configuration is **disabled** in the **Other** section > on the **ISP Redundancy** page.

    Note - SD-WAN does **not** support the ISP Redundancy configuration. You **must** disable ISP Redundancy in the Security Gateway object in SmartConsole.
8. Click **OK** to close the Security Gateway / Cluster properties window.

Security Policy Installation Using SD-WAN Interface IP Addresses

Starting from R82, Security Management can use SD-WAN interface IP addresses to establish Security Policy installation connectivity.

When Security Policy installation to a Security Gateway fails because the primary management IP address is unreachable, Security Management attempts to establish a TCP connection to the Security Gateway through the IP addresses of its SD-WAN interfaces.

Security Management tries the SD-WAN interface IP addresses in order. If a TCP connection cannot be established through the first SD-WAN interface IP address, Security Management tries the next SD-WAN interface IP address in the list. This process continues until a TCP connection is successfully established or all available SD-WAN interface IP addresses have been tried.

Use Case

In environments where a Security Gateway is connected to multiple ISPs, one or more ISP links might become unavailable.

If the Security Gateway's primary management IP address belongs to an unavailable ISP link, Security Management might be unable to establish the initial TCP connection through that address.

When SD-WAN interfaces are configured on the Security Gateway, Security Management can attempt Security Policy installation through the other SD-WAN interface IP addresses.

If routing is configured correctly on the Security Gateway, the kernel routing table might update the default route to use an available ISP link. In this case, if Security Management establishes a TCP connection through the IP address of an available SD-WAN interface, Security Policy installation traffic can flow symmetrically over that ISP path.

In some environments, traffic from Security Management might enter the Security Gateway through one SD-WAN interface and return through another SD-WAN interface. This traffic flow can also succeed if the ISP path supports asymmetric routing and does not block the traffic.

Updating SD-WAN Interface Information in the Security Management

Security Management learns the SD-WAN interface configuration when the administrator selects **Get Interfaces** in the Security Gateway object under **Network Management > Topology**. The retrieved interface information is saved in the Security Management database.

To enable Security Management to use SD-WAN interface IP addresses for Security Policy installation connectivity, select **Get Interfaces** after SD-WAN interfaces are configured on the Security Gateway.

This action is required only once after the SD-WAN interfaces are configured. The information is saved in the Security Management database and used for future Security Policy installations.

If you add additional SD-WAN interfaces later, select **Get Interfaces** again to update the saved interface information.

Important:

- Security Management attempts Security Policy installation only through the SD-WAN interface IP addresses configured in the Security Security Gateway object.
- If an SD-WAN interface is located behind a NAT device, Security Management does not initiate the connection to the translated NAT IP address. Security Management attempts the connection only to the actual SD-WAN interface IP address configured in the Security Gateway object.
- This capability applies only to policy installation from Security Management to Security Gateways. It does not apply to Security Gateway monitoring.

Security Gateway Connectivity to Security Management

In some scenarios, the Security Gateway initiates connections to the Security Management Server. For example, the Security Gateway may connect to the Security Management Server to fetch policy, retrieve CRLs, and send logs.

To allow the Security Gateway to use all available external interfaces when connecting to Security Management, configure a valid route to Security Management through each relevant path.

For example, if Security Management is reachable through the Internet, configure either a route to the Security Management Server or a default route through each relevant ISP next hop, with different priorities. If Security Management is reachable only through an MPLS network or another private network, configure the required route through the relevant MPLS or private-network path.

It is recommended to enable next-hop monitoring, such as **Ping on** or **IP Reachability Detection**, for each route so that routes remain active only when the relevant path is reachable.

With this routing configuration, if the active path goes down, the Security Gateway can fail over to the next available route and continue to reach Security Management.

Part 5 - Configuration of VPN and Security Policy in SmartConsole

Procedure

If this Security Gateway / Cluster must participate in VPN (see *"SD-WAN Connection (Steering Behavior) Types" on page 184*), configure the applicable VPN Community of type **Star**:

1. You must configure the Headquarters Security Gateways that work as Center VPN Gateways.

   Configure the applicable Encryption Domain.

2. You must configure the Branch Security Gateways that work as Satellite VPN Gateways:

   a. Configure the applicable Encryption Domain.

   b. Configure the correct Link Selection.

      See *"VPN - Link Selection" on page 235*.

   The correct configuration makes sure you do not lose all VPN connectivity in these scenarios:

   - The main IP address of the Security Gateway object is not one of the link selections.
   - SD-WAN Policy is not loaded.

3. On the **VPN Routing** page of the VPN Community object, select the required setting:

   - If you configure only an SD-WAN Connection Type "**Overlay**" (without "**Backhaul**"), then select **To center only** or **To center and to other satellites through center**.
   - If you configure an SD-WAN Connection Type "**Backhaul**", then select **To center or through the center to other satellites, to Internet and other VPN targets**.

Note - SD-WAN does **not** support Permanent Tunnels.

See the:

- *Site to Site VPN Administration Guide* for your version.
- *Security Management Administration Guide* for your version.

Part 6 - Configuration of Security Policy in SmartConsole

Procedure

See the *Security Management Administration Guide* for your version.

1. Configure the applicable Access Control rules.

   Important:

   a. You must add an explicit rule to allow the service "`echo-request`" between the Security Gateways that participate in this VPN Community.
      - This explicit rule is necessary for the WAN Link probing.
      - The position of this explicit rule must be above all rules that may drop this traffic.

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On

SD-WAN probing	Security Gateways that participate in this VPN Community	Security Gateways that participate in this VPN Community	`Any`
			
			or
			
			Object of the applicable VPN Community
				`echo-request`	`Accept`	`Log`
						
						or
						
						`None`
							`Policy Targets`
							
							or
							
							Security Gateways that participate in this VPN Community

   b. If you selected **Accept ICMP requests** in SmartConsole > **Menu** button > **Global properties** > **FireWall** page, then you must:
      i. Select **Last** or **Before Last** for this option on the **FireWall** page.
      ii. Configure an explicit rule to allow ICMP requests between the Security Gateways - this probing traffic must be encrypted, which requires an explicit rule.

   For more information, see *"SD-WAN Best Practices" on page 235* > sections about ICMP Probing.

2. Configure the applicable NAT rules to hide internal networks behind this Security

Gateway / Cluster.

Important - If you configure an SD-WAN Connection Type "**Overlay**", then it is best to avoid NAT on traffic between internal networks when you configure "Hide NAT".
Do **one** of these, based on your requirements:

- Add an explicit Manual NAT rule (above all Automatic NAT rules) to forbid NAT for traffic between the applicable Source and Destination networks:
  a. In the **Original** columns, select the applicable Source and Destination networks.
  b. In the **Translated** columns, remove all objects so that these cells show "`=Original`".

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
Internal networks behind this Security Gateway / Cluster	Internal networks behind this Security Gateway / Cluster	`Any`	`=Original`	`=Original`	`=Original`	`Policy Targets` or Object of this Security Gateway / Cluster	Overlay - disable NAT between internal networks
Automatic Generated Rules							

- In the properties of the VPN Community object > on the **Advanced** page, select **Disable NAT inside the VPN Community**.

3. Install the Access Control Policy on the Security Gateway / Cluster.

What is Next?

Follow *"Step 4 - SD-WAN Wizard" on page 158*

Step 4 - SD-WAN Wizard

This is a step in the Smart-1 Cloud Deployment.

Important:

- If you do **not** use the SD-WAN Wizard, then you must configure the required settings manually.
- The SD-WAN Wizard creates the required default rules only when you run it for the **first** time.

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle panel, click **Getting Started**.
5. In the **Configure SD-WAN** section, click **Open Wizard**.
6. In Step **(1) Environment**, click **Next**.

   To see more information, hover the mouse cursor over the icon.
7. In Step **(2) Uses Cases**:
   a. **Optional:** Select **Use only Internet use cases, but no Overlay VPN use cases**.

      This disables several use cases.

      To see more information, hover the mouse cursor over the icon.
   b. Click the predefined practices you want to disable (or enable again).
   c. Click **Next**.
8. In Step **(3) Quantum Gateways**:
   a. Select the connected Security Gateways you want to use.

      To see more information, hover the mouse cursor over the icon in the **Required** column.
   b. Click **Next**.

9. In Step **(4) WAN Link Mapping**:
    a. If you already have WAN Links configured on your Security Gateways, you can map them to specific interfaces.

    To see more information, hover the mouse cursor over the ⓘ icon in the column headers.

    b. Click **Next**.
10. In Step **(5) Summary**:
    a. Select the applicable option:
        - **I will publish the changes manually later**
        - **Publish the change now, and I will enforce the policy manually later**
        - **Publish and Enforce the policy now**
    b. Click **Done**.
11. Wait for the SD-WAN Wizard to create the required objects and the SD-WAN Policy.
12. If needed, change the object settings, add new objects, change the SD-WAN Policy rules.

    See:
    - *"Configuring SD-WAN Policy" on page 160*.
    - *"Configuring Steering Behavior" on page 171*.
    - *"WAN Link Mapping" on page 207*.
13. From the top toolbar, click **Publish** to save the changes.
14. From the top toolbar, click **Enforce** to apply the changes.

    The orange frame on this button means there are changes that are not enforced.

    In the popup window that opens, click **Publish & Enforce Policy**.
15. See *"SD-WAN Monitoring" on page 212*.

Configuring SD-WAN Policy

Important - If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.

Configuring SD-WAN Policy

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.

   The SD-WAN Policy opens.

#	Name	Source	Destination	Services & Applications	Behavior	Translated Source (NAT)	Enforcement
1	...	...	...	...	...	...	...
2	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...

Notes:

- If the icon appears in the column "**#**", it means this rule is disabled.
  To enable this rule, click the rule number > click > click **Enable**.
- If the icon appears in the column "**#**", it means you made changes in that row, but did not click **Publish** and **Enforce** yet.
- If the red oval frame with the icon appears around an object, it means this object is no longer available - an administrator deleted this object on the Management Server, which updated Check Point Portal.
  By design, Check Point Portal does not delete such objects from your configuration.
  You must manually change all places that contain this deleted object.

5. From the top toolbar, create a new rule.
6. **Optional:** In the **Name** column of the rule, click and enter the applicable text.

7. In the **Source** column of the rule, click the **(+)** icon > select the applicable asset objects > click **OK**.

   See *"Objects Supported in SD-WAN Policy" on page 169*.

8. In the **Destination** column of the rule, click the **(+)** icon > select the applicable asset objects > click **OK**.

   See *"Objects Supported in SD-WAN Policy" on page 169*.

   Best Practice - Use Updatable Objects in the "**Destination**" column of the SD-WAN Policy. This allows matching of application connections on the first packet and most accurate traffic steering.

9. In the **Services & Applications** column of the rule, click the **(+)** icon > click **Services**, **Applications** > select the applicable objects > click **OK**.

   See *"Objects Supported in SD-WAN Policy" on page 169*.

10. In the **Behavior** column of the rule, click the **(+)** icon > select the applicable Steering Behavior object > click **OK**.

    See *"Configuring Steering Behavior" on page 171*.

    Note - You can select only one Steering Behavior object in a rule. If you select a different object, then it replaces the current object.

11. In the **Translated Source (NAT)** column of the rule, click the **(+)** icon > select the applicable NAT Mapping object > click **OK**.

    See *"SD-WAN NAT for ISP" on page 271*.

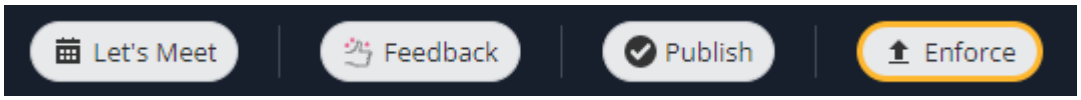
12. In the **Enforcement** column of the rule, click the **(+)** icon > select the applicable profile objects > click **OK**.

    Note - Select the profile you created in Check Point Portal:
    - *"Step 1 - Configuration in Check Point Portal" on page 68* (On-Premise Management Server)
    - *"Step 1 - Configuration in Check Point Portal" on page 118* (Smart-1 Cloud)

13. From the top toolbar, click **Publish** to save the changes.

14. From the top toolbar, click **Enforce** to apply the changes.

    The orange frame on this button means there are changes that are not enforced.

    In the popup window that opens, click **Publish & Enforce Policy**.

Note - To disable a rule, in the **#** column, click the 3-dots button ⋮ > click **Disable**.
Example:



Removing / Disabling SD-WAN Policy on the Security Gateway

To stop a Security Gateway from enforcing SD-WAN policy (that is, to uninstall, disable, or turn off SD-WAN policy on that Security Gateway):

1. Remove the Security Gateway from all SD-WAN Profiles:

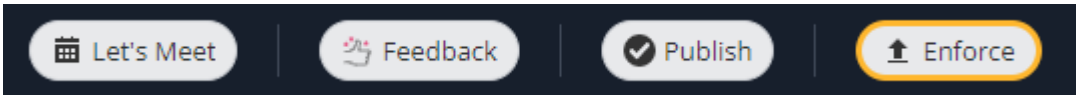
   After enforcement, the Security Gateway will no longer receive or enforce SD-WAN policy.

   a. In Check Point Portal, remove the Security Gateway object from any SD-WAN Profile that is selected in any SD-WAN policy rule.

   b. From the top toolbar, click **Publish** to save the changes.

   c. From the top toolbar, click **Enforce** to apply the changes.

      The orange frame on this button means there are changes that are not enforced.

      In the popup window that opens, click **Publish & Enforce Policy**.

2. If the Security Gateway is unreachable (for example, is not connected to the Internet at this time):

   If you cannot update the SD-WAN assignment from the Check Point Portal, you can remove the Nano-Agent locally on the Security Gateway with this command:

   ```
   cpnano -u
   ```

   This command will remove all SD-WAN Nano-Services, unregister the Security Gateway from the Check Point Portal, and uninstall the SD-WAN policy from the Security Gateway.

Note - Before uninstalling the Nano-Agent, make sure there are no other components that use it (for example, IoT) to avoid an impact on other features.

Dynamic Objects in SD-WAN Policy

On 19 August 2024, new predefined Dynamic Objects were added in Check Point Portal in the SD-WAN service.

These new predefined Dynamic Objects provide more precise traffic matching.

Notes:

- Support for these new Dynamic Objects is available in these Security Gateway versions:
  - R82.10 and higher
  - R82 Jumbo Hotfix Accumulator Take 14 and higher
  - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
  - Spark Firewall R81.10.15 and higher
- If you configure the SD-WAN Policy with new Dynamic Objects, but your Security Gateway runs a lower version than required, then your Security Gateway converts the new Dynamic Objects to the corresponding Zone objects.

Description of the new Dynamic Objects:

Dynamic Object "My VPN Domain"

The Dynamic Object "**My VPN Domain**" presents the local VPN Encryption Domain on the Security Gateway that establishes Site to Site VPN tunnels.

Notes:

- The Dynamic Object "**My VPN Domain**" also represents the external interface on the Security Gateway that establish Site to Site VPN tunnels.
- Use the Dynamic Object "**My VPN Domain**" in SD-WAN rules that use Steering object or type "Overlay".
- The Dynamic Object "**My VPN Domain**" will match traffic between VPN peers (for example, probing in "Overlay").
  No need to create a manual rule for such traffic.
- The Dynamic Object "**My VPN Domain**" replaces the Zone object "**My VPN Domain & Peer VPN Domain**".
- If you configure the SD-WAN Policy with the Dynamic Object "**My VPN Domain**", but your Security Gateway runs a lower version than required, then your Security Gateway converts the Dynamic Object "**My VPN Domain**" to the Zone object "**My VPN Domain & Peer VPN Domain**".

Dynamic Object "Peer VPN Domain"

On the Security Gateway establishes Site to Site VPN tunnels with its VPN peers, the Dynamic Object "**Peer VPN Domain**" represents one large VPN Encryption Domain of all SD-WAN VPN peers.

Notes:

- The Dynamic Object "**Peer VPN Domain**" also represents the external interface on the VPN peer Security Gateways that establish Site to Site VPN tunnels.
- Use the Dynamic Object "**Peer VPN Domain**" in SD-WAN rules that use Steering object or type "Overlay".
- The Dynamic Object "**Peer VPN Domain**" will match traffic between VPN peers (for example, probing in "Overlay").
  No need to create a manual rule for such traffic.
- The Dynamic Object "**Peer VPN Domain**" replaces the Zone object "**My VPN Domain & Peer VPN Domain**".
- If you configure the SD-WAN Policy with the Dynamic Object "**Peer VPN Domain**", but your Security Gateway runs a lower version than required, then your Security Gateway converts the Dynamic Object "**Peer VPN Domain**" to the Zone object "**My VPN Domain & Peer VPN Domain**".

Dynamic Object "SD-WAN Internet"

The Dynamic Object "**SD-WAN Internet**" represents the Internet - ranges of public IP addresses.

Notes:

- The Dynamic Object "**SD-WAN Internet**" does not contain these IP addresses:
  - Ranges of reserved IP addresses (private, public, multicast)
  - IP addresses of networks that are connected directly to the Security Gateway
  - Cluster Virtual IP addresses
  - Ranges of IP addresses that are represented by the Dynamic Objects "**My VPN Domain**" and "**Peer VPN Domain**"
  - Ranges of public IP addresses, for which there are specific static routes or dynamic routes (on roadmap)
- Use the Dynamic Object "**SD-WAN Internet**" in SD-WAN rules that use Steering objects or type "Local Breakout" or "Backhaul" to match outbound traffic.
- The Dynamic Object "**SD-WAN Internet**" replaces the Zone object "**SD-WAN Internet**".
- If you configure the SD-WAN Policy with the Dynamic Object "**SD-WAN Internet**", but your Security Gateway runs a lower version than required, then your Security Gateway converts the Dynamic Object "**SD-WAN Internet**" to the Zone object "**SD-WAN Internet**".
- For connections that undergo Destination NAT (such as with Inbound NAT / traffic for Published services), the Dynamic Object "**SD-WAN Internet**" matches the traffic against the destination IP address after NAT:
  - If the destination IP address after NAT matches the Dynamic Object "**SD-WAN Internet**" - the connection is matched to that SD-WAN rule
  - If the destination IP address after NAT does not match the Dynamic Object "**SD-WAN Internet**" (the IP address is private, or belongs to a directly connected network) - the connection is not matched to that SD-WAN rule

Important Notes

- The Zone object "**My VPN Domain & Peer VPN Domain**" represents all private networks as described in RFC 1918:
  - 10.0.0.0/8
  - 172.16.0.0/15
  - 192.168.0.0/16
- The Zone object "**SD-WAN Internet**" represents all networks other than the private networks that the Zone object "**My VPN Domain & Peer VPN Domain**" represents.
- If you configure your SD-WAN service for the first time after 19 August 2024, then the SD-WAN Wizard creates the required predefined SD-WAN Policy rules with the new Dynamic Objects.
- If you already SD-WAN Policy rules with the Zone objects "**My VPN Domain & Peer VPN Domain**" and "**SD-WAN Internet**":
  - You can continue using these Zone objects.
  - You can configure the SD-WAN Policy again to use the new Dynamic Objects (see the procedures below).
- If ranges of public IP addresses exist inside your networks that are not directly connected to the Security Gateway (but are routed), and these ranges are not represented by the Dynamic Objects "**My VPN Domain**" and "**Peer VPN Domain**", then at the top of the SD-WAN Policy create a bypass rule with the Steering of type "Overlay", so traffic for these ranges does match rules with the Steering of type "Local Breakout".
- To match "Overlay" traffic, configure this rule:

Source	Destination	Services & Applications	Behavior
My VPN Domain **Peer VPN Domain**	**Peer VPN Domain** **My VPN Domain**	`Any`	**Default overlay**

Notes:
- If in a Star VPN Community there are Center Gateways / Hub Gateways that route traffic between Spokes, then make sure to configure a rule for traffic from "**Peer VPN Domain**" to "**Peer VPN Domain**".
- If in the "**Services & Applications**" column you use "`Any`" rather than specific applications, then the SD-WAN log cannot show the application that generated this traffic.

Follow the applicable procedure below to get the new predefined Dynamic Objects in the SD-WAN Policy:

Add the new predefined Dynamic Objects without changing the existing SD-WAN Policy rules

If you configured your SD-WAN service for the first time before 19 August 2024, then follow these steps to **see** the new predefined Dynamic Objects:

1. From the left navigation panel, click **Network**.
2. In the middle panel, click **Getting Started**.
3. In the **Configure SD-WAN** section, click **Open Wizard**.
4. In this popup window, click **OK**:

   ```
   SD-WAN rules already exist. If you will choose to create new
   rules via the wizard, upon completion we recommend reviewing
   the SD-WAN Policy to make sure the new rules aren't
   overlapping.
   ```

5. Wait for 15 seconds.
6. In the top right corner of the **SD-WAN Setup** window, click **X** to close it.

You can now select the new Dynamic Objects in the SD-WAN Policy.

Add the new predefined Dynamic Objects in addition to the existing SD-WAN Policy rules

If you configured your SD-WAN service for the first time before 19 August 2024, then follow these steps to **add** the new predefined Dynamic Objects:

1. Note the number of the last SD-WAN rule.
2. From the left navigation panel, click **Network**.
3. In the middle panel, click **Getting Started**.
4. In the **Configure SD-WAN** section, click **Open Wizard**.
5. In this popup window, click **OK**:

   ```
   SD-WAN rules already exist. If you will choose to create new
   rules via the wizard, upon completion we recommend reviewing
   the SD-WAN Policy to make sure the new rules aren't
   overlapping.
   ```

6. Follow through this SD-WAN Wizard.

   See *"Step 4 - SD-WAN Wizard" on page 111*.

   The SD-WAN Wizard adds the new rules below the existing rules.
7. From the left navigation panel, click **Network**.
8. In the middle section, click **SD-WAN Policy**.
9. Change the new rules as required for your environment.

   Disable the previous rules - in the **#** column, click the 3-dots button > click **Disable**.
10. From the top toolbar, click **Publish** to save the changes.
11. From the top toolbar, click **Enforce** to apply the changes.

    In the popup window that opens, click **Publish & Enforce Policy**.

Objects Supported in SD-WAN Policy

This section provides a list of objects you can use in various columns of SD-WAN policy rules.

Supported shared objects in the "Source" and "Destination" columns of SD-WAN policy

- Host
- Network
- Address Range
- Security Zone
- Dynamic Object

  Note - See *"Dynamic Objects in SD-WAN Policy" on page 163*.

- Domain
- Security Gateway Object
- Cluster Object
- Cluster Member Object
- Network Groups
- Access Role

Supported shared updatable objects in the "Source" and "Destination" columns of SD-WAN policy

SD-WAN supports Updatable Objects documented in sk131852.

Supported shared objects in the "Services & Applications" column of SD-WAN policy

- `TCP` service
- `UDP` service
- `Other` service
- `SCTP` service
- `Service Group`
- Check Point Applications
- Application/Site Group
- Custom Application/Site
- DSCP Service Class

Configuring Steering Behavior

Important - If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.

Steering Behavior objects are mandatory part of SD-WAN Policy.

Steering Behavior determines how the Security Gateway sends traffic to the Internet or over an overlay.

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.
5. From the top toolbar, click **Manage Objects**.

   Note - From the top toolbar, you can:
   - Create a new Steering Behavior
   - Delete a selected Steering Behavior
   - Search for a Steering Behavior
   - Edit a selected Steering Behavior
6. When you create a new Steering Behavior, or edit an existing Steering Behavior:
   a. In the **Name** field, enter a descriptive name that represents this Steering Behavior.
   b. **Optional:** In the **Comment** field, enter an applicable text that describes this Steering Behavior.
   c. Configure the **Steering Candidates**:
      i. Click the **Steering Candidates** tab.
      ii. In the section **Connection Type**, select the applicable option:

      See *"SD-WAN Connection (Steering Behavior) Types" on page 184*.

Steering Behavior	Description
Internet with "Local Breakout Only"	This connection type represents a direct WAN Link to the Internet. See *"Routing Preference "Local Breakout Only"" on page 188*.
Internet with "Backhaul Only"	This connection sends traffic from VPN spoke sites to the Internet through the Central VPN hub site. This connection type enables the VPN spoke site to use the Public lines / Private lines to reach the Internet through the Headquarters. See *"Routing Preference "Backhaul Only"" on page 191*.
Internet with "Prioritize Local Breakout"	This connection type gives priority to the direct WAN Link (not through the Headquarters) to send **all** traffic directly to the Internet. If **all** direct WAN Links to the Internet are down, the Security Gateway uses the direct WAN Link with encrypted traffic to the Headquarters to connect to the Internet. See *"Routing Preference "Prioritize Local Breakout"" on page 195*.
Overlay	This connection type represents a direct WAN Link with encrypted traffic to the Headquarters. The direct WAN Link with encrypted traffic to the Headquarters provides redundancy. See *"SD-WAN Connection Type - "Overlay"" on page 200*.

iii. On the tab **Steering Candidates**, configure the applicable settings:

Steering Candidates are WAN Links on the corresponding Security Gateway.

Steering Behavior	Steering Candidates
Internet with "Local Breakout Only"	■ **All Relevant WAN Links** - To use all available WAN Links. ■ **Specific WAN Links** - To use only the selected WAN Links.
Internet with "Backhaul Only"	■ **All Relevant WAN Links** The Security Gateway uses all available WAN Links. ■ **Specific WAN Links** The Security Gateway uses only the selected WAN Links. ■ **Use the same settings for Branch to HQ connection** Controls which WAN Links the Security Gateway uses to connect from a Branch office to the Headquarters (**"All Relevant WAN Links"** or **"Specific WAN Links"**).
Internet with "Prioritize Local Breakout"	■ **All Relevant WAN Links** The Security Gateway uses all available WAN Links. ■ **Specific WAN Links** The Security Gateway uses only the selected WAN Links. ■ **Use the same settings for Branch to HQ connection** Controls which WAN Links the Security Gateway uses to connect from a Branch office to the Headquarters (**"All Relevant WAN Links"** or **"Specific WAN Links"**).
Overlay	■ **All Relevant WAN Links** - To use all available WAN Links. ■ **Specific WAN Links** - To use only the selected WAN Links.

d. **Optional:** Configure the **Criteria** settings:

Note - If you do **not** configure these thresholds explicitly, then the SD-WAN Security Gateway considers **all** available WAN Links as candidates and uses the best WAN Link based on the defined margins.

i. Click the **Criteria** tab.

ii. Click the **Thresholds** heading to expand this section and configure the applicable settings:

Security Gateway uses only WAN Links that meet the configured Link Quality Thresholds.

You can configure thresholds for:

- Latency
- Jitter
- Packet Loss
- Minimum Bandwidth

A WAN Link is eligible for traffic forwarding only when all configured threshold requirements are met. If any configured threshold is not met, the WAN Link is disqualified from traffic forwarding.

Note - Configuring a bandwidth threshold is optional. When configured, the SD-WAN Policy considers only WAN Links whose configured speed meets or exceeds the specified minimum bandwidth.
The threshold is based on the statically configured WAN Link speed and does not reflect real-time utilization or currently available bandwidth.
The bandwidth threshold is evaluated together with the configured latency, jitter, and packet-loss thresholds when determining WAN Link eligibility.

A disqualified WAN Link becomes eligible again only after it meets all configured threshold requirements.

If none of the WAN Links meet all configured threshold requirements, the SD-WAN Policy selects the WAN Link as follows:

Item	Local Breakout	Overlay
Link Aggregation	All WAN Links in the "UP" state are used in parallel.	All Overlay tunnels in the "UP" state are used in parallel.
Manual Order	The first WAN Link in the "UP" state, based on the defined order, is used.	The Overlay tunnel in the "UP" state from the first WAN Link, based on the defined order, is used.

Item	Local Breakout	Overlay
Link Attributes	The first WAN Link in the "UP" state, in the alphabetical order (by name), is used.	The first Overlay tunnel in the "UP" state, in the alphabetical order (by name), is used.

iii. Click the **WAN Link Utilization** heading to expand this section and configure the applicable settings:

Note - Only WAN Links that meet all configured latency, jitter, packet-loss, and bandwidth thresholds are eligible for selection.

- **Link Aggregation** - To use all available WAN Links (in parallel) that meet the maximum values you configured in the **Thresholds** section. This is the default setting.

  In the **Selection Method** field, select the applicable option:

  Note - This feature requires these Security Gateway versions:
  - R82.10 and higher
  - R82 Jumbo Hotfix Accumulator Take 14 and higher
  - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
  - Spark Firewall R81.10.15 and higher

  - **Connection Hash**

    Distributes the connections between the WAN Links based on a 4-tuple - [Source IP, Destination IP, Destination port, IP protocol].

    This is the default value.

  - **Round Robin**

    Distributes the connections between the WAN Links equally in a circular order.

  - **Proportionally To Download Bandwidth**

    Distributes the connections between the WAN Links based on a 4-tuple [Source IP, Destination IP, Destination port, IP protocol], proportionally to the download bandwidth configured in the corresponding interfaces on the Security Gateway.

    This requires the configuration of the download speed limit in the corresponding SD-WAN interface.

    See *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*".

  - **Proportionally To Upload Bandwidth**

    Distributes the connections between the WAN Links based on a 4-tuple [Source IP, Destination IP, Destination port, IP protocol], proportionally to the upload bandwidth configured in the corresponding interfaces on the Security Gateway.

    This requires the configuration of the download speed limit in the corresponding SD-WAN interface.

    See *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*".

- **Prioritize** - To use specific WAN Links (available only if in the **Steering Candidates** section, you selected **Specific WAN Links**).

  Select the applicable option:

Option	Description
Link attributes	Configures the SD-WAN Policy to select a better WAN Link among the WAN Links based on the current link attribute values. This is the default setting. • To configure the order, in which the SD-WAN Policy examines the link attributes, click the rows and drag them to the applicable positions. • To disable a link attribute, clear its checkbox. • In the "**Margin**" column, click the current value and configure the applicable difference value between the WAN Links for each attribute. The SD-WAN steering evaluates link attributes in the configured order. If the difference for the first attribute does not exceed its configured margin, the policy evaluates the next attribute in the list, and so on. If multiple WAN Links have different characteristics (for example, one link has lower packet loss while another link has lower latency), the characteristic with the higher evaluation priority determines the selected WAN Link. If the difference between the current attribute values of WAN Links exceeds the configured margin, the SD-WAN steering switches traffic to the WAN Link with the better value for the evaluated attribute. **Example** ◦ The configured latency threshold is 150 ms. ◦ WAN Link "ISP1" has a current latency of 100 ms. ◦ WAN Link "ISP2" has a current latency of 110 ms. ◦ The configured latency margin is 15 ms. ◦ If the difference between these latency values becomes greater than 15, then the SD-WAN Policy selects the WAN Link with the lower latency value.

Option	Description
Manual order of WAN Links	Configures the SD-WAN Policy to select WAN Links in a specific order, regardless of their link attribute values. SLA values are used only to determine WAN Link eligibility based on the configured thresholds and do not affect the order of WAN Link selection. • To select this option, on the tab **Steering Candidates**, you must select **Specific WAN Links** and select at least two WAN Links. • To configure the order, in which the SD-WAN Policy uses these WAN Links, click the rows and drag them to the applicable positions.

iv. Click the **Quality Check Methodology** heading to expand this section and configure the applicable settings.

These settings determine how a special "prober" on the Security Gateway measures the WAN Link quality.

a. Select the probe type:

- If you selected **Best Practice**:

  SD-WAN sends ICMP pings to a Google DNS Server (8.8.8.8).

- If you selected **Custom**:

  i. In the field **Using**, select the probing protocol:

  - **Ping** - The Security Gateway sends ICMP pings to the specified destination
  - **HTTP** - The Security Gateway sends HTTP packets to the specified destination

    Note - Support for the **HTTP** probing is integrated in:
    - R82.10 and higher
    - R82 Jumbo Hotfix Accumulator Take 14 and higher
    - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
    - Spark Firewall R81.10.15 and higher

  ii. In the field **Hosts**, enter the probing destination in the correct format:

  - For Ping probes, enter an IPv4 address (for example, 8.8.8.8)
  - For HTTP probes, enter an HTTP FQDN (for example: `http://www.example.com:8080`)

  Note - You can enter a maximum of 5 destinations.
  - This feature is called Multiple Target Probing (MTP).
  - The Security Gateway must run the R82 Jumbo Hotfix Accumulator Take 25 or higher.
  - ForSpark Firewall Appliances, this feature is still in the Early Availability stage.
    The Spark Firewall Appliance must run the R81.10.17 Early Availability firmware from sk180605.

b. In the **Check interval** field, configure a frequency of the WAN Link tests (in milliseconds).

Notes:

- For "Local Breakout":
  - This value determines how frequently the Security Gateway sends probes to the specified Internet target.
  - The Local Breakout SLA averages are calculated as follows:
    - Packet Loss: Based on the last 100 probe results.
    - Latency and Jitter: Based on the last 30 probe results.
- There are different thresholds for the "**Ping**" and the "**HTTP**" probing protocols.

e. **Optional:** Override the default QoS settings.

For more information, see *"EA Feature: QoS in SD-WAN" on page 301*.

i. Click the **QoS** tab.

ii. In the section **QoS Configuration**, select **Override according to**.

iii. Select the required QoS object.

iv. **Optional:** In the section **QoS on Upload and Download traffic**:

This setting applies the QoS configuration to the WAN candidates that you selected on the **Steering Candidates** tab in this Steering Behavior object.

i. Select **Override and choose specific Traffic Directions per WAN Link**.

ii. For at least one WAN Link, you must select **Use for Upload** or **Use for Download**.

Note - All other upload / download interfaces use the default QoS settings configured in WAN Link Mapping.

f. Click **OK**.

7. From the top toolbar, click **Publish** to save the changes.
8. From the top toolbar, click **Enforce** to apply the changes.

The orange frame on this button means there are changes that are not enforced.



In the popup window that opens, click **Publish & Enforce Policy**.

SD-WAN Connection (Steering Behavior) Types

SD-WAN supports different connection (Steering Behavior) types to steer traffic from internal networks behind the Branch Security Gateway to the Internet or the Security Gateway at Headquarters.

Comparison of SD-WAN Connection (Steering Behavior) Types

Steering Behavior	Use Case and Example	Requirements on the Security Gateway
"SD-WAN Connection Type - "Internet"" on page 188 - with *"Routing Preference "Local Breakout Only"" on page 188*	This connection type represents a direct WAN Link to the Internet. **Example:** 1. A Security Gateway with two ISPs. 2. The Zoom application traffic must go over an ISP Link with lower latency. 3. The backup transfer traffic must go over an ISP Link with higher latency.	▪ Application Control Software Blade. ▪ URL Filtering Software Blade

Steering Behavior	Use Case and Example	Requirements on the Security Gateway
"SD-WAN Connection Type - "Internet"" on page 188 - with *"Routing Preference "Backhaul Only"" on page 191*	This connection sends traffic from VPN spoke sites to the Internet through the Central VPN hub site. This connection type enables the VPN spoke site to use the Public lines / Private lines to reach the Internet through the Headquarters. **Example:** 1. A branch Security Gateway with two ISPs. 2. Regular web traffic must go over a direct WAN Link to the Internet. 3. Email traffic must go through the Headquarters Security Gateway for deep inspection. **Example topology:** ■ `User ---> Branch Gateway ---> ISP1 ---> (Internet)` ■ `User ---> Branch Gateway ---> ISP2 ---> HQ Gateway ---> (Internet)`	■ IPSec VPN Software Blade. ■ Site-to-Site VPN between the Branch Security Gateway and the Headquarters Security Gateway.

Steering Behavior	Use Case and Example	Requirements on the Security Gateway
"SD-WAN Connection Type - "Internet"" on page 188 - with *"Routing Preference "Prioritize Local Breakout"" on page 195*	This connection type gives priority to the direct WAN Link (not through the Headquarters) to send **all** traffic directly to the Internet. If **all** direct WAN Links to the Internet are down, the Security Gateway uses the direct WAN Link with encrypted traffic to the Headquarters to connect to the Internet. **Example:** 1. A branch Security Gateway with two ISPs. 2. All traffic must go over a direct WAN Link to the Internet (denoted "ISP1" below). 3. When the direct WAN Link to the Internet is down (denoted "ISP1" below), the Security Gateway connects to the Internet through the other WAN Link with encrypted traffic to the Headquarters (denoted "ISP2" below). **Example topology:** ■ `User ---> Branch Gateway ---> ISP1 ---> (Internet)` ■ `User ---> Branch Gateway ---> ISP2 ---> HQ Gateway ---> (Internet)`	■ IPSec VPN Software Blade. ■ Site-to-Site VPN between the Branch Security Gateway and the Headquarters Security Gateway.

Steering Behavior	Use Case and Example	Requirements on the Security Gateway
"SD-WAN Connection Type - "Overlay"" on page 200	This connection type represents a direct WAN Link with encrypted traffic to the Headquarters. The direct WAN Link with encrypted traffic to the Headquarters provides redundancy. **Example:** 1. A branch Security Gateway with two ISPs. 2. A Remote Desktop server is installed on an internal network behind the Headquarters Security Gateway. 3. A connection from an internal network behind a branch Security Gateway to the Remote Desktop server must go over a direct WAN Link (denoted "ISP1" below), while its latency is low. 4. When the latency of the direct WAN Link becomes greater than the latency of the direct private MPLS Link, the Remote Desktop connection must go over a direct private MPLS Link. **Example topology:** ■ `User ---> Branch Gateway ---> ISP1 ---> (Internet) ---> ISP2 ---> HQ Gateway ---> Remote Desktop` ■ `User ---> Branch Gateway ---> MPLS ---> HQ Gateway ---> Remote Desktop`	■ Application Control Software Blade. ■ URL Filtering Software Blade ■ Site-to-Site VPN between the Branch Security Gateway and the Headquarters Security Gateway.

SD-WAN Connection Type - "Internet"

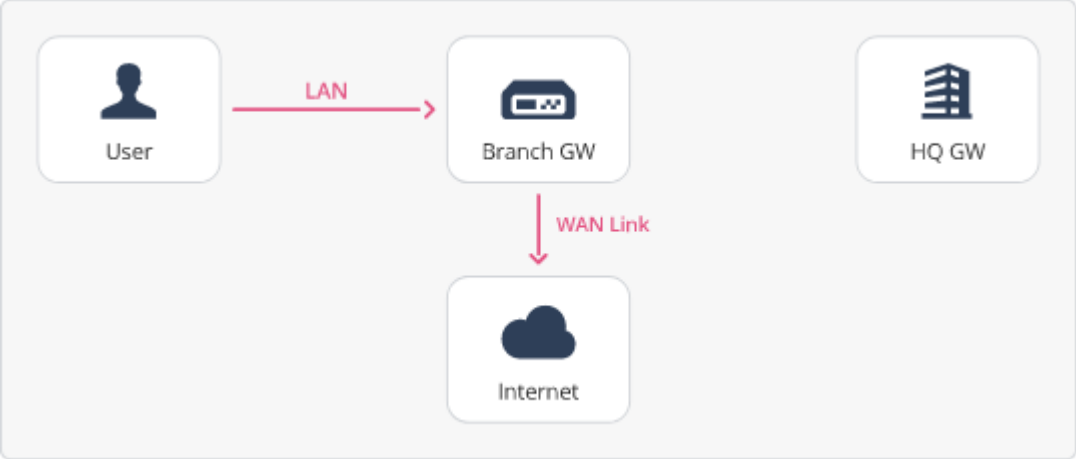
The connection (Steering Behavior) type "Internet" has these routing preference modes:

- Local Breakout Only
- Backhaul Only
- Prioritize Local Breakout

Routing Preference "Local Breakout Only"

Description of "Local Breakout Only"

This connection type represents a direct WAN Link to the Internet.



Use Case and Example for "Local Breakout Only"

Offices with multiple direct WAN Links to the Internet.

Example:

1. A Security Gateway with two ISPs.
2. The Zoom application traffic must go over an ISP Link with lower latency.
3. The backup transfer traffic must go over an ISP Link with higher latency.

Example of an SD-WAN Policy rule:

Traffic, using the "`YouTube`" services, must go from any source behind the Security Gateway to the Internet.

The Security Gateway sends the traffic through the WAN Links configured in the Steering Behavior, if the Access Control Policy allows this traffic.

Name	Source	Destination	Services & Applications	Behavior	Enforcement
Breakout	**Any**	**SD-WAN Internet**	**YouTube**	Select the applicable Steering object of type "Internet - Local Breakout Only"	<Applicable Profile>

Important Notes for "Local Breakout Only"

Important:

- Requirements for this connection type:
  1. In SmartConsole > **Menu** > **Manage policies and layers** > **Layers** page > **Access Control** page > edit the applicable Layer in your policy > **General** page > **Blades** section > select **Application & URL Filtering**.
  2. In the Security Gateway object, enable these Software Blades:
     a. **Application Control**
     b. **URL Filtering**
- Make sure the Access Control Policy and Threat Prevention Policy allow this traffic.
  See the:
  - *Security Management Administration Guide* for your version.
  - *Threat Prevention Administration Guide* for your version.
- If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.
  See *"Configuring Steering Behavior" on page 171*.
- On the Security Gateway, the SD-WAN Policy rules always have higher priority than the operating system routing table. When the Security Gateway marches traffic to an SD-WAN rule that has the "Local Breakout" behavior, the Security Gateway routes the traffic based on the configured steering behavior between all applicable ISPs that meet the criteria.
- The packet loss configured in the Steering object is calculated based on the last 100 probes.

Traffic Flow in "Local Breakout Only"

The Security Gateway sends the traffic directly to the Internet, based on the **Services & Applications** column of the SD-WAN Policy.

Configuring Steering Candidates in "Local Breakout Only"

In the section **Steering Candidates**, configure the applicable settings:

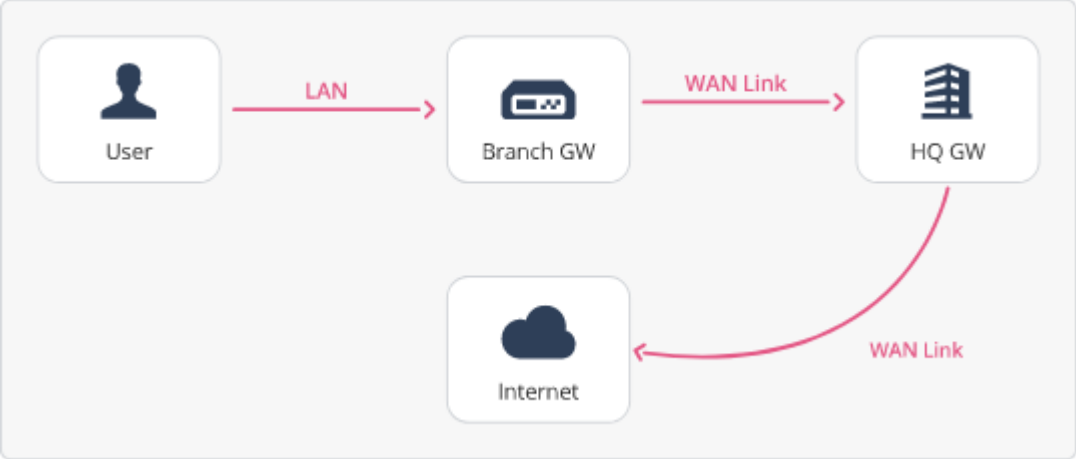
- **All Relevant WAN Links** - To use all available WAN Links.
- **Specific WAN Links** - To use only the selected WAN Links.

Routing Preference "Backhaul Only"

Description of "Backhaul Only"

This connection sends traffic from VPN spoke sites to the Internet through the Central VPN hub site.

This connection type enables the VPN spoke site to use the Public lines / Private lines to reach the Internet through the Headquarters.



Use Case and Example for "Backhaul Only"

Branch offices with a direct WAN Link to the Internet and with a direct WAN Link to the Headquarters.

Branch offices must send specific traffic to the Internet through the Headquarters Security Gateway.

Example:

1. A branch Security Gateway with two ISPs.
2. Regular web traffic must go over a direct WAN Link to the Internet.
3. Email traffic must go through the Headquarters Security Gateway for deep inspection.

Example topology:

- `User ---> Branch Gateway ---> ISP1 ---> (Internet)`
- `User ---> Branch Gateway ---> ISP2 ---> HQ Gateway ---> (Internet)`

Example of an SD-WAN Policy rule:

Name	Source	Destination	Services & Applications	Behavior	Enforcement
Backhaul Only	<Name of a Client Object> <Name of an Email Server Object>	<Name of a Client Object> <Name of an Email Server Object>	**Office365**	Select the applicable Steering object of type "Internet - Backhaul Only"	<Applicable Profile>

Important Notes for "Backhaul Only"

Important:

- Requirements for this connection type:
  1. In the Security Gateway object, enable the **IPSec VPN** Software Blade.
  2. Configure a Site-to-Site VPN tunnel between a Branch Security Gateway (that works as a Satellite VPN Gateway) and a Headquarters Security Gateway (that works as a Center VPN Gateway).
     Configure the applicable VPN Community of type **Star**.
     On the **VPN Routing** page, select **To center or through the center to other satellites, to Internet and other VPN targets**.
     This configuration is mandatory when working with Domain-Based VPN (see *"SD-WAN and Route-Based VPN" on page 266*).
     See the *Site to Site VPN Administration Guide* for your version.
- Make sure the Access Control Policy and Threat Prevention Policy allow this traffic.
  See the:
  - *Security Management Administration Guide* for your version.
  - *Threat Prevention Administration Guide* for your version.
- If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.
  See *"Configuring Steering Behavior" on page 171*.
- The IPSec VPN Software Blade on the Security Gateway makes the IKE negotiation routing decision, regardless the SD-WAN Policy rules.
- Each VPN tunnel from one SD-WAN interface on the SD-WAN Security Gateway to an SD-WAN interface on a peer SD-WAN Security Gateway is a VPN transport. Each SD-WAN Security Gateway constantly sends ICMP Echo Requests over each VPN transport to each VPN peer to select the best path to reach the VPN peer. The Security Gateway selects a VPN path for each packet. This preserves VPN connectivity during a failover of an existing VPN connection between different VPN transports.
- The packet loss configured in the Steering object is calculated based on the last 100 probes.

Traffic Flow in "Backhaul Only"

1. The Branch Security Gateway creates a Site-to-Site VPN tunnel with the Headquarters Security Gateway.
2. The Branch Security Gateway encrypts the traffic and sends the traffic directly to the Headquarters Security Gateway.
3. The Headquarters Security Gateway decrypts the traffic.
4. The Headquarters Security Gateway forwards the traffic to the Internet.
5. The response arrives from the Internet to the Headquarters Security Gateway.
6. The Headquarters Security Gateway inspects the traffic.
7. The Headquarters Security Gateway encrypts the traffic and sends the traffic directly to the Branch Security Gateway.
8. The Branch Security Gateway decrypts the traffic.

Configuring Steering Candidates in "Backhaul Only"

In the section **Steering Candidates**, configure the applicable settings:

- **All Relevant WAN Links**

  The Security Gateway uses all available WAN Links.

- **Specific WAN Links**

  The Security Gateway uses only the selected WAN Links.

- **Use the same settings for Branch to HQ connection**

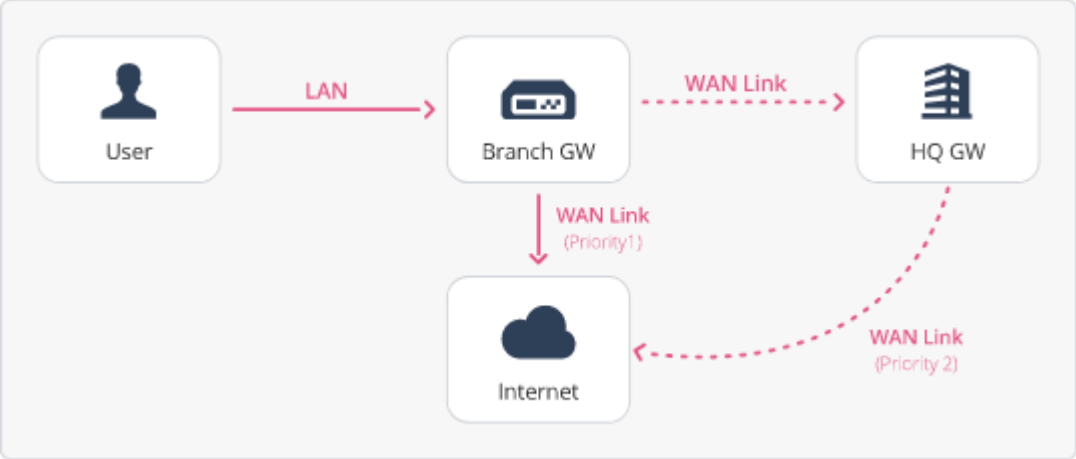
  Controls which WAN Links the Security Gateway uses to connect from a Branch office to the Headquarters ("**All Relevant WAN Links**" or "**Specific WAN Links**").

Routing Preference "Prioritize Local Breakout"

Description of "Prioritize Local Breakout"

This connection type gives priority to the direct WAN Link (not through the Headquarters) to send **all** traffic directly to the Internet.

If **all** direct WAN Links to the Internet are down, the Security Gateway uses the direct WAN Link with encrypted traffic to the Headquarters to connect to the Internet.



Use Case and Example for "Prioritize Local Breakout"

Example:

1. A branch Security Gateway with two ISPs.
2. All traffic must go over a direct WAN Link to the Internet (denoted "ISP1" below).
3. When the direct WAN Link to the Internet is down (denoted "ISP1" below), the Security Gateway connects to the Internet through the other WAN Link with encrypted traffic to the Headquarters (denoted "ISP2" below).

Example topology:

- `User ---> Branch Gateway ---> ISP1 ---> (Internet)`
- `User ---> Branch Gateway ---> ISP2 ---> HQ Gateway ---> (Internet)`

Special scenario:

To send **one** traffic type directly to the Internet, and send **another** traffic type to the Internet through the Headquarters, configure two Steering objects and two rules in the SD-WAN Policy (rule numbers below are only for convenience):

#	Name	Source	Destination	Services & Applications	Behavior
1	Connect through HQ	Select the applicable Source object(s)	Select the applicable Destination object(s)	Select a service or application	Select the applicable Steering object of type "Internet - Backhaul Only"
2	Connect directly	Select the applicable Source object(s)	Select the applicable Destination object(s)	Select a service or application	Select the applicable Steering object of type "Internet - Prioritize Local Breakout"

Example:

#	Name	Source	Destination	Services & Applications	Behavior
1	Connect through HQ	Internal_ Network	`SD-WAN Internet`	`Office365`	Connect through Headquarters
2	Connect directly	Internal_ Network	`SD-WAN Internet`	`http` `https`	Connect Directly

Traffic Flow in "Prioritize Local Breakout"

1. If at least one direct WAN Link to the Internet is up, the Security Gateway uses the "Local Breakout Only" connection:

   The Security Gateway sends the traffic directly to the Internet, based on the **Services & Applications** column of the SD-WAN Policy.

2. If **all** direct WAN Links to the Internet are down, the Security Gateway uses the "Backhaul Only" connection:

   a. The Branch Security Gateway creates a Site-to-Site VPN tunnel with the Headquarters Security Gateway.

   b. The Branch Security Gateway encrypts the traffic and sends the traffic directly to the Headquarters Security Gateway.

   c. The Headquarters Security Gateway decrypts the traffic.

   d. The Headquarters Security Gateway forwards the traffic to the Internet.

   e. The response arrives from the Internet to the Headquarters Security Gateway.

   f. The Headquarters Security Gateway inspects the traffic.

   g. The Headquarters Security Gateway encrypts the traffic and sends the traffic directly to the Branch Security Gateway.

   h. The Branch Security Gateway decrypts the traffic.

Important Notes for "Prioritize Local Breakout"

Important:

- Requirements for this connection type:
  1. In the Security Gateway object, enable the **IPSec VPN** Software Blade.
  2. Configure a Site-to-Site VPN tunnel between a Branch Security Gateway (that works as a Satellite VPN Gateway) and a Headquarters Security Gateway (that works as a Center VPN Gateway).
     Configure the applicable VPN Community of type **Star**. On the **VPN Routing** page, select **To center or through the center to other satellites, to Internet and other VPN targets**.
     This configuration is mandatory when working with Domain-Based VPN (see *"SD-WAN and Route-Based VPN" on page 266*).
     See the *Site to Site VPN Administration Guide* for your version.
- Make sure the Access Control Policy and Threat Prevention Policy allow this traffic.
  See the:
  - *Security Management Administration Guide* for your version.
  - *Threat Prevention Administration Guide* for your version.
- If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.
  See *"Configuring Steering Behavior" on page 171*.
- The IPSec VPN Software Blade on the Security Gateway makes the IKE negotiation routing decision, regardless the SD-WAN Policy rules.
- Each VPN tunnel from one SD-WAN interface on the SD-WAN Security Gateway to an SD-WAN interface on a peer SD-WAN Security Gateway is a VPN transport. Each SD-WAN Security Gateway constantly sends ICMP Echo Requests over each VPN transport to each VPN peer to select the best path to reach the VPN peer. The Security Gateway selects a VPN path for each packet. This preserves VPN connectivity during a failover of an existing VPN connection between different VPN transports.
- The routing preference "Prioritize Local Breakout" equals to having both "Local Breakout" and "Backhaul" enabled. "Backhaul" between two Security Gateways acts like "Overlay".
- The packet loss configured in the Steering object is calculated based on the last 100 probes.

Configuring Steering Candidates in "Prioritize Local Breakout"

In the section **Steering Candidates**, configure the applicable settings:

- **All Relevant WAN Links**

  The Security Gateway uses all available WAN Links.

- **Specific WAN Links**

  The Security Gateway uses only the selected WAN Links.

- **Use the same settings for Branch to HQ connection**

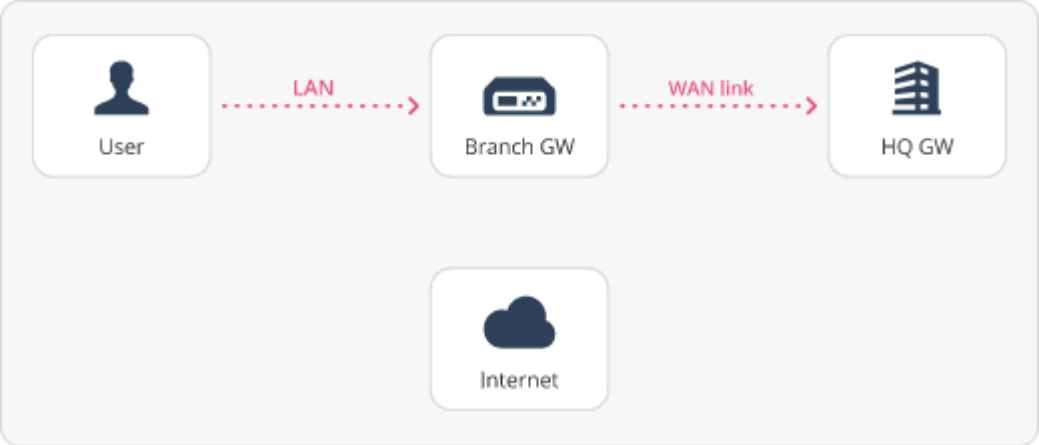
  Controls which WAN Links the Security Gateway uses to connect from a Branch office to the Headquarters ("**All Relevant WAN Links**" or "**Specific WAN Links**").

SD-WAN Connection Type - "Overlay"

This connection type represents a direct WAN Link with encrypted traffic to the Headquarters.

The direct WAN Link with encrypted traffic to the Headquarters provides redundancy.

Diagram for "Overlay"



Use Case and Example for "Overlay"

Branch offices with a direct WAN Link to the Internet and with a direct WAN Link to the Headquarters.

Branch offices must connect to a server behind the Headquarters Security Gateway.

Example:

1. A branch Security Gateway with two ISPs.
2. A Remote Desktop server is installed on an internal network behind the Headquarters Security Gateway.
3. A connection from an internal network behind a branch Security Gateway to the Remote Desktop server must go over a direct WAN Link (denoted "ISP1" below), while its latency is low.
4. When the latency of the direct WAN Link becomes greater than the latency of the direct private MPLS Link, the Remote Desktop connection must go over a direct private MPLS Link.

Example topology:

- `User ---> Branch Gateway ---> ISP1 ---> (Internet) ---> ISP2 ---> HQ Gateway ---> Remote Desktop`
- `User ---> Branch Gateway ---> MPLS ---> HQ Gateway ---> Remote Desktop`

Example of an SD-WAN Policy rule:

Traffic, using the "`Remote Desktop Control`" services, must go between an RDP Client behind the Branch Security Gateway and an RDP Server behind the Headquarters Security Gateway.

The Branch Security Gateway sends the traffic over this VPN tunnel, if the Access Control Policy allows this traffic.

Name	Source	Destination	Services & Applications	Behavior	Enforcement
Overlay	<Name of a Client Object> <Name of a Server Object>	<Name of a Client Object> <Name of a Server Object>	**Remote Desktop Control**	Select the applicable Steering object of type "Overlay"	<Applicable Profile>

Important Notes for "Overlay"

Important:

- Requirements for this connection type:

  1. In SmartConsole > **Menu** > **Manage policies and layers** > **Layers** page > **Access Control** page > edit the applicable Layer in your policy > **General** page > **Blades** section > select **Application & URL Filtering**.
  2. In the Security Gateway object, enable these Software Blades:
     a. **Application Control**
     b. **URL Filtering**
     c. **IPSec VPN**
  3. Configure a Site-to-Site VPN tunnel between a Branch Security Gateway (that works as a Satellite VPN Gateway) and a Headquarters Security Gateway (that works as a Center VPN Gateway).

     Configure the applicable VPN Community of type **Star**.

     On the **VPN Routing** page, select **To center only** or **To center and to other satellites through center**.

     See the *Site to Site VPN Administration Guide* for your version.
  4. SD-WAN Overlay steering is supported only between VPN peers that meet **all** of these conditions:
     a. Both VPN peers have SD-WAN enabled.
     b. Both VPN peers are managed by the same Check Point Management Server.
     c. Both VPN peers belong to the same Check Point Portal tenant.
     d. Both VPN peers use the same SD-WAN management method (either from SmartConsole, or from Check Point Portal > SD-WAN App).

     If any of these conditions is not met, the VPN peers establish VPN tunnels according to the settings configured in SmartConsole > Security Gateway object > **IPSec VPN** section > **Enhanced Link Selection**/ **Link Selection** page.

- Make sure the Access Control Policy and Threat Prevention Policy allow the "Overlay" traffic between the VPN Gateways.
  - The Access Control Policy must allow the ICMP probing (`echo-requests`) between the VPN Gateways.

    The applicable rule must be above the "Stealth" rule.

    If needed, in the **VPN** column of this rule, select only the required VPN Community.
  - The Access Control Policy must allow the ICMP probing (`echo-requests`) to be encrypted between the VPN Gateways:
    1. Click **Menu** > **Global properties** > click **Firewall** > -select **Accept ICMP requests** and in the drop-down menu, select any option except **First** > click **OK**.

       This makes sure to match the traffic on an explicit Access Control rule.
    2. Edit the applicable VPN Community object > click **Excluded Services** > make sure "`icmp-proto`" and "`echo-requests`" are not excluded from encryption.
    3. Edit the object of each VPN Gateway > click **Network Management** > click **VPN Domain** > clear the checkbox **Exclude gateway's external IP addresses from the VPN Domain** > click **OK**.
    4. Make sure the applicable `crypt.def` file on the Management Server does **not** exclude "`echo-requests`" from encryption between the VPN Gateways.

  See the:

  - *Security Management Administration Guide* for your version.
  - *Threat Prevention Administration Guide* for your version.
- If you did **not** use the SD-WAN Wizard during the initial deployment:
  - You must configure the required settings manually.

    See *"Configuring Steering Behavior" on page 171*.
  - For this connection type, you must configure a "Clean Up" rule in the SD-WAN Policy in Check Point Portal (as the last rule) to catch all the overlay traffic, including the ICMP probing.

    The SD-WAN Wizard creates this rule automatically.

    You can add more overlay network objects in the **Destination** column.

Name	Source	Destination	Services & Applications	Behavior	Enforcement
Any-VPN	**Any**	**My VPN Domain & Peer VPN Domain**	**Any**	Select the applicable Steering object of type "Overlay"	<Applicable Profile>

- The IPSec VPN Software Blade on the Security Gateway makes the IKE negotiation routing decision, regardless the SD-WAN Policy rules.
- Each VPN tunnel from one SD-WAN interface on the SD-WAN Security Gateway to an SD-WAN interface on a peer SD-WAN Security Gateway is a VPN transport.

  Each SD-WAN Security Gateway constantly sends ICMP Echo Requests over each VPN transport to each VPN peer to select the best path to reach the VPN peer.

  The Security Gateway selects a VPN path for each packet.

  This preserves VPN connectivity during a failover of an existing VPN connection between different VPN transports.
- The packet loss configured in the Steering object is calculated based on the last 100 probes.

Traffic Flow in "Overlay"

1. The Branch Security Gateway creates a Site-to-Site VPN tunnel with the Headquarters Security Gateway.
2. The Branch Security Gateway encrypts the traffic and sends the traffic directly to the Headquarters Security Gateway.
3. The Headquarters Security Gateway decrypts the traffic.
4. The Headquarters Security Gateway forwards the traffic to the destination server on the internal network.
5. The response arrives from the internal server to the Headquarters Security Gateway.
6. The Headquarters Security Gateway inspects the traffic.
7. The Headquarters Security Gateway encrypts the traffic and sends the traffic directly to the Branch Security Gateway.
8. The Branch Security Gateway decrypts the traffic.

Note - By default, the Branch Security Gateway uses all SD-WAN interfaces to create VPN tunnels to the peer Security Gateways. Meaning, if the Branch Security Gateway has two SD-WAN interfaces, it uses these two SD-WAN interfaces to send and receive traffic.

Configuring Steering Candidates in "Overlay"

In the section **Steering Candidates**, configure the applicable settings:

- **All Relevant WAN Links** - To use all available WAN Links.
- **Specific WAN Links** - To use only the selected WAN Links.

WAN Link Mapping

Important - If you did **not** use the SD-WAN Wizard during the initial deployment, then you must configure the required settings manually.

This section describes how to configure a mapping between WAN Links and Internet Service Providers.

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **WAN Link Mapping**.
5. Configure the WAN Links:
   a. From the top toolbar, click **Manage WAN Links**.

      Notes:
      - From the top toolbar, you can:
        - Create a new WAN Link
        - Delete a selected WAN Link
        - Search the WAN Links
        - Edit a selected WAN Link
      - If you hover over an existing WAN Link, the tooltip shows the Steering Behavior objects that use this WAN Link.

   b. To create a new WAN Link, click ✳(**New**) and select the type:

      Note - You cannot change the WAN Link type after you selected it.

      - **Public** - This represents a general public ISP link.

        Important - You can use a WAN Link of type "**Public**" for the connection types "Local Breakout" and "Overlay".

      - **Private** - This represents a private link (for example, MPLS).

        Important - You can use a WAN Link of type "**Private**" only for the connection type "Overlay" (you cannot use it for the connection type "Local Breakout").

   c. In the **Name** field, enter a short name that represents this WAN Link.

      This name appears in the Steering Behavior configuration.

d. **Optional:** In the **Comment** field, enter an applicable text that describes this WAN Link.

e. Click **OK**.

6. Configure the WAN Link Mapping.

   The **WAN Link Mapping** page shows this table:

#	Gateways	Name of WAN Link #1	Name of WAN Link #2	Name of WAN Link #...	Comment
1	Name of Security Gateway Object #1				
2	Name of Security Gateway Object #2				
3	Name of Security Gateway Object #...				
...	**Any**				

Notes:

- The column "**Gateways**" shows only the Security Gateways that you added to profiles of type **SD-WAN Profile**.
- In the column "**Gateways**", in the same cell you can select (group) Security Gateways that need the same WAN Link Mapping settings (for example, total bandwidth).
- By default, all cells are empty in the WAN Link columns.
  This means the SD-WAN Policy does not apply to the WAN Link.
- In the column "**Gateways**", you can hover on the Security Gateway object to see the summary of the WAN Link Mapping configuration.
- The last row with the object "**Any**" in the column "**Gateways**" is a fallback for WAN Link Mapping - which interface to use if an administrator did not configure WAN Link Mapping explicitly.
  This row automatically applies to all Security Gateways that are not configured explicitly in this table.
- If the  icon appears in the column "**#**", it means another administrator is currently making changes in that row.
  Hover over the lock icon to see the name of that administrator.
  The lock disappears after that administrator clicks **Publish** and **Enforce**.
- If the  icon appears in the column "**#**", it means you made changes in that row, but did not click **Publish** and **Enforce** yet.
- If the  appears in the column "**#**", it means there is a major error with the Security Gateway.
- If the  icon appears next to the Security Gateway name in the column "**Gateways**", it means either the Nano-Agent on that Security Gateway is not connected to the SD-WAN service, or that Security Gateway does not have an Access Control policy installed.
- If the  icon appears next to the interface name in a WAN Link column, it means such an interface name does not exist on any of the Security Gateways in this table.
- If the  icon appears next to the tag in a WAN Link column, it means such an interface tag does not exist on any of the Security Gateways in this table.
- If the  icon appears next to the tag in a WAN Link column, it means this interface tag is already mapped to another WAN Link.
- If the red oval frame with the  icon appears around an object, it means this object is no longer available - an administrator deleted this object on the Management Server, which updated Check Point Portal.
  By design, Check Point Portal does not delete such objects from your configuration.
  You must manually change all places that contain this deleted object.

Follow these steps in the applicable row:

a. To add a new row, from the top toolbar click **New**.

   The new row appears at the top of the table.

b. In the column "**Gateways**", click "**(+)**".

   Note - To remove an object from this column, hover over it and click "**x**".

c. Select the applicable Security Gateway / Cluster objects.

d. Click **OK**.

e. In the applicable column "**<Name of WAN Link>**", click **(+)**.

   The **WAN Link Mapping Rule** window opens.

f. In the section **Interface Mapping**, configure how to match traffic to an interface - only by the name, only by the tag, or both:

   - Select **By name** and select either one of the existing names, or **Other (Custom)** and enter the required interface name.
   - Select **By tag** and select either one of the existing tags, or **Other (Custom)** and enter the required interface tag.

     Note - Administrators configure these tags on the Security Gateway, in the interface properties.

     - For on-premises Management Server, see *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*".
     - For Smart-1 Cloud, see *"Step 3 - Configuration on Security Gateways" on page 130* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*"

g. In the section **Bandwidth**, configure the total bandwidth for the interface - download and upload.

   Important:

   - For more information about QoS, see *"EA Feature: QoS in SD-WAN" on page 301*.
   - Make sure to enter the values that match the ISP bandwidth.
   - If you configure bandwidth values in the interface settings in the Gaia OS on the Security Gateway, then those local values override the values in WAN Link Mapping.

h. In the section **QoS**, configure the required bandwidth limits for the interface - upload and download.

   In the field **Default QoS Action**, select the required QoS object.

   After you select a QoS object, you hover over it to see its settings.

   For more information about QoS, see *"EA Feature: QoS in SD-WAN" on page 301*.

i. In the section **Advanced Settings**, you can control the Symmetric Packet Return (see *"SD-WAN Symmetric Packet Return" on page 257*) for this specific interface:

   - Select **Inbound Symmetric Return** to enable the Symmetric Packet Return for this specific interface.

     This is the default.

     Best Practice - Select this option for Public WAN Links.

   - Clear **Inbound Symmetric Return** to disable the Symmetric Packet Return for this specific interface.

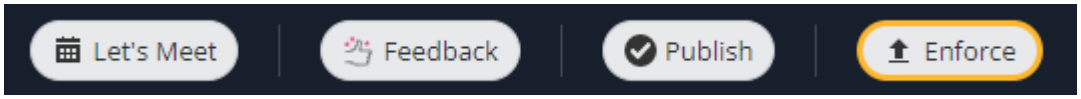
     Best Practice - Clear this option for Private WAN Links.

j. In the column "**Comment**", click in the cell, enter the applicable text, and press the Enter key.

   If this table contains many WAN Links, use the horizontal scrollbar below this table.

7. From the top toolbar, click **Publish** to save the changes.
8. From the top toolbar, click **Enforce** to apply the changes.

   The orange frame on this button means there are changes that are not enforced.



In the popup window that opens, click **Publish & Enforce Policy**.

SD-WAN Monitoring

Monitoring SD-WAN Status in Check Point Portal

Procedure

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Monitor**.
4. In the middle section, click **Dashboard**.
5. From the top, click the **General** tab.

The **General** tab shows these widgets:

- **Gateways**
- **Overlay Tunnels**

  The link **View Details** opens the dedicated tab with more data - see *"Monitoring Overlay Tunnels in Check Point Portal" on page 214*.
- **Steering Hits**

  This percentage breakdown is based on the the names of the Steering Hits that Security Gateways send in their logs.
- **Link Swaps**

  The link **View Details** opens the dedicated tab with more data - see *"Monitoring ISP Link Attributes in Check Point Portal" on page 214*.
- **Overall SLA**

  The link **View Details** opens the dedicated tab with more data.

- **Top Applications**

  Notes:
  - To see this data:
    1. The relevant license must exist in the corresponding User Center account.
    2. It is necessary to enable Log Sharing in SmartConsole on the on-premises Management Server.
       See *"Part 2 - Configure Object Sharing and Log Sharing" on page 72*.
  - By default, this widget shows the data from all Security Gateways. You can click **All Gateways** and select only specific Security Gateways.

- **Top Users**

  Notes:
  - To see this data:
    1. The relevant license must exist in the corresponding User Center account.
    2. It is necessary to enable Log Sharing in SmartConsole on the on-premises Management Server.
       See *"Part 2 - Configure Object Sharing and Log Sharing" on page 72*.
  - By default, this widget shows the data from all Security Gateways. You can click **All Gateways** and select only specific Security Gateways.

Monitoring ISP Link Attributes in Check Point Portal

Procedure

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Monitor**.
4. In the middle section, click **Dashboard**.
5. From the top, click the **Live Monitoring** tab.

Note - When you hover over the plotted line for the threshold (dashed line), the tooltip shows the threshold value as it was configured in the Steering Behavior object at the exact time you see the tooltip.

Monitoring Overlay Tunnels in Check Point Portal

Procedure

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Monitor**.
4. In the middle section, click **Dashboard**.
5. From the top, click the **Overlay Tunnels Monitoring** tab.

Monitoring SD-WAN Steering Events in Check Point Portal

Procedure

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Monitor**.
4. In the middle section, click **Events**.

Notes:

- In the top left corner, you can select the applicable time (the default is last 7 days).
- In the top search field, you can use Check Point Query Language.
  The basic query syntax is:

  ```
  [<Field>:] "<Filter Criterion>"
  ```

  To run a query for many criteria at the same time, use Boolean operators:

  ```
  [<Field 1>:] "<Filter Criterion 1>" {AND|OR|NOT}
  [<Field 2>:] "<Filter Criterion 2>" ...
  ```
- In the top right corner, you can refresh the search results and enable an automatic refresh.
- In the top right corner, you can export the search results.
- From the left side of search results, you can pull out the **Statistics** pane (click the arrows icon at the top) that shows a summary for the current search results.
- From the right side of search results, you can pull out the **Card** pane (click the arrows icon at the top) that shows data from the selected row.

Monitoring SD-WAN Traffic Logs in Check Point Portal

Procedure

Important:

- For the on-premises Management Server, you must enable the **Log Sharing** in SmartConsole (see *"Optional: Enable Log Sharing:" on page 80*).
- In Smart-1 Cloud, the **Log Sharing** is enabled by default.

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Monitor**.
4. In the middle section, click **Logs**.

Notes:

- In the top left corner, you can select the applicable time (the default is last 7 days).
- In the top search field, you can use Check Point Query Language.
  The basic query syntax is:

  ```
  [<Field>:] "<Filter Criterion>"
  ```

  To run a query for many criteria at the same time, use Boolean operators:

  ```
  [<Field 1>:] "<Filter Criterion 1>" {AND|OR|NOT}
  [<Field 2>:] "<Filter Criterion 2>" ...
  ```
- In the top right corner, you can refresh the search results and enable an automatic refresh.
- In the top right corner, you can export the search results.
- From the left side of search results, you can pull out the **Statistics** pane (click the arrows icon ⏩ at the top) that shows a summary for the current search results.
- From the right side of search results, you can pull out the **Card** pane (click the arrows icon ⏪ at the top) that shows data from the selected row.

Monitoring SD-WAN Policy in Check Point Portal

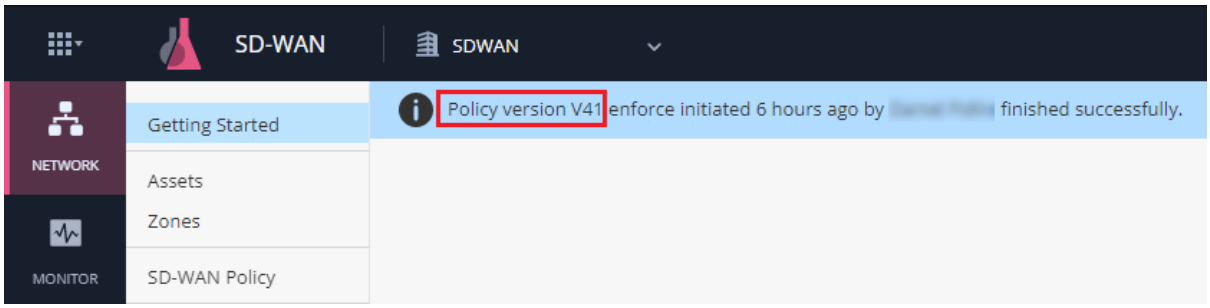
To see which policy the Security Gateways enforce, follow one of the procedures below.

Procedure 1 - Examine the Notification

1. From the left navigation panel, click **Network**.
2. A notification at the top shows the policy version.

   After you click the **x** icon on the right side of this notification, it does not appear anymore.

   Example:

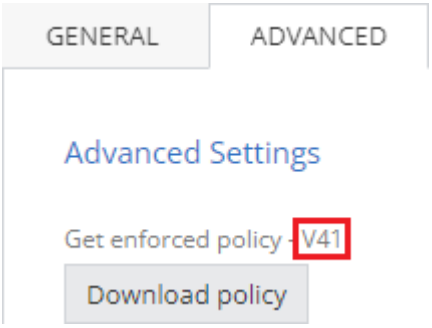


Procedure 2 - Examine the Profile

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Profiles**.
3. Click a profile.

   See *"The "Network" View" on page 42* > **Profiles**.
4. Click the **Advanced** tab.
5. In the **Advanced Settings** section, refer to the policy version in the line **Get enforced policy**.

   Example:



Monitoring the Connected Security Gateways in Check Point Portal

Procedure

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Agents**.

   See *"The "Network" View" on page 42* > **Agents**.

Monitoring SD-WAN on the Security Gateway

On the Security Gateway / Active Cluster Member, you can examine:

- If the Nano-Agent is installed properly.
- If the Security Gateway / Active Cluster Member is paired with Check Point Portal.

Note - SD-WAN does **not** support ClusterXL in the Load Sharing modes. In ClusterXL High Availability mode, SD-WAN runs only on the Active Cluster Member.

Procedure

1. Connect to the command line on the Security Gateway / Active Cluster Member.
2. Log in to the Expert mode.
3. Examine the status of the required Nano-Services:

   ```
   cpnano -s
   ```

   The section "`Service settings`" in the output must show "`Status: Running`" for these services:

   - `Check Point Orchestration Nano Service`
   - `Check Point Messaging Proxy Nano Service`
   - `Check Point SDWan Nano Service`
   - `Check Point Cpview Metric Provider Nano Service`
   - `Check Point SD-WAN Logger Nano Service`
4. Examine the SD-WAN policy:

   ```
   cpsdwan stat
   ```
5. Examine the data in CPView:
   a. Run:

      ```
      cpview
      ```

   b. From the top, click **Advanced** > **SDWAN**.
      - All "**State**" columns must show "**UP**".
      - The section **Overlay Probing Results** shows the current tunnels.

SD-WAN Configuration for DAIP Security Gateways

This section describes SD-WAN "Overlay" configuration for Security Gateways with a Dynamically Assigned IP Address (DAIP).

For frequently asked questions about DAIP, see sk167473.

SD-WAN Requirements for DAIP Security Gateways

SD-WAN Security Gateway	Supported Versions
Security Gateways that run Gaia OS	R81.20 Jumbo Hotfix Accumulator, Take 43 and higher.
Spark Firewall Appliances	R81.10.10 and higher.

SD-WAN Support for DAIP Security Gateways

- SD-WAN supports DAIP Security Gateways in a Star VPN Community or a Mesh VPN Community:
  - Supports a VPN tunnel when one VPN peer is a Security Gateway with a Dynamically Assigned IP Address (DAIP) and another VPN peer is a Security Gateway with a Static IP address.
  - Supports a VPN tunnel when all VPN peers are Security Gateways with a Dynamically Assigned IP Address (DAIP).

    SD-WAN supports this configuration only if the corresponding SD-WAN interfaces on all VPN peers receive their IP addresses dynamically and connect to the Internet directly (not through a NAT device).
- SD-WAN supports Security Gateways with different IP configuration on their SD-WAN interfaces - an SD-WAN interface with a Dynamically Assigned IP Address (DAIP), and other SD-WAN interfaces with a Static IP address.
  - Spark Firewall appliances can have one or more DAIP SD-WAN interfaces.
- SD-WAN supports automatic renewal of VPN tunnels on DAIP SD-WAN interfaces:
  - A VPN tunnel recovers automatically after an IP address changes on a DAIP interface that participates in this VPN tunnel:

    [Security Gateway] (DAIP SD-WAN interface) --- [VPN Tunnel]
  - A VPN tunnel recovers automatically after an IP address changes on an IP NAT device in front of an SD-WAN interface that participates in this VPN tunnel:

    [Security Gateway] (SD-WAN interface) (Dynamic IP NAT Device) --- [VPN Tunnel]

SD-WAN Known Limitations for DAIP Security Gateways

- Security Gateway object in SmartConsole must be configured as "**Dynamic address**" (on the **General Properties** page).

  Note - It is **not** supported to change this setting in an existing Security Gateway object.
  You must delete it and create a new object.

- IKE negotiation:

  - If each DAIP Security Gateway in a VPN Community uses a DAIP SD-WAN interface without a dynamic IP NAT device in front of it, then each VPN peer can initiate the IKE negotiation.

    [Security Gateway 1] (DAIP SD-WAN interface 1) <===> [VPN Tunnel] <===> (DAIP SD-WAN interface 2) [Security Gateway 2]

  - If a Security Gateway in a VPN Community has a dynamic IP NAT device in front it, then this DAIP Security Gateway can only be the IKE-initiator for this VPN tunnel (cannot be the IKE-responder).

    [Security Gateway 1] (SD-WAN interface 1) (Dynamic IP NAT Device) ===> [VPN Tunnel] ===> (SD-WAN interface 2) [Security Gateway 2]

- Configuration where a dynamic IP NAT device is connected in front of each SD-WAN Security Gateway is not supported (CGNAT-to-CGNAT):

  [Security Gateway 1] (SD-WAN interface 1) (Dynamic IP NAT Device 1) <===>

  <===> [VPN Tunnel] <===>

  <===> (Dynamic IP NAT Device 2) (SD-WAN interface 2) [Security Gateway 2]

- After an IP address changes on an IP NAT device in front of an SD-WAN interface that participates in a VPN tunnel, it takes approximately 5 minutes for the VPN tunnel to negotiate again:

  [Security Gateway] (SD-WAN interface) (Dynamic IP NAT Device) <===> [VPN Tunnel] <===>

- DNS resolving is not supported for DAIP Security Gateways.

- For a Branch Security Gateway that is configured as a DAIP Security Gateway and performs "Backhaul" through the Center Security Gateway (see *"Routing Preference "Backhaul Only"" on page 191*):

You must make sure that the Branch Security Gateway has a direct Internet access. When the IP address changes on the Branch Security Gateway, and its VPN tunnels go down, the Center Security Gateway and other VPN peers must be able to get the new IP address of the Branch Security Gateway.

You must configure the SD-WAN Policy to match connections that the Branch Security Gateway creates (local connections) to a Steering Behavior configured as "**Local Breakout Only**" (see *"Routing Preference "Local Breakout Only"" on page 188*) or "**Prioritize Local Breakout**" (see *"Routing Preference "Prioritize Local Breakout"" on page 195*).

SD-WAN Configuration for DAIP Security Gateways

Important - Schedule a maintenance window.

Part 1 - On a Security Gateway, configure the DAIP settings

Follow the applicable procedure.

Configuring a new Security Gateway that runs Gaia OS

Note - This applies only to a new Security Gateway, on which you can run the Gaia First Time Configuration Wizard.

1. During the Gaia First Time Configuration Wizard, in the **Dynamically Assigned IP** window, you must select **Yes**.

   Refer to the *Gaia Administration Guide* for your version > Chapter "*Configuring Gaia for the First Time*" > Section "*Running the First Time Configuration Wizard in Gaia Portal*".

2. Install the required R81.20 Jumbo Hotfix Accumulator.

3. Follow *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*" > subsection "*Procedure for a Security Gateway that runs Gaia OS*".

   In Gaia Portal, on the **SD-WAN** tab of the interface settings, select:

   a. **Use as SD-WAN interface**.

   b. **Directly accessible**.

Configuring an existing Security Gateway that runs Gaia OS

Note - This applies to a Security Gateway that was not configured as DAIP in the Gaia First Time Configuration Wizard.

Best Practice - Collect the Gaia Backup. Refer to the *Gaia Administration Guide* for your version > Chapter "*Maintenance*" > Section "*System Backup*".

1. Connect to the command line on the Security Gateway.

2. Log in to the Expert mode.

3. Configure this Security Gateway as DAIP:

   ```
   cpprod_util FwSetDAG 1
   ```

4. In Gaia Portal, configure each applicable interface as an SD-WAN interface:

   Note - For the applicable Gaia Clish commands, see *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WANinterfaces on the Security Gateway*" > subsection "*Procedure for a Security Gateway that runs Gaia OS*".

   a. In the **Network Management** section, click the **Network Interfaces** page.

   b. Select and edit each SD-WAN interface.

   c. On the **SD-WAN** tab of the interface settings, select:

      i. **Use as SD-WAN interface**.

      ii. **Directly accessible**.

   d. Click **OK**.

5. If you already configured a Security Gateway object in SmartConsole for this Security Gateway, then reset SIC on the Security Gateway.

   Procedure

   Best Practice - Perform this step over a direct connection to the Security Gateway - through the console port, or LOM Card (if it is installed).

   Note - For the complete procedure, see sk65764. In this step, you reset SIC only on the Security Gateway. In Part 2 below, you reset SIC in SmartConsole in the Security Gateway object.

   a. Run:

      ```
      cpconfig
      ```

   b. Enter the number of the option "**Secure Internal Communication**".

   c. Confirm that you wish to re-initialize the communication.

   d. Enter the new activation key.

      You must enter this key later in SmartConsole in the Security Gateway object (in Part 2 below).

   e. Exit from the Check Point Configuration Tool.

   f. The Security Gateway stops and starts all Check Point processes.

      Warning - If you are connected over SSH, your session may disconnect.

Configuring a Spark Firewall Appliance that runs Gaia Embedded OS R81.10.10 and higher

Note - For the complete procedure, see *"Step 3 - Configuration on Security Gateways" on page 83* > section "*Part 2 - Configuration of SD-WAN interfaces on the Security Gateway*" > subsection "*Procedure for a Spark Firewall Appliance that runs Gaia Embedded OS*" > subsection "*Configuration of a Spark Firewall Appliance in the WebUI*".

1. Connect to the WebUI.
2. From the left tree, click **Device**.
3. In the middle pane, expand the section **Network** and click **Internet**.
4. Select and edit the Internet connection.
5. At the top, click the **Configuration** tab:
   a. Expand the section **Internet Configuration**.
   b. In the **Type** field, select the applicable option :
      - If this interface gets its IP address dynamically, then select **DHCP**.
      - If this interface has a static IP address, then select **Static IP**.
6. Click **Save**.
7. If you already configured a Security Gateway object in SmartConsole for this Spark Firewall appliance, then reset SIC on the appliance.

   Procedure

   Note - For the complete procedure, see sk65764. In this step, you reset SIC only on the appliance. In Part 2 below, you reset SIC in SmartConsole in the Security Gateway object.

   a. Connect to the WebUI.
   b. From the left tree, click **Home**.
   c. In the middle pane, expand the section **Overview** and click **Security Management**.
   d. In the **Security Management Server** section, click **Advanced**.
   e. Click **Reinitialize Trusted Communication**.
   f. A warning message appears.
   g. Click **Yes**.
   h. The appliance unloads the central policy and applies only the local policy.

Part 2 - In SmartConsole, configure the Security Gateway Object

Follow the applicable procedure.

Note - If you already configured a Security Gateway object in SmartConsole, then you must reset SIC in this object, delete it, and then create a new object.

Resetting SIC in an existing Security Gateway object

1. Back up the current management database on the Management Server:
   a. Export the management database. See sk108902.
   b. Collect the CPinfo file. See sk92739.
2. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server that manages this Security Gateway.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click the existing Security Gateway object.
5. Reset the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:

   Note - For the complete procedure, see sk65764. In this step, you reset SIC in the Security Gateway object.

   a. Near the **Secure Internal Communication** field, click **Communication**.
   b. In the **Certificate state** field, click **Reset** and click **Yes** to confirm.

      Click **OK**.
   c. Click **OK**.
6. Click **OK**.
7. Right-click the Security Gateway > click **Delete**.

Configuring a new Security Gateway object that runs Gaia OS

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server that should manage this Security Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. From the top toolbar, click the **New** (✶) > **Gateway**.
4. In the **Check Point Security Gateway Creation** window, click **Classic Mode**.
5. In the **Name** field, enter the applicable name for this Security Gateway object.

6. Select **Dynamic Address**.

   Note - You must select this checkbox in these cases:
   - The SD-WAN interface receives its IP address dynamically (from a DHCP server, from a PPPoE provider).
   - The SD-WAN interface has a static IP address, but this IP address can change from time to time.
   - The SD-WAN interface has a static IP address that does not change, but connects to a NAT device that in turn receives its IP address dynamically.

7. Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:
   a. Near the **Secure Internal Communication** field, click **Communication**.
   b. In the **Platform** field, select **Open server / Appliance**.
   c. Enter the same **Activation Key** you entered:
      - During the Gaia First Time Configuration Wizard on a new Security Gateway.
      - When you reset SIC on an existing Security Gateway.
   d. Click **Initialize**.
   e. Click **OK**.
8. In the **Platform** section, select the correct options.
9. Enable the applicable Software Blades (refer to the list of SD-WAN limitations).
10. On the **Network Management** page, configure interfaces:
    a. Click **Get Interfaces** > **Get Interfaces With Topology** > click **Close**.
    b. Select and edit each interface.
    c. In each DAIP interface, in the **General** section, select **Dynamic IP**.
    d. Click **OK**.
11. Click **OK**.

Configuring a new Spark Firewall object that runs Gaia Embedded OS

1. Connect with SmartConsole to the applicable Security Management Server or Domain Management Server that should manage this Security Gateway.
2. From the left navigation panel, click **Gateways & Servers**.
3. From the top toolbar, click the **New** (✶) > **Gateway**.

4. In the **Check Point Security Gateway Creation** window, click **Classic Mode**.
5. In the **Name** field, enter the applicable name for this Security Gateway object.
6. Select **Dynamic Address**.
7. In the **Platform** section, select the correct options.
8. Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:
    a. Near the **Secure Internal Communication** field, click **Communication**.
    b. In the **Platform** field, select **Small Office Appliance**.
    c. In the **Authentication** section:
        i. Select **Initiate trusted communication securely by using a one-time password**.
        ii. Enter a one-time password (SIC activation key).
    d. In the **Trusted Communication Initiation** section:
        i. Select **Initiate trusted communication automatically when the Gateway connects to the Security Management server for the first time**.
        ii. In the field **Identify appliance according to**, select the applicable option and enter the required value.
    e. Click **OK**.
9. Enable the applicable Software Blades (refer to the list of SD-WAN limitations).
10. On the **Topology** page, configure each DAIP interface:
    a. In the **Security Blades** section, select **Manually defined on the Security Management server, based on the below Topology Table**.
    b. In the **Topology Table** section, select the interface and click **Edit**.
    c. In the **Security and VPN Blades Topology** section, select **External (leads out to the Internet)**.
    d. In the **IP settings** section, select **Dynamic IP**.
    e. Click **OK**.
    f. In the **Security Blades** section, if needed, select **Automatically calculated by the gateway, based on the gateway's Routing Table**.
11. Click **OK**.

Part 3 - In SmartConsole, configure the Access Control Policy

Procedure

If it is necessary to use "Overlay" probing, then configure the required Access Control rule:

For Security Gateways with a Dynamically Assigned IP Address (DAIP):

1. Configure this Access Control rule:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
For DAIP - Overlay Probing - Incoming	`Any`	`LocalMachine_All_Interfaces`	Name of the VPN Community	`echo-request`	`Accept`	`Log` or `None`	Only DAIP Security Gateways

Note - The object "`LocalMachine_All_Interfaces`" is enforced only on DAIP Security Gateways.

2. Install the Access Control policy only on the DAIP Security Gateways.

For Security Gateways that are VPN peers with DAIP Security Gateways:

1. Configure this Access Control rule:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
For Center GW - Overlay Probing - Incoming	`Any`	Security Gateways that are VPN peers with DAIP Security Gateways	Name of the VPN Community	`echo-request`	`Accept`	`Log` or `None`	Security Gateways that are VPN peers with DAIP Security Gateways

2. Install the Access Control policy only on the Center Security Gateway.

Part 4 - In Check Point Portal, configure the SD-WAN Policy

Procedure

If it is necessary to use "Overlay" probing, then configure these SD-WAN rules:

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the top toolbar, create the applicable new rules.

   Option 1 - Configure a specific rule for "Overlay" Probing

   For Security Gateways with a Dynamically Assigned IP Address (DAIP):

Name	Source	Destination	Services & Applications	Behavior	Enforcement
'Overlay' Probing - Incoming	`Any`	`LocalMachine_All_Interfaces`	`icmp-proto`	`Default overlay`	Select the applicable profile objects

   Note - The object "`LocalMachine_All_Interfaces`" is enforced only on DAIP Security Gateways.

   For Security Gateways that are VPN peers with DAIP Security Gateways:

Name	Source	Destination	Services & Applications	Behavior	Enforcement
'Overlay' Probing - Incoming	`Any`	Security Gateways that are VPN peers with DAIP Security Gateways	`icmp-proto`	`Default overlay`	Select the applicable profile objects

Option 2 - Configure more general rules for "Overlay" Probing

Name	Source	Destination	Services & Applications	Behavior	Enforcement
'Overlay' Probing - Incoming	`Any`	`My VPN Domain & Peer VPN Domain`	`icmp-proto`	Select the applicable Steering object of type "Overlay"	Select the applicable profile objects

4. From the top toolbar, click **Publish** to save the changes.
5. From the top toolbar, click **Enforce** to apply the changes.

   In the popup window that opens, click **Publish & Enforce Policy**.

SD-WAN Troubleshooting for DAIP Security Gateways

Procedure

You can use these CLI commands on the local Security Gateway to monitor if it learns the new IP address of a DAIP VPN peer:

CLI Syntax	Troubleshooting Information	Command Notes
`cpview`	1. At the top, click **Software-blades** > **VPN** > **Tunnel-Monitoring**. 2. In the bottom section **Dynamic table** shows this information for a DAIP Security Gateway: ■ The column **Main peer IP** shows "`0.0.0.x`". ■ The column **Peer IP** shows the last known peer IP address. This column must show a new IP address when the DAIP peer changes its IP address.	See sk101878.

CLI Syntax	Troubleshooting Information	Command Notes
`vpn tu tlist`	1. If the command output does not show Outbound SA or IPsec SA, then the VPN tunnel is "down". 2. The field "**To:**" shows the last known peer IP address. This field must show a new IP address when the DAIP peer changes its IP address.	1. Refer to the *CLI Reference Guide* for your version for your version > Chapter "*VPN Commands*" > Section "*vpn*" > Subsection "*vpn tu*". 2. See sk181147.
`vpn tu conn <Source IP> <Source Port> <Destination IP> <Destination Port> <Protocol>`	The traffic must pass over the updated VPN tunnel with the new IP address of a DAIP Security Gateway.	1. Refer to the *CLI Reference Guide* for your version > Chapter "*VPN Commands*" > Section "*vpn*" > Subsection "*vpn tu*". You can use the minus character "`-`" as a wildcard "`any`". 2. See sk181147.

SD-WAN Best Practices

This section describes different best practices for SD-WAN configuration.

VPN - Link Selection

Explanation

Best Practice - Always configure the Link Selection in the Security Gateway object. If the SD-WAN service on the Security Gateway goes down for some reason, this makes sure the Security Gateway uses the applicable interface for Site-to-Site VPN.

- When two or more Security Gateways with enabled SD-WAN participate in the same Site-to-Site VPN Community, these Security Gateways automatically initiate Site-to-Site VPN tunnels between their SD-WAN interfaces.

  These Security Gateways **ignore** the configuration in SmartConsole > Security Gateway object > **IPSec VPN** > **Link Selection**, and select the interfaces based on the WAN Link Mapping configuration.

- When a Security Gateway with enabled SD-WAN participate in the same Site-to-Site VPN Community with a Security Gateway without SD-WAN, these Security Gateways **use** the configuration in SmartConsole > Security Gateway object > **IPSec VPN** > **Link Selection**.

SD-WAN Policy - Rule Matching

Explanation

Best Practices:

1. Make sure that:
   - Traffic that should go through SD-WAN, matches the correct SD-WAN Policy rule and behavior.
   - Traffic that should **not** go through SD-WAN, does **not** match a "Local Breakout" rule, so it goes through the operating system routing.
2. In a rule with the "Local Breakout" behavior:
   - Do **not** use "**Any**" in the **Destination** column.
   - Do **not** use any object that can match non-Internet traffic (inter-VLAN communication, traffic to next hop gateways, traffic in DMZ networks, and so on) in the **Destination** column because the Security Gateway would send the matched non-Internet traffic directly to its ISPs.
3. In a rule with the "Backhaul" behavior:
   - Do **not** use "**Any**" in the **Destination** column.
   - Do **not** use any object that can match non-Internet traffic (inter-VLAN communication, traffic to next hop gateways, traffic in DMZ networks, and so on) in the **Destination** column because the Security Gateway would send the matched non-Internet traffic directly to its ISPs.
4. Configure rules with the "Overlay" behavior **above** rules with the "Local Breakout" behavior.
5. Do **not** use the "**Internet**" object in rules.
   This object cannot differentiate between an actual Internet traffic, "Overlay" traffic, or a cleartext traffic that is routed through an MPLS next hop router.

Note - The Security Gateway always matches the original connection direction.

The Security Gateway matches the first applicable rule in SD-WAN Policy and stops processing the rules.

The SD-WAN Policy rules that use the Breakout behavior work similar to Policy-Based Routing (PBR). During the routing process, the Security Gateway first applies these rules and overrides the operating system routes when these rules match (including the directly connected networks).

SD-WAN Rule	Guidelines and Security Gateway Behavior
Rule with the "Overlay" behavior	■ If the Security Gateway with enabled SD-WAN has to encrypt the traffic, and the VPN peer is **also** a Security Gateway with enabled SD-WAN, then the Security Gateway routes the traffic based on the rule steering behavior. ■ If the Security Gateway with enabled SD-WAN has to encrypt the traffic, and the VPN peer is a Security Gateway **without** enabled SD-WAN, then the Security Gateway routes the traffic based on the configured Link Selection in the Security Gateway object. ■ If the Security Gateway with enabled SD-WAN does **not** have to encrypt the traffic, the Security Gateway routes the traffic based on the operating system routing table.
Rule with the "Local Breakout" behavior	■ Make sure the Security Gateway does **not** match the "Overlay" traffic to rules with the "Local Breakout" behavior. Otherwise, the Security Gateway cannot use all VPN Transports / WAN Links to the SD-WAN VPN peer to forward the traffic. ■ The Security Gateway sends the cleartext traffic to its ISPs based on your steering configuration. Make sure the Security Gateway matches only the applicable outbound Internet traffic to rules with the "Local Breakout" behavior. Make sure the Security Gateway does **not** match cleartext non-Internet traffic (inter-VLAN communication, traffic to next hop gateways, traffic in DMZ networks, and so on).
Rule with the "Backhaul" behavior	■ The Branch Security Gateway encrypts the traffic and sends it to the Center Security Gateway over a Site-to-Site VPN tunnel. The Center Security Gateway sends this traffic to the Internet as a "Local Breakout". ■ The Center Security Gateway does **not** send the traffic to the Internet, if the traffic is designated the Center Security Gateway. This traffic behaves as "Overlay".

SD-WAN Probing

SD-WAN Overlay Probing

SD-WAN Overlay Probing is a mechanism to measure the SLA over SD-WAN Overlay Transports (the channels used to carry data between the SD-WAN interfaces on the local Security Gateway and the SD-WAN interfaces on the remote VPN peer.

The SD-WAN Overlay Probing method uses ICMP Echo Request packets that each SD-WAN interface on the local Security Gateway sends to each corresponding SD-WAN interface on the remote VPN peer.

Best Practice - Probing over an Overlay VPN tunnel must match an SD-WAN rule that contains the "Overlay" behavior. In such a rule, in the **Source** column **and** in the **Destination** column, you must include all real IP addresses of all SD-WAN interfaces of all SD-WAN Security Gateways (it is **not** necessary to include NATed IP addresses).

The Security Gateway sends the ICMP Echo Requests to its SD-WAN peer regardless of the SD-WAN Policy rules - the Security Gateway automatically sends this probing traffic from the applicable VPN interface.

The Security Gateway receives the ICMP Echo Replies from its SD-WAN peer based on the SD-WAN Policy rules.

Therefore, this asymmetric scenario is possible:

1. The Security Gateway "GW1" sends the ICMP Echo Requests through "ISP1" of "GW1" to the peer Security Gateway "GW2" through "ISP1" of "GW2".
2. The Security Gateway "GW2" sends the ICMP Echo Replies through "ISP2" of "GW2" to the Security Gateway "GW1" through "ISP1" of "GW1".

The SD-WAN Wizard creates these default SD-WAN Policy rules:

Source	Destination	Services & Applications	Behavior
Any	My VPN Domain Peer VPN Domain	Any	Overlay
Any	SD-WAN Internet	Any	Default breakout

For more information about these three Dynamic Objects, see *"Dynamic Objects in SD-WAN Policy" on page 163*.

- The purpose of the top rule with the Dynamic Objects "**My VPN Domain**" and "**Peer VPN Domain**" is also to match all encrypted traffic to all private IP addresses (for example, MPLS interfaces) of all Security Gateways and to apply the "Overlay" behavior to this traffic.
- The purpose of the bottom rule with the Dynamic Object "**SD-WAN Internet**" is also to match all encrypted traffic to the public IP addresses of all Security Gateways and to apply the "Overlay" behavior to this traffic.

  The Steering Behavior object "Default breakout" has the routing preference "Prioritize Local Breakout", which equals to having both "Local Breakout" and "Backhaul". "Backhaul" between two Security Gateways acts like "Overlay".

If it is necessary to change the default "Local Breakout" rule from the "Default breakout" behavior to the routing preference "Local Breakout Only", you must create this explicit rule **at the top** of the SD-WAN Policy:

Source	Destination	Services & Applications	Behavior
All your overlay external IP addresses of all Security Gateways	All your overlay external IP addresses of all Security Gateways	`icmp-proto`	Overlay

Note - If your Security Gateway runs:

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator Take 14 and higher
- R81.20 Jumbo Hotfix Accumulator Take 79 and higher
- Spark Firewall R81.10.15 and higher

Then you can use the Dynamic Object "**My VPN Domain**" and the Dynamic Object "**Peer VPN Domain**".
The Default Overlay rule that the SD-WAN Wizard creates with these Dynamic Objects matches the Overlay probing traffic automatically, without the need of the above explicit rule. See *"Dynamic Objects in SD-WAN Policy" on page 163*.

SD-WAN Next Hop Probing

SD-WAN Next Hop Probing is a basic way of checking the ISP status in a fast manner, simply by probing the next hop of each SD-WAN interface.

SD-WAN Next Hop Probing can detect link failures and outages faster than the "Local Breakout" Probing. As a result, SD-WAN failover occurs faster.

After the next hop stops responding:

1. The WAN Link or ISP associated with the corresponding SD-WAN interface is considered as "Down" immediately.
2. The Security Gateway generates the event "`ISP <X> DOWN`".
3. The "Local Breakout" Probing stop on the SD-WAN interface until the ISP state for this SD-WAN interface become "Up" again.

The ISP state changes to "Down" only in these cases:

- The SD-WAN interface link state changed to "Down".
- The next hop stopped responding, and the SD-WAN Next Hop Probing mechanism changed the ISP state.

Note - The ISP is marked as "down" after three consecutive lost packets and is immediately marked as "up" after the ISP replies again.

The default SD-WAN Next Hop Probing:

Version	Default Next Hop Probing
■ R82.10 and higher ■ R82 Jumbo Hotfix Accumulator Take 14 and higher ■ R81.20 Jumbo Hotfix Accumulator Take 79 and higher ■ Spark Firewall R81.10.15 and higher	By default, the Next Hop Probing uses ARP Requests. If the next hop does not respond to ARP Requests, then the Next Hop Probing automatically falls back to ICMP Echo Requests.
■ R81.20 Jumbo Hotfix Accumulator, Take 76 and lower ■ Spark Firewall from R81.10.05 to R81.10.10	By default, the Next Hop Probing uses ICMP Echo Requests. There is no fall back to another probing protocol.

Notes:

- When working with the SD-WAN Routing Preference "Prioritize Local Breakout", the traffic failover from the "Local Breakout" behavior to the "Backhaul" behavior occurs only after the state of **each** available ISP changes to "Down".
- If the next hop of the Security Gateway does not respond reliably to probing, or if it is necessary to disable the Next Hop Probing, then follow the procedure in the section *"SD-WAN Next Hop Probing on Cloud Firewall Gateways" on the next page*.

SD-WAN Next Hop Probing on Cloud Firewall Gateways

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- If your SD-WAN Security Gateway is a Virtual Machine in a cloud (a Cloud Firewall Gateway), and its next hop does not respond to ICMP Echo Requests, then you must disable the SD-WAN ICMP Probing on this Cloud Firewall Gateway.

1. Connect to the command line on the Cloud Firewall Gateway / each Cloud Firewall Cluster Member.
2. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

3. If the file `$FWDIR/conf/sdwan/sdwan_steering_params.json` exists, create a backup copy.

   Otherwise, create this file.

   Run this long command:

   ```
   if [ -f $FWDIR/conf/sdwan/sdwan_steering_params.json ] ;
   then echo "Creating the backup ..." ; cp -v
   $FWDIR/conf/sdwan/sdwan_steering_params.json{,BKP} ; else
   echo "Creating the file ..." ; touch
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; stat
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; fi
   ```

4. Edit the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

   ```
   vi $FWDIR/conf/sdwan/sdwan_steering_params.json
   ```

5. If this file is empty, then add all these lines.

   If this file already contains other parameters, then add this parameter on a new line:

   ```
   {
       "sdw_nexthop_probe_enabled" : 0
   }
   ```

6. Save the changes in the file and exit the editor.
7. Restart the SD-WAN Steering process:

   ```
   sdwan_steering_stop ; sdwan_steering_start
   ```

Warning - Until the SD-WAN Steering process starts again (in normal circumstances, it takes less than one minute):

- Existing and new VPN / Overlay connections are interrupted.
- Existing Local Breakout connections may be interrupted.
- New Local Breakout connections cannot undergo the SD-WAN Local Breakout routing.

SD-WAN Next Hop Probing onSpark Firewall Appliances

InSpark Firewall Appliances, the SD-WAN next hop probing is **disabled** by default.

Follow these steps to enable it when necessary:

1. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.
2. Log in to the Expert mode.
3. If the file `$FWDIR/conf/sdwan/sdwan_steering_params.json` exists, create a backup copy.

   Otherwise, create this file.

   Run this long command:

   ```
   if [ -f $FWDIR/conf/sdwan/sdwan_steering_params.json ] ;
   then echo "Creating the backup ..." ; cp -v
   $FWDIR/conf/sdwan/sdwan_steering_params.json{,BKP} ; else
   echo "Creating the file ..." ; touch
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; stat
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; fi
   ```
4. Edit the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

   ```
   vi $FWDIR/conf/sdwan/sdwan_steering_params.json
   ```
5. If this file is empty, then add all these lines.

   If this file already contains other parameters, then add this parameter on a new line:

   ```
   {
       "sdw_nexthop_probe_enabled" : 1
   }
   ```
6. Save the changes in the file and exit the editor.
7. Restart the SD-WAN Steering process:

   ```
   sdwan_steering_stop ; sdwan_steering_start
   ```

   Warning - Until the SD-WAN Steering process starts again (in normal circumstances, it takes less than one minute):
   - Existing and new VPN / Overlay connections are interrupted.
   - Existing Local Breakout connections may be interrupted.
   - New Local Breakout connections cannot undergo the SD-WAN Local Breakout routing.

Routes

Explanation

Best Practice - If the Security Gateway has a private line (for example, MPLS), which is part of the overlay, then configure routes that send traffic for all the overlay destination networks to the MPLS next hop.

In this case, even if all ISP links are down, and no active default route exist in the operating system kernel, the specific route on the private MPLS makes sure that the "Overlay" traffic continues to work over the private MPLS SD-WAN interface. Without an active route to the destination, the packet is lost in the routing table, before the VPN encryption takes place.

SD-WAN Advanced Configuration

This section describes advanced configuration in Check Point Portal and on the SD-WAN Security Gateway.

SD-WAN FEC

Introduction to FEC

Check Point SD-WAN Forward Error Correction (FEC) ensures the successful delivery of traffic by adding Error Correction Code (ECC) packets to the "Overlay" packet stream.

FEC can help improve reliability when a packet loss is high.

Important:

- Enable FEC only when the ISP line has consistently high packet loss between the Security Gateways that participate in "Overlay" with each other. If you enable FEC when the ISP line works correctly, then the throughput decreases.
- Enabling FEC applies only to new connections, and not to existing connections.

FEC Requirements

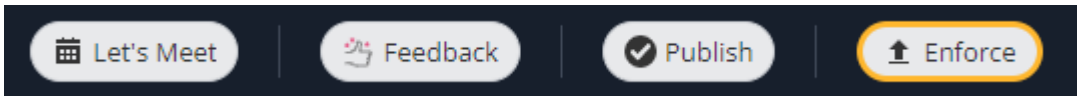
1. FEC requires at least two Security Gateways that participate in a Site to Site VPN tunnel with each other:
   - R82.10 and higher
   - R82 Jumbo Hotfix Accumulator Take 14 and higher
   - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
   - Spark Firewall R81.10.15 and higher
2. You must configure the each selected Security Gateway as described in *"SD-WAN Connection Type - "Overlay"" on page 200*.

FEC Configuration

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the top toolbar, click **FEC**.
4. Select the Security Gateways that participate in a Site to Site VPN tunnel with each other.
5. Click **OK**.

6. From the top toolbar, click **Publish** to save the changes.
7. From the top toolbar, click **Enforce** to apply the changes.

   The orange frame on this button means there are changes that are not enforced.

   In the popup window that opens, click **Publish & Enforce Policy**.

SD-WAN Circuit ID

The Circuit ID feature is available in these Security Gateway versions:

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator Take 14 and higher
- R81.20 Jumbo Hotfix Accumulator Take 79 and higher
- Spark Firewall R81.10.15 and higher

Overview

SD-WAN uses these WAN Link types (see *"WAN Link Mapping" on page 207*):

- **Public** - This represents a general public ISP link.

  Important - You can use a WAN Link of type "**Public**" for the connection types "Local Breakout" and "Overlay".

- **Private** - This represents a private link (for example, MPLS).

  Important - You can use a WAN Link of type "**Private**" only for the connection type "Overlay" (you cannot use it for the connection type "Local Breakout").

In SD-WAN, the circuit is a way to define a specific, closed WAN Network, through which VPN peers can communicate with each other.

Each WAN Link is configured with a Circuit ID number that is used to distinguish it from other WAN Links.

For example, SD-WAN does not create a VPN tunnel between a Local MPLS Link and a remote peer Internet Link.

The closed WAN Network:

- Can be **Public**, such as the worldwide Internet, where any connected device can communicate with another.

  The Internet is one global network. Therefore, a single common Circuit ID is required.

- Can be **Private**, such as a closed Point-to-Point, or an MPLS network, where only the devices connected to it can communicate with each another.

  - There may be multiple, different Private WAN circuits that a customer can use to connect the different sites.

    In such cases, multiple Circuit ID values may be required for different links.

  - Usually, it not possible to create a connection between different Private WAN Networks.

  - The same device can be connected to different Private WAN circuits, through different interfaces.

    As a result, the same device can be part of multiple WAN circuits.

How SD-WAN Uses the Circuit ID

Explanation

SD-WAN assigns different Circuit ID for Public WAN Links, and different Circuit ID for Private WAN Links:

- By default, each Public WAN Link gets the Circuit ID value 0 (zero).
- By default, each Private WAN Link gets the Circuit ID value 1 (one).

An SD-WAN Security Gateway always creates VPN tunnels only with VPN Peers that use the same Circuit ID as the local link.

The Nano-Agents on SD-WAN Security Gateways share the information about the configured WAN Links and their Circuit ID with Check Point Portal.

Example:

- Two SD-WAN VPN Peers.
- Each Security Gateway has two Public WAN Links and one Private WAN Link.

The VPN Peers will establish these VPN tunnels:

- Four VPN tunnels over the Public WAN Links

  (2 WAN Links on the first Security Gateway x 2 WAN Links on the second Security Gateway).

- One VPN tunnel over the Private WAN Link

  (1 WAN Link on the first Security Gateway x 1 WAN Link on the second Security Gateway).

The Need to Override the Default the Circuit ID

Explanation

Example:

- Two SD-WAN VPN Peers.
- Each Security Gateway has two Private WAN Links.
- The first Private WAN Link is connected to the interface `eth1`.
- The second Private WAN Link is connected to the interface `eth2`.

The VPN Peers will try to establish these four VPN tunnels over the two Private WAN Links:

VPN Tunnel	Interface on the First Security Gateway	Interface on the Second Security Gateway	VPN Tunnel Status
1	`eth1` (Circuit ID "1")	`eth1` (Circuit ID "1")	Established
2	`eth2` (Circuit ID "1")	`eth2` (Circuit ID "1")	Established
3	`eth1` (Circuit ID "1")	`eth2` (Circuit ID "1")	Down, constantly tries to establish
4	`eth2` (Circuit ID "1")	`eth1` (Circuit ID "1")	Down, constantly tries to establish

The cross-over VPN tunnels (between `eth1` and `eth2`, between `eth2` and `eth1`) are down, because these WAN Links have the same type (Private) and, therefore, have the same Circuit ID (value "1"). As a result, SD-WAN cannot distinguish these Private WAN Links from the Private WAN Links, on which it already established the VPN tunnels.

To resolve this conflict, you can configure a different value for the Circuit ID for different interfaces.

For example, for the interfaces `eth2`, configure the Circuit ID value "2":

VPN Tunnel	Interface on the First Security Gateway	Interface on the Second Security Gateway	VPN Tunnel Status
1	`eth1` (Circuit ID "1")	`eth1` (Circuit ID "1")	Established because the Circuit ID values are the same
2	`eth2` (Circuit ID "2")	`eth2` (Circuit ID "2")	Established because the Circuit ID values are the same
3	`eth1` (Circuit ID "1")	`eth2` (Circuit ID "2")	Not establish because the Circuit ID values are different
4	`eth2` (Circuit ID "2")	`eth1` (Circuit ID "1")	Not establish because the Circuit ID values are different

Use Cases to override the default the Circuit ID:

- Separate Circuit ID values are required for separate Private WAN Links (see the example above).
- It is necessary to establish VPN tunnels from Public LTE links only to peer LTE links (it is necessary to avoid LTE to Broadband tunnels, or any other pair of links).
- It is necessary to use specific ISP of the Headquarters Security Gateway only for VPN tunnel to a Cloud VPN peer.

  You do not want to use this ISP for VPN tunnels to your Branch Security Gateways or to any other VPN peer.

  You do not need this Cloud gateway (interface, or in general) to have a VPN tunnel to Branch Security Gateways.

  To accomplish this, you can configure the specific ISP WAN Link of the Headquarters Security Gateway and the ISP WAN Link of the Cloud gateway to use a different Circuit ID (for example, "2").
- There are three ISPs configured for "Local Breakout", but it is necessary to use only two ISPs for "Overlay" tunnels.

  For example, the first ISP is problematic for VPN (located behind a device that blocks IKE / NAT-T, or is just unreliable).

  To accomplish this, you can configure the third ISP to use a different Circuit ID value that is not used on any VPN peer.
- You have Private WAN Links that must be considered as Public WAN Links for "Local Breakout", but not for VPN.

  You have a Private MPLS link from a Branch Security Gateway to the Headquarters Security Gateway.

  You can route the traffic over the MPLS WAN Link in clear-text towards the Headquarters Security Gateway, such that the Branch Security Gateways can get to the Internet in clear-text through the Headquarters Security Gateway.

  You do not want to configure "Backhaul" over VPN, but to use the Private WAN Link as a third ISP, with manual priority for "Local Breakout".

  You want to avoid building VPN tunnels between Private links and Public links (which are all configured as Public, with the default Circuit ID "0").

  To accomplish this, you can change the Circuit ID of the true Private links to another value on all VPN Peers.

Configuring the Circuit ID

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- The value 0 is the default for Public WAN Links.
- The value 1 is the default for Private WAN Links.

Note - You can see the Circuit ID of the VPN peers on the Security Gateway:

- In the `$FWDIR/state/local/SDWAN/sdwan_steering_policy.json` file.
  In the section "`sdwan_steering_vpn_peers`" > refer to the section "*<Name of VPN Peer>*" > refer to the section "`Interfaces`" > refer to the section "*<Name of Interface>*" > refer to the parameter "`circuit_id`".
- In CPView (sk101878), click **Advanced** > **SD-WAN** > **Probing** > in the section **Overlay Probing Results**, you should see that VPN tunnels are established only on the links with the same Circuit ID.

Procedure to configure the Circuit ID on a Security Gateway that runs Gaia OS

You can configure the Circuit ID in Gaia Portal or Gaia Clish.

Configuration of a Security Gateway in Gaia Portal

1. Connect to Gaia Portal.
2. From the left tree, click **Network Interfaces**.
3. In the section **SD-WAN Interfaces**, select the required interface and click **Edit**.
4. In the section **Advanced Settings**:
5. Select **Override Circuit ID**.
6. Enter a value between 0 and 255.
7. Click **OK**.

Configuration of a Security Gateway in Gaia Clish

For more information, see *"SD-WAN Configuration in Gaia Clish" on page 293*.

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in.
3. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

4. Configure the required Circuit ID:

   ```
   set interface <Name of Interface> sdwan circuit-id <0-255>
   ```

   Example:

   ```
   set interface eth1 sdwan circuit-id 2
   ```

5. Examine the SD-WAN configuration on the interface:

   ```
   show interface <Name of Interface> sdwan
   ```

6. Save the configuration:

   ```
   save config
   ```

Procedure to configure the Circuit ID on a Spark Firewall Appliance that runs Gaia Embedded OS

You can configure the Circuit ID in WebUI or Gaia Clish.

Configuration of a Spark Firewall Appliance in WebUI

See the *R82.00.X Spark Firewall Appliances Centrally Managed Administration Guide* > "*Managing the Device*" > "*Configuring Internet Connectivity*".

1. Connect to the WebUI.
2. From the left tree, click **Device**.
3. In the middle pane, expand the section **Network** and click **Internet**.
4. Click the required Internet connection and click **Edit**.
5. Click the **Advanced** tab.
6. Expand the section **SD-WAN Settings**.
7. Select **Override circuit ID**.
8. Enter a value between 0 and 255.
9. Click **Save**.

Configuration of a Spark Firewall Appliance in Gaia Clish

1. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.

2. If your default shell is the Expert mode, go to Gaia Clish:

```
clish
```

3. Configure two Internet connections - one for each ISP.

   Use this command:

```
set internet-connection "<Name of Connection>" override-
circuit-id true circuit-id <0 - 255>
```

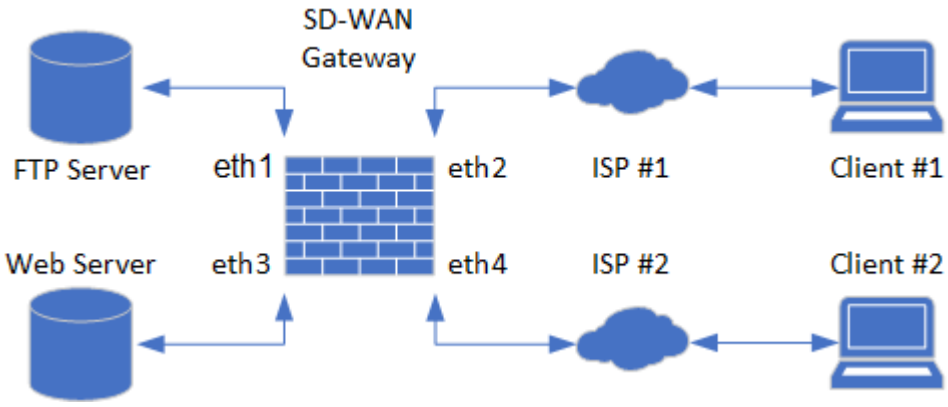
   See the *R82.00.X Spark Firewall Appliances CLI Reference Guide* > "*Configuring the Internet Connections*" > "*Setting Internet Connections*".

   Example:

```
set internet-connection Internet override-circuit-id true
circuit-id 2
```

SD-WAN Symmetric Packet Return

Example SD-WAN Topology



1. An SD-WAN Security Gateway is connected to two ISPs:
   - Interface `eth2` connects to ISP #1.

     The default route on the SD-WAN Security Gateway is through the interface `eth2` (ISP #1).
   - Interface `eth4` connects to ISP #2.
2. Two internal servers connect to the SD-WAN Security Gateway:
   - FTP Server connects to the interface `eth1`.
   - Web Server connects to the interface `eth3`.

Traffic Flow Through an SD-WAN Security Gateway Without Symmetric Packet Return

Note - The **asymmetric** packet return is the default behavior in these Security Gateway versions:

- R81.20 Jumbo Hotfix Accumulator, Take 76 and lower
- R81.20 without the R81.20 Jumbo Hotfix Accumulator
- Spark Firewall from R81.10.05 to R81.10.10

When the SD-WAN Security Gateway uses the Asymmetric Packet Return:

1. A **request** traffic "Client-to-Server" ("C2S") arrives from a Client (through an ISP) to the SD-WAN Security Gateway (in our example, at either interface **eth2** or interface **eth4**).
2. The SD-WAN Security Gateway passes the request traffic (if the Security Policy allows it) to the internal Server (in our example, through either interface **eth1** or interface **eth3**).
3. A **response** traffic "Server-to-Client" ("S2C") from an internal Server arrives at the SD-WAN Security Gateway (in our example, at either interface **eth1** or interface **eth3**).
4. The SD-WAN Security Gateway passes the response traffic (if the Security Policy allows it) to the Next Hop Gateway.

   By default, the SD-WAN Security Gateway always passes the response traffic to the Next Hop Gateway based on the configured default route (in our example, through the interface **eth2**).

   Based on our example:

   - If a request traffic arrived through ISP #1 at the interface **eth2**, then the Security Gateway sends response traffic through the same interface **eth2**.
   - If a request traffic arrived through ISP #2 at the interface **eth4**, then the Security Gateway also sends response traffic through the interface **eth2**.

   As a result, these issue occur:

   - A stateful Firewall at an ISP that did not pass the original request traffic, may drop this response traffic.
   - Traffic distribution through the Security Gateway interfaces is not optimal, because it sends all outbound traffic through the same interface.

   Possible workarounds:

   - Configure Policy Based Routing (PBR) rules based on the internal source IP address for the return (that is the original destination of the inbound traffic).

     See the *Gaia Advanced Routing Administration Guide* for your version.

- Configure the default route in which the next hop gateway is the ISP, from which the inbound traffic arrives and through which the traffic should return.

  For static routes, see the *Gaia Administration Guide* for your version.

  For dynamic routes, see the *Gaia Advanced Routing Administration Guide* for your version.

Traffic Flow Through an SD-WAN Security Gateway With Symmetric Packet Return

Note - The **symmetric** packet return is the default behavior in these Security Gateway versions:

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator Take 14 and higher
- R81.20 Jumbo Hotfix Accumulator Take 79 and higher
- Spark Firewall R81.10.15 and higher

When the SD-WAN Security Gateway uses the Symmetric Packet Return:

1. A **request** traffic "Client-to-Server" ("C2S") arrives from a Client (through an ISP) to the SD-WAN Security Gateway (in our example, at either interface **eth2** or interface **eth4**).
2. The SD-WAN Security Gateway passes the request traffic (if the Security Policy allows it) to the internal Server (in our example, through either interface **eth1** or interface **eth3**).
3. A **response** traffic "Server-to-Client" ("S2C") from an internal Server arrives at the SD-WAN Security Gateway (in our example, at either interface **eth1** or interface **eth3**).
4. The SD-WAN Security Gateway passes the response traffic (if the Security Policy allows it) to the Next Hop Gateway.

   By default, the SD-WAN Security Gateway always passes the response traffic to the Next Hop Gateway of the original ISP that sent the request traffic.

   Based on our example:

   - If a request traffic arrived through ISP #1 at the interface **eth2**, then the Security Gateway sends response traffic through the same interface **eth2**.
   - If a request traffic arrived through ISP #2 at the interface **eth4**, then the Security Gateway sends response traffic through the same interface **eth4**.

Controlling the Symmetric Packet Return for a specific SD-WAN interface:

By default, the SD-WAN Policy enables the Symmetric Packet Return on **all** SD-WAN interfaces (Public and Private) defined in the WAN Link Mapping on supported Security Gateways.

You can disable the Symmetric Packet Return for SD-WAN interfaces in two ways.

Procedure to control the Symmetric Packet Return for a specific SD-WAN interface - from Check Point Portal

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **WAN Link Mapping** (see *"WAN Link Mapping" on page 207*).
5. Edit the applicable interface for the applicable SD-WAN Security Gateway.
6. In the **WAN Link Mapping Rule** window, expand the **Advanced Settings** section at the bottom.
7. Configure the applicable setting:
   - Select **Inbound Symmetric Return** to enable the Symmetric Packet Return for this specific interface.

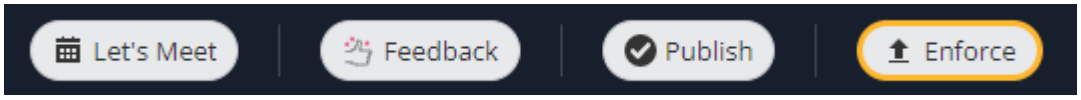
     This is the default.

     Best Practice - Select this option for Public WAN Links.

   - Clear **Inbound Symmetric Return** to disable the Symmetric Packet Return for this specific interface.

     Best Practice - Clear this option for Private WAN Links.
8. Click **OK**.
9. From the top toolbar, click **Publish** to save the changes.
10. From the top toolbar, click **Enforce** to apply the changes.

    The orange frame on this button means there are changes that are not enforced.

    In the popup window that opens, click **Publish & Enforce Policy**.

Procedure to control the Symmetric Packet Return for all SD-WAN interfaces - on the Security Gateway

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- This configuration has higher priority than the settings in Check Point Portal.
- This configuration applies to all SD-WAN interfaces on the Security Gateway.
- This configuration does **not** survive an upgrade to a higher major version.

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in.
3. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

4. Modify the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:
   a. If the file `$FWDIR/conf/sdwan/sdwan_steering_params.json` exists, create a backup copy.

      Otherwise, create this file.

      Run this long command:

      ```
      if [ -f $FWDIR/conf/sdwan/sdwan_steering_params.json ]
      ; then echo "Creating the backup ..." ; cp -v
      $FWDIR/conf/sdwan/sdwan_steering_params.json{,BKP} ;
      else echo "Creating the file ..." ; touch
      $FWDIR/conf/sdwan/sdwan_steering_params.json ; stat
      $FWDIR/conf/sdwan/sdwan_steering_params.json ; fi
      ```

   b. Edit the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

      ```
      vi $FWDIR/conf/sdwan/sdwan_steering_params.json
      ```

c. If this file is empty, then add all these lines.

   If this file already contains other configuration parameters, then add this configuration parameter on a new line:

   - To enable the Symmetric Packet Return for **all** local SD-WAN interfaces:

     ```
     {
         "sdw_default_symmetric_return_value" : true
     }
     ```

   - To disable the Symmetric Packet Return for **all** local SD-WAN interfaces:

     ```
     {
         "sdw_default_symmetric_return_value" : false
     }
     ```

d. Save the changes in the file and exit the editor.

5. Restart the SD-WAN Steering process:

   ```
   sdwan_steering_stop ; sdwan_steering_start
   ```

   Warning - Until the SD-WAN Steering process starts again (in normal circumstances, it takes less than one minute):
   - Existing and new VPN / Overlay connections are interrupted.
   - Existing Local Breakout connections may be interrupted.
   - New Local Breakout connections cannot undergo the SD-WAN Local Breakout routing.

Notes:

- Symmetric Packet Return supports SD-WAN interfaces for ISP lines of type **Private** (for example, MPLS) and of type **Public**.
  Consider disabling this feature on private interfaces if you want dynamic routing to control the return traffic instead of enforcing symmetric return paths.
- Symmetric Packet Return supports inbound traffic to servers behind the Security Gateway that are accessible directly with a Public IP address (without NAT).
- Symmetric Packet Return supports inbound traffic to servers behind the Security Gateway that are accessible with a Private IP address behind NAT - a device in front of the Security Gateway performs this NAT.
- Symmetric Packet Return supports inbound traffic, also when the Security Gateway performs Inbound HTTPS Inspection for that connection.
- Symmetric Packet Return supports inbound traffic to servers behind the Security Gateway that are accessible with a Private IP address behind NAT - the Security Gateway performs this NAT.
  The NAT IP address can be one of these:
  - The IP address of the external Security Gateway interface - configure the required Static NAT rules.
  - An IP address from a NAT Pool that contains IP addresses from a different subnet than the external Security Gateway interface.
    The Next Hop Gateway device will need to route this NAT Pool towards the point-to-point Security Gateway interface.
  - An IP address from a NAT Pool that contains IP addresses from the same subnet as the external Security Gateway interface.
    You must configure:
    - Static NAT rules.
    - Proxy ARP on the Security Gateway:
      - If you configure Manual NAT, then you must follow sk30197 (for Security Gateway) / sk114531 (for Spark Firewall).
      - If you configure Automatic NAT, the Security Gateway performs Proxy ARP automatically.

Limitations in Symmetric Packet Return:

- Symmetric Packet Return does not support inbound traffic sent to the Security Gateway itself (and not through the Security Gateway) - HTTPS, SSH, Remote Access VPN (on roadmap).

  For such inbound requests, the Security Gateway sends its response based on its routing table.

  Possible workaround on the Security Gateway:

  1. Configure the IP Reachability Detection feature.

     See the *Gaia Advanced Routing Administration Guide* for your version > Chapter "IP Reachability Detection".

  2. Select the configured Monitored IP address in the static default route.

     In the route's Gateway, configure such a priority value that:

     a. Users connect first to the Security Gateway through the public IP address of the main ISP (best priority).

     b. If this connection fails, the users connect to the Security Gateway through the public IP address of the another ISP.

     Note - The lower the priority value, the higher the preference.

     See the *Gaia Administration Guide* for your version > Chapter "Network Management" > Section "IPv4 Static Routes".

- Symmetric Packet Return supports inbound traffic only in these cases:
  - The inbound traffic did not match any SD-WAN rule.
  - The inbound traffic matches an SD-WAN rule with the Steering Behavior of type "Overlay" ("Local Breakout" is not supported).
- Symmetric Packet Return does not support traffic that arrives as already encrypted over the Site to Site VPN tunnel.

SD-WAN and Route-Based VPN

For information about Route-Based VPN and VPN Tunnel Interfaces (VTI), see the *Site to Site VPN Administration Guide* for your version > Chapter "*Route-Based VPN*".

SD-WAN Rules and VTI Routing

The routes on the Security Gateway control whether to encrypt traffic or not, and to what VPN peer:

A route on the Security Gateway can be one of these:

- Static route
- Dynamic route
- Policy-Based route (PBR)
- SD-WAN "Local Breakout"

If the traffic is routed through a VTI, then the Security Gateway encrypts the packet.

If the traffic is routed through a non-VTI interface, then the Security Gateway does not encrypt the packet (sends it as clear text), unless Domain-Based VPN decides otherwise.

For encrypted packets, SD-WAN "Overlay" selects the best path (VPN Transport / VPN Tunnel) to reach the pre-selected VPN peer:

For a connection that was not encrypted, SD-WAN "Overlay" does not affect the traffic (if matched).

In case of ECMP (Equal-Cost Multi-Path) routes configured towards two or more VTIs (VPN Peers):

1. The Security Gateway decides on the VTI (VPN Peer) based on the Operating System routes.
2. SD-WAN "Overlay" selects the best path to reach the selected VPN peer.

Roadmap - Support for SD-WAN "Overlay" to select the best VPN Peer based on SLA is on the roadmap.

SD-WAN Policy Considerations for Route-Based VPN

With dynamic routing, networks that send traffic that should be encrypted, can change frequently.

- Make sure to include all your overlay networks in the "Overlay" rules:
  - When only Private networks (as described in RFC 1918) are used for overlay network, you can use the Zone object **My VPN Domain & Peer VPN Domain**.
  - If you have subnets with Public IP addresses in your overlay network, make sure to include them in your "Overlay" rules.
  - Make sure to also include all IP addresses of the Security Gateway VTIs in your "Overlay" rules to get resiliency for BGP peering with the VPN peers.

  Roadmap - Including all networks learned through VTIs with the Dynamic Objects "**My VPN Domain**" and "**Peer VPN Domain**" is on the roadmap. For more information about these Dynamic Objects, see *"Dynamic Objects in SD-WAN Policy" on page 163*.

- Avoid matching traffic that should be encrypted with SD-WAN "Local Breakout" rules:

  Such traffic will be sent to the ISP in clear text, ignoring the Operating System routes to VTI.

  Note - "Local Breakout" routes take precedence over Static routes / Dynamic routes.

  Roadmap - Excluding all networks learned through VTIs (or other next hops during the operating system routing) with the Dynamic Object "**SD-WAN Internet**" is on the roadmap. For more information about these Dynamic Objects, see *"Dynamic Objects in SD-WAN Policy" on page 163*.

SD-WAN "Backhaul" and Route-Based VPN

For information about the SD-WAN Routing Preference "Backhaul Only", see *"Routing Preference "Backhaul Only"" on page 191*.

In SmartConsole, in the applicable Star VPN Community object > on the **VPN Routing** page, do **not** select the option "**To center or through the center to other satellites, to Internet and other VPN targets**". This option overrides all the operating system routing decisions (whether to VTI or not) and it tries to encrypt all traffic to the Center Gateway. Therefore, this option cannot be used with Route-Based VPN.

If you use a Star VPN Community, then on the Satellite SD-WAN Security Gateways, configure the default route to the Center Gateway VTI.

You can use a Static default route or a Dynamic default route to the Center Gateway VTI.

- If the default route to the Center Gateway VTI is a Dynamic route (while the default route for each ISP is a Static route):
  - The SD-WAN "Backhaul" mechanism would act as a backup only (by default).

    You can use it with the SD-WAN Routing Preference "Prioritize Local Breakout" (see *"Routing Preference "Prioritize Local Breakout"" on page 195*), because static routes have a lower Administrative Distance (AD=1) than dynamic routing protocols.

    The lower the Administrative Distance, the higher the routing preference.
  - You can configure a routemap (see the *Gaia Advanced Routing Administration Guide* for your version) if it is necessary to change the Administrative Distance of the specific Dynamic "VTI Default" route" to be lower than the Administrative Distance of Static routes.
- If the default route to the Center Gateway VTI is a Static route:
  - You can configure this operating system static route with the highest preference (active / kernel route) by configuring it with the lowest priority.

    You can use such a static route with the SD-WAN Routing Preference "Backhaul Only" or with the SD-WAN Routing Preference "Prioritize Local Breakout".

    If you use the SD-WAN Routing Preference "Prioritize Local Breakout", then it will override the operating system VTI route, as long as ISP Links are in the "Up" state.

- You can configure this operating system static route with the lowest preference by configuring it with the highest priority.

  This configures a backup mechanism at the operating system level (if ISP Links are in the "Down" state, the traffic should be encrypted over the Private link (such as MPLS)).

  You can use such a static route only with the SD-WAN Routing Preference "Prioritize Local Breakout".

Considerations when the active default route is configured to the Center Gateway VTI

1. The Security Gateway will not be reachable from the Internet, or from outside the Site to Site VPN tunnel.

   Roadmap - Support for connections to the Security Gateway itself in the Symmetric Packet Return feature is on the roadmap. See *"SD-WAN Symmetric Packet Return" on page 257*.

2. In the SD-WAN Policy, avoid matching the Steering Behavior of "Local Breakout Only" or "Prioritize Local Breakout" to traffic that the Security Gateway initiates while the active default route is set towards VTI.

   Roadmap - Support for local connections (initiated by the Security Gateway) is on the roadmap.

3. Configure the operating system-level probing for this default route to make sure that it is active only when the VPN tunnel is "Up" and there is a connectivity through the VPN tunnel.

   Configuring such a route without probing can leave the Security Gateway without Internet.

   As a result, the Security Gateway will not get SD-WAN Policy, and will not be able to fetch CRL from its Management Server (if connection to the Management Server goes over the Internet).

4. Consider using Policy Based Routing (PBR) to match this default route only for local networks, to avoid affecting the Security Gateway itself.

   On a Security Gateway that runs the Gaia operating system, you can override a PBR rule priority higher than 100 with a "Local Breakout" rule in the SD-WAN Policy.

   Roadmap - Support for an override of a PBR rule priority higher than 100 with a "Local Breakout" rule in the SD-WAN Policy on a Spark Firewall Appliance is on the roadmap.

5. On a DAIP Security Gateway (see *"SD-WAN Configuration for DAIP Security Gateways" on page 220*), when the default route is assigned by a DHCP server on one of the ISP interfaces:

   - On a Security Gateway that runs the Gaia operating system, it is **not** supported to configure a manual default route (through a VTI) to have a higher precedence than the kernel route (see sk151632).
   - On a Spark Firewall Appliance, you can configure a lower route priority through the Internet connection, such that the manual route will take precedence.

SD-WAN NAT for ISP

Introduction to NAT for each ISP

In SD-WAN Policy you can configure different NAT IP addresses for each ISP.

As a result, the selected Security Gateways apply NAT to their connections based on the corresponding ISP (WAN Link).

Other Security Gateways apply NAT to their connections based on the configuration in SmartConsole.

Note - SD-WAN Policy determines the applicable WAN Link, and then applies the configured NAT.

Supported Security Gateways

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator, Take 14 and higher (PRJ-56952)
- R81.20 Jumbo Hotfix Accumulator, Take 89 and higher (PRJ-56616)
- Spark Firewall R81.10.15, R82.00.00

Configuring NAT for each ISP

Part 1 - Configuring NAT Mapping

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.
5. In the applicable SD-WAN Policy rules, examine the **Source** column to calculate the number of source IP addresses in this column.

   You use this number later in the configuration of the NAT Mapping.
6. From the top toolbar, click **Manage Objects**.
7. From the top toolbar, click ✳ (**New**) > click **NAT**.
8. In the **Name** field, enter a descriptive name that represents this NAT Mapping.
9. **Optional:** In the **Comment** field, enter an applicable text that describes this NAT Mapping.

This comment is very useful when you select this object later in the SD-WAN Policy.

10. In the **NAT Method** section, select the applicable option - **Hide** or **Static** (you configure the NAT IP address later).

    Description of Hide NAT:

    - Provides a many-to-one mapping for IP addresses.
    - Performs source port translation.
    - Typically used for internal subnets or multiple hosts that need to share a single public IP address.
    - Designed to "hide" internal IP addresses behind one external IP address.

    Description of Static NAT:

    - Provides a one-to-one mapping for IP addresses.
    - Preserves the original source port (no port translation).
    - Typically used for servers or hosts that require a dedicated public IP address.
    - Suitable when consistent IP identity is required.

11. From the toolbar, click + (**Add**).

12. In the **NAT Gateway Configuration** window:
    a. In the **Gateway** field, select the applicable Security Gateway.
    b. For **each** WAN Link, configure the required NAT behavior:
        - **According to SmartConsole**

          This WAN Link applies NAT to its connections based on the configuration in SmartConsole.
        - **Hide Behind IP Address**

          This option appears only if in the **NAT Method** section, you selected **Hide**.

          This WAN Link applies Hide NAT to its connections based on the selected value in the **NAT Method** section.

          Enter the required IP address, or range of IP addresses.

          Important - For a range of IP addresses, you must configure the same number of IP addresses as configured in the **Source** column of the applicable SD-WAN Policy rules, in which you will select this NAT Mapping.
        - **Hide Behind Gateway**

          This option appears only if in the **NAT Method** section, you selected **Hide**.

          This WAN Link applies Hide NAT to its connections based on the selected value in the **NAT Method** section.

          The Security Gateway performs Hide NAT using the IP address of the corresponding WAN Link.
        - **Translated IP Address**

          This option appears only if in the **NAT Method** section, you selected **Static**.

          This WAN Link applies Static NAT to its connections based on the selected value in the **NAT Method** section.

          Enter the required IP address, or range of IP addresses.

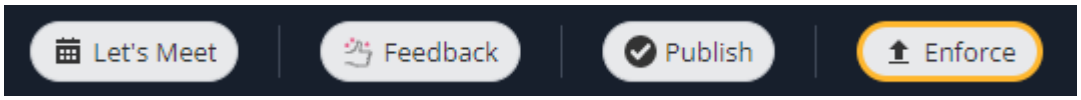
          Important - For a range of IP addresses, you must configure the same number of IP addresses as configured in the **Source** column of the applicable SD-WAN Policy rules, in which you will select this NAT Mapping.
    c. Click **OK**.
13. Close the **Manage Objects** panel.

Part 2 - Configuring SD-WAN Policy

1. Create a new rule, or edit an existing rule (see *"Configuring SD-WAN Policy" on page 160*).
2. In the **Translated Source (NAT)** column of the rule, click the **(+)** icon > click the required NAT Mapping object > click **OK**.

   Notes:
   - You can select only one NAT Mapping object in a rule.
   - The SD-WAN rule base evaluates traffic based on the direction defined in the matching criteria.
     Therefore, it matches outbound traffic only as the rules are built for outbound direction.
   - Unlike Automatic NAT rules in SmartConsole, SD-WAN rules do not automatically create reverse-direction handling.
     Therefore, you still need to configure inbound NAT rules in SmartConsole.
3. Click **OK**.
4. From the top toolbar, click **Publish** to save the changes.
5. From the top toolbar, click **Enforce** to apply the changes.

   The orange frame on this button means there are changes that are not enforced.

   In the popup window that opens, click **Publish & Enforce Policy**.

SD-WAN DSCP

Introduction to DSCP

Differentiated Services (DiffServ) specify a mechanism for classifying and managing network traffic, by assigning different classes to different traffic types, to prioritize specific traffic over another.

DiffServ uses a 6-bit Differentiated Services Code Point (DSCP) in the 6-bit differentiated services field ("DS" field) in the IP header for packet classification purposes. The "DS" field, together with the "ECN" field, replaces the outdated IPv4 "TOS" field.

SD-WAN has the ability to match such traffic based on the DSCP value, and apply the desired steering behavior.

Supported Security Gateways

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator, Take 14 and higher (PRJ-56952)
- R81.20 Jumbo Hotfix Accumulator, Take 89 and higher (PRJ-56616)
- Spark Firewall - planned

DSCP Classes

At this time, SD-WAN provides only predefined DSCP Classes:

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.
5. From the top toolbar, click **Manage Objects**.
6. Expand the folder **Check Point DSCP Service Classes**.
7. To see the configuration of each predefined DSCP class, click its object.
8. Close the **DSCP Service Class** panel.
9. Close the **Manage Objects** panel.

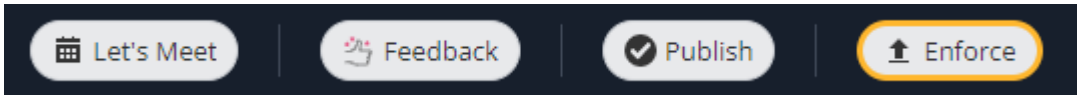
DSCP Configuration

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.

3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.
5. Create a new rule, or edit an existing rule (see *"Configuring SD-WAN Policy" on page 160*).
6. In the **Services & Applications** column of the rule, click the **(+)** icon > click **DSCP Service Classes** > select the applicable DSCP Service Class objects > click **OK**.

   Important - It is **not** supported to select DSCP classes and Application / Service objects in the same rule.
7. Click **OK**.
8. From the top toolbar, click **Publish** to save the changes.
9. From the top toolbar, click **Enforce** to apply the changes.

   The orange frame on this button means there are changes that are not enforced.

   In the popup window that opens, click **Publish & Enforce Policy**.

SLA-Based Prioritize Local Breakout in SD-WAN

For more information, see *"Routing Preference "Prioritize Local Breakout"" on page 195*.

Procedure for a Security Gateway that runs Gaia OS

When you configure the Steering Behavior to use the type "**Internet**" with the Routing Preference "**Prioritize Local Breakout**":

1. The Security Gateway uses direct WAN Links to connect to the Internet.
2. If the **Criteria** parameters (even if one of them) exceed the configured thresholds in the applicable Steering Behavior in all direct WAN Links to the Internet, the Security Gateway uses the WAN Link with encrypted traffic to the Headquarters to connect to the Internet (the "Backhaul" behavior).

You can change the Security Gateway behavior to fail over to the "Backhaul" behavior when all direct WAN Links to the Internet are down (because a link is down, or the probing next hop is down):

1. From the left navigation panel, click **Network**.
2. In the middle section, click **Profiles**.
3. Click the applicable SD-WAN profile.
4. Click the **Advanced** tab.
5. Click the left cell **key** and enter this parameter:

   ```
   sdw_bhl_prefer_brk
   ```

6. Click the right cell **value**, enter digit "0", and **press the Enter key**:

   ```
   0
   ```

   The row with the configured parameter must appear below the default empty row "`key - value`".
7. At the top, click **Publish**.
8. At the top, click **Enforce**.

Important:

- This parameter applies to all Security Gateways that use this SD-WAN Profile.
  If this behavior change is required only for some Security Gateways:
  1. Create a **new** SD-WAN Profile.
  2. Add only the applicable Security Gateways to this new profile.
  3. Configure the parameter "`sdw_bhl_prefer_brk`" in this new profile.
  4. Edit the SD-WAN Profile that contains Security Gateways, whose failover behavior must **not** change.
  5. Remove the applicable Security Gateways, for which you created a new SD-WAN Profile.
  6. At the top, click **Publish**.
  7. At the top, click **Enforce**.
- If the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file on a Security Gateway contains this parameter "`sdw_bhl_prefer_brk`", then the value of this parameter in this file takes precedence over the value of this parameter that you configured in an SD-WAN Profile.
  If you edit this file, then you must restart the SD-WAN Steering process on the Security Gateway:
  ```
  sdwan_steering_stop ; sdwan_steering_start
  ```
- To restore the default Security Gateway behavior (fail over based on the **Criteria** parameters), delete the key "`sdw_bhl_prefer_brk`" in the applicable SD-WAN profile, click **Publish**, and click **Enforce**.

Procedure for a Spark Firewall Appliance that runs Gaia Embedded OS

Important - In a Cluster, you must configure all the Cluster Members in the same way.

When you configure the Steering Behavior to use the type "**Internet**" with the Routing Preference "**Prioritize Local Breakout**":

1. The Security Gateway uses direct WAN Links to connect to the Internet.
2. If all direct WAN Links to the Internet are down (because a link is down, or the probing next hop is down), the Security Gateway uses the WAN Link with encrypted traffic to the Headquarters to connect to the Internet (the "Backhaul" behavior).

You can change the Security Gateway behavior to fail over to the "Backhaul" behavior if the **Criteria** parameters (even if one of them) exceed the configured thresholds in the applicable Steering Behavior in all direct WAN Links to the Internet:

1. Connect to the command line on the Spark Firewall Appliance / each Spark Firewall Cluster Member.
2. Log in.

3. If your default shell is Gaia Clish, then go to the Expert mode:

```
expert
```

4. Modify the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

   a. If the file `$FWDIR/conf/sdwan/sdwan_steering_params.json` exists, create a backup copy.

   Otherwise, create this file.

   Run this long command:

```
if [ -f $FWDIR/conf/sdwan/sdwan_steering_params.json ]
; then echo "Creating the backup ..." ; cp -v
$FWDIR/conf/sdwan/sdwan_steering_params.json{,BKP} ;
else echo "Creating the file ..." ; touch
$FWDIR/conf/sdwan/sdwan_steering_params.json ; stat
$FWDIR/conf/sdwan/sdwan_steering_params.json ; fi
```

   b. Edit the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

```
vi $FWDIR/conf/sdwan/sdwan_steering_params.json
```

   c. If this file is empty, then add all these lines.

   If this file already contains other configuration parameters, then add this configuration parameter on a new line:

```
{
    "sdw_bhl_prefer_brk" : 1
}
```

   Note - To restore the default Security Gateway behavior (fail over if all direct WAN Links to the Internet are down), remove this parameter from the configuration file.

   d. Save the changes in the file and exit the editor.

5. Restart the SD-WAN Steering process:

```
sdwan_steering_stop ; sdwan_steering_start
```

Warning - Until the SD-WAN Steering process starts again (in normal circumstances, it takes less than one minute):

- Existing and new VPN / Overlay connections are interrupted.
- Existing Local Breakout connections may be interrupted.
- New Local Breakout connections cannot undergo the SD-WAN Local Breakout routing.

SD-WAN in Layer 2

This feature adds support for Overlay tunnels over Layer 2 between SD-WAN Security Gateways that are connected to the same subnet. For example, over an MPLS line.

Configuration

Step 1 - Configure the Next Hop

You can configure the required settings in Gaia Portal or in Gaia Clish:

In Gaia Portal

1. With a web browser, connect to Gaia Portal on the Security Gateway / each Cluster Member.
2. Navigate to **Network Management** > **Network Interfaces**.
3. Double-click the relevant interface.
4. Click the **SD-WAN** tab.
5. Select **Use as SD-WAN interface**.
6. In the section **Next Hop**, select the applicable option based on how the peers of this specific interface are connected:
   - If all SD-WAN peers are connected over Layer 2:

     Select **No Next Hop (Layer-2 Only Interface)**.

     Note - The option **Accessible via NAT** becomes disabled.

   - If some SD-WAN peers are connected over Layer 3 and some SD-WAN peers are connected over Layer 2:

     Select **Use the following Next Hop IP address** and enter the relevant IP Address for the ISP, to which this interface connects.

     Note - Based on the destination IP address, this SD-WAN Security Gateway automatically detects how to use the configured Next Hop:
     - If the destination IP address does not belong to the same subnet as the IP address of this interface, then the Security Gateway forwards the Overlay traffic to the configured Layer 3 Next Hop.
     - If the destination IP address belongs to the same subnet as the IP address of this interface, then the Security Gateway forwards the Overlay traffic to the relevant Layer 2 peer.

- If all SD-WAN peers are connected over Layer 3:

  Select **Use the following Next Hop IP address** and enter the relevant IP Address for the ISP, to which this interface connects.

7. Click **OK**.

In Gaia Clish

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in.
3. If your default shell is the Expert mode, go to Gaia Clish:

   ```
   clish
   ```

4. For the applicable interface, configure the applicable next hop based on how the peers of this specific interface are connected:

   - If all SD-WAN peers are connected over Layer 2:

     ```
     set interface <Name of Interface> sdwan next-hop l2-only
     ```

   - If some SD-WAN peers are connected over Layer 3 and some SD-WAN peers are connected over Layer 2:

     ```
     set interface <Name of Interface> sdwan next-hop <IP Address of ISP Next Hop>
     ```

     Note - Based on the destination IP address, this SD-WAN Security Gateway automatically detects how to use the configured Next Hop:
     - If the destination IP address does not belong to the same subnet as the IP address of this interface, then the Security Gateway forwards the Overlay traffic to the configured Layer 3 Next Hop.
     - If the destination IP address belongs to the same subnet as the IP address of this interface, then the Security Gateway forwards the Overlay traffic to the relevant Layer 2 peer.

   - If all SD-WAN peers are connected over Layer 3:

     ```
     set interface <Name of Interface> sdwan next-hop <IP Address of ISP Next Hop>
     ```

5. Save the configuration:

   ```
   save config
   ```

Step 2 - Configure Circuit ID Values

Procedure

For information, see *"SD-WAN Circuit ID" on page 248*.

By default:

- The Circuit ID for a Public link is "0".
- The Circuit ID for a Private link is "1".

Follow these guidelines to configure Circuit ID values:

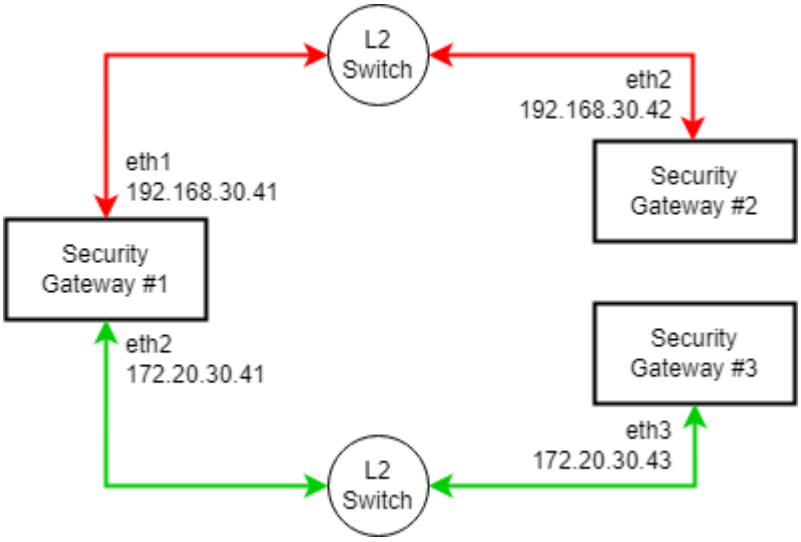
Use Case 1 - Security Gateway has multiple links only with Layer 2 peers

When a Security Gateway has multiple Layer 2 links, you **must** override the default Circuit ID value and configure **unique** Circuit ID for each Layer 2 link.

Note - This does not apply to the Circuit ID 0, which is reserved as the default for Public links.

If you do not change the default Circuit ID values, different Layer 2 links will share the same Circuit ID value and will not differentiate between peer Security Gateways on different subnets when they create Overlay tunnels. Assigning distinct Circuit ID values ensures that Overlay tunnels are established only within the appropriate subnets.

Example diagram:



These pairs of interfaces must have **unique** Circuit ID value for the Overlay tunnels:

- Between the interface `eth1` on the Security Gateway #1 (192.168.30.41) and the interface `eth2` on the Security Gateway #2 (192.168.30.42).
- Between the interface `eth2` on the Security Gateway #1 (172.20.30.41) and the interface `eth3` on the Security Gateway #3 (172.20.30.43).

By default, all these "Private" interfaces have the same Circuit ID value. As a result, they will try to establish Overlay tunnels with each other, although only specific pairs of interfaces should do this.

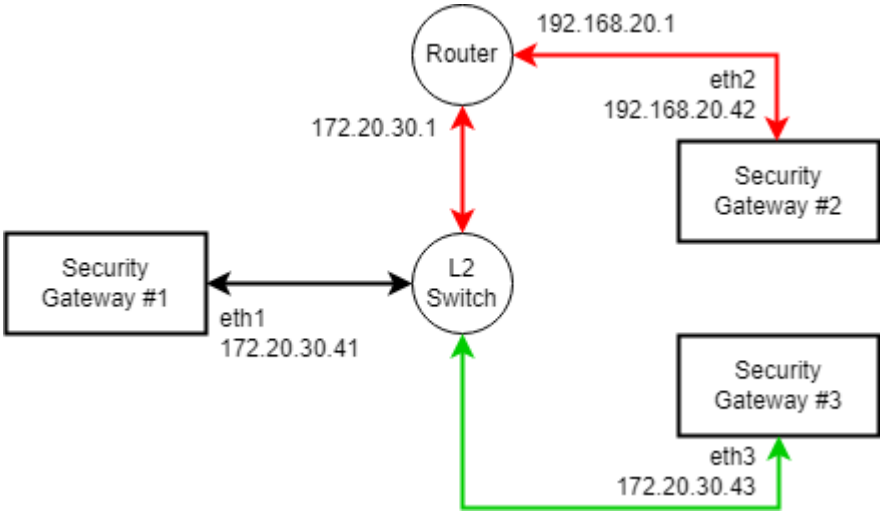
Use Case 2 - Security Gateway has Layer 3 peers and Layer 2 peers on the same interface

When the same interface on a Security Gateway connects both to Layer 3 peers (Public links) and to Layer 2 peers (Private links), there may be cases when it is necessary to override the default Circuit ID value and configure the **same** Circuit ID value on all relevant interfaces.

This ensures that the links can establish the necessary Overlay tunnels for both Layer 3 and Layer 2 communication.

If the Circuit ID values differ ("0" for Public links and "1" for Private links), the interfaces will be treated as separate circuits and will not be able to establish all the required Overlay tunnels with each other.

Example diagram:



These pairs of interfaces must have the **same** Circuit ID value for Overlay tunnels:

- Layer 3:

  Between the interface `eth1` on the Security Gateway #1 (172.20.30.41), through a Router, and the interface `eth2` on the Security Gateway #2 (192.168.20.42).

- Layer 2:

  Between the interface `eth1` on the Security Gateway #1 (172.20.30.41), through a Switch, and the interface `eth3` on the Security Gateway #3 (172.20.30.43).

By default, the Layer 3 ("Public") interfaces and the Layer 2 ("Private") interfaces have different Circuit ID values. As a result, the interface `eth1` on the Security Gateway #1 (172.20.30.41) will establish Overlay tunnels only with one type peers, although it should do this with both types of peers.

Step 3 - Configure WAN Link Mapping (only for Layer 2 peers)

Procedure

For information, see *"WAN Link Mapping" on page 207*.

If all SD-WAN peers of a specific interface are connected over Layer 2, you must configure the WAN Link Mapping as follows:

1. In the **Manage WAN Links** panel, create a new link of type **Private** and configure it.
2. On the **WAN Link Mapping** page, go to the row for the Security Gateway / Cluster.
3. In the column "**<Name of Private WAN Link>**", click **(+)**.
4. In the section **Interface Mapping**, select the applicable interface to which all SD-WAN peers are connected over Layer 2.

CPView output

If both Layer 3 and Layer 2 are used on the Security Gateway, then the CPView tool:

- On the **Advanced** > **SDWAN** > **Probing** page, in the **Nexthop Probing Results** section, shows the results only for Layer 3 (does not show the results for Layer 2).
- On the **Advanced** > **SDWAN** > **Probing** page, in the **Overlay Probing Results** section, shows the information for both Layer 3 and Layer 2.

SD-WAN Overlay ECMP and Symmetric Overlay Return

Equal-Cost Multi-Path (ECMP) Routing for SD-WAN Overlay

Overview

ECMP routing enables distribution of traffic across multiple SD-WAN peers that have equal routing cost.

In SD-WAN Overlay, ECMP enhances path selection by applying SLA-based steering logic, instead of relying on standard OS-based random distribution.

Configuration

Kernel Parameter

See sk26202 for instructions to configure kernel parameter values.

- Name:

  `sdw_ecmp_lb_enabled`

- Values:
  - `1` = enabled (this is the default)
  - `0` = disabled

Behavior when enabled

Connections are distributed across available SD-WAN peers using a round-robin method.

Behavior when disabled

Connections are consistently sent through a single selected peer, without load balancing.

SD-WAN ECMP Behavior

Peer Selection

- SD-WAN selects peers based on the Thresholds configured in an Overlay Steering object.
- Only peers that meet thresholds are preferred.

Selection Logic

- If multiple peers meet thresholds, connections are distributed using round-robin.
- If no peers meet thresholds but peers are "UP", one available peer is selected (fallback behavior).
- If no SD-WAN peers are available, routing falls back to the operating system.

Routing Behavior

Overlay Traffic (traffic matched by Overlay steering rules)

- If a route to an SD-WAN peer VTIs (OVI route) exists, then this route is always preferred.
- If no such route exists, then routing falls back to the operating system.

Backhaul Traffic (traffic matched by Internet steering object set to Backhaul)

- If a route to SD-WAN peer VTIs exists, then it is always preferred.
- If no SD-WAN VTI route exists:
  - If a route to non-SD-WAN VTI is active in the kernel, the it is used by the OS.
  - Otherwise, the Local Breakout is performed.

Limitations

- Maximum of 10 ECMP next-hop peers.
- ECMP applies only to SD-WAN overlay traffic.
- Load balancing is per connection (not per packet).
- SD-WAN ECMP logic does not apply to local connections (traffic initiated by the Security Gateway itself).

Symmetric Return for Overlay Connections

Overview

Symmetric Return ensures that response traffic is sent through the same SD-WAN peer from which the original encrypted connection was received.

This behavior maintains path symmetry and prevents out-of-state packet drops.

This feature is independent of ECMP load balancing and is introduced as part of the ECMP capabilities.

Configuration

Kernel Parameter

See sk26202 for instructions to configure kernel parameter values.

- Name:

  `sdw_ovi_symret_enabled`

- Values:
  - `1` = enabled (this is the default)
  - `0` = disabled

Behavior when enabled

Return traffic (server-to-client) always exits through the original ingress SD-WAN peer to ensure path symmetry.

Behavior when disabled

Return traffic is routed based on standard OS routing decisions. May result in asymmetric paths.

Example Topology

Spoke1 -> Hub1 / Hub2 -> Spoke2

Flow of Client-to-Server traffic

Traffic originating from Spoke1 reaches Spoke2 via Hub2.

Flow of return traffic

- If Symmetric Return is enabled:

  Spoke2 sends the response back through Hub2, which is the original ingress peer.

- If Symmetric Return is disabled:

  Spoke2 determines the return path based on:

  - The local OS routing table.
  - ECMP decisions.

  As a result, return traffic may be sent via Hub1, leading to asymmetric routing.

Important Notes:
Symmetric Return applies even if:

- No explicit route exists for the remote spoke network.
- The system still returns traffic via the original ingress peer.

Scope

Applies only to:

- SD-WAN Overlay traffic.
- SD-WAN Peers with VTI enabled.

SD-WAN Steering Enforcement when Selected Links are Down

Overview

By default, when all WAN link candidates defined in a steering object (used in an SD-WAN rule) have their physical link down, the Security Gateway defers the routing decision to the operating system routing table.

This behavior allows traffic to continue flowing through alternative routes, even if they are not part of the defined SD-WAN policy.

Note - This feature applies to Local Breakout traffic only. It does not apply to SD-WAN Overlay (VPN) traffic.

Behavior

Behavior when this feature is disabled (default)

1. Traffic matches an SD-WAN rule.
2. All WAN Link candidates in the steering object have their physical link down.
3. The Security Gateway defers the routing decision to the operating system.
4. Traffic may be forwarded through other available interfaces.

Behavior when this feature is enabled

1. Traffic matches an SD-WAN rule.
2. All WAN Link candidates in the steering object have their physical link down.
3. The Security Gateway enforces the steering decision.
4. No fallback to operating system routing occurs.
5. Traffic is not forwarded if no WAN Link candidates are available.

Example

A steering object is configured with a single WAN Link (for example, "WAN1") and is used in an SD-WAN rule.

1. Traffic matching this SD-WAN rule must be routed through "WAN1".
2. The physical interface associated with "WAN1" goes down.

This is the Security Gateway's behavior:

- Behavior when this feature is disabled (default)
  - The Security Gateway defers the routing decision to the operating system.
  - Traffic may be routed through a different available WAN Link.
- Behavior when this feature is enabled
  - The Security Gateway attempts to forward traffic according to the SD-WAN steering decision (via "WAN1").
  - Because the physical link is down, the traffic is not forwarded.
  - No fallback to other WAN Links occurs.

Logging

- The SD-WAN log reflects the steering decision based on the configured SD-WAN rule.
- When the feature is enabled, the logged steering decision corresponds to the actual forwarding behavior.
- When the feature is disabled, logs may show the WAN Link candidates from the steering object, even if traffic is ultimately routed via the operating system.

Configuration

This feature is controlled by an advanced SD-WAN steering parameter:

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **Profiles**
5. Select the relevant SD-WAN Profile and click **Edit**.
6. Click the **Advanced** tab.
7. In **Advanced Settings**, configure the following:

a. **Key**:

```
sdw_add_blackhole_isp_route
```

b. **Value**:

```
true
```

8. Save the changes.
9. In SmartConsole, install the Access Control policy on the relevant Security Gateways.

Note - If the parameter is explicitly defined on the Security Gateway in the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file, then the local configuration takes precedence and is not overridden by the **Advanced Settings** in the SD-WAN profile.

Use Case

Use this feature when strict adherence to SD-WAN steering policy is required, and traffic must not be forwarded through unintended WAN Links under any condition.

SD-WAN Configuration in Gaia Clish

This section describes the Gaia Clish commands for configuring SD-WAN interfaces on the Security Gateway / each Cluster Member that run the Gaia OS.

For Spark Firewall Appliances that run the Gaia Embedded OS, see the *R82.00.X Spark Firewall Appliances CLI Reference Guide*.

The "add" command

This command configures the specified value on a new SD-WAN interface.

```
add interface <Name of Interface> sdwan next-hop <IP Address>
      circuit-id <1 - 255>
      download-speed <1 - 1000000>
      is_mpls {true | false}
      nat <IP Address after NAT>
      tag <Tag Name>
      upload-speed <1 - 1000000>
```

The "set" command

This command configures the specified value on an existing SD-WAN interface.

```
set interface <Name of Interface> sdwan
      circuit-id <1 - 255>
      download-speed <1 - 1000000>
      is_mpls {true | false}
      nat <IP Address after NAT>
      next-hop <IP Address>
      tag <Tag Name>
      upload-speed <1 - 1000000>
```

The "delete" command

This command removes the configured value.

```
delete interface <Name of Interface> sdwan
      circuit-id
      download-speed
      is_mpls
      nat
      tag
      upload-speed
```

The "show" command

This command shows the configured value.

```
show interface <Name of Interface> sdwan
      circuit-id
      download-speed
      is_mpls
      link-type
      nat
      next-hop
      tag
      upload-speed
```

Parameters for Gaia Clish Commands

Parameter	Description
`circuit-id`	**Optional:** Specifies the Circuit ID. See *"SD-WAN Circuit ID" on page 248*. **Note** - This parameter is available only in these Security Gateway versions: ■ R82 and higher ■ R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464)
`download-speed`	**Optional:** Specifies the download speed limit (in Mbps). See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**. **Note** - This parameter is available only in these Security Gateway versions: ■ R82 and higher ■ R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464)
`is_mpls`	Specifies that this interface connects to a Private Link (for example, MPLS) **Note** - This parameter is available only in these Security Gateway versions: ■ R81.20 Jumbo Hotfix Accumulator, Take 76 and lower. ■ R81.20 without the Jumbo Hotfix Accumulator.
`link-type`	Shows the WAN Link type. See *"WAN Link Mapping" on page 207*. **Note** - This parameter is available only in these Security Gateway versions: ■ R82 and higher ■ R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464)

Parameter	Description
`nat`	Specifies that an external device or an ISP applies NAT on the source IP address of all traffic from this interface. In the "`add`" and "`set`" commands, enter the applicable IP address after this external NAT, as the peers receive it. **Notes:** ■ In Gaia Portal, this corresponds to the option "**Accessible via NAT**". ■ You do not need to configure NAT rules in SmartConsole.
`next-hop`	Specifies the next hop IP Address for the ISP, to which this interface connects
`tag`	**Optional:** Specifies the interface tag. See the description and the example in *"WAN Link Mapping" on page 38*.
`upload-speed`	**Optional:** Specifies the download speed limit (in Mbps). See *"Configuring Steering Behavior" on page 171* > **Criteria** > **WAN Link Utilization** > **Link Aggregation** > **Selection Method**. **Note** - This parameter is available only in these Security Gateway versions: ■ R82 and higher ■ R81.20 Jumbo Hotfix Accumulator, Take 79 and higher (PRJ-53464)

SD-WAN Settings Profile

Overview

The SD-WAN Settings Profile provides a centralized way to define SD-WAN steering settings and related parameters and apply them to selected Security Gateway. The profile allows administrators to group gateways and control how SD-WAN behavior is applied on those gateways using a single configuration entity.

Configuration

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **Profiles**.
5. Click **Set New Profile** > **SD-WAN Settings Profile**

6. On the tab **General:**
    a. In the section **Basic**:
        i. In the field **Name**, enter the desired name for this profile.
    b. In the section **SD-WAN Gateways**:
        i. Click **[+]**.
        ii. Select the required Security Gateways.
7. On the tab **Overlay Probing** configure the desired probing settings for Overlay VPN tunnels:
    a. **Passive overlay probing**

        Passive overlay probing monitors VPN tunnel health by using actual traffic instead of frequent active probes, reducing CPU and bandwidth usage. It measures packet loss based on ESP sequence numbers and activates only when there is enough traffic to provide reliable data. If traffic stops or packet loss exceeds a threshold, the system immediately switches to active probing at a normal rate. Steering decisions always rely on active probing results, while passive probing operates in the background to optimize resource usage.
    b. **On-demand overlay probing**

        On-demand overlay probing reduces resource usage by sending probes only when traffic is present on a VPN tunnel. When traffic flows, the system sends active probes to measure transport health and make steering decisions. If traffic stops, probing is paused to conserve bandwidth and CPU, while tunnels remain established for quick reconnection. This approach optimizes performance in large SD-WAN mesh networks without compromising tunnel availability.
8. On the tab **Advanced**:

    You can configure the applicable parameters that change the default Security Gateway behavior.

    Check Point Support provides these parameters when applicable.

    a. Click the left cell key and enter the parameter name.
    b. Click the right cell value, enter the required value, and press the Enter key (or click the [+] icon).

        Notes:
        - To edit the key-value pair, hover over it, click the edit icon, make the required change, and click the apply icon.
        - To delete the key-value pair, hover over it and click the delete icon.

SD-WAN GraphQL API

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Support**.
4. In the middle section, click **API**.
5. In the left pane, enter the API call code you wish to run.
6. From the top toolbar, click the **Play** button (or press the CTRL+Enter keys) to run the API call.
7. The middle pane shows the API response.

Notes:

- The right pane contains the GraphQL documentation of all available functions.
- If you run an API call that changes the configuration, you must save the changes manually in one of these ways:
  - Click the **Publish** button in Check Point Portal
  - Run the API call "**publishChanges**".

Upgrading an SD-WAN Security Gateway

This section applies to:

- Local upgrade with CPUSE on a Security Gateway / Cluster Member.
- Central installation from SmartConsole onto a Security Gateway / Cluster object.
- Central installation with the Central Deployment Tool (sk111158) onto a Security Gateway / Cluster object.

To see the supported upgrade / installation methods, refer to the *Release Notes* for your version.

Upgrading the Current Version

You can upgrade an existing SD-WAN Security Gateway / Cluster by installing an **upgrade package** with any supported method (see the Release Notes document for the new version).

Clean Install of a New Version

You can "upgrade" an existing SD-WAN Security Gateway / Cluster by performing a Clean Install of a new version with any supported method (see the Release Notes document for the new version).

There are two options:

- If you do **not** plan to configure this Security Gateway / Cluster for SD-WAN again, then you must follow this action plan:
  1. Uninstall the Nano-Agent from the Security Gateway / each Cluster Member with this command in the Expert mode:

     ```
     cpnano -u
     ```

  2. Perform a Clean Install of a new version on the Security Gateway / each Cluster Member.
- If you **plan** to configure this Security Gateway / Cluster for SD-WAN again, then you must follow this action plan:
  1. Perform a Clean Install of a new version on the Security Gateway / each Cluster Member.
  2. Configure the Security Gateway / each Cluster Member for SD-WAN again.

Early Availability Features

EA Feature: QoS in SD-WAN

This section describes an SD-WAN feature in the Early Availability stage.

Important:

- Contact the SD-WAN team to get information about the new R82.20 SD-WAN Early Availability features before starting your journey.
- To get this feature, you must install the R82.20 Early Availability packages on the SD-WAN Security Gateway.
  See the "**Downloads**" section in sk180605.

Introduction to QoS in SD-WAN

SD-WAN Policy can apply QoS settings to ensure traffic priority for the relevant applications.

The SD-WAN Security Gateway performs the required QoS calculations based on the available bandwidth of the applicable interface:

1. Traffic arrives at the Security Gateway.

   If the Access Control policy allows this traffic, continue.

2. If the SD-WAN Policy matches the traffic to a rule with a specific Steering Behavior, continue.

   Otherwise, the Security Gateway forwards the traffic based on the operating system's routing table.

3. The SD-WAN Policy examines the Steering Behavior object to determine the relevant WAN Link.
4. The SD-WAN Policy examines the QoS override settings in the Steering Behavior object.
5. The SD-WAN Policy examines WAN Link Mapping for the QoS settings in the relevant interface.
6. The Security Gateway examines the bandwidth settings in the specific interface in the Gaia OS.
7. The Security Gateway performs the required QoS calculations and processes the traffic accordingly.

Configuring QoS in SD-WAN

Note - The SD-WAN service automatically creates the default QoS object called **Default QoS** with the **Priority (Weight)** value **Medium** in these cases:

- When you connect your Management Server to Check Point Portal.
- When you run the SD-WAN Wizard.

Workflow

1. Configure the required QoS objects (Weight, Limit, Guarantee, DSCP tagging).

   A QoS object determines an interface (ISP) per traffic direction (Upload or Download) in one of these configuration places:

   - WAN Link Mapping - the QoS settings of the relevant WAN Link.
   - The SD-WAN Policy rule that contains a Steering Behavior object with possible override settings on its **QoS** tab.

2. In the WAN Link Mapping, configure which QoS object to use, if not explicitly configured in the Steering Behavior objects.

   You can select the **Default QoS** object, if nothing else is available or wanted.

3. Optional: In the applicable Steering Behavior objects, configure the required QoS settings to override the QoS settings you configured in WAN Link Mapping.

Part 1 - Configuring QoS Objects

1. Log in to *Check Point Portal*.
2. Click the top left **Menu** > in the section **Hybrid Mesh Network Security**, click **SD-WAN**.
3. From the left navigation panel, click **Network**.
4. In the middle section, click **SD-WAN Policy**.
5. From the top toolbar, click **Manage Objects**.
6. From the top toolbar, click ✳ (**New**) > click **QoS**.
7. In the **Name** field, enter a descriptive name that represents this QoS object.
8. **Optional:** In the **Comment** field, enter an applicable text that describes this QoS object.

   This comment is very useful when you select this object later in the SD-WAN Policy.

9. In the **Thresholds** section:

a. Select the required **Priority (Weight)** - **Low**, **Medium**, **High**, or **Critical**.

   This QoS priority determines the traffic precedence relative to priorities configured in other QoS objects that are used in the SD-WAN Policy.

   The SD-WAN Security Gateway performs the required calculation to understand the weight relation between different rules.

   These calculations are based on the number of available QoS objects, number of active QoS objects (with active connections), and their QoS priority.

   These calculations include two steps:

   i. **Relative Weight** - calculated during each installation of the SD-WAN Policy:

   ```
   Relative Weight = (Value of the QoS priority) /
   (Total number of QoS objects in the SD-WAN Policy)
   ```

   The Default QoS object is always used in WAN Link Mapping.

   Each QoS priority has a predefined internal weight value used for this calculation:

   - Critical priority - 800
   - High priority - 400
   - Medium priority - 200
   - Low priority - 100

   ii. **On-the-fly calculation** - when the SD-WAN Policy matches traffic to a rule:

   ```
   Bandwidth for each active QoS object = (Total
   available interface bandwidth) x [(Relative Weight
   of each active QoS object) / (Total relative
   weights of active QoS objects)]
   ```

   The final calculated QoS settings are applied later, such that specific traffic is Prioritized, Limited, or Guaranteed, making best usage of the link's bandwidth.

b. **Optional:** Configure the **Limit** - either based on % of total bandwidth, or in Mbps.

This value determines the maximum limit of total bandwidth that may be used for traffic that matches a rule with this QoS object.

Important:
- In a QoS object, the "limit" value cannot be greater than the total bandwidth available on the interface. Otherwise, policy installation fails.
- If traffic reaches the configured priority (weight) or limit, then the final QoS decision is based on the lowest of these two values.

c. **Optional:** Configure the **Guarantee** - either based on % of total bandwidth, or in Mbps.

This value determines the guaranteed bandwidth for traffic that matches a rule with this QoS object.

Important:
- In a QoS object, the "guarantee" value cannot be greater than the "limit" value. Otherwise, policy installation fails.
- In all configured QoS objects, the sum of all "guarantee" values cannot be greater than 90% of the total bandwidth available on the interface. Otherwise, policy installation fails.
- If traffic reaches the configured "priority" ("weight") value or the "guarantee" value, then the final QoS decision is always based on the "guarantee" value.

10. **Optional:** In the **DSCP Tagging** section:

This setting adds DSCP tags to signal to other devices across the network to prioritize specific traffic, ensuring critical traffic is handled with higher importance.

a. Select **Enable DSCP tagging**.

b. In the field **Packets will be tagged as**, select the applicable DSCP behavior.

11. Click **OK**.

The QoS object now appears in **Manage Objects** > **Custom QoS**.

12. Close the **Manage Objects** panel.

Part 2 - Configuring QoS settings in WAN Link Mapping

In the WAN Link Mapping, configure which QoS object to use, if not explicitly configured in the Steering Behavior objects.

See *"WAN Link Mapping" on page 207*.

Part 3 - Configuring QoS settings in Steering Behavior objects

Optional: In the applicable Steering Behavior objects, configure the required QoS settings to override the QoS settings you configured in WAN Link Mapping.

1. Click the **QoS** tab.
2. In the section **QoS Configuration**, select **Override according to**.
3. Select the required QoS object.
4. **Optional:** In the section **QoS on Upload and Download traffic**:

   This setting applies the QoS configuration to the WAN candidates that you selected on the **Steering Candidates** tab in this Steering Behavior object.

   a. Select **Override and choose specific Traffic Directions per WAN Link**.

   b. For at least one WAN Link, you must select **Use for Upload** or **Use for Download**.

Note - All other upload / download interfaces use the default QoS settings configured in WAN Link Mapping.

Part 4 - Configuring SD-WAN Policy

1. Create a new rule, or edit an existing rule (see *"Configuring SD-WAN Policy" on page 160*).
2. From the top toolbar, click **Publish** to save the changes.
3. From the top toolbar, click **Enforce** to apply the changes.

   The orange frame on this button means there are changes that are not enforced.

   In the popup window that opens, click **Publish & Enforce Policy**.

Example QoS Calculation

Example

One interface on a Security Gateway for "ISP1" with a total bandwidth of 500 Mbps.

Five QoS objects (four QoS objects are active - excluding the QoS object with the Priority "High"):

- The Default QoS object with: Priority = Medium (internal weight value 200), no Limit, no Guarantee
- A custom QoS object #1 with: Priority = Critical (internal weight value 800), Limit = 400 Mbps, Guarantee = 200 Mbps
- A custom QoS object #2 with: Priority = Critical (internal weight value 800), Limit = 400 Mbps, Guarantee = 200 Mbps
- A custom QoS object #3 with: Priority = High (internal weight value 400), no Limit, no Guarantee (in our example, this object is not active)
- A custom QoS object #4 with: Priority = Low (internal weight value 100), Limit = 40 Mbps, no Guarantee

Calculations:

1. Relative weight calculation:

   ```
   Relative Weight = (Value of the QoS priority) / (Total
   number of QoS objects in the SD-WAN Policy)
   ```

   - Relative Weight for the "Critical" priority = 800 / 5 objects = 160
   - Relative Weight for the "High" priority = 400 / 5 objects = 80
   - Relative Weight for the "Medium" priority = 200 / 5 objects = 40
   - Relative Weight for the "Low" priority = 100 / 5 objects = 20

2. On-the-fly calculation:

   ```
   Bandwidth for each active QoS object = (Total available
   interface bandwidth) x [(Relative Weight of each active QoS
   object) / (Total relative weights of active QoS objects)]
   ```

   In our example, only these QoS objects are active:

- The Default QoS object with the "Medium" priority
- A custom QoS object #1 with the "Critical" priority
- A custom QoS object #2 with the "Critical" priority
- A custom QoS object #4 with the "Low" priority

Therefore:

- Total relative weights of active QoS objects = (160 x 2) + 40 + 20 = 380
- Bandwidth for the active QoS object #1 with the "Critical" priority = 500 Mbps x (160 / 380) = 210 Mbps
- Bandwidth for the active QoS object #2 with the "Critical" priority = 500 Mbps x (160 / 380) = 210 Mbps
- Bandwidth for the active Default QoS object with the "Medium" priority = 500 Mbps x (40 / 380) = 55 Mbps
- Bandwidth for the active QoS object #4 with the "Low" priority = 500 Mbps x (20 / 380) = 25 Mbps

For **each** of the QoS objects with the "Critical" priority, these settings apply:

- Bandwidth = 210 Mbps
- Limit = 400 Mbps
- Guarantee = 200 Mbps

Because the Guarantee is configured, the remaining bandwidth for other QoS objects is:

```
Remaining bandwidth = (Total bandwidth of the interface) -
(Total "Guarantee") = 500 - (200 + 200) = 100 Mbps
```

This means that if the total traffic that matches the QoS objects with the "Critical" priority reaches the maximum of 190 Mbps + 190 Mbps = 380 Mbps, the remaining matched QoS objects may be left with little to almost no bandwidth.

In this example, the remaining 100 Mbps will again be calculated by the on-the-fly calculation:

- Active QoS object 1 with the "Critical" priority = 100 Mbps x (160 / 380) = 42 Mbps
- Active QoS object 2 with the "Critical" priority = 100 Mbps x (160 / 380) = 42 Mbps

- Active QoS object 3 with the "Medium" priority = 100 Mbps x (40 / 380) = 11 Mbps
- Active QoS object 4 with the "Low" priority = 100 Mbps x (20 / 380) = 5 Mbps

There may also be times when the QoS objects with higher priorities use most of the available bandwidth, leaving very little bandwidth for the QoS objects with lower priorities. As a result, the SD-WAN Security Gateway may reach a point where it must drop traffic.

EA Feature: IPv6 in SD-WAN

This section describes an SD-WAN feature in the Early Availability stage.

Important:

- Contact the SD-WAN team to get information about the new R82.20 SD-WAN Early Availability features before starting your journey.
- To get this feature, you must install the R82.20 Early Availability packages on the SD-WAN Security Gateway.
  See the "**Downloads**" section in sk180605.

Overview

SD-WAN supports IPv6 traffic only for Local Breakout scenarios.

SD-WAN can steer IPv6 traffic to local IPv6 Internet links.

SD-WAN does not support IPv6 for Overlay VPN and tunnel selection.

SD-WAN ignores "Overlay" rules that contain IPv6 objects (a warning appears).

Important - SD-WAN features that are related to Overlay (such as *tunnel-based steering*) operate only on IPv4.

Prerequisite

Enable IPv6 support on the SD-WAN Security Gateway and reboot it.

See the *Gaia Administration Guide* for your version.

Important - Without IPv6 support enabled, the Security Gateway does not install IPv6 SD-WAN rules. As a result, it handles IPv6 traffic using the OS routing (not SD-WAN routing).

SD-WAN Behavior in IPv6

When IPv6 support and SD-WAN are enabled on the Security Gateway:

- The Security Gateway loads a separate IPv6 Firewall instance.

  This IPv6 Firewall instance handles SD-WAN rule matching for IPv6 traffic.

- The Security Gateway loads a separate SD-WAN steering process (`sdwan_steering6`).

  This process handles all probes over IPv6 and steering decisions for IPv6.

- The Security Gateway inspects IPv6 traffic independently from IPv4 traffic.

IPv6 Support in SD-WAN Interfaces

An SD-WAN interface can operate in one of these modes:

- IPv4 single-stack.
- IPv6 single-stack.
- Dual-stack (IPv4 and IPv6 on the same interface).

Depending on the configuration, an interface can have:

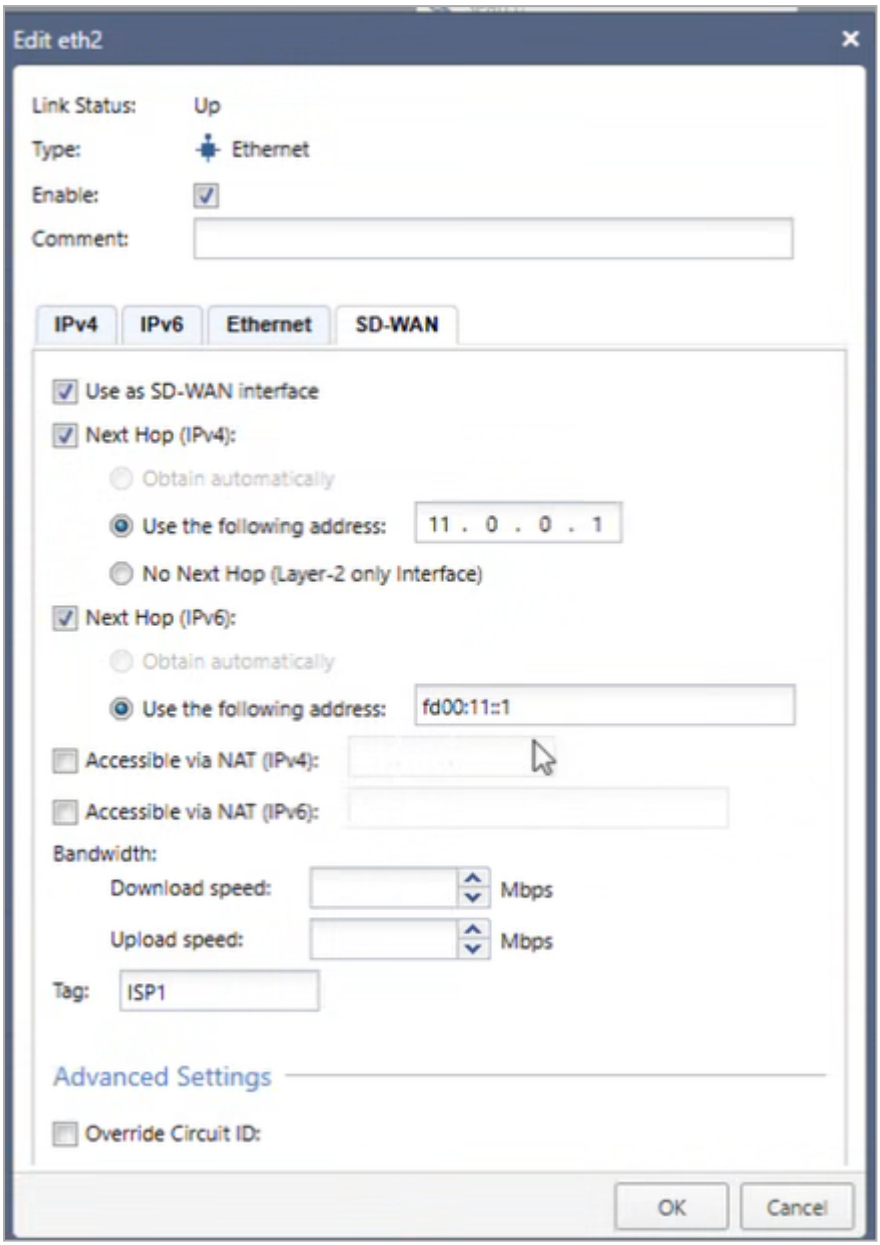
- Only an IPv4 next hop.
- Only an IPv6 next hop.
- Both IPv4 and IPv6 next hops.

Configuring SD-WAN Next Hop for IPv6

Procedure in Gaia Portal

1. With a web browser, connect to Gaia Portal.
2. In the navigation tree, click **Network Management** > **Network Interfaces**.
3. Select an interface from the list and click **Edit**.
4. At the top, click the **SD-WAN** tab.
5. For IPv6 single-stack:
    a. Select **Next Hop (IPv6)**.
    b. Enter the required next-hop IPv6 address.
6. For dual-stack, also:
    a. Select **Next Hop (IPv4)**.
    b. Enter the required next-hop IPv4 address.
7. Click **OK**.

Example:



Procedure in Gaia Clish

1. Connect to the command line on the Security Gateway.
2. Log in to Gaia Clish.
3. For IPv6 single-stack, configure the required next-hop IPv6 address:

   ```
   set interface <Name of Interface> sdwan nexthop <IPv6 Address of Next Hop>
   ```

4. For dual-stack, also configure the required next-hop IPv4 address:

```
set interface <Name of Interface> sdwan nexthop <IPv4
Address of Next Hop>
```

5. Save the changes:

```
save config
```

6. Examine the configuration:

```
show interface <Name of Interface> sdwan
```

Configuring "Accessible via NAT"

SD-WAN supports configuring NAT accessibility separately for IPv4 and IPv6.

Note - This configuration applies to future IPv6 Overlay support.
Overlay does not support IPv6 at this time.

Procedure in Gaia Portal

1. With a web browser, connect to Gaia Portal.
2. In the navigation tree, click **Network Management** >**Network Interfaces**.
3. Select an interface from the list and click **Edit**.
4. At the top, click the **SD-WAN** tab.
5. For IPv6 single-stack:
   a. Select **Accessible via NAT (IPv6)**.
   b. Enter the required IPv6 address.
6. For dual-stack, also:
   a. Select **Accessible via NAT (IPv4)**.
   b. Enter the required IPv4 address.
7. Click **OK**.

Procedure in Gaia Clish

1. Connect to the command line on the Security Gateway.
2. Log in to Gaia Clish.
3. For IPv6 single-stack, configure the required IPv6 address:

```
set interface <Name of Interface> sdwan nat <IPv6 Address>
```

4. For dual-stack, also configure the required IPv4 address:

```
set interface <Name of Interface> sdwan nat <IPv4 Address>
```

5. Save the changes:

```
save config
```

6. Examine the configuration:

```
show interface <Name of Interface> sdwan
```

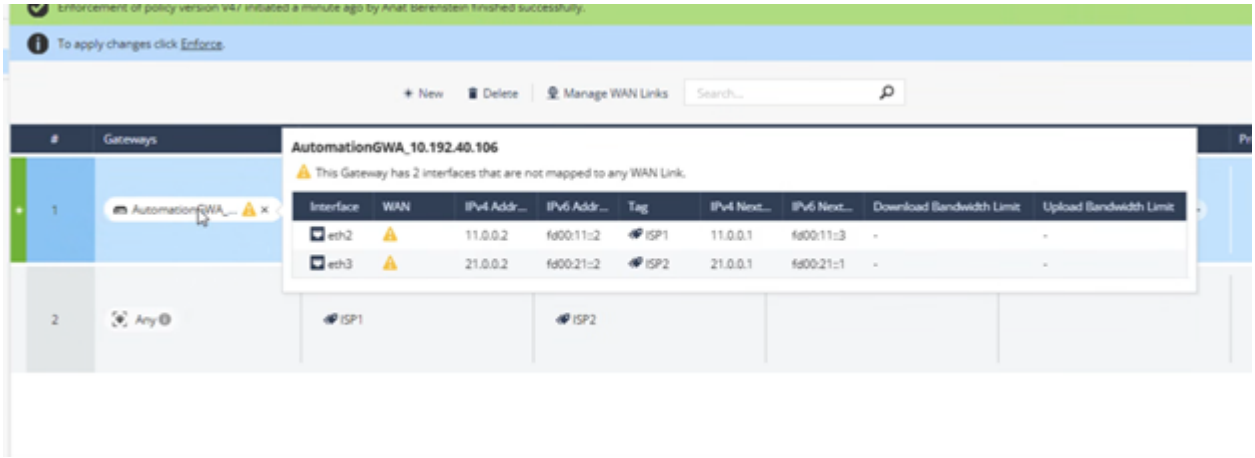
WAN Link Mapping

Explanation

See *"WAN Link Mapping" on page 207*.

The **Network** view > **WAN Link Mapping** shows both IPv4 and IPv6 addresses for each Security Gateway.

Example:



SD-WAN Policy Behavior with IPv6

Explanation

Open **Steering Object** > click the **Criteria** tab > scroll down to the **Quality Check Methodology** section.

The IP version of the probe target must match the IP version used by traffic in the SD-WAN rule.

- If a rule uses IPv4 objects, the steering object must probe an IPv4 target.
- If a rule uses IPv6 objects, the steering object must probe an IPv6 target.
- If a rule includes both IPv4 and IPv6 objects, the steering object must include both IPv4 and IPv6 probe targets.

If the probe target does not match the traffic IP version, the SD-WAN policy fails or is not applied to this traffic.

IPv6 objects in SD-WAN rules:

- Security Gateway that only have an IPv4 address configured on their SD-WAN interfaces ignore SD-WAN rules with IPv6 objects.
- Security Gateways that have an IPv6 address configured on their SD-WAN interfaces install and enforce SD-WAN rules with IPv6 objects.

NAT per ISP with IPv6

See *"SD-WAN NAT for ISP" on page 271*.

NAT Configuration

The NAT per ISP feature supports NAT addresses for both IPv4 and IPv6.

Example:



Source Object Compatibility

IPv4 NAT only:

- Source must include: IPv4 objects, IPv4+IPv6 objects, or Dynamic Objects.
- Behavior:
  - NAT is applied only to IPv4 source traffic.
  - IPv6 source traffic is forwarded without NAT translation.

IPv6 NAT only:

- Source must include: IPv6 objects, IPv4+IPv6 objects, or Dynamic Objects.
- Behavior:
  - NAT is applied only to IPv6 source traffic.
  - IPv4 source traffic is forwarded without NAT translation.

IPv4 and IPv6 NAT:

- Source must include: IPv4 objects, IPv4+IPv6 objects, or Dynamic Objects.
- Behavior:
  - IPv4 source traffic is translated using the configured IPv4 NAT address.
  - IPv6 source traffic is translated using the configured IPv6 NAT address.

Monitoring and Statistics

Explanation

Live Dashboard

IPv6 SD-WAN statistics are **not** available in the **Monitor** view > **Dashboard** > **Live Monitoring** tab.

CPView (sk101878)

IPv6 statistics are available in:

- **cpview** > **Advanced** > **SD-WAN**
- Separate tabs exist for:
  - IPv4 probes and steering decisions.
  - IPv6 probes and steering decisions.

Internal Architecture and Troubleshooting

Firewall Instances and SD-WAN Processes

Firewall and SD-WAN use separate processing paths for IPv4 and IPv6 traffic.

IP Version	Firewall Instance	SD-WAN Process
IPv4	FW	`sdwan_steering`
IPv6	FW6	`sdwan_steering6`

Each IP version uses a dedicated SD-WAN steering process, and each process maintains its own:

- SD-WAN policy files.
- SD-WAN probe targets.
- SD-WAN steering decisions.
- SD-WAN kernel tables.
- SD-WAN log files.

Steering and Kernel Tables

The process "`sdwan_steering`" on Security Gateway:

- Probes IPv4 targets.
- Writes steering decisions to the Security Gateway IPv4 kernel tables.

  To view entries in these tables, run: `fw tab -t <table_name>`

The process "`sdwan_steering6`" on the Security Gateway:

- Probes IPv6 targets.
- Writes steering decisions to the Security Gateway IPv6 kernel tables.

  To view entries in these tables, run: `fw6 tab -t <table_name>`

Log Files

IP Version	Log File on Security Gateway
IPv4 SD-WAN	`$FWDIR/log/sdwan_steering.elg`
IPv6 SD-WAN	`$FWDIR/log/sdwan_steering6.elg`

Policy Installation Behavior

- SD-WAN rules that contain IPv4 objects and probing targets are installed into this file on the Security Gateway:

  `$FWDIR/state/local/SDWAN/sdwan_steering_policy.json`

- SD-WAN rules that contain IPv6 objects and probing targets are installed into this file on the Security Gateway:

  `$FWDIR/state/local/SDWAN/sdwan_steering6_policy.json`

Each SD-WAN rule includes:

- Traffic matching objects.
- Steering settings.
- Probe targets.

Important - IPv6 SD-WAN rules are installed only if at least one SD-WAN interface has an IPv6 next hop configured.

IPv6 Traffic Flow with SD-WAN

1. An IPv6 connection arrives at the Security Gateway.
2. If all these conditions are met:
   a. IPv6 support is enabled on the Security Gateway.
   b. At least one SD-WAN interface is configured with an IPv6 next hop.
   c. A matching SD-WAN rule exists.

   Then:

   d. The FW6 instance evaluates the connection against the SD-WAN rule base.
   e. The FW6 instance consults the IPv6 SD-WAN steering kernel tables based on the matched rule.
   f. The Security Gateway uses SD-WAN to route the IPv6 traffic through the selected ISP.
3. If IPv6 support is enabled on the Security Gateway and at least one IPv6-enabled SD-WAN interface exists, but no SD-WAN rule matches the traffic:
   a. SD-WAN does not steer the traffic
   b. The Security Gateway uses OS to route the IPv6 traffic.
4. If the Security Gateway does not have an IPv6-enabled SD-WAN interface:
   a. The Security Gateway does not evaluate IPv6 SD-WAN rules.
   b. The Security Gateway uses OS to route the IPv6 traffic.

Limitations

- The Security Gateway ignores SD-WAN rules with IPv6 objects if there are no IPv6-enabled SD-WAN interface on the Security Gateway.
- In such a case, the Security Gateway uses OS routing (not SD-WAN routing).
- The Security Gateway installs SD-WAN rules with IPv6 objects only when at least one SD-WAN interface is configured with an IPv6 next hop.
- The Security Gateway splits (internally) SD-WAN rules that contain both IPv4 and IPv6 objects and processes these rules by separate Firewall instances and by separate SD-WAN steering processes.
- If an IPv6 SD-WAN rule requires probing but the steering object does not include an IPv6 probe target, the SD-WAN policy fails on the Security Gateway (even if there is at least one IPv6-enabled SD-WAN interface).

  In such a case, the Security Gateway uses OS routing (not SD-WAN routing).
- SD-WAN does not support IPv6 Overlay steering.
- You must configure IPv6 next hops manually. SD-WAN does not support automatically learned next hops (for example, from DHCP or DHCPv6).

SD-WAN Troubleshooting

Troubleshooting SD-WAN Installation

The "cpsdwan stat" command shows no policy installed, or shows a previous policy version

Symptoms:

- Output of the "`cpsdwan stat`" command shows no policy installed.
- Output of the "`cpsdwan stat`" command shows a previous policy version compared to the policy version in the output of the "`cpnano -s`" command.

Solution:

1. On the Security Gateway, examine the Nano-Agent status:
   a. Connect to the command line on the Security Gateway.
   b. Log in to the Expert mode.
   c. Examine the Nano-Agent status:

      ```
      cpnano -s
      ```

      Examine the lines that are highlighted in the example output below:

      - Your output must show the same statuses

- Examine the dates

Example:

```
---- Check Point Nano Agent ----
Version: 1.2301.472956
Status: Running
Last update attempt: 2023-04-20T14:50:06.545687
Last update: 2023-04-20T14:50:06.557303
Last update status: Succeeded Policy version: 91
Last policy update: 2023-04-20T11:51:10.857490
Last manifest update: None
Last settings update: 2023-04-20T11:51:10.857490
Registration status: Succeeded
Manifest status: None
Upgrade mode: automatic
Fog address: inext-agents.cloud.ngen.checkpoint.com
Agent ID: XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXX
Profile ID: XXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
Tenant ID: XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXX
Registration details:
    Name:
    Type: Quantum
    Platform:
    Architecture:
Service policy:
    sdwan: /etc/cp/conf/sdwan/sdwan.policy
Service settings:

---- Check Point Orchestration Nano Service ----
Type: Public, Version: 1.2301.472956, Created at: 2023-01-05T14:56:54+0200
Status: Running

---- Check Point Messaging Proxy Nano Service ----
Type: Public, Version: 1.2301.472956, Created at: 2023-01-05T14:56:54+0200
Status: Running

---- Check Point SD-WAN Nano Service ----
Type: Public, Version: 1.2301.472956, Created at: 2023-01-05T14:56:54+0200
Status: Running

---- Check Point SD-WAN Logger Nano Service ----
Type: Public, Version: 1.2301.472956, Created at: 2023-01-05T14:56:54+0200
Status: Running

---- Check Point Cpview Metric Provider Nano Service ----
Type: Public, Version: 1.2301.472956, Created at: 2023-01-05T14:56:54+0200
Status: Running
```

2. In Check Point Portal > **SD-WAN** application:
   a. Go to the **Network** view > **SD-WAN Policy** page.
   b. From the top, click **WAN Link Mapping**.
   c. Make sure you configured all required interfaces.
   d. Close the **WAN Link Mapping** window.

e. Examine SD-WAN Policy to make sure there are no steering objects that select only a specific interface, such as "WAN 2" that has no association to an actual interface on the Security Gateway in the **WAN Link Mapping** window.

3. Go to the **Monitor** view > **Events** page.
4. Search for policy installation failures - examine the reason and the remediation suggestion.
5. Advanced troubleshooting on the Security Gateway:
   a. Examine the status of the "`sdwan_steering`" process - it must be running:
      i. Run:

      ```
      cpwd_admin list | grep -E "APP|steering"
      ```

      The "`STAT`" column must show "`E`" (executing).

      ii. Run:

      ```
      ps -aux | grep sdwan_steering | grep -v grep
      ```

      iii. If the process is **not** running, then contact *Check Point Support* and include this information:
         - The complete CLI outputs
         - Does the `/var/log/dump/usermode/` directory contain core dump files for the "`sdwan_steering`" process?
         - These files:
            - `$FWDIR/log/sdwan_steering.elg`
            - `$FWDIR/log/cpsdwan.elg`
            - `/var/log/nano_agent/cp-nano-sdwan.dbg`
            - `/var/log/nano_agent/cp-nano-orchestration.dbg`

b. Fetch the latest SD-WAN policy that was downloaded from Check Point Portal:

   i. Fetch the latest SD-WAN policy:

   ```
   cpsdwan fetch_new
   ```

   ii. Wait for the command to complete.

   iii. Immediately collect and examine this log file:
   `$FWDIR/log/cpsdwan.elg`

   If the reason for the fetch failure is not sufficiently clear from the output or from the `$FWDIR/log/cpsdwan.elg` file, then:

      i. Fetch the latest SD-WAN policy under the debug:

      ```
      TDERROR_ALL_ALL=5 cpsdwan fetch_new
      ```

      ii. Wait for the command to complete.

      iii. Immediately collect and examine these log files:

      - `$CPDIR/log/cpsdwan_fw_fetchlocal_out.elg`
      - `$FWDIR/log/cpsdwan.elg`
      - `$FWDIR/log/fwk.elg`

c. If fetching the latest SD-WAN policy downloaded from Check Point Portal failed, and the reason for the fetch failure is not clear, then fetch the SD-WAN policy from the local directory:

   i. Make sure there is an updated / acceptable policy version:

   ```
   cpnano -s | grep version
   ```

   ii. Fetch the local policy:

   ```
   cpsdwan fetch_local
   ```

   iii. Immediately collect and examine these log files:

   - `$FWDIR/log/sdwan_steering.elg`
   - `$FWDIR/log/cpsdwan.elg`
   - `/var/log/nano_agent/cp-nano-sdwan.dbg`
   - `/var/log/nano_agent/cp-nano-orchestration.dbg`

6. Contact *Check Point Support* and include the complete CLI outputs and log files.

Spark Firewall Appliance fails to install SD-WAN Policy with the "Failed to Initialize VPN Transports" event

See sk184225.

Spark Firewall Cluster Members Fail to Onboard to SD-WAN

Environment:

- Product: Spark Firewall
- Deployment: Spark Firewall Cluster

Symptoms:

- On Spark Firewall Cluster Members the Nano-Agent does not download SD-WAN Nano-Services, even though the cluster object is included in an SD-WAN Profile, and the SD-WAN Profile is used by SD-WAN policy rules.
- The `$FWDIR/log/cpsdwan.elg` file on Spark Firewall Cluster Members contains an error similar to:

```
Failed to run get value of field ifType, in interface
<ClusterObjectInterfaceName>
```

As a result the Cluster Members fail to onboard to SD-WAN, and SD-WAN policy and Nano-Services are not properly downloaded and enforced.

Cause:

The Spark Firewall Cluster object in SmartConsole contains an interface name that does not exist in the operating system on the Spark Firewall Cluster Members.

Because of this mismatch:

- The `cpsdwan` command fails when trying to download and validate all gateway data.
- The process cannot correctly obtain the cluster object UUID.
- Therefore, the Cluster Member does not recognize that the they belong to any SD-WAN Profile, and SD-WAN onboarding fails for that Cluster Member.

Solution:

Correct the interface configuration in the Spark Firewall Cluster object, so it matches the actual interfaces on the Spark Firewall Cluster Members.

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Spark Firewall Cluster object.
4. Go to the **Topology** tab.
5. For each interface:

a. Verify that the interface names configured in the cluster object match the real interface names on the Spark Firewall Cluster Members.

b. Correct any wrong / outdated / non-existing interface names.

6. Install the Access Control Policy on the Spark Firewall Cluster object.

After the policy installation:

- The "`cpsdwan`" command should be able to:
  1. Download and verify the gateway data.
  2. Identify the correct cluster object's UUID for the Spark Firewall Cluster Member.
- The Nano-Agent on Spark Firewall Cluster Members should now download SD-WAN Nano-Services and complete SD-WAN onboarding.

The 'cpsdwan stat' command persistently shows "Currently fetching policy, please try again later"

Symptoms:

- A new SD-WAN policy version is not installed on the Security Gateway.
- Output of the "`cpsdwan stat`" command persistently shows "`Currently fetching policy, please try again later`".
- Output of the "`cpnano -s`" command may show "`Failed to update services' policy configuration files`" or another failure message.

Cause

"`cpsdwan`" is an on-demand process that runs as part of the SD-WAN policy installation. It may not exit correctly after policy installation.

Solution:

1. On the Security Gateway, examine the status of the "`cpsdwan`" processes:
   a. Connect to the command line on the Security Gateway.
   b. Log in to the Expert mode.
   c. Examine the status of the "`cpsdwan`" processes:

```
ps aux | grep -E "COMMAND|cpsdwan" | grep -v grep
```

Examine the value in the "TIME" column to see how long each "cpsdwan" process has been running.

If this column shows a long time (counting from the policy installation), then this confirms the root cause.

2. On the Security Gateway, examine the $FWDIR/log/cpsdwan.elg file for lock failures:

```
grep -n 'failed to lock cpsdwan' $FWDIR/log/cpsdwan.elg
```

If the output shows numerous lines, then this confirms the root cause.

3. To investigate this issue, collect the diagnostic information from the Security Gateway and contact *Check Point Support*:
   a. Output of this command:

```
cpnano --info
```

   b. Output of this command:

```
cpwd_admin list | grep -E "APP|steering"
```

   c. Log files:
      i. $FWDIR/log/cpsdwan.elg*
      ii. $FWDIR/log/sdwan_steering.elg*

4. As an immediate workaround, terminate the "cpsdwan" processes:
   a. Terminate the "cpsdwan" processes gracefully:

```
pkill -TERM -e -x cpsdwan
```

   b. Examine the status of the "cpsdwan" processes:

```
ps aux | grep -E "COMMAND|cpsdwan" | grep -v grep
```

   c. If the "cpsdwan" processes are still running, terminate them forcefully:

```
pkill -KILL -e -x cpsdwan
```

   d. Examine the status of the "cpsdwan" processes:

```
ps aux | grep -E "COMMAND|cpsdwan" | grep -v grep
```

Troubleshooting SD-WAN "Local Breakout Only"

For background information, see *"SD-WAN Connection Type - "Internet"" on page 188*.

The Inbound NAT return traffic ignores SD-WAN policy rules, or does not return symmetrically

Symptom:

The return non-encrypted traffic (such as return packets from an internal server to a client on the Internet) ignores SD-WAN policy rules and takes over routing decisions.

The return non-encrypted traffic (such as return packets from an internal server to a client on the Internet) ignores SD-WAN policy rules, or does not return symmetrically.

Cause:

By default, the routing decision for the return packet, for a non-encrypted connection, is based on the operating system routing table.

The Symmetric Packet Return feature was added to route the return packets in a symmetric way, from the original ISP, through which they arrived. See *"SD-WAN Symmetric Packet Return" on page 257*.

The Symmetric Packet Return feature is available in:

- R82.10 and higher
- R82 Jumbo Hotfix Accumulator Take 14 and higher
- R81.20 Jumbo Hotfix Accumulator Take 79 and higher
- Spark Firewall R81.10.15 and higher

Note - It is **not** possible to match Server-to-Client (S2C) packets to SD-WAN Policy rules.

Inbound NAT stopped working with SD-WAN

Symptom:

Inbound NAT stopped working with SD-WAN.

Solution:

Capture the traffic on the Security Gateway with FW Monitor (sk30583).

Filter for the applicable traffic to see what is the routing behavior for the connections.

If the traffic capture shows that the packet enters the Security Gateway and the Security Gateway sends the packet back - towards the ISP Next Hop (instead of passing it through), then it is possible the connection matches a "Local Breakout" / "Backhaul" rule that marks the packet to be routed to an ISP.

Available options:

- **Option 1:**

  You can use the Dynamic Object "**SD-WAN Internet**" that makes sure to match the traffic against the destination after NAT, and not against the original destination.

  Support for the Dynamic Object "**SD-WAN Internet**" is available in:

  - R82.10 and higher
  - R82 Jumbo Hotfix Accumulator Take 14 and higher
  - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
  - Spark Firewall R81.10.15 and higher

  For information about this Dynamic Object "**SD-WAN Internet**", refer to the *"Configuring SD-WAN Policy" on page 160*.

- **Option 2:**

  In the SD-WAN Policy, make sure the traffic that is directed to your public NAT Pool IP addresses does not match a rule with a "Local Breakout" / "Backhaul" steering behavior.

  If such a rule is necessary in your SD-WAN Policy, then configure another rule above it to match the traffic to all your public NATed IP addresses with an "Overlay" action.

  As a result, because the traffic is not encrypted, the operating system would make the routing decision and not SD-WAN.

The "SD-WAN" section in the traffic logs for connections the Security Gateway created, shows wrong SD-WAN routing decision

Symptom:

The "**SD-WAN**" section in the Security Gateway logs for connections the Security Gateway created (to Cloud / Check Point Portal applications / Smart-1 Cloud / the public IP address of the on-premises Management Server), shows an SD-WAN routing decision that perhaps is not the correct one.

Cause:

You can safely ignore the "**SD-WAN**" section in the Security Gateway logs for connections initiated by the Security Gateway.

SD-WAN does not enforce any action on such connections.

These logs just show the theoretical decision.

To see the outgoing interface, capture the traffic with FW Monitor (sk30583) or CPPCAP (sk141412).

SD-WAN overrides my directly connected networks / Gaia OS routes

Symptom:

SD-WAN routing decision overrides my directly connected networks / Gaia OS routes on the Security Gateway.

Cause:

This is by design.

If traffic matches an SD-WAN Policy rule with the Steering Behavior "Local Breakout Only" or "Backhaul Only", then the Security Gateway sends the traffic to the selected ISP, regardless of all the other routes.

If traffic matches an SD-WAN Policy rule with the Steering Behavior "Overlay", and the traffic is not encrypted to an SD-WAN peer, then the Security Gateway sends the traffic based on the active kernel routes.

Important - Make sure only the required traffic can match the SD-WAN Policy rules, especially with the Steering Behavior "Local Breakout" or "Backhaul".

CPView shows that the state of the "Local Breakout" probing target is "DOWN"

Symptom:

CPView > **Advanced** > **SD-WAN** page > **"Local Breakout" Probing Results** section shows that the state of the "Local Breakout" target probing is "DOWN".

Cause:

This usually means that the Security Gateway did not receive the ICMP Echo Reply from the nexthop probing target.

Solution:

1. Make sure the state of the applicable interface is "UP" on the nexthop probing target.
2. Make sure the nexthop probing target is configured to respond to ARP Requests **or** to ICMP Echo Requests from the Security Gateway.

   Important - If the nexthop probing target does not respond to ARP Requests and ICMP Echo Requests (for example, it is currently down), then the Security Gateway does not try to probe the "Local Breakout" targets.

   The Security Gateway uses ARP Probing by default in these versions:

   - R82.10 and higher
   - R82 Jumbo Hotfix Accumulator Take 14 and higher
   - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
   - Spark Firewall R81.10.15 and higher
3. Connect to the command line on the Security Gateway.
4. Log in to the Expert mode.
5. Examine the state of the applicable ISP.

   Important - If the Security Gateway detects the state of the ISP as "DOWN", the Security Gateway does not try to probe the "Local Breakout" / Internet target for that ISP.

   a. Run:

   ```
   cpview
   ```

   b. Go to **Advanced** tab > **SD-WAN** page > **Nexthop Probing Results** section, and refer to the **ISP State**.
6. Continue the troubleshooting:

- If the nexthop is "Down":

  a. Use the CPPCAP tool (sk141412) to capture the ICMP traffic between the Security Gateway (on the applicable interface) and the nexthop probing target.

  ```
  cppcap -i <Name of Interface> -f "icmp and host <IP Address of Nexthop Probing Target>" -o /var/log/cppcap_probing.cap
  ```

  b. Make sure the Security Gateway does not drop this ICMP traffic to and from the nexthop probing target:

  For more information about the kernel debug procedure on a Security Gateway, see the *Check Point Firewall Guide* for your version > chapter "Kernel Debug".

  ```
  fw ctl zdebug -m fw + drop
  ```

- If the nexthop is "UP", but the "Local Breakout" probe is "DOWN":

  a. Use the CPPCAP tool (sk141412) to capture the ICMP traffic between the Security Gateway (on the applicable interface) and the "Local Breakout" probing target (such as 8.8.8.8).

  ```
  cppcap -i <Name of Interface> -f "icmp and host <IP Address of "Local Breakout" Probing Target>" -o /var/log/cppcap_probing.cap
  ```

  b. Make sure the Security Gateway does not drop this ICMP traffic to and from the "Local Breakout" probing target:

  ```
  fw ctl zdebug -m fw + drop
  ```

SLA information does not appear in Check Point Portal from a specific Security Gateway

Symptom:

Check Point Portal > **SD-WAN** > **Monitor** view > **Dashboard** page does not show the SLA information from a specific Security Gateway. This issue occurs all the time, or randomly from time to time.

Solution:

Follow these steps on the Security Gateway:

1. Make sure the timezone, the date, and the time are configured correctly.
2. Check if the Security Gateway provides the SD-WAN information.

   In the Expert mode, run (this command is available in R82 and higher, see sk101878):

   ```
   cpview -mf SDWAN
   ```

   A JSON output must appear after several seconds.
3. Make sure the "`sdwan_steering`" process is running.

   Run:

   ```
   cpwd_admin list | grep -E "PID|SDWAN_STEERING"
   ```

   In the output:

   a. The `APP` column must show `SDWAN_STEERING`

   b. The `STAT` column must show "`E`" (executing)

   c. The `#START` column must show the digit "`1`" (started only one time)
4. Make sure the Nano-Agent is running without errors:

   ```
   cpnano -s
   ```
5. Make sure the disk partitions have free disk space:

   ```
   df -kh
   ```

   On a Spark Firewall Appliance, if the `/tmp` partition is full, then these options are available:

- Temporary option:

  Reboot the Spark Firewall Appliance.

- Permanent option:

  If the `/tmp` partition repeatedly gets full, then it is necessary to understand which files are created that fill this partition.

  As an immediate step, you can increase the site of the `/tmp` partition in Gaia Clish:

  a. Run:

  ```
  set temp-dir-size tmp-dir-size <Size in Megabytes>
  ```

  Example for 60 MB: `set temp-dir-size tmp-dir-size 60`

  b. Reboot:

  ```
  reboot
  ```

6. If the issue persists, then contact *Check Point Support*.

Frequent "ISP Down" and Link Swap events due to the Next Hop device not responding in time to ARP Requests

Topology:

SD-WAN WAN interface with a configured next hop device.

Symptoms:

- In **Check Point Portal > SD-WAN > Monitor > Events**, you see many ISP Down" / "Link Down" events for a specific ISP / SD-WAN link.
- Traffic may intermittently fail over to backup ISP links, even though the physical line and the next hop device are up.
- Capture of ARP traffic on the SD-WAN interface shows:
  1. The Security Gateway sends frequent ARP Requests for the next hop IP address.
  2. The next hop device does not respond in time or at all to these ARP Requests.

Cause:

The SD-WAN steering process monitors the next hop availability using the ARP-based probing.

Default behavior:

- Probe rate in normal conditions: 2 ARP requests every 550 ms.
- Response timeout: 300 ms (time to wait for an ARP reply).
- Failure threshold: After 3 consecutive missed ARP Responses, the Security Gateway marks the ISP link as "down" and sends an event about "ISP Down" / "Link Down".

Some next hop devices (for example, certain equipment, or overloaded Layer 3 devices) do not respond reliably when probed at this relatively high ARP rate and short timeout.

As a result:

- ARP Replies arrive too late or are dropped.
- The SD-WAN steering process interprets this as packet loss / next hop failure.
- The link is incorrectly marked as "down", generating frequent "ISP Down" / "Link Down" events and causing the SD-WAN link swap.

Solution:

Adjust the ARP probing parameters in SD-WAN steering on this specific Security Gateway:

- Reduce the ARP probe rate.
- Increase the response timeout.

Recommended values:

- Send 1 ARP request every 1000 ms (1 second).
- Wait 700 ms for any ARP Response before declaring a timeout.

This reduces the load on the next hop device and gives it more time to respond, thus minimizing false "ISP Down" / "Link Down" events.

Procedure:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in.
3. If your default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```

4. Modify the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

a. If the file `$FWDIR/conf/sdwan/sdwan_steering_params.json` exists, create a backup copy.

   Otherwise, create this file.

   Run this long command:

   ```
   if [ -f $FWDIR/conf/sdwan/sdwan_steering_params.json ]
   ; then echo "Creating the backup ..." ; cp -v
   $FWDIR/conf/sdwan/sdwan_steering_params.json{,BKP} ;
   else echo "Creating the file ..." ; touch
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; stat
   $FWDIR/conf/sdwan/sdwan_steering_params.json ; fi
   ```

b. Edit the `$FWDIR/conf/sdwan/sdwan_steering_params.json` file:

   ```
   vi $FWDIR/conf/sdwan/sdwan_steering_params.json
   ```

c. If this file is empty, then add all these lines.

   If this file already contains other configuration parameters, then add these configuration parameters on new lines:

   ```
   {
       "sdw_nexthop_probe_parallel_reqs" : 1,
       "sdw_nexthop_packet_loss_timeout" : 700,
       "sdw_nexthop_probe_rate" : 1000
   }
   ```

d. Save the changes in the file and exit the editor.

5. Restart the SD-WAN Steering process:

   ```
   sdwan_steering_stop ; sdwan_steering_start
   ```

   Warning - Until the SD-WAN Steering process starts again (in normal circumstances, it takes less than one minute):
   - Existing and new VPN / Overlay connections are interrupted.
   - Existing Local Breakout connections may be interrupted.
   - New Local Breakout connections cannot undergo the SD-WAN Local Breakout routing.

6. Capture the ARP traffic on the SD-WAN interface to make sure:

   a. The Security Gateway sends ARP Requests for the next hop IP address with the newly configured intervals.

   b. The next hop device responds in time to all these ARP Requests.

7. In **Check Point Portal > SD-WAN > Monitor > Events**, the number of "ISP Down" / "Link Down" events from this specific Security Gateway should decrease significantly.

Security Gateway loses Internet connectivity when the Primary ISP fails, even though SD-WAN uses multiple ISPs

Platform: Security Gateway / Spark Firewall

Symptoms:

When the primary ISP fails, the Security Gateway loses Internet connectivity, even though SD-WAN is configured with multiple ISPs:

- Connectivity from the Security Gateway itself to the Internet is lost.
- Communication to Smart-1 Cloud / Management Server over the Internet is lost.
- VPN tunnels may fail to negotiate after CRL expiration grace period (because the gateway cannot reach CRL servers).
- Communication from the gateway to the Check Point Portal is lost.

On the Security Gateway:

- The Gaia Clish command "`show route`" shows that the failed primary ISP is still the active default route.
- Traffic originating from the gateway itself (local connections) is still sent via the failed ISP, instead of failing over to the secondary ISP as expected.

Cause:

- By default, local connections (traffic originating from the Security Gateway itself, e.g., management, CRL checks, Check Point Portal, etc.) are routed according to the Gaia main routing table, not by SD-WAN rules.
- SD-WAN does not manage or update Gaia main routing table.

Therefore, even if SD-WAN correctly fails over user traffic between ISPs, the default static route in Gaia may still point to the primary ISP, causing local traffic to continue using the failed link.

Solution:

- Use Gaia Route Reachability (recommended)

  Configure the static default route to be reachability-aware, so that the Security Gateway automatically switches to the next priority ISP default route when the primary ISP loses Internet connectivity.

In Gaia Portal or Gaia Clish:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in.
3. Edit the default static route and do one of these:
   - Use ping (sk156812) to only monitor the next hop.
   - Configure IP Reachability Detection to monitor an external target (e.g., a public IP or DNS server), and attach this check to the default static routes (for all default routes except the last priority / last-resort route).

     See the *Gaia Advanced Routing Administration Guide* for your version.
4. When the primary ISP becomes unreachable based on these checks:
   - Gaia marks the default route via that ISP as unreachable.
   - Gaia automatically moves to the next priority default route (e.g., via the secondary ISP).

In Spark Firewall for each Internet connection, configure the appropriate reachability check in the Connection Monitoring tab of that Internet connection.

This ensures that local traffic that the Security Gateway generates (to the Management Server, Smart-1 Cloud, CRL, Check Point Portal, etc.) will follow ISP failover logic.

- Apply SD-WAN Local Breakout Rules to Local Connections

  Alternatively, there is an option to let SD-WAN local breakout rules also apply to local connections (traffic originating from the gateway itself), by enabling a kernel parameter.

  - This effectively allows SD-WAN to steer traffic that the Security Gateway generates to the Internet according to SD-WAN local breakout policy, instead of Gaia's static routing only.
  - To enable this behavior, contact *Check Point Support* and request SD-WAN R&D to enable the relevant kernel parameter on the Security Gateway.

  Use this option when you want SD-WAN to fully control both user traffic and traffic that the Security Gateway generates, and when adjusting Gaia routing (Option 1) is not sufficient or not desired.

Troubleshooting SD-WAN "Overlay"

For background information, see *"SD-WAN Connection Type - "Overlay"" on page 200*.

After an SD-WAN link failover, the "Overlay" traffic is disconnected and stops passing

Symptom:

After an SD-WAN link failover, the "Overlay" traffic is disconnected and stops passing.

Solution:

1. In Check Point Portal > **SD-WAN** application > **Network** view > **SD-WAN Policy** page:
   a. In the Steering Behavior object "**Overlay**", make sure you selected the WAN link, to which you expected the traffic to fall back.

      As a result, this "Overlay" traffic and probing traffic would match the "Overlay" steering behavior that uses the WAN link.

   b. Make sure that this "Overlay" traffic and probing traffic do **not** match a rule with the Steering Behavior object "**Breakout**".
2. On the Security Gateway, after the SD-WAN link failover:
   a. Connect to the command line on the Security Gateway.
   b. Log in to Gaia Clish.
   c. Make sure that you have at least one VPN tunnel in the status "Up" with the VPN peer:
      i. Run:

      ```
      cpview
      ```

      ii. At the top, click **Advanced** tab > **SD-WAN** page.
      iii. Refer to the section **Overlay Probing Results** > column **State**.

d. Examine the routing table:

```
show route
```

After the previously active SD-WAN interface goes down, you must make sure that there is still another active route (either the default route or a static route) that includes the destination for the "Overlay" connection.

Without such an active route, the operating system cannot route the "Overlay" traffic.

The SD-WAN selects the route to the "Overlay" destination (and not the operating system based on a static route).

This route in the operating system is necessary only for the "Overlay" traffic to flow from the inbound chain to the outbound chain, where the Security Gateway encrypts the traffic, and SD-WAN selects the best VPN transport to the VPN peer.

e. Examine the VPN connections and their VPN tunnels:

Syntax:

```
vpn tu conn <Source IP> <Source Port> <Destination IP>
<Destination Port> <Protocol>
```

Note - The minus character "-" is a wildcard "`any`".

For more information, refer to the *CLI Reference Guide* for your version > Chapter "**VPN Commands**" > Section "**vpn**" > Section "**vpn tu**".

Example 1:

```
vpn tu conn - - - - -
```

Example 2:

```
vpn tu conn 192.168.10.10 - 192.168.20.10 443 6
```

CPView shows that the "Overlay" probing state is "DOWN"

Symptom:

CPView > **Advanced** > **SD-WAN** page shows that the state of the "Overlay" probing is "DOWN".

Solution:

1. Make sure the nexthop device for the SD-WAN interface is up.
2. Connect to the command line on the Security Gateway.
3. Log in to Gaia Clish..
4. Make sure the VPN tunnel is established and "Up" from the SD-WAN interface to the required interface on the VPN peer:

   For more information about these commands, refer to the *CLI Reference Guide* for your version > Chapter "**VPN Commands**" > Section "**vpn**" > Section "**vpn tu**".

   a. Run:

   ```
   vpn tu
   ```

   and enter the digit **2** for the option "**List all IPsec SAs**".

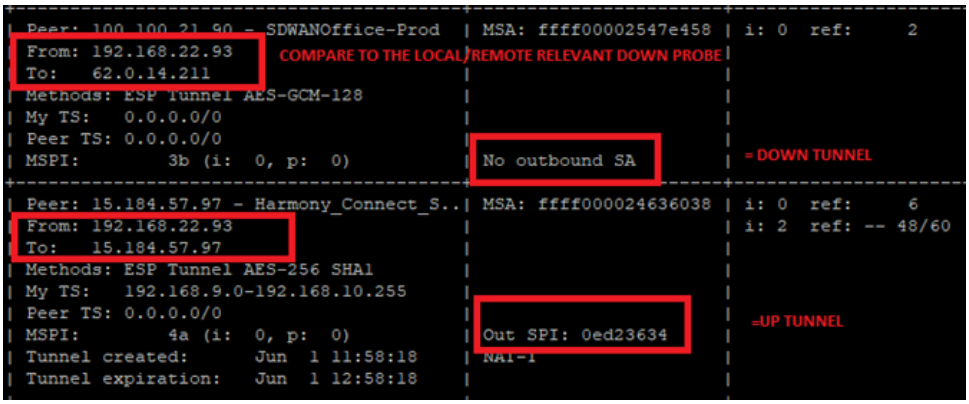
b. Run:

```
vpn tu tlist
```

If the command output does **not** show Outbound SA or IPsec SA, then the VPN tunnel is "down".

Example of a "`vpn tu tlist`" output:

- The top section shows "`No outbound SA`". Meaning, this VPN tunnel is "down".
- The bottom section shows a value in the "`Out SPI`" field. Meaning, this VPN tunnel is "up".



c. Run:

```
vpn tu conn <Source IP Address> - <Destination IP Address> - 1
```

Note - The minus character "-" is a wildcard "`any`" because ICMP does not use traffic ports.

Example: `vpn tu conn 192.168.3.57 - 172.16.4.68 - 1`

Run this command with the IP addresses of the overlay probing connection that is down.

The connection must be encrypted and must pass through a VPN tunnel that is "up".

5. If the VPN tunnel is "down", then understand why:

a. Examine the Security Gateway logs in SmartConsole / SmartView.

   Filter for the applicable Source IP address, Destination IP address, and Ports 500 (IKE) and 4500 (NAT-T).

   Determine whether the VPN peers send and respond to the IKE negotiation traffic.

b. Capture the traffic on the Security Gateway with FW Monitor (sk30583).

   Filter for the applicable Source IP address, Destination IP address, and Ports 500 (IKE) and 4500 (NAT-T).

   Determine whether the VPN peers send and respond to the IKE negotiation traffic.

c. Examine the Security Gateway logs in SmartConsole / SmartView.

   Filter for the action "`Key Install`".

   Determine the reason for the failure. For example, an invalid IPsec certificate. The Source IP address of a VPN Gateway is not known to its VPN peer (Invalid ID).

   For additional information, see: sk164840, sk88780, sk112054.

d. Collect the VPN debug as described in sk180488.

e. Contact *Check Point Support* and include the CLI outputs, VPN debug outputs, and log files.

6. If VPN tunnel is "up", but CPView shows it as "down", then the Security Gateway does not receive the ICMP Replies from the VPN peer.

   a. Make sure the Security Policy on each VPN peer explicitly allows the ICMP Echo Request traffic between these VPN peers on their external interfaces.

   b. Make sure the SD-WAN Policy:

      i. Matches the ICMP Echo Request traffic between these VPN peers on the "Overlay" steering object.

      ii. Has all available WAN interfaces selected.

   c. Make sure the Encryption Domain of the Security Gateway does not include the subnets of the SD-WAN peer.

      If the Encryption Domain contains the VPN peer subnets, the Security Gateway does not encrypt the traffic it sends to the VPN peer.

   d. Capture the traffic on the Security Gateway with FW Monitor (sk30583).

Use the "-F" parameter to filter for the ICMP package between the Security Gateway and its VPN peer.

Example syntax (port "0" means "any"):

```
fw monitor -F "192.168.22.33,0,141.10.60.1,0,1" -F
"172.20.44.55,0,192.168.22.33,0,1"
```

The FW Monitor traffic capture must show:

i. The ICMP Echo Request traffic from the Security Gateway (encrypted in the Pre-Outbound chain "oE") to the VPN peer.

ii. The ICMP Echo Reply traffic from the VPN peer to the Security Gateway (decrypted in the Pre-Inbound chain "iD").

If this ICMP traffic is **not** encrypted, then:

i. In SmartConsole, examine the Access Control policy.

   Make sure there is an explicit rule to accept this ICMP traffic.

ii. Open the Security Gateway object > expand **Network Management** > click **VPN Domain**.

   Make sure you did not exclude the external interface that establish the VPN tunnel from the VPN Domain.

iii. Make sure you did not exclude this ICMP traffic in the `crypt.def` file (see sk25675).

iv. Make sure you did not exclude this ICMP traffic in the corresponding VPN Community object on the **Excluded Services** page.

If the ICMP Echo Reply traffic from the VPN peer to the Security Gateway does not get to the Post-Inbound chain "I", then determine why the Security Gateway drops it:

i. Examine the Security Gateway logs in SmartConsole / SmartView.

ii. Collect the kernel debug:

   For more information about the kernel debug procedure on a Security Gateway, see the *Check Point Firewall Guide* for your version > chapter "Kernel Debug".

   ```
   fw ctl zdebug -m fw + drop | grep 'value'
   ```

CPView does not show the "Overlay" steering objects

Symptom:

CPView > **Advanced** > **SDWAN** > **Probing** > the section "**Steering Objects Results**" does not show the "Overlay" steering objects.

Cause:

This is by design.

CPView shows only the "Local Breakout" and "Backhaul" steering objects.

FW Monitor traffic capture of the "Overlay" traffic does not show the expected outbound interface on Post-Outbound chain "O"

Symptom:

FW Monitor (sk30583) traffic capture of the "Overlay" traffic between a client and a server does not show the expected outbound interface on Post-Outbound chain "`O`".

Cause:

FW Monitor shows the outbound interface based on the routing table.

This does not mean that it was the actual interface that routed the packet.

Solution:

To see the real interface that routed the traffic, do **one** of these:

- In the applicable Security Gateway logs, examine the "**SD-WAN**" section.
- Capture the ESP / NAT-T traffic with the CPPCAP tool (sk141412) in the Expert mode:

  ```
  cppcap -i <Name of Interface> -f "esp or port 4500" -o
  /var/log/cppcap_ESP_NATT.cap
  ```

- Examine the VPN connections and their VPN tunnels:

  Syntax:

  ```
  vpn tu conn <Source IP> <Source Port> <Destination IP>
  <Destination Port> <Protocol>
  ```

  Note - The minus character "`-`" is a wildcard "`any`".

For more information, refer to the *CLI Reference Guide* for your version > Chapter "**VPN Commands**" > Section "**vpn**" > Section "**vpn tu**".

Example 1:

```
vpn tu conn - - - - -
```

Example 2:

```
vpn tu conn 192.168.10.10 - 192.168.20.10 443 6
```

Expected VPN Transports to VPN Peers are missing from the list

Symptom:

- CPView > **Advanced** > **SDWAN** > **Probing** > the section "**Overlay Probing Results**" does not show the expected VPN Transports to VPN peers.
- Check Point Portal > **SD-WAN** > **Monitor** view > **Dashboard** page > **Overlay Tunnels Monitoring** tab does not shows the expected VPN transports to VPN peers.

For example, there are no VPN transports to a specific VPN Peer, or to a specific interface of a VPN peer.

The kernel debug "`fw ctl zdebug -m fw + drop`" on the Security Gateway (see *"Troubleshooting SD-WAN with Kernel Debug" on page 385*) may show these traffic drops between the IP addresses of the interfaces on the local Security Gateway and the IP addresses of the interfaces on the VPN Peer Security Gateway:

```
fw_log_drop_ex: Packet proto=1 <Local IP Address>:0 ->
<Peer IP Address>:<Port> dropped by vpn_encrypt_chain
Reason: encrypt drop; sdwan_get_vpn_transport_id: Could
not find transport id, vpn_transport=[<Peer IP
Address>, 12, <Peer IP Address>] kiss_htab_bl_get_ret_
val=-1 (_set1); vpn_sdwan_get_transport: Could not find
transport entry in defaults transports for peer gateway
<Peer IP Address>, conn=<dir 1, <Local IP Address>:0 ->
<Peer IP Address>:<Port>IPP 1> rule_uuid=<UUID>.;
```

Solution:

1. In SmartConsole, make sure the names of interfaces in the object of each involved VPN Peer Security Gateway match the names of interfaces in the Operating System.
   - In the object for a Security Gateway that runs the Gaia OS, go to the page **Network Management**.
   - In the object for a Spark Firewall Appliance that runs the Gaia Embedded OS, go to the page **Topology**.

   Important - In a cluster object, the names of the Cluster Virtual Interfaces must be identical to the corresponding physical / virtual interfaces on the cluster members. For example, if you paired the interfaces on cluster members with the names "`eth1`", then the Cluster Virtual Interface must also have the name "`eth1`".
2. In SmartConsole, make sure the involved VPN Peer Security Gateways / Clusters participate in the correct VPN Community.

3. Make sure the involved VPN Peer Security Gateways / Cluster Members have SD-WAN enabled and the Nano-Agent is running and communicating with the Internet:

   Note - In a cluster, run these commands on **each** cluster member.

   a. Run:

   ```
   cpsdwan stat
   ```

   The output must show the SD-WAN policy is installed.

   b. Run:

   ```
   cpnano -s
   ```

   The output must show the SD-WAN Nano-Services are **running**, and the connectivity to the Internet did not fail.

4. If you recently made changes in the objects of the involved VPN Peer Security Gateways / Clusters, then install the Access Control policy on each VPN Peer Security Gateway / Cluster.

5. On each VPN Peer Security Gateway / Cluster Member, run:

   ```
   jq . $FWDIR/state/local/SDWAN/sdwan_steering_policy.json
   ```

   The output must show the relevant Security Gateway / each relevant Cluster Member in the section "`sdwan_steering_vpn_peers`".

   a. If the VPN peer does not appear in the output at all, it most probably means one of these (other causes are also possible):

   - The local Security Gateway / Cluster does not have the SD-WAN information about that VPN peer from Check Point Portal.
   - The local Security Gateway / Cluster does not participate in the same VPN community with this VPN peer.

b. If the VPN peer appears in the output, then in the section of this VPN peer, the sub-section "`interfaces`" must show the configured interfaces and must show the "Circuit ID" number for each interface.

   Important - Make sure the same interface name appears in all these places:
   i. In the Gaia operating system on the Security Gateway / each Cluster Member.
   ii. In SmartConsole > Security Gateway / Cluster object > **Network Management** page.
   iii. In the `sdwan_steering_policy.json` file > in the section "`interfaces`" > in the "`name`" value.

c. In the upper section of the output, the section "`sdwan_steering_vpn_local`" must show the configured interfaces and must show the "Circuit ID" number for each interface for the local Security Gateway / Cluster Member.

d. When the VPN Peer Security Gateways / Clusters are managed by the same Security Management Server / Domain Management Server:

   - The section "`sdwan_steering_vpn_local`" and the section "`sdwan_steering_vpn_peers`" must show the same "`Domain UUID`" value. If the value is not the same in these sections, then these VPN Peers behave if they are managed by different Management Servers.
   - If you configured a Global VPN Community on a Multi-Domain Security Management Server, and the VPN Peer Security Gateways / Cluster are managed by different Domain Management Servers:
     - The section "`sdwan_steering_vpn_local`" and the section "`sdwan_steering_vpn_peers`" will show different "`Domain UUID`" values.
     - The section "`sdwan_steering_vpn_peers`" will show the names of interfaces on the VPN peers managed as "`ifc-<Number>`".

     Support for "Overlay" in a Global VPN Community is available in:
     - R82 and higher
     - R81.20 Jumbo Hotfix Accumulator Take 79 and higher
     - Spark Firewall R81.10.15 and higher

Important:
- If the "`Circuit ID`" numbers for the local Security Gateway / Cluster Member and for the VPN Peer are different, then the VPN Transport cannot be created between them. This is by design.
- It is **not** supported to use a dummy object that represents a Management Server.
  For example, in the Security Gateway / Cluster object properties > on the **Fetch Policy** page.

6. Examine the `$FWDIR/log/sdwan_steering.elg` file for errors about the VPN Peer.
7. Examine the VPN tunnel details with dedicated tools:
   a. Run:

   ```
   vpn tu tlist
   ```

   The output must show tunnels with "`From:`" and "`To:`" fields indicating the SD-WAN interfaces on the local Security Gateway / Cluster Member and on the VPN Peer.

   b. Run:

   ```
   vpn tu conn - - - - -
   ```

   The output must show connections that are passing between these:
   - Encryption Domain of the local Security Gateway / Cluster Member
   - Encryption Domain of the VPN Peer

   The output must show connections with "`From:`" and "`To:`" fields indicating the SD-WAN interfaces on the local Security Gateway / Cluster Member and on the VPN Peer.

   If the above dedicated tools show the VPN tunnels and VPN connections, then this may be a display issue in the CPView tool.
8. If the issue persists, then contact *Check Point Support* and include these files from each the involved Security Gateway:
   a. CPinfo file (sk92739)
   b. `$FWDIR/log/sdwan_steering.elg`
   c. `$FWDIR/log/cpsdwan.elg`
   d. `$FWDIR/state/local/SDWAN/sdwan_steering_policy.json`

e. `/var/log/nano_agent/cp-nano-sdwan.dbg`

f. `/var/log/nano_agent/cp-nano-orchestration.dbg`

g. Run this command and include the output file "`/var/log/vpn_tu_tlist.txt`":

```
vpn tu tlist >> /var/log/vpn_tu_tlist.txt
```

h. Run this command and include the output file "`/var/log/vpn_tu_conn.txt`":

```
vpn tu conn - - - - - >> /var/log/vpn_tu_conn.txt
```

i. Screenshot from CPView:

   i. Run: `cpview`

   ii. At the top, click **Advanced** > **SDWAN** > **Probing**.

   iii. If needed, scroll to down to the relevant section.

   iv. Take a screenshot - press the "**C**" key.

   v. Press the **CTRL+C** keys to exit the CPView tool.

   vi. Include the screenshot file "`cpview_<PID>.cap<Number>`"

   This file is created in the current working directory, in which you ran the `cpview` command.

   Example: `cpview_25117.cap0`

Significant increase in the CPU load on a Security Gateway after enabling SD-WAN "Overlay" with multiple VPN Peers

Symptoms:

After enabling SD-WAN "Overlay" on a Security Gateway, or after adding multiple SD-WAN VPN Peers:

1. Output of the "`top`" command shows significant increase in the CPU load in the processes "`fw_worker`".

   CPView (sk101878) > **CPU** > **Overview** shows significant increase in the CPU load in the "`CoreXL_FW`" instances.

2. Output of the "`fw tab -t connections -u -s`" command (see sk65133) shows significant increase in the number of concurrent connections (the `#VALS` column).

3. Output of the "`fwaccel conns`" command shows that ICMP connections are forwarded to the Firewall kernel.

Cause:

1. Each SD-WAN "Overlay" Peer sends ICMP Echo Request packets to probe the configured next hop (see *"SD-WAN Probing" on page 238* and *"Configuring Steering Behavior" on page 171*).

2. When the value of the kernel parameter "`fw_allow_simultaneous_ping`" is set to "1" (one), the Security Gateway handles each ICMP Echo Request packet as a new ICMP connection. Therefore, the Security Gateway does not accelerate these ICMP connections in SecureXL, but forwards them to the Firewall kernel for complete inspection.

Important - Understand why the value of this kernel parameter was set to "1". There are cases when this value is required, so traffic sent directly to Cluster Members over a Site to Site VPN tunnel can reach them. See sk26874.

Solution:

1. Connect to the command line on the Security Gateway.

2. Log in to Gaia Clish or the Expert mode.

3. Get the current value of the kernel parameter "`fw_allow_simultaneous_ping`":

   ```
   fw ctl get int fw_allow_simultaneous_ping
   ```

4. If the current value of this kernel parameter is "1" (one), then set its value to "0" (zero) temporarily:

```
fw ctl set int fw_allow_simultaneous_ping 0
```

5. Examine the CPU load in one of these ways:
   - Run "`cpview`" > go to **CPU** > **Overview** > examine the CPU load in the "`CoreXL_FW`" instances.
   - Run "`top`" > examine the CPU load in the processes "`fw_worker`".
6. To set the value of this kernel parameter to "0" (zero) permanently, run:

```
fw ctl set -f int fw_allow_simultaneous_ping 0
```

Route-Based VPN traffic that is routed towards a VTI is not encrypted and is sent in clear-text

Symptoms:

- Traffic that should be routed through the VTI is not encrypted and is sent in clear-text.
- Local outgoing connections from the SD-WAN Security Gateway's VTI to the remote VPN peer's VTI (for example, BGP traffic) are not encrypted and are sent in clear-text.
- Kernel debug on the SD-WAN Security Gateway may show this message (when the debug flag "`fw ctl debug -m VPN + policy`" is enabled):

  ```
  init_encryption_params: Traffic accepted by a breakout rule - change to clear
  ```

Cause:

The traffic is matching a Local Breakout rule, which by design disables VPN encryption.

Solution:

Make sure that all VPN traffic matches an SD-WAN rule with the "**Overlay**" behavior and not with the "**Internet** > **Local Breakout Only**" behavior.

Overlay traffic is not working through Site-to-Site VPN between SD-WAN Peers

Environment:

- Product: Security Gateway / Spark Firewall
- Features:
  - SD-WAN Overlay (Site-to-Site VPN over multiple transports)
  - IPSec VPN (Domain-Based VPN or Route-Based VPN)

Symptom:

- Some or all Overlay connections do not pass over a Site-to-Site VPN between SD-WAN peers.
- Applications that should use Overlay (encrypted via SD-WAN transports) fail, or time out.
- SD-WAN Overlay transports appear configured, but specific connections do not work as expected.

Troubleshooting:

Run the following checks on both peers, filtering the same connection on both sides.

Examine the packet path with the FW Monitor

On each Security Gateway, run (see the *CLI Reference Guide* for your version > "fw monitor"):

```
fw monitor -F "192.168.1.1,0,192.168.2.1,0,0" -F
"192.168.2.1,0,192.168.1.1,0,0"
```

In the filters, replace the example IP addresses with your applicable source and destination IP addresses.

Examine how the packet passes through the inspection points in the Security Gateway:

- "`i`" - Packet is entering from NIC (pre-inbound)
- "`I`" - Packet is after the inbound chain (post-inbound)
- "`o`" - Packet is before the outbound chain (pre-outbound)
- "`O`" - Packet is leaving NIC (post-outbound) - should be "`Oe`" for encrypted traffic

Scenario 1 - packet passes only the "i" chain (no "I", "o", "O")

Cause:

The Security Gateway probably dropped this packet.

If the connection appears only at the "i" inspection point, it usually means the packet was dropped very early (unless destination NAT changes the destination IP address, so it no longer matches your "fw monitor" filter).

Next steps:

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Start the script capture:

   ```
   script /var/log/drops.txt
   ```

4. Run the kernel debug for drops:

   ```
   fw ctl zdebug + drop
   ```

5. Reproduce the problematic connection.
6. Stop the script capture.

   Press the CTRL+D keys.

7. Examine the output file for relevant drops:

   ```
   /var/log/drops.txt
   ```

If you see this line:

```
vpn_sdwan_get_transport: Could not find SD-WAN rule uuid for
connection <connection>;
```

this means:

- There is no SD-WAN rule match for this connection.
- Because Overlay traffic requires an SD-WAN rule, the packet is dropped.

Additional prints that can indicate the same issue - usually requires further verification in a full kernel debug (see *"Troubleshooting SD-WAN with Kernel Debug" on page 385*):

`fw_log_drop_ex: <connection> dropped by vpn_drop_and_log`
`fw_log_drop_ex: <connection> dropped by vpn_encrypt_chain_ reason: encrypt drop`
`fw_log_drop_ex: <connection> dropped by vpn_drop_and_log Reason: Failed to process the first VPN packet`
`fw_log_drop_ex: <connection> dropped by vpn_drop_and_log Reason: Failed to enforce VPN policy (11)`

In such cases, the Security Gateway log in SmartConsole may show the action as "**Accept**" instead of "**Encrypt**".

Solution:

1. Make sure your SD-WAN rule base covers this traffic with an Overlay steering object.
2. Verify that:
   a. Source, destination, services, and applications match the Overlay rule.
   b. The SD-WAN profile that contains this rule is correctly assigned to both peers.
   c. You can verify the rule match for this connection with this command in the Expert mode:

```
fw ctl zdebug -m SDWANRB all | grep PROB
```

Scenario 2 - packet passes only the "i", "I" chains (no "o", "O")

Cause:

- The operating system on the Security Gateway does not have a route to the destination.
- There is no routed outbound interface, so the Security Gateway cannot forward the packet.
- For the R82 Security Gateway that runs SecureXL in the UPPAK mode, there may be a route to the destination that points to a dead next hop (no ARP resolution).

Next steps:

1. Connect to the command line on the Security Gateway.
2. Log in to Gaia Clish.
3. Examine the static routes:

   ```
   show route
   ```

Solution:

1. Ensure you have default routes with different priorities for all your ISPs.
2. If needed, add specific routes to all Overlay networks via private links (for example, MPLS interfaces).
3. In Route-Based VPN setups, make sure routes to remote Overlay networks point to the VTI interfaces that connect to the VPN peer.
4. For the R82 Security Gateway that runs SecureXL in the UPPAK mode, make sure that the active route points to a live next hop.

Scenario 3 - packet passes only the "i", "I", "o" chains (no "O")

Cause:

The Security Gateway stops processing the packet during the outbound - before it could send it / encrypt it (unless source NAT changes the source IP address and your "`fw monitor`" filter no longer matches).

To see where exactly the Security Gateway stops processing the packet, add "`-p all`" in the syntax:

```
fw monitor -p all -F "192.168.1.1,0,192.168.2.1,0,0" -F
"192.168.2.1,0,192.168.1.1,0,0"
```

In the filters, replace the example IP addresses with your applicable source and destination IP addresses.

Warning - This syntax prints many lines. This increases the CPU utilization on the Security Gateway.

Use this "`fw monitor`" syntax together with a full kernel debug (see *"Troubleshooting SD-WAN with Kernel Debug" on page 385*) to understand where and why the connection stops (for example, VPN policy, routing, SD-WAN).

Scenario 4 - packet passes all the chains "i", "I", "o", "O", "Oe"

This usually indicates that the Security Gateway routed and encrypted the packet.

In rare cases, even when the packet reaches the "Oe" chain, it may still fail to be encrypted at a later stage. In such scenarios, a relevant drop is usually visible when running:

```
fw ctl zdebug + drop
```

For these cases, collect a full kernel debug together with VPN debug.

To confirm that the packet was successfully encapsulated and sent over the wire, run the `tcpdump` command on both sides for ESP or NAT-T packets that carry the encapsulated traffic. This helps verify that the packet was transmitted and whether it was received by the peer gateway.

Confirm the encryption also with the "vpn tu conn" command while reproducing the problematic connection

Syntax:

```
vpn tu conn <Source IP> <Source Port> <Destination IP>
<Destination Port> <Protocol>
```

Note - The minus character "-" is a wildcard "any".

For more information, refer to the *CLI Reference Guide* for your version > Chapter "**VPN Commands**" > Section "**vpn**" > Section "**vpn tu**".

The output for a normally encrypted connection should look similar to this:

```
instance <X>: 'src=[<IP>,<sport>], dest=[<IP>,<dport>],
<Protocol>' Encrypted
+--------------------------------------+------------------
----+---------------------+
| Peer: <Main Peer IP> - <Peer Name>      | MSA: XXXXXXXXXX
   | i: 1  ref:     X    |
| From: <Local Tunnel Interface IP>       |
   | i: 3  ref:     X    |
| To:   <Remote Tunnel Interface IP>      |
   |                      |
| Methods: ESP Tunnel PFS AES-256 SHA1 g..|
   |                      |
| My TS:  x.x.x.x/x                       |
   |                      |
| Peer TS: x.x.x.x/x                      |
   |                      |
| MSPI:    XXXXXX (i:  1, p:  0)          | Out SPI: XXXXXX
   |                      |
| Tunnel created:      <DATE,TIME>        | [Optional:NAT-T]
   |                      |
| Tunnel expiration:   <DATE,TIME>        |
   |                      |
+--------------------------------------+------------------
----+---------------------+
```

On the receiving Security Gateway, the "`vpn tu conn`" command will show the tunnel details for the reply packets of this connection.

Based on the "`vpn tu conn`" output, follow the applicable scenario below.

The "`vpn tu conn`" output shows "`From`" and "`To`" fields and valid "`Out SPI`"

If the "`vpn tu conn`" output shows:

1. The "`From`" and "`To`" fields (then this is a Tunnel Per Interface (TPI) transport - the **SDWAN**-style)
2. A valid "`Out SPI`"

then the traffic is encrypted.

If the connection still does not work:

1. Run the "`fw monitor`" command on both Security Gateways to see where packets or replies are failing.

2. Run the "`tcpdump`" command on both Security Gateways to make sure the ESP / NAT-T packets (encapsulated data) reach the other side without loss.
3. Collect a full kernel debug on both Security Gateways (see *"Troubleshooting SD-WAN with Kernel Debug" on page 385*).

The "`vpn tu conn`" output does not show "`From`" and "`To`" fields

If the "`vpn tu conn`" output does not show the "`From`" and "`To`" fields, this tunnel is using the Legacy Link Selection (not the SD-WAN TPI Overlay)

1. Verify the peer is identified as an SD-WAN Peer in:

   CPView (sk101878) > **Advanced** > **SD-WAN** > **Overlay probing results**
2. If the CPView does not show the peer, refer to:

   "Troubleshooting SD-WAN "Overlay"" on page 340

The "`vpn tu conn`" output shows "`From`" and "`To`" fields, does not show valid "`Out SPI`", shows tunnel state as "`Disconnected`

If the "`vpn tu conn`" output:

1. Show the "`From`" and "`To`" fields
2. Does not show a valid "`Out SPI`"
3. Shows the tunnel state as "`Disconnected`"

then the VPN tunnel is Down, and the connection is still trying to use it.

In the "`fw ctl zdebug + drop`" output you will see drops like this:

```
dropped by fw_ipsec_encrypt_on_tunnel_instance Reason: No
error - tunnel is not yet established
```

Troubleshooting:

1. Check if other TPI tunnels to this peer are connected:

   ```
   vpn tu tlist -p <Main IP address of Peer>
   ```

   If there are other connected TPI tunnels, the connection should have used them:

   a. Make sure the traffic is covered by an Overlay steering object that uses all available WAN links.

b. If CPView (sk101878) > **Advanced** > **SD-WAN** > **Overlay probing results** shows all transports to this peer as "`DOWN`", even though there are VPN tunnels in the status "`UP`" (as the "`vpn tu tlist`" command shows), this can explain why a random tunnel is chosen for a connection. In this case, follow *"Troubleshooting SD-WAN "Overlay"" on page 340*.

2. If there are no other connected tunnels to this peer:

   a. Capture the IKE negotiation traffic on both peers:

   ```
   tcpdump -nnei <Name of Interface> host <IP Address of Tunnel Peer> and port 500 or port 4500
   ```

   b. Verify:

      i. No NAT is applied on outbound IKE packets:

         i. Source IP address is as expected.

         ii. Source ports remain 500 / 4500 (not translated to a high port).

      ii. All packets flow in both directions.

      iii. No drops for IKE packets ("`fw ctl zdebug + drop`").

   c. Collect the VPN debug on both sides:

      - For Security Gateways follow, sk180488
      - ForSpark Firewall Appliances, follow sk62482

   d. Contact *Check Point Support* to investigate the IKE negotiation issue.

The "`vpn tu conn`" output shows "`instance <X> ... Clear`"

Make sure the traffic is not matching these:

- Implied rules.
- Services that you excluded in the settings of the applicable VPN Community.

If it is unclear why the traffic is handled in clear, enable the kernel debug. For more information, see the *Check Point Firewall Guide* for your version > chapter "Kernel Debug".

If the "`vpn tu conn`" output shows:

```
instance <X>: 'src=[<IP>,<sport>], dest=[<IP>,<dport>], TCP'
Clear
```

instead of:

```
instance <X>: 'src=[<IP>,<sport>], dest=[<IP>,<dport>], TCP'
Encrypted
```

this means the Security Gateway did not attempt to encrypt the connection, and sent the traffic in clear.

Troubleshooting:

- For Domain-Based VPN, make sure the applicable source IP address and destination IP address are included in the VPN Domains on both peers:

  ```
  fw tab -t vpn_routing -u
  ```

- For Route-Based VPN:
  - Make sure the destination IP address is routed through the VTI of the VPN peer.

    Run in Gaia Clish:

    ```
    show route
    ```

  - In the "`fw monitor`", the outbound interface (`o`, `O`) should be the VTI.
  - Make sure the VTI is valid. Otherwise, the Security Gateway drops the traffic ("`fw ctl zdebug + drop`").
  - SD-WAN Local Breakout Only - make sure the connection is not matching a Local Breakout Only steering object that forces clear-text routing instead of VPN / Overlay for Route-Based VPN.
    - Check the SD-WAN rule matching for the connection in the Expert mode:

      ```
      fw ctl zdebug -m SDWANRB all | grep PROB
      ```

    - Verify the connection matches the expected Overlay rule.

Collecting the kernel debug when everything looks OK, but traffic still does not pass

Use this procedure when:

- There are VPN tunnels in the status "UP" to the VPN peer.
- The VPN peer is identified as an SD-WAN peer.
- But Overlay traffic still does not work as expected.

Follow the instructions in *"Troubleshooting SD-WAN with Kernel Debug" on page 385*.

Troubleshooting SD-WAN "Backhaul Only" / "Prioritize Local Breakout"

For background information, see *"SD-WAN Connection Type - "Internet"" on page 188*.

After configuring "Backhaul", my Branch Gateway (local connections) tries to access the Internet from the Center Gateway over the VPN tunnel. How to configure it to use the local Internet lines?

In Check Point Portal > **SD-WAN** application, create this rule in the **Network** view > **SD-WAN Policy** page and click **Enforce** at the top:

Name	Source	Destination	Services & Applications	Behavior	Enforcement
Backhaul bypass encryption	Security Gateway object	SD-WAN Internet	Applicable objects	Steering behavior object that is configured with one of these: ■ Local Breakout Only ■ Prioritize Local Breakout	Security Gateway object

Notes:

- This configuration only overrides the encryption for local connections.
- To send traffic for local connections, the Security Gateways uses the Gaia OS routing table (not the "Local Breakout" mechanism).

The Security Gateway drops SSH / Gaia Portal access from the Internet with the log "Cleartext traffic should be encrypted"

When in the Star VPN Community > **VPN Routing** page you select the option "**To center, or through the center to other satellites, to internet and other VPN targets**", the Security Gateway expect all traffic that originates from outside its VPN Domain to be encrypted.

To allow specific traffic to your Security Gateway from the Internet, these options are available:

- Exclude specific ports, if applicable, in the Star VPN Community > **Excluded Services** page.
- Follow sk25675.

Important - If you use SD-WAN "Overlay", then do **NOT** select the option "**Exclude gateway's external IP addresses from the VPN Domain**" in the Security Gateway object > "**Network Management**" section > "**VPN Domain**" page. This option interrupts the "Overlay" probing mechanism.

What is the correct NAT and Access configuration on Branch and Center Gateway in SD-WAN "Backhaul"?

Follow these steps in SmartConsole:

1. Configure the Network object:
   a. Open the **Network** object that represents your Branch LAN network.
   b. In the left panel, click the **NAT** page.
   c. Select **Add automatic address translation rules**.
   d. In the **Translation method** field, select **Hide**.
   e. Select **Hide behind the gateway**.
   f. In the **Install on gateway** field, select **All** (to include the Branch Gateway and the Center Gateway).
   g. Click **OK**.

   Best Practice - applies only to R82 and higher, and to R81.20 Jumbo Hotfix Accumulator, Take 41 or higher:
   If it is necessary for the Center Gateway to detect the original source IP address of the Branch local connections, then in the VPN Community object > **Advanced** page, select the option **Disable NAT inside the VPN community**.
2. Configure the Access Control for the Branch Gateway:

   Allow traffic from the Branch network to the Internet.
3. Configure the Access Control for the Center Gateway:

   Allow traffic from the Branch network to the Internet.
4. Install the Access Control policy for the Branch Gateway.
5. Install the Access Control policy for the Center Gateway.

If it is necessary to perform Hide NAT on the Branch Gateway when it sends traffic to the Internet (towards the Center Gateway):

1. Configure the VPN Community object:
   a. Open the VPN Community object.
   b. On the **Advanced** page, clear the option **Disable NAT inside the VPN community**.
   c. Click **OK**.
2. Configure the Access Control for the Center Gateway:

Allow traffic from the Branch Gateway to the Internet.

3. Configure the Branch Gateway object:
   a. Open the Branch Gateway object.
   b. In the **NAT** section, click the **Advanced** page.
   c. Select **Add automatic address translation rules to hide this Gateway behind another Gateway**.
   d. In the **Translation method** field, select **Hide**.
   e. Select **Hide behind Gateway**.
   f. In the **Install on gateway** field, select **All** (to include the Branch Gateway and the Center Gateway).
   g. Click **OK**.
4. Install the Access Control policy for the Branch Gateway.
5. Install the Access Control policy for the Center Gateway.

The Branch Gateway lost access to Smart-1 Cloud and to Identity and Trust. Not possible to fetch policy from the cloud.

1. Examine the VPN connections and their VPN tunnels - is the traffic to Check Point Portal sent encrypted?
   a. Connect to the command line on the Branch Gateway.
   b. Log in to the Expert mode.
   c. Run this command with the applicable filters:

   ```
   vpn tu conn <Source IP> <Source Port> <Destination IP>
   <Destination Port> <Protocol>
   ```

   Note - The minus character "-" is a wildcard "`any`".

   For more information, refer to the *CLI Reference Guide* for your version > Chapter "**VPN Commands**" > Section "**vpn**" > Section "**vpn tu**".
2. If the traffic is encrypted, then investigate why does not it pass (a VPN tunnel is down? traffic is dropped? and so on).
3. If the VPN tunnel is down, and you must make changes in the policy, then you can:
   a. Completely unload the current security policy.
   b. Make the required changes in the policy.
   c. Install the policy on the Branch Gateway.

   Steps:
   a. Connect to the command line on the Branch Gateway - either through the Console port, or through the LOM Card if installed.
   b. Log in.
   c. Disconnect all networks from the Branch Gateway, except the connection to the Internet (to Check Point Portal).

d. Unload the current security policy:

```
fw unloadlocal
```

Warnings:

- The "`fw unloadlocal`" command prevents all traffic from passing through the Security Gateway (Cluster Member), because it disables the IP Forwarding in the Linux kernel on the Security Gateway (Cluster Member).
- The "`fw unloadlocal`" command removes all policies from the Security Gateway (Cluster Member). This means that the Security Gateway (Cluster Member) accepts all incoming connections destined to all active interfaces without any filtering or protection enabled.

For more information, refer to the *CLI Reference Guide* for your version > Chapter "**Security Gateway Commands**" > Section "**fw**" > Section "**fw unloadlocal**".

e. Make the required changes in the policy.

f. Install the policy on the Branch Gateway.

g. Examine the Access Control policy information on the Branch Gateway:

```
cpstat -f policy fw
```

h. Connect all networks to the Branch Gateway.

Troubleshooting SD-WAN in Check Point Portal

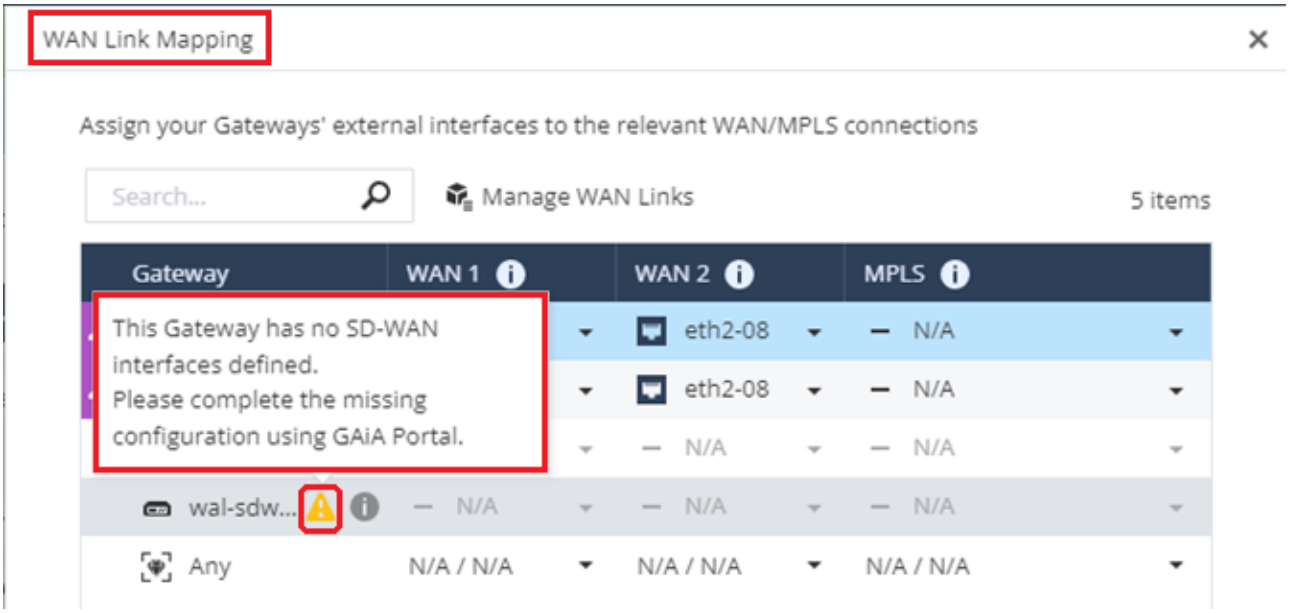
Warning "This Gateway has no SD-WAN interfaces defined. Please complete the missing configuration using GAIA Portal." in WAN Link Mapping

Symptom:

1. In the **WAN Link Mapping** window, the yellow triangle icon appears near an SD-WAN Security Gateway.
2. When you hover the mouse cursor over this icon, the information popup appears:

```
This Gateway has no SD-WAN interfaces defined. Please
complete the missing configuration using GAIA Portal.
```

Example:



Solution:

1. In Check Point Portal:
   a. In the **SD-WAN** application, go to the **Network** view > **Agents** page.
   b. At the top, click the **List View** button.
   c. The top section must show the SD-WAN Security Gateway object.
   d. Click the SD-WAN Security Gateway object.

e. The bottom section must show:

i. **Status: Connected**

ii. **Policy version: <Integer Value>**

2. In SmartConsole:

a. From the left navigation panel, click **Gateways & Servers**.

b. Open the Security Gateway object.

c. In the left pane, click **Network Management**.

d. Examine the configuration of interfaces:

- The names of interface (you can click **Get Interfaces** > **Get Interface with Topology** (do not click **Accept**) to see the actual interface names.
- The topology of the SD-WAN interfaces must be **External** (otherwise, they do not appear in the **WAN Link Mapping** window).

3. On the Security Gateway, examine the interface configuration in **one** of these ways:

- On the Security Gateway:
  - In Gaia Portal:

    Network Interfaces page > **SD-WAN Interfaces** section
  - In Gaia Clish:

    ```
    show interface <Name of Interface> sdwan
    ```

    or

    ```
    show configuration sdwan
    ```
  - In the Expert mode:

    ```
    sdwan_conf show
    ```

- On the Spark Firewall Appliance:

  Make sure you configured Internet connections in **one** of these ways:

  - In WebUI:

    Device view > **Network** section > **Internet**

  - In Gaia Clish:

    ```
    show internet-connections
    ```

  - In the Expert mode:

    ```
    sdwan_conf show
    ```

4. On the Security Gateway, examine the Nano-Agent status:
   a. Log in to the Expert mode.
   b. Run:

      ```
      cpnano -s
      ```

      All statuses must be **Succeeded** or **Running**.
5. On the Security Gateway, make sure the Access Control Policy is installed:

   ```
   cpstat -f policy fw
   ```

"WAN Link Mapping" window still shows an SD-WAN Security Gateway although its object was deleted in SmartConsole

Symptom:

In Check Point Portal > **SD-WAN** application > the **Network** view > **SD-WAN Policy** page > **WAN Link Mapping** window still shows an SD-WAN Security Gateway object, although an administrator deleted its object in SmartConsole.

Solution:

1. In Check Point Portal > **SD-WAN** application, delete the SD-WAN Security Gateway object from **all** profiles of type "**SD-WAN Profile**":
   a. Go to the **Network** view > **Profiles** page.
   b. Click a profile of type "**SD-WAN Profile**".
   c. Click the **General** tab.
   d. In the **SD-WAN Gateways** section, click the SD-WAN Security Gateway object.
   e. From the top toolbar, click **Delete** (the "x" icon).
2. In Check Point Portal > **SD-WAN** application, delete the SD-WAN Security Gateway object from the **Agents** page:
   a. Go to the **Network** view > **Agents** page.
   b. Delete the SD-WAN Security Gateway object:
      - In the Grid View:

        In the SD-WAN Security Gateway object, in the top right corner, click the 3-dots and click **Delete**.
      - In the List View:

        Click the SD-WAN Security Gateway object > from the top toolbar, click **Delete** (the "garbage can" icon).
3. At the top, click **Publish**.

Missing network objects in Check Point Portal SD-WAN

Symptom:

Some network objects are missing in Check Point Portal > **SD-WAN** application > **Network** view > **SD-WAN Policy** page > in the picker of the **Source** and / or **Destination** fields or rules.

Solution:

Make sure the required object appears in **SD-WAN** application > **Network** view > **Assets** page.

- The object appears on the **Assets** page:

  Contact *Check Point Support*.

- The object does **not** appear on the **Assets** page:

1. In SmartConsole, make sure this object exists.
2. In SmartConsole, make sure you published the session that created this object.
3. In SmartConsole, make sure the Management Server is connected correctly to Check Point Portal:
    a. From the left navigation panel, click **Infinity Services**.
    b. At the top of this page, the Check Point Portal Account must appear with the status **Active**.
    c. At the bottom of this page, **Configuration Sharing** must show:
        i. It is enabled (to verify, click the **Edit** button).
        ii. Its status is **Active** (green).
        iii. The last sync time is after the last publish.
    d. If **Configuration Sharing** shows the status "**Error**", or if the last sync is not up to date, then follow sk181504.
        - If sk181504 did not resolve the issue, or if your Management Server is Smart-1 Cloud, then contact *Check Point Support*.
        - If **Configuration Sharing** shows the status "**Active**", and the last sync time is after the last publish, but the issue persists, then contact *Check Point Support*.

Troubleshooting traffic that does not match SD-WAN rules

Symptom:

- In SmartConsole, the "**Accept**" / "**Encrypt**" log for the relevant connection shows no SD-WAN rule information, or an unexpected SD-WAN rule as the match.
- On the Security Gateway in Expert mode, the "`fw ctl zdebug -m SDWANRB + all | grep PROB`" command shows the connection with "`SD-WAN, no match`", or an unexpected SD-WAN rule match.
- The Security Gateway is enforcing the latest SD-WAN policy, as confirmed by `cpsdwan stat`.
- In SmartConsole -> Infinity Services tab, the **Configuration Sharing** is enabled, it's status is Active, the last sync time is after the last session publish & SD-WAN policy was enforced after the last sync. For Configuration sharing issues or missing objects see *"Missing network objects in Check Point Portal SD-WAN" on page 375*.

Scenario 1: Traffic Expected to Match an SD-WAN Rule with the SD-WAN Internet Special Object (destination)

Background:

The SD-WAN Internet object is a smart object that, from the gateway's perspective, excludes:

- Reserved IP address ranges.
- Directly connected networks.
- Local VPN Domain.
- Peer VPN Domains.

In other words Internet is "everything" minus reserved, local, and VPN-domain ranges.

Key behavior:

- If the connection destination IP falls inside the excluded ranges table, the traffic will not match the SD-WAN Internet object.
- If the connection source IP falls inside the SD-WAN Internet table, the traffic will not match the SD-WAN Internet object, even if the rule's Source column includes that source IP.

- If the traffic is subject to Destination NAT, SD-WAN matching is done against the post-NAT (translated) destination of the connection.

Notes:

- The Security Gateway runs a version that supports the SD-WAN Internet object.
- For more information, refer to *"Dynamic Objects in SD-WAN Policy" on page 163*.

Solution:

1. On-the-fly check: Is the destination IP address considered as "Internet"?

   a. To check if a specific destination IP address is treated as Internet by the Security Gateway, run in the Expert mode:

   ```
   fw ctl zdebug -m NRB + all | grep sdwanrb_is_ip_in_
   internet
   ```

   b. While this debug runs, initiate the problematic connection.

   You should see log lines showing the result of "`sdwanrb_is_ip_in_internet`" evaluation for the destination IP address.

2. To see the content of the kernel tables used by the SD-WAN Internet object, run on the Security Gateway in the Expert mode:

   ```
   fw tab -t sdwan_internet_ranges1 -u
   fw tab -t sdwan_internet_ranges2 -u
   ```

   Only one of these tables should contain data .

   If the destination IP address that you expect to be considered "Internet" is not in the table (or the table is empty), proceed with the steps below.

3. If the SD-WAN Internet Ranges table contain wrong data or is empty, run on the Security Gateway in the Expert mode:

   a. Start the SD-WAN Steering debug:

   ```
   fw debug sdwan_steering on TDERROR_SDWAN_SDWAN=3
   ```

   b. Fetch the SD-WAN policy again:

   ```
   cpsdwan fetch_local
   ```

c. Return the SD-WAN steering debug level to the normal value:

```
fw debug sdwan_steering on TDERROR_SDWAN_SDWAN=1
```

d. To check the SD-WAN steering log for Internet ranges calculation:

i. Open the `$FWDIR/log/sdwan_steering.elg` file.

ii. Search for: `SDWInternetRanges`

iii. Verify that the ranges make sense and include your expected Internet ranges.

e. Collect these log files for *Check Point Support*:

```
$FWDIR/log/sdwan_steering.elg*
```

Scenario 2: Traffic expected to match a rule with Dynamic Objects "My VPN Domain" / "Peer VPN Domain"

To collect SD-WAN policy direction files:

Background:

- "My VPN Domain" and "Peer VPN Domain" SD-WAN are dynamic objects that are populated from the kernel table "`vpn_routing`".
- The kernel table "`vpn_routing`" is built from the VPN Domain configuration in the Security Gateway objects, on the VPN Community objects, as well as from definitions in the relevant `*.def` files on the Management Server.

Notes:

- The Security Gateway runs a version that supports these dynamic objects.
- For detailed behavior and version support, refer to *"Dynamic Objects in SD-WAN Policy" on page 163*.

1. To check the content of these dynamic objects, run on the Security Gateway in the Expert mode:

a. Show the list of all dynamic objects:

```
dynamic_objects -l
```

b. Check if a specific destination IP address is listed in any of these dynamic objects:

```
dynamic_objects -ip <IP_ADDRESS>
```

If the IP address is included in the kernel table "vpn_routing" but not included in the expected dynamic object (for example, "My_VPN_Domain" or "Peer_VPN_Domain"), proceed to the next step.

2. To check the kernel table "vpn_routing", run on the Security Gateway:

   a. Show the entries in the kernel table:

   ```
   fw tab -t vpn_routing -u [-f]
   ```

   b. Verify if the problematic IP address is included in the "vpn_domain" range of the local Security Gateway, or the relevant remote SD-WAN peer.

   c. For remote peers, confirm if the peer is recognized as an SD-WAN peer:

   ```
   cpview
   ```

   Navigate to **Advanced** > **SD-WAN** > refer to **Overlay probing results**.

   If the peer is not identified as SD-WAN, its ranges will not be included in "Peer VPN Domain" dynamic object.

   d. If the IP address is missing from the right "vpn_domain" range in the kernel table "vpn_routing", change the VPN Domain configuration in SmartConsole for the local Security Gateway object, and/or the remote gateway / VPN Community.

   e. Install the Access Control policy.

   f. Check again.

   If the IP address is included in kernel table "vpn_routing" but not included in the expected dynamic object (for example, "My_VPN_Domain" or "Peer_VPN_Domain"), proceed to the next step.

3. IP address is included in the kernel table "vpn_routing" but is missing from Dynamic Objects.

   Note - Global ranges that are not explicitly defined, but are only implicitly derived from the third option in the VPN Routing tab of the VPN Community, are not added to the Peer VPN Domain dynamic object.

   If the IP address is present in the kernel table "vpn_routing", but does not appear in the relevant dynamic object, run on the Security Gateway in the Expert mode:

a. Start the SD-WAN steering debug:

```
fw debug sdwan_steering on TDERROR_SDWAN_SDWAN=5
```

b. Fetch the SD-WAN policy locally:

```
cpsdwan fetch_local
```

c. Return the SD-WAN steering debug level to the normal value:

```
fw debug sdwan_steering on TDERROR_SDWAN_SDWAN=1
```

d. Collect these log files for *Check Point Support*:

```
$FWDIR/log/sdwan_steering.elg*
```

Look for references such as "`CreateDynamicObject`" in the "`sdwan_steering.elg`" files.

Scenario 3: General Data Collection and Deep-Dive Debug

- Collect the directory with the SD-WAN policy direction files:
  `$FWDIR/state/local/SDWAN`

  You can inspect these files to look for the relevant IP range in the installed policy files.

  Note - IP addresses appear in policy files only when explicitly defined. IP addresses included via dynamic or special objects (for example, “My VPN Domain”, “Peer VPN Domain”, “SD-WAN Internet”) are translated on the gateway and therefore do not appear in the policy files.

  Download the original SD-WAN profile policy from Check Point Portal:

  1. From the left navigation panel, click **Network**.
  2. In the middle section, click **Profiles**.
  3. Click the relevant profile.
  4. Click **Advanced** tab.
  5. Click **Download**.

  Compare the SD-WAN policy on the Security Gateway with the profile in Check Point Portal.

- Kernel Debug for SD-WAN Rule Matching:

  Use this when traffic does not match the expected SD-WAN rule and policy or object checks give no explanation.

1. Connect to the command line on the Security Gateway.
2. Reset any previous debug configuration:

```
fw ctl debug 0
fw ctl set int simple_debug_filter_off 1
fwaccel dbg resetall
```

3. Allocate the debug buffer:

```
fw ctl debug -buf 8200
```

4. Enable the required kernel debug flags:
   a. FW module:

```
fw ctl debug -m fw + drop conn
```

   b. SDWAN module:

```
fw ctl debug -m SDWAN all
```

   c. SDWANRB module:

```
fw ctl debug -m SDWANRB all
```

   d. NRB module:

```
fw ctl zdebug -m NRB all
```

   e. If the issue involves an overlay (VPN) connection, also enable VPN module:

```
fw ctl debug -m VPN all
```

5. Enable the SecureXL Debug.
   a. Default module:

      ```
      fwaccel dbg -m default all
      ```

   b. SDWAN module:

      ```
      fwaccel dbg -m sdwan all
      ```

   c. If Overlay / VPN is relevant:

      ```
      fwaccel dbg -m vpn all
      ```

   d. Optional - API module for extra details:

      ```
      fwaccel dbg -m api all
      ```

6. Start the kernel debug:

   ```
   fw ctl kdebug -T -f > /var/log/kernel_debug.txt
   ```

7. Reproduce the issue - initiate the connection that does not match the expected SD-WAN rule.
8. Stop the kernel debug:

   Press the CTRL+C keys and run:

   ```
   fw ctl debug 0
   fwaccel dbg resetall
   ```

9. Collect the debug output files.

   Provide these files to *Check Point Support* for further analysis.

   Also mention the connection details that was tested during the kernel debug (source, destination IP, port, protocol).

   a. Kernel debug output:

   ```
   /var/log/kernel_debug.txt
   ```

   b. SD-WAN steering logs:

   ```
   $FWDIR/log/sdwan_steering.elg
   ```

   c. SD-WAN policy files - the entire directory `$FWDIR/state/local/SDWAN`

   d. Name of the relevant SD-WAN profile in Check Point Portal.

Troubleshooting SD-WAN with Kernel Debug

For complete information about the kernel debug procedure, see the *Check Point Firewall Guide* for your version > Chapter "Kernel Debug".

How to debug the traffic match to the SD-WAN Policy rules on an SD-WAN Security Gateway?

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Start the minimum kernel debug:

   ```
   fw ctl zdebug -m SDWANRB all | grep PROB
   ```

4. Press the **CTRL+C** keys to stop the kernel debug.

How to run the full kernel debug on an SD-WAN Security Gateway?

Warning - Schedule a maintenance window. This procedure significantly increases the load on the CPU of your Security Gateway.

Important:

- Always consult *Check Point Support* about the specific debug flags to troubleshoot your issue.
- To minimize the CPU load, do **not** capture traffic during this debug procedure.

Procedure:

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Reset the kernel debug options:

   ```
   fw ctl debug 0
   ```

4. Reset the kernel debug filter:

   ```
   fw ctl set int simple_debug_filter_off 1
   ```

5. Reset the SecureXL debug options:

   ```
   fwaccel dbg resetall
   ```

6. Allocate the debug buffer:

```
fw ctl debug -buf 8200
```

7. Configure the required kernel debug flags:
   a. Enable the debug flags in the "FW" module:

      ```
      fw ctl debug -m fw + drop conn route
      ```

      For VPN and NAT issues, **also** enable these debug flags in the "FW" module:

      ```
      fw ctl debug -m fw + vm xlate xltrc
      ```

   b. Enable the debug flags in the "SDWAN" module:

      ```
      fw ctl debug -m SDWAN all
      ```

   c. Enable the debug flags in the "SDWANRB" module:

      ```
      fw ctl debug -m SDWANRB all
      ```

   d. If the issue is related to an "Overlay" connection, then enable the debug flags in the "VPN" module:

      ```
      fw ctl debug -m VPN all
      ```

   e. **Optional:** Enable the debug flags in the "APPI" module to get more information:

      ```
      fw ctl debug -m APPI all
      ```

   f. **Optional:** Enable the debug flags in the "UP" module to get more information:

      ```
      fw ctl debug -m UP all
      ```

8. Configure the required SecureXL debug flags:
   a. Enable the debug flags in the "DEFAULT" module:

      ```
      fwaccel dbg -m default all
      ```

   b. Enable the debug flags in the "SDWAN" module:

      ```
      fwaccel dbg -m sdwan all
      ```

c. If the issue is related to an "Overlay" connection, enable the debug flags in the "VPN" module:

```
fwaccel dbg -m vpn all
```

d. **Optional:** Enable the debug flags in the "API" module to get more information:

```
fwaccel dbg -m api all
```

e. **Optional:** Only if your Security Gateway is **not** under a traffic load, enable the debug flags in the "PKT" module to get more information:

```
fwaccel dbg -m pkt all
```

9. Start the kernel debug:

```
fw ctl kdebug -T -f > /var/log/kernel_debug.txt
```

10. If the issue is related to an "Overlay" connection, then start the VPN debug in the user space as described in sk180488:

- Syntax for R81.20 and higher (regardless of a Jumbo Hotfix Accumulator):

```
vpn debug trunc ALL=5
```

- Syntax for R81.10 (regardless of a Jumbo Hotfix Accumulator):

```
vpn debug trunc ALL=5
ike debug trunc
ike debug on TDERROR_ALL_ALL=5
```

11. Replicate the issue / wait for the issue to occur.
12. Write down the details of the problematic connections:
    a. Source IP address
    b. Destination IP address
    c. Port numbers
    d. Protocol
    e. Time of the connections
13. Press the **CTRL+C** keys to stop the kernel debug and the SecureXL debug.
14. Reset the kernel debug options:

```
fw ctl debug 0
```

15. Reset the SecureXL debug options:

    ```
    fwaccel dbg resetall
    ```

16. If the issue is related to an "Overlay" connection, then stop the VPN debug in the user space as described in sk180488:

    ```
    vpn debug off
    ```

17. Collect these files from the Security Gateway:

    a. The kernel debug output:

       `/var/log/kernel_debug.txt`

    b. The VPN user space debug output:

       See the list of files in sk180488.

    c. The log files for the SD-WAN Steering daemon:

       `$FWDIR/log/sdwan_steering.elg*`

    d. The CPinfo output file (sk92739).