QUANTUM

23 June 2025

REMOTE ACCESS VPN

R81.20

Administration Guide

Check Point Copyright Notice

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 R81.20

For more about this release, see the R81.20 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
08 June 2025	Updated: ■ *"IP Pool Configuration" on page 74*
10 April 2025	Updated: ■ *"SCV Configuration on the Management Server" on page 97*
16 December 2024	Updated: ■ *"SAML Support for Remote Access VPN" on page 178*
08 July 2024	Updated: ■ *"SAML Support for Remote Access VPN" on page 178*
19 June 2024	Updated: ■ *"Secure Configuration Verification" on page 91* Added: ■ *"Secure Configuration Verification - Advanced" on page 106*
17 June 2024	Updated: ■ *"SAML Support for Remote Access VPN" on page 178*
09 June 2024	Updated: ■ *"Configuring Multiple Log-in Options" on page 42* - added recommendation that username and password should not be the only authentication method
28 November 2023	Moved documentation of SSL Network Extender (SNX) to the new SSL Network Extender (SNX) Administration Guide.
14 November 2023	Updated: ■ *"Remote Access Advanced Configuration" on page 151* ■ *"SAML Support for Remote Access VPN" on page 178*
26 July 2023	Updated: ■ *"SAML Support for Remote Access VPN" on page 178*

Date	Description
29 June 2023	Updated: ■ *"Dynamic Split Tunneling for SaaS Using Updatable Objects" on page 192* ■ *"Machine Certificate" on page 122*
10 May 2023	Updated: ■ *"Desktop Security" on page 82* ■ *"SAML Support for Remote Access VPN" on page 178*
19 April 2023	Updated: ■ *"strongSwan Client Support" on page 196*
30 March 2023	Updated: ■ *"SAML Support for Remote Access VPN" on page 178*
16 March 2023	Updated: ■ *"Dynamic Split Tunneling for SaaS Using Updatable Objects" on page 192*
12 February 2023	Updated: ■ *"User and Client Authentication for Remote Access" on page 40* ■ *"SAML Support for Remote Access VPN" on page 178*
15 January 2023	Added: ■ *"Advanced VPN Domain Configuration" on page 25* Updated: ■ *"Secure Configuration Verification" on page 91* ■ *"Secondary Connect" on page 175*
20 November 2022	First release of this document

Table of Contents

Check Point VPN

IPsec VPN

The IPsec VPN solution lets the Security Gateway encrypt and decrypt traffic to and from other gateways and clients. Use SmartConsole to easily configure VPN connections between Security Gateways and remote devices.

For Site to Site Communities, you can configure Star and Mesh topologies for VPN networks, and include third-party gateways.

The VPN tunnel guarantees:

- Authenticity - Uses standard authentication methods
- Privacy - All VPN data is encrypted
- Integrity - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

Remote Access VPN

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point's Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade extends the functionality of Remote Access solutions to include many clients and deployments.

VPN Connectivity Modes

The IPsec VPN Software Blade lets the Firewall overcome connectivity challenges for remote clients. Use VPN connectivity modes to make sure that remote users can connect to the VPN tunnels. These are some examples of connectivity challenges:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a hotel LAN with internal IP addresses
- It is necessary for the remote client to use protocols that are not supported

Office Mode

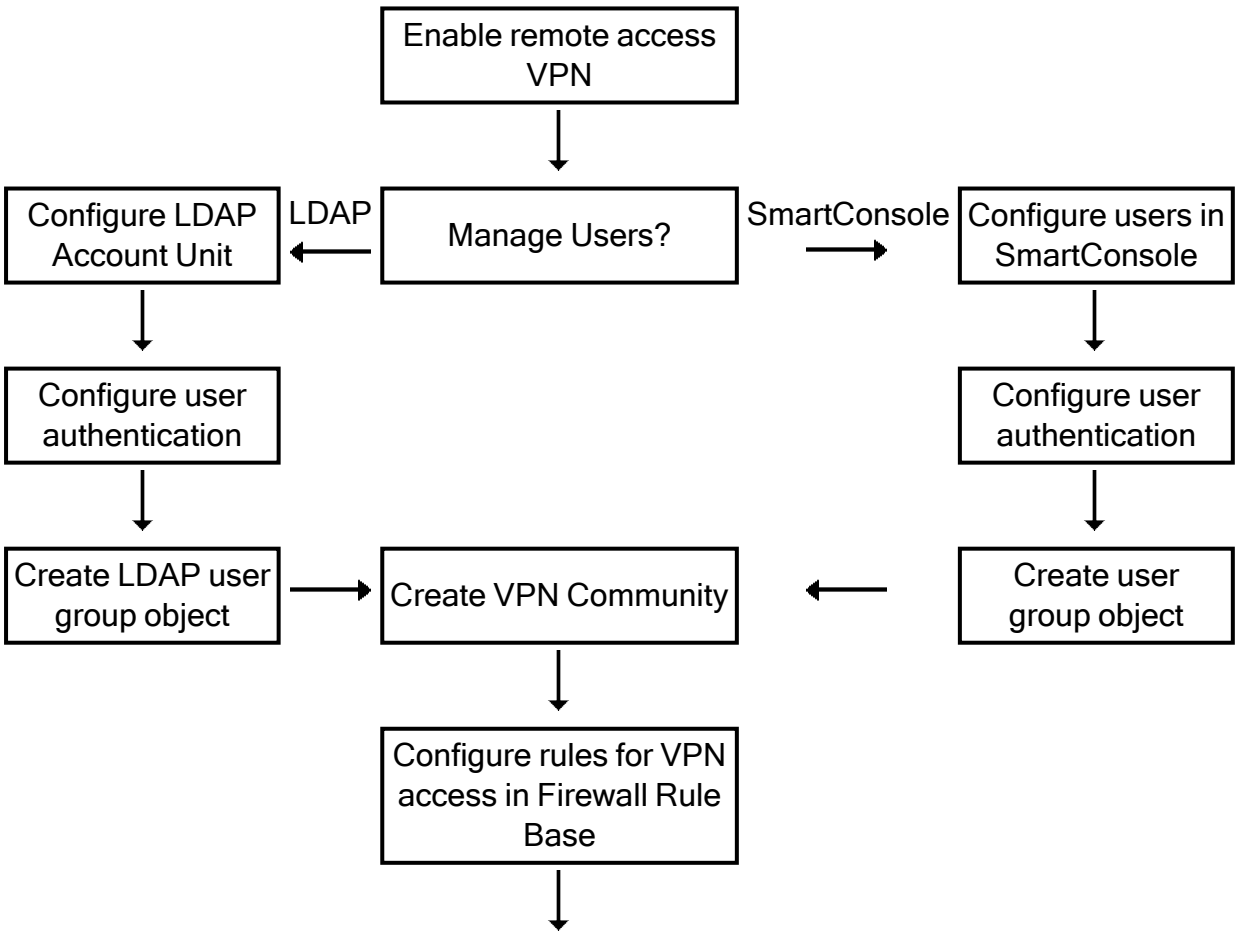
Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and do not have VPN routing problems.

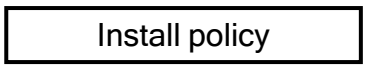
Visitor Mode

Remote users can be restricted to use HTTP and HTTPS traffic only. Visitor Mode lets these users tunnel all protocols with a regular TCP connection on port 443.

Sample Remote Access VPN Workflow

Use SmartDashboard to enable and configure the Security Gateway for remote access VPN connections. Then add the remote user information to the Security Management Server: create and configure an LDAP Account Unit or enter the information in the SmartDashboard user database. You can also configure the Firewall to authenticate the remote users. Define the Firewall access control and encryption rules. Create the LDAP group or user group object that is used for the Firewall rules. Then create and configure the encryption settings for the VPN community object. Add the access rules to the Firewall Rule Base to allow VPN traffic to the internal networks.





VPN Components

VPN is composed of:

- VPN endpoints, such as Security Gateways, Security Gateway clusters, or remote clients (such as laptop computers or mobile phones) that communicate over a VPN.
- VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.
- VPN Management tools, such as Security Management Server and SmartConsole. The SmartConsole lets organizations define and deploy Intranet, and remote Access VPNs.

Understanding the Terminology

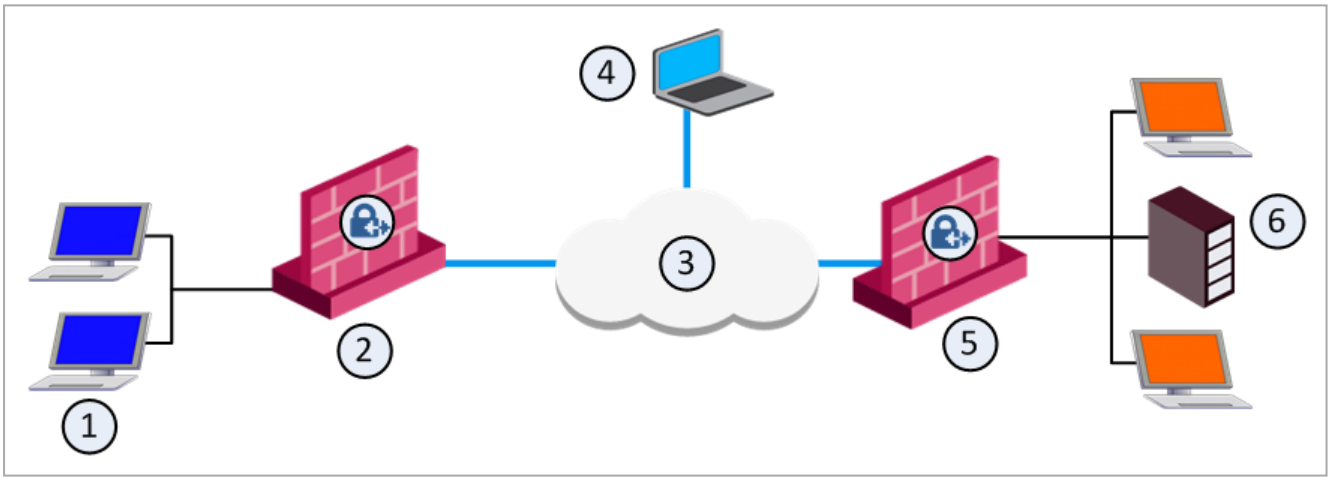
- **VPN** - Virtual Private Network. A secure, encrypted connection between networks and remote clients on a public infrastructure, to give authenticated remote users and sites secured access to an organization's network and resources.
- **VPN Domain** - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.
- **VPN Community** - A named collection of VPN domains, each protected by a VPN gateway.
- **VPN Security Gateway** - The gateway that manages encryption and decryption of traffic between members of a VPN Domain, typically located at one (Remote Access VPN) or both (Site to Site VPN) ends of a VPN tunnel.
- **Site to Site VPN** - An encrypted tunnel between two gateways, typically of different geographical sites.
- **Remote Access VPN** - An encryption tunnel between a Security Gateway and remote access clients, such as Endpoint Security VPN, and communities.
- **Remote Access Community** - A group of computers, appliances, and devices that access, with authentication and encryption, the internal protected network from physically remote sites.
- **IKE (Internet Key Exchange)** - An Encryption key management protocol that enhances IPSec by providing additional features, flexibility, and ease of configuration.
- **IPsec** - A set of secure VPN protocols that manage encryption keys and encrypted packet traffic, to create a standard for authentication and encryption services.

Establishing a Connection between a Remote User and a Security Gateway

A VPN tunnel establishment process is initiated to allow the user to access a network resource protected by a Security Gateway. An IKE negotiation takes place between the peers.

During IKE negotiation, the peers' identities are authenticated. The Security Gateway verifies the user's identity and the client verifies that of the Security Gateway. The authentication can be performed using several methods, including digital certificates issued by the Internal Certificate Authority (ICA). It is also possible to authenticate using third-party PKI solutions and pre-shared secrets.

After the IKE negotiation ends successfully, a secure connection (a VPN tunnel) is established between the client and the Security Gateway. All connections between the client and the Security Gateway VPN domain (the LAN behind the Security Gateway) are encrypted inside this VPN tunnel, using the IPsec standard. Except for when the user is asked to authenticate in some manner, the VPN establishment process is transparent.



Item	Description
1	Host 1. Part of VPN Site 1.
2	VPN Gateway 1. Part of VPN Site 1.
3	Internet
4	Remote Client
5	VPN Gateway 2. Part of VPN Site 2.

Item	Description
6	LDAP Server. Part of VPN Site 2.

In the figure:

1. The remote user initiates a connection to Security Gateway 1.
2. User management is not performed via the VPN database, but by LDAP server belonging to VPN Site 2.
3. Authentication takes place during the IKE negotiation.
4. Security Gateway 1 verifies that the user exists by querying the LDAP server behind Security Gateway 2.
5. After the user's existence is verified, the Security Gateway authenticates the user, for example by validating the user's certificate.
6. After IKE is successfully completed, a tunnel is created and the remote client connects to Host 1.
7. If the client is behind the Security Gateway (for example, if the user accesses the corporate LAN from a company office), connections from the client to destinations that are also behind the LAN Security Gateway are not encrypted.

Getting Started with Remote Access

Overview of the Remote Access Workflow

This is an overview of the workflow to give your employees remote access to your VPN Security Gateway.

1. Enable the IPsec VPN Software Blade on the Security Gateway and do basic Security Gateway configuration (see *"Basic Security Gateway Configuration" below*).
2. Add the Security Gateway to the Remote Access VPN Community (see *"Basic Security Gateway Configuration" below*).
3. Include users in the Remote Access VPN Community (see *"Including Users in the Remote Access Community" on the next page*).
4. Configure user authentication (see *"Configuring User Authentication" on page 23*).
5. Configure VPN access rules in the security policy (see *"Configuring VPN Access Rules for Remote Access" on page 23*).
6. If necessary, define the Desktop Policy (see *"Desktop Security" on page 82*).
7. Install policy on the Security Gateway.
8. Deploy the remote access client to users (see *"Deploying Remote Access Clients" on page 24*).

Basic Security Gateway Configuration

As a best practice, use these Security Gateway settings for most remote access clients. See the documentation for your client for more details.

These instructions use the default Remote Access VPN Community, **RemoteAccess**. You can also create a new Remote Access VPN Community with a different name.

To configure a Security Gateway for remote access:

1. In SmartConsole, right click the Security Gateway (Cluster) object and select **Edit**.
2. In the **Network Security** tab, select **IPsec VPN** to enable the Software Blade.

   Note that some clients also require the **Mobile Access** Software Blade.

See the section "**Required Licenses**" in *"Check Point Remote Access Solutions" on page 27*.

3. Add the Security Gateway to the **Remote Access VPN Community**:
   a. From the **Check Point Gateway** tree, click **IPsec VPN**.
   b. In **This Security Gateway participates in the following VPN Communities**, make sure the Security Gateway shows or click **Add** to add the Security Gateway.
   c. Click the **RemoteAccess** community.
   d. Click **OK**.

      The ICA automatically creates a certificate for the Security Gateway.
4. Set the VPN Domain for the Remote Access community.

   The default is **All IP Addresses behind Gateway are based on Topology information**. To configure a VPN domain manually, see *"Advanced VPN Domain Configuration" on page 25*
5. Configure **Visitor Mode**.
   a. Select **IPsec VPN** > **VPN Clients** > **Remote Access**.
   b. Select **Support Visitor Mode** and keep **All Interfaces** selected.
   c. Optional: Select the Visitor Mode **Service**, which defines the protocol and port of client connections to the Security Gateway.
6. Configure **Office Mode**.
   a. From the **Check Point Gateway** tree, select **VPN Clients** > **Office Mode**.

      The default is **Allow Office Mode to all users**.
   b. Optional: Select **Offer Office Mode to group** and select a group.
   c. Select an Office Mode method (see *"Office Mode" on page 64*).
7. Click **OK**.
8. Install the Access Control Policy.

Including Users in the Remote Access Community

By default, the Remote Access VPN Community includes a user group, **All Users,** that includes all defined users. You can use this group or add different user groups to the Remote Access VPN Community. The community can contain users defined in LDAP, which includes Active Directory, or users defined on the Security Management Server.

For more information about user groups and LDAP, see the *R81.20 Security Management Administration Guide*.

To add user groups to a Remote Access VPN Community in SmartConsole:

1. From the left navigation panel, click **Security Policies**.
2. In the top section, click **Access Control**.
3. In the bottom section **Access Tools**, click **VPN Communities**.
4. Right-click the **Remote Access Community** object and click **Edit**.
5. Click **Participant User Groups**.
6. Add or remove groups.
7. Click **OK**.

Configuring User Authentication

Users must authenticate to the VPN Security Gateway with a supported authentication method. You can configure authentication methods for the remote access Security Gateway in:

- **Gateway Properties** > **VPN Clients** > **Authentication**
- SmartDashboard > **Mobile Access** tab > **Authentication**
- **Gateway Properties** > **Mobile Access** > **Authentication**

If no authentication methods are defined for the Security Gateway, users select an authentication method from the client.

For details, see *"User and Client Authentication for Remote Access" on page 40*.

Configuring VPN Access Rules for Remote Access

You must configure rules to allow users in the Remote Access VPN Community to access the LAN. You can limit the access to specified services or specified clients. Configure rules in SmartConsole > **Security Policies** > **Access Control**.

To make a rule apply to a VPN Community, the **VPN** column of the Rule Base must contain one of these:

- **Any** - The rules applies to all VPN Communities. If you configure a new VPN Community after the rule was created, the rule also applies to the new VPN Community.

- **One or more specified VPN communities** - For example, **RemoteAccess**. Right-click in the VPN column of a rule and select **Specific VPN Communities**. The rule applies to the communities shown in the VPN column.

Examples:

- This rule allows traffic from all VPN Communities to the internal network on all services:

Name	Source	Destination	VPN	Services & Applications
Allow all remote access	* Any	Internal_ Network	* Any	* Any

- This rule allows traffic from RemoteAcccess VPN Community to the internal network on HTTP and HTTPS.

Name	Source	Destination	VPN	Services & Applications
Allow RemoteAccess community	* Any	Internal_ Network	RemoteAccess	HTTP HTTPS

- This rule allows traffic from RemoteAcccess VPN Community to the internal network on all services when the traffic starts from the Endpoint Security VPN client.

Name	Source	Destination	VPN	Services & Applications
Allow all from Endpoint Security VPN	Endpoint Security VPN Access Role	Internal_ Network	RemoteAccess	* Any

See *"Configuring Policy for Remote Access VPN" on page 36* for details of how to create Access Roles for Remote Access and VPN Clients to include them in rules in the Access Control Rule Base.

Deploying Remote Access Clients

See the documentation for your remote access client for deployment instructions.

Make sure that users have:

- The site name or URL.
- The credentials or hardware required to authenticate.

Advanced VPN Domain Configuration

If a Security Gateway participates in more than one VPN Community, you can configure a different VPN Domain for the Security Gateway for each VPN Community in which it participates. In SmartConsole, you can configure a specific VPN Domain for a Security Gateway in the Security Gateway object **or** in the VPN Community object.

To configure a specific VPN Domain in the Security Gateway Object:

1. Open the **Network Management** > **VPN Domain** page.
2. In the line **Set Specific Domain for Gateway Communities**, click **Set**.
3. Select the VPN Community for which it is necessary to override the VPN Domain and click **Set**.
4. Select the applicable option:
   - **According to the gateway**

     This configuration option use the VPN Domain that is configured in the **Network Management** folder > **VPN Domain** page > **VPN Domain** section.
   - **User defined**

     Select the applicable Network or Group object (or create a new object).

     This configuration option overrides:

     - The VPN Domain that is configured in the Security Gateway object > **Network Management** folder > **VPN Domain** page > **VPN Domain** section.
     - The VPN Domain that is configured in the Meshed / Star VPN Community object > **Gateways** page.
     - The VPN Domain that is configured in the Remote Access VPN Community object > **Participating Gateways** page.
5. Click **OK** to close the Set Specific VPN Domain for Gateway Communities window.
6. Click **OK** to close the **Communities Specific VPN Domain** window.

To configure a specific VPN Domain in the VPN Community Object:

1. In the **Objects** pane, click **VPN Communities**.
2. Click the applicable VPN Community.

The VPN Community configuration window opens.

3. In the **Gateways** pane, double-click the relevant Security Gateway object (or create a new object).

   The VPN Domain configuration window opens.

4. Select the applicable option:

   - **According to the gateway**

     This configuration option use the VPN Domain that is configured in the **Network Management** folder > **VPN Domain** page > **VPN Domain** section.

   - **User defined**

     Select the applicable Network or Group object (or create a new object).

     This configuration option overrides:

     - The VPN Domain that is configured in the Security Gateway object > **Network Management** folder > **VPN Domain** page > **VPN Domain** section.
     - The VPN Domain that is configured in the Meshed / Star VPN Community object > **Gateways** page.
     - The VPN Domain that is configured in the Remote Access VPN Community object > **Participating Gateways** page.

5. Click **OK** to close the VPN Domain configuration window.
6. Click **OK** to close the VPN Community configuration window.

Check Point Remote Access Solutions

Secure Remote Access

In today's business environment, it is clear that workers require remote access to sensitive information from a variety of locations and a variety of devices. Organizations must also make sure that their corporate network remains safe and that remote access does not become a weak point in their IT security.

Types of Solutions

All of Check Point's Remote Access solutions provide:

- Enterprise-grade, secure connectivity to corporate resources.
- Strong user authentication.
- Granular access control.

Factors to consider when choosing remote access solutions for your organization:

- **Client-Based vs. Clientless** - Does the solution require a Check Point client to be installed on the endpoint computer or is it clientless, for which only a web browser is required. You might need multiple solutions within your organization to meet different needs.
- **Secure Connectivity and Endpoint Security** - Which capabilities does the solution include?
    - **Secure Connectivity** - Traffic is encrypted between the client and VPN Security Gateway. After users authenticate, they can access the corporate resources that are permitted to them in the access policy. All Check Point solutions supply this.
    - **Endpoint Security** - Endpoint computers are protected at all times, even when there is no connectivity to the corporate network. Some Check Point solutions supply this.

Client-Based vs. Clientless

Check Point remote access solutions use IPsec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:

- **Client-based** - Client application installed on endpoint computers and devices. The client supplies access to most types of corporate resources according to the access privileges of the user.
- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Secure Connectivity and Endpoint Security

You can combine secure connectivity with additional features to protect the network or endpoint computers.

- **Secure Connectivity** - Traffic is encrypted between the client and VPN Security Gateway and strong user authentication is supported. All Check Point solutions supply this.

  These solutions require licenses based on the number of users connected at the same time.
- **Security Verification for Endpoint computers** - Makes sure that devices connecting to the Security Gateway meet security requirements. Endpoint machines that are not compliant with the security policy have limited or no connectivity to corporate resources. Some Check Point solutions supply this.
- **Endpoint Security**:
  - **Desktop Firewall** - Protects endpoint computers at all times with a centrally managed security policy. This is important because remote clients are not in the protected network and traffic to clients is only inspected if you have a Desktop Firewall. Some Check Point solutions supply this
  - **More Endpoint Security Capabilities** - Check Point solutions can include more Endpoint Security capabilities, such as anti-malware, disk encryption and more.

  These solutions require licenses based on the number of clients installed.

Remote Access Solution Comparison

Details of the newest version for each client and a link for more information are in sk67820.

SSL VPN Portal and Clients	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6
Mobile Access Web Portal	Windows, Linux, Mac OS, iOS, Android	Clientless	SSL	Supported	Not Supported	Supported
SSL Network Extender for Mobile Access Software Blade	Windows, Linux, Mac OS	On demand Client through Mobile Access Portal)	SSL	Supported	Not Supported	Not Supported
Capsule Workspace for iOS (previously Mobile Enterprise)	iOS	Client	SSL	Supported for MDM Cooperative Enforcement - Jailbreak & Root Detection features (see sk98201)	Not Supported	Supported
Capsule Workspace for Android (previously Mobile Enterprise)	Android	Client	SSL	Supported for MDM Cooperative Enforcement - Jailbreak & Root Detection features (see sk98201)	Not Supported	Supported

Layer-3 VPN Tunnel Clients	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6
Capsule Connect for iOS (previously Mobile VPN)	iOS	Client	IPsec / SSL	Supported for MDM Cooperative Enforcement (see sk98201)	Not Supported	Not Supported
Capsule VPN for Android (previously Mobile VPN)	Android	Client	IPsec/SSL	Supported for MDM Cooperative Enforcement (see sk98201)	Not Supported	Not Supported
Check Point VPN Plugin for Windows 8.1	Windows 8.1	Pre-installed client	SSL	Not Supported	Not Supported	Not Supported
Check Point Capsule VPN for Windows 10	Windows 10	Client	SSL	Not Supported	Not Supported	Not Supported
Check Point Mobile for Windows	Windows	Client	IPsec	Supported	Not Supported	Not Supported

Layer-3 VPN Tunnel Clients Integrated with Endpoint Security	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6
Endpoint Security VPN for Windows	Windows	Client	IPsec	Supported	Supported	Not Supported
Endpoint Security VPN for macOS	Mac OS	Client	IPsec	Supported supported starting from Endpoint Security VPN for macOS client version E88.40	Supported	Not Supported
Endpoint Security Suite Remote Access VPN Software Blade	Windows, Mac OS	Client	IPsec	Supported	Supported	Not Supported

Additional Remote Access Solutions	Supported Operating Systems	Client or Clientless	Encryption Protocol	Security Verification for Endpoint Devices	Desktop Firewall on Endpoint Devices	IPv6
SecuRemote	Windows	Client	IPsec	Not Supported	Not Supported	Not Supported

Summary of Remote Access Options

Below is a summary of each Remote Access option that Check Point offers. All supply secure remote access to corporate resources, but each has different features and meets different organizational requirements.

Details of the newest version for each client and a link for more information are in sk67820.

SSL Network Extender

SSL Network Extender is a thin SSL VPN on-demand client installed automatically on the user's machine through a web browser. It supplies access to all types of corporate resources.

SSL Network Extender has two modes:

- **Network Mode** - Users can access all application types (Native-IP-based and Web-based) in the internal network. To install the Network Mode client, users must have administrator privileges on the client computer.

  Supported Platforms: Windows, macOS, Linux

- **Application Mode** - Users can access most application types (Native-IP-based and Web-based) in the internal network, including most TCP applications. The user does not require administrator privileges on the endpoint machine.

  Supported Platforms - Windows

Required Licenses - Mobile Access Software Blade on the Security Gateway

Where to Get the Client - Included with the Security Gateway. See sk67820.

For more information, see the SSL Network Extender (SNX) Administration Guide.

Capsule Workspace for iOS

Capsule Workspace for iOS is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Microsoft Exchange services. It also gives secure access to Capsule Docs protected documents. It was previously called Mobile Enterprise.

Capsule Workspace is ideal for mobile workers who have privately-owned smart phones or tablets. It protects only the business data inside the App and does not require device-level security measures, such as device-lock or device-wipe.

Required Licenses - Mobile Access Software Blade on the Security Gateway and a mail license on the Security Management Server

Supported Platforms - iOS

Where to Get the Client - Apple App Store

Capsule Workspace for Android

Capsule Workspace for Android is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Microsoft Exchange services. It also gives secure access to Capsule Docs protected documents. It was previously called Mobile Enterprise.

Capsule Workspace for Android is ideal for mobile workers who have privately-owned smart phones or tablets. It protects only the business data inside the App and does not require device-level security measures, such as device-lock or device-wipe.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Android

Where to Get the Client - Google Play Store

Capsule Connect for iOS

Capsule Connect is a full L3 tunnel app that gives users network access to all mobile applications. It supplies secure connectivity and access to all types of corporate resources. It was previously called Mobile VPN.

Required Licenses - Mobile Access Software Blade on the Security Gateway and a mail license on the Security Management Server

Supported Platforms - iOS 6.0 +

Where to Get the Client - Apple App Store

Capsule VPN for Android

Capsule VPN for Android devices is an L3 VPN client. It supplies secure connectivity and access to corporate resources using L3 IPSec/SSL VPN Tunnel. It was previously called Mobile VPN.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Android 4 + (ICS+)

Where to Get the Client - Google Play Store

Check Point VPN Plugin for Windows 8.1

Check Point VPN Plugin for Windows 8.1 is an L3 VPN client. It supplies secure connectivity and access to corporate resources using L3 SSL VPN Tunnel.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Windows 8.1

Where to Get the Client - Pre-installed with Windows.

Check Point Capsule VPN for Windows 10

Check Point Capsule VPN for Windows 10 is an L3 VPN client. It supplies secure connectivity and access to corporate resources using L3 SSL VPN Tunnel.

Required Licenses - Mobile Access Software Blade on the Security Gateway

Supported Platforms - Windows 10

Where to Get the Client - Microsoft Software & Apps store.

Check Point Mobile for Windows

Check Point Mobile for Windows is an IPsec VPN client. It is best for medium to large enterprises that do not require an Endpoint Security policy.

The client gives computers:

- Secure Connectivity
- Security Verification

Required Licenses - IPsec VPN and Mobile Access Software Blades on the Security Gateway.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Endpoint Security VPN

Endpoint Security VPN is an IPsec VPN client that replaces SecureClient. It is best for medium to large enterprises.

The client gives computers:

- Secure Connectivity
- Security Verification
- Endpoint Security that includes an integrated Desktop Firewall, centrally managed from the Security Management Server.

Required Licenses - The IPsec VPN Software Blade on the Security Gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Note - Endpoint Security VPN on macOS includes a Desktop Firewall but not Security Verification.

Endpoint Security VPN for macOS

Endpoint Security VPN combines Remote Access VPN with Endpoint Security in a client that is installed on endpoint computers. It is recommended for managed endpoints that require a simple and transparent remote access experience together with Desktop Firewall rules. It includes:

- Enterprise Grade Remote Access Client that replaces SecureClient for Mac.
- Integrated Desktop Firewall, centrally managed from the Security Management Server.

Required Licenses - The IPsec VPN Software Blade on the Security Gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

Supported Platforms for Users - macOS

Where to Get the Client - Check Point Support Center - sk67820.

Endpoint Security Suite

The Endpoint Security Suite simplifies endpoint security management by unifying all endpoint security capabilities in a single console. Optional Endpoint Security Software Blades include: Firewall, Compliance Full Disk Encryption, Media Encryption & Port Protection, and Anti-Malware & Program Control. As part of this solution, the Remote Access VPN Software Blade provides full, secure IPsec VPN connectivity.

The Endpoint Security suite is best for medium to large enterprises that want to manage the endpoint security of all of their endpoint computers in one unified console.

Required Licenses - Endpoint Security Container and Management licenses and an Endpoint VPN Software Blade on the Security Management Server.

Supported Platforms - Windows, macOS

Where to Get the Client - Check Point Support Center - sk67820.

SecuRemote

SecuRemote is a secure, but limited-function IPsec VPN client. It provides secure connectivity.

Required Licenses - IPsec VPN Software Blade on the Security Gateway. It is a **free** client and does not require additional licenses.

Supported Platforms - Windows

Where to Get the Client - Check Point Support Center - sk67820.

Configuring Policy for Remote Access VPN

Step 1 - Create a Security Gateway/Cluster object

a. Install the required Security Gateway / Cluster Members and configure their interfaces.

   For more information, see the *R81.20 Installation and Upgrade Guide*.

b. In SmartConsole, create a new object.

   For more information, see the *R81.20 Security Management Administration Guide* > **Managing Objects** section.

c. Establish the Secure Internal Communication (SIC).

   For more information, see the *R81.20 Security Management Administration Guide* > **Secure Internal Communications (SIC)** section.

d. Get the interfaces and configure their topology settings.

   For more information, see the *R81.20 Gaia Administration Guide* > **Network Management** chapter > **Network Interfaces** topic

Step 2 - Configure the required Remote Access VPN settings in the Security Gateway / Cluster object

a. Create a Security Gateway network object.

b. On the **General Properties** page, select **VPN**.

c. Initialize a secure communication channel between the VPN module and the Security Management Server by clicking **Communication**

d. On the **Topology** page, define the interfaces and the VPN domain.

   The ICA automatically creates a certificate for the Security Gateway.

Step 3 - Configure the applicable Host, Network, Group, User and Access Role objects

For more information, see the *R81.20 Security Management Administration Guide* > **Managing Objects** section.

Step 4 - Configure the Remote Access VPN Community

a. From the Objects Bar, click **VPN Communities**.

b. Double-click **RemoteAccess**.

The **Remote Access** window opens.

c. On the **Participating Gateways** page, click the Add button and select the Security Gateways that are in the Remote Access Community.

d. On the **Participating User Groups** page, click the Add button and select the group that contains the Remote Access users.

e. Click **OK**.

f. Publish the changes.

Step 5 - Configure the applicable Access Control rules

These rules apply to traffic from the Remote Access VPN clients to internal resources behind the Security Gateway.

For more information, see the > *R81.20 Security Management Administration Guide* > Chapter "Creating an Access Control Policy".

Column	Description
Source	Select the applicable Host, Network, Group, User, and Access Role objects.
Destination	Select the applicable Host, Network, and Group objects.
VPN	Select the Remote Access VPN Community object
Services & Applications	Select only the specific service objects to make the rule as restrictive as possible.
Action	Select the applicable action.

Example:

Source	Destination	VPN	Services & Applications	Action
Office_Mode_ Network	MyWebServer	RemoteAccess	http https	Accept

Step 6 - Install the Access Control Policy

In SmartConsole, install the Access Control Policy on the Security Gateway/Cluster object.

Step 7 - Optional: Advanced Configuration

The encryption properties of the users participating in a Remote Access community are set by default. If you must modify the encryption algorithm, the data integrity method and/or the Diffie-Hellman group, you can either do this globally for all users or configure the properties per user.

To modify the user encryption properties globally:

a. From Menu, click **Global Properties**.

b. From the navigation tree, click **Remote Access > VPN- Authentication and Encryption**.

c. From the **Encryption algorithms** section, click **Edit**.

The **Encryption Properties** window opens.

d. In the **IKE Security Association (Phase 1)** tab, configure the applicable settings:

- **Support encryption algorithms** - Select the encryption algorithms that will be supported with remote hosts.
- **Use encryption algorithms** - Choose the encryption algorithm that will have the highest priority of the selected algorithms. If given a choice of more than one encryption algorithm to use, the algorithm selected in this field will be used.
- **Support Data Integrity** - Select the hash algorithms that will be supported with remote hosts to ensure data integrity.
- **Use Data Integrity** - The hash algorithm chosen here will be given the highest priority if more than one choice is offered.
- **Support Diffie-Hellman groups** - Select the Diffie-Hellman groups that will be supported with remote hosts.
- **Use Diffie-Hellman group** - Client users utilize the Diffie-Hellman group selected in this field.

e. Click **OK**.

f. Install policy.

To configure encryption policies for specified users:

a. Open **Global Properties**, and click **Remote Access > Authentication and Encryption**.

b. From the **Encryption algorithms** section, click **Edit**.

c. In the **Encryption Properties** window, click the **IPSEC Security Association (Phase 2)** tab.

d. Clear **Enforce Encryption Algorithm and Data Integrity on all users**.

e. Click **OK** and close the **Global Properties** window.

f. For each user:

   i. From the Objects Bar, double-click the user.

   ii. From the navigation tree, click **Encryption**.

   iii. Click **Edit**.

   The **IKE Phase 2 Properties** window is displayed.

   iv. Click the **Encryption** tab.

   v. Click **Defined below**.

   vi. Configure the **Encryption Algorithm** and **Data Integrity**.

   vii. Click **OK** and close the **User Properties** window.

g. Install policy.

User and Client Authentication for Remote Access

Client-Security Gateway Authentication Schemes

Authentication is a key factor in establishing a secure communication channel among Security Gateways and remote clients. Various authentication methods are available, for example:

- Digital certificates
- Pre-shared secrets
- Other authentication methods

On Mobile Access and IPsec VPN Security Gateways, you can configure multiple login options. The options can be different for each Security Gateway and each Software Blade. Users select one of the available options to log in with a supported client.

See the documentation for each client to learn which authentication methods are supported.

Digital User Certificates

Digital Certificates are the most recommended and manageable method for authentication. Both parties present certificates as a means of proving their identity. Both parties verify that the peer's certificate is valid (i.e. that it was signed by a known and trusted CA, and that the certificate has not expired or been revoked).

Digital certificates are issued either by Check Point's Internal Certificate Authority or third-party PKI solutions. Check Point's ICA is tightly integrated with VPN and is the easiest way to configure a Remote Access VPN. The ICA can issue certificates both to Security Gateways (automatically) and to remote users (generated or initiated).

Generate digital certificates easily in SmartConsole > **Security Policies** > **Access Tools** > **Client Certificates**.

The administrator can also initiate a certificate generation on the ICA management tool. It is also possible to use third-party Certificate Authorities to create certificates for authentication between Security Gateways and remote users. The supported certificate formats are PKCS#12, CAPI, and *Entrust*.

Users can also be given a hardware token for storing certificates. This option offers the advantage of higher level of security, since the private key resides only on the hardware token.

As part of the certificate validation process during the IKE negotiation, both the client and the Security Gateway check the peer's certificate against the *Certificate Revocation List* (CRL) published by the CA which issued the certificate. If the client is unable to retrieve a CRL, the Security Gateway retrieves the CRL on the client's behalf and transfers the CRL to the client during the IKE negotiation (the CRL is digitally signed by the CA for security).

Pre-Shared Secret

This authentication method has the advantage of simplicity, but it is less secure than certificates.

Both parties agree upon a password before establishing the VPN. The password is exchanged "out-of-band", and reused multiple times. During the authentication process, both the client and Security Gateway verify that the other party knows the agreed-upon password.

Other Authentication Methods

These user authentication methods are supported for remote access.

- **Security Gateway Password** - Users enter their password that are on the Security Gateway.
- **DynamicID One Time Password** - Users enter the number shown in an SMS message to a specified cellphone number or by email.
- **OS Password** - Users enter their Operating System password.
- **SecurID One Time Password** - Users enter the number shown on a Security Dynamics SecurID card.

  SoftID (a software version of RSA's SecurID) and various other One Time Password cards and USB tokens are also supported.
- **RADIUS** - Users enter the correct response, as defined by the RADIUS server.
- **TACACS** - Users enter the correct response, as defined by the TACACS or TACACS+ server.
- **SAA** - SAA is an OPSEC API extension to Remote Access Clients that enables third party authentication methods, such as biometrics, to be used with Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote.

Multiple Login Options

On Mobile Access and IPsec VPN Security Gateways, you can configure multiple login options. The options can be different for each Security Gateway and each supported Software Blade, and for some client types. Users select one of the available options to log in with a supported client.

Each configured login option is a global object that can be used with multiple gateways and the Mobile Access and IPsec VPN Software Blades.

Configuring Multiple Log-in Options

Configure login options from: **Gateway Properties** > **VPN Clients** > **Authentication**

If Mobile Access is enabled, you can also configure login options from:

- In SmartDashboard **Gateway & Servers**, double-click a Security Gateway object. From the **Gateway Properties** window > **Mobile Access** > **Authentication**
- In SmartDashboard > **Mobile Access** tab > **Authentication**

The login options selected for IPsec VPN clients, such as Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote, show in the **VPN Clients** > **Authentication** page in the **Multiple Authentication Client Settings** table.

The login options selected for Mobile Access clients, such as the Mobile Access portal and Capsule Workspace, show in the **Mobile Access** > **Authentication** page in the **Multiple Authentication Client Settings** table.

To configure multiple login options for IPsec VPN Clients:

1. From the **Gateway Properties**, select **VPN Clients** > **Authentication**.
2. In the **Multiple Authentication Clients Settings** table, see a list of configured login options.

   The default login options are:

   - **Personal_Certificate** - Requires a user certificate.
   - **Username_Password** - Requires a username and password.

     Important - As a best security practice, we recommend to configure another authentication method in addition to username and password. In the next step, click **Edit** and configure one or more additional authentication methods.

   - **Cert_Username_Password** - Require a username and password and a user certificate.
3. Click **Add** to create a new option or **Edit** to change an option. Each configured login option is a global object that can be used with multiple gateways and Software Blades.
4. For each login option select one or more **Authentication Factors** and relevant **Authentication Settings**.

For example, if you select **SecurID**, select the SecurID **Server** and **Token Card Type**. If you select **Personal Certificate**, select which certificate field the Security Gateway uses to fetch the username (see *"Certificate Parsing" below*).

5. Select **Customize Display** to configure what users see when they log in with this option (see *"Customize Display Settings" below*).

   Click **OK**.

6. Use the **Up** and **Down** arrows to set the order of the login options.

   Notes:

   - If you include **Personal Certificates**, it must be first.
   - If you include **DynamicID**, it cannot be first.

7. Click **OK**.

Customize Display Settings

Enter descriptive values to make sure that users understand what information to input. These fields must all be the same language but they do not need to be in English.

- **Headline** - The title of the login option, for example, **Log in with a Certificate** or **Log in with your SecurID Pinpad**.
- **Username label** - A description of the username that users must enter, for example, **Email address** or **AD username**.
- **Password label** - A description of the password that users must enter, for example, **AD password**.

Certificate Parsing

When you select **Personal Certificate** as a Login option, you can also configure what information the Security Gateway sends to the LDAP server to parse the certificate. The default is the DN. You can configure the settings to use the user's email address or a serial number instead.

To change the certificate parsing:

1. In the **Multiple Authentication Clients Settings** table on the **Authentication** page, select a **Personal_Certificate** entry and click **Edit**.

   The **Authentication Factor** window opens.

2. In the **Authentication Settings area** in the **Fetch Username from** field, select the information that the Security Gateway uses to parse the certificate.
3. Click **OK**.
4. Install the policy.

Deleting Login Options

To permanently delete a Login option:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.
2. In SmartDashboard go to the **Mobile Access** tab > **Authentication** page.
3. From the list of login options, select an option and click **Delete**.

Multi-Factor Authentication with DynamicID

Multi-factor authentication is a system where two or more different methods are used to authenticate users. Using more than one factor delivers a higher level of authentication assurance. DynamicID is one option for multi-factor authentication.

Users who successfully complete the first-phase authentication can be challenged to provide an additional credential: a DynamicID One Time Password (OTP). The OTP is sent to their mobile communications device (such as a mobile phone) via SMS or directly to their email account.

On Security Gateways, DynamicID is supported for all Mobile Access and IPsec VPN clients.

Configuring DynamicID

Basic DynamicID configuration is shown here. For **Advanced** configuration options, see the *R81.20 Mobile Access Administration Guide*.

To configure global DynamicID settings that all gateways use:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree, click **Authentication**.
3. From the **Dynamic ID Settings** section, click **Edit**.
4. Enter the DynamicID Settings (see *"DynamicID Settings" on the next page*).
5. Click **OK**.
6. Click **Save**.
7. Close SmartDashboard.
8. In SmartConsole, install the policy.

To configure DynamicID settings for a specified Security Gateway:

1. In SmartConsole, in the **Gateways & Servers** view, double-click the Security Gateway.
2. From the navigation tree, select **VPN Clients > Authentication**.
3. From the **Dynamic ID Settings** section, clear the **Use Global Settings** option.
4. Click **Edit**.
5. Enter the DynamicID Settings (see *"DynamicID Settings" below*).
6. Click **OK**.
7. Install the policy.

DynamicID Settings

This table explains parameters used in the SMS Provider and Email Settings field. The value of these parameters is automatically used when sending the SMS or email.

Parameter	Meaning
$APIID	The value of this parameter is the API ID.
$USERNAME	The value of this parameter is the username for the SMS provider.
$PASSWORD	The value of this parameter is the password for the SMS provider.
$PHONE	User phone number, as found in Active Directory or in the local file on the Security Gateway, including digits only and without a + sign.
$EMAIL	The email address of the user as found in Active Directory or in the local `SmsPhones.lst` file on the Security Gateway. If the email address should be different than the listed one, it can be written explicitly.
$MESSAGE	The value of this parameter is the message configured in the Advanced Two-Factor Authentication Configuration Options in SmartDashboard.
$RAWMESSAGE	The text from $Message, but without HTTP encoding.

Enter this information in the DynamicID Setting window:

1. Fill in the **Provider and Email Settings** field using one of these formats:

   a. To let the DynamicID code to be delivered by SMS only, use the following syntax:

   ```
   https://api.example.com/http/sendmsg?api_
   id=$APIID&user=$USERNAME&password=$PASSWORD&to=$PHONE&tex
   t=$MESSAGE
   ```

   b. To let the DynamicID code to be delivered by email only, without an SMS service provider, use the following syntax:

   - For SMTP protocol:

     ```
     mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvp
     n@example.com;BODY=$RAWMESSAGE
     ```

   - For SMTPS protocol on port 465:

     ```
     mail:TO=$EMAIL;SMTPSERVER=smtps://username:password@s
     mtp.example.com;FROM=sslvpn@example.com;BODY=$RAWMESS
     AGE
     ```

   - For SMTP protocol with START_TLS:

     ```
     mail:TO=$EMAIL;SSL_
     REQUIRED;SMTPSERVER=smtp://username:password@smtp.exa
     mple.com;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
     ```

   - For SMTP protocol on port 587 with START_TLS:

     ```
     mail:TO=$EMAIL;SSL_
     REQUIRED;SMTPSERVER=smtp://username:password@smtp.exa
     mple.com:587;FROM=sslvpn@example.com;BODY=$RAWMESSAGE
     ```

   c. To let the DynamicID code to be delivered by SMS or email, use the following syntax:

   ```
   sms:https://api.example.com/sendsms.php?username=$USERNAM
   E&password=$PASSWORD&phone=$PHONE&smstext=$MESSAGE
   mail:TO=$EMAIL;SMTPSERVER=smtp.example.com;FROM=sslvpn@ex
   ample.com;BODY=$RAWMESSAGE
   ```

Note - If the SMTP username and password contain special characters, use these:

!	#	$	%	&	'	(
%21	%23	%24	%25	%26	%27	%28
)	*	+	,	/	:	;
%29	%2A	%2B	%2C	%2F	%3A	%3B
=	?	@	[	]		
%3D	%3F	%40	%5B	%5D		

2. In the **SMS Provider Account Credentials** section, enter the credentials received from the SMS provider:
   - **Username**
   - **Password**
   - **API ID** (optional)

Internal User Database vs. External User Database

Remote Access functionality includes a flexible user management scheme. Users are managed in a number of ways:

- INTERNAL - A Security Gateway can store a static password in its local user database for each user configured in Security Management Server. No additional software is needed.
- LDAP - LDAP is an open industry standard that is used by multiple vendors. Check Point products integrate LDAP with Check Point User Directory. Manage the users externally on the LDAP server, and changes are reflected on the SmartDashboard. Security Gateways query the User Directory data for authentication.
- RADIUS - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme that provides security and scalability by separating the authentication function from the access server.

  When employing RADIUS as an authentication scheme, the Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the Security Gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard.

- SecurID Token Management ACE/Server - Developed by RSA Security, SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/Server, and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time-use access code that changes every minute or so. When a user attempts to authenticate to a protected resource, that one-time-use code must be validated by the ACE/Server.

  When employing SecurID as an authentication scheme, the Security Gateway forwards authentication requests by remote users to the ACE/Server. ACE manages the database of RSA users and their assigned hard or soft tokens. The VPN module acts as an ACE/Agent 5.0, which means that it directs all access requests to the RSA ACE/Server for authentication. For agent configuration see ACE/Server documentation.

The differences between user management on the internal database, and User Directory:

- User Directory is done externally and not locally.
- If you change User Directory templates the change is applied to users dynamically, immediately.

Defining User and Authentication Methods in LDAP

1. Obtain and install a license that enables the VPN module to retrieve information from an LDAP server.
2. Create an LDAP account unit.
3. Define users as LDAP users. A new network object for LDAP users is created on the Users tree. (The LDAP users also appear in the objects list window to the right.)

For more information see: LDAP and User Management in the *R81.20 Security Management Administration Guide*.

Managing User Certificates

Managing user certificates involves:

Tracing the status of the user's certificate

The status of a user's certificate can be traced at any time in the **Certificates** tab of the user's Properties window. The status is shown in the **Certificate state** field. If the certificate has not been generated by the user by the date specified in the **Pending until** field, the registration key is deleted.

If the user is defined in LDAP, then tracing is performed by the ICA management tool.

Automatically renewing a certificate

ICA certificates for users can be automatically renewed a number of days before they expire. The client initiates a certificate renewal operation with the CA before the expiration date is reached. If successful, the client receives an updated certificate.

Automatic certificate renewal is enabled by default.

Revoking certificates

The way in which certificates are revoked depends on whether they are managed internally or externally, using LDAP.

When a user is deleted, their certificate is automatically revoked. Certificates can be disabled or revoked at any time.

If the certificate is already active or was not completed by the user, you can revoke it by clicking **Revoke** in the **Certificates** tab of the **User Properties** window.

If users are managed in LDAP, certificates are revoked using the ICA management tool.

Tracing the Status of User's Certificate

The status of a user's certificate can be traced at any time in the **Certificates** tab of the user's Properties window. The status is shown in the **Certificate state** field. If the certificate has not been generated by the user by the date specified in the **Pending until** field, the registration key is deleted.

If the user is defined in LDAP, then tracing is performed by the ICA management tool.

Revoking Certificates

The way in which certificates are revoked depends on whether they are managed internally or externally, using LDAP.

For Internally Managed Users

When a user is deleted, their certificate is automatically revoked. Certificates can be disabled or revoked at any time.

If the certificate is already active or was not completed by the user, you can revoke it by clicking **Revoke** in the **Certificates** tab of the **User Properties** window.

For Users Managed in LDAP

If users are managed in LDAP, certificates are revoked using the ICA management tool.

Multiple Certificates per User

Check Point VPN lets you define many certificates for each user. This lets users connect from different devices without the necessity to copy or move certificates from one device to another. Users can also connect from different devices at the same time.

User Certificate Creation Methods when Using the ICA

Check Point's Internal Certificate Authority (ICA) offers two ways to create and transfer certificates to remote users:

1. The administrator **generates** a certificate in the Security Management Server for the remote user, saves it to removable media, and transfers it to the client "out-of-band."
2. The administrator **initiates** the certificate process on the Security Management Server (or ICA management tool), and is given a registration key. The administrator transfers the registration key to the user "out-of-band." The client establishes an SSL connection to the ICA (using the CMC protocol) and completes the certificate generation process using the registration key. In this way:
   - Private keys are generated on the client.
   - The created certificate can be stored as a file on the machines hard-drive, on a CAPI storage device, or on a hardware token.

   This method is especially suitable for geographically spaced-remote users.

Creating Remote Access VPN Certificates for Users

This section contains procedures for creating Remote VPN user certificates and sending them to end users.

There are two basic procedures for supplying remote access VPN certificates to users.

- **Sending a P12 File:**
  - The administrator creates a p12 certificate file and sends it to users.
  - The user saves the p12 file on the device and specifies the certificate using a remote VPN Client.
  - Users authenticate by entering a certificate password when starting a remote access VPN connection.
- **Using a Registration key:**

- The administrator creates a registration key and sends it to the user.
- The user enrolls the certificate by entering the registration key in a Remote Access VPN client. The user can optionally save the p12 file to the device. The user must do this in an administrator-defined period of time.
- End users authenticate using this certificate. A password can also be required according to the security policy settings. If the user saves the p12 file to the device, a password is always necessary.

Enabling a User Certificate

To enable a user certificate:

1. In SmartConsole, from the **Objects Bar** click **Users > Users**.
2. Create a new user or double-click an existing user.

   The **User Properties** window opens.
3. From the navigation tree, click **Encryption**.
4. Click **Edit**.

   The **IKE Phase 2 Properties** window opens.
5. Click the **Authentication** tab and make sure that **Public key** is selected.
6. Click **OK**.
7. Publish the SmartConsole session.

Creating a P12 Certificate File

After creating a user certificate, you must then make this certificate available to remote access users. Use this procedure to create a p12 certificate.

To create a p12 certificate file for remote access VPN users:

1. Create the user certificate (see *"Enabling a User Certificate" above*).
2. In the **User Properties** window, from the navigation tree click **Certificates**.
3. In the **Certificates** page, click **New**.
4. Select **Certificate file (.p12)**.
5. In the **Certificate File (.P12)** window, enter and confirm the certificate password.
6. **Optional:** Enter descriptive text in the **Comment** field.
7. Click **OK** and enter a path to save the p12 file.

The new certificate shows in the **Certificate**. The status is set to **Valid**.

8. Click **OK**.
9. Send the .p12 file to the end user by secure email or other secure means.

Creating Certificate Registration Key

After creating a user certificate, you must then make this certificate available to remote access users. Use this procedure to create a certificate registration key that lets the user enroll the certificate for use with a device.

To create a certificate registration key:

1. Create the user certificate (see *"Enabling a User Certificate" on the previous page*).
2. In the **User Properties** window, from the navigation tree click **Certificates**.
3. In the **Certificates** pane, click **New**.
4. Select **Registration key for certificate enrollment**.
5. In the **Registration Key for Certificate Enrollment** window, select the number of days before the certificate expires.
6. Click the email button to send the registration key to the user.
7. **Optional:** Enter descriptive text in the **Comment** field.
8. Click **OK**.

Instructions for End Users

Remote Access VPN users can use many different clients to connect to network resources. It is the administrator's responsibility to give appropriate instructions to end users to make sure that they successfully enroll the certificate.

The *"Creating Remote Access VPN Certificates for Users" on page 50* section gives some general procedural guidelines that apply to many VPN clients. For detailed instructions, refer to the VPN client documentation.

Enrolling User Certificates - ICA Management Tool

To use the ICA Management to enroll a user certificate:

1. In SmartConsole, from the **Objects Bar** click **Users > Users**.
2. Create a new user or double-click an existing user.

   The **User Properties** window opens.
3. From the navigation tree click **Encryption**.

4. Click **Edit**.

   The **IKE Phase 2 Properties** window opens.

5. Click the **Authentication** tab, and select **Public Key**.
6. Click **OK**.
7. Publish the changes.
8. Enroll the user certificate using the **ICA management tool**.

Using Certificates Using Third Party PKI

Using third party PKI involves creating a certificate for the user and can also include a certificate for the Security Gateway.

You can use a third-party OPSEC PKI certificate authority that supports the PKCS#12, CAPI or Entrust standards to issue certificates for Security Gateways and users. The Security Gateway must trust the CA and have a certificate issued by the CA.

See *"Certificate Parsing" on page 43* to configure which information the Security Gateway sends to the LDAP server to parse the certificate.

By default, for users managed on an LDAP server, the full distinguished name (DN) which appears on the certificate is the same as the user's name. But if the user is managed on the internal database, the user name and DN on the certificate will not match. For this reason, the user name in the internal database must be either the full DN which appears on the certificate or just the name which appears in the CN portion of the certificate. For example, if the DN which appears on the certificate is:

```
CN=John, OU=Finance, O=Widget Enterprises, C=US
```

The name of the user on the internal database must be one of these:

- `John`
- `CN=John, OU=Finance, O=Widget Enterprises, C=US`

Note - The DN on the certificate must include the user's LDAP branch. Some PKI solutions do not include (by default) the whole branch information in the subject DN, for example the DN only includes the common name. This can be rectified in the CA configuration.

Configuring Third-Party PKI Certificates

To use a third-party PKI solution:

1. In SmartConsole, from the **Objects Bar** click **Users > Users**.
2. Create a new user or double-click an existing user.

   The **User Properties** window opens.

3. From the navigation tree, click **Encryption**.
4. Click **Edit**.

   The **IKE Phase 2 Properties** window opens.
5. Click the **Authentication** tab and select **Public key**.
6. Define the third party Certificate Authority as an object in SmartDashboard.
7. Optional: Generate a certificate for your Security Gateway from the third party CA.
8. Generate a certificate for the remote user from the third party CA. (Refer to relevant third party documentation for details.)
9. Transfer the certificate to the user.
10. In **Global Properties** > **Authentication** window, add or disable suffix matching.

    For users with certificates, it is possible to specify that only certificates with a specified suffix in their DN are accepted. This feature is enabled by default, and is required only if:

    - Users are defined in the internal database, *and*
    - The user names are not the full DN.

All certificates DN's are checked against this suffix.

Note - If an hierarchy of Certificate Authorities is used, the chain certificate of the user must reach the same root CA that the Security Gateway trusts.

Using a Pre-Shared Secret

When using pre-shared secrets, the remote user and Security Gateway authenticate each other by verifying that the other party knows the shared secret: the user's password.

To enable authentication with pre-shared secrets:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access >VPN Authentication**.
3. In the **Support authentication methods** section, select **Pre-Shared Secret (ForSecuRemote client / SecureClient users)**.
4. Click **OK**.
5. Configure the Authentication settings for each applicable user:
   a. From the Objects Bar, double-click the user.

      The **User Properties** window opens.

b. From the navigation tree, click **Encryption**.

c. Select **IKE** and click **Edit**.

The **IKE Phase 2 Properties** window opens.

d. From the Authentication tab, click **Password (Pre-Shared Secret)**.

e. Enter and **Confirm** the **Password (Pre-shared secret)**.

f. Click **OK**.

6. Publish the SmartConsole session
7. Give the password to the user.

NT Group / RADIUS Class Authentication Feature

Authentication can take place according to NT groups or RADIUS classes.

In this way, remote access users are authenticated according to the remote access community group they belong to.

Note - Only NT groups are supported, not Active Directory.

Granting User Access Using RADIUS Server Groups

The Security Gateway lets you control access privileges for authenticated RADIUS users, based on the administrator's assignment of users to RADIUS groups. These groups are used in the Security Rule Base to restrict or give users access to specified resources. Users are unaware of the groups to which they belong.

Remote Authentication Dial-In User Service (RADIUS) is an external authentication method that provides security and scalability by separating the authentication function from the access server.

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. For administrators, the Security Management Server forwards the authentication requests. The RADIUS server, which stores user account information, does the authentication.

The RADIUS protocol uses UDP to communicate with the Security Gateway or the Security Management Server.

RADIUS servers and RADIUS server group objects are defined in SmartConsole.

To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, **RAD_<group to which the RADIUS users belong>**) to which the users belong.

Use these RADIUS attributes (refer to RFC 2865):

- For SecurePlatform - attribute "Class" (25)
- For other operating systems, including Gaia, Windows, and IPSO- attribute "Vendor-Specific" (26)

Sample workflow for RADIUS authentication configuration:

1. Create a RADIUS host object.
2. Configure the RADIUS server object settings.
3. Configure Security Gateways to use RADIUS authentication.
4. Define user groups.
5. Configure RADIUS authentication settings for user.
6. Complete the RADIUS authentication configuration.

Configuring Authentication for NT groups and RADIUS Classes

To enable this group authentication feature:

1. Set the `add_radius_groups` property in the `$FWDIR/conf/objects.C` file to `true`.
2. Define a generic* profile, with RADIUS as the authentication method.
3. Create a rule in the Policy Rule Base whose "source" is this group of remote users that authenticate using NT Server or RADIUS.

Office Mode IP assignment file

This method also works for Office Mode. The group listed in the `$FWDIR/conf/ipassignment.conf` file points to the group that authenticates using NT group authentication or RADIUS classes (see *"Office Mode through the "ipassignment.conf" File" on page 78*).

Associating a RADIUS Server with a Security Gateway

You can associate users with the RADIUS authentication server in the **User Properties** > **Authentication** tab.

You can override that association and associate a Security Gateway with a RADIUS server.

To configure RADIUS association, use the `dbedit` command (see sk13301).

To associate one or more RADIUS servers to a Security Gateway:

```
modify network_objects <gateway obj> radius_server servers:<radius obj>
```

To turn off the RADIUS-gateway association:

```
modify users <user obj> use_fw_radius_if_exist false
```

Configuring RADIUS Objects

To create a new RADIUS host object:

1. In SmartConsole, the **Objects** tab, click **New > Host**.

   The **New Host** window opens.
2. Enter the **Object Name** and the **IP Address** of the new RADIUS host object, and click **OK**.
3. Install the policy.

To configure the RADIUS server object settings:

1. In SmartConsole, the **Objects** tab, click **New > More > Server > More > RADIUS**.

   The **RADIUS Server Properties** window opens.
2. Configure new server properties:
   - Enter the **Name** of the RADIUS server object.
   - Select the RADIUS **Host** object.
   - Select the **Service** - **RADIUS** (on port 1645) or **NEW-RADIUS** (on port 1812 service).

     Note - The default setting is **RADIUS**, but the RADIUS standards group recommends using **NEW-RADIUS**, because port 1645 can conflict with the datametrics service running on the same port.
   - Enter the **Shared Secret** that you configured on the RADIUS server

- Select the version - **RADIUS Ver. 1.0 Compatible** (RFC 2138 compliant) or **RADIUS Ver. 2.0 Compatible** (RFC 2865 compliant)
- Select the peer authentication **Protocol** - **PAP** or **MS-CHAP v2**
- If you use more than one RADIUS authentication server, select the **Priority**

3. Click **OK**.

To configure a Security Gateway to use RADIUS authentication:

1. In SmartConsole, go to the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.
2. In the Security Gateway Properties window that opens, select **Other > Legacy Authentication**.
3. In the **Enabled Authentication Schemes** section, select **RADIUS**.
4. Click **OK**.

Configuring RADIUS Settings for Users

To define a RADIUS user group:

1. In SmartConsole, the **Objects** tab, click **New > More > Users > User Group**.

   The **New User Group** window opens.
2. Enter the name of the group in this format: **RAD_<*group_name*>**.

   Make sure the group is empty.
3. Click **OK**.
4. Install the policy.

To configure RADIUS authentication settings for users with Security Gateway user accounts:

1. Create new internal user profile for each user. In SmartConsole, click **Objects** > **New**> **More**> **User**> **User**.

   The **User Properties** window opens.
2. In the **General Properties** tab, configure these settings:
   - Enter a **User Name** for the RADIUS server.
   - Set the **Expiration Date**.
3. In the **Authentication** tab, configure these settings:

- Select **RADIUS** from the **Authentication method** list
- From the **RADIUS Server** list, select the RADIUS object that you configured earlier

4. Click **OK**.

To configure RADIUS authentication settings for users without Security Gateway user accounts:

Create a new external user profile for each user in SmartDashboard, which opens from SmartConsole.

1. Open SmartDashboard:
   a. In SmartConsole, go to the **Manage & Settings** tab.
   b. Click **Blades**.
   c. Click one of the links for **Configure in SmartDashboard**.
2. From the **Network** object tree, click the **Users** icon.
3. Right-click **External User Profiles** and select **New External User Profile** > **Match all users** (or **Match by domain**).

   If you support more than one external authentication scheme, set up External User Profiles with the **Match By Domain** setting.

   The **External User Profile Properties** window opens.
4. In the **General Properties** tab, configure these settings:
   - Enter a **User Name** for the RADIUS server. (When configuring **Match all users** as an External User Profile, the name **"generic*"** is automatically assigned)
   - Set the **Expiration Date**.
5. In the **Authentication** tab, configure these settings:
   - Select **RADIUS** from the **Authentication Scheme** list.
   - From the **Select a RADIUS Server or Group of Servers** list, select the RADIUS object that you configured earlier
6. Click **OK**.
7. Close SmartDashboard.
8. Install policy in SmartConsole.

Completing RADIUS Authentication Configuration

To complete the RADIUS authentication configuration:

1. In SmartConsole, create the required Access Control rules to allow access to users authenticated through the RADIUS server.
2. Make sure that communication between the firewall and the server is not NATed in the Address Translation Rule Base.
3. Save the changes.
4. Close all SmartConsole windows connected to the Management Server.
5. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
6. Change the value of the **add_radius_groups** attribute from `false` to `true`.
7. Save and then close Database Tool (GuiDBEdit Tool).
8. Connect with SmartConsole to the Management Server.
9. Install the policy.
10. On the RADIUS server, edit the RADIUS users to include a "`class`" RADIUS attribute on the users **Return** list that corresponds to the user group that they access.

To use a different attribute instead of the "`class`" attribute:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Change the value of the **firewall_properties** attribute **radius_groups_attr** to the new RADIUS attribute.
4. Save the changes.
5. Close Database Tool (GuiDBEdit Tool).
6. Open SmartConsole.
7. Install the policy.
8. On the RADIUS server, make sure that you use the same RADIUS attribute on users' Return lists that corresponds to the Firewall user group that they access.

Authentication on a RADIUS Server over MS-CHAPv2 with UPN

To enable authentication of Remote Access VPN Clients on a RADIUS server over Microsoft Challenge-Handshake Authentication Protocol (MS-CHAPv2) with UPN (<username>@<domain>):

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Get the current value:

   ```
   ckp_regedit -p SOFTWARE/Checkpoint/VPN1 | grep --color RADIUS_
   MSCHAPV2_UPN
   ```

4. To enable this feature:

   ```
   ckp_regedit -a SOFTWARE/Checkpoint/VPN1 RADIUS_MSCHAPV2_UPN -n
   1
   ```

   This command applies immediately and does **not** require a restart.

   To disable this feature:

   ```
   ckp_regedit -a SOFTWARE/Checkpoint/VPN1 RADIUS_MSCHAPV2_UPN -n
   0
   ```

Working with RSA Hard and Soft Tokens

If you use SecurID for authentication, you must manage the users on RSA's ACE management server. ACE manages the database of RSA users and their assigned hard or soft tokens. The client contacts the site's Security Gateway. The Security Gateway contacts the ACE Server for user authentication information. This means:

- The remote users must be defined as RSA users on the ACE Server.
- On the Security Gateway, the SecurID users must be placed into a group with an external user profile account that specifies SecurID as the authentication method.

SecurID Authentication Devices

Several versions of SecurID devices are available. The older format is a small device that displays a numeric code, called a *tokencode*, and time bars. The token code changes every sixty seconds, and provides the basis for authentication. To authenticate, the user must add to the beginning of the tokencode a special password called a PIN number. The time bar indicates how much time is left before the next tokencode is generated. The remote user is requested to enter both the PIN number and tokencode into the client connection window.

The newer format resembles a credit card, and displays the tokencode, time bars and a numeric pad for typing in the PIN number. This type of device mixes the tokencode with the entered PIN number to create a *Passcode*. The client requests only the passcode.

SoftID operates the same as the passcode device but consists only of software that sits on the desktop.

The Advanced view displays the tokencode and passcode with COPY buttons, allowing the user to cut and paste between softID and the client:

Enabling Hybrid Mode and Methods of Authentication

Hybrid mode allows the Security Gateway and remote access client to use different methods of authentication.

To enable Hybrid Mode:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access > VPN Authentication**.
3. In the **Support authentication methods** section, click **Support Legacy Authentication for SC (hybrid mode), L2TP (PAP), and Nokia clients (CRACK)**.
4. Click **OK**.
5. Install the policy.

Defining User Authentication Methods in Hybrid Mode

To define the Hybrid Mode authentication for a user:

1. From the Objects Bar, double-click the user.

   The **User Properties** window opens.
2. From the navigation tree, click **Authentication**.

3. Select the **Authentication Scheme**.
4. Configure the necessary settings.
5. Click **OK**.
6. Install the policy.
7. Give these credentials to the user.

Office Mode

The Need for Remote Clients to be Part of the LAN

As remote access to internal networks of organizations becomes widespread, it is essential that remote users are able to access as many of the internal resources of the organization as possible. Typically, when remote access is implemented, the client connects using an IP address locally assigned by, for example, an ISP. The client may even receive a non-routable IP which is then hidden behind a NATing device. Because of this, several problems may arise:

- Some networking protocols or resources may require the client's IP address to be an internal one. Router ACLs (access lists), for example, might be configured to allow only specific or internal IP addresses to access network resources. This is difficult to adjust without knowing the remote client's IP address in advance.
- When assigned with a non-routable IP address a conflict may occur, either with similar non-routable addresses used on the corporate LAN, or with other clients which may receive the same IP address while positioned behind some other hiding NAT device.

  For example, if a client user receives an IP address of 10.0.0.1 which is entered into the headers of the IPSec packet. The packet is NATed. The packet's new source IP address is 192.168.17.5. The Security Gateway decapsulates the NATed IP and decrypts the packet. The IP address is reverted to its original source IP address of 10.0.0.1. If there is an internal host with the same IP, the packet will probably be dropped (if Anti-Spoofing is turned on). If there is no duplicate IP, and the packet is forwarded to some internal server, the server will then attempt to reply to a non-existent address.
- Two remote users are assigned the same IP address by an ISP (for example, two users are accessing the organization from hotels which provide internal addresses and NAT them on the outbound). Both users try to access the internal network with the same IP address. The resources on the internal network of the organization may have difficulty distinguishing between the users.

Office Mode

Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected. The address may be taken either from a general IP address pool, or from an IP address pool specified per user group. The address can be specified per user, or via a DHCP server, enabling the use of a name resolution service. With DNS name resolution, it is easier to access the client from within the corporate network.

It is possible to allow all your users to use Office Mode, or to enable the feature for a specific group of users. This can be used, for example, to allow privileged access to a certain group of users (e.g., administrators accessing the LAN from remote stations). It is also useful in early integration stages of Office Mode, allowing you time to "pilot" this feature on a specific group of users, while the rest of the users continue to work in the traditional way.

Office Mode is supported with the following:

- Endpoint Security VPN
- SSL Network Extender
- Crypto
- L2TP

How Office Mode Works

When you connect to the organization, an IKE negotiation is initiated automatically to the Security Gateway. When using Office Mode, a special IKE mode called config mode is inserted between phase 1 and phase 2 of IKE. During config mode, the client requests an IP from the Security Gateway. Several other parameters are also configurable this way, such as a DNS server IP address, and a WINS server IP address.

After the Security Gateway allocates the IP address, the client assigns the IP to a Virtual Adapter on the Operating system. The routing of packets to the corporate LAN is modified to go through this adapter. Packets routed in this way bear the IP address assigned by the Security Gateway as their source IP address. Before exiting through the real adapter, the packets will be IPsec encapsulated using the external IP address (assigned to the real adapter) as the source address. In this way, non-routable IP addresses can be used with Office Mode; the Office Mode non-routable address is concealed within the IPsec packet.

For Office Mode to work, the IP address assigned by the Security Gateway needs to be routable to that Security Gateway from within the corporate LAN. This lets packets on the LAN being sent to the client to be routed back through the Security Gateway (see *"Office Mode and Static Routes in a Non-flat Network" on page 68*).

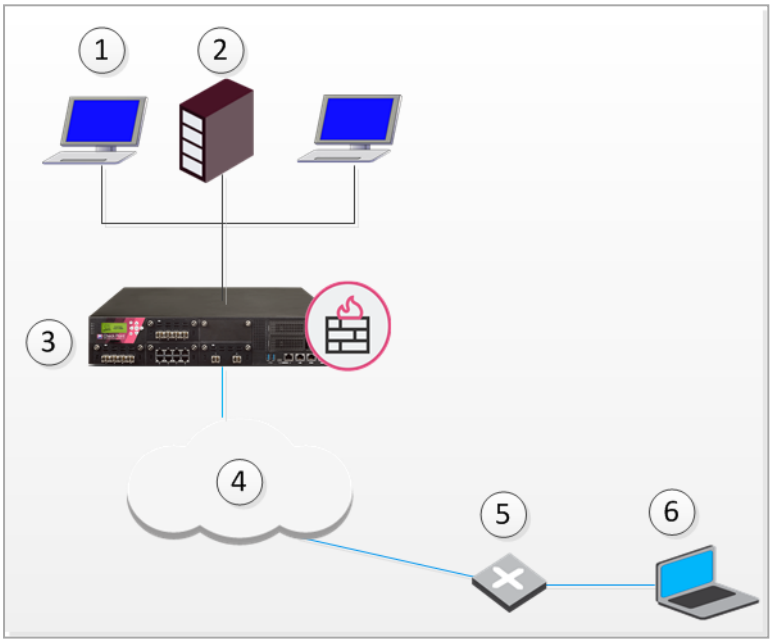
Note - A remote user with SecuRemote client only is not supported in Office Mode.

A Closer Look

The following steps illustrate the process taking place when a remote user connected through Office Mode wishes to exchange some information with resources inside the organization:

- The user is trying to connect to some resource on the LAN, thus a packet destined for the internal network is to be sent. This packet is routed through the virtual interface that Office Mode had set up, and bears the source IP address allocated for the remote user.

- The packet is encrypted and builds a new encapsulating IP header for it. The source IP of the encapsulating packet is the remote client's original IP address, and its destination is the IP address of the Security Gateway. The encapsulated packet is then sent to the organization through the Internet.
- The Security Gateway of the organization receives the packet, decapsulates and decrypts it, revealing the original packet, which bears the source IP allocated for the remote user. The Security Gateway then forwards the decapsulated packet to its destination.
- The internal resource gets a packet seemingly coming from an internal address. It processes the packet and sends response packets back to the remote user. These packets are routed back to the (internal) IP address assigned to the remote user.
- The Security Gateway gets the packet, encrypts and encapsulates it with the remote users' original (routable) IP address and returns the packet back to the remote user:



Item	Description
1	Host IP Address 10.0.01
2	Server
3	Gateway
4	Internet
5	ISP Router
6	User's machine

- The remote host uses the Office mode address in the encapsulated packet and 10.0.0.1 in the encapsulating header.
- The packet is NATed to the new source address: 192.168.17.5
- The Security Gateway decapsulates the NATed IP address and decrypts the packet. The source IP address is the Office Mode address.
- The packet is forwarded to the internal server, which replies correctly.

Assigning IP Addresses

The internal IP addresses assigned by the Security Gateway to the remote user can be allocated using one of the following methods:

- IP Pool
- DHCP Server

IP Pool

The System Administrator designates a range of IP addresses to be utilized for remote client machines. Each client requesting to connect in Office Mode is provided with a unique IP address from the pool.

IP Assignment Based on Source IP Address

IP addresses from the IP pool may be reserved and assigned to remote users based on their source IP address. When a remote host connects to the Security Gateway, its IP address is compared to a predefined range of source IP addresses. If the IP address is found to be in that range, then it is assigned an Office Mode IP address from a range dedicated for that purpose.

The IP addresses from this reserved pool can be configured to offer a separate set of access permissions given to these remote users.

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server can be used to allocate IP addresses for Office Mode clients. When a remote user connects to the Security Gateway using Office Mode, the Security Gateway requests the DHCP server to assign the user an IP address from a range of IP addresses designated for Office Mode users.

Security Gateway DHCP requests can contain various client attributes that allow DHCP clients to differentiate themselves. The attributes are pre-configured on the client side operating system, and can be used by different DHCP servers in the process of distributing IP addresses. Security Gateways DHCP request can contain the following attributes:

- Host Name
- Fully Qualified Domain Name (FQDN)

- Vendor Class
- User Class

RADIUS Server

A RADIUS server can be used for authenticating remote users. When a remote user connects to a Security Gateway, the username and password are passed on to the RADIUS server, which checks that the information is correct, and authenticates the user. The RADIUS server can also be configured to allocate IP addresses.

Note - Authentication and IP assignment must be performed by the same RADIUS server.

Office Mode and Static Routes in a Non-flat Network

A flat network is one in which all stations can reach each other without going through a bridge or a router. One segment of a network is a "flat network". A static route is a route that is manually assigned by the system administrator (to a router) and needs to be manually updated to reflect changes in the network.

If the LAN is non-flat (stations reach each other via routers and bridges) then the OM address of the remote client must be statically assigned to the routers so that packets on the LAN, destined for the remote client, are correctly routed to the Security Gateway.

IP Address Lease duration

When a remote user's machine is assigned an Office mode IP address, that machine can use it for a certain amount of time. This time period is called the "IP address lease duration." The remote client automatically asks for a lease renewal after half of the IP lease duration period has elapsed. If the IP lease duration time is set to 60 minutes, a renewal request is sent after 30 minutes. If a renewal is given, the client will request a renewal again after 30 minutes. If the renewal fails, the client attempts again after half of the remaining time, for example, 15 minutes, then 7.5 minutes, and so on. If no renewal is given and the 60 minutes of the lease duration times out, the tunnel link terminates. To renew the connection the remote user must reconnect to the Security Gateway. Upon reconnection, an IKE renegotiation is initiated and a new tunnel created.

When the IP address is allocated from a predefined IP pool on the Security Gateway, the Security Gateway determines the IP lease duration period. The default is 15 minutes.

When using a DHCP server to assign IP addresses to users, the DHCP server's configuration determines the IP lease duration. When a user disconnects and reconnects to the Security Gateway within a short period of time, it is likely that the user will get the same IP address as before.

Using Name Resolution - WINS and DNS

To facilitate access of a remote user to resources on the internal network, the administrator can specify WINS and DNS servers for the remote user. This information is sent to the remote user during IKE config mode along with the IP address allocation information, and is used by the remote user's operating system for name-to-IP resolution when the user is trying to access the organization's internal resources.

Anti-Spoofing

With Anti-Spoofing, a network administrator configures which IP addresses are expected on each interface of the Security Gateway. Anti-Spoofing ensures IP addresses are only received or transmitted in the context of their respective Security Gateway interfaces. Office Mode poses a problem to the Anti-Spoofing feature, since a client machine can connect and authenticate through several interfaces, e.g. the external interface to the Internet, or the wireless LAN interface; thus an Office Mode IP address may be encountered on more than one interface. Office Mode enhances Anti-Spoofing by making sure an encountered Office Mode IP address is indeed assigned to the user, authenticated on the source IP address on the IPsec encapsulating packet, i.e. the external IP.

Using Office Mode with Multiple External Interfaces

Typically, routing is performed before encryption in VPN. In some complex scenarios of Office Mode, where the Security Gateway may have several external interfaces, this might cause a problem. In these scenarios, packets destined at a remote user's virtual IP address will be marked as packets that are supposed to be routed through one external interface of the Security Gateway. Only after the initial routing decision is made do the packets undergo IPsec encapsulation. After the encapsulation, the destination IP address of these packets is changed to the original IP address of the client. The routing path that should have been selected for the encapsulated packet might be through a different external interface than that of the original packet (since the destination IP address changed), in which case a routing error occurs. Office Mode has the ability to make sure that all Office Mode packets undergo routing after they are encapsulated.

Office Mode Per Site

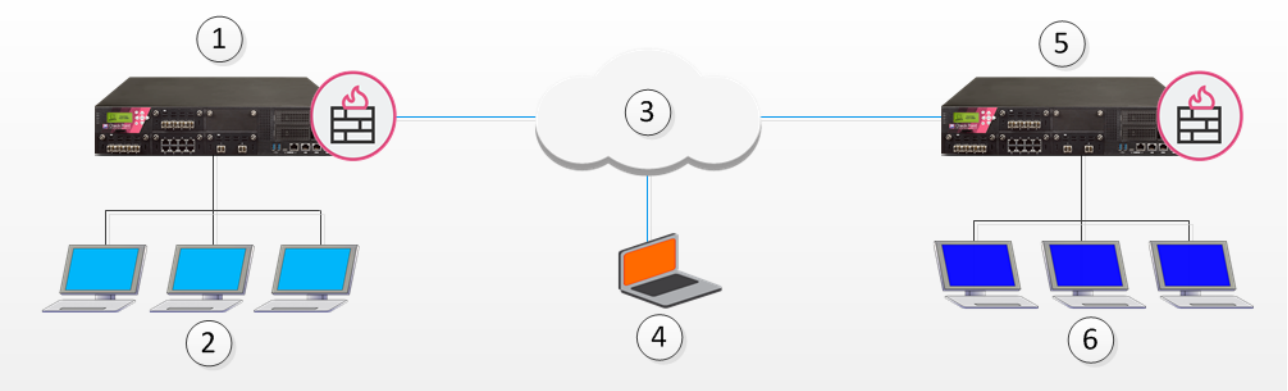
After a remote user connects and receives an Office Mode IP address from a Security Gateway, every connection to that Security Gateways encryption domain will go out with the Office Mode IP as the internal source IP. The Office Mode IP is what hosts in the encryption domain will recognize as the remote user's IP address.

The Office Mode IP address assigned by a specific Security Gateway can be used in its own encryption domain and in neighboring encryption domains as well. The neighboring encryption domains should reside behind Security Gateways that are members of the same VPN community as the assigning Security Gateway. Since the remote hosts' connections are dependent on the Office Mode IP address it received, if the Security Gateway that issued the IP becomes unavailable, all he connections to the site will terminate.

In order for all Security Gateways on the site to recognize the remote users Office Mode IP addresses, the Office Mode IP range must be known by all of the Security Gateways and the IP ranges must be routable in all the networks. However, when the Office Mode per Site feature is in use, the IP-per-user feature cannot be implemented.

Note - When Office Mode per Site is activated, Office Mode Anti-Spoofing is not enforced.

In this scenario:



Item	Description
1	Security Gateway 1
2	VPN Domain A
3	Internet
4	Remote Host
5	Security Gateway 2
6	VPN Domain B

- The remote user makes a connection to Security Gateway 1.
- Security Gateway 1 assigns an Office Mode IP address to the remote user.

- While still connected to Security Gateway 1, the remote user can make a connection to hosts behind Security Gateway 2 using the Office Mode IP address issued by Security Gateway 1.

Enabling IP Address per User

In some configurations, a router or other device restricts access to portions of the network to specified IP addresses. A remote user connecting in Office Mode can get a specified IP address, or an IP address from a specified range, which will allow the connection to pass through the router.

Note - If this feature is implemented, you must enable Anti-Spoofing for Office Mode (see *"Anti-Spoofing" on page 69*).

You can use a DHCP server or IP Pool to allocate IP addresses.

DHCP Server

To configure Office Mode addresses that are allocated by a DHCP server:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway Properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **VPN Clients > Office Mode**.
3. Enable Office Mode for a **group** or **all users**.
4. In the Office Mode Method section select these options:
   - Click **Using one of the following methods**
   - Click **Automatic (using DHCP)**
5. Click **MAC address for DHCP allocation**, select **calculated per user name**
6. Click **OK**.
7. Install the Access Control Policy.
8. Connect to the command line on the Security Gateway.
9. Run this command to get the MAC address assigned to the user:

   ```
   vpn macutil <username>
   ```
10. On the DHCP Server make a new reservation, specifying the IP address and MAC address, assigning the IP address for the exclusive use of the given user.

The "ipassignment.conf" File

The `$FWDIR/conf/ipassignment.conf` file on the Security Gateway, is used to implement the IP-per-user feature. It lets the administrator to assign specific addresses to specific users or specific ranges to specific groups when they connect using Office Mode or L2TP clients.

Note:

- You must add this file manually on all Security Gateways.
- The Simultaneous Login is not supported for the SSL Network Extender (SNX) client when the Office Mode Method is configured to allocate IP addresses from the `$FWDIR/conf/ipassignment.conf` file. See sk176343.

Sample ipassignment.conf File

```
# This file is used to implement the IP-per-user feature.  It allows the
# administrator to assign specific addresses to specific users or specific
# ranges to specific groups when they connect using Office Mode or L2TP.
#
# The format of this file is simple:  Each line specifies the target
# gateway, the IP address (or addresses) we wish to assign and the user
# (or group) name as in the following examples:
#
# Gateway        Type   IP Address                                    User Name
# =============  =====  ========================================
=========================================
# Paris-GW,              10.5.5.8,                                     Jean
# Brasilia,      addr   10.6.5.8, wins=(192.168.3.2,192.168.3.3)  Joao  # comments are allowed
# Miami,         addr   10.7.5.8, dns=(192.168.3.7,192.168.3.8)
CN=John,OU=users,O=cpmgmt.acme.com.gibeuu
# 10.1.1.2       range  100.107.105.110-100.107.105.119/24        Finance
# *              net    10.7.5.32/28  suffix=(acct.acme.com)      Accounting
#
# Note that real records do not begin with a pound-sign (#), and the commas
# are optional.  Invalid lines are treated as comments.  Also, the
# user name may be followed by a pound-sign and a comment.
#
# The first item is the gateway name or address.  On lines that assign
# multiple IP addresses to a group of users or a network (range or net
# in the second item) this should be the physical address of the gateway,
# or an asterisk (*) to signify all gateways.
# On lines that assign one IP for one user this could be the gateway
# name as well.  A gateway will only honor lines that refer to it.
#
# The second item is a descriptor.  It can be 'addr', 'range' or 'net'.
# 'addr' specifies one IP for one user.  This prefix is optional.
# 'range' and 'net' specify a range of addresses.  These prefixes are
# required.
#
# The third item is the IP address or addresses.  In the case of a single
# address, it is specified in standard dotted decimal format.
# ranges can be specified either by the first and last IP address, or using
# a net specification.  In either case you need to also specify the subnet
# mask length ('/24' means 255.255.255.0).  With a range, this is the subnet
# mask.  With a net it is both the subnet mask and it also determines the
# addresses in the range.
#
# After the third item come any of three keyword parameters.  These are
# specifications for WINS (or NBNS) servers, for DNS servers and a DNS
# suffix.  The parameters themselves are on the format 'keyword=(params)'
# where the params can be one address (such as "192.168.3.2"), several
# IP addresses (such as "192.168.3.2,192.168.3.3") or a string (only
# for the DNS suffix.  The relevant keywords are "dns", "wins" and
# "suffix" and they are not case-sensitive.
# Inside the keyword parameters there must be no spaces or any other
# extra characters.  These will cause the entire line to be ignored.
#
# The last item is the user name.  This can be a common name if the
# user authenticates with some username/password method (like hybrid
# or MD5-Challenge) or a DN if the user authenticates with a
# certificate.
#
```

Office Mode Considerations

IP Pool versus DHCP

The question of whether IP addresses should be assigned by the Firewall (using IP pools) or by a DHCP server is a network administration and financial issue. Some network administrators may prefer to manage all of their dynamic IP addresses from the same location. For them, a central DHCP server might be preferable. On the other hand, purchasing a DHCP server can be viewed by some as an unnecessary financial burden, in which case the IP pool option might be preferred.

Routing Table Modifications

IP addresses, assigned by Office Mode need to be routed by the internal LAN routers to the Security Gateway (or Security Gateway cluster) that assigned the address. This is to make sure packets, destined to remote access Office Mode users, reach the Security Gateway in order to be encapsulated and returned to the client machine. This may require changes to the organization's routing tables.

Configuring Office Mode

Before configuring Office Mode the assumption is that standard VPN Remote Access has already been configured.

Before starting the Office Mode configuration, you must select an internal address space designated for remote users using Office Mode. This can be any IP address space, as long as the addresses in this space do not conflict with addresses used within the enterprise domain. It is possible to choose address spaces which are not routable on the Internet, such as 10.x.x.x.

The basic configuration of Office Mode is using IP pools. You can also configure Office Mode using DHCP for address allocation (see *"DHCP Configuration" on page 79*).

IP Pool Configuration

Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway.

To deploy the basic Office Mode using IP pools:

1. From the Objects Bar click **New > Network**.

   The **New Network** window opens.

2. In the **General** tab, set the IP address pool range:

a. Enter a **Name** for the network.

b. In **Network Address** enter the first IP address.

c. In **Net Mask** enter the subnet mask according to the required amount of IP addresses (entering 255.255.255.0, for example, will designate all 254 IP addresses from 10.130.56.1 to 10.130.56.254 for Office Mode addresses.)

d. Click **OK** and publish the changes.

3. Click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway Properties window opens and shows the **General Properties** page.

4. From the navigation tree, click **VPN Clients > Office Mode**.

5. Configure these settings:

   a. In the **Office Mode Method** section:

      i. Select **Using one of the following methods**.

      ii. Select **Manual (using IP pool)**.

      The option **Automatic (using DHCP)** is **not** supported when working with SSL Network Extender.

      iii. From **Allocate IP from network** drop-down list, select the applicable IP Pool network object.

      Notes :

      - In a Cluster object, you must configure this setting on the **Cluster Members** page > edit each Cluster Member object > click **VPN** tab.
      - In Cluster Load Sharing mode, you must divide the IP Pool to different pool on each cluster member. This is to prevent race conditions where two members allocate the same free IP. ClusterXL in High Availability mode supports both two different and the same IP Pool for the two Cluster Members.

      iv. Click **Optional Parameters**, and in the **IP lease duration** field, enter the number of minutes that the IP address is used by the remote host.

      Click **OK**.

b. In the **Anti-Spoofing** section:

i. Select **Perform Anti-Spoofing on Office Mode addresses**.

ii. **Optional:** From **Additional IP Address for Anti-Spoofing** drop-down list, select the applicable object.

6. Click **OK**.
7. Install the Access Control Policy.

To specify which WINS and DNS servers Office Mode users can use:

Note - Configure WINS and DNS servers on the Security Management Server only when IP Pool is the selected method.

1. Create a DNS server object.
   a. From the **Objects** panel click **New > Host**.
   b. In the **General** page, enter the **Object Name** and **IP address** settings.
   c. In the **Servers** page, click **DNS Server**.
   d. Click **OK**.
2. Create a WINS server object.
   a. From the **Objects** panel click **New > Host**.
   b. In the **General** page, enter the **Object Name** and **IP address** settings.
   c. Click **OK**
3. Publish the SmartConsole session.
4. From the left navigation panel, click **Gateways & Servers**.
5. Double-click the Security Gateway / Cluster object.
6. From the navigation tree, click **VPN Clients > Office Mode**.
7. Click **Optional Parameters**.
8. In the **DNS Servers** section, select **Primary** and select the applicable DNS server object.
9. In the **WINS Servers** section, select **Primary** and select the applicable WINS server object.
10. Click **OK**.
11. Click **OK**.
12. Install the Access Control Policy.

Configuring IP Assignment Based on Source IP Address

Configure the settings of the **IP Assignment Based on Source IP Address** feature in the `$FWDIR/conf/user.def` file. This file is located on the Security Management Server, which manages the gateways used for remote access.

You must define a range of source IP addresses and a range of Office Mode addresses. The `$FWDIR/conf/user.def` file can contain multiple definitions for multiple gateways.

The first range defined in each line is the source IP address range. The second range in the line is the Office Mode IP address range.

For example:

```
all@module1 om_per_src_range={<10.10.5.0, 10.10.5.129; 1.1.1.5,
1.1.1.87>,
                              <10.10.9.0, 10.10.9.255; 1.1.1.88,
1.1.1.95>};
all@module2 om_per_src_range={<70.70.70.4, 70.70.70.90;
8.8.8.6,8.8.8.86>};
```

In this scenario:

- (10.10.5.0, 10.10.5.129), (10.10.9.0, 10.10.9.255), and (70.70.70.4, 70.70.70.90) are the VPN remote clients source IP address ranges
- (1.1.1.5, 1.1.1.87), (1.1.1.88, 1.1.1.95), and (8.8.8.6, 8.8.8.68) are the Office Mode IP addresses that will be assigned to the remote users whose source IP falls in the range defined on the same line.

For example: A user with a source IP address between 10.10.10.5.0 and 10.10.5.129, will receive an Office Mode address between 1.1.1.5 and 1.1.1.87.

The IP Assignment Based on the Source IP Address is enabled with a flag in the `$FWDIR/conf/objects_5_0.c` file on the Security Management Server.

Add an attribute into the object of the Security Gateway:

1. Connect with the *Database Tool (GuiDBEdit Tool)* to the Security Management Server (Domain Management Server).
2. In the top left pane, go to **Global Properties > Properties**.
3. In the top right pane, select **firewall_properties**.
4. In the bottom pane, edit the **om_use_ip_per_src_range** parameter and select one of these values:
   - **exclusively** - If the remote host IP is not found in the source range, the remote user does not get an Office Mode IP address.

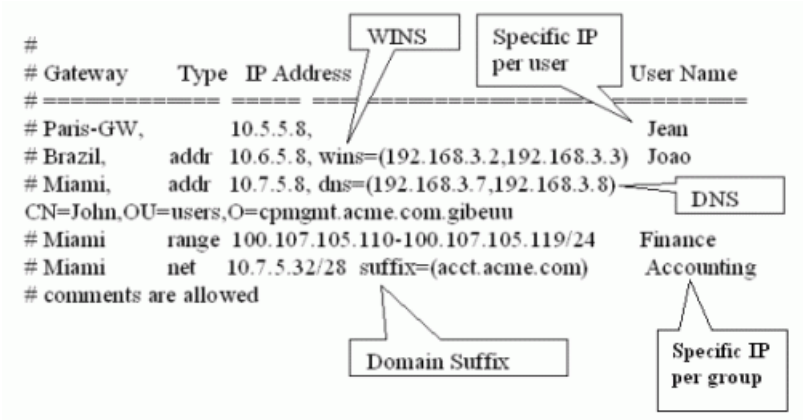
- **true** - If the remote host IP is not found in the source IP range, the user will get an Office Mode IP address using another method.
- **false** - The parameter is not used (this is the default).

Office Mode through the "ipassignment.conf" File

You can over-ride the Office Mode settings created on Security Management server. Edit the plain text file called `ipassignment.conf` in `$FWDIR/conf` on the Check Point Security Gateway. The Security Gateway uses these Office Mode settings and not those defined for the object in Security Management server.

The `ipassignment.conf` file controls:

- An **IP per user/group**, so that a particular user or user group always receives the same Office Mode address. This allows the administrator to assign specific addresses to users, or particular IP ranges/networks to groups when they connect using Office Mode.
- A different **WINS server** for a particular user or group.
- A different **DNS server**.
- Different **DNS domain suffixes** for each entry in the file.



Subnet masks and Office Mode Addresses

You cannot use the **ipassignment.conf** file to assign a subnet mask to a single user. If using IP pools, the mask is taken from the network object, or defaults to 255.255.255.0 if using DHCP.

Checking the Syntax

You can make sure the syntax of the **ipassignment.conf** file is correct with the command "`vpn ipafile_check`".

From a shell prompt run: `vpn ipafile_check ipassignment.conf`

The two parameters are:

- `warn` - Show errors.
- `detail` - Show all details.

Example:

```
[Expert@MyGW:0]# vpn ipafile_check ipassignment.conf warn
Reading file records...
Invalid IP address specification in line 0057
Invalid IP address specification in line 0058
Invalid subnet in line 0060

[Expert@MyGW:0]# vpn ipafile_check ipassignment.conf detail
Reading file records...

Line 0051 is a comment (starts with #)
Line 0052 is a comment (starts with #)
Line 0053 is a comment (starts with #)
Line 0054 is a comment (starts with #)
Line 0055 is a comment (starts with #)
Line 0056 ignored because it is empty
Invalid IP address specification in line 0057
Invalid IP address specification in line 0058
line 0059 is OK. User="paul"
Invalid subnet in line 0060
line 0061 is OK. Group="dns=1.1.1.1
Line 0062 ignored because it is empty
Line 0063 ignored because it is empty
Could not read line 64 in conf file - maybe EOF
[Expert@MyGW:0]#
```

DHCP Configuration

To configure Office Mode with a DHCP server:

1. On your DHCP server's configuration, make sure that you have designated an IP address space for Office Mode users (e.g., 10.130.56.0).
2. From the Objects Bar click **New > Host**.
3. Configure the settings for the name, IP address, and subnet mask.
4. Click **OK** and publish the changes.
5. Double-click the Remote Access Security Gateway object.

   The Security Gateway Properties window opens and shows the **General Properties** page.
6. From the navigation tree, click **VPN Clients > Office Mode**.

7. Configure these settings:
   a. Click **Automatic (use DHCP)**
   b. From **Use specific DHCP server**, select the DHCP server
   c. In **Virtual IP address for DHCP server replies**, enter an IP address from the sub network of the IP addresses which are designated for Office Mode usage.

      Office Mode supports DHCP Relay method for IP assignment, so you can direct the DHCP server as to where to send its replies. The routing on the DHCP server and that of internal routers must be adjusted so that packets from the DHCP server to this address are routed through the Security Gateway.
   d. **Optional:** In the **Additional IP addresses for Anti-Spoofing**, select the network object you have created with the IP address range you have set aside for Office Mode on the DHCP server.
8. Click **OK**.
9. Install the Access Control Policy.

To create a new network object for Office Mode on the DHCP server:

1. From the Objects Bar click **New > Network**.

   The **New Network** window opens.
2. In **Network Address** enter the first address that is used (e.g. 10.130.56.0).
3. In **Net Mask** enter the subnet mask according to the amount of addresses that is used.

   For example, the IP address 255.255.255.0 designates that all 254 IP addresses from 10.130.56.1 until 10.130.56.254 are set aside for remote host Office Mode addresses on the DHCP server.
4. Click **OK**.
5. Install the Access Control Policy.
6. Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway.

   For example, in the example above it is required to add routes to the class C sub network of 10.130.56.0 through the Security Gateway's IP address.
7. Make sure that the remote access clients are also configured to use Office Mode.

Office Mode - Using a RADIUS Server

To configure the RADIUS server to allocate IP addresses:

1. From the Objects Bar, click **Servers > RADIUS**.
2. Right-click the RADIUS server and click **Edit**.

   The **RADIUS Server Properties** window opens.
3. Click the **Accounting** tab.
4. Select **Enable IP Pool Management**.
5. Select the service the RADIUS server uses to communicate with remote users.
6. Click **OK**.
7. Install the Access Control Policy.

To configure the RADIUS server to perform authentication for remote users:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway Properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **VPN Clients > Office Mode.**
3. In the **Office Mode Method** section, click **From the RADIUS server used to authenticate the user**.
4. Click **OK**.
5. Install the Access Control Policy.

Use First Office Mode IP

To configure all gateways to work in Office Mode:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Remote Access > VPN - Advanced**.
3. In the **Office Mode** section, click **Use first allocated Office Mode IP address for all connections to the Security Gateways of the site**.
4. Click **OK**.
5. Install the Access Control Policy.

Desktop Security

The Need for Desktop Security

Security Gateways enforce Security Policies on traffic that passes through the Security Gateways in the network. Remote clients are located outside of the protected network and traffic to the remote clients does not pass through the Security Gateways. Therefore remote clients are vulnerable to attack.

Attackers can also use unprotected remote access clients to access the protected network, through the VPN tunnel.

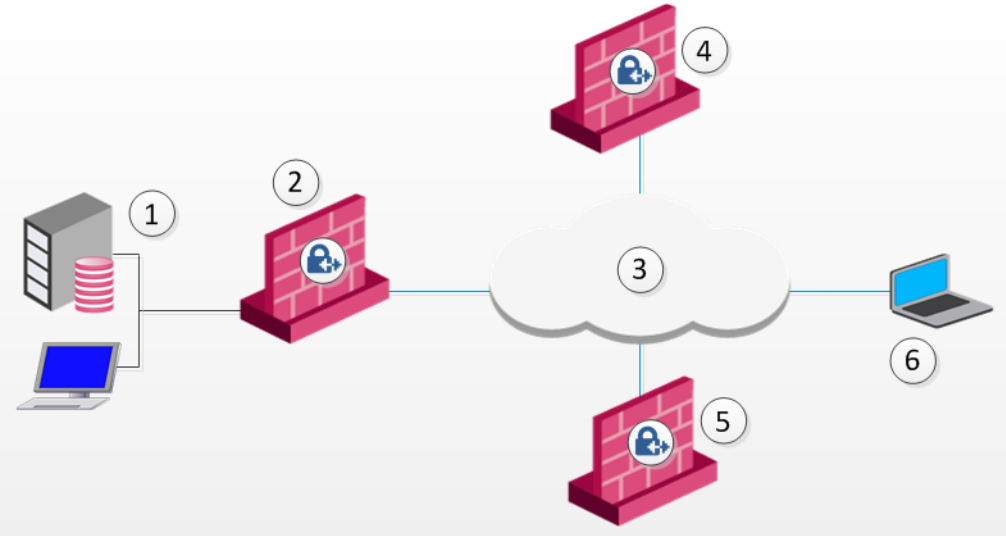
Desktop Security Solution

Check Point clients that include Desktop Security, such as Endpoint Security VPN, enforce a Desktop Security Policy on the client to give it Firewall protection. The administrator defines the Desktop Security Policy in the Desktop Rule Base in SmartDashboard. You can assign rules to specified user groups or to all users.

The Security Management Server downloads the Desktop Security Policy to a Policy Server, which is a feature that you enable on the Remote Access Security Gateway. Remote Access Client computers download their Desktop Security Policies from the Policy Server when they connect to the Security Gateway.

Clients enforce the Desktop Policy to accept, encrypt, or drop connections based on the Source, Destination, and Service.

Note - If you use Endpoint Security VPN as part of the Check Point Endpoint Security Suite, you can configure if your client Firewall comes from Desktop Security in SmartDashboard or SmartEndpoint.



Item	Description
1	Security Management Server
2	Firewall
3	Internet
4	Security Gateway and Policy Server
5	Security Gateway
6	Remote Access Client

The Desktop Security Policy

The Desktop Security Policy has Inbound and Outbound rules.

- **Inbound rules** - Enforced on connections going to the client computer.
- **Outbound rules** - Enforced on connections that originate from the client computer.

Each rule defines traffic by source, destination, and service. The rule defines what action to enforce on traffic that matches.

- **Source** - The network object that initiates the communication.
- **Destination** - The user group and location for Inbound communications, or the IP address of Outbound communications.
- **Service** - The service or protocol of the communication.
- **Action** - **Accept**, **Encrypt**, or **Block**.

Connections to computers inside of the organization, for example, all of the machines in the VPN domain of the Security Gateway, are automatically encrypted, even if the rule that lets them pass is an Accept rule.

Implied Rules

In addition to the rules that you define, the Desktop Security Policy has implicit rules added to the end of the inbound and outbound policies.

- The implicit **outbound** rule allows all connections that originate from the client to go out, if they do not match previous blocking rules:

  Any Destination, **Any** Service = **Accept**.

- The implicit **inbound** rule blocks all connections coming to the client that do not match

previous rules:

Any Source, **Any** Service = **Block**.

User Granularity

You can define different rules for remote users based on locations and user groups.

- **Locations** - Set rules to be implemented by physical location. For example, a user with a laptop in the office building will have a less restrictive policy than when the same user on the same laptop connects from a public wireless access point.
- **User Groups** - Set rules to be implemented for some users and not others. For example, define restrictive rules for most users, but give system administrators more access privileges. In addition, you can define rules to be enforced for all remote users, by not specifying a specific user group, but rather all users.

Rules apply to user groups, not individual users. The client does not identify user groups, so it must get group definitions from the Security Gateway when it connects. The Security Gateway resolves the user groups of the authenticated user and sends this information to the client. The client enforces the rules that apply to the user, based on the user groups.

Rules can also be applied to radius groups on the RADIUS server.

Default Policy

When a client is started, and before it connects to the Policy Server, it enforces a "default policy," which consists of the rules defined for all users in the last policy downloaded from the Policy Server. This is because at this point, the client does not know to which groups the user belongs. The default policy is enforced until the user downloads an updated policy (and the current user's group information) from a Policy server.

If a client loses its connection to the Policy Server, it enforces the default policy until the connection is restored and a Policy is downloaded.

Known Limitations

It is not supported to run Remote Access VPN clients (including Check Point Mobile Access Clients) inside of a Virtual Desktop Infrastructure (VDI).

Configuring Desktop Security

To enable the Security Gateway to be a Policy Server for Desktop Security:

1. Click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.

2. On the **Network Security** tab, select **IPsec VPN** and **Policy Server**.

3. Click **OK.**
4. Publish the changes.

To activate the Desktop Security policy:

1. Click **Security Policies** and open the **Manage Policies** window (CTRL + T).
2. Click the **All** icon.
3. Select the policy to edit and click **Edit**.

   The policy window opens.
4. Select **Desktop Security**.
5. Click **OK.**
6. Install policy.

To configure the Desktop Policy rules:

1. Click **Security Policies,** and from the navigation tree, click **Access Control > Desktop**.
2. Click **Open Desktop Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Desktop** tab.
3. Configure the inbound rules: Click **Rules>Add Rule** to add rules to the policy.

   In inbound rules, the client computer (the desktop) is the destination. Select user groups to which the rule applies.
4. Configure the outbound rules. Click **Rules>Add Rule** to add rules to the policy.

   In outbound rules, the client computer (the desktop) is the source. Select user groups to which the rule applies.
5. Click **Save** and close SmartDashboard.
6. Install the policy.

   Make sure that you install the Advanced Security policy on the Security Gateways and the Desktop Security policy on your Policy Servers.

Operations on the Rule Base

Define the Desktop Security Policy. Rules are managed in order: what is blocked by a previous rule cannot be allowed later.

The right-click menus of the Rule Base include these options:

- **Add Rule** - Add a rule above or below the selected rule.
- **Delete** - Delete rules which are no longer necessary.
- **Hide** - Hide rules that are irrelevant to your current view, to enhance readability of your Rule Base. Hidden rules are still applied.
- **Disable Rule** - Rules that are currently not implemented, but might be in the future, can be disabled.
- **Where Used** - See where the selected network object is included in other rules.
- **Copy as Image** - Copy a picture of the rule to your clipboard.
- **Copy Rule UID** - Copy the unique UID for the rule.
- **View Rule Logs** - See logs for traffic that matched this rule.
- **Negate Cell** - If a cell is negated, the rule will then be an "all-except" the object or service. For example, if http is negated in the **Service** column, all services except http are included in the rule.

Making a Rule for FTP

If clients use active FTP, you must add a rule to the Desktop Security Policy to specifically allow the service that you need. Select be one of the **active FTP** services that is not *ftp-pasv*.

To add the Active FTP Rule:

1. In SmartDashboard, open the **Desktop** tab.
2. Right-click the **Outbound rules** and select **Add**.
3. In the rule, select one of the FTP services as the service and **Accept** as the action.

Policy Server

A Policy Server is installed on a Security Gateway, when you enable it in the **General Properties** > **Network Security** tab. It serves as a repository for the Desktop Security Policy. Client machines download their Desktop Security Policies from the Policy Server.

When the client computer connects or re-authenticates to the site, it automatically checks the Policy Server for updates and downloads them.

Location-Based Policies

Location-based policies add location awareness support for the Desktop Firewall using these policies:

- **Connected Policy** - Enforced when:
  - VPN is connected.
  - VPN is disconnected and Location Awareness determines that the endpoint computer is on an internal network. The Connected Policy is not enforced "as is" but modified according to the feature's mode (the `disconnected_in_house_fw_policy_mode` property).
- **Disconnected Policy** - Enforced when the VPN is not connected and Location Awareness sees that the endpoint computer is not on an internal network.

Location-Based Polices for Desktop Firewall are disabled by default.

Configuring Location Awareness

The Location Awareness configuration is based on these properties in the client configuration file:

- **disconnected_in_house_fw_policy_enabled** - Defines if the feature is enabled or disabled.

  Possible values are:
  - `true` - enabled
  - `false` - disabled **(default)**
- **disconnected_in_house_fw_policy_mode** - Defines which policy will be enforced after Location Awareness detection.

  Possible values are:
  - `encrypt_to_allow` - Connected policy will be enforced, based on last connected user. Encrypt rules will be transformed to Allow rules **(default)**.
  - `any_any_allow` - "Any - Any - Allow" will be enforced.

To enable Location Awareness for desktop firewall:

1. On a Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Add the `disconnected_in_house_fw_policy_enabled` entry to the file:

```
:disconnected_in_house_fw_policy_enabled (
    :gateway (disconnected_in_house_fw_policy_enabled
    :default (true)
    )
)
```

3. Save the file and install the policy.

To configure the location based policy:

1. On a Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Add the `disconnected_in_house_fw_policy_mode` entry to the file:

```
:disconnected_in_house_fw_policy_mode (
    :gateway (disconnected_in_house_fw_policy_mode
    :default (encrypt_to_allow)
    )
)
```

3. Save the file and install the policy.

Note - It is highly recommended to configure default values for these properties in `trac_client_1.ttm` for all gateways.

Logs and Alerts

Desktop Security logs are saved locally on the client computer in:

- 32-bit systems:

  `C:\Program Files\CheckPoint\Endpoint Connect\trac_fwpktlog.log`

- 64-bit systems:

  `C:\Program Files(x86)\CheckPoint\Endpoint Connect\trac_fwpktlog.log`

Alerts are saved and uploaded to the Security Management Server when the client connects.

You can see alerts in the **Logs** tab in the SmartConsole Logs & Monitor view.

Blocking or Allowing IPv6 Traffic

By default, the desktop firewall allows IPv6 traffic to the client.

To block IPv6 traffic to the client:

1. On the Security Gateway, open this file for editing:

   `$FWDIR/conf/trac_client_1.ttm`

2. Add these lines:

```
:allow_ipv6 (
    :gateway (allow_ipv6
    :default (false)
    )
)
```

3. Save and close the file.
4. Install policy.

Wireless Hotspots

Desktop Policy can support wireless hotspots.

A proxy might be required.

Desktop Security Considerations

Plan your Desktop Security policy to balance considerations of security and convenience. You want to let users work as freely as possible, but at the same time, make it hard to attack the remote user's computer. Important points:

- Do not explicitly allow a service in the inbound policy unless the user has a server running on that port. If you do allow a service on inbound connections to the client, define who is allowed to open the connection, and from where.
- The best way to implement the outbound policy is to use rules only to block specified problematic services (such as Netbus) and allow the rest. A restrictive policy (for example, allow only POP3, IMAP and HTTP and block all the rest) will make it more difficult for your users to work. If you allow only specified services in the outbound policy and block all others, you will have to update the policy often when you learn that users need a different service.
- Outbound connections to the encryption domain of the organization are always encrypted automatically , even if the outbound rule for the service specifies **Accept**.
- Keep in mind that the implied rules (see *"Implied Rules" on page 83*) might allow or block services which were not explicitly handled in previous rules. For example, if a server runs on a client computer, you must create an explicit rule that allows the connection to the client computer. If you do not, the connection will be blocked by the inbound implicit block rule.

Letting Users Disable the Desktop Firewall

You can configure if Endpoint Security VPN users can choose to disable the firewall policy on their local machines.

If this option is enabled, when users right-click the client icon, they can select **Disable Security Policy**.

To change the 'Allow disable firewall' setting:

1. On the Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file with a text editor.
2. Find the line `:allow_disable_firewall` and set the value:
   - **true** - Users can disable their firewall policy.
   - **false** - Users do not have the option to disable their firewall policy.
   - **client_decide** - Takes the value from a file on the client machine
3. Save the file and install the policy.

Avoiding Double Authentication for Policy Server

When using Policy Server High Availability, it is possible that users will connect to the organization through one Security Gateway and to a Policy Server which is installed on a different module. In this case they will be prompted twice for authentication - once for the Security Gateway module and the other for the Policy Server. If a user usually connects to the organization through a specific Security Gateway, and this Security Gateway has a Policy Server module installed on it, this double authentication can be avoided by configuring the user's profile to use the **High Availability among all Policy Servers, trying selected first** option, and selecting the primary Policy Server as that one the Security Gateway through which the user usually connects to the organization. This way, after the user authenticates to the Security Gateway, he will automatically be authorized to download the security policy from the Policy Server installed on that Security Gateway.

Secure Configuration Verification

Use Case

Network and Firewall administrators can use different tools to control computers inside their organization. For example, to disable dangerous components such as Java and ActiveX controls in browsers, install Anti-Virus, and make sure they are run correctly.

For remote users who access the organization from outside of the LAN, the administrator cannot enforce control of the computer with the same tools. For example, suppose the remote user has ActiveX enabled, and connects to a website containing a malicious ActiveX control which infects his or her computer. When the remote user connects to the organization's LAN, the LAN becomes vulnerable as well.

A properly configured Desktop Security Policy, cannot protect against this type of attack, because the attack does not target a vulnerability in the access control to the endpoint computer. Instead it takes advantage of the vulnerable configuration of applications on the endpoint computer.

Introduction to Secure Configuration Verification (SCV)

Secure Configuration Verification (SCV) makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Use SCV to:

- Get reports on the configuration of remote clients.
- Make sure that clients comply with the organization's security policy.
- Block connectivity from clients that do not comply.

SCV does not replace the Desktop Security Policy, but works with it.

SCV uses SCV checks, which are DLLs (*plug-ins*) on the client, that are invoked and enforced according to the policy that you configure on the Management Server. SCV checks include sets of conditions that define a securely configured client system. Checks can include, for example, the user's browser configuration, the version of the Anti-Virus software installed on the desktop computer, and the operation of the personal firewall policy. These security checks are performed at pre-defined intervals by the remote access client. Based on the results of the SCV checks, the Security Gateway decides whether to allow or block connections from the client to the LAN.

- If the client passes **all** of the SCV checks, the client is compliant. The Security Gateway allows the connection.

- If the client fails **one** of the SCV checks, it is **not** compliant. You can configure the Security Gateway to reject connections from non-compliant endpoint computers, or to accept such connections and create a log entry.

Check Point's SCV solution comes with many predefined SCV checks for the operating system and user's browser, and also allows OPSEC partners, such as Anti-Virus software manufacturers, to add SCV checks for their own products.

Introduction to the *local.scv* file

You configure an SCV policy in the *local.scv* file on the Management Server. The file path is *$FWDIR/conf/local.scv*. This section describes the format and syntax of the file.

Format of the local.scv file

Sets and Sub-sets

Each set has a certain purpose which was predefined for it. For example, one set can be used to define certain parameters, another could specify certain actions that should take place in a certain event etc. Sets are differentiated by their names and hierarchy in a recursive manner. Each set can have a sub-set, and each sub-set can have a sub-set of its own and so on. Subsets can also contain logical expressions. Sets and sub-sets with more than one sub-sets/conditions are delimited by left and right parentheses **()**, and start with the set/sub-set name. Differentiation between sub-sets/expressions with the same hierarchy is done using the colon **:**. .For example:

```
(SetName
    :SubSetName1 (
        :ExpressionName1_1 (5)
        :ExpressionName1_2 (false)
    )
    :SubSetName2 (
        :ExpressionName2_1 (true)
        :SubSetName2_1 (
            :ExpressionName2_1_1 (10)
        )
   )
)
```

In the example above the set named `SetName` has two subsets - `SubSetName1` and `SubSetName2`:

- `SubSetName1` has two conditions in it (`ExpressionName1_1` and `ExpressionName1_2`).

- `SubSetName2` has one condition (`ExpressionName2_1)` and one subset (`SubSetName2_1`) in it.
- `SubSetName2_1` has one condition as well `(ExpressionName2_1_1`).

The "local.scv" Sets

The `local.scv` policy files contains one set called SCVObject.

This set must always be present and contains all the subsets which deal with the SCV checks and parameters.

SCVObject has these subsets:

- **SCVNames** - This section is the main SCV policy definition section, in which all of the SCV checks and actions are defined. This is the definition part of the SCV policy, and doesn't actually determine the SCV checks that will be performed. In this section sets of tests are defined. Later on, the administrator will choose from these sets those he wants to run on the user's desktop.
- **SCVPolicy** - This section specifies the names of the SCV checks that should actually be performed on the client's machine, from the SCV checks defined in **SCVNames**.
- **SCVGlobalParams** - This section contains some global SCV parameters.

The Difference between SCVNames and SCVPolicy

- The "`SCVNames`" section defines the different parameters for the checks.
- The "`SCVPolicy`" section states which checks are enforced.

To enforce a specific SCV check (such as Windows Security Monitor):

1. Configure the check's parameters in the "`SCVNames`" section.
2. Include the name of the check in the "`SCVPolicy`" section.

Logical expressions in the local.scv file

The expressions that you can use are set by the manufacturer. The names of the expressions are determined by the SCV check. The value of an expression is **true** or **false**, according to the result of an SCV check.

Logical Operators for Comparison Operators

You can use these logical comparison operators when working with RegMonitor in the SCV policy. Other logical operations are not supported:

Logical Operator	Description
=	Equals
!=	Does not equal
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to

Expressions are evaluated by checking the value of the expression (which corresponds to an SCV check) and comparing it with the value defined for the expression (the value in the parentheses). For example, in the browser monitor SCV check provided with the client, you can specify the following expression:

```
:browser_major_version (5)
```

This expression checks whether the version of the Internet Explorer browser installed on the client is 5.x. If the (major) version is 5, this expression is evaluated as true, otherwise it is evaluated as false. The name of the expression (e.g. "browser_major_version") is determined by the SCV application and is supplied by manufacturer.

If several expressions appear one after the other, they are logically ANDed, meaning that only if all expressions are evaluated as true, then the value of all of them taken together is true. Otherwise (if even one of the expressions is false), the value of all of them is false. For example:

```
:browser_major_version (5)
:browser_minor_version (0)
```

These expressions are ANDed. If the version of Internet Explorer is 5 AND the minor version is 0 (i.e. version 5.0), then the result is true, otherwise it is false. If the version of Internet Explorer is, for example, 4.0, then the first expression is false and the second one is true, and the result of both of them is false.

Logical Sections

As mentioned earlier, subsequent expressions are automatically ANDed. However, sometimes it is necessary to perform a logical OR between expressions, instead of logical AND. This is done by using labels:

The **begin_or (orX)** label - this label starts a section containing several expressions. The end of this section is marked by the **end (orX)** label (**X** should be replaced with a number which differentiates between different sections OR sections). All of expressions inside this section are logically ORed, producing a single value for the section. For example:

```
:begin_or(or1)
:browser_major_version (5)
:browser_major_version (6)
:end(or1)
```

This section checks whether the version of Internet Explorer is 5 OR 6 - if it is then the result is true, otherwise it is false.

The **begin_and (andX)** label - this label is similar to the **begin_or (orX)** label, but the expressions inside are evaluated and logically "AND"-ed. The end of this section is marked by the **end (andX)** or the **end (orX)** label. As mentioned earlier, simple subsequent expressions are automatically "AND"-ed. The reason that this label exists is to allow nested "AND"-ed sections inside "OR"-ed sections. For example, if an administrator considers old browsers as secure since they do not have a lot of potentially unsafe components, and new browsers as secure, since they contain all the latest security patches, the administrator can configure these SCV rules:

```
:begin_or (or1)
:begin_and (and1)
:browser_major_version (5)
:browser_minor_version (0)
:browser_version_operand (">=")
:end (and1)
:begin_and (and2)
:browser_major_version (3)
:browser_minor_version (0)
:browser_version_operand ("<=")
:end (and2)
:end (or1)
```

In the example above, the first AND section checks whether the version of IE >= 5.0, the second "AND" section checks whether the version of IE is <=3.0 and they are "OR"-ed. The entire example is evaluated as true only if the version of IE is larger than (or equal to) 5.0 "OR" lower than (or equal to) 3.0.

Example:

```
:browser_major_version (7)
```

This expression is a Check Point SCV check. It checks whether the version of the Internet Explorer browser installed on the client is 7.x. If the major version is 7, this expression is **true**.

Grouping Expressions

If several expressions appear one after the other, they are checked on AND logic. Only if all expressions are true, then the value of all of them together is true.

Example:

```
:browser_major_version (7)
                    :browser_minor_version (0)
```

If the version of Internet Explorer is 7 AND the minor version is 0 (version 7.0), the result is **true**. If the version is 6.0, the first expression is **false** and the second one is **true**: result is **false**.

Influential Expressions

Some expressions can influence the way in which others are evaluated.

Example:

```
:browser_major_version (10)
                         :browser_minor_version (0)
                    :browser_version_operand (">=")
```

The third expression influences the way that the first and second are evaluated:

- If the version of Internet Explorer is greater than or equal to (">=") 10, the result is **true**.
- If the version is 9, the result is **false**
- If the version is 11, the result is **true**.

Expressions and Labels with Special Meanings

There are several expressions and labels which have special meaning:

- **begin_admin (admin)** - This label starts a section defining several actions which are performed only if the client is considered as one that does not meet SCV by previous expressions in the subset (i.e. if previous expressions in the subset have returned a value of false). The end of this section is marked by the **end (admin)** label.

- **send_log (alert / log)** - Use this label as part of the **begin_admin (admin) - end (admin)** section to define where the client should send logs when it does not meet the SCV check.

  If the value of this label is **alert**, the client sends a log to the Security Management Server and to the client's diagnostic tool.

  If the value of the label is **log**, the client sends a log **only** to the client's diagnostic tool.

- **mismatchmessage ("Message")** - This expression is used as part of the **begin_admin (admin) - end (admin)** section, and specifies that a popup message should be shown on the remote user's desktop, indicating the problem. The text in the inverted commas (**Message**) should be replaced by a meaningful text which should instruct the client about the possible sources of the problem and the action he should perform.

For example:

```
:browser_major_version (5)
:browser_minor_version (0)
:browser_version_operand (">=")
:begin_admin (admin)
:send_log (alert)
:mismatchmessage ("The version of your Internet Explorer browser
is old.
For security reasons, users with old browsers are not allowed to
access
the local area network of the organization. Please upgrade your
Internet
Explorer to version 5.0 or higher. If you require assistance in
upgrading
or additional information on the subject, please contact your
network
administrator.")
:end (admin)
```

In this example, if the user's IE browser's version is lower than 5.0, an alert is sent to the Security Management Server machine and a popup message is shown to the user with indication of the problem.

SCV Configuration on the Management Server

Step 1: Enable SCV Check on the Management Server

From SmartConsole Menu, click **Global Properties**.

From the navigation tree, click **Remote Access > Secure Configuration Verification (SCV)**.

Configure the settings:

- **Apply Secure Configurations on Simplified Mode** - Specifies if SCV is applied to all remote access rules in the simplified policy mode.
- **Upon Verification failure** - Specifies the action that is performed when the client fails one or more SCV checks. The options are to **Block** the client's connection or to **Accept** it and send a log about the event.
- **Basic configuration verification on client's machine** - Specifies whether the Remote Access Client performs SCV checks to determine if the policy is installed on all network interfaces cards on the client's desktop, and if only TCP/IP protocols are installed on these interfaces.
- **Configurations Violation Notification on client's machine** - Specifies if a log record is saved on the Security Management Server machine indicating that a remote user is not verified by SCV (this is a general indication, without a specification of a certain SCV check the user's desktop had failed).

From the left navigation tree, below **Access Control**, click **Access Control Policy**. In the Access Control Policy, make sure that all connections where you configure SCV match a rule that is explicitly defined for Remote Access VPN.

Example Access Rules:

No.	Source	Destination	VPN	Services & Applications	Action
1 (Management Rule - Not relevant for this example)	_	_	_	_	_
2	MP_ Role	Host_ 10.10.0.10	Any	icmp-proto http	Accept
3	MP_ Role	Host_ 10.10.0.10	RemoteAccess	ssh	Accept

For an HTTP connection from *MP_Role* to *Host_10.10.0.10*, SCV policy is **not** enforced. This is because the connection matches *Rule 2*. *Rule 2* is for any VPN, and is not explicitly for Remote Access VPN.

For an SSH connection from *MP_Role* to *Host_10.10.0.10*, SCV policy is enforced. This is because the connection matches *Rule 3*, which is explicitly for Remote Access VPN.

For more information, see the*R81.20 Security Management Administration Guide* > chapter *Creating an Access Control Policy*.

Click **OK** and publish the changes.

Step 2: Create the SCV Policy on the Management Server

Configure an SCV Policy in the text file `$FWDIR/conf/local.scv` on the Management Server. The `local.scv` file is a policy file, containing sets, subsets and expressions. In general, you can use the pre-defined checks (in the *SCVNames* section of the `local.scv` file) as templates and list the modified checks in the SCV Policy section, without writing new SCV subsets. You do not need to use expressions to create a basic SCV policy.

1. In the `$FWDIR/conf/local.scv` file, configure one or more of these SCV checks to create a basic SCV policy:

   "Groupmonitor"

   This checks that the logged on user belongs to the expected domain user groups.

Parameter	Description
`"builtin\ administrator" (false)`	A name of a user group. The user must belong to this group for the machine configuration to be verified.

   "OsMonitor"

   For Windows 10 and Windows 11, `osMonitor` checks for version build numbers to do the checks. To support this functionality on Windows 10, you must have both these parameters:

   - `os_build_number_10`
   - `os_build_operand_10`

   If the parameter "enforce_screen_saver_minutes_to_activate" does not appear, the screen saver configuration is not checked.

   OSMonitor does not support **begin_or** or **begin_and**.

Parameter	Description
`enforce_screen_ saver_minutes_to_ activate (3)`	Time in minutes for the screen saver to activate. If the screen saver does not activate within this time, then the client is not considered verified. In addition, the screen saver must be password protected.

Parameter	Description
screen_saver_ mismatchmessage ("Your screen saver settings do not meet policy requirements")	Mismatch message for the screen saver check. The screen saver will not be checked if the property "enforce_screen_saver_minutes_to_activate" does not appear, or if the time is set to zero.
service_pack_ version_operand_8 (">=")	Operator for checking the operating system's service pack on Windows 8.
major_os_version_ number_81 (6)	Specifies the major version required for Windows 8.1 operating systems to be verified.
minor_os_version_ number_81 (3)	Specifies the minor version required for Windows 8.1 operating systems to be verified.
os_version_operand_ 81 ("==")	Operator for checking the operating system's major and minor version on Windows 8.1.
service_pack_major_ version_number_81 (0)	Specifies the major service pack version required for Windows 8.1 operating systems to be verified.
service_pack_minor_ version_number_81 (0)	Specifies the minor service pack version required for Windows 8.1 operating systems to be verified.
service_pack_ version_operand_81 (">=")	Operator for checking the operating system's service pack on Windows 8.1.
major_os_version_ number_10 (10)	Specifies the major version required for Windows 10 operating systems to be verified.
minor_os_version_ number_10 (0)	Specifies the minor version required for Windows 10 operating systems to be verified.
os_version_operand_ 10 ("==")	Operator for checking the operating system's major and minor version on Windows 10.
os_build_number_10 (0)	Specifies the version build number required for Windows 10 operating systems to be verified.

Parameter	Description
`os_build_operand_10 (">=")`	Operator for checking the operating system's version build number on Windows 10.
`major_os_version_ number_11 (10)`	Specifies the major version required for Windows 11 operating systems to be verified.
`minor_os_version_ number_11 (0)`	Specifies the minor version required for Windows 11 operating systems to be verified.
`os_version_operand_ 11 ("==")`	Operator for checking the operating system's major and minor version on Windows 11.
`os_build_number_11 (0)`	Specifies the version build number required for Windows 11 operating systems to be verified.
`os_build_operand_11 (">=")`	Operator for checking the operating system's version build number on Windows 11.
`os_version_ mismatches ("Please upgrade your operating system")`	Message to be displayed in case of a non-verified configuration for the operating system's version/service pack. The operating system's version and the service pack will not be checked if none of the parameters appear in the scv file.

"ProcessMonitor"

This check is for process activity. It supports AND and OR sections.

It is based on the process name, with an additional hash check option for running processes.

ProcessName.exe (`true`| `false`)

ProcessName.exe (`true`;<SHA1 hash value>)

For example: `calc.exe (true;9018A7D6CDBE859A430E8794E73381F77C840BE0)`

If the value is true, the client is compliant if this process is running.

If the value is false, the client is compliant if the process is not running.

Note - Checking the SHA1 hash value can impact performance.

"RegMonitor"

These checks are for the system registry. RegMonitor supports AND and OR sections.

Parameters

`PredefinedKeys` (HIVE)

Specify the registry hive from one of these choices:

- `HKEY_CURRENT_USER`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`

To configure a check for `HKEY_CLASSES_ROOT`, use `HKEY_LOCAL_MACHINE\Software\Classes and HKEY_CURRENT_USER\Software\Classes`.

Note - If the values of these parameters do not include the name of the registry hive, the `HKEY_LOCAL_MACHINE` hive is used by default. If you want to use another hive, you must explicitly use it in the value of the parameter.

Parameter	Description
`value (registry_value_path)`	The path of a registry `DWORD` will be checked. The value should be an operator followed by a number, e.g. `"Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer>=414"`
`string (registry_string_path)`	The path of a registry string will be checked. The string's value is compared to the given value, in the way that DWORDs are compared.
`keynexist (registry_key_path)`	The path of a registry key to be checked for exclusion. For the machine to be verified, the key should not exist.
`keyexist (reistry_key_path)`	The path of a registry key to be checked for inclusion. For the machine to be verified, the key must exist.

2. In SmartConsole, install the policy.

Step 3 (Optional): Create SCV policy per Security Gateway

Starting R81.20 Jumbo Hotfix Accumulator Take 90, you can create a customized SCV policy per Security Gateway.

Procedure

1. Copy the file `$FWDIR/conf/local.scv` on the Management Server to a new file on the same path.
2. Rename the file to `$FWDIR/conf/local.scv_<Gateway_Name>`.

   Note - `<Gateway_Name>` is the exact Security Gateway object name in SmartConsole.
3. Edit the `$FWDIR/conf/local.scv_<Gateway_Name>` file and make the required changes.
4. Save the `$FWDIR/conf/local.scv_<Gateway_Name>` file.

During the policy installation on a Security Gateway, the Management Server looks for a `local.scv` file with the Security Gateway's name.

If the file exists, the Management Server uses it, and if it does not, the Management uses the general `local.scv` file.

SCV Configuration on the Endpoint Computer

1. **Optional -** If you intend to use an OPSEC SCV third-party application, install the application on the client and enable the application's integration with SCV (see the application's documentation for information on how to do this).
2. Start the client and connect to the Security Gateway to receive the SCV

Example of WindowsSecurityMonitor configuration

```
: SCVEpsNames (
                : (WindowsSecurityMonitor
                :type (plugin)
                :parameters (
                :VirusProtectionRequired (true)
                :VirusProtectionRequiredMismatchMessage ("Please see
that your AntiVirus is updated and active")
```

```
                :VirusProtectionInstalledPrograms ("Trend Micro
  OfficeScan Antivirus;Kaspersky Anti-Virus")
                :VirusProtectionInstalledProgramsMismatchMessage
  ("Please see that your AntiVirus is Trend Micro or Kaspersky")
                :WindowsUpdateRequired (true)
                :WindowsUpdateRequiredMismatchMessage ("Please turn on
  Windows automatic Updates")
                :SpywareProtectionRequired (true)
                :SpywareProtectionRequiredMismatchMessage
  ("AntiMalware is not updated or active")
                :SpywareProtectionInstalledPrograms ("none")
                :SpywareProtectionInstalledProgramsMismatchMessage
  ("")
                :NetworkFirewallRequired (true)
                :NetworkFirewallRequiredMismatchMessage ("Please check
  the your network firewall is turned on")
                :NetworkFirewallInstalledPrograms ("Kaspersky Anti-
  Virus")
                :NetworkFirewallInstalledProgramsMismatchMessage
  ("Please check that Kaspersky Anti-Virus firewall is installed on your
  machine")
                )
                )
                )
```

The "SCVNames" section

In this section the administrator specifies the names and different checks for the SCV products. Here is a general definition of an SCV check subset of SCVNames:

```
: (SCVCheckName1
    :type (plugin)
    :parameters (
        :Expression1 (value)
        :Expression2 (value)
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Failure Message")
        :end (admin)
    )
)
```

The test section begins with the name of the SCV check (SCVCheckName1). SCVCheckName1 defines the name of the set of tests. It is defined in the SCV application and should be provided by the SCV manufacturer. The **type (plugin)** expression specifies that the test is performed by an SCV DLL plugin. The **parameters** subset is where the SCV rules and actions are defined. The **type (plugin)** expression and the **parameters** subset should always be specified when defining a subset of SCV checks (such as SCVCheckName1).

The "SCVPolicy" section

This section defines the names of the SCV checks that should be enforced (the names are part of the SCV check names specified in SCVNames). This section's general structure is:

```
:SCVPolicy (
:(SCVCheckName1)
:(SCVCheckName2)
)
```

SCVGlobalParams

This section includes global parameters for SCV.

```
:SCVGlobalParams (
    :disconnect_when_not_verified (false)
    :block_connections_on_unverified (false)
    :not_verified_script ("myscript.bat")
    :not_verified_script_run_show (true)
    :not_verified_script_run_admin (false)
    :not_verified_script_run_always (false)
    :allow_non_scv_clients (false)
)
```

Secure Configuration Verification - Advanced

Advanced SCV Policy

Additional SCV Checks

The default SCV checks (plug-ins) are part of the Endpoint Security VPN and Check Point Mobile for Windows installation:

- **OS Monitor** - Verifies Operating System version, Service Pack, and Screen Saver configuration (activation time, password protection, *etc.*).
- **HotFix Monitor** - Verifies that operating system security patches are installed, or not installed.
- **Group Monitor** - Verifies that the user logged into the operating system and is a member of specified Domain User Groups.
- **Process Monitor** - Verifies that a process is running, or not running, on the endpoint computer (for example, that a file sharing application is not running, or that Anti-Virus is running).
- **Browser Monitor** - Verifies Internet Explorer version and configuration settings, such as Java and ActiveX options.
- **Registry Monitor** - Verifies System Registry keys, values, and their contents.
- **Anti-Virus Monitor** - Verifies that an Anti-Virus is running and checks its version. Supported: Norton, Trend Office Scan, and McAfee.
- **SCVMonitor** - Verifies the version of the SCV product, specifically the versions of the SCV DLLs installed on the client's machine.
- **HWMonitor** - Verifies CPU type, family, and model.
- **ScriptRun** - Runs a specified executable on the client machine and checks the return code of the executable. For example, a script can check if a certain file is present on the client machine. It can perform additional configuration checks that you choose.
- **Windows Security Monitor** - Verifies that components monitored by Window Security Center are installed and enforced (for example, check if there is Anti-Virus installed and running). You can define which components you want to check.

Anti-Virus monitor

This check is for the type and signature of Anti-Virus. It does not support **begin_or** or **begin_and**.

Parameter	Description
`Type ("av_type")`	Type of Anti-Virus. For example, "Norton", "VirusScan", "McAfee", "OfficeScan", or "ZoneLabs".
`Signature (x)`	Required Virus definition file signature. The signature's format depends on the Anti-Virus type. ■ Norton Antivirus example: ">=20031020" (format for Norton's AV signature is "yyyymmdd") ■ TrendMicro Officescan example: "<650" ■ McAfee VirusScan example: (">404291") for a signature greater than 4.0.4291 ■ Zone Labs format: (">X.Y.Z") where X = Major Version, Y = Minor Version, and Z = Build Number of the .dat signature file

"BrowserMonitor"

This check is only for Internet Explorer version, or only the browser settings for a certain zone. If none of these parameters appear, **BrowserMonitor** will not check the security settings of the restricted zones:

- `restricted_download_signed_activex`
- `restricted_run_activex`
- `restricted_download_files`
- `restricted_java_permissions`

If the parameter "browser_major_version" does not appear or is equal to zero, the IE version number is not checked.

BrowserMonitor does not support the **begin_or** or **begin_and**, and does not support the **admin** parameters.

Parameter	Description
`browser_major_version (#)`	Major version number of Internet Explorer. If this field does not exist in the local.scv file, or if this value is 0, the IE version will not be checked as part of the BrowserMonitor check.
`browser_minor_version (#)`	Internet Explorer minor version number.

Parameter	Description
`browser_version_operand (">=")`	The operator used for checking the Internet Explorer's version number.
`browser_version_ mismatchmessage ("Please upgrade your Internet Browser.")`	Message to be displayed for a non-verified configuration of Internet Explorer.
`intranet_download_signed_ activex (enable)`	The maximum permission level that IE should have for downloading signed ActiveX controls from within the local Intranet.
`intranet_run_activex (enable)`	The maximum permission level that IE should have for running signed ActiveX controls from within the local Intranet.
`intranet_download_files (enable)`	The maximum permission level that IE should have for downloading files from within the local Intranet.
`intranet_java_permissions (low)`	The maximum security level that IE Explorer should have for running java applets from within the local Intranet.
`trusted_download_signed_ activex (enable)`	The maximum permission level that IE should have for downloading signed ActiveX controls from trusted zones.
`trusted_run_activex (enable)`	The maximum permission level that IE should have for running signed ActiveX controls from trusted zones.
`trusted_download_files (enable)`	The maximum permission level that IE should have for downloading files from trusted zones.
`trusted_java_permissions (medium)`	The maximum security level that IE should have for running java applets from trusted zones.
`internet_download_signed_ activex (disable)`	The maximum permission level that IE should have for downloading signed ActiveX controls from the Internet.
`Internet_run_activex (disable)`	The maximum permission level that IE should have for running signed ActiveX controls from the Internet.

Parameter	Description
`internet_download_files (disable)`	The maximum permission level that IE should have for downloading files from the Internet.
`internet_java_permissions (disable)`	The maximum security level that IE should have for running java applets from the Internet.
`restricted_download_signed_ activex (disable)`	The maximum permission level that IE should have for downloading signed ActiveX controls from restricted zones.
`restricted_run_activex (disable)`	The maximum permission level that IE should have for running signed ActiveX controls from restricted zones.
`restricted_download_files (disable)`	The maximum permission level that IE should have for downloading files from restricted zones.
`restricted_java_permissions (disable)`	The maximum security level that IE should have for running java applets from restricted zones.
`send_log (type)`	Whether to send a log to Security Management server for specifying that the client is not verified: **log** or **alert**. Does not support **begin_admin**.
`internet_options_mismach_ message ("Your Internet browser settings do not meet policy requirements")`	Mismatch message for the Internet Explorer settings.

"Groupmonitor"

This checks that the logged on user belongs to the expected domain user groups.

Parameter	Description
`"builtin\ administrator" (false)`	A name of a user group. The user must belong to this group for the machine configuration to be verified.

"HotFixMonitor"

This check is for Check PointHotfixes. Some of these parameters may not appear at all, or may appear more than once in the **local.scv** file. These parameters can be in OR and AND sections.

Parameter	Description
`HotFix_Number (true)`	A number of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: "823980(true)" verifies that Microsoft's RPC patch is installed on the operating system.
`HotFix_Name (true)`	The full name of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: "KB823980 (true)" verifies that Microsoft's RPC patch is installed on the operating system.

"HWMonitor"

This check is for CPU details. It does not support the **begin_or** or **begin_and**.

Parameter	Description
`cputype ("GenuineIntel")`	The CPU type as described in the vendor ID string. The string has to be exactly 12 characters long. For example: "GenuineIntel", or "AuthenticAMD", or "aaa bbb ccc " where spaces count as a character.
`cpufamily` (6)	The CPU family.
`cpumodel` (9)	The CPU model.

"SCVMonitor"

This check is for the version of SCV. It does not support **begin_and** or **begin_or**.

Parameter	Description
`scv_version (">=541000076")`	SCV build-version of the SCV DLLs. This is not the same as the build number of Endpoint Security VPN. The string is an operator followed by the DLL's version number in the format "vvshhhbbb". For example, if you want the DLL version to be at least 54.1.0.220, the syntax should be: `scv_version (">=541000220")`

"ScriptRun"

This check lets you run a specified executable on the client machine and checks the return code of the executable. For example, a script can check if a certain file is present on the client machine. It can perform additional configuration checks that you choose. If you do not enter a real script name, no script runs.

Important - If you enter invalid values for any of the attributes, for example letters instead of numbers, the computer that runs the script is considered not compliant.

Parameter	Description
`exe ("c:\Users\nonadmin\script.exe')`	The name and full path of the executable script on users' machines. The extension can be any executable, for example, .pl, .bat.
`script_run_cycle (#)`	After how many cycles to run the script. A cycle is an interval defined in the gobal `scv_checks_interval`. It is 20 second by default and by default the script runs after every cycle (1).
`run_as_admin (no)`	Determines if the script runs with Administrator or User permissions. The default is "no". If the value is "yes" the script runs with Administrator permissions.
`run_timeout (#)`	Time in seconds to wait for the executable to finish running. If it does not finish in the set time, the machine is considered not compliant. The default value is 0, no timeout.

"user_policy_scv"

This check is for user behavior and user notifications.

Parameter	Description
`logged_on_to_ policy_server` (`true` or `false`)	Specifies whether the user has to be logged on to a Policy Server to meet SCV.

Parameter	Description
`policy_refresh_rate` ("**[INTEGER]**")	Time, in hours, for which the desktop policy remains valid. After 168 hours the desktop policy is not considered valid, and the user does not meet SCV any longer. If this parameter is not specified, the policy is not checked for freshness.
`mismatchmessage` ("**[YOUR MESSAGE]**")	The message shown to the user of the endpoint computer when the *user_policy_scv* check fails.
`dont_enforce_while_connecting`	If this parameter is present, the user meets SCV while connecting to the Security Gateway. The user meets SCV only for the duration of the connect process.

"SCVGlobalParams"

These parameters specify what the Remote Access client does when the endpoint computer is not compliant with the SCV policy.

Parameter	Description
`ect_when_not_verified (true/false)`	If "`true`", the Remote Access client stops the connection to the Security Gateway when the endpoint computer fails the SCV check.
`block_connections_on_unverified` (`true/false`)	If "true", the Remote Access client blocks the connection to the Security Gateway when the endpoint computer

Parameters:

Do not enclose boolean parameters (`true` or `false`) n quotation marks.

- `block_connections_on_unverified` (true/false)
- `ip_forwarding_mismatchmessage` ("Message string placed here")

  The value is a string displayed when ip forwarding is enabled. For example: ip_forwarding_mismatchmessage ("Please....etc")

  This is relevant only if IP Forwarding is part of the SCV checks, that is, if the parameter is defined as "True".

- `not_verified_script` ("script_name.bat")

  The name of executable that will be run when the Desktop does not meet SCV. The next three parameters provide more options related to the running of the executable.

- `not_verified_script_run_show` (true/false)

If "`true`", the executable's progress will be displayed in an onscreen window.

- `not_verified_script_run_admin` (true/false)

  If "`true`", the executable will run with administrator privileges.

- `not_verified_script_run_always` (true/false)

  If "`true`", the executable will run every time the Desktop does not meet SCV. If "false", it will run once per the Remote Access client session.

- `:allow_non_scv_clients` (true/false)

  If "`true`", the client will send a verified state to the enforcing Security Gateway even if the OS does not support SCV.

SCV Checks for macOS Endpoint Computers

Starting from the standalone Remote Access VPN Client version E88.40, you can configure SCV checks for macOS endpoint computers in the *local.scv* configuration file on the Management Server. The file syntax and functionality of an SCV check is the same for Windows and macOS. These sections of the file are relevant for macOS endpoint computer:

- `:SCVPolicyMac`
- `:SCVNamesMac`
- `:SCVGlobalParams` (relevant for Windows and macOS)

To apply the SCV check on the macOS endpoint computer, you must change the value of a registry parameter.

Step 1: Management Server Configuration

1. Connect to the command line on the Management Server.
2. Log in to the Expert mode.
3. On a Multi-Domain Server, switch to the context of the Domain Management Server:

   ```
   [Expert@HostName]# mdsenv <Domain_Name>
   ```

4. Back up the *$FWDIR/conf/local.scv* file.

   ```
   [Expert@HostName]# cp $FWDIR/conf/local.scv
   $FWDIR/conf/local.scv_ORIGINAL
   ```

5. Edit and configure the *$FWDIR/conf/local.scv* file:

   ```
   [Expert@HostName]# vi $FWDIR/conf/local.scv
   ```

6. Add the `:SCVNamesMac` and `:SCVPolicyMac` sections to the file. In this example, an SCV policy checks if some applications are running:

```
                                                                :SCVNamesMac (
                                                                : (OsMonitor
                                                                :type (plugin)
                                                                :parameters (
                                                                :major_os_vers
                                                                :minor_os_vers
                                                                :os_version_op
                                                                :begin_admin (
                                                                :send_log (ale
                                                                :mismatchmessa
                                                                :end (admin)
                                                                )
                                                                )
                                                                : (ProcessMoni
                                                                :type (plugin)
                                                                :parameters (
                                                                :begin_or (or1
                                                                :begin_and (an
                                                                :ping (true)
                                                                :Weather (true
                                                                :end (and1)
                                                                :begin_and (an
                                                                :Calculator (t
                                                                :Calendar (tru
                                                                :end (and2)
                                                                :end (or1)
                                                                :begin_admin (
                                                                :send_log (ale
                                                                :mismatchmessa
processes are running: ping and Weather or calculator and
calendar")
                                                                :end (admin)
                                                                )
                                                                )
                                                                : (groupmonito
                                                                :type (plugin)
                                                                :parameters (
                                                                :begin_and (or
                                                                :"test_group"
                                                                :"everyone" (f
                                                                :end (or1)
                                                                :begin_admin (
                                                                :send_log (ale
```

```
                                                                    :mismatchmessa
non-authorized user. Make sure you are logged on as an
authorized user.")
                                                                    :securely_conf
                                                                    :end (admin)
                                                                    )
                                                                    )
                                                                    : (AntiVirusMo
                                                                    :type (plugin)
                                                                    :parameters (
                                                                    :type ("CrowdS
                                                                    :signature ("2
                                                                    :begin_admin (
                                                                    :send_log (ale
                                                                    :mismatchmessa
the LiveUpdate option).")
                                                                    :end (admin)
                                                                    )
                                                                    )
                                                                    )
                                                                    :SCVPolicyMac
                                                                    : (ProcessMoni
                                                          )
```

7. Install the policy.

Step 2: macOS Endpoint Computer Configuration

This procedure requires superuser privileges on the macOS endpoint computer.

1. Open the Terminal on the macOS endpoint computer.
2. Stop the GUI process:

   ```
   sudo launchctl bootout gui/$(id -u)
   /Library/LaunchAgents/com.checkpoint.eps.gui.plist
   ```

3. Stop the Check Point VPN service:

   ```
   sudo launchctl bootout system
   /Library/LaunchDaemons/com.checkpoint.epc.service.plist
   ```

4. In a text editor, open the Remote Access VPN client registry file. This is the default file path:

   ```
   /Library/Application Support/Checkpoint/Endpoint
   Connect/registry/HKLM_registry.data
   ```

5. Change the value of the "`disable SCV`" parameter:
   - To **enable** the feature, set the value of the parameter to "0".
   - To **disable** the feature, set the value of the parameter to "1".
6. Start the GUI process:

```
sudo launchctl bootstrap gui/$(id -u)
/Library/LaunchAgents/com.checkpoint.eps.gui.plist
```

7. Start the Check Point VPN service:

```
sudo launchctl bootstrap system
/Library/LaunchDaemons/com.checkpoint.epc.service.plist
```

Third Party SCV Checks

SCV checks can be written by third party vendors using Check Point's OPSEC SCV SDK.

Allowing Clients without SCV

The **Allow non SCV clients** option lets you allow Security Gateway connections from clients that do not have SCV, such as SecuRemote. The setting does not take effect if the endpoint client does have SCV. Therefore, if this option is configured, the Security Gateway still requires SCV compliance from Check Point Mobile for Windows or Endpoint Security VPN before they can access resources behind the Security Gateway. By default, this option is disabled.

To enable Allow non SCV Clients in the global parameters:

1. On the Security Management Server, edit the `$FWDIR/conf/local.scv` file.
2. In the **SCVGlobalParams** section, set the value of the **allow_non_scv_clients** parameter to **true.**
3. Install the Desktop Policy.
4. The change occurs when a client connects.

Disconnect When Not Verified

This feature lets you disconnect the client if it becomes non-compliant while connected to the VPN.

1. On the Security Management Server, edit the `$FWDIR/conf/local.scv` file.
2. In the **SCVGlobalParams** section, set the value of the **disconnect_when_not_verified** parameter:
   - **true** - A connected, non-compliant client is automatically disconnected from the VPN. A notification is shown to the user.
   - **false** - A connected, non-compliant client stays connected to the VPN. This is default.

Not Verified Script

This feature lets you configure script-running if a client becomes non-compliant.

If you can run scripts on non-compliant clients, you can use them to send remediations.

For example, you can run a script that install an Anti-Virus, or a script that opens an HTML page with a link to the remediation.

1. Edit the `$FWDIR/conf/local.scv` file on the Security Management Server.
2. In the **SCVGlobalParams** section, find the **not_verified_script**.
3. In the value, put the name of the script.
   - You must supply the script to the client computers.
   - If necessary, you must make sure it is in the search path.
4. Set the value of the **not_verified_script_run_show** parameter:
   - **true** - The user will see the script running.
   - **false** - The script run will be hidden (default).
5. Set the value of the **not_verified_script_run_admin** parameter:
   - **true** - The script will run under the Remote Access Clients Service account with administrator permissions, even if the user does not have these permissions.
   - **false** - The script will run under the local user account permissions (default). If administrator permissions are necessary, the script will fail.
6. Set the value of the **not_verified_script_run_always** parameter:
   - **true** - The script runs every time the client becomes non-compliant.
   - **false** - The script runs the first time that the client becomes non-compliant. (default)

SCV Intervals

This feature lets you change the default interval after which the SCV checks run. By default, the interval is 20 seconds, so checks run at 20 second intervals.

To change the interval in the global parameters:

1. On the Security Management Server, edit the `$FWDIR/conf/local.scv` file.
2. In the **SCVGlobalParams** section, set the value of the **scv_checks_interval** parameter to a desired number of seconds.

   If you set the value to 0 or enter an invalid value, such as a letter, the interval will be the default 20 seconds.
3. Install the Desktop Policy.

   The change takes effect when a client connects.

Configuring SCV Exceptions

Configure exceptions for hosts that can be accessed using selected services even if the client is not compliant.

You can allow a connection even if the client is non-compliant. For example, the client has to download the latest update or Anti-Virus version required by the SCV check.

To make exceptions for non-compliant remote clients:

1. Select the **Apply Secure Configuration Verification on Simplified mode Firewall Policies** option.
2. Click the **Exceptions** button.

   The **Secure Configuration Verification Exceptions** window opens.
3. Click **Add**.
4. Double-click **None**.
5. Add the Hosts from the encryption domain you want to exclude from the SCV check and the specific services to communicate with them.
6. Click **OK**.
7. Install policy.

The Skip firewall enforcement option lets you allow gateway connections from clients that do not have a firewall enforced, such as Check Point Mobile for Windows. By default, this option is disabled so that firewall enforcement is required as part of the SCV check.

Notes -
This parameter is not related to the `NetworkFirewallRequired` parameter in the Window Security Monitor check.
Endpoint Security VPN ignores the parameter skip_firewall_enforcement_check. It always checks for firewall enforcement.

To enable Skip firewall enforcement in the global parameters:

1. On the Security Management Server, edit the `$FWDIR/conf/local.scv` file.
2. In the **SCVGlobalParams** section, set the value of the **skip_firewall_enforcement_check** parameter to **true.**
3. Install the Desktop Policy.

   The change takes effect when a client connects.

Finding Exact Product Names

You can include lists of products in the WindowsSecurityMonitor check for these parameters:

- `NetworkFirewallInstalledPrograms`
- `VirusProtectionInstalledPrograms`
- `SpywareProtectionInstalledPrograms`

You must write the names of the products the same as they are shown in the Windows Management Instrumentation Tester tool. The product only shows if it is installed on that computer.

To find names in the Windows Management Instrumentation Tester tool:

1. Open the command prompt as an administrator and enter **wbemtest.**

   The Windows Management Instrumentation Tester opens.
2. Click **Connect.**
3. In the **Namespace** field, enter **root\SecurityCenter** and click **Connect**.

   In Windows 7 some of the products are registered in **root\SecurityCenter2**.
4. Click **Enum Instances**.
5. In the **Class Info** Window, enter the class of product without spaces:
   - AntiVirusProduct
   - FirewallProduct
6. Double click an instance that shows in the **Query Results**.

7. In the **Object editor** window, scroll down to the **displayName** property. Copy the name listed and use that in the parameters of the check.

Troubleshooting SCV

"file is corrupt"

Symptom	Client shows an error message: `Compliance Policy file is corrupt. Please contact your system administrator.`
Scenario	An SCV check defined in the **SCVPolicy** section is not defined in the **local.scv** policy, **SCVNames** section.
Solution	Make sure that the SCVNames section includes all the checks that are to be run on clients.

"unsupported format"

Symptom	Client shows an error message: `Compliance Policy is in an supported format`
Scenario	Can be one of these issues: ■ There is no **SCVObject** section in the **local.scv** policy file. ■ An SCV plug-in configured in the **local.scv** policy file does not exist on the client computer, or it has a functionality issue. ■ The SCV Check type as defined in the local.scv policy is not a plug-in. ■ The **local.scv** policy context has an incorrect format. ■ The **local.scv** file was edited on an operating system that is different than the Security GatewaySecurity Gateway operating system and the file was saved in an encoding that the Security Gateway cannot read.
Solution	See the SCV section in this Administration Guide and follow the instructions to edit and maintain the **local.scv** file.

"policy is not updated"

Symptom	Client shows an error message: `Compliance policy is corrupt. Please connect again to update the policy.`
Scenario	The policy enforced on the client computer is not updated with the latest security policy defined on the Security Gateway.

Solution	Connect the client computer again to the Security Gateway. The client pulls the latest security policy when it connects to the Security Gateway.

Machine Certificate

Authentication with a machine certificate is supported for Endpoint Security clients connecting to a Security Gateway.

Machine certificate authentication supports these modes:

- **User and machine authentication** - Authenticate with a machine certificate and a user authentication method.
- **Machine-only authentication** - Authenticate with a machine certificate only. This mode is available before and after the user logs in to Windows.

Note - Machine certificate authentication works with the Endpoint Client only. For more details on how to configure this feature on the client side, see the "Machine Authentication" section in these Administration Guides:

- *Remote Access VPN Clients for Windows Administration Guide*
- *Endpoint Security VPN for macOS Administration Guide*

Limitations:

- The machine must be defined on a **Microsoft** AD server.
- The Subject field of a machine certificate must not be empty.

  The hostname must be the first value.

  For example:

  CN = DESKTOP-12345, OU= Computers, DC = example, DC = com
- Machine-only authenticated tunnels require the Security Gateway authentication method to be “Defined on user record (Legacy authentication)” or a certificate based realm.
- Check Point Desktop Policy with Machine Groups is not supported.
- The Check Point Management Server does not provide machine certificate enrollment or distribution functionality.
- You must use Access Roles for the machine entity. Objects such as machine@location are not supported.

Feature Configuration Steps

1. **Adding the root CA on the LDAP Server to the Trusted CA in Management**

   Refer to sk149253.

This CA is necessary for the machine authentication procedure.

2. **Creating LDAP Account Unit**

   Refer to sk31841.

3. **Setting up the Authentication enforcement**

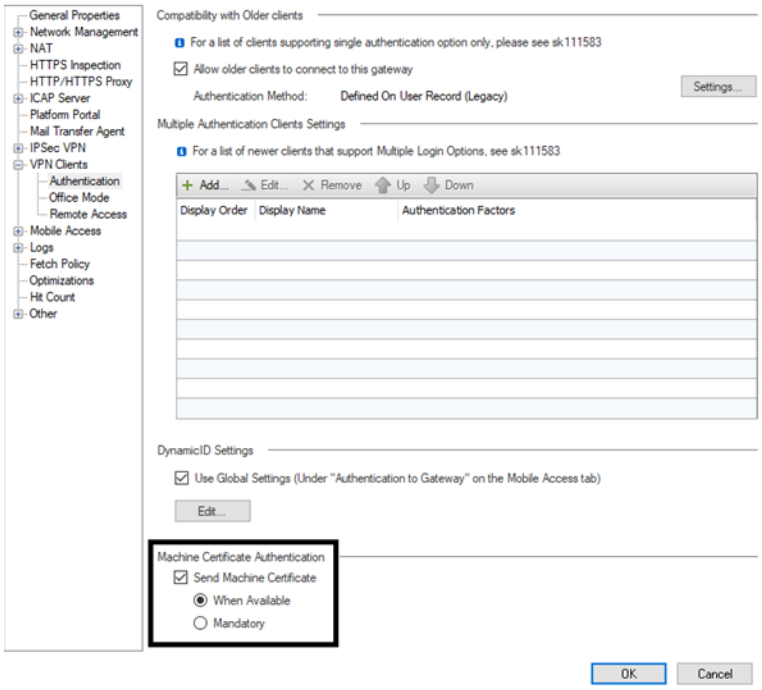
   Feature status definitions

   - **Disabled** - The feature is off. Machine certificate authentication does not occur.
   - **When available** - Clients are allowed to connect with or without a machine certificate. If the Gateway receives a machine certificate, it tries to authenticate the machine.

     Note - If the machine certificate is not valid, the connection fails.
   - **Mandatory** - Clients can not connect without a machine certificate.

   Set the Status of the Machine Certificate Authentication

   a. Enable the Identity Awareness Software Blade and walk through the Wizard.
   b. Apply the basic **Remote Access** configuration (*community*, *office mode*, and *visitor mode*).
   c. Go to **VPN Clients > Authentication**.
   d. At the bottom of the screen, check **Send Machine Certificate**.
   e. Choose **When Available** or **Mandatory**.
   f. Click **OK**.



4. **Policy configuration for Users and Machines**

Install the Access Control Policy

a. Connect with SmartConsole to the Management Server.

b. Go to the **Objects Menu**.

c. Left-click on **New**.

d. Select **More > User > Access Role**.

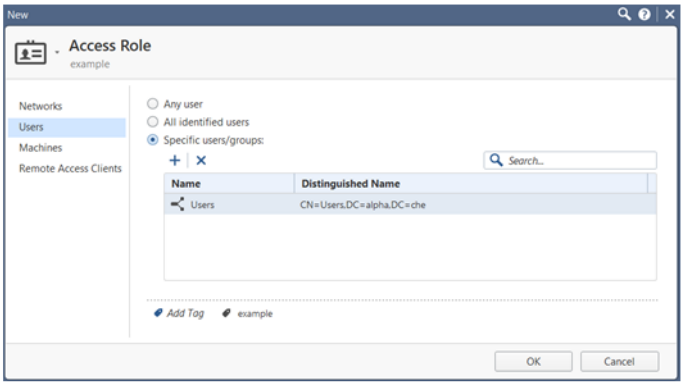
The New Access Role window will open.

e. From the left tree, click the **Users** pane.

f. On the **Users** pane, select one of these:

- **Any user**
- **All identified users** - This includes any user identified by a supported authentication method *(internal users*, *Active Directory users*, or *LDAP users*).

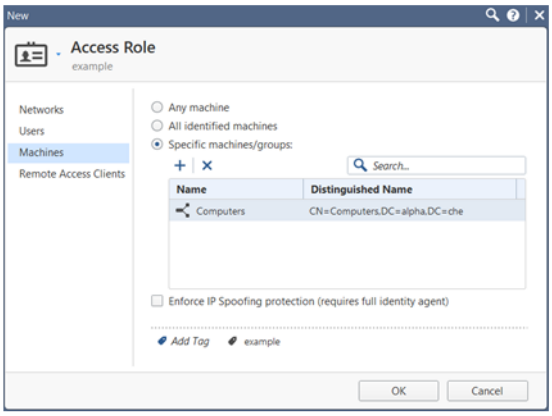
- **Specific users/groups** - For each user or user group, click to select the user or the group from the list.



g. From the left tree, click the **Machines** pane.

h. On the **Machines** pane, select one of these:

- **Any machine**
- **All identified machines** - Includes machines identified by a supported authentication method (*Active Directory*).
- **Specific machines** - For each machine, click to select the machine from the list.



i. Click **OK**.

j. From the left navigation panel, click **Security Polices**.

k. Choose your network policy tab.

l. In **Access Control**, select **Policy**.

m. Right-click in the **Source** column > **Add new items...** .

n. Left-click on the **Access Role**.

o. Right-click in the **VPN** column > **Specific VPN communities...**.

p. Add **RemoteAccess** community.

q. Install the Access Control policy on the Security Gateway / Cluster.

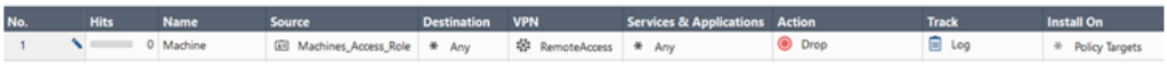
5. **Policy Examples**

Example 1

The **Source** field contains the object `Machines_Access_Role`.

In the access role, choose **Specific machines/groups** on the **Machines** pane and add **LDAP machine/machines group** (leave **Any user** and **Any Network** on corresponding panes).

If a client connects with the machine authentication (**Machine only** or **Machine and User**), this rule matches if the Machine matches the LDAP Machine group.

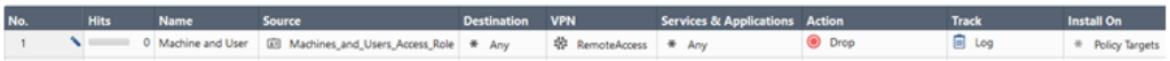


Example 2

The **Source** field contains the object `Machines_and_Users_Access_Role`.

In the access role, choose **Specific users/groups** on the **Users** pane and add **LDAP user/users group**. Leave **Any machine** and **Any Network** in the corresponding panes.

If a client connects with user authentication (**User only** or **Machine and User**), this rule matches if the User matches the LDAP User group.

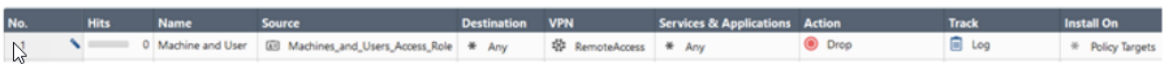


Example 3

The **Source** field contains the object `Machines_and_Users_Access_Role`.

In the access role you should choose **Specific machines/groups** on the **Machines** pane and **Specific users/groups** in the **Users** pane. Leave **Any Network** in the corresponding pane.

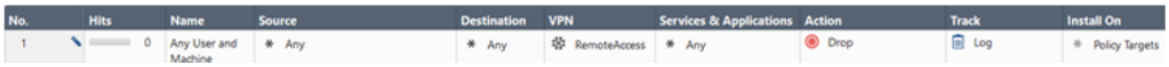
A connection with **Machine** and **User authentication** can match this rule if the Machine and User both match the appropriate LDAP groups.



Example 4

Policy **Source** field contains the object `Any`.

If a client connects with **User** (**User only** or **Machine and User**), this rule matches.



6. **Optional - UPN with Machine Certificate**

   To use the **UserPrincipalName** as the User Login Attribute instead of **DN**, create a **machine_certificate** realm.

   - This makes it possible to configure different realms for machines and users.
   - Users can log in with their **UPN** without an impact on the machine authentication.
   - The user realm must still have one authentication factor.
   - After you create the realm, you can change the LDAP lookup type of the user-selected realm to **UPN** instead of **DN**.

   To create the machine_certificate realm:

   a. Back up the Security Management Server / applicable Domain Management Server.

      Refer to:

      - sk108902 - Best Practices - Backup on Gaia OS.
      - sk91400 - System Backup and Restore feature in Gaia.
      - sk98153 - How to take a snapshot of Endpoint Security Management Server database.

   b. Close **all** SmartConsole windows.

      Note - To make sure there are no active sessions, run the "`cpstat mg`" command in the Expert mode on the Security Management Server / in the context of *each*Domain Management Server.

   c. Connect with *Database Tool (GuiDBEdit Tool)* to the Security Management Server / applicable Domain Management Server.

   d. In the top left pane, go to **Table** > **Network Objects** > **network_objects**.

   e. In the top right pane, select the **Machine_Cert_GW** object.

   f. Press the **CTRL+F** keys (or go to the **Search** menu > click **Find**) > paste **realms_for_blades** > click **Find Next**.

g. In the lower pane, right-click on the **realms_for_blades** object > select **New...**

   The **Add/Edit Owned Object** window opens.

h. In the **Add/Edit Owned Object** window:

   i. In the **Name** field, enter **machine_certificate**.

   ii. In the **Value** field, select **realm_blade_entry**.

   iii. Click **OK**.

   The **Add/Edit Owned Object** window closes.

i. Press the **CTRL+F** keys (or go to the **Search** menu > click **Find**) > paste **auth_schemes** > click **Find Next**.

j. In the lower pane, right-click on the **auth_schemes** object > select **Add...**

   The **Element Add/Edit** window opens.

k. In the **Element Add/Edit** window:

   i. In the **Index** field, enter **0**.

   ii. Leave the **Name** field empty.

   iii. In the **Object** field, select **realm_auth_scheme**.

   iv. Click **OK**.

   The **Element Add/Edit** window closes.

l. Press the **CTRL+F** keys (or go to the **Search** menu > click **Find**) > paste **display_string** > click **Find Next**.

m. In the lower pane, right-click on the **display_string** object > select **Edit...**

   The **Edit** window opens.

n. In the **Edit** window:

   i. In the **Value** field, enter **machine_certificate**.

   ii. Click **OK**.

   The Edit window closes.

o. Save the changes: go to the **File** menu > click **Save All**.

p. Close the Database Tool (GuiDBEdit Tool).

q. Connect with SmartConsole to the Security Management Server / applicable Domain Management Server.

r. Install the Access Control Policy on the applicable Security Gateway / Cluster / VSXVirtual System object.

L2TP Clients

Introduction to Layer Two Tunneling Protocol (L2TP) Clients

Some organizations prefer to use L2TP clients for remote access to internal networks, rather than the more feature-rich and secure Check Point clients. There are L2TP clients built into many operating systems.

Check Point Security Gateways can create VPNs with L2TP IPsec clients. This explanation focuses on the Microsoft IPsec / L2TP client.

You can access a private network through the Internet by using a virtual private network (VPN) connection with the Layer Two Tunneling Protocol (L2TP). L2TP is an industry-standard Internet tunneling protocol.

Creating a Remote Access environment for users with Microsoft IPsec / L2TP clients is based on the same principles as those used for setting up Check Point Remote Access Clients. Make sure that you understand how to configure Remote Access VPN before you begin to configure Remote Access for Microsoft IPsec / L2TP clients.

Establishing a VPN between a IPsec / L2TP Client and a Security Gateway

To allow the user at the Microsoft IPsec / L2TP client to access a network resource protected by a Security Gateway, a VPN tunnel is established between the Microsoft IPsec / L2TP client and the Security Gateway, as shown below.

Item	Description
1	Internal hosts
2	Security Gateway
3	Internet
4	Remote IPsec Client

The process of the VPN establishment is transparent to the user, and works as follows:

1. A user at an IPsec / L2TP client initiates a connection to a Security Gateway.
2. The IPsec / L2TP client starts an IKE (Internet Key Exchange) negotiation with the peer Security Gateway. The identities of the remote client machine and the Security Gateway may be authenticated one of these ways:
   - Through exchange of certificates
   - Through pre-shared key

     Note - this option is less secure, since pre-shared key is shared among all L2TP clients.

   Only authenticated machine can establish a connection.
3. Both peers exchange encryption keys, and the IKE negotiation ends.
4. Encryption is now established between the client and the Security Gateway. All connections between the client and the Security Gateway are encrypted inside this VPN tunnel, using the IPsec standard.
5. The Client starts a short L2TP negotiation, at the end of which the client can pass to the Security Gateway L2TP frames that are IPsec encrypted and encapsulated.
6. The Security Gateway now authenticates the user at the Microsoft IPsec / L2TP client. This authentication is in addition to the client machine authentication in step 3. This identification can happen with these methods.
   - A Certificate (EAP)
   - An MD5 challenge (EAP), whereby the user is asked to enter a username and a password (pre-shared secret)
   - A username and a password (PAP)
7. The Security Gateway allocates to the remote client an Office Mode IP address to make the client routable to the internal network. The address can be allocated from all of the Office Mode methods.
8. The Microsoft IPsec / L2TP client connects to the Security Gateway, and can browse and connect to locations in the internal network.

Behavior of an L2TP Connection

When using an IPsec / L2TP client, it is not possible to connect to organization and to the outside world at the same time.

This is because when the client is connected to the Security Gateway, all traffic that leaves the client is sent to the Security Gateway, and is encrypted, whether or not it is intended to reach the protected network behind the Security Gateway. The Security Gateway then drops all encrypted traffic that is not destined for the encryption domain of the Security Gateway.

Security Gateway Requirements for IPsec / L2TP

In order to use Microsoft IPsec / L2TP clients, the Security Gateway must be set up for remote access. The setup is very similar to that required for remote access using Check Point Remote Access Clients, and involves creating a Remote Access community that includes the Security Gateways and the user groups.

An additional requirement is to configure the Security Gateway to supply addresses to the clients by means of the Office Mode feature.

L2TP Global Configuration

Certain settings related to L2TP authentication can be configured globally for Security Gateways of version R71 and higher. These setting are configured in the global properties configuration section of the SmartConsole.

All L2TP clients can be configured to use a Pre-shared key for IKE in addition to the standard user authentication.

To use a Pre-shared key for IKE, go to **Global Properties** > **Remote Access** > **VPN - Authentication and Encryption** and select **Support L2TP with Pre-Shared Key**.

Note - IKE Security Association created for L2TP cannot be used for regular IPsec traffic.

Authentication of Users

There are two methods used to authenticate an L2TP connection:

- Using Legacy Authentication
- Using certificates

Authentication Methods

L2TP clients can use any of the following Authentication schemes to establish a connection:

- Check Point password
- OS password
- RADIUS

- LDAP
- TACACS

Using a username and password verifies that a user is who they claim to be. All users must be part of the Remote Access community and be configured for Office Mode.

Certificates

During the process of establishing the L2TP connection, two sets of authentication are performed. First, the client machine and the Security Gateway authenticate each other's identity using certificates. Then, the user at the client machine and the Security Gateway authenticate each other using either certificates or a pre-shared secret.

The Microsoft IPsec / L2TP client keeps separate certificates for IKE authentication of the client machine, and for user authentication.

On the Security Gateway, if certificates are used for user authentication, then the Security Gateway can use the same certificate or different certificates for user authentication and for the IKE authentication.

Certificates for both clients and users can be issued by the same CA or a different CA. The users and the client machines are defined separately as users in SmartConsole.

Certificates can be issued by:

- The Internal Certificate Authority (ICA) on the Security Management Server
- OPSEC certified Certificate Authority

User Certificate Purposes

It is possible to make sure that PKI certificates are used only for a defined purpose. A certificate can have one or more purposes, such as "client authentication", "server authentication", "IPsec" and "email signing". Purposes appear in the Extended Key Usage extension in the certificate.

The certificates used for IKE authentication do not need any purposes. For the user authentication, the Microsoft IPsec / L2TP client requires that

- The user certificate must have the "client authentication" purpose
- The Security Gateway certificate must have the "server authentication" purpose

Most CAs (including the ICA) do not specify such purposes by default. This means that the CA that issues certificates for IPsec / L2TP clients must be configured to issue certificates with the appropriate purposes (in the Extended Key Usage extension).

It is possible to configure the ICA on the Security Management Server so that the certificates it issues have these purposes. For OPSEC certified CAs, it is possible to configure the Security Management Server to create a certificate request that includes purposes (in the Extended Key Usage extension).

It is also possible to configure the Microsoft IPsec / L2TP clients so that they do not validate the Security Gateway certificate during the L2TP negotiation. This is not a security problem because the client has already verified the Security Gateway certificate during IKE negotiation.

Configuring Remote Access for Microsoft IPsec / L2TP Clients

Establishing a Remote Access VPN for Microsoft IPsec / L2TP clients requires configuration to be performed both on the Security Gateway and on the client machine. The configuration is the same as setting up Check Point Remote Access Clients, with a few additional steps.

High-level workflow to create a Remote Access deployment:

1. Configure a Remote Access environment, including objects and authentication credentials (normally certificates) for the users.
2. Configure support for Office Mode and L2TP on the Security Gateway.
3. On the client machine, place the user certificate in the User Certificate Store, and the client machine certificate in the Machine Certificate Store.
4. On the client machine, set up the Microsoft IPsec / L2TP client connection profile.

Configuring a Remote Access Environment

Configure the network to use VPN connections for Remote Access.

Defining the Client Machines and their Certificates

1. Define a user that corresponds to each client machine, or one user for all machines, and generate a certificate for each client machine user. The steps are the same as those required to define users and their certificate.
2. Add users that correspond to the client machines to a user group, and add the user group to the Remote Access VPN community.

Configuring Office Mode and L2TP Support

To configure L2TP support:

1. Configure Office Mode (see *"Office Mode" on page 64*).
2. Click **Gateways & Servers** and double-click the Security Gateway.

The Security Gateway Properties window opens and shows the **General Properties** page.

3. From the navigation tree, click **VPN Clients > Remote Access**.
4. Click **Support L2TP**.
5. Select the **Authentication Method** for the users:
   - To use EAP certificates, choose **Smart Card or other Certificates (encryption enabled)**.
   - To use an EAP username and a shared secret (password), choose **MD5-challenge**.

   Notes:
   - The chosen authentication method is relevant only when clients are configured with EAP.
   - Pay attention that the configuration on the realm is the enforcement of the authentication method (in the Security Gateway object properties: **Remote Access** > **Authentication** > **Allow old users to connect** > **Settings** > **Authentication method**).
6. For **Use this certificate**, select the certificate that the Security Gateway presents in order to authenticate itself to users.
7. Click **OK** and publish the changes.

Preparing the Client Machines

1. In the Windows **Services** window of the client machine, make sure that the **IPsec Policy Agent** is running. It should preferably be set to Automatic.
2. Make sure that no other IPsec Client is installed on the machine.

Placing the Client Certificate in the Machine Certificate Store

1. Log in to the client machine with administrator permissions.
2. Run the Microsoft Management Console. Click **Start > Run**
3. Enter `mmc`, and press Enter.
4. Select **Console > Add/Remove Snap-In**.
5. In the **Standalone** tab, click **Add**.
6. In the **Add Standalone Snap-in** window, select **Certificates**.
7. In the **Certificates snap-in** window, select **Computer account**.

8. In the **Select Computer** window select the computer (whether local or not) where the new certificates have been saved.
9. Click **Finish** to complete the process and click **Close** to close the **Add/Remove Snap-in** window.
10. The MMC **Console** window appears, where a new certificates branch has been added to the Console root.
11. Right-click on the **Personal** entry of the **Certificates** branch and select **All Tasks > Import**. A Certificate Import Wizard is displayed.
12. In the Certificate Import Wizard, browse to the location of the certificate.
13. Enter the certificate file password.
14. In the **Certificate Store** window make sure that the certificate store is selected automatically based on the certificate type.
15. Select **Finish** to complete the Import operation.
16. Go to the **Certificate** subdirectory (under **Personal**). There is one certificate with the user name and a second certificate with the management name.
17. Select the management certificate and drag it to the **Certificates** list under the **Trusted Root Certificate** subdirectory.
18. Exit from the MMC console. You do not have to save it. You can see the changes in Internet Explorer Properties.

Using the MMC, the certificate can be seen in the certificate store for the "Local Computer".

Placing the User Certificate in the User Certificate Store

1. On the client machine, double-click on the user's certificate icon (the **.p12** file) in the location where it is saved. A Certificate Import Wizard is displayed
2. Enter the password.
3. In the **Certificate Store** window make sure that the certificate store is selected automatically based on the certificate type.
4. Select **Finish** to complete the Import operation.

Using the MMC, the certificate can be seen in the certificate store for the "current user".

Setting up the Microsoft IPsec/L2TP Client Connection Profile

Once the Client machine's certificate and the user's certificate have been properly distributed, set up the L2TP connection profile. The instruction might be slightly different on different versions of Windows.

To configure the L2TP profile:

1. On the client machine, go to the **Network and Sharing Center**.
2. Select **Set up a new connection or network**> **Connect to a workplace** > **Use my Internet connection (VPN).**
3. In **Internet address**, enter the IP address or the resolvable host name of the Security Gateway.
4. In **Destination name**, enter a name for the new connection, for example, L2TP_ connection.
5. On Windows 7: Select **Don't connect now; just set it up so I can connect later**.
6. Click **Next**.
7. Click **Create**.
8. Click **Close**.

To complete the L2TP connection configuration:

1. In the **Network and Sharing Center**, click **Change adapter settings**.
2. Right-click on the connection you created and select **Properties**.
3. In the **Security** tab, under **Type of VPN**, select **Layer 2 Tunneling Protocol with IPSEC (L2TP/IPSEC)**.
4. Click **Advanced settings**, and in the **L2TP** tab:
   - If you configured the Security Gateway to support preshared key, you can select preshared key for authentication and enter the preshared key.
   - If you configured the Security Gateway to use Smart Card or another certificate, you can select Use certificate for authentication.
5. Click **OK**.
6. Under **Authentication** select **Use Extensible Authentication protocols** or **Allow these protocols**.
   - If you select **Use extensible Authentication protocols** (EAP): Select **MD5-challenge**, or **Smart Card or other Certificates**. Choose the authentication method you configure on the Security Gateway (on Support L2tp).
   - If you select **Allow these protocols**: Select **Unencrypted password (PAP)**.
7. Click **OK**.

Configuring User Certificate Purposes

A CA that issues certificates for IPsec/L2TP clients must be configured to issue certificates with the appropriate purposes.

Alternatively, the Microsoft IPsec/L2TP Client can be set to not require the "Server Authentication" purpose on the Security Gateway certificate.

Configuring the CA to Issue Certificates (L2TP)

To configure the CA with the ICA Management Tool:

1. Run the ICA Management tool:
2. Change the property **IKE Certificate Extended Key Usage** property to the value 1, to issue Security Gateway certificates with the "server authentication" purpose.
3. Change the property **IKE Certificate Extended Key Usage** to the value 2 to issue user certificates with the "client authentication" purpose.

   If you are using an OPSEC certified CA to issue certificates, use the *Database Tool (GuiDBEdit Tool)* to change the value of the global property **cert_req_ext_key_usage** to **1**. This causes the Security Management Server to request a certificate that has purposes (Extended Key Usage extension) in the certificate.

To configure the CA with SmartConsole:

1. Click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway Properties window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPsec VPN**.
3. In the **Repository of Certificates Available to the Gateway** section, click **Add**.
4. The **Certificate Properties** window opens.
5. Configure the settings for the certificate and click **OK**.
6. Select the certificate and click **View**.
7. Make sure that the Extended Key Usage Extension appears in the certificate.
8. From the navigation tree, click **VPN Clients > Remote Access**.
9. In the **L2TP Support** section, select the new certificate.
10. Click **OK** and publish the changes.

To Configure the Microsoft IPsec/L2TP Clients so they do not Check for the "Server Authentication" Purpose

The following procedure tells the Microsoft IPsec/L2TP Client not to require the "Server Authentication" purpose on the Security Gateway certificate.

1. In the client machine, right-click on the **My Network Places** icon on the desktop and select **Properties**.
2. In the **Network and Dial-up Connections** window, double-click the L2TP connection profile.
3. Click **Properties**, and select the **Security** tab.
4. Select **Advanced (custom settings)**, and click **Settings**.
5. In the **Advanced Security Settings** window, below **Logon security**, select **Use Extensible Authentication Protocol (EAP)**, and click **Properties**.
6. In the **Smart Card or other Certificate Properties** window, uncheck **Validate server certificate**, and click **OK**.

Note - The client validates all aspects of the Security Gateway certificate, during IKE authentication, other than the "Server Authentication" purpose.

Making the L2TP Connection

1. Click on **Connect** to make the L2TP connection.
2. To view the IP address assigned to the connection, either view the **Details** tab in the connection **Status** window, or use the "`ipconfig /all`" command.

For More Information

The L2TP protocol is defined in RFC 2661. Encryption of L2TP using IPsec is described in RFC 3193. For information about the L2TP protocol and the Microsoft IPsec/L2TP client, see the Network and Dial Up Connections Help in Windows for your version.

VPN Routing - Remote Access

The Need for VPN Routing

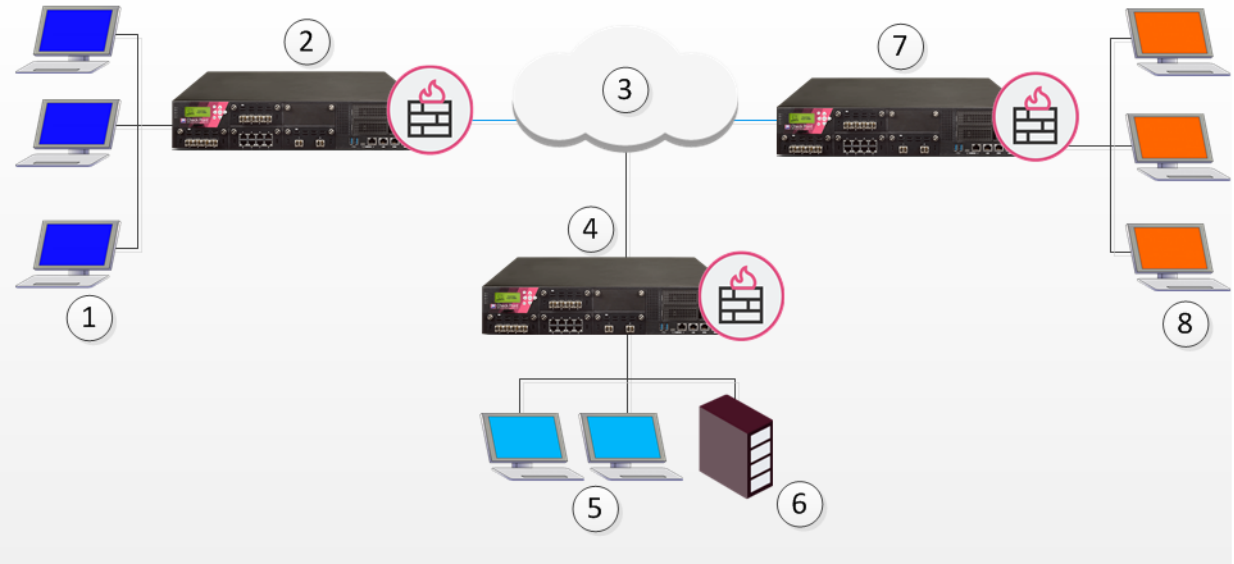
There are a number of scenarios in which a Security Gateway or remote access clients cannot connect directly to another Security Gateway (or clients). Sometimes, a given Security Gateway or client is incapable of supplying the required level of security. For example:

- Two Security Gateways with **dynamically assigned IP addresses** (DAIP Security Gateways). Hosts behind either Security Gateway need to communicate; however, the changing nature of the IP addresses means the two DAIP Security Gateways cannot open VPN tunnels. At the moment of tunnel creation, the exact IP address of the other is unknown.
- Remote access client users wish to have a private conversation using **Voice-over-IP** (VoIP) software or utilize other client-to-client communication software such as Microsoft NetMeeting. Remote access clients cannot open connections directly with each other, only with configured Security Gateways.

In all cases, a method is needed to enhance connectivity and security.

Check Point Solution for Greater Connectivity and Security

VPN routing provides a way of controlling how VPN traffic is directed. VPN routing can be implemented with Security Gateway modules and remote access clients. Configuration for VPN routing is performed either directly through SmartConsole (in simple cases) or by editing the VPN routing configuration files on the Security Gateways (in more complex scenarios).



Item	Description
1	Host machines
2	Security Gateway A
3	Internet
4	Security Gateway B
5	Host machines
6	Security Management Server
7	Security Gateway C
8	Host machines

In the figure above, one of the host machines behind Security Gateway A needs to connect with a host machine behind Security Gateway B. For either technical or policy reasons, Security Gateway A cannot open a VPN tunnel with Security Gateway B. However, both Security Gateways A and B can open VPN tunnels with Security Gateway C, so the connection is routed through Security Gateway C.

As well as providing enhanced connectivity and security, VPN routing can ease network management by hiding a complex network of Security Gateways behind a single Hub.

Hub Mode (VPN Routing for Remote Clients)

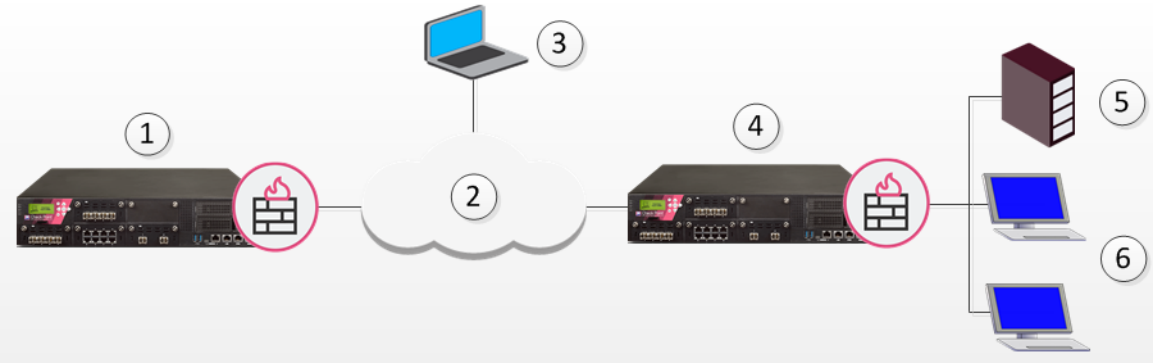
VPN routing for remote access clients is enabled via Hub Mode. In Hub mode, all traffic is directed through a central Hub. The central Hub acts as a kind of router for the remote client. Once traffic from remote access clients is directed through a Hub, connectivity with other clients is possible as well as the ability to inspect the subsequent traffic for content.

When using Hub mode, enable Office mode. If the remote client is using an IP address supplied by an ISP, this address might not be fully routable. When Office mode is used, rules can be created that relate directly to Office mode connections.

Note - Office mode is not supported in SecuRemote.

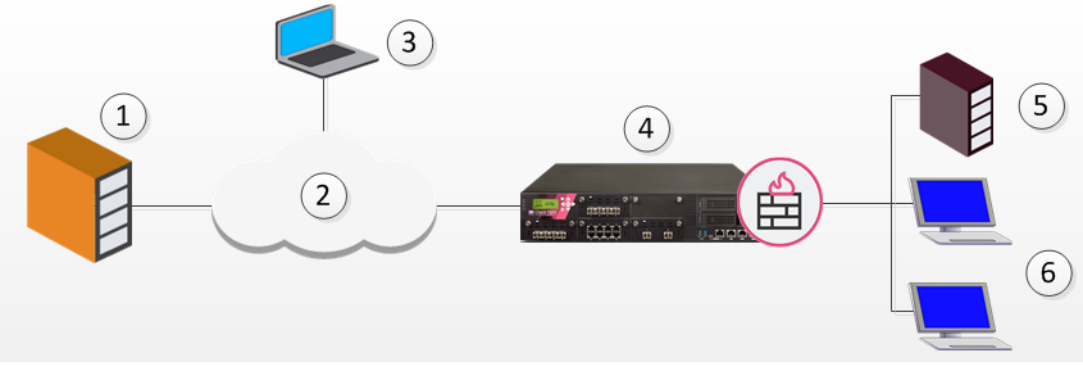
Allowing Clients to Route all Traffic Through a Security Gateway

In the following figure, the remote client needs to connect with a server behind Security Gateway 2. Company policy states that all connections to this server must be inspected for content. For whatever reason, Security Gateway 2 cannot perform the required content inspection. When all the traffic is routed through Security Gateway 1, connections between the remote client and the server can be inspected.



Item	Description
1	Security Gateway 1
2	Internet
3	Remote client
4	Security Gateway 2
5	Server
6	Hosts

Suppose the same remote client needs to access an HTTP server on the Internet. The same company policy regarding security still applies.



Item	Description
1	HTTP Server
2	Internet
3	Remote client
4	Security Gateway

Item	Description
5	OSPEC Certified UFP server
6	Hosts

The remote client's traffic is directed to the Security Gateway where it is directed to the UFP (URL Filtering Protocol) server to check the validity of the URL and packet content, since the Security Gateway does not possess URL-checking functionality. The packets are then forwarded to the HTTP server on the Internet.

NATing the address of the remote client behind the Security Gateway prevents the HTTP server on the Internet from replying directly to the client. If the remote client's address is not NATed, the remote client will not accept the clear reply from the HTTP server.

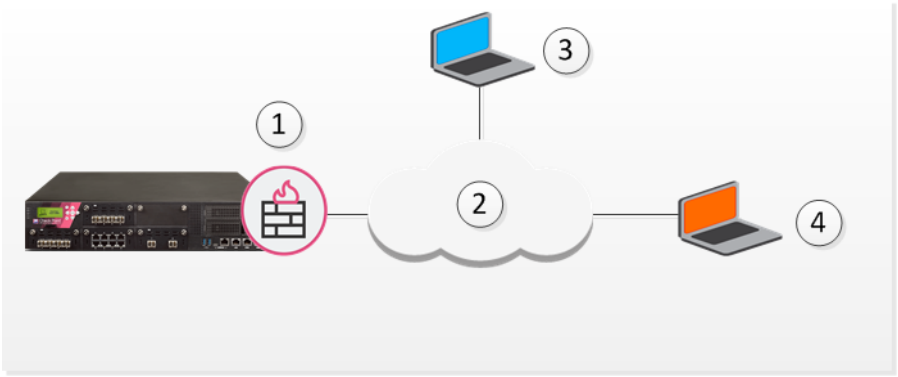
Remote Client to Client Communication

Remote client to client connectivity is achieved in two ways:

- By routing all the traffic through the Security Gateway
- Including the Office Mode range of addresses in the VPN domain of the Security Gateway

Routing all Traffic through the Security Gateway

Two remote users use VoIP software to hold a secure conversation. The traffic between them is directed through a central Hub, as shown in the following figure.

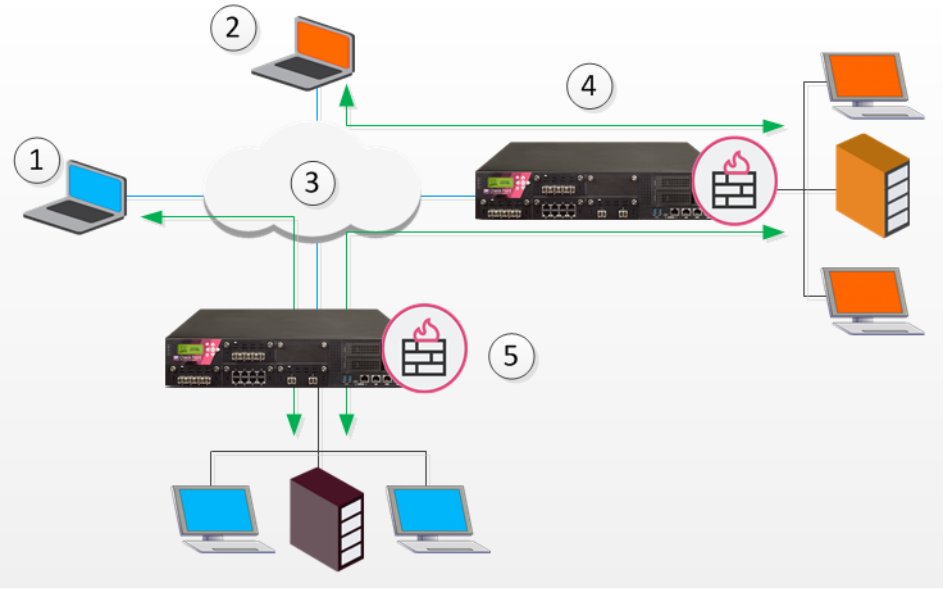


Item	Description
1	Security Gateway
2	Internet
3	Remote Client VoIP
4	Remote Client VoIP

For this to work:

- **Allow VPN clients to route traffic through this Security Gateway** must be enabled on the Security Gateway.
- The remote client must be configured with a profile that enables all traffic to be routed through the Security Gateway.
- Remote clients are working in connect mode.

If the two remote clients are configured for Hub mode with different Security Gateways, the routing takes place in three stages - each remote client to its designated Security Gateway, then between the Security Gateways:



Item	Description
1	Remote Client 1
2	Remote Client 2
3	Internet
4	Security Gateway A
5	Security Gateway B

In the figure above, remote client 1 is configured for Hub mode with Security Gateway B. Remote client 2 is configured for Hub mode with Security Gateway A. For the connection to be routed correctly:

- Office mode must be enabled.
- VPN configuration files on both Security Gateways must include the Office Mode address range used by the other. The VPN configuration file on Security Gateway A directs all traffic aimed at an Office Mode IP address of Security Gateway B towards Security Gateway B. A connection leaves Remote Client1 and is sent to Security Security Gateway B. From Security Gateway B the connection is passed to Security Security Gateway A. Security Security Gateway A once more redirects the traffic towards Remote Client 2. The reply from Remote Client2 follows the same path but in reverse.
- Office mode addresses used by both Security Gateways must be non-overlapping.

Configuring VPN Routing for Remote Access VPN

Common VPN routing scenarios can be configured through a VPN star community, but not all VPN routing configuration is handled through SmartConsole. VPN routing between Security Gateways (star or mesh) can be also be configured by editing the configuration file `$FWDIR/conf/vpn_route.conf`

VPN routing cannot be configured between Security Gateways that do not belong to a VPN community.

Hub Mode for Remote Access Clients

To enable Hub Mode for Remote Access clients:

1. Click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **VPN Clients > Remote Access**.
3. In the **Hub Mode configuration** section, click **Allow VPN clients to route all traffic through this Security Gateway**.
4. Click **OK**.
5. From the Objects Bar, click **VPN Communities**.
6. Double-click the Remote Access community object.
7. From the **Participating Gateways** page, make sure that the Hub Security Gateway is in the window.
8. On the **Participant User Groups** page, select the remote access users or user groups.
9. Click **OK**.
10. Create the access control rule in the Access Control Policy.

VPN routing traffic is handled in the Security Policy Rule Base as a single connection, matched to one rule only.

11. Click **OK** and publish the changes.
12. Configure the profile on the remote client to route all communication through the designated Security Gateway.

Adding the Office Mode Range to the VPN Domain

SmartConsole includes a default object for Office Mode IP addresses, **CP_default_Office_Mode_addresses_pool**. You can use the default object, or create a new one for your network.

To create a new Office Mode IP address object:

1. In SmartConsole, click **Objects >Object Explorer** (Ctrl+E).
2. Click **New > Network**.
3. Enter the **Name**, **IP address** and **Net mask**.
4. Click **OK** and publish the changes.

To configure VPN routing for remote access clients with the VPN domain:

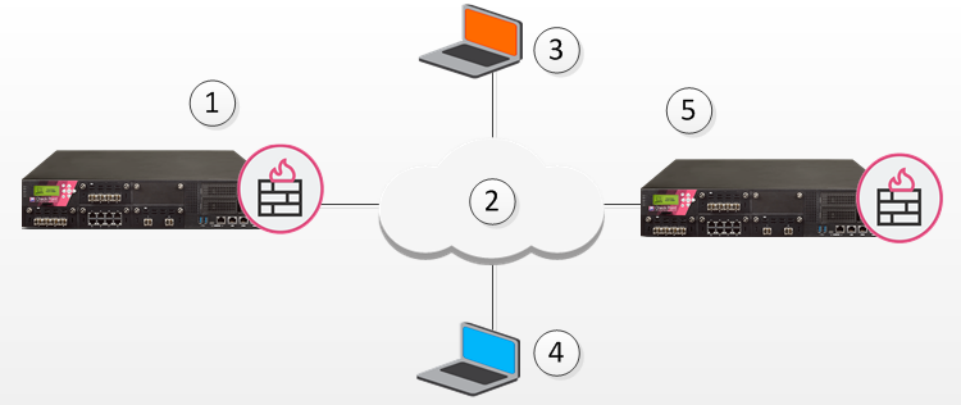
1. Create a network group, click **New > Network Group**.
2. Add these network groups:
   - VPN domain
   - Office Mode
3. Click **OK** and publish the changes.
4. Click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
5. From the navigation tree, click **Network Management > VPN Domain**.
6. Click **Manually defined**.
7. Select the new network group.
8. Click **OK** and publish the changes.

   The remote clients must connect to the site and perform a site update before they can communicate with each other.

Client to Client via Multiple Hubs Using Hub Mode

The figure below shows two remote clients each configured to work in Hub mode with a different Security Gateway:



Item	Description
1	Hub 1
2	Internet
3	Remote Client 1
4	Remote Client 2
5	Hub 2

Remote Client 1 works in Hub mode with Hub 1. Remote Client 2 works in Hub mode with the Hub 2. In order for VPN routing to be performed correctly:

- Remote clients must be working in Office mode
- Office mode address range of each Security Gateway must be included in the vpn_ route.conf file installed on the other Security Gateway.

Destination	Next hop router interface	Install On
Hub1_OfficeMode_range	Hub1	Hub2
Hub2_OfficeMode_range	Hub2	Hub1

When Remote Client 1 communicates with Remote Client 2:

- The traffic first goes to the Hub 1, since Remote Client 1 is working in Hub mode with Hub 1.

- Hub 1 identifies Remote Client 2's IP address as belonging to the Office mode range of Hub 2.
- The `vpn_route.conf` file on Hub 1 identifies the next hop for this traffic as Hub 2.
- The traffic reaches the Hub 2; Hub 2 redirects the communication to Remote Client 2.

Link Selection for Remote Clients

Link Selection is a method used to determine which interface to use for incoming and outgoing VPN traffic and the best possible path for the traffic. Using Link Selection, you choose which IP addresses are used for VPN traffic on each Security Gateway.

Load Sharing and Service Based Link Selection are not supported when the peer is a Remote Access Client. If the Probing Redundancy mode configuration is Load Sharing and the peer is a remote access client, High Availability will be enforced for the client's tunnel.

Link selection is configured on each Security Gateway in the **Security Gateway Properties** > **IPSec VPN** > **Link Selection** window. The settings apply to both:

- Security Gateway to Security Gateway connections
- Remote access client to Security Gateway connections

You can configure Link Selection for remote users separately. These settings override the settings configured on the Link Selection page.

Configuring Link Selection for Remote Access Only

To configure separate Link Selection settings for remote access VPN:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. In the top left pane, to **Network Objects** > **network_objects**.
4. In the top right pane, select the Security Gateway / cluster object.
5. In the bottom pane, change the value of `apply_resolving_mechanism_to_SR` to `false`.
6. In the bottom pane, edit the `ip_resolution_mechanism` attribute to determine how remote access clients resolve the IP address of the local Security Gateway. Select **one** of the these:
   - `mainIpVpn` - Always use the main IP address specified in the **IP Address** field on the **General Properties** page of the Security Gateway

- `singleIpVpn` - The VPN tunnel is created with the Security Gateway using an IP address set in `single_VPN_IP_RA`
- `singleNATIpVPN` - The VPN tunnel is created using a NATed IP address set in `single_VPN_IP_RA`
- `topologyCalc` - Calculate the IP address used for the VPN tunnel by network topology based on the location of the remote peer

Note -Probing is **not** supported for Remote Access VPN. Do **not** select `oneTimeProb` or `ongoingProb`.

7. Save changes (**File** menu > **Save All**).
8. Close the Database Tool (GuiDBEdit Tool).
9. Connect with SmartConsole to the Management Server.
10. In SmartConsole, install the Access Policy on the Security Gateway / cluster object.

Directional VPN in Remote Access Communities

Directional VPN for Remote Access Communities lets you reject connections to or from a specified network object.

Source	Destination	VPN	Service	Action
Any	Any	Remote_Access_Community => MyIntranet	Any	drop
Any	Any	Remote_Access_Community => Any Traffic	Any	accept

Connections are not allowed between remote users and hosts within the "MyIntranet" VPN community. All other connections that start from the Remote Access Community, from inside or outside of the VPN communities, are allowed.

User Groups as the Destination in RA communities

User groups can be placed in the destination column of a rule. This makes:

- Configuring client to client connections easier
- Configuring "back connections" between a remote client and a Security Gateway possible.

Source	Destination	VPN	Service	Action
Any	Remote_ Users@Any	Any Traffic => Remote_Access_ Community	Any	accept

To include user groups in the destination column of a rule:

- The rule must be directional
- In the VPN column, the Remote Access community must be configured as the endpoint destination

Configuring Directional VPN with Remote Access Communities

To configure Directional VPN with Remote Access communities:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **VPN > Advanced**.
3. Click **Enable VPN Directional Match in VPN Column**.
4. Click **OK** and publish the changes.
5. Go to **Security Policies > Access Control Policy.**
6. Right-click the VPN cell for the rule, and select **Directional Match Condition**.

   The **New Directional Match Condition** window opens.
7. Configure the directional VPN:
   - From **Traffic reaching from**, select the source of the connection
   - From **Traffic leaving to**, select the connection's destination
8. Click **OK**.
9. Install policy.

Remote Access Advanced Configuration

Domain Controller Name Resolution

If clients are configured in Connect Mode and Office Mode, clients automatically resolve the NT domain name using dynamic WINS.

Otherwise, clients resolve the NT domain name using either LMHOSTS or WINS.

LMHOSTS

Enter the relevant information (see below) the `$FWDIR/conf/dnsinfo.C` file on the Security Gateway, and install the policy.

```
(
     :LMdata(
          :(
               :ipaddr (<IP address>)
               :name (<host name>)
               :domain (<domain name>)
          )
          :(
               :ipaddr (<IP address>)
               :name (<host name>)
               :domain (<domain name>)
          )
     )
)
```

When the topology is updated, the name resolution data will be automatically transferred to the `dnsinfo` entry of the `userc.C` file and then to its `LMHOSTS` file.

Authentication Timeout and Password Caching

The Problem

Users consider multiple authentications during the course of a single session to be a nuisance. At the same time, these multiple authentications are an effective means of ensuring that the session has not been hijacked (for example, if the user steps away from the endpoint computer for a period of time). The problem is finding the correct balance between convenience and security.

The Solution

Multiple authentication can be reduced by:

- Increasing the re-authentication interval
- Caching the user's password

Re-Authentication Interval

For Connect Mode, the countdown to the timeout begins from the time that the Remote Access client is connected.

To set the length of time between re-authentications:

1. From Menu, select **Global Properties**.
2. From the navigation tree, click **Remote Access**> **Endpoint Security VPN**.
3. In **Re-authenticate user every**, select a number of minutes between re-authentications.
4. Click **OK.**
5. Install Policy.

Password Caching

When the timeout expires, the user will be asked to authenticate again. If password-caching is enabled, clients will supply the cached password automatically and the authentication will take place transparently to the user. In other words, the user will not be aware that re-authentication has taken place.

Password caching is possible only for multiple-use passwords. If the user's authentication scheme implement one-time passwords (for example, SecurID), then passwords cannot be cached, and the user will be asked to re-authenticate when the authentication time-out expires. For these schemes, this feature should **not** be implemented.

To configure password caching:

1. From Menu, select **Global Properties**.
2. From the navigation tree, click **Remote Access**> **Endpoint Security VPN**.
3. In **Enable password caching**, select an option.
4. If Password caching is enabled, in **Cache password for**, select the amount of minutes it is cached for.

Secure Domain Logon (SDL)

The Problem

When a Remote Access client user logs on to a domain controller, the user has not yet entered credentials, and so the connection to the domain controller is not encrypted.

The Solution

When the Secure Domain Logon (SDL) feature is enabled, after the user enters the OS user name and password (but before the connection to the domain controller is started), the **User Authentication** window appear. When the user enters the Remote Access client credentials, the connection to the domain controller takes place over an encrypted tunnel.

Configuring SDL Timeout

Because SDL depends on the synchronization of concurrent processes, flexibility in defining timeouts is important.

The SDL Timeout feature controls the period, during which a user must enter their domain controller credentials.

When the allocated time expires and no cached information is used (if applicable), the Secure Domain Logon fails.

The timeout is controlled by the global parameter `sdl_netlogon_timeout`:

Procedure

1. Publish the SmartConsole session.
2. Close all SmartConsole windows connected to the Management Server.
3. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
4. In the top left pane, go to **Table** > **Global Properties** > **firewall_properties**.
5. In the top right pane, click **global_properties**.
6. Click the **Search** menu > **Find** (or press the **CTRL+F** keys).
7. In the Find window:
   a. In the **Find what** field, paste: `sdl_netlogon_timeout`
   b. In the **Search in** section, selection only **Fields**
   c. Click **Find Next**
8. In the lower pane:

a. Right-click `sdl_netlogon_timeout` > click **Edit**

b. Enter the applicable integer value of seconds

c. Click **OK**.

9. Click the **File** menu > **Save All**.
10. Click the **File** menu > **Exit**.
11. Connect with SmartConsole to the Management Server.
12. Install the Access Control policy on the applicable VPN Gateway.

Cached Information

When the Remote Access client computer successfully logs on to a domain controller, the user's profile is saved in cache. This cached information will be used if subsequent logons to the domain controller fail, for whatever reason.

To configure this option in the Windows Registry:

1. Go to `HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon`.
2. Create a new key "`CachedLogonCount`" with the valid range of values from 0 to 50.

   The value of the key is the number of previous logon attempts that a server will cache.

   A value of 0 disables logon caching.

   A value greater than 50 keeps only 50 logon attempts in the cache.

Configuring Secure Domain Logon

1. Configure the Remote Access client to use LMHOSTS (all platforms) or WINS (all platforms except Windows 9x).
2. Define the site where the domain controller resides and download/update the topology.
3. If the endpoint computer is not already a domain member, configure it to be a domain member.
4. Reboot the computer.
5. Log in to the computer.

Using Secure Domain Logon

1. When the Windows **Logon** window appears, enter the operating system credentials.
2. Click **OK**.

   The **Logon** window appears.

3. Enter the Remote Access client credentials during the defined time (see *"Configuring SDL Timeout" on page 153*).

If you fail to logon and no cached information is used, wait one minute and try again.

If SDL is already configured on the endpoint computer, the administrator can customize the Remote Access client installation packages with SDL enabled by default.

Create a self-extracting Remote Access client package using the VPN Configuration Utility and select **Enable Secure Domain Logon**. See the *Remote Access Clients for Windows Administration Guide* for your release on the Endpoint Security home page.

Post-Connect Script

The Post-Connect feature runs a script on an endpoint computer after the Remote Access client establishes a VPN connection.

The Post-Connect script runs with user-level permissions.

For security reasons, it is not supported to run the Post-Connect script, if a Secure Domain Login occurs before a Windows login.

Simultaneous Login and Aggressive Simultaneous Login Prevention (SLP)

You can use Simultaneous Login Prevention (SLP) to restrict the ability of a user to log in to Remote Access VPN more than once.

SLP is supported only if you configure the same authentication method for the user from all devices (see *"strongSwan Client Support" on page 196*).

To configure simultaneous login settings:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway / Cluster object.
3. From the navigation tree, click **Remote Access**.
4. Below **Simultaneous Login**, select one of these:
   - **User is allowed several simultaneous login** - a user can log in to Remote Access VPN from more than one device at the same time
   - **User is allowed only single login** - a user can log in to Remote Access VPN from only one device
5. Click **OK**.
6. Install the policy on the VPN Gateway.

Aggressive SLP enables a VPN Gateway to automatically disconnect a remote user with more than one simultaneous login. When Aggressive SLP is enabled, inactive VPN tunnels are disconnected.

To enable Aggressive SLP:

1. On the VPN Gateway command line, run this command in the Expert mode:

```
ckp_regedit -a \\SOFTWARE\\CheckPoint\\VPN1 aggresive_slp_sc_
disconnect -n 1
```

2. In SmartConsole, install policy on this VPN Gateway.

To disable Aggressive SLP:

1. On the VPN Gateway command line, run this command in the Expert mode:

```
ckp_regedit -a SOFTWARE\\CheckPoint\\VPN1 aggresive_slp_sc_
disconnect -n 0
```

2. In SmartConsole, install policy on this VPN Gateway.

To check the configuration status of Aggressive SLP:

On the VPN Gateway command line, run this command in the Expert mode

```
grep slp $CPDIR/registry/HKLM_registry.data
```

One of these outputs appears:

- `aggresive_slp_sc_disconnect ("[4]1")` - shows that Aggressive SLP is enabled.
- `aggresive_slp_sc_disconnect ("[4]0")` - shows that Aggressive SLP is disabled.

Perfect Forward Secrecy (PFS)

In cryptography, Perfect Forward Secrecy (PFS) refers to the condition in which the compromise of a current session key or long-term private key does not cause the compromise of earlier or subsequent keys. Security Gateways meet this requirement with a PFS mode. When PFS is enabled, a new Diffie-Helman (DH)key is generated during IKE phase II, and renewed for each key exchange. .

To enable VPN Gateway to enforce PFS for Remote Access clients:

1. On the VPN Gateway command line, run this command in the Expert mode:

   ```
   ckp_regedit -a \\SOFTWARE\\CheckPoint\\VPN1 force_ra_pfs -n 1
   ```

2. In SmartConsole, install policy on this VPN Gateway.
3. **Optional:** To change the DH group, in SmartConsole, go to Menu > **Global properties** > **Remote Access** > **VPN - Authentication and Encryption** > **Encryption algorithms** > **Edit** > **Phase 1** > **Use Diffie-Hellman group**.

To stop a Security Gateway from enforcing PFS for Remote Access clients:

1. On the Security Gateway command line, run this command in the Expert mode

   ```
   ckp_regedit -d \\SOFTWARE\\CheckPoint\\VPN1 force_ra_pfs
   ```

2. In SmartConsole, install policy on this Security Gateway.

To check the configuration status of PFS on the Security Gateway:

1. On the Security Gateway command line, run this command in the Expert mode

   ```
   cat $CPDIR/registry/HKLM_registry.data | grep force_ra_pf
   ```

2. If the `force_ra_pfs` parameter exists, then it is printed. This means that PFS is enforced.

How to Work with non-Check Point Firewalls

If a Remote Access client is located behind a non-Check Point firewall, the following ports must be opened on the firewall to allow VPN traffic to pass:

Port	Description
UDP port 500	Always, even if using IKE over TCP
TCP port 500	Only if using IKE over TCP
IP protocol 50 ESP	Unless always using UDP encapsulation
UDP port 2746	Only if using MEP, interface resolving or interface High Availability
UDP port 259	Only if using MEP, interface resolving or interface High Availability

Resolving Internal Names with an Internal DNS Server

Problem:

Remote Access Clients use an internal DNS server to resolve the names of internal hosts (behind the Security Gateway) with non-unique IP addresses.

Solution:

Best practice is:

- For Endpoint Security VPN and Check Point Mobile for Windows, use Office mode.
- For SecuRemote, use the Split DNS feature (see *"Split DNS" below*).

Split DNS

Split DNS uses a SecuRemote DNS Server, an object that represents an internal DNS server that you can configure to resolve internal names with private IP addresses (RFC 1918). It is best to encrypt the DNS resolution of these internal names.

After you configure a SecuRemote DNS server to resolve traffic from a specified domain and install policy, it takes effect. If users try to access that domain while connected to the VPN, the request is resolved by the SecuRemote DNS server. The internal DNS server can only work when users are connected to the VPN.

You can configure multiple SecuRemote DNS servers for different domains.

Configuring Split DNS

To configure a Remote Access client DNS server for Split DNS:

1. In SmartConsole, in the Objects tree, select **New** > **More** > **Server**> **More**> **SecuRemote DNS**.

   The **New SecuRemote DNS** window opens.

2. In the **General** tab, enter a name for the server and select the host on which it runs.
3. In the **Domains** tab, click **Add** to add the domains that will be resolved by the server.

   The Domain window opens,

4. Enter the **Domain Suffix** for the domain that the Remote Access client's DNS server will resolve, for example, `checkpoint.com`.
5. In the **Domain Match Case** section, select the maximum number of labels that can be in the URL before the suffix. URLs with more labels than the maximum will not be sent to that DNS.
   - **Match only *.suffix** - Only requests with 1 label are sent to the Remote Access client's DNS server. For example, "`www.checkpoint.com`" and "`whatever.checkpoint.com`" but not "`www.internal.checkpoint.com`".
   - **Match up to x labels preceding the suffix** - Select the maximum number of labels. For example, if you select 3, then the SecuRemote DNS Server will be used to resolve "`www.checkpoint.com`" and "`www.internal.checkpoint.com`" but not "`www.internal.inside.checkpoint.com`".
6. Click **OK**.
7. Install the policy.

Enabling or Disabling Split DNS

Split DNS is automatically enabled. On Endpoint Security VPN and Check Point Mobile for Windows, you can edit a parameter in the `trac_client_1.ttm` configuration file to set if Split DNS is enabled, disabled, or depends on the Remote Access client settings.

To change the setting for Split DNS on the Security Gateway:

1. On the Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file with Vi editor.

   ```
   vi $FWDIR/conf/trac_client_1.ttm
   ```

2. Add the "`split_dns_enabled`" property to the file:

   ```
   :split_dns_enabled (
       :gateway (
           :map (
               :true (true)
               :false (false)
               :client_decide (client_decide)
           )
           :default (client_decide)
       )
   )
   ```

3. Set the value in the `:default` attribute:

- **true** - enabled
- **false (default)** - disabled
- **client_decide** - Takes the value from a file on the endpoint computer

4. Save the changes in the file and exit the editor.
5. In SmartConsole, install policy on this Security Gateway.

Multiple Entry Points for Remote Access VPNs

The Need for Multiple Entry Point (MEP) VPN Gateways

The VPN Gateway provides a single point of entry to the internal network. The VPN Gateway makes the internal network "available" to remote computer. If the VPN Gateway fails, the internal network is no longer available.

To solve this issue, configure several VPN Gateways (**Multiple Entry Points** - MEP) for the same internal network.

The Check Point Solution for Multiple Entry Points

In an MEP environment, you install two VPN Gateways to provide remote access to your internal network(s).

You configure how a Remote Access client selects a VPN Gateway.

Note - The MEP VPN Gateways do not have to be at the same geographical site.

Prerequisite

Before you configure MEP, make sure that the same Login Option is configured for all Security Gateways that participate in MEP. For more information, see *"Multiple Login Options" on page 41*

MEP Methods

There are different ways for Remote Access clients to connect to MEP VPN Gateways:

- **First to Respond** - The Remote Access client connects to the first VPN Gateway that responds.
- **Primary/Backup** - The Remote Access client connects to the VPN Gateway that you configured as Primary. If the Primary VPN Gateway does not respond, the Remote Access client connects to the VPN Gateway that you configured as Backup. If the Backup VPN Gateway does not respond, the Remote Access client fails the entire remote access VPN connection.
- **Random Selection** - In a Load Sharing MEP environment, the Remote Access client randomly selects one of the configured VPN Gateways and assigns priority to that VPN Gateway. The Remote Access client uses the selected VPN Gateway for all subsequent connections.

Visitor Mode and MEP

The VPN Gateway discovery mechanism used in an MEP environment runs over UDP (proprietary Check Point communication). This creates a special challenge for Remote Access clients that work in Visitor Mode, because all traffic is tunneled over a regular TCP connection.

In an MEP environment:

- A special Visitor Mode handshake is used as a probing method to test the availability of the VPN Gateways.
- When a MEP failover occurs, the Remote Access client disconnects and the user has to reconnect to the VPN site in the usual way. See sk115996 for information on configuration.
- In a *Primary-Backup* configuration, the Remote Access client reconnects to the backup VPN Gateway only when the Primary VPN Gateway is unavailable. When the Primary VPN Gateway is available again, the Remote Access client stays connected to the Backup VPN Gateway and does not connect to the Primary VPN Gateway.
- All the VPN Gateways in the MEP must support Visitor Mode.

Routing Return Packets

These are the ways to configure the routing for return packets:

- Enable NAT for the Office Mode network.
- If the client is configured to ignore Office Mode, use the IP Pool NAT.

IP Pool NAT

IP pool NAT maps source IP addresses from remote VPN domains to an IP address from a pool of registered IP addresses. To maintain symmetric sessions with MEP Security Gateways, the MEP Security Gateway does NAT with a range of IP addresses dedicated to that specific Security Gateway and should be routed within the internal network to the originating Security Gateway (. When the returning packets reach the Security Gateway, the Security Gateway restores the original source IP address and forwards the packets to the source.

Configuring MEP

To configure MEP, select an MEP selection method:

- **First to Respond**
- **Primary/Backup**
- **Load Distribution**

Defining MEP Method

Define MEP configuration as one of these:

- **Implicit** - MEP methods and the identities of VPN Gateways are taken from the topology and configuration of VPN Gateways. VPN Gateways are in fully overlapping encryption domains or have Primary-Backup VPN Gateways.
- **Manual** - You can edit the list of MEP VPN Gateways in the Remote Access clients' TTM file.

Important - You must edit the required configuration file on Remote Access clients to identify the MEP settings.

To define MEP topology:

1. On the Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Find `automatic_mep_topology`.

   If you do not see this parameter, add it manually as shown here:

   ```
   :automatic_mep_topology (
       :gateway (
           :map (
               :true (true)
               :false (false)
               :client_decide (client_decide)
           )
           :default (true)
       )
   )
   ```

3. Set the value of "`:default`" to:
   - `true` - For implicit configuration
   - `false` - For manual configuration
4. **For Manual MEP only** - Make sure that the value of "`:enable_gw_resolving`" is "`(true)`".
5. Save the changes in the file and exit the editor.
6. In SmartConsole, install the policy on the VPN Gateway.

First-to-Respond

When more than one Security Gateway lead to the same (overlapping) VPN domain, they are considered MEP by the remote peer. In a First-to-Respond configuration, the remote peer chooses the first Security Gateway that responds to the probing protocol. To configure First-to-Respond, define the part of the network that is shared by all the Security Gateways into one group. Then, assign that group as the VPN domain.

To configure Implicit First-to-Respond in SmartConsole:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the navigation tree, click **Network Management > VPN Domain**.
4. Select **User defined**.
5. Click the **[...]** button and select the applicable **Group** or **Network** object.

   Click **New** to create the required objects from this menu.
6. Click **OK**.
7. Repeat steps 2-6 for each Security Gateway object.

   Note - Make sure to use the same VPN domain for all Security Gateways.

To configure Manual First-to-Respond:

1. On the Management Server, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Make these changes:
   - In the "`:mep_mode ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(first_to_respond)`"
   - In the "`:ips_of_gws_in_mep ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(<Primary-IP-Address>&#<Secondary-IP-Address>&#<Tertiary-IP-Address>&#)`".

     Example:

     `:default(192.168.20.240&#192.168.20.250&#)`
3. Save the changes in the file and exit the editor.
4. In SmartConsole, install policy on the VPN Gateway.
5. Connect with a Remote Access client.

   The configuration is applied.

Primary-Backup

To configure Implicit Primary-Backup:

1. In SmartConsole, click **Menu** > **Global properties**.
2. From the left navigation tree, click **VPN > Advanced**.
3. Select **Enable Backup Gateway**.
4. Click **OK**.
5. In SmartConsole, install policy on the VPN Gateway.

To configure the backup Security Gateway settings:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the primary Security Gateway.
3. From the left navigation tree, click **IPsec VPN**.
4. At the bottom of the page, select **Use Backup Gateways**.
5. From the drop-down menu, select the backup Security Gateway.
6. Determine if the backup Security Gateway uses its own VPN domain.
7. To configure the backup Security Gateway without a VPN domain of its own:
    a. Double-click the Security Gateway and from the navigation tree click **Network Management > VPN Domain**.
    b. Click **Manually defined**.
    c. Click the field and select the group or network that contains only the backup Security Gateway.
    d. Click **OK** and publish the changes.
8. To configure the backup Security Gateway that has a VPN domain of its own:
    a. Make sure that the IP address of the backup Security Gateway is not included in the VPN domain of the primary Security Gateway.
    b. For each backup Security Gateway, define a VPN domain that does not overlap with the VPN domain of the other backup Security Gateways.
9. Configure IP pool NAT or Hide NAT to handle return packets (see *"Configuring Return Packets" on page 169*).

To configure Manual Primary-Backup:

1. On the Management Server, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Make these changes:
   - In the "`:mep_mode ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(primary_backup)`"
   - In the "`:ips_of_gws_in_mep ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(<Primary-IP-Address>&#<Secondary-IP-Address>&#<Tertiary-IP-Address>&#)`".

     Example:

     `:default(192.168.20.240&#192.168.20.250&#)`
3. Save the changes in the file and exit the editor.
4. In SmartConsole, install policy on the VPN Gateway.
5. Connect with a Remote Access client.

   The configuration is applied.

Load Distribution

When you enable this option, the load distribution is dynamic and the remote client randomly selects a Security Gateway.

To configure Implicit Load Distribution for Remote Access clients:

1. Click **Menu** > click **Global properties**.
2. From the left navigation tree, click **Remote Access > VPN Advanced**.
3. In the **Load distribution** section, select **Enable load distribution for Multiple Entry Point configurations (Remote Access connections)**.
4. Click **OK**.
5. Configure the same VPN domain in all Security Gateways.
6. Install policy on the Security Gateways.

To configure Manual Load Distribution:

1. On the Security Gateway, edit the `$FWDIR/conf/trac_client_1.ttm` file.
2. Make these changes:
   - In the "`:mep_mode ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(load_sharing)`"
   - In the "`:ips_of_gws_in_mep ()`" section, change

     from "`:default (client_decide)`"

     to "`:default(<Primary-IP-Address>&#<Secondary-IP-Address>&#<Tertiary-IP-Address>&#)`".

     Example:

     `:default(192.168.20.240&#192.168.20.250&#)`
3. Save the changes in the file and exit the editor.
4. In SmartConsole, install policy on the VPN Gateway.
5. Connect with a Remote Access client.

   The configuration is applied.

Configuring Return Packets

These are the configurations for clients that do not use Office Mode:

- IP pool NAT addresses that belong to the IP Pool NAT (see *"Configuring IP Pool NAT" on page 173*).
- Hide NAT (see *"Configuring NAT" on the next page*).

Configuring NAT

Configure NAT on the **NAT** page in the **Virtual System** window. Hide or Static NAT addresses configured in this manner are automatically forwarded to the Virtual Router to which the Virtual System is connected. Alternatively, you can manually add NAT routes on the **Topology** page in the **Virtual Router** window.

To configure NAT for a Virtual System on a VSX Gateway:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server / Target Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Virtual System object.
4	From the left navigation tree, click **NAT** > **Advanced**. The **Advanced** page opens.
5	Select **Add Automatic Address Translation**.
6	Select the **Translation method**. ■ **Hide** - Hide NAT only allows connections originating from the internal network. Internal hosts can access internal destinations, the Internet and other external networks. External sources cannot initiate a connection to internal network addresses. Select one of these options: • **Hide behind Gateway** - Hides the real address behind the VSX Gateway external interface address. This is equivalent to hiding behind the address `0.0.0.0` for IPv4, or `::` for IPv6. • **Hide behind IP Address** - Hides the real address behind a virtual IP address, which is a routable, public IP address that does not belongs to any real machine. ■ **Static** - Static NAT translates each private address to a corresponding public address. Enter the static IP address.
7	From the **Install on Gateway** list, select the VSX Gateway.
8	Click **OK**.
9	Install the Access Control Policy on this Virtual System.

To configure NAT for a Virtual System on a VSX Cluster:

Use case - Perform Hide NAT on traffic a Virtual System itself generates in a VSX Cluster, so that the Virtual System could connect to external resources (for example, update Anti-Bot signatures from the Check Point cloud).

Step	Instructions
1	Connect to the command line on each VSX Cluster Member.
2	Log in to the Expert mode.
3	Switch to the context of the applicable Virtual System: `[Expert@HostName:0]# vsenv <VSID>`
4	Get the Funny IP address of the applicable Virtual System interface, through which the applicable traffic goes out. **Note** - Funny IP address is the IP address that belongs to cluster's internal communications network (open the VSX Cluster object properties and go to the "Cluster Members" pane). Run one of these commands: ▪ `[Expert@HostName:<VSID>]# fw getifs` ▪ `[Expert@HostName:<VSID>]# \ifconfig` Write down the Funny IP address.
5	Connect with SmartConsole to the Security Management Server / Target Domain Management Server that manages this Virtual System.
6	From the left navigation panel, click **Gateways & Servers**.
7	Create a new **Node Host** object and assign to it the Funny IP address you wrote down in Step 4.
8	Create a new **Node Host** object and assign to it the NATed IP address.
9	From the left navigation panel, click **Security Policies**.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>10</td><td>In the Access Control > NAT policy, create the applicable NAT rule to hide the traffic from the Virtual System behind the NATed IP address:
<table>
<tr><th>Original Source</th><th>Original Destination</th><th>Original Services</th><th>Translated Source</th><th>Translated Destination</th><th>Translated Services</th><th>Install On</th><th>Comments</th></tr>
<tr><td>Node Host object with the Funny IP address of the Virtual System</td><td><code>Any</code></td><td><code>Any</code></td><td>Node Host object with the NATed IP address of the Virtual System</td><td><code>= Original</code></td><td><code>= Original</code></td><td><code>Policy Targets</code> or Virtual System object</td><td>Applicable text.
For example: Manual NAT rule for VSXcluster3-VS2 Funny IP</td></tr>
</table></td></tr>
<tr><td>11</td><td>Install the Access Control Policy on this Virtual System.</td></tr>
</table>

Configuring IP Pool NAT

For each Security Gateway, create a network object that represents the IP pool NAT addresses for that Security Gateway.

To configure NAT for an IP pool for Remote Access VPN in SmartConsole:

1. Configure the applicable global IP Pool NAT settings:
   a. Click **Menu** > **Global properties**.
   b. From the left navigation tree, click **NAT - Network Address Translation**.
   c. Select **Enable IP Pool NAT**.
   d. Configure the applicable logging settings:
      - **Address exhaustion track** - controls whether to generate a log if the IP Pool is exhausted.
      - **Address allocation and release track** - controls whether to generate a log for each allocation and release of an IP address from the IP Pool.
   e. Click **OK**.
   f. Publish the SmartConsole session
2. For **each** Security Gateway / Cluster that participates in Remote Access VPN, create an applicable object (**Network**, **Group**, or **Address Range**) that represents the IP pool of NAT addresses for that Security Gateway / Cluster.
   a. Click **Objects** > **Object Explorer** (or press CTRL+E).
   b. Create the new object.
   c. Configure the IP address(es).
   d. Click **OK**.
   e. Publish the SmartConsole session
3. Configure the applicable IP Pool NAT settings in **each** Security Gateway / Cluster object:
   a. From the left navigation panel, click **Gateways & Servers**.
   b. Double-click the Security Gateway / Cluster object, which performs the IP pool NAT translation.
   c. From the left navigation tree, click **NAT** > **IP Pool NAT**.
   d. Click **Allocate IP Addresses from**, and select the corresponding IP pool object.
   e. Select **Use IP Pool NAT for VPN client connections**.

f. **Optional:** Select **Use IP Pool NAT for Security Gateway to Security Gateway connections**.

g. Click **OK**.

4. Install the Access Control policy on all managed Security Gateways and Clusters.
5. Edit the routing table of each internal router, so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway.

Disabling MEP

1. Connect with SmartConsole to the Management Server.
2. Click **Menu** > **Global properties**.
3. From the left navigation tree, click **Advanced**.
4. Click the **Configure** button.
5. From the left navigation tree, click **SecuRemote/SecureClient** > **IKE/IPSec Settings**.
6. Select the option **desktop_disable_mep**.
7. Click **OK**.
8. Install the Access Control policy on all managed Security Gateways and Clusters.

Important:

- This change applies to all managed Security Gateways and Clusters.
- When MEP is disabled, MEP RDP probing and fail over are not performed. As a result, remote hosts connect to the Security Gateway defined without considering the MEP configuration. Remote Access clients use Visitor Mode instead of RDP to probe gateways.

Secondary Connect

Secondary Connect

With Secondary Connect, end users can access resources behind multiple VPN Gateways at the same time. Users log in once to a selected site and get access to resources behind different VPN Gateways. VPN Gateways create tunnels dynamically as needed, based on the destination of the traffic.

Secondary Connect is enabled by default.

Traffic flows directly from the end user's computer to the VPN Gateway, without site-to-site communication. The end user's computer and the VPN Gateway automatically create a VPN tunnel based on routing parameters from the network topology and destination server IP address.

End users can access all VPN Gateways that are in a Remote Access Community on the same Management Server or Domain.

Use Case: Your organization has Remote Access VPN Gateways in New York and Tokyo. You log in to a VPN site that connects you to the New York gateway. To access a resource behind the Tokyo gateway, your computer and the Tokyo gateway create a VPN tunnel.

In an environment with Secondary Connect, the client first connects to the **Primary** Security Gateway, and then through a secondary VPN to the **Secondary** Security Gateway.

Secondary Connect is compatible with legacy SecureClient settings.

For Security Gateway requirements for Secondary Connect, see sk65312.

Configuring Secondary Connect

Note - You must configure or disable Secondary connect for each Primary and Secondary VPN Gateway seperately.

Prerequistes

- All VPN Gateways that participate in Secondary Connect must have a server certificate that is signed by the Internal Certificate Authority.
- If you use Office Mode IP addresses, make sure that the Primary VPN Gateway and the Secondary VPN Gateway use different IP addresses, to prevent conflicts. The endpoint user's computer uses the Office Mode IP address issued to it by the first Security Gateway to access the secondary Security Gateway. If the endpoint user's computer does not cache authentication credentials, the endpoint user must enter credentials again to access resources on a different Security Gateway.

Note - On a VSX Gateway, this is the path for "*trac_client_1.ttm*":

/var/opt/CPsuite-R81.20/fw1/CTX/CTX<VSID>/conf/trac_client_1.ttm

" *CTX<VSID>*" represents the Virtual System context: "*CTX00001*" for VS1, "*CTX00002*" for VS2, and so on.

To disable Secondary Connect:

Note - Make sure the Security Gateway has a server certificate that is signed by the Internal Certificate Authority.

1. On each Security Gateway, edit the "*$FWDIR/conf/trac_client_1.ttm*" file.
2. Set the "`:default`" value of "`automatic_mep_topology`" to "`true`".
3. Find `enable_secondary_connect`. If you do not see this parameter, add it manually:

```
:enable_secondary_connect (
    :gateway (
        :map (
            :true (true)
            :false (false)
            :client_decide (client_decide)
        )
        :default (true)
    )
)
```

4. Change the "`:default`" value of "`enable_secondary_connect`" to "`false`".
5. Save the file.
6. Install the Access Control Policy.

To enable Secondary Connect:

1. Make sure the Security Gateway has a server certificate that is signed by the Internal Certificate Authority.
2. On each Security Gateway, edit the "`$FWDIR/conf/trac_client_1.ttm`" file.
3. Set the "`:default`" value of "`automatic_mep_topology`" to "`true`".
4. Find "{`enable_secondary_connect`". If you do not see this parameter, add it manually:

```
:enable_secondary_connect (
    :gateway (
        :map (
            :true (true)
            :false (false)
            :client_decide (client_decide)
        )
        :default (false)
    )
)
```

5. Change the "`:default`" value of "`enable_secondary_connect`" to "`true`".
6. Save the file.
7. Install the Access Control policy.

SAML Support for Remote Access VPN

You can configure Remote Access VPN to recognize identities from a cloud-based SAML Identity Provider.

Requirements

These are the required versions of products to use this feature with an R81.20 Management Server:

Product	Requirement
Management Server	R81.20
SmartConsole	R81.20
Security Gateway	■ Check Point Quantum R81.20 (Titan) ■ R81.10 with the R81.10 Jumbo Hotfix Accumulator, Take 9 or higher ■ R81 with the R81 Jumbo Hotfix Accumulator, Take 42 or higher ■ R80.40 with the R80.40 Jumbo Hotfix Accumulator: • Gateway mode - Take 114 or higher • VSX mode - Take 119 or higher **Important** - To use the feature with at least one iSecurity Gateway of version R81.10 and lower, you must download a script to the Management Server. See *"Step 4: Configure the Identity Provider as an Authentication Method" on page 183*.
Endpoint Security Client	■ Endpoint Security Client for Windows - version E84.70 build 986102705 or higher ■ Endpoint Security Client for macOS - version E85.30 or higher ■ Android Capsule VPN - requires R81.20 Jumbo Hotfix Accumulator take 43 or higher on the Security Gateway ■ Capsule Connect for iOS - requires R81.20 Jumbo Hotfix Accumulator take 43 or higher on the Security Gateway **Important** - To see the lowest Endpoint Security Client version that your Security Gateway supports, see the Release Notes document for the version of your Security Gateway > Chapter "Supported Clients and Agents".

Configuration

Basic SAML Configuration for Remote Access VPN

Step 1: Configure Remote Access VPN

Note - If the Security Gateway is already configured to support Remote Access VPN, make sure the configuration applies to SAML and then click **OK**. For more information about configuring Remote Access VPN, see *"Getting Started with Remote Access" on page 21*.

1. Use SmartConsole to connect to the Security Management Server / relevant Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the object of the relevant Security Gateway.
4. In **General Properties** > **Network Security** tab, select the **IPsec VPN** Software Blade.
5. From the left tree, click **IPsec VPN**.
6. In the section **This Security Gateway participates in the following VPN communities**, click **Add**.

   The **Add this Gateway to Community** window opens.
7. Select the relevant Remote Access VPN community.
8. Click **OK**.
9. From the left tree, expand the **VPN Clients** > click **Remote Access** > select **Support Visitor Mode**.
10. From the left tree, click **VPN Clients** > click **Office Mode** > select **Allow Office Mode** > select the relevant Office Mode Method.
11. Click **OK**.

    The Security Gateway object closes.
12. Open the Security Gateway object.
13. From the left tree, click **VPN Clients** > **SAML Portal Settings**:
    a. Make sure the **Main URL** field contains the fully qualified domain name (FQDN) of the Security Gateway.

b. Make sure the domain name ends with a DNS suffix registered to your organization.

Example:

```
https://MyGateway1.mycompany.com/saml-vpn
```

c. In the **Accessibility** section, select the relevant settings.

14. Click **OK**.

Step 2: Configure an Identity Provider Object

Important - Do this step for each Security Gateway that participates in Remote Access VPN

1. In SmartConsole, from the right navigation panel click **New** > **More** > **User/Identity** > **Identity Provider**.

   A **New Identity Provider** window opens.

2. In the **New Identity Provider** window, configure these settings:

   a. Enter the applicable name and comment at the top.

   b. In the **Gateway** field, select the Security Gateway to do the SAML authentication.

   c. In the **Service** field, select **Remote Access VPN**.

   SmartConsole populates these fields automatically:

   - **Identifier (Entity ID)** - the URL that uniquely identifies a service provider (in this configuration, the Security Gateway).
   - **Reply URL** - the URL to which the SAML assertions are sent.

3. Configure the SAML application on the Identity Provider's website.

   Important - Do **not** close the **New Identity Provider** window in SmartConsole while you configure the SAML application on the Identity Provider's website.

   Note - Depending on your Identity Provider, you may need to purchase a premium subscription to use the features necessary to configure SAML for Remote Access VPN.

   Follow the Identity Provider's instructions.

a. Copy the values of the Identifier **(Entity ID)** and **Reply URL** fields from the SmartConsole **New Identity Provider** window and enter them in the relevant fields on the Identity Provider's website.

   Notes:
   - The names of the target fields on the Identity Provider's website may differ for specific Identity Providers.
   - In Microsoft Azure, if you configure two or more Identity Provider objects for the same Security Gateway, make sure you paste all Entity IDs and all Reply URLs in the same Enterprise Application.

b. Make sure you configure the Identity Provider to send the authenticated username in the email format "`alias@domain`".

   Important - The primary email address for a user must be the same in the on-premises LDAP directory and in the user directory of the Identity Provider. This email address must be unique.

c. **Optional:** To receive the Identity Provider's groups where users are defined, configure the Identity Provider to send the group names as values of the attribute "`group attr`".

d. Before you complete the configuration, get this information from the Identity Provider:

   - **Entity ID** - A URL that uniquely identifies the application.
   - **Login URL** - A URL to use the application.
   - **Certificate** - For secure communication between the Security Gateway and the Identity Provider.

   Note - Some Identity Providers provide this information in a metadata XML file.

4. In the **New Identity Provider** window, in the **Data received from the SAML Identity Provider** section, select one of these options:

   - **Import the Metadata File**

     Click **Import From File** and select the metadata file from your Identity Provider.

- **Insert Manually**

  a. Enter the **Identifier (Entity ID)** and the **Login URL** you copied from the Identity Provider.

  b. Click **Import from File** and select the Certificate File from the Identity Provider.

  Note - The Identity Provider object in SmartConsole does not support the import of a RAW Certificate.

Step 3: Configure a Generic External User Profile Object

Note - Do this step only if you do **not** use an on-premises Active Directory (LDAP).

1. From the left navigation panel, click **Manage & Settings**.
2. From the left tree, click **Blades**.
3. In the **Mobile Access** section, click **Configure in SmartDashboard**.

   Legacy SmartDashboard opens.
4. In the lower left pane, click the **Users** tab.
5. In the **Users** tab, right-click on an empty space and select **New** > **External User Profile** > **Match all users**.
6. Configure the **External User Profile** properties:

   a. On the **General Properties** page:

   - In the **External User Profile name** field, make sure the default name is `generic*`.
   - In the **Expiration Date** field, enter the date.

   b. On the **Authentication** page, from the **Authentication Scheme** drop-down list, select **Undefined**.

   c. On the **Location**, **Time**, and **Encryption** pages, configure the relevant settings.

   d. Click **OK**.
7. From the top toolbar, click **Menu** (top left button) > **File** > **Update**.
8. Close Legacy SmartDashboard.
9. In SmartConsole, install the Access Control Policy.

Step 4: Configure the Identity Provider as an Authentication Method

1. From the left navigation panel, click **Gateways & Servers**.
2. Open the relevant Security Gateway object.
3. From the left tree, expand **VPN Clients** > click **Authentication**.
4. Clear the checkbox **Allow older clients to connect to this gateway**.
5. In the section **Multiple Authentication Clients Settings**, add a new object (click **Add** > click **New**) or edit an existing object (click **Edit**).

   The Remote Access client shows the authentication methods in the order shown in this section.

   For more information about Multiple Authentication Clients, see *"User and Client Authentication for Remote Access" on page 40*.
6. In the **Multiple Login Options** window:
   a. From the left tree, click **Login Option**.
      - In the **General Properties** section:
        - In the **Name** field, enter the name of the object in the database.
        - In the **Display Name** field, enter the name that appears in the **Multiple Authentication Clients Settings** table and Security Gateway portals.
      - In the **Authentication Methods** section:
        i. In the section **Authentication Factors**, select **Identity Provider**.
        ii. Click the "**+**" button > select the Identity Provider object.
        iii. Click **OK**.

   Note - For Remote Access Multiple Entry Point (MEP), you must configure the same **Login Option** on all Security Gateways that participate in MEP. Make sure to add all the Identity Provider objects (one per Security Gateway) to a dedicated **Login Option**.

b. From the left tree, click **User Directories**.

i. Select **Manual configuration**.

ii. Do **one** of these steps:

- If you use an on-premises Active Directory (LDAP):

  Select only **LDAP users** > select **All Gateway's Directories**.

  In the **Common lookup type** drop-down menu, select **Email Address (mail)**.

- If you do **not** use an on-premises Active Directory (LDAP), select only **External User profiles**.

c. Click **OK**.

7. In the Security Gateway object, click **OK**.
8. Publish the SmartConsole session.
9. Configure the required settings in the management database:

a. **Optional:** As a Best Practice, install the Access Control Policy. The Management Server creates a revision snapshot. You can revert to this revision snapshot if you make mistakes in manual database configurations or if you want to remove SAML Support for Remote Access VPN.

Refer to:

- sk108902 - Best Practices - Backup on Gaia OS.
- sk91400 - System Backup and Restore feature in Gaia.
- sk98153 - How to take a snapshot of Endpoint Security Management Server database.

b. Close **all** SmartConsole windows.

Note - To make sure there are no active sessions, run the "`cpstat mg`" command in the Expert mode on the Security Management Server / in the context of *each* Domain Management Server.

c. Connect with the *Database Tool (GuiDBEdit Tool)* to the Security Management Server / applicable Domain Management Server.

d. In the top left pane, go to **Table** > **Network Objects** > **network_objects**.

e. In the top right pane, select the Security Gateway object.

f. Press `CTRL + F` (or go to the **Search** menu > click **Find**) > paste **realms_for_blades** > select **Match whole string only** > click **Find Next**.

g. Below **realms_for_blades**, select the attribute **vpn** and examine only its inner attributes.

h. Below the **directory** attribute > the **fetch_options** attribute, look for these attributes:

- **do_generic_fetch**
- **do_internal_fetch**
- **do_ldap_fetch**
- **fetch_type**

If these attributes do **not** appear, then right-click the attribute **fetch_options** > click **Edit** > do not change anything > click **OK** (do **not** make any changes).

i. Configure the required settings:

- If you use an on-premises Active Directory (LDAP):
  i. Below the attribute **fetch_options** - If the current value of the attribute **do_generic_fetch** is not **false**, then right-click the attribute **do_generic_fetch** > click **Edit** > select the value **false** > click **OK**.
  ii. Below the attribute **directory** - Right-click the attribute **UserLoginAttr** > click **Edit** > select the value **mail** > click **OK**.
- If you do **not** use an on-premises Active Directory (LDAP):
  i. Below the attribute **fetch_options** - If the current value of the attribute **do_internal_fetch** is not **false**, then right-click the attribute **do_internal_fetch** > click **Edit** > select the value **false** > click **OK**.
  ii. Below the attribute **fetch_options** - If the current value of the attribute **do_ldap_fetch** is not **false**, then right-click the attribute **do_ldap_fetch** > click **Edit** > select the value **false** > click **OK**.

j. Right-click the attribute **fetch_type** > click **Edit** > select the value **fetch_options** > click **OK**.

k. Do steps (c)-(j) again for all applicable Security Gateways.

l. Save all changes (click the **File** menu > click **Save All**).

m. Close the Database Tool (GuiDBEdit Tool).

10. Use SmartConsole to connect to the Security Management Server / relevant Domain Management Server.

11. Open each Security Gateway object and examine the settings of each Software Blade that uses authentication - VPN, Mobile Access, and Identity Awareness.
    - Make sure to select the option **LDAP Users** only for Software Blades that use LDAP.
    - Make sure to select the option **External user profiles** only for Software Blades that do **not** use LDAP.
12. To use the feature with one or more Security Gateways of version R81.10 and lower, you must download a script to the Management Server.
    a. Download this script to your computer.
    b. Make sure that the Security Gateways have the necessary Jumbo Hotfix Accumulators installed. See *"Requirements" on page 178*.
    c. Copy the script from your computer to the Management Server.

    Note - If you copy a file over SCP to the Management Server, the user that connects must have the default shell `/bin/bash` in Gaia OS.

    d. Connect to the command line on the Management Server.
    e. Log in to the Expert mode.
    f. On a Multi-Domain Server, go to the main MDS context:

    ```
    mdsenv
    ```

    Note - On a Multi-Domain Server, if you do not want to enable SAML in all existing domains, document the UIDs of each domain. Run:
    `mgmt_cli show domains`

    g. Go to the directory where you uploaded the script.

h. Assign the execution permissions to the script. Run:

```
chmod u+x allow_VPN_RA_for_R8040_and_above_gateways_V2.sh
```

Run the script (the first argument must be "1"):

```
/allow_VPN_RA_for_R8040_and_above_gateways_V2.sh 1
```

Note - If the Management API is configured using a TCP port that is not the default port `443` (see output of the `api status` command), then do **one** of these:

- Add the port number as the second argument in the script: `./allow_VPN_RA_for_R8040_and_above_gateways.sh 1 <Apache Port Number>`
- Add '`--port <Apache Port Number>`' in the syntax of each `mgmt_cli` command in this script.

i. When the script prompts you to enter your user name and password, enter your SmartConsole credentials.

j. When the script prompts you to enter a Domain UID:

- To enable SAML on one of the domains of a Multi-Domain Server, enter the UID of the domain (to see the UID, run "`mgmt_cli show domains`").
- In other cases, or to enable SAML in all domains, leave the prompt empty and press `Enter`.

13. In SmartConsole, install the Access Control Policy on each Security Gateway.

Step 5: Install and Configure Remote Access VPN Clients

Note - This step is relevant only for Endpoint Security Client for Windows and Endpoint Security Client for macOS.

1. Install Remote Access VPN clients for Windows or for macOS. For more information, see sk172909.
2. **Optional:** Configure the Identity Provider browser mode. By default, the Windows client uses its embedded browser, and the macOS client uses the Safari browser to prove its identity in the Identity Provider's portal.

Configuring Remote Access VPN client for Windows to use the endpoint computer's default browser (example: Chrome):

Note - This configuration is supported starting from Remote Access VPN client for Windows version E87.30.

a. Log in to the Windows endpoint computer as an Administrator.

b. Open a plain text editor.

c. Open the *trac.defaults* file in the text editor.

File location on 32-bit Windows:

```
%ProgramFiles%\CheckPoint\Endpoint Connect\trac.defaults
```

File location on 64-bit Windows:

```
%ProgramFiles(x86)%\CheckPoint\Endpoint
Connect\trac.defaults
```

d. Change the value of the "**idp_browser_mode**" attribute from "**embedded**" to "**default_browser**".

e. Save the changes in the file and close the text editor.

f. Stop the Remote Access VPN client and start it again.

g. Open the Windows Command Prompt and run these commands:

i. `net stop TracSrvWrapper`

ii. `net start TracSrvWrapper`

Configuring Remote Access VPN client for macOS to use the endpoint computer's default browser (example: Chrome):

Note - This configuration is supported starting from Remote Access VPN client for macOS version E87.30.

a. Log in to the macOS endpoint computer as an Administrator.

b. Open a plain-text editor.

c. Open the *trac.defaults* file in the text editor. File location:

```
/Library/Application Support/Checkpoint/Endpoint
Security/Endpoint Connect/Trac.defaults
```

d. Change the value of the `idp_browser_mode` attribute from "**embedded**" to "**default_browser**".

e. Save the changes in the file and close the text editor.

f. Stop the Remote Access VPN client and start it again.

g. Open the Terminal and run these commands:

   i. `sudo launchctl stop com.checkpoint.epc.service`

   ii. `sudo launchctl start com.checkpoint.epc.service`

Configuring Remote Access VPN client for Windows to use the Internet Explorer browser:

a. Log in to the Windows endpoint computer as an Administrator.

b. Open a plain text editor.

c. Open the `trac.defaults` file in the text editor.

   - On 32-bit Windows:

     ```
     %ProgramFiles%\CheckPoint\Endpoint
     Connect\trac.defaults
     ```

   - On 64-bit Windows:

     ```
     %ProgramFiles(x86)%\CheckPoint\Endpoint
     Connect\trac.defaults
     ```

d. Change the value of the "**idp_browser_mode**" attribute from "**embedded**" to "**IE**".

e. Keep the changes in the file and close the text editor.

f. Stop the Remote Access VPN client and start it again. Open the Windows Command Prompt as an Administrator and run these commands:

   i. `net stop TracSrvWrapper`

   ii. `net start TracSrvWrapper`

Configuring the browser mode for a Windows endpoint computer in a configuration file on the Remote Access VPNGateway:

Starting from Remote Access VPN Client for Windows version E88.41, you can configure the browser mode for the endpoint computer in a configuration file on the Remote Access VPNGateway. The `idp_browser_mode` parameter in the *trac_client_1.ttm* file controls the browser mode. For more information, see sk75221.

Step 6: Configure the Group Authorization

Authorization is for these types of groups:

- Identity Provider groups - The groups the Identity Provider sends.
- Internal groups - The groups that are received from User Directories configured in SmartConsole (internal user groups or LDAP groups).

To configure the Identity Provider groups:

1. In the Identity Provider's interface, configure a SAML attribute:
   a. Define an optional attribute named **group_attr**.
   b. Configure the attribute according to the Identity Provider's requirements.
2. In SmartConsole, create an internal User Group object with this name (case-sensitive, spaces not supported):

   EXT_ID_<*Name_of_Role*>

   For example, for a role in the Identity Provider's interface with the name **my_group**, create an internal User Group object in SmartConsole with the name **EXT_ID_my_group.**

   Note - In Microsoft Azure, Identity Tags are not supported for Remote Access connections.

Identity Provider groups and Internal groups (example: LDAP) are used for authorization.

Authorization types: Remote Access VPN Community and Access Roles

- Remote Access VPN Community - Grants users access to Remote Access VPN. For more information, see *"User and Client Authentication for Remote Access" on page 40*.
- Access Roles (requires the Identity Awareness Software Blade) - Grants access to users according to policy rules and user identities. For more information, see the *R81.20 Identity Awareness Administration Guide* > Chapter "Configuring Identity Awareness" > Section "Creating Access Roles".

To apply authorization by Remote Access VPN, add the applicable group to the Remote Access VPN.

To apply authorization by Access Roles, add the applicable group to an Access Role in the Access Control Policy.

Advanced SAML Configuration for Remote Access VPN

Starting from R81.20 Jumbo Hotfix Accumulator Take 89, you can configure these advanced SAML features:

- Request Signing: Verifies authenticity of SAML requests.
- Assertion Decryption: Protects confidentiality of user attributes.
- Forced Re-authentication: Enables mandatory login for each session.

For configuration instructions, refer to sk182042.

Known Limitations

- This feature supports only IPsec VPN clients.
- All Remote Access VPN users and endpoint computers must be configured in an Identity Provider for authentication. This applies to managed endpoint computers and non-managed endpoint computers.
- In the SAML-based authentication flow, the Identity Provider issues the SAML ticket after one or multiple verification activities.
- SAML authentication cannot be configured with more authentication factors in the same login option. The **Machine Certificate Authentication** option is supported. To use Multiple Factor Authentication, configure the external Identity Provider to have multiple verification steps. The complexity and number of verification activities depends on the configuration of the Identity Provider.
- For Windows and macOS endpoint computers or appliances (managed and non-managed), Check Point Remote Access VPN client must be installed.
- In the security Rule Base, you can only enforce identities received from remote access SAML authentication at the VPN termination point.
- Connecting from a CLI to a realm with Identity Provider is not supported.
- Remote Access VPN client for ATMs is not supported.
- Secure Domain Logon (SDL) with Identity Provider is not supported.
- Identity Tags are not supported for Remote Access VPN connections.

Dynamic Split Tunneling for SaaS Using Updatable Objects

To decrease load on a VPN Gateway, you can exclude traffic for SaaS from your Remote Access VPN Tunnel in Hub Mode.

Chain of Events:

1. Administrator configures which services to exclude from the Remote Access VPN Tunnel.
2. The VPN Gateway dynamically fetches the IP addresses of configured services from the Internet, and sends this information to Remote Access VPN clients.
3. Remote Access VPN clients exclude traffic for these services from the Remote Access VPN Tunnel.

Prerequisites

This feature requires:

- Security Management Server - version R81.20 or higher
- Security Gateway - version R81.20 or higher
- Remote Access VPN clients for Windows OS - version E86.20 or higher.

Configuration

To exclude SaaS services from a Remote Access VPN tunnel in Hub mode:

Step 1 - Configure the settings in SmartConsole

a. Connect with SmartConsole to the Security Management Server / Domain Management Server that manages this Security Gateway / Cluster.

b. Configure Remote Access VPN.

See *"Getting Started with Remote Access" on page 21*.

c. Configure Hub Mode.

See *"Hub Mode (VPN Routing for Remote Clients)" on page 141*

d. Configure a dedicated encryption domain for Remote Access VPN.

See *"Advanced VPN Domain Configuration" on page 25*

e. From the left navigation panel, click **Gateways & Servers**.

f. Open the Security Gateway / Cluster object:

   i. In the left navigation tree, click **Network Management** > **VPN Domain**.

   ii. Select **User defined**.

   iii. In the **Encryption Domain** field, select the **Group** object you configured for the Remote Access VPN community.

   iv. In this **Group** object, add a **Simple Group** object with a name that begins with:

   ```
   exclusions_
   ```

   Important - Dynamic Split Tunneling uses a Simple Group object, which can include only the following object types: Updatable, Dynamic, or Domain. However, a Simple Group object with a name starting with **exclusions_** must not contain nested groups.

   v. Add the applicable object for your SaaS to this simple group.

   vi. Click **OK**.

g. In SmartConsole, install the Access Control Policy on the Security Gateway / Cluster object.

Step 2 - Configure the required settings in the Remote Access VPN client

To enable the feature on the Remote Access VPN client, do **one** of these:

- **Edit the '$FWDIR/conf/trac_client_1.ttm' file on the Security Gateway**

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

  b. Log in to the Expert mode.

  c. Back up the current *$FWDIR/conf/trac_client_1.ttm* file:

  ```
  cp -v $FWDIR/conf/trac_client_1.ttm{,_BKP}
  ```

  d. Edit the current *$FWDIR/conf/trac_client_1.ttm* file:

  ```
  vi $FWDIR/conf/trac_client_1.ttm
  ```

  e. In the main parameter "*trac_client_1*", add the new parameter "*split_tunnel*" as appears below:

  ```
  (
      :trac_client_1 (
          :split_tunnel (
              :gateway (
                  :default (true)
              )
          )

          :<other_parameters> (
          ... ...
          )
      )
  )
  ```

  f. Save the changes in the file and exit the editor.

  g. In SmartConsole, install the Access Control policy on the Security Gateway / Cluster Object.

  The feature is available on the VPN client after the administrator makes a new connection between the Security Gateway and a Remote Access VPN tunnel.

- **Edit the 'trac.defaults' file on the VPN client (located in the VPN client's installation folder)**

Note - For information on how to prepare an installation package with the VPN Configuration Utility, see sk122574.

a. Go to the VPN client installation directory:

Operating System	Default Path
Windows OS 32-bit	One of these: • `%ProgramFiles%\CheckPoint\Endpoint Security\Endpoint Connect\` • `%ProgramFiles%\CheckPoint\Endpoint Connect\`
Windows OS 64-bit	One of these: • `%ProgramFiles(x86)%\CheckPoint\Endpoint Security\Endpoint Connect\` • `%ProgramFiles(x86)%\CheckPoint\Endpoint Connect\`
macOS	`/Library/Application Support/Checkpoint/Endpoint Security/Endpoint Connect/`

b. Create a copy of the current *trac.defaults* file.

c. Edit the current *trac.defaults* file with an advanced plain-text editor (such as Notepad++, UltraEdit, PSPad).

d. Configure the value of the "`split_tunnel`" parameter to "`true`":

```
split_tunnel          STRING          true          GW_USER
  0
```

Important - Do **not** change other predefined strings in this line - "`STRING`", "`GW_USER`", and "`0`".

e. Save your changes and close the file.

f. Restart the computer with the VPN client installed.

The VPN client starts to exclude SaaS services the next time it creates a new Remote Access VPN tunnel to the Security Gateway.

strongSwan Client Support

Remote Access client with IKEv2 has the ability to use the strongSwan Client.

strongSwan Client Installation

For strongSwan client installation, follow the instructions in the strongSwan documentation.

strongSwan Client Configuration

The configuration contains these sections:

Section	Description
Certificate	This section describes: ■ The "`ipsec.conf`" file ■ The "`ipsec.secrets`" file ■ The "`strongswan.conf`" file ■ The "`cacerts`" folder ■ The "`certs`" folder ■ The "`private`" folder
Username and Password	This section describes: ■ The "`ipsec.conf`" file ■ The "`ipsec.secrets`" file ■ The "`strongswan.conf`" file
Features Configuration	This section describes: ■ The "`pfs`" feature ■ The "`reauth`" feature ■ The "`rekey`" feature ■ The strict use of IKE and ESP methods ■ Dead Peer Detection (DPD)
Special Configuration	This section describes: ■ How to use an encrypted private key to connect ■ The encryption domain

Certificate

1. **ipsec.conf file**

   File:

   `/etc/strongswan/ipsec.conf`

   Description:

   In this file, you configure how the strongSwan client communicates with Check Point Security Gateway through certificate authentication.

   The contact of the file:

   - `config setup`
     - `charondebug="ike 4, knl 4, cfg 3, chd 4"`
   - `conn CONNECTION_NAME`
     - `type=tunnel`

       By default, this is a tunnel.
     - `leftfirewall=yes`
     - `authby=pubkey`
     - `keyexchange=ikev2`
     - `left=<`*`CLIENT_EXTERNAL_IP_ADDRESS`*`>`

       By default, this is `%any`.

       The value `%any` for the local endpoint signifies an address that fills (by automatic keying) during negotiation.

       If the local peer initiates the connection setup, routing table queries determine the correct local IP address.
     - `leftsourceip=%config`

       Makes the peer ask for virtual IP (Office Mode IP), DNS, and other settings.
     - `right=<`*`GW_EXTERNAL_IP_ADDRESS`*`>`
     - `rightid=<`*`GW_EXTERNAL_IP_ADDRESS`*`>`

- `leftcert=<CLIENT_CERTIFICATE_FILE>`

  Example: `StrongSwanPublicCert.cer`

- `rightsubnet=ENCRYPTION_DOMAIN_WE_WANT_TO_CONNECT`

  If you want to connect to the entire encryption domain, use `0.0.0.0/0`.

- `ike=<IKE_METHODS_AS_CONFIGURED_ON_THE_GW>`

  Example: `aes256-sha1-modp1024`

  You must configure the Security Gateway to support those methods.

- `esp=<IPSEC_METHODS_AS_CONFIGURED_ON_THE_GW>`

  Example: `3des-sha1`

  You must edit the Gateway to support those methods.

- `ikelifetime=<TIME_WHICH_AFTER_THE_IKE_SA_IS_NOT_VALID>`

  Example: `24h`

  Absolute time after which an IKE SA expires.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `lifetime=<TIME_WHICH_AFTER_THE_IPSEC_SA_IS_NOT_VALID>`

  Example: `1h`

  Absolute time after which an IPsec SA expires.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `reauth=yes`

- `rekey=yes`

- `margintime=<TIME_TO_START_REKEY_OR_REAUTH_BEFORE_EXPIRY>`

  Example `1M`

  Time before SA expiry the rekeying should start.

  Example: If the time of `lifetime` is `1h` and `margintime` is `1`, then `1m` before the `1h` ends, Security Gateway starts the rekey process.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `rekeyfuzz=<RANDOM_TIME_PERCENTAGE_FOR_REKEY_AND_REAUTH>`

  Example: `50%`

  The percentage by which `margintime` randomly increases (may exceed 100%).

  You can disable randomization with `rekeyfuzz=0%`.

  This is the formula of the rekytime of IPsec SAs and IKE SA:

  ```
  rekeytime = lifetime - (margintime + random(0, margintime * rekeyfuzz))
  ```

- `auto=add`

- `dpdaction=restart`

  Restart immediately triggers an attempt to re-negotiate the connection after no response from the Gateway.

- `dpddelay=<TIME_TO_SEND_R_U_THERE_MESSAGE>`

  Example: `30s`

  Defines the period time interval with which `R_U_THERE` messages and `INFORMATIONAL` exchanges go to the peer.

  These only go if no other traffic is received.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `dpdtimeout=<TIMEOUT_INTERVAL_TO_DELETE_THE_CONNECTION>`

  Example: `60s`

  Defines the `timeout` interval, after which all connections to a peer delete in case of inactivity.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

Advanced configuration and explanation:

See the strongSwan documentation in the section for General Connection Parameters.

2. **ipsec.secrets file**

   File:

   `/etc/strongswan/ipsec.secrets`

   Description:

   It this file, you configure the strongSwan private key.

   The contact of the file:

   `THE_SITE_IP_ADDRESS (OPTIONAL) : RSA CLIENT_CERT_KEY_FILE`

   Example: `StrongSwanPrivateKey.pem`

3. **strongswan.conf file**

   File:

   `/etc/strongswan/strongswan.conf`

   Description:

   The strongSwan Configuration file adds more plugins, sends the vendor ID, and resolves the DNS.

   The contact of the file:

```
charon {
  load_modular = yes
  send_vendor_id = yes
  plugins {
    include strongswan.d/charon
    resolve {
      file = /etc/resolv.conf
    }
  }
}
include strongswan.d/*.conf
```

   Advanced configuration and explanation:

   See the strongSwan documentation in the section for the `strongswan.conf` file.

4. **certs folder**

   Directory Path:

   `/etc/strongswan/ipsec.d/certs`

   File:

   `StrongSwanPublicCert.cer`

   or

   `StrongSwanPublicCert.pem`

   Description:

   This folder contains all the client public certificates.

5. **private folder**

   Directory Path:

   `/etc/strongswan/ipsec.d/private`

   File:

   `StrongSwanPrivateKey.pem`

   Description:

   This folder contains all the client private certificates.

Username and Password

1. **ipsec.conf file**

   File:

   `/etc/strongswan/ipsec.conf`

   Description:

   In this file, you configure how the strongSwan client communicates with Check Point Security Gateway through username and password authentication.

   The contact of the file:

   - `config setup`
     - `charondebug="ike 4, knl 4, cfg 3, chd 4"`
   - `conn CONNECTION_NAME`
     - `type=tunnel`

       This is the default.
     - `leftfirewall=yes`
     - `rightauth=pubkey`
     - `leftauth=eap-gtc`
     - `keyexchange=ikev2`
     - `eap_identity=<`*`USERNAME`*`>`
     - `left=<`*`CLIENT_EXTERNAL_IP_ADDRESS`*`>`

       This configuration is not a necessity.

       By default, it is `%any`. The value `%any` for the local endpoint signifies an address that fills in (by automatic keying) during negotiation.

       If the local peer initiates the connection setup, routing table queries determine the correct local IP address.

- `leftsourceip=%config`

  Makes the peer ask for the virtual IP (Office Mode IP), DNS, and other settings.

- `right=<GW_EXTERNAL_IP_ADDRESS>`
- `rightid=<GW_EXTERNAL_IP_ADDRESS>`
- `rightsubnet=<ENCRYPTION_DOMAIN_WE_WANT_TO_CONNECT>`

  If you want to connect to the entire encryption domain, use `0.0.0.0/0`.

- `ike=<IKE_METHODS_AS_CONFIGURED_ON_THE_GW>`

  Example: `aes256-sha1-modp1024`

  You must configure the Security Gateway to support those methods.

- `esp=<IPSEC_METHODS_AS_CONFIGURED_ON_THE_GW>`

  Example: `3des-sha1`

  You must configure the Security Gateway to support those methods.

- `ikelifetime=<TIME_WHICH_AFTER_THE_IKE_SA_IS_NOT_VALID>`

  Example: `24h`

  Absolute time after which an IKE SA expires.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `lifetime=<TIME_WHICH_AFTER_THE_IPSEC_SA_IS_NOT_VALID>`

  Example: `1h`

  Absolute time after which an IPsec SA expires.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `reauth=yes`
- `rekey=yes`

- `margintime=<TIME_TO_START_REKEY_OR_REAUTH_BEFORE>`

  Example `1M`

  If the time of 'lifetime' is `1h` and margintime is `1m`, then `1m` before the `1h` ends, Security Gateway starts the rekey process.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `rekeyfuzz=<RANDOM_TIME_PERCENTAGE_FOR_REKEY_AND_REAUTH>`

  Example: `50%`

  The percentage by which margintime randomly increases. It may exceed 100%.

  You may disable randomization with `rekeyfuzz=0%`.

  This is the formula of the rekytime of IPsec SAs and IKE SA:

  ```
  rekeytime = lifetime - (margintime + random(0,
  margintime * rekeyfuzz))
  ```

- `auto=add`

- `dpdaction=restart`

  A restart immediately triggers an attempt to re-negotiate the connection after no response from the Gateway.

- `dpddelay=<TIME_TO_SEND_R_U_THERE_MESSAGE>`

  Example: `30s`

  This defines the period time interval with which "`R_U_THERE`" messages and "`INFORMATIONAL`" exchanges go to the peer.

  These go if the peer receives no other traffic.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

- `dpdtimeout=<TIMEOUT_INTERVAL_TO_DELETE_THE_CONNECTION>`

  Example: `60s`

  This defines the `timeout` interval, after which all connections to a peer delete in case of inactivity.

  It can be hours (`h`), minutes (`m`), and seconds (`s`).

Advanced configuration and explanation:

See the strongSwan documentation in the ipsec.conf: conn section.

2. **ipsec.secrets file**

   File:

   ```
   /etc/strongswan/ipsec.secrets
   ```

   Description:

   In this file, you configure the strongSwan password.

   The contact of the file:

   ```
   USERNAME : EAP "PASSWORD"
   ```

   Note - We do **not** recommend the use of an authentication method that stores a user's clear passwords in the file.

3. **strongswan.conf file**

   File:

   `/etc/strongswan/strongswan.conf`

   Description:

   The strongSwan Configuration file adds more plugins, sends the vendor ID, and resolves the DNS.

   The contact of the file:

```
charon {
  load_modular = yes
  send_vendor_id = yes
  plugins {
    include strongswan.d/charon
    resolve {
      file = /etc/resolv.conf
    }
  }
}
include strongswan.d/*.conf
```

   Advanced configuration and explanation:

   See the strongSwan documentation in the strongswan.conf section.

4. **cacerts folder**

   Directory Path:

   `/etc/strongswan/ipsec.d/cacerts`

   File:

   `internal_ca.crt`

   Description:

   The internal CA file of all the Gateway, LDAP, and RADIUS servers are the Trusted CA for the client to authenticate the servers for each connection.

You can find these settings in SmartConsole in **Trusted CA**.

Features Configuration

- `pfs`
  - You must add the "`esp=`" section with the proper DH group.
  - Example: `esp=3des-sha1-modp1024`
- `reauth`
  - `ikelifetime=<`*`TIME_WHICH_AFTER_THE_IKE_SA_IS_NOT_VALID`*`> , reauth=yes`
- `rekey`
  - `lifetime=<`*`TIME_WHICH_AFTER_THE_IPSEC_SA_IS_NOT_VALID`*`> , rekey=yes`
- Strict use of IKE and ESP methods
  - You must add the "`ike=`" or "`esp=`", or both at the end.
  - Example: `ike=aes256-sha1-modp1024! , esp=3des-sha1!`
- Dead Peer Detection

  You must add the "`dpdaction=restart`" in the "`ipsec.conf`" file to check the liveliness of the IPsec peer and to keep it alive.

Special Configuration

- **How to use an encrypted private key to connect**
  - In the `ipsec.secrets` file, you must add the passphrase for the private key.
  - **File:**

    `/etc/strongswan/ipsec.secrets`

    Description:

    In this file, you configure the strongSwan password.

    The contact of the file:

    Example: `<THE_SITE_IP_ADDRESS> : <RSA CLIENT_CERT_KEY_FILE> StrongSwanPrivateKey.pem "<PASSPHRASE_FOR_THE_PRIVATE_KEY>" Source`

- **Encryption Domain**
  - In some scenarios, if you change the encryption domain with an addition or a removal of a network, you must modify the client "`ipsec.conf`" file.
  - Three ways to configure.

    Note - Two of these require edits on the client side after changes (not recommended).

    - Uses the universal IP to connect to the entire Encryption Domain without client side edits.
    - Specifies one specific network for the connection and requires client side modification.
    - Specifies several networks for the connections and requires client side modification.

- In this setup, three networks are on the encryption domain.

  - Uses the universal IP to connect to the entire Encryption Domain.
    - Configure the "rightsubnet" as a universal IP which is 0.0.0.0/0.

      In this configuration, there are routes to the entire Encryption Domain.
    - If you add or remove any network, it requires no modification on the client side.

      Note - This choice is highly recommended.
  - Specifies one specific network for the connection.
    - Choose one specific network, such as eth0 at `10.10.1.0/24`.

      Configure the "rightsubnet" to be "`10.10.1.0/24`" for one tunnel to this network.
    - **Note** - If a change in the Encryption Domain now has the network as `10.10.10.0/24`, you must change it on the client side.

- Specifies several networks for the connections.
  - If you do not want to connect to the Encryption Domain or to one network, you can connect to two or more networks.

    Configure these with the "`also`" macro, which includes connection definitions defined in the ipsec.conf file and add the change to this connection.
  - Example:

    ```
    conn conn_to_eth 0

    //full configuration with
    "rightsubnet=10.10.10.0/24"

    conn coon_to_eth 1

    rightsubnet=192.168.1.0/24

    also=coon_to_eth 0
    ```
  - **Notes:**
    - You must still run the `up` command to establish this connection. If there are any changes in the Encryption Domain that relate to these networks, you must reconfigure the client side.
    - If a network is not accessible to you, the connection fails.

Debian and Ubuntu Special Configuration

To use EAP authentication on Debian and Ubuntu machines, you must run these commands to install the required plugins before a strongSwan restart:

- `sudo apt-get install libstrongswan-extra-plugins`
- `sudo apt-get install libcharon-extra-plugins`

Useful strongSwan Commands

On CentOS and Fedora, the primary command is: `strongswan`.

On Ubuntu and Debian, the primary command is: `ipsec`.

- "`strongswan restart`", or "`ipsec restart`"

  Terminates all IPsec connections, stops the IKE daemon "`charon`", parses the "`ipsec.conf`" file, and starts the IKE daemon "`charon`".

- "`strongswan rereadsecrets`", or "`ipsec rereadsecrets`"

  Reads all secrets defined in the `ipsec.secrets` file and updates them.

- "`strongswan update`", or "`ipsec update`"

  Determines any changes in the "`ipsec.conf`" file and updates the configuration on the active IKE daemon "`charon`".

  Configuration changes do not affect established connections.

  Note - To use changes in the "`ipsec.conf`" or "`ipsec.secrets`" file, you must run the command with the "`rereadsecrets`" options (not with the "`update`" option). For full command syntax, go to the `strongswan.org` web site (see the `IpsecCommand` section).

How to Convert a P12 File into a Private Key and Public Cert

- **XCA Tool**
  - Use the XCA tool.
  - Download it from the hohnstaedt.de site in the XCA directory.
- **OpenSSL Commands**
  - `openssl pkcs12 -in <P12_CERTIFICATE>.p12 -clcerts -nokeys -out <EXTRACTED_CERTIFICATE>.crt`
  - `openssl pkcs12 -in <P12_CERTIFICATE>.p12 -nocerts -out <EXTRACTED_PRIVATE>.key`

Known Limitations

- **Simultaneous Login**

  Two simultaneous connections for the same user are not supported. Each connection must be an individual user or the first connection disconnects.

- **Office Mode with Multiple External Interfaces**

  Enhancements for Gateways with multiple external interfaces require NAT-T usage on the client side.

  Enforcement requires the NAT-T environment, or the configuration of "`forceencaps = yes`" in the "`ipsec.conf`" file.

- **Back Connection**

  Connections from the encryption domain to the assigned IP address of the client by the Security Gateway are not supported.

- **Realms**

  Realms are not supported. The client uses “Legacy authentication”.

- **Machine Authentication**

  Machine authentication is not supported.

- **Two-Factor Authentication**

  Two-Factor Authentication is not supported.

- **Encryption Domain**

  Encryption domain changes must deploy on the client side with configuration file changes in some scenarios.

- **Advanced Remote Access features are not supported**

  - Certificate enrollment.
  - Link Selection.
  - Location Awareness.
  - Multiple Entry Point (MEP).
  - Secondary Connect.
  - Secure Configuration Verification (SCV).
  - Visitor Mode.

- **IPv6**

IPv6 is not supported.

- **Certificate Usage**

  The customer deploys the certificates.

- **Certificate Authentication**

  Certificate authentication with ICA is only supported without a CRL check.

Resolving Connectivity Issues

While there are a few connectivity issues regarding VPN between Security Gateways, remote access clients present a special challenge. Remote clients are, by their nature, mobile. During the morning they may be located within the network of a partner company, the following evening connected to a hotel LAN or behind some type of enforcement or NATing device. Under these conditions, a number of connectivity issues can arise:

- Issues involving NAT devices that do not support fragmentation.
- Issues involving service/port filtering on the enforcement device

Check Point Solution for Connectivity Issues

Check Point resolves NAT related connectivity issues with a number of features:

- IKE over TCP
- Small IKE phase II proposals
- UDP encapsulation
- IPsec Path Maximum Transmission Unit (IPsec PMTU)

Check Point resolves port filtering issues with **Visitor Mode** (the formal name for this is *TCP Tunneling*).

Other Connectivity Issues

Other connectivity issues can arise, for example when a remote client receives an IP address that matches an IP on the internal network. Routing issues of this type are resolved using Office Mode (see *"Office Mode" on page 64*).

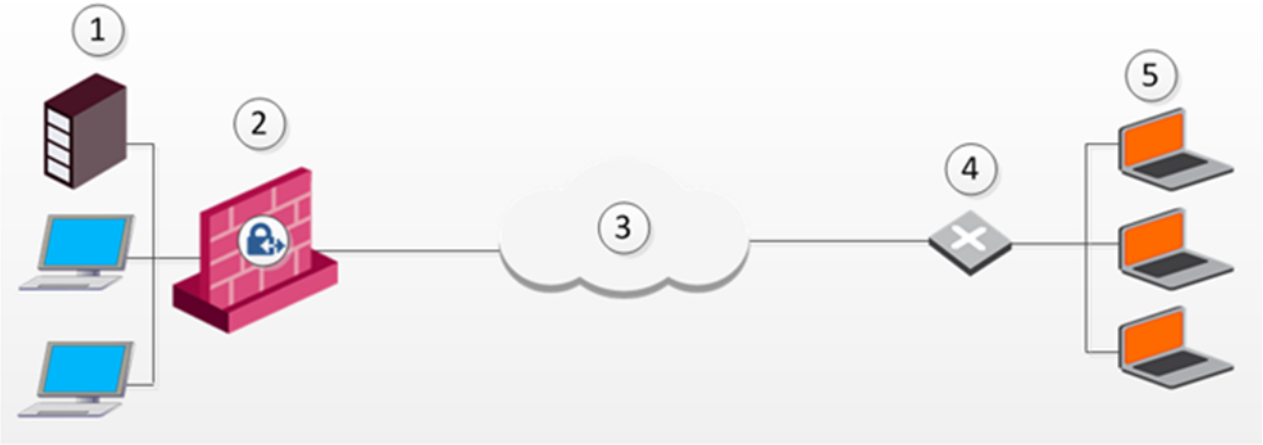
Other issues, such as Domain Name Resolution involving DNS servers found on an internal network protected by a Security Gateway, are resolved with Split DNS (see *"Split DNS" on page 158*).

Overcoming NAT Related Issues

NAT related issues arise with *hide* NAT devices that do not support packet fragmentation.

When a remote access client attempts to create a VPN tunnel with its peer Security Gateway, the IKE or IPsec packets may be larger than the Maximum Transmission Unit (MTU) value. If the resulting packets *are* greater than the MTU, the packets are fragmented at the Data Link layer of the Operating System's TCP/IP stack.

Problems arise when the remote access client is behind a hide NAT device that does not support this kind of packet fragmentation:



Item	Description
1	Server
2	Security Gateway
3	Internet
4	Router
5	Remote Client

Hide NAT not only changes the IP header but also the port information contained in the UDP header. For example, if the UDP packet is too long, the remote client fragments the packet. The first fragment consists of the IP header plus the UDP header and some portion of the data. The second fragment consists of only the IP header and the second data fragment. The NATing device does not know how to wait for all the fragments, reassemble and NAT them.

When the first fragment arrives, the NAT device successfully translates the address information in the IP header, and port information in the UDP header and forwards the packet. When the second fragment arrives, the NATing device cannot translate the port information because the second packet does not contain a UDP header; the packet is dropped. The IKE negotiation fails.

During IKE phase I

To understand why large UDP packets arise, we need to take a closer look at the first phase of IKE. During IKE phase I, the remote access client and Security Gateway attempt to authenticate each other. One way of authenticating is through the use of certificates. If the certificate or Certificate Revocation List (CRL) is long, large UDP packets result, which are then fragmented by the operating system of the remote client.

Note - If the VPN peers authenticate each other using pre-shared secrets, large UDP packets are not created; however, certificates are more secure, and thus recommended.

IKE Over TCP

IKE over TCP solves the problem of large UDP packets created during IKE phase I. The IKE negotiation is performed using TCP packets. TCP packets are not fragmented; in the IP header of a TCP packet, the DF flag ("do not fragment") is turned on. A full TCP session is opened between the peers for the IKE negotiation during phase I.

During IKE phase II

A remote access client does not have a policy regarding methods of encryption and integrity. Remote access clients negotiate methods for encryption and integrity via a series of proposals, and need to negotiate *all* possible combinations with the Security Gateway. This can lead to large UDP packets which are once again fragmented by the remote client's OS before sending. The NAT device in front of the remote client drops the packet that has no UDP header (containing port information). Again, the IKE negotiation fails.

Why not use IKE over TCP again, as in phase I?

IKE over TCP solves the fragmentation problem of long packets, but in phase II there are times when the Security Gateway needs to *initiate* the connection to the remote client. (Only the remote client initiates phase I, but either side can identify the need for a phase II renewal of keys; if the Security Gateway identifies the need, the Security Gateway initiates the connection.)

If the Security Gateway initiates the connection, the Security Gateway knows the IP address of the NATing device, but cannot supply a port number that translates to the remote client *behind* the NATing device. (The port number used during previous connections is only temporary, and can quickly change.) The NATing device cannot forward the connection correctly for the remote client; the connection initiated by the Security Gateway fails.

It is possible to use IKE over TCP, but this demands a TCP connection to be always open; the open session reserves the socket on the Security Gateway, taking up valuable system resources. The more reasonable solution is to keep open the port on the NATing device by sending UDP "keep alive" packets to the Security Gateway, and then performing IKE phase II in the usual way. However, there is still a need to shorten the UDP packets to prevent possible fragmentation.

Small IKE Phase II Proposals

Both Security Gateway and remote peer start the IKE negotiation by proposing a small number of methods for encryption and integrity. The more common methods are included in the small proposals.

If proposals match between the remote client and the Security Gateway, the proposed methods are used; if no match is found, a greater number of proposals are made. Usually a match is found with the small proposals, and fragmentation is no longer an issue. However, there are cases where a match is not found, and a larger number of proposals need to be made. (This will most likely happen in instances where the remote Security Gateway uses AES-128 for encryption, and AES-128 is not included in the small proposals.)

A greater number of proposals can result in larger UDP packets. These larger packets are once again fragmented at the Data Link Layer of the TCP/IP stack on the client, and then discarded by the hide NAT device that does not support fragmentation. In the case of AES-128, this method of encryption can be included in the small proposals by defining AES-128 as the preferred method.

During IPsec

NAT Traversal (UDP Encapsulation for Firewalls and Proxies)

Having successfully negotiated IKE phases I and II, we move into the IPsec stage. Data payloads encrypted with AES and SHA, for example, are placed within an IPsec packet. However, this IPsec packet no longer contains a TCP or UDP header. A hide NAT device needs to translate the port information inside the header. The TCP/UDP header has been encrypted along with the data payload and can no longer be read by the NATing device.

A port number needs to be added. UDP Encapsulation is a process that adds a special UDP header that contains readable port information to the IPsec packet.

IPsec Path Maximum Transmission Units

IPsec Path MTU is a way of dealing with IPsec packet fragmentation. The Data Link layer imposes an upper limit on the size of the packets that can be sent across the physical network, **the Maximum Transmission Unit**, or MTU. Before sending a packet, the TCP/IP stack of the operating system queries the local interface to obtain its MTU. The IP layer of the TCP/IP stack compares the MTU of the local interface with the size of the packet and fragments the packet if necessary.

When a remote client is communicating across multiple routers with a Security Gateway, it is the smallest MTU of *all* the routers that is important; this is the *path MTU* (PMTU), and for remote access clients there is a special *IPsec PMTU* discovery mechanism to prevent the OS of the client from fragmenting the IPsec packet if the IPsec packet is too large.

However, the PMTU between the remote client and the Security Gateway will not remain constant, since routing across the Internet is dynamic. The route from Security Gateway to client may not be the same in both directions, hence each direction may have its own PMTU. VPN handles this in two ways:

- Active IPsec PMTU
- Passive IPsec PMTU

Active IPsec PMTU

After IKE phase II but before the IPsec stage, the remote access client sends special discovery IPsec packets of various sizes to the Security Gateway. The DF (do not fragment) bit on the packet is set. If a packet is longer than any router's MTU, the router drops the packet and sends an ICMP error message to the remote client. From the largest packet not fragmented, the remote client resolves an appropriate PMTU. This PMTU is not conveyed directly to the OS. Unknown to the operating system, during the TCP three-way handshake, the Maximum Segment Size (MSS) on the SYN and SYN-ACK packets are changed to reflect the PMTU. This is known as *Active IPsec PMTU*.

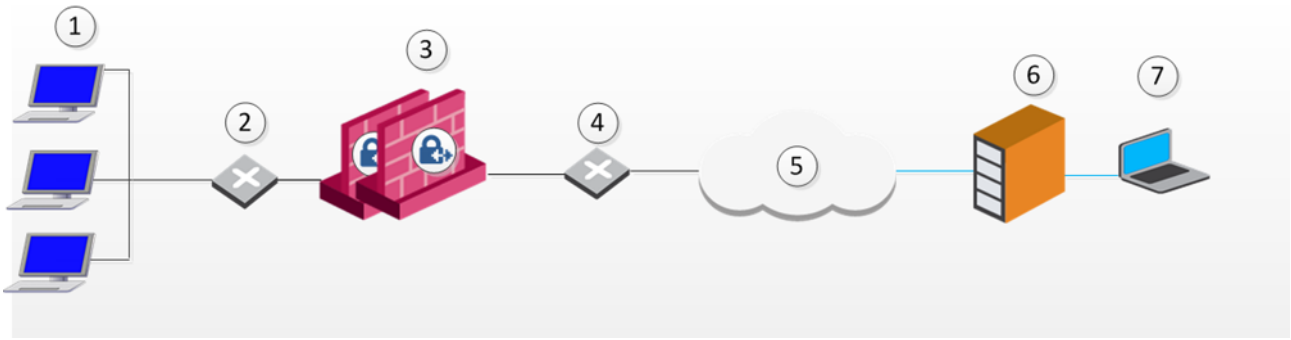
Passive IPsec PMTU

Passive IPsec PMTU solves the problem of dynamic Internet routing. Passive IPsec PTMU is a process that occurs when either side receives an ICMP error message resulting from a change in the routing path. Since routes change dynamically on the Internet, if a different router needs to fragment the packet that has the DF bit set, the router discards the packet and generates an ICMP "cannot fragment" error message. The error message is sent to the VPN peer that sent the packet. When the peer receives this error message, the peer decreases the PMTU and retransmits.

Note - From the system administrator perspective, there is nothing to configure for PMTU; the IPsec PMTU discovery mechanism, both active and passive, runs automatically.

NAT and Back Connections from Security Gateway to Client

In the following figure, the remote client is behind a NATing device and connecting to a Security Gateway or cluster:



Item	Description
1	LAN
2	Internal Switch
3	Security Gateway or cluster
4	External Switch
5	Internet
6	NATing Device
7	Remote Access client

This is also true if the NATing is performed on the Security Gateway side.

Usually to communicate with hosts behind a Security Gateway, remote access VPN client must initialize a connection to the VPN Security Gateway. However, once a remote access VPN client has opened a connection, the hosts behind the VPN Security Gateway can open a return or back connection to the remote access VPN client. For a back connection to succeed, the remote access client's details must be maintained on all the devices between the remote access VPN client and the VPN Security Gateway, and on the VPN Security Gateway itself.

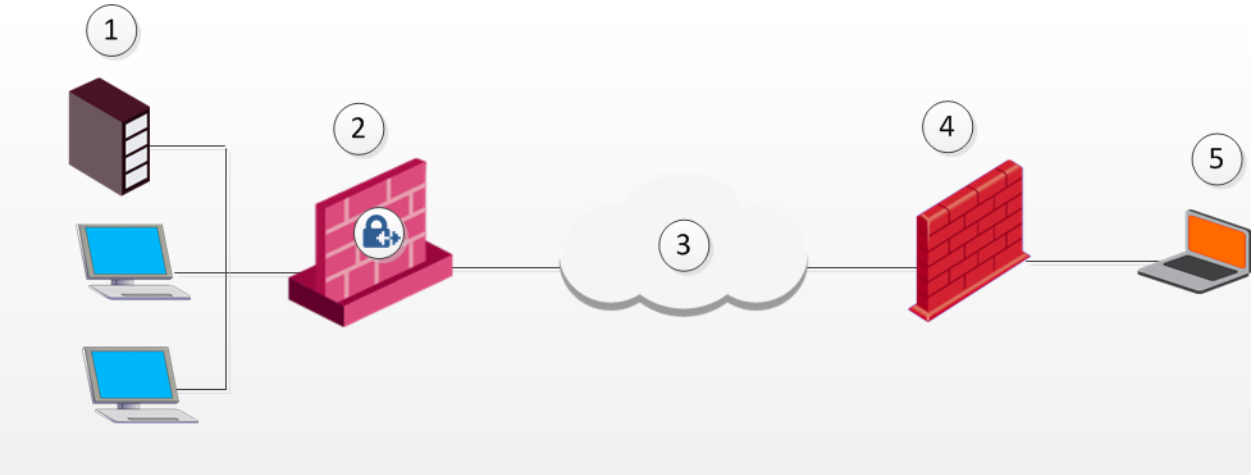
1. In SmartConsole, click **Menu > Global properties**.
2. Select the **Remote Access** page.
3. Click **Remote Access** > In the **Additional Properties** section, select **Enable Back Connections (from gateway to client)**.
4. Click **OK**.
5. Install the Access Control Policy on the VPN Security Gateway.

Overcoming Restricted Internet Access

When a user connects to the organization from a remote location such as hotel or the offices of a customer, Internet connectivity may be limited to web browsing using the standard ports designated for HTTP, typically port 80 for HTTP and port 443 for HTTPS. Since the remote client needs to perform an IKE negotiation on port 500 or send IPsec packets (which are not the expected TCP packets; IPsec is a different protocol), a VPN tunnel cannot be established in the usual way. This issue is resolved using **Visitor Mode**, formally known as *TCP Tunneling*.

Visitor Mode

Visitor Mode tunnels *all* Client-to-Gateway communication through a regular TCP connection on port 443.



Item	Description
1	Host Server
2	Check Point Security Gateway
3	Internet
4	Non-Check Point VPN peer that works with Visitor Mode to allow traffic to the client
5	Remote Access Client

All required VPN connectivity between the Client and the Server is tunneled inside this TCP connection. This means that the peer Security Gateway needs to run a Visitor Mode (TCP) server on port 443.

Number of Users

To obtain optimal performance of the Visitor Mode server:

- Minimize the number of users allowed Visitor Mode if performance degrades
- Increase the number of sockets available on the OS by editing the appropriate values, for example the socket descriptor on Linux systems

Allocating Customized Ports

The organization decides that it would like to use a customized port for the Visitor Mode Server other than the typically designated port 443. In this scenario, another port that is *mutually agreed* upon by *all* the remote locations and the home organization, can be used for Visitor Mode. This solution works well with business partners; the partner simply agrees to open a port for the visitor Mode connections. If the chosen port is not represented by a pre-defined service in SmartDashboard, this service must be created in order for the port to be used. If a port has been mutually agreed upon, and there is a proxy, configure the proxy to allow traffic destined to this port.

Note - All partner Security Gateways must agree on the *same* allocated port, since the Visitor Mode server on the VPN peer will be listening on only one port.

If you change the port for Visitor Mode, then in the Remote Access VPN client, you must name the Remote Access VPN Gateway site in this format:

[Security Gateway's IP address or Hostname]:PORT

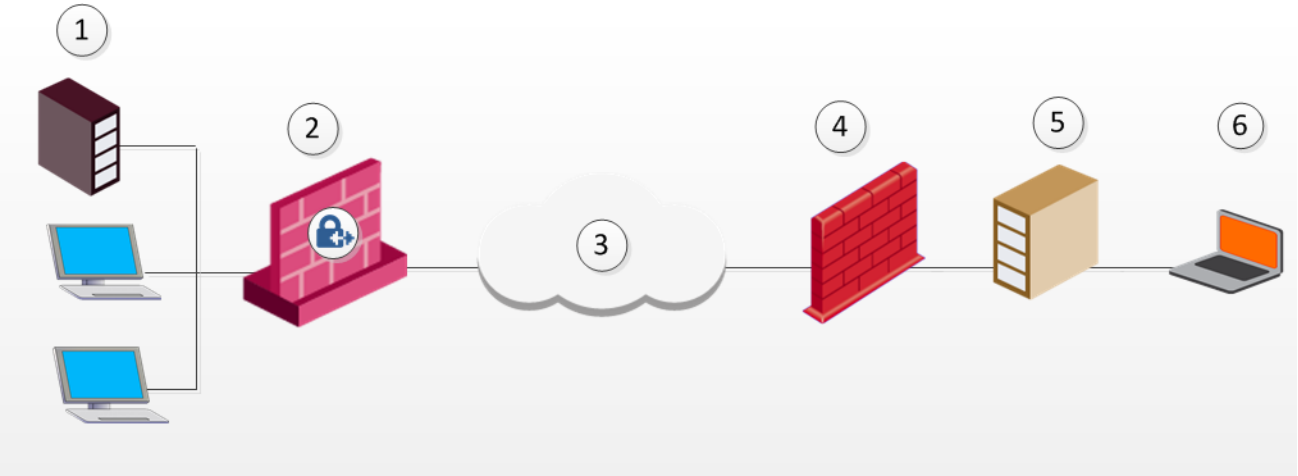
Example -*example-gw.company.com:1720*

For more information about creating a site in the Remote Access VPN client, see:

- *Remote Access VPN Clients for Windows Administration Guide* > "Getting Started with Remote Access Clients" chapter > "Helping Users Create a Site" section
- *Endpoint Security VPN for macOS Administration Guide* > "Helping Your Users" chapter > "Helping Users Create a Site" section

Visitor Mode and Proxy Servers

Visitor Mode can still be utilized in instances where the remote location runs a proxy server. In this scenario, the remote user enables Visitor Mode connections to pass through the proxy server.



Item	Description
1	TCP Server
2	Security Gateway
3	Internet
4	Non-Check Point VPN peer on a remote location
5	Remote location's proxy server
6	Remote Access Client

Visitor Mode When the Port 443 is Occupied By an HTTPS Server

If the designated port is already in use, for example reserved for HTTPS connections by a Server at the organization's Security Gateway, a log is sent "`Visitor Mode Server failed to bind to xxx.xxx.xxx.xxx:yy (either port was already taken or the IP address does not exist)`" to Security Management Server.

If the peer Security Gateway is *already* running a regular HTTP server that also listens on the standard HTTPS port 443, then it must be set up with two external interfaces, both of which have public IP addresses - one for the HTTP server, and one for the Visitor Mode server. This second routable address can be achieved in two ways:

- installing an additional network interface for the Visitor Mode server, *or*
- by utilizing a virtual IP on the same network interface which is blocking the port.

On the Security Gateway object running the Visitor Mode server, **General Properties** > **Remote Access page** > there is a setting for **Allocated IP address**. All the available IP addresses can be configured to listen on port 443 for Visitor Mode connections.

Visitor Mode in a MEP Environment

Visitor Mode also works in a MEP environment. For more information, see *"Visitor Mode and MEP" on page 162*.

Interface Resolution

For *interface resolution* in a Visitor Mode environment, it is recommended to use static IP resolution or dedicate a single interface for Visitor Mode.

Configuring Remote Access Connectivity

This section describes how to configure Remote Access connectivity in SmartDashboard and DBedit.

Configuring Small IKE phase II Proposals

Small phase II IKE proposals always include AES-256, but not AES-128. Suppose you want to include AES-128 in the small proposals:

1. Open the command line database editing tool **DBedit**. There are two properties that control whether small proposals are used or not, one for pre-*NG with Application Intelligence*, the other for *NG with Application Intelligence*.
   - `phase2_proposal` - determines whether an old client (pre-*NG with Application Intelligence*) will try small proposals - default "false".
   - `phase2_proposal_size` - determines whether a new client (for *NG with Application Intelligence*) will try small proposals - default "true".
2. In **Global Properties** > **Remote Access** page > **VPN - Advanced** subpage > **User Encryption Properties** section, select **AES-128**. This configures remote users to offer AES-128 as a small proposal.

Configuring Visitor Mode

Visitor Mode requires the configuration of both the Server and the Client. See also: *"Visitor Mode and MEP" on page 162*.

Visitor Mode and Clusters

Cluster support is limited. The High Availability and Load Sharing solutions must provide "stickiness". That is, the visitor mode connection must always go through the same cluster member.

Failover from cluster member to cluster member in a High Availability scenario is not supported.

Configuring Remote Clients to Work with Proxy Servers

1. In the Remote Access client, select **Detect Proxy from Internet Explorer Settings**.
2. Enter a username and password for proxy authentication. This information is later transferred with the "connect" command to the proxy server.

Remote Access clients can read any of the Visitor Mode settings, but only if:

- The client is connected to a LAN or WLAN
- Secure Domain Logon (SDL) is **not** enabled.

Note - Visitor mode attempts to connect to the proxy server without authenticating. If a user name and password is required by the proxy, the error message "proxy requires authentication appears".

Windows Proxy Replacement

If a Remote Access client is on a LAN\WLAN and a proxy server is configured on the LAN, the client replaces the proxy settings so that new connections are not sent to the VPN domain via the proxy but go directly to the LAN\WLAN's Security Gateway. This feature works with and without Visitor Mode.

When a Remote Access client replaces the proxy file, it generates a similar plain script PAC file containing the entire VPN domain IP ranges and DNS names (to be returned as "DIRECT"). This file is stored locally, since the Windows OS must receive this information as a plain script PAC file. This file replaces the automatic configuration script as defined in Internet Explorer.

Configuring Windows Proxy Replacement

Windows proxy replacement is configured either on the Security Gateway or on the Remote Access client.

Proxy Replacement for the Security Gateway

To configure the Security Gateway to support Visitor Mode:

1. From Menu, click **Global Properties**.
2. From the navigation tree, click **Advanced**.
3. In the **Advanced Configuration** page, click **Configure**.

   The **Advanced Configuration** window opens.
4. From the navigation tree, click **VPN Advanced Properties > Remote Access VPN**.
5. Select one of these options:
   - **ie_proxy_replacement** - When selected, Windows proxy replacement is always performed, even if Visitor Mode is not enabled
   - **ie_proxy_replacement_limit_to_tcpt** - When selected, the proxy replacement is only when Visitor Mode is enabled

CLI Commands

For more about the CLI commands, see the *R81.20 CLI Reference Guide*.

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Encryption Domain
The networks that a Security Gateway protects and for which it encrypts and decrypts VPN traffic.

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Remote Access VPN
An encrypted tunnel between remote access clients (such as Endpoint Security VPN) and a Security Gateway.

Route-Based VPN
A routing method for participants in a VPN community, defined by network routes.

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Site to Site VPN
An encrypted tunnel between two or more Security Gateways. Synonym: Site-to-Site VPN. Contractions: S2S VPN, S-to-S VPN.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VPN Community
A named collection of VPN domains, each protected by a VPN gateway.

VPN Tunnel
An encrypted connection between two hosts using standard protocols (such as L2TP) to encrypt traffic going in and decrypt it coming out, creating an encapsulated network through which data can be safely shared as though on a physical private line.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.