



Check Point
SOFTWARE TECHNOLOGIES LTD.

04 June 2020

1500 APPLIANCE SERIES

R80.20.01

Locally Managed

Administration Guide

Models: V-80, V-80W, V-81, V-81W, V-81WL [Classification: Protected]



Check Point
SOFTWARE TECHNOLOGIES LTD.

INFINITY

Check Point Copyright Notice

© 2020 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

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



Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



Check Point R80.20.01

For more about this release, see the R80.20.01 [home page](#).



Latest Version of this Document

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
4 June 2020	Corrected LED information
18 May 2020	Updated <i>"Configuring Internet Connectivity" on page 50</i>
04 March 2020	Updated <i>"Configuring High Availability" on page 99</i>
11 February 2020	Fixed links to appliance homepage
31 December 2019	First release of this document

Table of Contents

Check Point 1500 Appliance Series Overview	8
Setting up the Check Point Appliance	9
Connecting the Cables	10
First Time Deployment Options	11
Zero Touch Cloud Service	12
Deploying from a USB Drive or SD Card	13
Sample Configuration File	13
Preparing the Configuration Files	14
Deploying the Configuration File - Initial Configuration	14
Deploying the Configuration File - Existing Configuration	14
Viewing Configuration Logs	15
Troubleshooting Configuration Files	15
Configuration File Error	15
Suggested Workflow - Configuration File Error	15
Sample Configuration Log with Error	16
Using the set property Command	17
Configuration and Upgrade Scenarios	18
Configuring Cloud Services	18
Configuring a Guest Network	18
Configuring VPN	20
Configuring Remote Access VPN	20
Configuring Site to Site VPN with a Preshared Secret	21
Configuring Site to Site VPN with a Certificate	22
Managing Clusters	25
Configuring a Cluster	25
Upgrading a Cluster	26
Configuring QoS	28
Enabling VoIP Traffic	29
Appliance Configuration	30
Introduction to the WebUI Application	30

The Home Tab	31
Viewing System Information	31
Controlling and Monitoring Software Blades	32
Setting the Management Mode	34
Configuring Cloud Services	36
Managing Licenses	39
Viewing the Site Map	41
Notifications	41
Managing Active Devices	42
Viewing Monitoring Data	44
Viewing Reports	46
Using System Tools	48
Managing the Device	50
Configuring Internet Connectivity	50
Monitoring	55
Configuring Wireless Network	56
Configuring the Local Network	60
Configuring a Hotspot	69
Configuring the Routing Table	71
Configuring MAC Filtering	74
Configuring the DNS Server	77
Configuring the Proxy Server	78
Backup, Restore, Upgrade, and Other System Operations	79
Configuring Local and Remote System Administrators	84
Configuring Administrator Access	90
Managing Device Details	92
Managing Date and Time	93
Configuring DDNS and Access Service	94
Using System Tools	95
Managing Installed Certificates	95
Managing Internal Certificates	97
Configuring High Availability	99
Advanced Settings	102

Managing the Access Policy	132
Configuring the Firewall Access Policy and Blade	132
Working with the Firewall Access Policy	137
Defining Firewall Servers	143
Defining NAT Control	146
Advanced - Creating and Editing NAT Rules	149
Working with User Awareness	151
Configuring the QoS Blade	154
Working with QoS Policy	156
SSL Inspection Policy	159
SSL Inspection Exceptions	162
SSL Inspection Advanced	163
Managing Threat Prevention	164
Configuring Threat Prevention Blade Control	164
Configuring Threat Prevention Policy Exceptions	167
Viewing Infected Devices	169
Viewing the IPS Protections List	172
Advanced Threat Prevention Engine Settings	173
Configuring the Anti-Spam Blade Control	178
Configuring Anti-Spam Exceptions	180
Managing VPN	181
Configuring the Remote Access Blade	181
Configuring Remote Access Users	184
Remote Access Connected Remote Users	187
Configuring Remote Access Authentication Servers	188
Configuring Advanced Remote Access Options	191
Configuring the Site to Site VPN Blade	194
Configuring VPN Sites	195
Configuring Advanced Site to Site Community Settings	201
Viewing VPN Tunnels	202
Configuring Advanced Site to Site Settings	203
Managing Trusted CAs	205
Managing Installed Certificates	207

Managing Internal Certificates	209
Managing Users and Objects	211
Working with User Awareness	211
Configuring Local Users and User Groups	214
Configuring Local and Remote System Administrators	216
Managing Authentication Servers	222
Managing Applications & URLs	225
Managing System Services	227
Managing Service Groups	230
Managing Network Objects	232
Managing Network Object Groups	234
Logs and Monitoring	235
Viewing Security Logs	235
Viewing System Logs	237
Configuring External Log Servers	238
Notifications	240
Managing Active Devices	240
Wireless Active Devices	240
Paired Mobile Devices	241
Viewing Infected Devices	241
Viewing VPN Tunnels	242
Viewing Active Connections	243
Access Points	244
Viewing Monitoring Data	244
Viewing Reports	244
Using System Tools	244
SNMP	245
Advanced Configuration	247
Upgrade Using a USB Drive	247
Upgrade Using an SD Card	249
Boot Loader	250
Upgrade Using Boot Loader	251
Restoring Factory Defaults	252

Check Point 1500 Appliance Series Overview

Check Point 1500 appliance series includes the 1550 and 1590 appliances. These appliances support the Check Point Software Blade architecture and provide independent modular security building blocks. You can quickly enable and configure the Software Blades to meet your specific security needs.

Check Point 1550 and 1590 appliances deliver integrated unified threat management to protect your organization from today's emerging threats. Based on proven Check Point security technologies such as Stateful Inspection, Application Intelligence, and SMART (Security Management Architecture), the appliances provides simplified deployment while delivering uncompromising levels of security.

These appliances run an embedded version of the Gaia operating system. The appliances include core configuration elements such as clish interface, SNMPv2/3 and routing stack implementations. In addition to the Gaia features, Embedded Gaia contains support for built-in network switches, wireless networks, 4G LTE Internet connectivity, multiple Internet connections (more than 2) in High Availability or Load Sharing mode, Policy Based Routing, and DDNS support. Quick deployment with USB is supported for all appliances, and with SD card and Dual SIM card for the 1590 appliances. For more information, see the 1500 appliance series product page.

This guide describes all aspects that apply to the Check Point 1550 and 1590 Appliances.

Note - Some topics only apply to specific appliances or models.

Appliance	Model	Appliance Homepage
1550	V-80 Wired, V-80W WiFi	sk157412
1590	V-81 Wired, V-81W WiFi, V-81WL LTE-WiFi, V-81WD DSL-WiFi	sk157412

For front, side, and back panel details for each appliance, see the relevant *Getting Started Guide*.

Review these materials before doing the procedures in this guide:

- R80.20.01 SMB Release Notes
- Known Limitations
- Resolved Issues
- *Getting Started Guide*
- [Small Business Security video channel](#)

See the SMB R80.20.01 [home page](#).

Setting up the Check Point Appliance

To set up the Check Point 1550 and 1590 Appliance:

1. Remove the Check Point Appliance from the shipping carton and place it on a tabletop.
2. Identify the network interface marked as LAN1. This interface is preconfigured with the IP address 192.168.1.1.

Connecting the Cables

To connect the cables:

1. Connect the power cable to the appliance. The appliance is connected directly to the power source. For 1530/1550 appliances only: Turn on the power button located on the back panel.
2. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

When the LED turns a solid blue, the appliance is ready for login.

Note - The LED is red if there is an alert or error.

3. Connect the standard network cable to the LAN1 port on the appliance and to the network adapter on your PC.

- **If you use an external modem:**

Connect the Ethernet cable to the WAN port on the appliance back panel and plug it into your external modem or router's PC/LAN network port. The Internet LED on the appliance front panel lights up when the Ethernet is connected.

First Time Deployment Options

There are different options for first time deployment of your Small and Medium Business (SMB) gateways:

- First Time Configuration Wizard - For more information, see the *Getting Started Guide* for your appliance model.
- ["Zero Touch Cloud Service" on page 12](#)
- ["Deploying from a USB Drive or SD Card" on page 13](#)

Note - SD card deployment is supported only in 1590 appliances.

Zero Touch Cloud Service

The Zero Touch Cloud Service lets you easily manage the initial deployment of your gateways in the [Zero Touch Portal](#).

Note - You cannot use Zero Touch if you connect to the internet through a proxy server.

Zero Touch enables a gateway to automatically fetch settings from the cloud when it is connected to the internet for the first time.

Note - The appliance is fully configured after you complete the First Time Configuration Wizard (click **Finish** on the final screen or click **Quit** on an earlier screen after you enter a username and password). To use the Zero Touch Cloud Service after this point, you must first restore the factory defaults.

If the gateway connects to the internet using DHCP, the gateway fetches the Zero Touch settings without any additional action. If no DHCP service is available, you must run the First Time Configuration Wizard, configure the Internet Connection settings, and then fetch the settings from the Zero Touch server.

To connect to the Zero Touch server from the First Time Configuration Wizard:

1. In the **Welcome** page of the First Time Configuration Wizard, click **Fetch Settings from the Cloud**.
2. In the window that opens, click **Yes** to confirm that you want to proceed.
3. The **Internet connection** page of the First Time Configuration Wizard opens. Configure your Internet connection and click **Connect**.
4. The settings are automatically downloaded and installed.
5. A new window opens and shows the installation status. It may take several minutes until the installation is complete.

Note - If a collision is detected between an internal network (LAN) and an IP returned via DHCP (WAN), the conflicting LAN address is changed automatically. If a colliding LAN IP address is changed, a message appears in the system logs.

When you reconnect to the WebUI or click **Refresh**, the browser opens to show the status of the installation process.

After the gateway downloads and successfully applies the settings, it does not connect to the Zero Touch server again.

For more information on how to use Zero Touch, see [sk116375](#) and the [R80.20 Zero Touch Web Portal Admin Guide](#).

Deploying from a USB Drive or SD Card

You can deploy the Check Point Appliance configuration files from a USB drive or SD card (1590 appliances only) and quickly configure many appliances without using the First Time Configuration Wizard. The configuration file lets you configure more settings and parameters than are available in the First Time Configuration Wizard.

Note - SD card deployment is not supported for 1550 appliances.

You can deploy configuration files in these conditions:

- An appliance with default settings is not configured at all.
- An appliance that already has an existing configuration.

The Check Point Appliance starts, automatically mounts the USB drive, and searches the root directory for a configuration file.

Note - The USB drive must be formatted in FAT32. SD cards are formatted with ext4.

Sample Configuration File

This is a sample Check Point 1550 Appliance configuration file for USB deployment.

```
set time-zone GMT+01:00
(Amsterdam/Berlin/Bern/Rome/Stockholm/Vienna)
set ntp server primary 10.1.1.10
set ntp server secondary

set user admin type admin password aaaa
set interface WAN ipv4-address 10.1.1.134 subnet-mask
255.255.255.192 default-gw 10.1.1.129

delete interface LAN1_Switch

set dhcp server interface LAN1 disable
set interface LAN1 ipv4-address 10.4.6.3 subnet-mask
255.255.255.0

add interface LAN1 vlan 2
set dhcp server interface LAN1:2 disable
set interface LAN1:2 ipv4-address 10.4.3.3 subnet-mask
255.255.255.0

set dhcp server interface LAN2 disable
set interface LAN2 ipv4-address 192.168.254.254 subnet-mask
255.255.255.248
set interface LAN2 state on

set admin-access interfaces WAN access allow

set hostname DEMOgw01
```

Preparing the Configuration Files

The Check Point Appliance Massive Deployment configuration files are composed of Gaia Clish commands. These are the file names that you can use:

- `autoconf.clish`
- `autoconf.<MAC address>.clish`

<MAC address> is the specified MAC address in this format: `XX-XX-XX-XX-XX`

You can create multiple configuration files for Check Point Appliance gateways. The gateways run both files or only one of them. First the `autoconf.clish` configuration file is loaded. If there is a configuration file with the same MAC address as the gateway, that file is loaded second.

Use the `#` symbol to add comments to the configuration file.

Deploying the Configuration File - Initial Configuration

This section describes how to deploy a configuration file on a USB drive to Check Point Appliance. You must configure and format the file correctly before you deploy it. You can insert the USB drive in the front or rear USB port. Make sure the USB drive is formatted in FAT32.

You can deploy the configuration file to the Check Point Appliance when the appliance is off or when it is powered on.



Important - Do not remove the USB drive or insert a second USB drive while the configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive for the initial configuration:

1. Insert the USB drive into a Check Point Appliance.
 - Check Point Appliance is OFF - Turn on the appliance. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.
 The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.
 When the LED turns a solid blue, the appliance is ready for login.
Note - The LED is red if there is an alert or error.
 - Check Point Appliance is ON - The appliance automatically detects the USB drive.
2. The Check Point Appliance locates the USB configuration file and begins to run the script. The Power LED blinks blue while the script runs.
3. The configuration script finishes and the Check Point The Power LED is a constant blue.
4. Remove the USB drive from the Check Point Appliance.

Deploying the Configuration File - Existing Configuration

To edit or upgrade the existing configuration of a Check Point Appliance, deploy a configuration file. Use the `set property` command to set the appliance to use a configuration file on a USB drive. The USB drive can be inserted in the front or the rear USB port.

You can deploy the configuration file to the Check Point Appliance either when the appliance is off or when it is powered on.



Important - Do not remove the USB drive or insert a second USB drive while the Check Point Appliance configuration script runs. This may cause a configuration error.

To deploy the configuration file from a USB drive to a configured appliance:

1. From the CLI, enter the command: `set property USB_auto_configuration once`
The appliance is set to use a configuration script from a USB drive.
2. Insert the USB drive in the appliance (the appliance automatically detects the USB drive).
The Power LED comes on and is a constant blue.
3. The appliance locates the USB configuration file and begins to run the script. The Power LED blinks blue while the script runs.
4. The configuration script finishes.
The Power LED is a constant blue and the screen displays: `System Started`.
5. Remove the USB drive from the appliance.

Viewing Configuration Logs

After the Check Point Appliance is successfully configured from a USB drive, a log is created.

- The log file is called `autonconf.<MAC>.<timestamp>.<log>`
- The log file is created in the USB root directory and in `/tmp` on the appliance.

Troubleshooting Configuration Files

This section discusses the scenario where the configuration file fails and the Check Point Appliance is not fully configured.

Configuration File Error

If there is an error and the configuration file fails, the appliance is not fully configured and is no longer in the initial default condition. The commands in the configuration file that show before the error are applied to the appliance. You can examine the configuration log to find where the error occurred.

When the appliance is not fully configured, the First Time Configuration Wizard shows in the Web UI. However, not all of the settings from the failed configuration file show in the First Time Configuration Wizard.

Best Practice - Check Point recommends that you do not use the First Time Configuration Wizard to configure an appliance when the configuration file fails. Restore the default settings to a partially configured appliance before you use the First Time Configuration Wizard to ensure that the appliance is configured correctly.

Suggested Workflow - Configuration File Error

This section contains a suggested workflow that explains what to do if there is an error with the configuration file on a USB drive. Use the `set property USB_auto_configuration` command when you run a configuration file script on a configured appliance.

1. The USB drive with the configuration file is inserted into a USB port on the Check Point Appliance.
2. The Power LED on the front panel blinks red. There is a problem with the configuration file script.

Sample console output displaying an error Booting Check Point RD-6281-A User Space...INIT: Entering runlevel: 3.....sd 2:0:0:0: [sda] Assuming drive cache: write throughsd 2:0:0:0: [sda] Assuming drive cache: write through.....System Started...Start running autoconfiguration CLI script from USB2 ... Error.autoconf.00-1C-7F-21-07-94.2011-07-21.1248.log was copied to USB2

3. The log file is created and contains the configuration details.
 - The log file is called `autonconf.<MAC>.<timestamp>.<log>`
 - The log file is created in the USB root directory and in `/tmp` on the appliance.
4. Analyze the log file to find the problem.

If you cannot repair the configuration file:

1. Remove the USB drive.
2. Run the CLI command: `restore default-settings`.
3. Connect to the Web UI and use the First Time Configuration Wizard to configure the appliance.

If you understand the error and know how to repair the configuration file:

1. Remove the USB drive.
2. Run the CLI command: `restore default-settings`.
3. Insert the USB drive and run the repaired configuration script again.

Sample Configuration Log with Error

This is a sample configuration log file for a configuration script that fails.

```
set hostname Demo1
set hostname: Setting hostname to 'Demo1'
OK

set interface WAN internet primary ipv4-address 66.66.66.11
Error: missing argument 'subnet-mask' for a new connection
Autoconfiguration CLI script failed, clish return code = 1
```


Using the set property Command

The `set property` CLI command controls how the Check Point Appliance runs configuration scripts from a USB drive. These commands do not change how the First Time Configuration Wizard in the Web UI configures the appliance.

- `set property USB_auto_configuration off` - The appliance does not run configuration scripts from a USB drive.
- `set property USB_auto_configuration once` - The appliance only runs the next configuration script from a USB drive.
- `set property USB_auto_configuration any` - The appliance always runs configuration scripts from a USB drive.

Configuration and Upgrade Scenarios

This chapter contains workflows for common configuration and upgrade scenarios.

Configuring Cloud Services

Introduction

Cloud Services lets you connect your Check Point Appliance to a Cloud Services Provider that uses a Web-based application to manage, configure, and monitor the appliance.

Prerequisites

Before you connect to Cloud Services, make sure you have:

- Received an email from your Cloud Services Provider that contains an activation link. When you click the link, your Check Point Appliance automatically connects to Cloud Services.
- Or
- The Service Center IP address, the Check Point Appliance gateway ID, and the registration key. Use these details to manually connect your Check Point Appliance to Cloud Services.

To automatically connect to Cloud Services:

1. Make sure the Check Point Appliance was configured with the First Time Configuration Wizard. See the Check Point Appliance Getting Started Guide.
2. In the email that the Security Gateway owner gets from the Cloud Services Provider, click the **activation link**.

After you log in, a window opens and shows the activation details sent in the email.

3. Make sure the details are correct and click Connect.

For more details, see ["Configuring Cloud Services" on page 36](#).

To manually connect to Cloud Services:

1. In the WebUI, go to the **Home > Cloud Services** page.
2. Follow the Connect to Cloud Services procedure in ["Configuring Cloud Services" on page 36](#).

Configuring a Guest Network

In some situations, you need to allow guest access to the Internet from within your organization. At the same time, you may want to restrict access to internal network resources. When you configure a guest network with a Hotspot, you can control network access. If you set user authentication options, you can then monitor the users that connect to the network.

Prerequisites

- You must have a wireless network enabled on your appliance. The guest network is actually a Virtual Access Point (VAP).
- You must define the network interfaces that redirect users to the Hotspot portal when they browse from those interfaces.

Configuration

1. Go to **Device > Wireless Network**.
2. Click **Guest** and follow the wizard instructions. See ["Configuring Wireless Network" on page 56](#).
 - Set the network protection (unprotected or protected network).
 - Set the access and log policy options in the **Access Policy** tab.
3. Make sure that the **Use Hotspot** checkbox is selected in the wizard.
4. Make sure you defined the network interfaces for Hotspot. See ["Configuring the Local Network" on page 60](#).
5. Configure the Hotspot - Go to **Device > Hotspot** and set the options. See ["Configuring a Hotspot" on page 69](#).
6. If necessary, you can limit access to the Hotspot for specified user groups in the Access section.

Monitoring

Connect to the network and open a browser session. You see the customized Hotspot portal.

Note - You are shown the Hotspot portal one time in the given timeout period. The default timeout period is 4 hours.

User activity on this network is logged with user names if the Log traffic option was selected.

Configuring VPN

This section describes how to configure these VPN configuration scenarios:

- Remote access VPN
- Site to site VPN using a preshared secret
- Site to site VPN using a certificate

Configuring Remote Access VPN

Introduction

Use these options for remote access:

- Check Point VPN clients
- Check Point Mobile clients
- Check Point SSL VPN
- L2TP VPN client

Prerequisites

- In **VPN > Blade Control**, make sure:
- Remote Access control is set to On and the **Allow traffic from Remote Access users (by default)** option is selected.
- Select the applicable connection methods.
- For more details, see ["Configuring the Remote Access Blade" on page 181](#).
- If the gateway uses a dynamic IP address, we recommend you use the DDNS feature. See ["Configuring DDNS and Access Service" on page 94](#).
- For the Check Point VPN client or Mobile client method, make sure that the applicable client is installed on the hosts. Click **How to connect** for more information.

Remote Access Configuration

These are the methods to configure remote access users:

- Local users
- RADIUS users
- AD users

To allow only specified users to connect with a remote access client, set group permissions for the applicable user type. Select the arrow next to the **Add** option and select the relevant group option. See ["Configuring Remote Access Users" on page 184](#).

To configure local users:

For new users:

1. Go to **VPN > Remote Access Users**.
2. Click **Add** to add local users.
3. Make sure that the **Remote Access permissions** checkbox is selected.

For more information, see ["Configuring Remote Access Users" on page 184](#).

For existing users:

1. Go to **VPN > Remote Access Users**.
2. Click **Edit** to make sure that the **Remote Access permissions** checkbox is selected.

For more information, see ["Configuring Remote Access Users" on page 184](#). To configure RADIUS users:

1. Go to **VPN > Authentication Servers**.
2. Click **Configure** to add a RADIUS server. See ["Configuring Remote Access Authentication Servers" on page 188](#).
3. Click **permissions for RADIUS users** to set access permissions.

To configure AD users:

1. Go to **VPN > Authentication Servers** and click **New** to add an AD domain. See ["Configuring Remote Access Authentication Servers" on page 188](#).
2. Click **permissions for Active Directory users** to set access permissions.

L2TP VPN Client configuration

For L2TP VPN Client configuration, click **L2TP Pre-shared key** to enter the key after you enable the L2TP VPN client method.

Advanced Options

For more information on advanced Remote Access options, for example Office Mode network, see ["Configuring Advanced Remote Access Options" on page 191](#).

Monitoring

To make sure Remote Access is working:

Use the configured client to connect to an internal resource from a remote host.

Configuring Site to Site VPN with a Preshared Secret

Introduction

In this Site to Site VPN configuration method a preshared secret is used for authentication.

Prerequisites

- Make sure the Site to Site VPN blade is set to On and **Allow traffic from remote sites (by default)** is selected. See ["Configuring the Site to Site VPN Blade" on page 194](#).
- The peer device that you connect to must be configured and connected to the network. If it is a DAIP gateway, its host name must be resolvable.

Configuration

Enter a host name or IP address and enter the preshared secret information. For more information, see ["Configuring VPN Sites" on page 195](#).

Monitoring

To make sure the VPN is working:

1. Send traffic between the local and peer gateway.
2. Go to **VPN > VPN Tunnels** to monitor the tunnel status. See ["Viewing VPN Tunnels" on page 202](#).

Configuring Site to Site VPN with a Certificate

Introduction

In this Site to Site VPN configuration method a certificate is used for authentication.

Prerequisites

- Make sure the Site to Site VPN blade is set to On and **Allow traffic from remote sites (by default)** is selected. See ["Configuring the Site to Site VPN Blade" on page 194](#).
- The peer device that you connect to must be configured and connected to the network. If it is a DAIP gateway, its host name must be resolvable.
- You must reinitialize certificates with your IP address or resolvable host name. Make sure the certificate is trusted on both sides.
- VPN encryption settings must be the same on both sides (the local gateway and the peer gateway). This is especially important when you use the Custom encryption option.

Configuration

1. Reinitialize certificates - Use the **Reinitialize certificates** option described in ["Managing Installed Certificates" on page 95](#). Make sure this is done on both the local and peer gateway (if they both use locally managed Check Point appliances).
2. Trust CAs on the local and peer gateways - Use one of these procedures:
 - Exchange CAs between gateways
 - Sign a request using one of the gateway's CAs.
 - Authenticate by using a 3rd party CA.
 - Authenticate with an existing 3rd party certificate.

3. Use certificate authentication to create the VPN site.

- a. Follow the instructions in *"Configuring VPN Sites" on page 195*.
- b. To make sure the specified certificate is used, enter the peer gateway's certificate information in **Advanced > Certificate Matching**.

Trust Procedures

Exchange CAs between gateways:

Click **Add** to add the Trusted CA of the peer gateway. This makes sure the CA is uploaded on both the local and peer gateways. See *"Managing Trusted CAs" on page 205*.

Sign a request using one of the gateway's CAs:

You create a request from one gateway that must be signed by the peer gateway's CA.

1. Use the **New Signing Request** option in *"Managing Installed Certificates" on page 95*.
2. Export this request using the **Export** option.
3. Use the peer gateway's internal CA to sign the request on the peer gateway.
If the peer gateway is a locally managed Check Point gateway, go to **VPN > Trusted CAs** and use the **Sign a Request** option. For more information, see *"Managing Trusted CAs" on page 205*.
4. **Upload the signed request to the local gateway.**
 - a. Go to **VPN > Installed Certificates**.
 - b. Select the installed certificate that you asked the remote peer to sign.
 - c. Upload the certificate with the **Upload Signed Certificate** option. See *"Managing Installed Certificates" on page 95*.
5. Make sure that the CA is installed on both of the gateways. Use the **Add** option in *"Managing Trusted CAs" on page 205*.

Authenticate by using a 3rd party CA

You create a signing request from each peer gateway. Follow the steps above in *Sign a request using one of the gateway's CAs* to sign it with a 3rd party CA.

Note that a 3rd party CA can either issue *.crt, *.p12, or *.pfx certificate files.

1. **Upload the certificate using the appropriate upload option.**
 - a. Go to **VPN > Installed Certificates**.
 - b. Select the installed certificate that you asked the remote peer to sign.
 - c. Upload the certificate with the **Upload Signed Certificate** or **Upload P12 Certificate** option. See *"Managing Installed Certificates" on page 95*.
2. Make sure that the 3rd party CA is installed on both of the gateways. Use the **Add** option in *"Managing Trusted CAs" on page 205*.

Authenticate with an existing 3rd party certificate:

1. Create a P12 certificate for the local and peer gateway.
2. Upload the P12 certificate using the **Upload P12 Certificate** option on each gateway.

3. Make sure that the 3rd party CA is installed on both of the gateways. Use the **Add** option in ["Managing Trusted CAs" on page 205](#).

Monitoring

To make sure the VPN is working:

1. Pass traffic between the local and peer gateway.
2. Go to **VPN > VPN Tunnels** to monitor the tunnel status. See ["Viewing VPN Tunnels" on page 202](#).

Managing Clusters

Configuring a Cluster

Introduction

Configure a cluster to maintain connections in the organization's network when there is a failure in a cluster member. The cluster provides redundancy.

Cluster High Availability is supported. In High Availability, only one gateway is active at a time. When there is a failover, the standby member becomes active. There is no load sharing between the members of the cluster.

All cluster configuration is done through the active member.

Note - Bridge and switch configurations are not supported in cluster configuration.

Configuration workflow:

1. Complete the First Time Configuration Wizard on both appliances. In the **Local Network** page of the wizard, clear the **Enable switch on LAN ports** checkbox.
2. Configure network settings on the appliance that is the primary (active) member.
3. Connect a sync cable between the appliances.
4. Configure the active member.
5. Configure the standby member.

Prerequisites

- In **WebUI > Device > Local Network**, delete bridge and switch configurations before you start to configure a cluster.
- The appliances in a cluster must have the same hardware, firmware, and licenses.

Note - Connect the sync cable only after you complete the First Time Configuration Wizard and remove the switch on both appliances. No additional configuration is required on both members.

Best Practice - Designate the same LAN port for the Sync interface. The default Sync interface is LAN2/SYNC.

For the primary (active) cluster member:

1. Connect to the appliance that is the primary cluster member.
2. In the WebUI, go to **Device > High Availability** and click **Configure Cluster**.
3. Follow the wizard steps and configure the appliance as a primary member. For more information, see ["Configuring High Availability" on page 99](#).

For the secondary (standby) cluster member:

1. Connect to the appliance that is the secondary cluster member.
2. Go to **Device > High Availability** and click **Configure Cluster**.

3. Follow the wizard steps and configure the appliance as a secondary member. For more information, see ["Configuring High Availability" on page 99](#).

Complete other configuration requirements such as access policy, VPN, and Threat Prevention parameters. The primary and secondary members now synchronize their configuration.

Monitoring the Cluster

Best Practice - After the cluster is successfully configured, connect to `https://my.firewall`. This redirects you to the WebUI **Home** > **System** page for the active cluster member.

To log in to each appliance:

Go to `https://<IP>:4434.<IP>` is the IP address of a specified member.

Note - Not all options are available as all cluster configuration is done through the active member. The WebUI of the standby cluster member only has one tab: **Device**.

To show the status of the cluster member:

Go to **Device** > **High Availability**.

Upgrading a Cluster

When you upgrade a cluster member, you can maintain network connectivity during an upgrade. One member of the cluster remains active while the other cluster member is upgraded. The system is always active and there is no downtime during the upgrade process.

In a High Availability cluster, only one member is active at a time. The other appliance is standby. To upgrade a cluster, first upgrade the standby appliance and then upgrade the active member.

Upgrade workflow:

1. Upgrade the standby member in the WebUI **Device** > **System Operations** page.
The standby member automatically reboots.
2. In the active member's WebUI **Device** > **High Availability** page, wait for the status to show "Active" and "Standby."
3. Upgrade the active member.
The active member automatically reboots.

Note - The upgrade process is the same for each cluster member. Only manual upgrade is supported.

After the reboot:

- The former active member is now the standby member.
- The former standby member is now the active member.

To manually upgrade a cluster member:

1. On the **Device > System Operations** page, click **Manual Upgrade**.

The Upgrade Software Wizard opens.

2. Follow the Wizard instructions to upgrade the cluster member.

The upgrade process automatically reboots the member.

To see the status of each cluster member:

Go to **Device > High Availability**.

Configuring QoS

Introduction

The QoS (bandwidth control) policy is a set of rules that lets you set bandwidth parameters that control the flow of traffic to and from your network. They make sure that important traffic is prioritized and your business has minimal disruption when there is network congestion.

QoS can be activated on Internet connections and requires at least one Internet connection is configured with the maximum download and/or upload speeds. You get the speed information from your ISP.

QoS policy rules apply separately on each configured Internet connection.

Prerequisites

In **Access Policy > QoS > Blade Control**, make sure the QoS blade is turned on.

Configuration

1. In **Device > Internet**, select an Internet connection and click **Edit**.
2. In the **Advanced** tab, edit the **QoS Settings**.

These values are used as a 100% percent baseline when you calculate QoS weight. For more details, see ["Configuring Internet Connectivity" on page 50](#).

3. You can use these options:
 - A default QoS policy that requires defining only a number of parameters. See ["Configuring the QoS Blade" on page 154](#).
 - Define manual rules for further granularity if necessary in **Access Policy > QoS > Policy**. See ["Working with QoS Policy" on page 156](#).

Enabling VoIP Traffic

Introduction

Follow these configuration procedures to allow SIP traffic to pass through the gateway when:

- The SIP server is located on external networks. For more advanced topologies, refer to [sk113573](#).
- The gateway's NAT configuration is set to its default settings (with internal networks hidden behind its external IP address).

Configuration

To allow application-level inspection and NAT of the SIP protocol:

1. Go to **Users & Objects > Services**.
2. Edit the **SIP_UDP** and **SIP_TCP** built in services by enabling SIP inspection on both services - Clear the **Disable inspection for this service** checkbox in each service object. For more details, see *"Viewing System Information" on page 31*.

To allow the SIP server to connect to internal phones from the Internet:

1. Go to **Access Policy > Policy**.
2. Add a rule to the **Incoming, Internal and VPN traffic** Rule Base that allows SIP traffic.
Source - A network object that holds the IP address of the SIP server.
Destination - A network object that holds the IP addresses of the phones behind the gateway
Service - SIP
Action - Accept
For more information, see *"Working with the Firewall Access Policy" on page 137*.
3. **Optional** - Configure a log for this rule.

Appliance Configuration

This chapter contains instructions for special Check Point Appliance features.

Introduction to the WebUI Application

The Check Point Appliance uses a web application to configure the appliance.

After you use the First Time Configuration Wizard (see the *Check Point Appliance Getting Started Guide*), when you connect to the appliance with a browser (with the appliance's IP or, if the appliance is used as a DNS proxy or DHCP server, to "my.firewall"), it redirects the web page to a secure https site and asks for administrator credentials. When you log in, you can select the **Save user name** checkbox to save the administrator's user name. The name is saved until you clear the browser's cookies.

When you log in correctly, the WebUI opens to **Home > System**. The left pane lets you navigate between the different pages of each of these tabs:

- **Home**
- **Device**
- **Access Policy**
- **Threat Prevention**
- **VPN**
- **Users & Objects**
- **Logs & Monitoring**

To log in to the WebUI in a different language:

In the browser page that shows the Login window, select the language link at the bottom of the page.

The log in page changes immediately to the selected language. The next login from the same computer is in the selected language (saved in a browser cookie). The language is kept until you clear the browser's cookies.

Note - If the locale of a user matches a localized WebUI, the Login window automatically loads in the specified language. Only English is supported as the input language.

The Home Tab

This chapter describes the Home tab of the WebUI application.

Viewing System Information

The **Home > System** page shows an overview of the Check Point Appliance.

The Check Point Appliance requires only minimal user input of basic configuration elements, such as IP addresses, routing information, and blade configuration. The initial configuration of the Check Point 1550 Appliance can be done through a First Time Configuration Wizard. When initial configuration is completed, every entry that uses `http://my.firewall` shows the WebUI **Home > System** page.

- **System Information** - Shows the appliance model, installed software version, name, MAC address, system date and time (with the GMT setting), and system uptime.
- **Notifications** - Shows events and their type/severity.
- **Network** - Shows Internet information and wireless network/radio status.
If applicable, click the links to configure Internet and Wireless options.
- **Statistics** - Shows live data graphs of packet rate and throughput.

To monitor your device's internet connection from your mobile device, you must first configure this on the WebUI **Home > System** page.

To configure connection monitoring:

1. In the WebUI, go to **Home > System > Internet connections** and click **Edit**.

The **Edit Internet Connection** window opens.

2. In the **Connection Monitoring** tab, check or clear:
 - **Automatically detect loss of connectivity to the default gateway**. This pings the default gateway to detect if connectivity is lost.
 - **Monitor connection state by sending probe packets to one or more servers on the Internet**. This uses other methods and servers to detect connectivity loss.
3. If you selected **Monitor connection state**, select the **connection probing** method:
 - Probe DNS servers
 - Ping addresses
4. If you selected **Ping addresses**, enter the IP address(es).
5. Select the settings for:
 - **Recovery time** (seconds)
 - **Max latency allowed** (milliseconds)
 - **Probing frequency for active connections** (seconds)
6. Click **Apply**

Controlling and Monitoring Software Blades

The **Home > Security Dashboard** page shows you the active blades and lets you quickly navigate to the blade configuration page.

It also gives you:

- Access to the basic settings of the blades with the **Settings** button (cogwheel icon) and lets you activate the blades.
- Access to statistics for each blade (graph icon)
- Alerts you if there are blades that are missing licenses, service blades which are not up-to-date, and active blades which require additional configuration (for example, site-to-site VPN where the user did not configure any sites). When applicable, there is a triangle in the upper right hand corner of the specified blade.

The software blades are shown in these groups on this page based on where they are configured in the WebUI:

- **Access Policy** - Contains the Firewall, Application & URL Filtering, User Awareness, and QoS blades.
- **Threat Prevention** - Contains the Intrusion Prevention (IPS), **Anti-Virus**, **Anti-Bot**, **Threat Emulation**, and **Anti-Spam** blades.
- **VPN** - Contains the Remote Access and Site to Site VPN blades. It also contains certificate options.

You can click the tab name link or Software Blade link to access the tab for further configuration.

To turn a Software Blade on or off:

1. Slide the lever of the specified blade to the necessary **ON** or **OFF** position.
2. When you turn off the Firewall blade, click **Yes** in the confirmation message.

Note - Software Blades that are managed by Cloud Services show a lock icon. You cannot toggle between on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

To see or edit setting information:

1. Click the cogwheel icon next to the On/Off lever.
The blade settings window opens.
2. View the details or select options to change current settings.
3. Click **Apply**.

To view statistics:

1. Click the bar graph icon.
The blade statistics window opens.

2. If the blade is turned on:
 - View the graph and details.
 - To go to other blade statistics, click the arrows in the header.
3. If the blade is turned off:
 - Click **View demo** to see an example of the statistics shown
 - Click the X icon to close the demo.

To view an alert:

1. Hover over the alert triangle.
2. Click the applicable link.

Setting the Management Mode

The **Home > Security Management** page shows information for the management mode of the appliance. You can also test Internet Connectivity from this page.

To set the management type:

Select one of the options:

- **Locally** - To manage the appliance using the local web application (WebUI). Click **Apply** and then **Yes** when asked to confirm.
- **Centrally** - To manage the appliance using the Security Management Server.

When centrally managed, it shows the trust status between the appliance and the Security Management Server. When a policy is prepared in SmartConsole you can fetch the policy from this window.

Security Management Server

In this section you can view the status of the management connection, last policy installation, adjust trust settings, and initialize a connection.

1. In the Security Management Server section, click **Settings** to adjust trust settings or **Setup** to initialize a connection. The Welcome to the Security Management Server Configuration Wizard shows.
2. Click **Next**. In the One Time Password (SIC) page, select an option for authenticating trusted communication:

- Initiate trusted communication securely by using a one-time password - The one-time password is used to authenticate communication between the appliance and the Security Management Server in a secure manner.

Enter a one-time password and confirm it. This password is only used to establish the initial trust. When established, trust is based on security certificates.

Important - This password must be identical to the Secure Communication authentication one-time password configured for the appliance object in the SmartDashboard of the Security Management Server.

- Initiate trusted communication without authentication (not secure) - Select this option only if you are sure that there is no risk of imposture (for example, when in a lab setting).

3. Click **Next**. In the Security Management Server Connection page, select a connection method:
 - To connect to the Security Management Server now, select **Connect to the Security Management Server now**, enter the Security Management Server IP or name and click **Connect**. When you successfully connect to the Security Management Server, the security policy is automatically fetched and installed.

 If the Security Management Server is deployed behind a 3rd party NAT device, select **Always use this IP address** and manually enter the IP address the appliance used to reach the Security Management Server. This IP address overrides, from this point on, the automatic calculating mechanism that determines the routeable IP address of the Security Management Server for each appliance.

 If trust was established but the gateway could not fetch the policy, you can investigate the issue with the Security Management Server administrator. When the issue is resolved, click the **Fetch Policy** button that shows instead of the **Connect** button.
 - To connect to the Security Management Server later, select **Connect to the Security Management Server later**.
4. Click **Finish**.

To reinitialize trusted communication with the Security Management Server:

1. In the Security Management Server section, click **Advanced** to reinitialize trusted communication.
2. Click **Reinitialize Trusted Communication**.

A Warning message shows.

3. Click **Yes**.

Note - You need to coordinate this operation with the Security Management Server administrator, as reinitialization is necessary on both sides.

Security Policy

To obtain the security policy from the Security Management Server, click **Fetch Policy**. This option is available only if trust is established with the Security Management Server.

Internet

To test connectivity, click **Test Connection Status**. A status message shows the results of the test. You can click **Settings** to configure Internet connections.

Configuring Cloud Services

On the **Home > Cloud Services** page, you can connect the appliance to Cloud Services. The Cloud Services Provider uses a Web-based application to manage, configure, and monitor your appliance.

To connect the appliance to Cloud Services:

1. Click the activation link in the email that the Security Gateway owner gets from the Cloud Services Provider.
2. Log in.
A window opens and shows the activation details sent in the email.
3. Make sure the activation details are correct and click **Connect**.

If the appliance is connected to a different Cloud Services Provider, you are asked if you want to continue.

Alternatively, follow the connection procedure below.

When you successfully connect, a security policy and other settings are pushed to the appliance. The settings defined by Cloud Services contain your activated blades, security policy, and service settings.

After Cloud Services are turned on, these identification details are shown in the WebUI:

- At the bottom of the login page - The name defined by the Cloud Services Provider for your Security Gateway and the MAC address of the Check Point Appliance.
- At the top of the WebUI application (near the search box) - The name of your Check Point Appliance.

These are the sections on this page:

- **Cloud Services - This section shows Cloud Services details.**
 - The **Configure** option lets you configure initial connectivity.
 - When connected, you can click **Details** to see connectivity details and **Fetch now** to get updated activated blades, security policy and service settings.
 - When disconnected, you can click **Refresh** to try and reconnect to Cloud Services.
- **Managed Security Blades** - Shows a colorful or black and white icon for defined security blades. You can click the icon text to open the corresponding page in the WebUI.
 - Dark blue icon - Shown for a blade that is remotely managed by Cloud Services. The blade is turned on in the plan.
Remotely managed blade pages show a lock icon. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.
 - Gray icon - Shown for a blade that is remotely managed by Cloud Services. The blade is turned off in the plan.
 - No icon - Shown for a security blade that is locally managed in the Check Point1550 Appliance. The blade is not managed by Cloud Services.
If no blades are remotely managed, all of the blades icons are gray.
- **Available Services** - Shows the services that are managed by the Cloud Services Provider. If a service has a **Settings** button, you can click it to show read-only setting information. You cannot

change the setting information. Services in a gray font show services that are not provided by Cloud Services.

These are the available services:

- Reports - Periodic network and security reports sent by email. Click **Settings** to see the time frames set for your gateway.
- Logs - Logs are stored with the Cloud Services Provider.
- Dynamic DNS - A persistent domain name is set by Cloud Services.
- Firmware Upgrades - Firmware upgrades are managed remotely by Cloud Services.
- Periodic Backup - Backups are scheduled by Cloud Services.

Before you can connect to Cloud Services, make sure you have:

- Received an email from your Cloud Services Provider that contains an activation key for your Check Point1550 Appliance and also an activation link
- Or
- The Service Center IP address, the Check Point1550 Appliance gateway ID, and the registration key

Workflow to connect to Cloud Services:

1. Connect to Cloud Services Provider and establish a secure connection.
Make sure the gateway registration information is correct.
2. Get the security policy and settings.
3. Install the security policy and settings.

When you connect for the first time, the appliance must verify the certificate of the Cloud Services Provider against its trusted Certificate Authority list. If verification fails, you get a notification message. You can stop or ignore the verification message and continue.

To connect to Cloud Services:

1. Click **Configure** or **Edit**.
The Configure Cloud Services window opens.
2. Select **Activation key** or **Activation details** and enter the specified information.
3. Click **Apply**.

The Check Point Appliance tries to connect to the Cloud Services Provider. The Cloud Services section shows a progress indicator and shows the connection steps.

Note - If you see a message that the identity of your Cloud Services Provider cannot be verified but you are sure of its identification, click **Resolve** and then **Ignore and reconnect**.

When connectivity is established, the Cloud Services section at the top of the page shows:

- The date of the synchronization
- The On/Off lever shows that Cloud Services is turned on.

A **Cloud Services Server** widget is shown on the status bar and shows **Connected**. If you click this widget, the Cloud Services page opens.

To test connectivity to the Cloud Services:

1. Open a console connection.
2. Log in.
3. Run this CLI command:

```
test cloud-connectivity <service-center-addr> <addr>
```

To get an updated security policy, activated blades, and service settings:

Click **Fetch now**.

The Check Point Appliance gets the latest policy, activated blades, and service settings from Cloud Services.

Managing Licenses

The **Home > License** page shows the license state for the Software Blades. From this page, the appliance can connect to the Check Point User Center with its credentials to pull the license information and activate the appliance.

In most cases, you must first register the appliance in your Check Point User Center account or create one if you don't already have one. A User Center account is necessary to receive support and updates.

If you have Internet connectivity configured:

1. Go to **Home > License**.
2. Click **Activate License**.

You are notified that you successfully activated the appliance license.

If you were not able to activate the license, it may be because:

- There is a connectivity issue such as a proxy between your appliance and the Internet.
- Or
- Your appliance is not registered.

If there is a proxy between your appliance and the Internet, you must configure the proxy details before you can activate your license.

To configure the proxy details:

1. Click **Set proxy**.
2. Select **Use proxy server** and enter the proxy server **Address** and **Port**.
3. Click **Apply**.
4. Click **Activate License**.

If your appliance is not registered:

1. Browse to: <https://smbregistration.checkpoint.com>
2. Enter the **MAC address** and **Registration key**. These values can be found on the **Home > License** page.
3. Select **Hardware Platform**.
4. Select **Hardware Model**.
5. Click **Activate License**.

You are notified that you successfully activated the appliance license.

After initial activation, the **Activate License** button shows as **Reactivate**. If you make changes to your license, click **Reactivate** to get the updated license information.

If you are offline while configuring the appliance:

1. Browse to [Check Point User Center](#)
2. Enter the appliance's credentials, MAC address, and registration key from the **Home > License** page.
3. After you complete the registration wizard, you are prompted to download the activation file. Download it to a local location. This is needed for the next step.
4. In **Home > License**, click **Offline**.
The Import Activation File window opens.
5. **Browse** to the activation file you downloaded and click **Import**.

The activation process starts.

The region is set when the license is installed. The region determines the wireless frequency and parameters, as the regulations vary according to region.

If you are using a trial license, only **basic radio settings**, are allowed in all zones. A warning that selected wireless radio settings are not applied shows on the **Summary** page of the First Time Configuration Wizard and also on the **Device > License** page. For more information on basic wireless radio settings, see [sk159693](#).

If you select a country and install a valid license, but the wireless region of the device does not match the selected country, a warning message shows and you must edit the country information. When the country and wireless region match, you see the full settings.

Viewing the Site Map

The **Home > Site Map** page shows a site map of the WebUI. It shows all of the tabs and the pages they contain.

Click the link to any page directly from the Site Map page.

Notifications

The **Notifications** page shows events in a table.

For each event:

- Time
- Severity - Type of event, such as Security Alert, Attention Required, or Informative Event
- Subject
- Message

To filter:

Enter text in the search filter.

To view details of a security event:

Click the event row in the table and click **View Details**.

To set the notification setting:

1. Click **Settings**.
The **Notifications Settings** window opens.
2. Under **Mobile notifications**, select **Send push notifications** and select the types of notifications.
3. Click **Apply**.

This page is available from the **Home** and **Logs & Monitoring** page.

Managing Active Devices

The **Active Devices** page shows a list of the devices identified in internal networks. The information includes:

- Name
- IP addresses
- MAC Address
- Device Details - Type of device.
- Network Access - Indicates whether the device is blocked from network activity.
- Interface - Interface name.
- Services - Shows incoming and outgoing services. Incoming services usually indicate servers.
- Zone - Shows if the appliance is connected physically or through a wireless connection.

To temporarily block a device:

Select the device and click **Block**.

Manage the display:

- **Save as** - Save a selected device as a network object or server.

When you select this option, the New Network Object (see ["Managing Network Objects" on page 232](#)) window or New Server Wizard (see ["Defining Firewall Servers" on page 143](#)) opens. Enter the information in the fields and click **Apply**. Use these objects to reserve IP addresses to MAC addresses in the DHCP server and also add this object name as a device in the local DNS service. Network objects and server objects can be used in the security configurations, for example in the Access Policy and IPS exceptions

A server object also allows you to configure access and NAT if applicable as part of the object. If access and/or NAT are configured, automatic access rules are created in the Access Policy Rule Base.

- **Filter** - Filter the list by servers, active devices, or known devices.
- **Details** - Select a row in the list and click **Details** to show additional properties of the device.
- **Refresh** - Refresh the information in the list.
- **Start/Stop Traffic Monitor** - Gather upload and download packet rates for active devices. The information is shown in the added Traffic column in the table.

This operation may affect performance.
To stop, click **Stop Traffic Monitoring**.

The display shows the devices connected to the gateway through a Hotspot. You can revoke the Hotspot access for one or more devices. This disconnects the device from the gateway and requires the device to log in again through the Hotspot.

To revoke the Hotspot access:

1. Click the record for the relevant device.
2. Click **Revoke Hotspot Access**.

The access for that device is revoked. You must log in again through the Hotspot to reconnect the device to the gateway.

Note - This page is available from the **Home** and **Logs & Monitoring** tabs.

Viewing Monitoring Data

The **Monitoring** page shows network, security, and troubleshooting information. When you enter this page, the latest data shows. You can click **Refresh** to update information. To see a sample monitoring report, click **Demo**. To close the sample reports, click **Back**.

The number of current connections in the system is shown for **VPN Tunnels**, **Active Devices**, and **Connections**. You can click the links to open the corresponding WebUI pages.

The Monitoring page is divided into these sections:

- Network
- Security
- Troubleshooting

To expand or collapse the sections, click the arrow icon in the section's title bar.

Network

By default, network statistics are shown for the last hour. You can also see statistics for the last day. Select the applicable option **Last hour** or **Last day** from the Network section's title bar.

The data is automatically refreshed for the time period:

Last hour - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15 AM.

Last day - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.

- **Bandwidth Usage** - The doughnut chart shows the top 10 applications or users that consumed the most bandwidth in the selected time frame (last hour or last day). Click the **Applications** or **Users** links to toggle between the statistics. To show user information the User Awareness blade must be activated.
- **Top Bandwidth Consuming** - Shows statistics for the top bandwidth consuming application, category, site, and user in percentages and the amount of traffic (MB or GB).
- **Traffic** - By default, shows the total amount of traffic received and sent in an area graph. The time axis reflects the time frame (last hour or last day) selected for the Network section. For last hour, the graph shows 5 minute intervals and for last day, hourly intervals. You can click the **Received** and **Sent** links to see only the amount of traffic received or sent. The orange area on the graph represents sent traffic. The blue area represents received traffic.

If you hover over a time interval, a popup box shows:

- The date and time
- The traffic sent or received
- The total traffic for that time interval
- Total traffic statistics - Next to the area graph you can see total traffic statistics for the last day or hour.

Security

- **Infected devices** - Shows the number of:
 - Infected devices
 - Infected servers
 - Recently active infected devices

You can click **All Infected Devices** to open the **Logs & Monitoring > Infected Devices** page.

- **High risk applications** - Shows:
 - The number of high risk applications
 - The most used high risk applications
 - The top users of high risk applications.

You can click **Applications Blade Control** to open the **Access Policy > Firewall Blade Control** page to see Applications and URL Filtering settings.

- **Security events** - Shows the number of:
 - Anti-Bot - Malwares detected by the Security Gateway.
 - Anti-Virus - Malwares detected by the Security Gateway.
 - Threat Emulation - Malicious files found since the last reboot and how many files scanned.
 - The number of IPS attacks.

You can click the links to open the **Threat Prevention > Blade Control** page.

Troubleshooting

- **System Resources** - Click **CPU, memory and disk usage** to see CPU, memory, and disk usage information.
- **Device Info** - Shows Security Gateway information.
- Links to pages that can be useful for monitoring and troubleshooting purposes.

Note - This page is available from the **Home** and **Logs & Monitoring** tabs.

Viewing Reports

The **Reports** page shows network analysis, security analysis, and infected devices reports by a selected time frame (monthly, weekly, daily, and hourly).

These elements influence the times shown in reports:

- Rounding off of time
- System reboot

Rounding Off of Time

The times shown in generated reports are rounded down:

- For hourly reports - At one minute intervals. For example, if you generate a report at 10:15:45 AM, the report represents data from 9:15 to 10:15.
- For daily reports - At hourly intervals. For example, if you generate a report at 10:15 AM, the report represents data from the last 24 hours ending at 10:00 AM of the current day.
- For weekly reports - At four hour intervals, starting with 00:00, 04:00, 08:00 and so on. For example, if you generate a report at 11:55 AM, the report represents data from the last week ending at 08:00 AM of the current day.
- For monthly reports - At four hour intervals, starting with 00:00, 04:00, 08:00, 12:00 and so on. For example, if you generate a report at 11:15 AM, the report represents data from the last month ending at 08:00 AM of the current day.

System Reboot

In the first 24 hour cycle after an appliance starts up (after installation or an update), the system adds one more time interval to the delta of the next applicable report interval.

For example, for weekly reports that are generated at pair hour intervals, the appliance requires 1 more hours plus the delta for the first applicable pair hour.

- For an appliance that started at 00:00 AM - The first weekly report is generated at 04:00 AM. The total of 4 hours derives from the first delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 4 hours.
- For an appliance that started at 01:59 AM - The first weekly report is generated at 04:00 AM. The generated time derives from the delta of the first applicable pair hour which is 02:00 and the added 2 hours. The total wait is 2 hours.

After you start up an appliance, reports are generated:

- Hourly reports - 2-3 minutes from startup.
- Daily reports - 1-2 hours from startup.
- Weekly reports - 2-4 hours from startup.
- Monthly reports - 4-8 hours from startup.

Note - Only the last generated report for each report type is saved in the appliance. When you generate a new report, you override the last saved report for the specified type.

To generate a report:

Click the applicable time frame link at the top of the page (**Monthly**, **Weekly**, **Daily** or **Hourly**).

The line below the links shows the selected report and its time frame. To refresh the data shown, click **Generate**.

The report includes these sections:

- Executive Summary
- Table of Contents
- Report Pages

Executive Summary

The first page of the report is the executive summary and shows:

- The number of Anti-Bot, Anti-Virus, and Threat Emulation malware detected by the Security Gateway and the number of IPS attacks.
- Top bandwidth consuming statistics by category, site, and user. You can click the **Top category**, **Top site**, or **Top user** link to get to the applicable report page. It also shows **Bandwidth Usage by Applications** statistics for the top 5 applications in a doughnut chart and total traffic received and sent.
- The number of infected devices, servers, and recently active infected devices.
- The number of high risk applications, the most used high risk applications, and the top users of high risk applications.
- The Security Gateway name, version, and MAC address.

Table of Contents

The table of contents contains links to the network analysis, security analysis, and infected devices reports. Click a link to go directly to the selected section.

Report Pages

Each report page shows a detailed graph, table, and descriptions.

Note - This page is available from the **Home** and **Logs & Monitoring** tabs.

Using System Tools

On the **Tools** page you can:

- Monitor system resources.
- Show the routing table.
- Verify the appliance connectivity to Cloud Services.
- Display DSL Statistics (DSL models only)
- Generate a CPInfo file.
- Ping or trace an IP address.
- Perform a DNS lookup.
- Capture packets.
- Download the console-USB driver

To monitor system resources:

1. Click **Monitor System Resources**. The **System Resources** page opens and shows the following information:
 - **CPU Usage History** (automatically refreshed)
 - **Memory Usage History** - memory is calculated without memory that was preallocated to handle traffic and without cache memory. This gives a more accurate picture of the actual memory usage in the appliance but it may differ from figures you receive from Linux tools. The information is automatically refreshed.
 - **Disk Usage** - click the Refresh button for the most updated disk usage information.
2. Click **Close** to return to the **Tools** page.

To show the routing table:

1. Click **Show Routing Table**. The output appears in the Command Output window.
2. Click **Close** to return to the **Tools** page.

To verify the appliance connectivity to Cloud Services:

Click **Test Cloud Cloud Services**.

The Cloud Services Ports Test window opens and shows the available ports and their state.

To display DSL statistics:

Click DSL **Statistics**. A window opens and shows the statistic parameters.

To generate a CPInfo file:

1. Click **Generate CPInfo File**. A message next to the button shows the progress.
2. Click **Download CPInfo File** to view or save the CPInfo file.

To ping or trace an IP address:

1. Enter an IP or host name in the **Device Name or IP Address** field.
2. Click **Ping** or **Trace Route**. The output appears in the Command Output window.
3. Click **Close** to return to the **Tools** page.

To perform a DNS lookup:

1. Enter a **Host Name or IP Address**.
2. Click **Lookup**. The output appears in the Command Output window.
3. Click **Close** to return to the Tools page.

To capture packets:

If a packet capture file exists, a note shows the date of the file and you can download it before you start a new packet capture that overwrites the existing file.

1. Select an option from the **Select Network** list.
2. Click **Start** and then **Stop** when you want to stop packet capturing.
3. Click **Download File** to view or save the capture file.

You can activate packet capture and go to other WebUI application pages while the packet capture runs in the background. However, the packet capture stops automatically if the WebUI session ends. Make sure you return to the packet capture page, stop and download the capture result before you end the WebUI session.

Note - The capture utility uses tcpdump. "fw monitor" is available through the command line interface.

When the mini-USB is used as a console connector, Windows does not automatically detect and download the driver needed for serial communication. You must manually install the driver. For more information, see [sk11713](#).

To download the Windows driver for Mini-USB console socket:

Click the **Download** link.

Note - This page is available from the **Home**, **Device**, and **Logs & Monitoring** tabs.

Managing the Device

This section describes how to set up and manage your Check Point Appliance.

Configuring Internet Connectivity

The **Device > Internet** page shows how the Check Point Appliance connects to the internet. You can configure a single internet connection or multiple connections in High Availability or Load Balancing configurations. When multiple internet connections are defined, the page shows them in a table. You can add a new connection and edit, delete, or disable existing connections. When there are multiple internet connections, you can select which mode to use - **High Availability** or **Load Balancing**. You can also monitor the servers and internet connections (see ["Monitoring" on page 55](#) below).

We recommend you contact your local Internet Service Provider (ISP) to understand how to configure your specific internet connection.

Note - IPv6 is not currently supported.

Note - ADSL/VDSL settings are relevant only for devices that have a DSL port.

To configure internet connectivity:

1. Click **Configure Internet** (if not configured at all), **Add** (for another internet connection), or **Edit**.

The New or Edit Internet Connection window opens.

2. Configure the fields in the tabs:

Configuration tab

Note - When you change the connection type, the appliance may disconnect from the internet.

- **Connection name** - Enter a name for the connection or leave the default "InternetN" label (where N indicates an incrementing number).
- **Interface name** -
- **WAN** or **DMZ** is for most types of Internet connections.
Note - DMZ is not supported in 1550 appliances.
- **LAN**. You can also use unassigned LAN ports with no VLANs for internet connections. When you delete the internet connection, the port reverts to an unassigned LAN.
- **ADSL/VDSL**. If you select the ADSL/VDSL interface, you must select one of these for the connection type: PPPoE, IPoE - static IP, or IPoE - dynamic IP.

You can create a maximum of 32 internet connections.

Unassigned LAN ports use case - If your company is in a region where internet connections supplied by ISPs are unreliable and experience multiple disconnections, you can connect your appliances to multiple internet connections from different ISPs.

IPv4 connection types:

- **Connection type** - Select the connection type:
- **DHCP** - Dynamic Host Configuration Protocol (DHCP) automatically issues IP addresses within a specified range to devices on a network. The device retains the assigned address for a specified administrator-defined period. This does not apply to the ADSL/VDSL interface.
- **Static IP** - A fixed (non-dynamic) IP address.
- **PPPoE** - A network protocol to encapsulate Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly in DSL systems. PPPoE can run directly over the ADSL/VDSL interface. It can also run over WAN or DMZ interfaces that are typically connected to an external DSL modem. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings**.
- **IPoE - dynamic IP** (DSL only) - The Internet IP of the appliance is imported through DHCP.
- **IPoE - static IP** (DSL) - The Internet IP of the appliance is determined statically. You must enter the **IP address**, the **subnet mask**, **default gateway** and **DNS Server Settings**.
- **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.
- **L2TP** - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol. It does not provide any encryption or confidentiality but relies on an encryption protocol that it passes within the tunnel to provide privacy.
- **Bridge** - Connects multiple network segments at the data link layer (Layer 2).
- **LTE** - Both SIM cards are used for the internet connection with a failover between them.
- **Analog Modem** - Connect to the Internet with an analog modem through a USB or serial port. For this option, select the USB/Serial option in Interface name.

Note - If you use an analog modem through the serial port, you cannot connect to the appliance with the serial port or get terminal server functionality. For more on the terminal server, go to **Device > AdvancedSettings**.

Fill in the fields that are shown for the connection type.

Note - You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | \ " # + \

To configure LTE internet connection (LTE WiFi models only):

1. Click **Configure Internet** (if not configured at all), **Add** (for another internet connection), or **Edit**.
The New or Edit Internet Connection window opens.
2. In the **Configuration** tab, select **Cellular** for **Interface name**.
3. Click **Apply**.

Note - This closes the Edit Internet Connection window.

The remaining steps are optional additional settings and are not essential for configuration.

4. In the **Cellular** tab, under **Cellular settings**, select the **Primary SIM** and which SIM to disable: **SIM 1**, **SIM 2** or **Neither**.
 - SIM 1 - Micro-SIM
 - SIM 2 - Nano-SIM
5. For each SIM, enter the **APN** and **PIN** number.
6. Configure the **Connection Monitoring** and **Advanced** tabs as for other interface connections.
7. Click **Apply**.

Note - The **Cellular** tab is disabled unless you select **Cellular** for the interface name. Only appliances that support LTE show the Cellular tab.

For PPPoE over ATM over VDSL/ADSL or IPoE over ATM over VDSL/ADSL or for an ADSL interface:

Enter the **VPI number** and **VCI number** you received from your service provider, and the **Encapsulationtype** (LLC or VC_MUX).

For WAN/DMZ interfaces and static, DHCP, PPPoE, PPTP, and L2TP connection types

Or

For VDSL/ADSL interfaces and IPoE - dynamic IP and IPoE - static IP connection types over PTM:

- **Use connection as VLAN** - Select this checkbox to add a virtual Internet interface.
- **VLAN ID** - Enter a VLAN ID between 1 and 4094.

If you are in an Annex L system, in Advanced Settings, you must enable the Annex L and disable the Annex J/M.

If you are in an Annex M system, in Advanced Settings, you must enable Annex J/M and disable the Annex L. In all other Annex systems, no changes are needed to the default configuration.

Notes:

- Multiple internet connections can be established over a single VDSL/ADSL connection carrying PTM traffic or in the case of WAN and DMZ interfaces.
- Only one internet connection can be established over a VDSL/ADSL interface carrying ATM traffic or a USB interface.
- One IPoE or PPPoE connection can be established over ATM running over the DSL interface.
- A single IPoE connection or multiple PPPoE connections can be established over one untagged DSL interface carrying PTM traffic.
- A single IPoE connection or multiple PPPoE connections can be established over one VLAN tagged DSL interface carrying PTM traffic.
- A single DHCP or Static IP connection can be established over a USB interface.
- A single DHCP or Static IP connection or multiple PPPoE connections can be established over one untagged or one VLAN tagged WAN or DMZ interface.

- When all the ADSL standards are turned off in the Advanced Settings and you can only connect using the VDSL2 standard, the VPI, the VCI and the encapsulation options still appear even though they are not used to open an internet connection.

Connection Monitoring tab

- **Automatically detect loss of connectivity to the default gateway** - Select this option to detect connectivity loss by sending ARP requests (pinging) to the default gateway and expecting responses.
- **Monitor connection state by sending probe packets to one or more servers on the Internet** - Select this option to detect connectivity loss by using more methods and servers.
 - **Connection probing method** - Select one of the options.
 - **Ping addresses** - When you select this option, you can configure up to three servers by IP address or host name.
 - **Probe DNS servers** - When you select this option, the appliance probes the DNS servers as defined in the Internet connection and expects responses.

Advanced tab

For PPPoE

- **IP Address Assignment** (PPPoE IPv4 only) - In **Local tunnel IP address**, select if the IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**.
- **Service Provider Settings** - In **Service**, enter a service name (optional) and select the **Authentication method**.
- **Connect on demand** - Select the **Connect on demand** checkbox if necessary. This is relevant only when you are in high availability mode.

For PPTP and L2TP

- **IP Address Assignment** -
 - In **Local tunnel IP address**, select if the IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**.
 - In **WAN IP assignment**, select if the WAN IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**, **Subnet mask**, and **Default gateway**.
- **Service Provider Settings** - In **Service**, enter a service name (optional) and select the **Authentication method**.
- **Connect on demand** - Select the **Connect on demand** checkbox if necessary. This is relevant only when you are in high availability mode.

Port Settings

- If necessary, select **Use custom MTU value** and set the **MTU size**.

Note - For a DMZ interface the MTU value is applied to all LAN ports.

To avoid fragmentation (which slows transmission), set the MTU according to the smallest MTU of all the network devices between your gateway and the packet destination

For static and DHCP mode, set MTU to 1500 or lower.

For PPPoE connections, set MTU to 1492 or lower.

Note - When the gateway is behind a modem that works as a NAT device, the MTU value of the gateway must be the same value as in the modem. If the modem has a PPPoE connection, set the MTU in the gateway to 1492 or lower.

- **MAC address clone** - If you select **Override default MAC address**, you can override the default MAC address used by the Internet connection. This is useful when the appliance replaces another device and wants to mimic its MAC address.
- If necessary, select **Disable auto negotiation**. This lets you manually define the link speed of the Internet connection.
 - Select the **Link Speed**.

QoS Settings (bandwidth control) - supported in IPv4 connections only

To enable QoS bandwidth control for download and upload for this specified connection, select the applicable **Enable QoS (download)** and/or **Enable QoS (upload)** checkboxes. Enter the maximum Kbps rates for the selected options as provided by your ISP for the Internet upload and download bandwidth.

Make sure that the QoS blade is turned on. You can do this from **Home > Security Dashboard > QoS > ON**.

ISP Redundancy - supported in IPv4 connections only

Multiple Internet connections can be configured in High Availability or Load Sharing modes. When you configure more than one Internet connection, the **Device > Internet** page lets you toggle between these options. The Advanced setting of each Internet connection lets you configure each connection's priority or weights based on the set mode.

- Clear the **Route traffic through this connection by default** checkbox when you do not want this Internet connection used as a default route for this gateway. The connection is used by the device only if specific, usually service-based, routing rules are defined for it. This is commonly used when you have a connection that is used for dedicated traffic. When you clear this option, this connection does not participate in High Availability or Load Balancing.
- **High Availability - Priority** - Select the priority for the connection. Lower priority connections are only used if higher priority connections are unavailable.
- **Load Balancing - Weight** - The traffic to the Internet is divided between all available connections based on their weights.

NAT Settings

If the gateway's global hide NAT is turned on in the **Access Policy > NAT** page, you can disable NAT settings for specified internet connections.

To disable NAT settings:

1. Go to **Device > Internet**.
2. Select an internet connection and click **Edit**.
The **Edit Internet Connection** window opens.
3. Click **Advanced > NAT Settings**.
4. Select **Do not hide internal networks behind this internet connection**.
5. Click **Apply**.

Monitoring

Click the **Monitor** link to open the Monitoring Servers window. For each connection you configure, you can see the:

- Server name
- IP address
- Packet loss
- Failures
- Latency - How much time it takes for a data packet to get from one designated point to another.
- Jitter - The difference between the minimum and maximum latency results of a ping test. Can be used to determine network and broadband stability.

For Cellular connections only: Click the **Monitor cellular modem** link to open the Cellular Modem Monitoring window to see this information:

- Cellular radio
- Cellular modem
- Operator
- SIM cards - Which SIM is active, primary or disabled.

Configuring Wireless Network

The **Device > Wireless** page shows the wireless network settings (if applicable). You can configure your main wireless network and also additional guest or standard wireless networks (VAPs - Virtual Access Points).

- **Guest** wireless network - Uses hotspot by default and is unprotected by default (no password required).
- **Standard** wireless network - Is a protected wireless network that requires a password and does not use a hotspot by default.

To delete the wireless network, go to **Device > Local Network**.

If multiple wireless networks (VAPs) are defined, the page shows them in a table, where you can add a new guest or standard wireless network and edit, delete, or disable existing ones.

To turn the Wireless network on or off:

- Move the slider to select the **On** or **Off** option. If you configured multiple VAPs, selecting **Off** turns them all off.
Note- If you turn off the wireless radio and then turn it back on, the VAPs remain disabled. To enable the VAPs, you must select the relevant entries in the table and click **Enable**.
- To disable or enable the Wireless network, click **Disable/Enable**.

To edit the radio settings:

1. Click **Radio settings**.
2. Select the correct **Operation mode**, **Channel**, **Channel width**, and **Transmitter power**.
3. Click **Advanced** to set the **Guard Interval** and **Antenna control**.
4. Click **Apply**.

This configuration is global for all wireless networks. Some options may not be available or allowed depending on your country's wireless standards.

1550 appliances only: The wireless client search options depend on the frequency that the appliance is set to. The Check Point Appliance can be configured to only one frequency at a time and is set to 2.4 GHz by default. If you change the radio settings to 802.11 ac or 802.11 ac/n, the frequency automatically changes to 5 GHz. The **Home > System** page shows the wireless radio status.

1590 appliances only: There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

Dynamic Frequency Selection (DFS) detects radar signals that must be protected against interference from 5.0 GHz (802.11ac/n) radios. When these signals are detected, the operating frequency of the 5.0 GHz (802.11ac/n) radio switches to one that does not interfere with the radar systems. DFS is enabled by default.

To edit a wireless network:

Click **Edit Settings**.

The **Edit** window opens in the **Configuration** tab.

Configuration tab

Configure the fields in these tabs:

- **Network name (SSID)** - Enter a name for the wireless network or use the default name. This is the name shown to clients that look for access points in the transmission area.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.

Wireless Security

- **Protected network (recommended)** - This is the recommended wireless security setting.
- **Security type** - Select the security technology used in your wireless network. WPA/WPA2 is the most compatible option. WPA2 is the most secure.
- **Encryption type** - Select the encryption method.
- **Authenticate using** - Select **Password** or **RADIUS server (Enterprise mode)** to determine how the users authenticate.

The Password option allows a single password for all users. This option is known as **WPA Personal**.

The **RADIUS servers(Enterprise mode)** option requires defining RADIUS servers in the **Users & Objects > Authentication Servers** page. Each user that tries to connect to the wireless network is authenticated through the RADIUS server. This option is also known as **WPA Enterprise**.

- **Network password** - When authenticating using a password, enter a password or click **Generate** for an automatically generated password.
 - **Show** - To see the password, select this option. To hide it, clear the checkbox.
- **Unprotected network (not recommended)** - Without a password, any wireless client can connect to this network. This option is not recommended.

Advanced Settings

- **Hide the Network Name (SSID)** - When selected, this wireless network name is not automatically shown to users scanning for them. Connecting to the wireless network can be done manually by adding the specified network name.
- **Allow Station-to-Station Traffic** - When selected, allows wireless stations on this network to communicate with each other. When cleared, traffic between wireless stations is blocked.
- **Enable MAC address filtering** - When selected, by default, all wireless devices are not allowed to connect to the wireless network. To allow a specific device to connect, add a new MAC address to the table. Click **New**, enter the device's **MAC address** and click **Apply**.

Wireless Network tab

Interface Connection

- **Assigned to** - Select **Separate network** or one of the existing configured networks. When selecting a separate network configure this information:
 - **IP address** - IPv4.
 - **Subnet mask** - for IPv4 addresses

DHCPv4 Server

Select one of the options:

- **Enabled** - Enter the **IP address range** and if necessary the **IP address exclude range**. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
- **Relay** - Enter the DHCP server IP address.
- **Disabled**

Access Policy tab

These options create automatic rules that are shown in the **Access Policy > Firewall Policy** page.

- **Allow access from this network to local networks (Wireless network is trusted)**
- **Log traffic from this network to local networks**

Advanced tab

Click the checkbox to exclude from DNS proxy.

DNS Server Settings (For DHCPv4)

These settings are effective only if a DHCPv4 server is enabled.

- **Auto** - This uses the DNS configuration of the appliance as configured in the **Device > DNS** and **Device > Internet** pages.
- **Use the following IP addresses** - Enter the IP addresses for the **First DNS server**, **Second DNS server**, and **Third DNS server**.

Default Gateway

Select one of these options:

- **Use this gateway's IP address as the default gateway.**
- **Use the following IP address** - Enter an IP address to use as the default gateway.

WINS

Select one of these options:

- **Use the WINS servers configured for the internet connection**
- **Use the following WINS servers** - Enter the IP addresses of the **First** and **Second** WINS servers.

Lease

- **Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

Other Settings

You can optionally configure these additional parameters so they will be distributed to DHCP clients:

- **Time servers**
- **Call manager**
- **TFTP server**

- TFTP boot file
- X-Windows display manager
- Avaya IP phone
- Nortel IP phone
- Thomson IP phone

Custom Options

Lets you add custom options that are not listed above. For each custom option, you must configure the name, tag, type, and data fields.

When you finish editing the network, click **Apply**.

Configuring the Local Network

The **Device > Local Network** page lets you set and enable the local network connections, switches, bridge or wireless network (on wireless devices only).

A bridge connects two or more local area networks (LANs). A switch is similar to a bridge but can perform data transmission between multiple port pairs at the same time.

The Network table shows all available network connections.

The page also lets you:

- Configure multiple **switches** (port based VLANs) between the available local LAN interfaces and wireless networks. Between the LAN ports of a switch, traffic is not monitored or inspected.
- Configure multiple **bridges** between interfaces. Traffic in a bridge is always monitored and inspected by the appliance.
- Create and configure tag based **VLANs** (802.1q) on any of the LAN interfaces or DMZ.

Note - DMZ is not supported in 1550 appliances.

- Create and configure **VPN tunnels (VTI)** which can be used to create routing rules which determine which traffic is routed through the tunnel and therefore also encrypted (Route based VPN).
- On wireless devices - Add new **wireless networks (Virtual Access Points)**. This can also be done through the **Device > Wireless** page.

There are two radio transmitters: 2.4 GHz and 5 GHz. Each network is configured separately under a specified transmitter.

You can also use unassigned LAN ports to create an internet connection. In the table, these ports have the status **Assigned to Internet**.

Notes:

- LAN ports assigned to internet connections can only be disabled from the **Internet** page.
- You cannot edit a LAN port assigned to an internet connection. When you click **Edit**, the window opens, but when you click **Apply**, a warning shows that this deletes the connection.
- When you create a bridge or switch surface, these LAN ports do not appear in the selection box as optional ports.
- You cannot disable one of the switch ports. You can disable the switch or configure the requested port as unassigned.

To create any of the above options:

Click **New** and choose the option you want.

To edit/delete/enable/disable any of the above options:

Select the relevant row and click **Edit/Delete/Enable/Disable**.

Notes:

- Physical interfaces cannot be deleted.
- Editing an interface that is part of a switch or a bridge lets you remove it from the switch or bridge.

- When a LAN or DMZ interface is part of an Internet connection, it is still visible on this page, but can be only be configured through the **Device > Internet** page.
- For each network, the table on this page shows you:
 - Name - Name of the network, interfaces that participate (if there are multiple interfaces), and a description (optional)
 - Local IP Address
 - Subnet Mask
 - MAC Address
 - Status - Shows a status for physical interfaces and wireless networks:
 - Physical interfaces - Shows cable connection status of each physical interface that is enabled. Otherwise, it shows disabled.
 - Wireless networks - Shows if the wireless network is up or disabled.

To create/edit a switch:

Note - Between the LAN ports of a switch, traffic is not monitored or inspected. MAC filtering is disabled.

Configure the fields in the tabs:

Configuration tab

1. In **Switch Configuration**, select or clear the interfaces you want to be part of the switch. The table shows you which interfaces are already part of the switch (shown with checkmarks in the table) and which interfaces are not assigned yet and can be added to the switch (empty checkboxes in the table). For example, if LAN8 is already part of another switch, it does not show in this table.
2. From **Assigned to**, select an option:
 - **Unassigned** - The switch is not part of any network and cannot be used
 - **Separate network** - When you select a separate network, configure the settings for the switch
 - **Monitor Mode** - See below
3. Choose the **IP address** and **Subnet mask** the switch uses.
4. **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.
5. In **DHCP Server**:

Select one of the options:

- **Enabled** - Enter the **IP address range** and if necessary the **IP address exclude range**. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specified IP addresses if you define network objects in the **Users & Objects > Network Objects** page. To reserve specified IP addresses, you must have the device MAC address.
- **Relay** - Enter the DHCP server IP address.
- **Disabled**

Monitor Mode

Security Gateways can monitor traffic from a Mirror Port or Span Port on a switch.

With Monitor Mode, the appliance uses Automatic Learning or user-defined networks to identify internal and external traffic, and to enforce policy.

Automatic Learning - The appliance automatically recognizes external networks by identifying the default gateway's network from requests to the Internet (specifically, requests to Google). The rest of the networks are considered internal.

User-Defined Networks - You can manually define internal networks. If a network is not defined as internal, it is considered external.

In both Automatic Learning and user-defined networks:

- Traffic to internal hosts is inspected by the Incoming/Internal/VPN Rule Base.
- Traffic to external hosts is inspected by the Outgoing Rule Base.
- Threat prevention's default configuration is optimized to inspect suspicious traffic from external hosts to internal hosts.

To configure monitor mode in the WebUI:

1. Go to **Device > Local Network**.
2. Select an interface and double-click.
The **Edit** window opens in the **Configuration** tab.
3. In the **Assigned To** drop-down menu, select **Monitor Mode**.
The **Manually define internal networks** checkbox shows.
4. To use Automatic Learning, do not select **Manually define internal networks** and click **Apply**.
5. To use your own network definitions, select **Manually define internal networks**.
The network definition features and table show.
6. Click **New**.
7. Enter the network **IP address**.
8. Enter the **subnet**. An internal network can be a 255.255.255.255 subnet, for one host. For example, to monitor the traffic after the router, enter the IP address of the Default Gateway and the 255.255.255.255 subnet.
9. Click **Apply**.

The Internal network you defined (with Monitor Mode in the name) shows in the list of interfaces.

Note - You can configure multiple local networks to be in monitor mode at the same time.

After you configure monitor mode:

1. Go to **Device > Advanced Settings**.
2. Turn off **Anti-Spoofing**.

To configure monitor mode in CLI:

1. To define a port for Monitor Mode:

```
> set interface <portName> monitor-mode
```

2. To configure Monitor Mode Automatic Learning, disable user-defined networks:

```
> set monitor-mode-configuration use-defined-networks false
```

3. To configure Monitor Mode with user-defined networks:

```
> add monitor-mode-network ipv4-address <IP> subnet-mask <mask>
```

```
> set monitor-mode-configuration use-defined-networks true
```

4. To see user-defined Internal networks:

```
> show monitor-mode-network
```

5. To disable Anti-Spoofing:

```
> set antispoofing advanced-settings global-activation false
```

If you do not see the Monitor Mode option:

1. Run this CLI command:

```
set monitor-mode-configuration allow-monitor-mode true
```

2. Select an interface and click **Edit**.

Monitor Mode is now added to the options list.

For more information on monitor mode, see [sk112572](#).

To edit a physical interface:

Configure the fields in the tabs. Note that for the DMZ there is an additional tab **Access Policy**:

Configuration tab

- **Assigned to** - Select the required option:
 - **Unassigned** - The physical interface is not part of any network and cannot be used.
 - One of the existing configured **switches** or **bridges**

- **Separate network** - When selecting a separate network configure this information:

- **IP address**
- **Subnet mask**
- DHCP Server settings

Select one of the options:

Enabled - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.

Relay - Enter the DHCP server IP address.

Disabled

Note - When you create a switch, you cannot remove the first interface inside unless you delete the switch.

Advanced tab

The options that are shown vary based on interface type and status. Configure the options that are applicable:

- **Description** - Enter an optional description. The description is shown in the local network table next to the name.
- **MTU size** - Configure the Maximum Transmission Unit size for an interface. Note that in the Check Point Appliance, the value is global for all physical LAN and DMZ ports.
- **Disable auto negotiation** - Select this option to manually configure the link speed of the interface.
- **Override default MAC address** - This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address of the network's interface:
 - When the device has two separate local networks connected to the same external switch.
 - If the ISP is searching for the gateway MAC address to accept the connection. If you upgrade your new gateway, the ISP may block it because the new gateway has a different MAC address. In this case, you can override the gateway MAC address with the old one.

Best Practice - This is a rare configuration. Do not select this option unless you are sure you need it.

- **Exclude from DNS proxy** - Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

Access Policy tab (only for DMZ)

These options create automatic rules that are shown in the **Access Policy > Firewall Policy** page.

- **Allow access from this network to local networks**
- **Log traffic from this network to local networks**

To create/edit a tag based VLAN:

You can create a new VLAN only if you have at least one physical interface that is not part of an existing network (switch or bridge).

Note - For more information on the maximum number of VLANs that you can configure for each appliance, refer to [sk113247](#)

Configure the fields in the tabs:

Configuration tab

- **VLAN ID** - Enter a number that is the virtual identifier.
- **Assigned to** - Select the physical interface where the new virtual network is created.
- **IP address**
- **Subnet mask**
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.
- **DHCP Server settings**

Select one of the options:

- **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
- **Relay** - Enter the DHCP server IP address.
- **Disabled**

To create/edit a VPN Tunnel (VTI):

A Virtual Tunnel Interface (VTI) is a virtual interface on a Security Gateway that is related to an existing, Route Based VPN tunnel. The Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community. Each peer Security Gateway has one VTI that connects to the tunnel.

The VPN tunnel and its properties are defined by the VPN community that contains the two gateways. You must define the VPN community and its member Security Gateways before you can create a VTI.

Configure the fields in the tab:

Configuration tab

- **VPN Tunnel ID** - A number identifying the VTI.
- **Peer** - The name of the remote VPN site. See ["Configuring VPN Sites" on page 195](#).
The VPN tunnel interface can be numbered or unnumbered. Select the applicable option:
- **Numbered VTI** - You configure a local and remote IP address for a numbered VTI:
 - **Local IPv4 address** - The IP address to be used for the local point-to-point virtual interface.
 - **Remote IP address** - The IP address to be used at the peer gateway's point-to-point virtual interface.
- **Unnumbered VTI** - When the VTI is unnumbered, it is not necessary to configure local and remote IP addresses. You define a local interface to use as the source IP address for outbound traffic.
 - **Internet connection** - Select from the list.
 - **Local bridge interface** - Select the local interface from the list.

To create/edit a bridge:

Configure the fields in the tabs:

Configuration tab

- In **Bridge Configuration**, select the networks you want to be part of the bridge.
- **Enable Spanning Tree Protocol** - When Spanning Tree Protocol (STP - IEEE 802.1d) is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.
- Enter a **Name** for the bridge interface. Note that you can only enter "brN" where N is a number between 0 and 9. For example, br2.
- Select the **IP address** and **Subnet mask**.
- **Use Hotspot** - Select this checkbox to redirect users to the Hotspot portal before allowing access from this interface. Hotspot configuration is defined in the **Device > Hotspot** page.
- **DHCP Server**

Select one of the options:

- **Enabled** - Enter the IP address range and if necessary the IP address exclude range. The appliance's own IP address is automatically excluded from this range. You can also exclude or reserve specific IP addresses by defining network objects in the **Users & Objects > Network Objects** page. Reserving specific IP addresses requires the MAC address of the device.
- **Relay** - Enter the DHCP server IP address.
- **Disabled**

Advanced tab

- **MTU size** - Configure the Maximum Transmission Unit size for an interface.
- **Disable auto negotiation** - Select this option to manually configure the link speed of the interface.
- **Override default MAC address** - This option is for local networks except those on VLANs and wireless networks. Use this option to override the default MAC address used by the network's interface, when the device has two separate local networks connected to the same external switch.
Best Practice - This is a rare configuration. Do not select this option unless you are sure you need it.
- **Exclude from DNS proxy** - Select this checkbox for any network that you do not want exposed to internal domains. In guest VAPs (wireless network for guests), this is selected by default.

To create/edit a Virtual Access Point (VAP):

See the **Device > Wireless Network** help page.

DHCP/SLAAC Settings tab

The values for the DHCP options configured on this tab will be distributed by the DHCP server to the DHCP clients.

DNS Server Settings (For DHCPv4)

These settings are effective only if a DHCPv4 server is enabled.

Select one of these options:

- **Auto** - This uses the DNS configuration of the appliance as configured in the **Device > DNS** and **Device > Internet** pages.
- **Use the following IP addresses** - Enter the IP addresses for the **First DNS server**, **Second DNS server**, and **Third DNS server**.

Default Gateway

Select one of these options:

- **Use this gateway's IP address as the default gateway**
- **Use the following IP address** - Enter an IP address to use as the default gateway.

WINS

Select one of these options:

- **Use the WINS servers configured for the internet connection**
- **Use the following WINS servers** - Enter the IP addresses of the **First** and **Second** WINS servers.

Lease section

- **Lease time** - Configure the timeout in hours for a single device to retain a dynamically acquired IP address.

Other Settings

You can optionally configure these additional parameters so they will be distributed to DHCP clients:

- **Time servers**
- **Call manager**
- **TFTP server**
- **TFTP boot file**
- **X-Windows display manager**
- **Avaya IP phone**
- **Nortel IP phone**
- **Thomson IP phone**

Custom Options

Lets you add custom options that are not listed above. For each custom option, you must configure the name, tag, type, and data fields.

Configuring a Hotspot

In the **Device > Hotspot** page, if a network interface was defined for hotspot, you can configure:

- Guest access - A session is created for an IP address when a user accepts terms or authenticates in the Hotspot portal. The session expires after the configured timeout (240 minutes by default).
- Hotspot portal - Customize the portal's appearance.
- Hotspot exceptions - Define specified IP addresses, IP ranges or networks to exclude from the Hotspot.

If no network interface was defined for the Hotspot, click **Configure in Local Network**.

In the Access section of the page, you can configure if authentication is required and allow access to all users or to a specified user group (Active Directory, RADIUS or local).

Hotspot is automatically activated in the system.

To turn off Hotspot:

1. Go to **Device > Advanced Settings**.
2. Search for Hotspot and double-click the entry.
3. Select **Disabled**.
4. Click **Apply**.

To configure Hotspot for an interface:

1. Click **Configure in Local Network**.
The **Local Network** window opens.
2. Select interface and click **Edit**.
The **Edit <interface>** window opens.
3. Select **Use Hotspot**.
4. Click **Apply**.

Any user that browses from configured interfaces is redirected to the Check Point Hotspot portal.

To configure Hotspot exceptions:

1. Click **Manage Exceptions**.
The Manage Hotspot Network Objects Exceptions window opens.
2. Select the objects to add as exceptions.
The Selected Network Objects window shows the selected objects. To remove an object from the list, click the **x** next to it.
3. To filter the object list, enter the filter value. The list shows the objects that match the filter.
4. If necessary, click **New** to add new objects to the list. For information on how to create a new object, see the **Users & Objects > Network Objects** page.

5. Click **Apply**.

The added objects are excluded from the Hotspot.

To require user authentication:

1. Select the **Require Authentication** checkbox.
2. You can allow access to **All users** or to a **Specific user group**.
3. If you selected **Specific user group**, enter the group's name in the text box.
4. Click **Apply**.

Any user/user group that browses from configured interfaces is redirected to the Check Point Hotspot portal and must enter authentication credentials.

To configure the session timeout:

1. In **Session timeout**, enter the number of minutes that defines how long a user stays logged in to the session before it ends.
2. Click **Apply**.

To customize the portal appearance:

1. Click **Customize Hotspot portal**.
2. For **Portal title** - Keep the default or enter a different title.
3. For **Portal message** - Keep the default or enter a different message.
4. For **Terms of use** - Select this checkbox to add an "I agree with the following terms and conditions" checkbox on the Hotspot portal page. Enter the terms and conditions text in the text box. When users click the "terms and conditions" link, this text shows.
5. To customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness), click **Upload**, browse to the logo file and click **Apply**. If necessary, click **Use Default** to revert to the default logo.
6. Click **Apply**.

To prevent simultaneous login to the Hotspot portal:

1. Go to **Device > Advanced Settings**.
2. Select **Hotspot**.
3. Click **Edit**.

The **Hotspot** window opens.

4. Click the checkbox for **Prevent simultaneous login**.
5. Click **Apply**.

The same user cannot log in to the Hotspot portal from more than one computer at a time.

On the **Active Devices** page (available through the **Home** and **Logs & Monitoring** tabs), you can revoke Hotspot access for connected users.

Configuring the Routing Table

The **Device > Routing** page shows routing tables with the routes added on your appliance.

On this page:

- You can add or edit routes and configure manual routing rules. You cannot edit system defined routes.
- You can specify routes for and associate IP addresses with selected VPN tunnels. To add, delete, and modify the IP addresses, use dynamic routing protocols.

For every route:

Table Columns	Description
Destination	The route rule applies only to traffic whose destination matches the destination IP address/network.
Source	IPv4 only. The route rule applies only to traffic whose source matches the source IP address/network.
Service	IPv4 only. The route rule applies only to traffic whose service matches the service IP protocol and ports or service group.
Next Hop	The next hop gateway for this route, with these options: <ul style="list-style-type: none"> ■ Specified IP address of the next hop gateway. ■ Specified Internet connection from the connections configured in the appliance. ■ Specified VPN Tunnel Interface (VTI)/
Metric	Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is selected.

To add a new static route (IPv4 addresses):

1. In **Device > Routing**, above the **Routing Table**, click **New**.

The **New Routing Rule** window opens with this message: Traffic from **any source** to **any destination** that belongs to **any service** should be routed through the **next hop**.

2. Click **next hop** and select an option in the new window that opens:
 - **IP Address** - Enter the IP address.
 - **Internet connection** - Select an internet connection.
 - **VPN Tunnel (VTI)** - Select the VPN Tunnel.

3. Click **OK**.

4. Click **any source** and select an option in the new window that opens:
 - **Any**
 - **Specified IP address** - Enter the **IP Address** and **Mask**
5. Click **any destination** and select an option in the new window that opens:
 - **Any**
 - **Specified IP address** - Enter the **IP Address** and **Mask**
6. Click **OK**.
7. Click **any service** and select a service name or enter a service name in the search field. You can create a new service or service group.

Note - Static routes are not supported for source based or service based routes using VTI (VPN).
8. **Optional** - Enter a comment.
9. Enter a **Metric** between 0 and 100. The default is 0.
10. Click **Apply**.

To configure a default route:

1. Go to **Device > Local Network** page.
2. Select an interface and click **Edit**.

The **Edit** window opens in the **Configuration** tab.
3. Click the **DHCP Server options** tab.
4. In the **Default Gateway** section,
 - Click **Use this gateway's IP address as the default gateway**.
 - Or
 - Select **Use the following IP address** and enter an IP address.
5. Click **Apply**.

To edit a default route:

1. In **Device > Internet**, click the Internet connection.
2. Click **Edit**.

The **Edit Internet Connection** window opens in the **Configuration** tab.
3. Set the **Default gateway** (next hop) to a different IP address.
4. Click **Apply**.

When no default route is active, this message shows: "Note - No default route is configured. Internet connections might be down or not configured."

For Internet Connection High Availability, the default route changes automatically on failover (based on the active Internet connection).

When a network interface is disabled, all routes that lead to it show as **inactive** in the routing page. A route automatically becomes active when the interface is enabled. Traffic for an inactive route is routed based on active routing rules (usually to the default route).

The edit, delete, enable, and disable options (on the **Device > Local Network** page) are only available for manually defined routing rules created on this page. You cannot edit, delete, enable, and disable routing rules created by the operating system for directly attached networks or rules defined by the dynamic routing protocol.

To edit an existing route:

Select the route and click **Edit**.

To delete an existing route:

Select the route and click **Delete**.

To enable/disable an existing route:

Select the route and click **Enable** or **Disable**.

Configuring MAC Filtering

MAC Filtering lets you manage a whitelist of MAC addresses that can access the LAN. All others are blocked. The list is global for all interfaces defined on physical LAN ports.

Note - This feature is currently not supported but will be in later versions.

To enable MAC filtering:

1. Turn the slider to **ON**.
2. Add a MAC address to the LAN MAC Filter whitelist.

Note - MAC filtering is not active when no MAC addresses are defined.

After MAC filtering is enabled, you can disable the feature for specified networks.

To edit the LAN MAC Filter whitelist:

1. Go to **Device > MAC Filtering > LAN MAC Filter**.
2. To add a new MAC Address, click **Add > New**.
3. To select MAC addresses from the list of Active Devices, click **Add > Select**.
4. To edit a MAC address, select it from the list and click **Edit**.
5. To delete a MAC address, select it from the list and click **Delete**.

To disable MAC filtering for a specific interface:

1. Go to **Device > Local Network**.
2. Select a LAN interface and click **Edit**
The Edit LAN window opens.
3. Click **Advanced**.
4. Select **Disable MAC filtering**.
To enable, clear this option.
5. Click **Apply**.

Limitations

- MAC filtering is not supported on external interfaces and over switches between physical LAN ports (port-based VLANs). If you configure a physical switch between multiple LAN ports, you cannot activate MAC filtering on this network. Replace the switch with a bridge configuration.
- To disable MAC filtering for a bridged LAN interface, you must reboot.
- Traffic from a remote encryption domain is not MAC filtered.
- Broadcast traffic such as ARP and DHCP is not blocked.
- To configure MAC filtering for a DMZ interface, you must use CLI. You cannot configure MAC filtering in the WebUI.

Note - DMZ is not supported in 1550 appliances.

802.1x Authentication Protocol

IEEE 802.1x is a port-based network access protocol that provides an authentication mechanism for devices that are physically attached to the network.

802.1x authentication is enabled only when you define a LAN or a DMZ network as a separate network and a RADIUS server is defined.

Workflow

1. Configure a RADIUS Server. See ["Managing Authentication Servers" on page 222](#).
2. Define it on the appliance
3. Activate 802.1x authentication on a separate LAN interface (includes the DMZ when not used as an internet connection), or a tag-based VLAN interface defined on one of the LAN physical ports.

If you configure a physical switch (port-based VLAN) between multiple LAN ports, you cannot activate the 802.1x protocol on this network. Replace the switch with a bridge configuration.

To enable 802.1x authentication on a separate LAN interface:

1. Go to **Device > Local Network**.
2. Select the LAN interface and click **Edit**.
The **Edit** window opens in the **Configuration** tab.
3. For **Assigned to**: select **Separate network**.
4. In the **Advanced** tab, select **Activate 802.1x authentication**.
5. Enter a time for **Re-authentication frequency (in seconds)**.
6. Click **Apply**.

To enable 802.1x authentication on a tag based VLAN interface:

1. Go to **Device > Local Network**.
2. Select the LAN and click **New > VLAN**.
The **New VLAN** window opens in the **Configuration** tab.
3. For **Assigned to**: select the LAN ID.
4. In the **Advanced** tab, select **Activate 802.1x authentication**.
5. Enter a time for **Re-authentication frequency (in seconds)**.
6. Click **Apply**.

To disable 802.1x authentication on an interface:

1. Go to **Device > Local Network**.
Select the LAN interface and click **Edit**.
2. The **Edit** window opens in the **Configuration** tab.
3. Click the **Advanced** tab.

4. Clear **Activate 802.1x authentication**.
5. Click **Apply**.

To configure logging for MAC filtering and 802.1x authentication:

1. Go to **Device > Advanced Settings**.
2. Set the value of the **MAC Filtering settings - Log blocked MAC addresses** attribute to
 - **Enabled** - To enable logging
 - **Disabled** - To disable logging.

Note - This attribute is available only in Locally Managed mode. In Centrally Managed mode, configure logging with CLI.

3. **Optional** -
 - To reduce the number of logs, specify the value of the **MAC Filtering settings - Log suspension** attribute in seconds.
 - To show all logs, set the value to "0".

Note - Traffic dropped in the WiFi driver is not logged.

Configuring the DNS Server

In the **Device > DNS** page you can configure the DNS server configuration and define the domain name.

To configure DNS:

1. Select to define up to three DNS servers which is applied to all Internet connections or use the DNS configuration provided by the active Internet connection (Primary).

If you select **Configure DNS servers**, make sure that you enter valid IP addresses.

Use the first option if your DNS servers are located in the headquarters office. In this case, all DNS requests from this branch office are directed to these DNS servers.

The second option allows a more dynamic definition of DNS servers. The gateway uses the DNS settings of the currently-active Internet connection (in case of static IP - the DNS manually provided under "Internet connection" -> Edit, in case of DHCP / Dialers - the DNS automatically provided by the ISP). If Internet Connection High Availability is enabled, the DNS servers switch automatically upon failover.

2. By default, the Check Point Appliance functions as your DNS proxy and provides DNS resolving services to internal hosts behind it (network objects). This option is global and applies to all internal networks.

To get IP addresses directly from the DNS servers defined above, clear the **Enable DNS Proxy** checkbox.

When DNS proxy is enabled, **Resolve Network Objects** controls if the DNS proxy treats the local network objects as a **hosts list**. When selected, the local DNS servers resolves network object names to their IP addresses for internal network clients.

3. Enter a **Domain Name**. There are two separate uses of the domain name:
 - Local hosts (the Security Gateway and network objects) are optionally appended with the domain name when DNS resolving is performed.
 - DNS queries that do not contain a domain name are automatically appended with the domain name.

Note these syntax guidelines:

- The domain name must start and end with an alphanumeric character.
- The domain name can contain periods, hyphens, and alphanumeric characters.

4. Click **Apply**.

Configuring the Proxy Server

In the **Device > Proxy** page, you can configure a proxy server to use to connect to the Check Point update and license servers.

To configure a proxy server:

1. Select **Use a proxy server**.
2. Enter a **Host name or IP address**.
3. Enter a **Port**.
4. Click **Apply**.

Backup, Restore, Upgrade, and Other System Operations

In the **Device > System Operations** page you can:

- Reboot
- Restore factory default settings
- Revert to the factory default image and settings
- Automatically or manually upgrade the appliance firmware to the latest Check Point version
- Revert to earlier firmware image
- Backup appliance settings to a file stored on your desktop computer
- Restore a backed up configuration

To reboot the appliance:

1. Click **Reboot**.
2. Click **OK** in the confirmation message.

To restore factory default settings:

1. Click **Default Settings**.
2. Click **OK** in the confirmation message.

The factory default settings are restored. The appliance reboots to complete the operation.

Note - This does not change the software image. Only the settings are restored to their default values (IP address `https://192.168.1.1:4434`, the username: admin and password: admin).

To revert to the factory default image:

1. Click **Factory Defaults**.
2. Click **OK** in the confirmation message.

The factory default settings are restored. The appliance reboots to complete the operation.

Note - This restores the default software image which the appliance came with and also the default settings (IP address `https://192.168.1.1:4434`, the username: admin and password: admin).

To make sure you have the latest firmware version:

Click **Check now**.

To automatically upgrade your appliance firmware when Cloud Services is not configured:

1. Click **Configure automatic upgrades**.
The Automatic Firmware Upgrades window opens.
2. Click **Perform firmware upgrades automatically**.

3. Select the upgrade option to use when new firmware is detected:
 - Upgrade immediately
 - Or
 - Upgrade according to this frequency.
4. If you selected **Upgrade according to this frequency**, select one of the **Occurs** options:
 - **Daily** - Select the Time of day.
 - **Weekly** - Select the Day of week and Time of day.
 - **Monthly** - Select the Day of month and Time of day.
5. Click **Apply**.

Notes:

- When a new firmware upgrade is available, a note shows the version number. Click **Upgrade Now** to upgrade it immediately, or click **More Information** to see what is new in the firmware version.
- If the gateway is configured by Cloud Services, automatic firmware upgrades are locked. They can only be set by Cloud Services.

To manually upgrade your appliance firmware:

1. Click **Manual Upgrade**.
The Upgrade Software Wizard opens.
2. Follow the Wizard instructions.

Note - The firewall remains active while the upgrade is in process. Traffic disruption can only be caused by:

- Saving a local image before the upgrade (this causes the Firewall daemon to shut down). This may lead to disruption in VPN connections.
- The upgrade process automatically reboots the appliance.

To revert to an earlier firmware image:

1. Click **Revert to Previous Image**.
2. Click **OK** in the confirmation message.
The appliance reboots to complete the operation.

To backup appliance settings:

1. Click **Backup**.
The **Backup Settings** page opens.
2. To encrypt the backup file, select the **Use File Encryption** checkbox. Set and confirm a password.
3. To back up the security policy installed on the appliance, select the **Backup Security Policy** checkbox. You can add **Comments** about the specific backup file created.

4. Click **Save Backup**. The File Download dialog box appears. The file name format is <current software version>-<YY-Month-day>-<HH_MM_Seconds>.zip
5. Click **Save** and select a location.

To restore a backed up configuration:

1. Click **Restore**. The Restore Settings page appears.
2. Browse to the location of the backed up file.
3. Click **Upload File**.

Important Notes

- To *replace* an existing appliance with another one (for example, upon hardware failure) you can restore the settings saved on your previous appliance and reactivate your license (through **Device > License**).
- To *duplicate* an existing appliance you can restore the settings of the original appliance on the new one.
- Restoring settings of a different version is supported, but not automatically between every two versions. If the restore action is not supported between two versions, the gateway does not allow you to restore the settings.

Using the Software Upgrade Wizard:

Follow the instructions in each page of the Software Upgrade Wizard.

During the wizard click **Cancel** to quit the wizard.

Welcome

Click the **Check Point Download Center** link to download an upgrade package as directed. If you already downloaded the file, you can skip this step.

Upload Software

Click **Browse** to select the upgrade package file.

Click **Upload**. This may take a few minutes. When the upload is complete, the wizard automatically validates the image. A progress indicator at the bottom of the page tells you the percentage completed. When there is successful image validation, an "Upload Finished" status shows.

Upgrade Settings

The system always performs an upgrade on a separate flash partition and your current-running partition is not affected. You can always switch back to the current image if there is an immediate failure in the upgrade process. If the appliance does not come up properly from the boot, disconnect the power cable and reconnect it. The appliance automatically reverts to the previous image.

Click the **Revert to Previous Image** button on the System Operations page to return to an earlier image. The backup contains the entire image, including the firmware, all system settings and the current security policy.

When you click **Next**, the upgrade process starts.

Upgrading

The Upgrading page shows an upgrade progress indicator and checks off each step as it is completed.

- Initializing upgrade process
- Installing new image

Backing up the System

In the **Device > System Operations** page you can backup and restore system settings.

To create a backup file:

1. Click **Create Backup File**.

The **Backup Settings** window opens.

2. To encrypt the file, click **Use file encryption**.

If you select this option, you must enter and confirm a password.

3. **Optional** - Add a comment about the backup file.

4. Click **Create Backup**.

System settings are backed up.

The backup file includes all your system settings such as network settings and DNS configuration. The backup file also contains the Secure Internal Communication certificate and your license.

If you want to *replace* an existing appliance with another one, you can restore the settings of your previous appliance and re-activate your license (through **License Page > Activate License**).

If you want to *duplicate* an existing appliance, you can restore the settings of the original appliance on the new one. Make sure to change the IP address of the duplicated appliance (**Device > Internet** page) and generate a new license.

To configure a periodic backup to the FTP server:

1. Go to **Device > System Operations > Backup and Restore System Settings**.
2. Click **Settings**.

The **Periodic Backup Settings** window opens.

3. Click **Enable scheduled backups**.
4. Configure the file storage destination (see below).
5. **Optional** - Select **Use file encryption**.

If you select this option, you must enter and confirm a password.

6. In **Schedule Periodic Backup**, select frequency:
 - **Daily** - Select time of day (hour range).
 - **Weekly** - Select day of week and time of day.
 - **Monthly** - Select day of month and time of day. **Note** - If a month doesn't include the selected day, the backup is executed on the last day of the month.
7. Click **Apply**.

To configure a file storage destination:

1. In **Device > System Operations > Backup and Restore System Settings**, click **Settings**.
The **Periodic Backup Settings** window opens.
2. Click **Enable scheduled backups**.
3. Enter a **Backup server path**.
4. Enter a username and password.
5. Click **Apply**.

Configuring Local and Remote System Administrators

The **Device > Administrators** page lists the Check Point Appliance administrators and lets you:

- Create new local administrators.
- Configure the session timeout.
- Limit login failure attempts.
- Generate a QR code to connect the mobile application with the appliance for the first time.

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

Administrator Roles:

- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the **Tools** page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.
- **Mobile Administrator** - Mobile administrators are allowed all networking operations on all interfaces. They can change their own passwords, generate reports, reboot, change events and mobile policy, active hosts operations and pairing. They cannot login from or access the WebUI.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.

To create a local administrator:

1. Click **New**.

The **Add Administrator** page opens.

2. Configure the parameters (name, password, and password confirmation). The hyphen (–) character is allowed in the administrator name. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ' " # + \
3. Select the **Administrator Role**.
4. Click **Apply**.

The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

To edit the details of locally defined administrators:

1. Select the administrator from the table and click **Edit**.
2. Make the relevant changes.
3. Click **Apply**.

To delete a locally defined administrator:

1. Select an administrator from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

Note - You cannot delete an administrator who is currently logged in.

To allow access for administrators defined in a remote RADIUS server:

1. Make sure administrators are defined in the remote RADIUS server.
2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.
3. When you have a configured RADIUS server, click **Edit permissions**.

The **RADIUS Authentication** window opens.

4. Click the **Enable RADIUS authentication for administrators** checkbox.

Use roles defined on RADIUS server is selected by default.

5. Configure the role for each user on the RADIUS server. See additional details below.

Note - A user without role definition will get a login error.

6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:
 - Super Admin
 - Read only
 - Networking Admin
 - Mobile Admin
7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
8. Click **Apply**.

To set the Session Timeout value for both local and remotely defined administrators:

1. Click **Security Settings**.

The **Administrators Security Settings** window opens.

2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.
3. To limit login failure attempts, click the **Limit administrators login failure attempts** checkbox.
4. Enter the number of **Maximum consecutive login attempts** allowed before an administrator is locked out.
5. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.
6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.
7. Click **Apply**.

Note - This page is available from the **Device** and **Users & Objects** tabs.

To connect the mobile application with the appliance for the first time:

1. Click **Mobile Pairing Code**.

The **Connect Mobile Device** window opens.

2. Select an administrator from the pull down menu.
3. Click **Generate**.

This generates a QR code to connect the Check Point WatchTower mobile application with the appliance for the first time.

For more information about the mobile application, see the [Check Point SMB WatchTower App User Guide](#).

Configuring a RADIUS Server for non-local Check Point Appliance users:

Non-local users can be defined on a RADIUS server and not in the Check Point Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

Note - The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.

Note - If you define a RADIUS user with a null password (on the RADIUS server), the appliance cannot authenticate that user.

To configure a Steel-Belted RADIUS server for non-local appliance users:

1. Create the dictionary file `checkpoint.dct` on the RADIUS server, in the default dictionary directory (that contains `radius.dct`). Add these lines in the `checkpoint.dct` file:

```
@radius.dct
MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2 data=%s%]
ATTRIBUTE CP-Gaia-User-Role CheckPoint-VSA(229, string) r
ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-VSA(230, integer) r
```

2. Add these lines in the `vendor.ini` file on the RADIUS server (keep in alphabetical order with the other vendor products in this file):

```
vendor-product = Check Point Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add this line in the `dictionary.dcm` file:

```
"@checkpoint.dct"
```

4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

```
CP-Gaia-User-Role = <role>
```

Where `<role>` allowed values are:

Administrator Role	Value
Super Admin	adminRole
Read only	monitorrole
Networking Admin	networkingrole
Mobile Admin	mobilerole

To configure a FreeRADIUS server for non-local appliance users:

1. Create the dictionary file `dictionary.checkpoint` in the `/etc/freeradius/` on the RADIUS server.

Add these lines in the `dictionary.checkpoint` file:

```
#Check Point dictionary file for FreeRADIUS AAA server
VENDOR CheckPoint 2620
ATTRIBUTE CP-Gaia-User-Role 229 string
CheckPoint
ATTRIBUTE CP-Gaia-SuperUser-Access 230 integer
CheckPoint
```

2. Add this line in the `/etc/freeradius/dictionary` file

```
"$INCLUDEdictionary.checkpoint"
```

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

```
CP-Gaia-User-Role = <role>
```

Where *<role>* is the name of the administrator role that is defined in the WebUI.

Administrator Role	Value
Super Admin	adminRole
Read only	monitorrole
Networking Admin	networkingrole
Mobile Admin	mobilerole

To configure an OpenRADIUS server for non-local appliance users:

1. Create the dictionary file `dict.checkpoint` in the `/etc/openradius/subdicts/` directory on the RADIUS server:

```
# Check Point Gaia vendor specific attributes
# (Formatted for the OpenRADIUS RADIUS server.)
# Add this file to etc/openradius/subdicts/ and add the line
# "$include subdicts/dict.checkpoint" to
/etc/openradius/dictionaries
# right after dict.ascend.
$add vendor 2620 CheckPoint
$set default vendor=CheckPoint
    space=RAD-VSA-STD
    len_ofs=1 len_size=1 len_adj=0
    val_ofs=2 val_size=-2 val_type=String
    nodec=0 noenc=0
$add attribute 229 CP-Gaia-User-Role
$add attribute 230 CP-Gaia-SuperUser-Access val_type=Integer
val_size=4
```

2. Add this line in the `/etc/openradius/dictionaries` file immediately after `dict.ascend`:

```
$include subdicts/dict.checkpoint
```


3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

```
CP-Gaia-User-Role = <role>
```

Where *<role>* is the name of the administrator role that is defined in the WebUI.

Administrator Role	Value
Super Admin	adminRole
Read only	monitorrole
Networking Admin	networkingrole
Mobile Admin	mobilerole

To log in as a Super User:

A user with super user permissions can use the Check Point Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Check Point Appliance platform over SSH or serial console.
2. Log in to the Gaia Gaia Clish shell with your user name and password.
3. Run: `expert`
4. Enter the Expert mode password.

Configuring Administrator Access

The **Device > Administrator Access** page lets you configure the IP addresses and interface sources that administrators can use to access the Check Point Appliance. You can also configure the Web and SSH ports.

First set the interface sources from which allowed IP addresses can access the appliance.

To set the interface sources from which administrator access is allowed:

Select one or more of the options:

- **LAN** - All internal physical ports
- **Trusted wireless** - Wireless networks that are allowed access to the LAN by default (only in Wireless Network models.)
- **VPN** - Uses encrypted traffic through VPN tunnels from a remote site or uses a remote access client
- **Internet** - Clear traffic from the Internet (not recommended to allow access from all IP addresses)

To allow administrator access from any IP address:

1. Select the **Any IP address** option. This option is less secure and not recommended. We recommend you allow access from the Internet to specific IP addresses only.
2. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
3. Click **Apply**. An administrator can access the Check Point Appliance using any IP address through the allowed interface sources.

To allow administrator access from specified IP addresses:

1. Select the **Specified IP addresses only** option.
2. Click **New**.
The **IP Address Configuration** page shows.
3. Select **Type**:
 - IPv4 address
 - IPv4 network
4. Enter the IP address or click **Get IP from My Computer**.
5. Click **Apply**.

The IP address is added to the table.

6. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
7. Click **Apply**. An administrator can access the Check Point Appliance using the configured IP addresses through the allowed interface sources.

To allow administrator access from both specified and any IP addresses:

Select this option when it is necessary to allow administrator access from the Internet (you must define the specified IP addresses). Access from other sources is allowed from any IP address.

1. Select the Internet source checkbox.
2. Select the **Specified IP addresses from the internet and any IP address from other sources** option.
3. Click **New**.

The **IP Address Configuration** page shows.

4. Select **Type**:
 - IPv4 address
 - IPv4 network
5. Enter the IP address or click **Get IP from My Computer**.
6. Click **Apply**.

The IP address is added to the table.

7. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
8. Click **Apply**. An administrator can access the Check Point Appliance using the configured IP addresses through the allowed interface sources.

To delete administrator access from a specific IP address:

1. Select the IP Address you want to delete from the IP Address table.
2. Click **Delete**.

Important Notes:

- Configuring different access permissions for LAN and Internet is not supported when your Internet Connection is configured in bridge mode (the option **Allow administration access from** does not show Internet or LAN).
- An automatic implied rule is defined to allow the access specified here. There is no need to add an explicit rule in the Access Policy page to allow this access.
- When you block the IP address or the interface group through which you are currently connected, you are not disconnected immediately. The access policy is applied immediately, but your current session remains active until you log out.

Managing Device Details

On the **Device > Device Details** page, you can:

- Enter an **Appliance Name** to identify the appliance.
Note - The appliance name can only contain alphanumeric characters and the hyphen character. Do not use the hyphen as the first or last character.
- **For wireless devices only** - Configure the **Country**. The allowed wireless radio settings vary based on the standards in each country.
- Assign a Web portal certificate.

To assign a Web portal certificate:

1. Click the downward arrow next to the **Web portal certificate** field.
The list of uploaded certificates shows.
2. Select the desired certificate.
Note - You cannot select the default VPN certificate.
3. Click **Apply**.
4. Reload the page.

Managing Date and Time

The **Device > Date and Time** page shows the current system time and lets you define the Check Point Appliance date and time, optionally using NTP.

To manually configure date and time:

1. Select the **Set Date and Time Manually** option.
2. Enter the current **Date** and **Time**. Click the calendar icon to enter the date. Specify whether the time is AM or PM.
3. Click **Apply**.

To use Network Time Protocol (NTP) to synchronize the clocks of computers on the network:

1. Select the **Set Date and Time Using a Network Time Protocol (NTP) Server** option.
2. Enter the Host name or IP addresses of the **Primary NTP Server** and **Secondary NTP Server**. If the Primary NTP Server fails to respond, the Secondary NTP Server is queried.
3. Set the **Update Interval (minutes)** field.
4. Select the **NTP Authentication** checkbox if you want to supply a **Shared Secret** and a **Shared Secret Identifier** (this is optional). You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ' " # + \
5. Click **Apply**.

Time Zone

1. From the **Local Time Zone** list, select the correct time zone option.
2. Select the **Automatically adjust clock for daylight saving changes** checkbox to enable automatic daylight saving changes.
3. Click **Apply**.

Configuring DDNS and Access Service

In the **Device > DDNS & Device Access** page, you can:

- Configure DDNS account details in one of the supported providers.
- Configure a service that lets you remotely connect to the appliance in instances where it is behind NAT, a firewall, or has a dynamically assigned IP address.

DDNS

When you configure DDNS, the appliance updates the provider with its IP addresses. Users can then connect to the device with a host name from the provider instead of IP addresses.

This is especially important for remote access users who connect to the device to the internal network through VPN.

To configure DDNS:

1. Select **Connect to the appliance by name from the Internet (DDNS)**.
2. Enter the details of your account on the page:
 - **Provider** - Select the DDNS provider that you set up an account with.
 - **User name** - Enter the user name of the account.
 - **Password** - Enter the password of the account. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | \ " # + \
 - **Host name** - Enter your routable host name as defined in your DDNS account.

For more information about these details, refer to your provider's website.

3. Make sure **Reinitialize internal certificates** is selected. When you enable this feature or change settings, you must reinitialize the internal certificates for them to be valid for the new DNS.

Reach My Device

Reach My Device lets you remotely connect to the appliance from the Internet so that you can use the WebUI or CLI when necessary. This is done by tunneling the administrative UI or CLI connections through a Check Point Cloud Service. Such configuration is very useful in instances where the appliance is behind a NAT device or firewall, and cannot be reached directly. In addition, the feature makes it easier to access an appliance with a dynamically assigned IP address.

To register to the Reach My Device service:

1. Click **Register**.
The Reach My Device window opens.
2. For **Host Name**, use the default host name or enter a name for this Check Point Appliance to enable remote access.
3. If the host name was already defined, select **Register with an existing homename** and enter the **Validation token** of the gateway. This token verifies that an existing name belongs to this appliance owner.

4. Click **Apply**.

The validation token, web link, and shell link are shown on the page.

5. Go to **Device > Administrator Access**. Configure **Internet** as a source for administrator access and **Set specified IP addresses**.

When the gateway participates in VPN, you can exclude the WAN interface (or any other interface used for the Internet connection) from the encryption domain and use Reach My Device traffic without a VPN tunnel.

In the **VPN Site to Site global settings Advanced Setting**, enable **Do not encrypt connections originating from the local gateway**.

How to access the gateway with the Reach My Device service:

When registration is complete, an outgoing tunnel to the Check Point Cloud Service is established with the appliance's IP address.

Remote Access to the WebUI

Web Link - Use this URL in a browser to remotely access the appliance. For example: `https://mygateway-web.smbrelay.checkpoint.com`. When the login page shows, enter the applicable user name and password.

Remote Access to the CLI

Shell Link - Use this URL in a browser to open an SSH connection to the appliance to use CLI commands. For example: `https://mygateway-shell.smbrelay.checkpoint.com`. Enter the administrator credentials.

Using System Tools

See ["Using System Tools" on page 48](#).

Managing Installed Certificates

On the **Installed Certificates** page, you can create and manage appliance certificates or upload a P12 certificate. Uploaded certificates and the default certificates are displayed in a table. To see certificate details, click the certificate name.

You can upload a certificate signed by an intermediate CA or root CA. All intermediate and root CAs found in the P12 file are automatically uploaded to the trusted CAs list.

Note - This page is available from the **Device** and **VPN** tabs.

On the **VPN Remote Access Blade Control** page, after you enable the SSL VPN feature, you can select and assign a certificate from the list of the installed certificates (with the exception of the Default Web Portal certificate). You can also do this on the **Remote Access Advanced** tab.

On the **Device > Device Details** page, you can select and assign a Web portal certificate from the list of installed certificates (with the exception of the Default certificate).

Installed certificates are used in site-to-site VPN, SSL VPN, and the Web portal.

When Cloud Services is turned on and the appliance is configured by Cloud Services, the Cloud Services Provider certificate is downloaded automatically to the appliance. The Cloud Services Provider certificate is used by community members configured by Cloud Services. **Note** - If you turn Cloud Services off, the Cloud Services Provider certificate is removed.

These are the steps to create a signed certificate:

1. Create a signing request.
2. Export the signed request (download the signing request from the appliance).
3. Send the signing request to the CA.
4. When you receive the signed certificate from the CA, upload it to the appliance.

To create a new certificate to be signed by a CA:

1. Click **New Signing Request**. The New Certificate Request window opens.
2. Enter a **Certificate** name.
3. In the **Subject DN** enter a distinguished name (e.g. CN=myGateway).
4. **Optional** - to add alternate names for the certificate, click **New**. Select the **Type** and enter the **Alternate name** and click **Apply**.
5. Click **Generate**.

The new signing request is added to the table and the status shows "Waiting for signed certificate".

Note - You cannot edit the request after it is created.

If the new signing request is signed by the Internal CA and the Organization Name is not defined in the DN, the Internal CA automatically generates the Organization Name.

To export the signing request:

Click **Export**.

To upload the signed certificate when you receive the signed certificate from the CA:

1. Select the signing request entry from the table.
2. Click **Upload Signed Certificate**.
3. Browse to the signed certificate file (*.crt).
4. Click **Complete**.

The status of the installed certificate record changes from "Waiting for signed certificate" to "Verified".

To upload a P12 file:

1. Click **Upload P12 Certificate**.
2. Browse to the file.
3. Edit the **Certificate name** if necessary.
4. Enter the certificate **password**.
5. Click **Apply**.

Managing Internal Certificates

In the **Certificates Internal Certificate** page you can view details of an internal VPN certificate. You can also view and reinitialize the certificate used by the internal CA that signed the certificate and can be used to sign external certificates.

Note - This page is available from the **Device** and **VPN** tabs.

When you create an internal VPN certificate, when a certificate that is signed by the internal CA is used, the CA's certificate must be reinitialized when the Internet connection's IP addresses change.

To avoid constant reinitialization, we recommend you use the DDNS feature. See **Device > DDNS**. When DDNS is configured, you only need to reinitialize the certificate once. Changes in the DDNS feature configuration by default automatically reinitialize certificates.

To reinitialize certificates:

1. Click **Reinitialize Certificates**.

The Reinitialize Certificates window opens.

2. Enter the **Host/IP address**.

Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.

3. Select the number of years for which the Internal VPN Certificate is valid. The default is 3. The maximum value allowed is 20.
4. Click **Apply**.

Note - The internal VPN certificate expiration date cannot be later than the CA expiration date.

To replace an internal CA certificate:

1. Click **Replace Internal CA Certificate**.

The Upload a P12 Certificate window opens.

2. Click **Browse** to select the CA certificate file that includes the private key.
3. Enter the **Certificate name** and private key's password to allow the device to sign certificates with the uploaded CA.
4. Enter the **Host/IP address**.

Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.

5. Click **Apply**.

To export an internal CA certificate:

Click **Export Internal CA Certificate** to download the internal CA certificate.

To sign a remote site's certificate request by the internal CA:

1. Click **Sign a Request**. A file upload window opens.
2. Click **Browse** to upload the signing request file as created in the remote site. In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.
3. Click **Download**. The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

Configuring High Availability

In the **Device > High Availability** page you can create a cluster of two appliances for high availability.

Note - You cannot create a cluster when you have a switch or bridge defined in your network settings on the appliance. If necessary, change network settings in the **Device > Local Network** page.

After you define a cluster, you can select to **Enable** or **Disable** the cluster.

The page shows the configured interfaces for monitoring or high availability enabled in a table, where you can edit them.

Interface options in cluster mode:

- **High Availability** - Two physical interfaces in 2 cluster members act as a single interface toward the network, using a single virtual IP address.
Note - In this cluster solution, each interface has a local IP address in addition to the shared single virtual IP address.
- **Sync** - Two physical interfaces must be defined as Sync interfaces and connected between the members to allow proper failover as needed. The default is to use LAN2/Sync physical port.
- **Non HA** (also called **private**) - The physical interface in this member does not participate in High Availability functions.
- **Monitored** (also called **private monitored**) - The physical interface in this member is not coupled with another interface on the other member as in High Availability interface mode. The interface's status is still monitored, and if a problem occurs the member will fail over to the second one.

To change network configuration details of the cluster members:

1. Reset the cluster configuration on the secondary member.
2. Perform the configuration changes on the primary member and click **Reinitialize Trust**.
3. Reconnect the secondary member which fetches the new configuration.

To reset configuration settings:

Click **Reset Cluster Configuration**.

Note - This deletes all configuration settings. You must run the wizard again to configure the cluster.

One member of the cluster is the primary active. The other member is the secondary inactive.

To failover from the primary to the other member:

1. Click **Force Member Down**.
A confirmation message shows.
2. Click **Yes**.

The primary gateway is now the inactive member of the cluster. The secondary gateway is now active.

If you want to disable the secondary gateway, you must failover to the primary.

Note - Only one member of a cluster can be down at a time. For the inactive member, the **Force Member Down** button is now **Disable Force Member Down**.

To failover to the original primary member:

1. Click **Disable Force Member Down**.

A confirmation message shows.

2. Click **Yes**.

The original primary member is now the active member of the cluster.

To see detailed information about the cluster status:

Click **Diagnostics**.

To create a cluster:

1. Click **Configure Cluster**.

The New Cluster Wizard opens.

2. In Step 1: Gateway Priority, select one of the options:

- **Configure as primary member** - If this appliance must be configured first.
- **Configure as secondary member** - If a primary member is already configured and this appliance connects to it.

3. Click **Next**.

4. For a primary member:

- a. In Step 2: SIC Settings, enter a **password** and **confirm** it. This password is used for establishing trust between the members. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ` " # + \
- b. The default Sync interface is LAN2. If it is necessary to change it, click **Advanced** and select a different **Sync Interface**. You can also change the predefined **Sync IP Address** and **Sync IP Subnet**.

Note - Make sure that changes you make here are also made on the other cluster member.

- c. Click **Next**.
- d. In Step 3: Gateway Interfaces (1 out of N), you can define the cluster IP on the related interfaces. Enter the necessary details.

By default, the appliance monitors the interface condition if the interface is enabled for high availability. If there is a failure, it automatically fails over to the secondary cluster member. When the interface is not enabled for high availability, you can select it for monitoring.

- e. Click **Next**. Do step d. again for all related interfaces in your network.

Note - For Internet connections, you can only enable High Availability on Static IP Internet connections. Other types of Internet connections can be used for monitoring only.

5. For a secondary member:

- a. In Step 2: SIC Settings, enter the Secure Internal Communication **password**.
- b. Click **Establish Trust**.

6. Click **Finish**.

When the cluster is successfully configured, you see the status of the members on this page.

After the cluster is configured, when you connect to the cluster IP address you are automatically redirected to the active cluster member. To log in to specified member, you must log in with the member's IP address.

Note that the WebUI of the secondary member (standby member) only has some options available for fine tuning. This is because all cluster management is done from the active member.

Upgrading a cluster member:

- Upgrade each cluster member individually.
- Start with the standby member.
- After upgrade, the appliance automatically reboots.
- Only manual upgrade is supported.

To manually upgrade a cluster:

1. Go to **Device > System Operations**.
2. Click **Manual Upgrade**.
The Upgrade Software Wizard opens.
3. Follow the wizard instructions.

IPv6 address are currently not supported. High Availability cluster only supports IPv6 in dual mode.

Advanced Settings

The **Device > Advanced Settings** page is for advanced administrators or [Check Point Support](#). You can configure values for multiple advanced settings for the various blades.

Important - Changing these advanced settings without fully understanding them can be harmful to the stability, security, and performance of this appliance. Continue only if you are certain that you understand the required changes.

For further details regarding the attributes, consult with [Check Point Support](#) when necessary.

To filter the list of attributes:

1. Enter text in the **Type to filter** field.
The search results are dynamically shown as you type.
2. To cancel the filter, click **X** next to the search string.

To configure the appliance attributes:

1. Select an attribute.
2. Click **Edit**.
The attribute window opens.
3. Configure the settings, or click **Restore Defaults** to reset the attribute to the default settings. For more details on the attributes, see the next sections.
4. Click **Apply**.

To reset all the appliance attributes to the default settings:

1. From the **Advanced Settings** window, click **Restore Defaults**.
The **Confirm** window opens.
2. Click **Yes**.

All appliance attributes are reset to the default settings.

Table: Administrators RADIUS authentication Attributes

Administrators RADIUS authentication Attribute	Description
Local authentication (RADIUS server)	Perform local administrator authentication only if RADIUS server is not configured or is inaccessible.

Table: Aggressive Aging Attributes

Aggressive Aging Attribute	Description
Multiple parameters	<p>Aggressive Aging helps manage the connections table capacity and memory consumption of the firewall to increase durability and stability.</p> <p>Aggressive Aging introduces a new set of short timeouts called aggressive timeouts. When a connection is idle for more than its aggressive timeout it is marked as "eligible for deletion". When the connections table or memory consumption reaches the user defined threshold, Aggressive Aging begins to delete "eligible for deletion" connections, until memory consumption or connections capacity decreases back to the desired level.</p> <p>Aggressive Aging allows the gateway machine to handle large amounts of unexpected traffic, especially during a Denial of Service attack.</p> <p>If the defined threshold is exceeded, each incoming connection triggers the deletion of ten connections from the "eligible for deletion" list. An additional ten connections are deleted with every new connection until the memory consumption or the connections capacity falls below the enforcement limit. If there are no "eligible for deletion" connections, no connections are deleted at that time, but the list is checked after each subsequent connection that exceeds the threshold.</p> <p>Timeout settings are a key factor in memory consumption configuration. When timeout values are low, connections are deleted faster from the table, enabling the firewall to handle more connections concurrently. When memory consumption exceeds its threshold, it is best to work with shorter timeouts that can maintain the connectivity of the vast majority of the traffic.</p> <p>The major benefit of Aggressive Aging is that it starts to operate when the machine still has available memory and the connections table is not entirely full. This way, it reduces the chances of connectivity problems that might have occurred under low-resource conditions.</p>

Table: Aggressive Aging Attributes (continued)

Aggressive Aging Attribute	Description
	<p>To configure Aggressive Aging:</p> <ol style="list-style-type: none"> 1. Select Enable Aggressive Aging of connections when appliance is under load. 2. To log Aggressive Aging events, select Log Aggressive Aging events. The logs are shown in Logs & Monitoring > Security Logs under the IPS blade. 3. Select the checkboxes of the Aggressive Aging Timeouts that you want to enforce and enter the Aggressive Aging timeout. Make sure that the Aggressive timeouts are lower than the default timeouts. The default timeouts can be viewed and configured in the Device > Advanced Settings > Stateful Inspection attributes. <p>To configure when the Aggressive Aging timeouts are enforced:</p> <ol style="list-style-type: none"> 1. Under Aggressive Aging Timeouts are enforced when section, select whether they are enforced if the connections table exceeds a limit, if memory exceeds a limit, or if both exceed their limits. 2. Enter the percentage that you want to define as the limit to either connections table or memory consumption. If you select both, the values in the percentage fields of the other options are applied. Default is 80%, with connections from the "eligible for deletion" list being deleted if either the connections table or memory consumption passes this limit.

Table: Anti-Spam policy Attributes

Anti-Spam Policy Attributes	Description
All mail track	Tracking options for emails that are not considered spam or suspected spam. Tracking such emails can have a performance impact.
Allowed mail track	Tracking options for emails that are manually allowed in the Threat Prevention > Anti-Spam Exceptions page.
Content based Anti-Spam timeout	Indicates the timeout (in seconds) to wait for an answer from the cloud during content-based Anti-Spam inspection.
E-mail size scan	Indicates the maximal size of an email's content to scan (in KB)

Table: Anti-Spam policy Attributes (continued)

Anti-Spam Policy Attributes	Description
IP reputation fail open	Indicates the action to take upon an internal error during Anti-Spam IP reputation test.
IP reputation timeout	Indicates the timeout (in seconds) to wait for an IP reputation test result.
Scan outgoing emails	Scan the content of emails which are sent from the local network to the Internet.
Transparent proxy	Use a transparent proxy for inspected email connections. When disabled, configuration of the proxy address and port is required on client machines.

Table: Anti-Spoofing Attributes

Anti-Spoofing Attribute	Description
Enable global Anti-Spoofing	Indicates if Anti-Spoofing is enabled automatically on all interfaces according to their zone.

Table: Application & URL Filtering Attributes

Application & URL Filtering Attribute	Description
Block when service is unavailable	Indicates if web requests are blocked when the Check Point categorization and widget definitions Online Web Service is unavailable.
Categorize cached and translated pages	Indicates if to perform URL categorization of cached pages and translated pages created by search engines.
Custom App over HTTPS	Indicates whether custom URLs and applications will be matched over HTTPS traffic using SNI field. Important note: as SNI field in HTTPS traffic is browser-dependent and promiscuous, it does not guarantee 100% match.
Enforce safe search	Indicates if the URL Filtering policy overrides the Safe Search settings in the user's browser. Regardless of what the user has selected, the strictest Safe Search settings are applied. Explicitly sexual content is filtered out of the search engine's results.
Fail mode	Indicates the action to take on traffic in case of an internal system error or overload.

Table: Application & URL Filtering Attributes (continued)

Application & URL Filtering Attribute	Description
Track browse time	Shows in logs the total time that users are connected to different sites and applications in an HTTP session
Use HTTP referer header	Indicates if the HTTP "referer" header (originally a misspelling of referrer) is used by the inspection engine to improved application identification.
Web site categorization mode	<p>Indicates the mode that is used for website categorization:</p> <p>Background - Requests are allowed until categorization is complete. When a request cannot be categorized with a cached response, an uncategorized response is received. Access to the site is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is then cached locally for future requests (default). This option reduces latency in the categorization procedure.</p> <p>Hold - Requests are blocked until categorization is complete. When a request cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.</p>

Table: Capacity Optimization Attributes

Capacity Optimization Attribute	Description
Connections hash table size	<p>Indicates the size of the connections hash table in bytes.</p> <p>This value must be an integer that is an exponential power of two and approximately four times the maximum concurrent connections parameter.</p>
Maximum concurrent connections	Indicates the overall maximum number of concurrent connections.

Table: Cloud Services Firmware Upgrade Attributes

Cloud Services Firmware Upgrade Attribute	Description
Service access maximum retries	Indicates the maximum number of retries when failing to upgrade using the service.
Service access timeout until retry	Indicates the time (in seconds) to wait when there is a connection failure to the service before the next retry.

Table: Cluster Attributes

Cluster Attribute	Description
Use virtual MAC	<p>Indicates if a virtual MAC address is used by all members to allow a quicker failover by the network's switch.</p> <p>Using the virtual MAC address:</p> <ul style="list-style-type: none"> ■ Minimizes the potential traffic outage during fail-over. ■ Removes the need to use G-ARPs for NATed IP addresses.

Table: DDNS Attributes

DDNS Attribute	Description
Iterations	Number of DNS updates.

Table: DHCP Relay Attributes

DHCP Relay Attribute	Description
Use internal IP addresses as source	Select Use internal IP addresses as source if DHCP relay packets from the appliance originate from internal IP addresses. This may be required if the DHCP server is located behind a remote VPN site.

Table: Firewall Policy Attributes

Firewall Policy Attribute	Description
Blocked packets action	Action for blocked packets: Drop, reject or automatic (drop from external and reject from internal).
Log implied rules	Produce log records for connections that match implied rules.

Table: General Temporary Directory Size Attributes

General Temporary Directory Size Attribute	Description
General temporary directory size	Controls the size (in MB) of the general temporary directory.

Table: General Temporary Directory Size Attributes (continued)

General Temporary Directory Size Attribute	Description
System temporary directory size	Controls the size (in MB) of the temporary directory that is used by the system.

Table: Hardware Options Attributes

Hardware Options Attribute	Description
Reset to factory defaults timeout	The amount of time (in seconds) that you need to press and hold the factory defaults button on the appliances' back panel to restore to the factory defaults image.

Table: Hotspot Attributes

Hotspot Attribute	Description
Enable portal	Select Disabled to disable the hotspot feature entirely.
Prevent simultaneous log-in	The same user will not be allowed to login via hotspot portal from more than one machine in parallel.

Table: IP Fragments Parameters

IP Fragments Parameters Attribute	Description
Multiple parameters	<p>These parameters let you configure how the appliance handles IP fragments. It can either block fragmented IP packets or drop fragments when a configured threshold is reached.</p> <p>Select one of these options:</p> <ul style="list-style-type: none"> ■ Forbid IP Fragments - Fragmented IP packets are dropped. ■ Allow IP Fragments - Fragmented IP packets are allowed if they do not exceed a configured threshold. When selecting this option, you can configure the maximum number of accepted incomplete packets. You can also configure the timeout (in seconds) for holding unassembled fragmented packets before discarding them.

Table: IPS Additional Parameters

IPS Additional Parameters Attribute	Description
Max ping limit	Indicates the maximal ping packet size that are allowed when the 'Max Ping Size' protection is active.
Non-standard HTTP ports	Enable HTTP inspection on non-standard ports for the IPS blade.

Table: IPS Engine Settings

IPS Engine Settings Attribute	Description
Allow protocol unknown commands	<p>Normally, the IPS engine blocks protocols (e.g. POP3, IMAP,...) commands that it does not recognize.</p> <p>When the advanced setting is set to <code>true</code>, IPS allows the traffic.</p>

Table: IPS Engine Settings (continued)

IPS Engine Settings Attribute	Description
Configure error page options for supported web protections - multiple parameters	<p>Some web based protections can show an error page upon detection. This error page is configurable.</p> <p>The protections that support the error page:</p> <ul style="list-style-type: none"> ■ Malicious Code protector ■ Cross-Site Scripting ■ LDAP Injection ■ SQL Injection ■ Command Injection ■ Directory Traversal ■ Directory Listing ■ Error Concealment ■ HTTP Format Sizes ■ ASCII Only Request ■ ASCII Only Response Headers ■ HTTP Methods <p>Select one of these options that applies to all such protections:</p> <p>Do not show</p> <ul style="list-style-type: none"> ■ Show pre-defined HTML error page - You can configure an HTML page that opens when an attack is detected. To configure the page, go to Advanced Settings > IPS engine settings > HTML error page configuration. ■ Redirect to another URL - Enter a URL to which users are redirected when an attack is detected. You can also select to add an error code that provides more information about the detected attack. This is not recommended because the information can be misused by an attacker.

Table: IPS Engine Settings (continued)

IPS Engine Settings Attribute	Description
HTML error page configuration - multiple parameters	<p>These settings allow you to configure a pre-defined HTML error page that is seen when the error page advanced settings are set to Show pre-defined HTML error page. Select one of these options:</p> <ul style="list-style-type: none"> ■ Logo URL - Optionally enter a URL that leads to your company logo. ■ HTML error page configuration - Shows an error code that provides more information about the detected attack. This is not recommended because the information can be misused by an attacker. ■ Send detailed error code - You can enter manually defined text that is shown in the HTML page. Enter the text in the Description box. For example, "Access denied due to IPS policy violation."

Table: Internal Certificates Setting Attributes

Internal Certificate Settings Attribute	Description
Configure internal CA certificate expiration	The number of years the internal CA certificate is valid. This applies the next time the certificate is re-initialized.

Table: Internet Attributes

Internet Attribute	Description
Reset Sierra USB on LSI error	Indicates whether Sierra type USB modems will be reset when they send an invalid LSI signal

Table: Managed Service Attributes

Managed Services Attribute	Description
Allow seamless administrator access from remote Management Server	Indicates if an administrator can access the appliance from a remote Security Management Server without the need to enter an administrator user name and password.
Show device details in Login	Indicates if appliance details are shown when an administrator accesses the appliance.

Table: Mobile Setting Attributes

Mobile Settings Attribute	Description
Mobile Settings - Notification cloud server URL	Cloud server URL used for sending mobile notifications.
Mobile Settings - Pairing code expiration	Time (in hours) till pairing code is expired. Type: Integer
Mobile Settings - Verify SSL certificate	Verify SSL certificate when sending mobile notification to cloud server

Table: NAT Attributes

NAT Attribute	Description
ARP manual file merge	Indicates, when automatic ARP detection is enabled, to use the ARP definitions in a local file with higher priority. Manual proxy ARP configuration is required for manual Static NAT rules. If a manual ARP configuration is defined in the local.arp file and Automatic ARP configuration is enabled, both definitions are maintained. If there is a conflict between the definitions (the same NAT IP address appears in both), then the manual configuration is used.

Table: NAT Attributes (continued)

NAT Attribute	Description
Multiple parameters - IP Pool NAT	<p>An IP Pool is a range of IP addresses (an Address Range, a network or a group of one of these objects) routable to the gateway. When a connection is opened to a server, the gateway substitutes an IP address from the IP Pool for the source IP address. Reply packets from the server return to the gateway, which restores the original source IP address and forwards the packets to the source.</p> <p>When using IP Pool NAT, select an existing IP address range object. It must be previously defined in the Users & Objects > Networks Objects page. The IP Pool NAT mechanism allocates IP addresses from this range.</p> <p>Use IP Pool NAT for VPN clients connections - Applies to connections from VPN remote access clients to the gateway.</p> <p>Use IP Pool NAT for gateway to gateway connections - Applies to site to site VPN connections.</p> <p>Prefer IP Pool NAT over Hide NAT - Specifies that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.</p> <p>Reuse IP addresses from the Pool for different destinations - Select this option to reuse IP addresses from the Pool for different destinations.</p> <p>Unused addresses interval - Configure in minutes the time interval it takes for unused addresses to return to the IP addresses pool.</p> <p>Address exhaustion tracking - Specifies the type of log to issue if the IP Pool is exhausted.</p> <p>Address allocation and release tracking - Specifies whether to log each allocation and release of an IP address from the IP Pool.</p>
Automatic ARP detection	When internal devices in the local network are defined using static NAT, the appliance must make sure packets to the static NAT IP address reach it. This option enables the appliance to automatically respond to ARP requests for those IP addresses.
Increase hide capacity	Indicates if hide-NAT capacity is given additional space.
NAT enable	Indicates if the device's NAT capabilities are enabled.
NAT cache expiration	Indicates the expiration time in minutes for NAT cache entries.
NAT cache number of entries	Indicates the maximum number of NAT cache entries.

Table: NAT Attributes (continued)

NAT Attribute	Description
NAT hash size	Indicates the hash bucket size of NAT tables.
NAT limit	Indicates the maximum number of connections with NAT.
Perform cluster hide fold	Indicates if local IP addresses are hidden behind the cluster IP address when applicable, as opposed to being hidden behind each cluster member's physical IP address.
Translate destination on client side	Translates destination IP addresses on client side (for automatically generated NAT rules).
Translate destination on client side (manual rules)	Translates destination IP addresses on client side (for manually configured NAT rules).

Table: Notification Policy Attributes

Notification Policy Attribute	Description
Notification Language	Notification language

Table: Privacy Setting Attributes

Privacy Settings Attribute	Description
Help Check Point improve its products by sending data	Customer consent.

Table: QoS Blade Attributes

QoS Blade Attribute	Description
Logging	Indicates if the appliance logs QoS events when the QoS blade is enabled.

Table: Reach My Device Attributes

Reach My Device Attribute	Description
Ignore SSL certificate	Indicates if the SSL certificate should be ignored when running the access service.
Server address	Indicates the address of the remote server that allows administration access to the appliance from the Internet even when behind NAT.

Table: Report Settings

Report Settings Attribute	Description
Max Period	Maximum period to collect and monitor data. You must reboot the appliance to apply changes.

Table: Serial Port Attributes

Serial Port Attribute	Description
Multiple Parameters	<p>With the serial port parameters you can configure the console port on the back panel of the appliance.</p> <p>You can disable it completely (clear the Enable serial port checkbox) if necessary and configure port speed and flow control settings. Note that these settings must match the configuration of the device connected to the console port.</p> <p>There are three modes for working with this port:</p> <ul style="list-style-type: none"> ■ Console - This is the default mode configured. The port is used to access the appliance's console. ■ Active - Instead of connecting through the port to the appliance's console, the data is relayed to a specified telnet server which can now be viewed through this port. Enter the Server TCP port of the telnet server and the IP address of the server. Two different IP server IP addresses can be configured (Primary server and Secondary server). ■ Passive - In this mode the flow of data is reversed and the appliance connects through the serial port to the console of the connected device. This console is accessible through a telnet connection to a configured port on the appliance. In Listen on TCP port, enter the port number. <p>To configure an implicit rule that allows traffic from any source to this port, make sure Implicitly allow traffic to this port is selected. If you do not create an implicit rule, you must manually define an access rule in the Firewall Rule Base.</p> <p>Two appliances, one in active mode and the other in passive mode, can allow a client to remotely connect to a console connected to the appliance in passive mode over the internet using a telnet connection.</p>

Table: SSL Inspection Attributes

SSL Inspection Attribute	Description
Additional HTTPS ports	Additional HTTPS ports for SSL inspection (a comma separated list of ports/ranges).
Log empty SSL connections	Log connections that were terminated by the client before data was sent. This might indicate the client did not install the CA certificate.
Retrieve intermediate CA certificates	Indicates if the SSL inspection mechanism will perform its validations on all intermediate CA certificates in the certificate chain.
Track validation errors	Choose if the SSL Inspection validations are tracked.

Table: SSL Inspection Attributes (continued)

SSL Inspection Attribute	Description
Validate CRL	Indicates if the SSL inspection mechanism will drop connections that present a revoked certificate.
Validate Expiration	Indicates if the SSL inspection mechanism will drop connections that present an expired certificate.
Validate unreachable CRL	Indicates if the SSL inspection mechanism will drop connections that present a certificate with an unreachable CRL.
Validate untrusted certificates	Indicates if the SSL inspection mechanism will drop connections that present an untrusted server certificate.

Table: Stateful Inspection Attributes

Stateful Inspection Attribute	Description
Accept out of state TCP packets	Indicates if TCP packets which are not consistent with the current state of the TCP connection are dropped (when set to 0) or accepted (when set to any other value).
Accept stateful ICMP errors	Accept ICMP error packets which refer to another non-ICMP connection (for example, to an ongoing TCP or UDP connection) that was accepted by the Rule Base.
Accept stateful ICMP replies	Accept ICMP reply packets for ICMP requests that were accepted by the Rule Base.
Accept stateful UDP replies for unknown services	Specifies if UDP replies are to be accepted for unknown services. In each UDP service object it is possible to configure whether UDP replies for it are accepted if the service is matched on a rule which accepts traffic. This parameter refers to all connections which are not covered by the service objects.
Accept stateful other IP protocols replies for unknown services	Accept stateful other IP protocols replies for unknown services. In each service object it is possible to configure whether replies for it are accepted if the service is matched on a rule which accepts traffic. This parameter refers to all no TCP/UDP connections which are not covered by the service objects.
Allow LAN-DMZ DPI	Allow Deep Packet Inspection in traffic between internal networks and the DMZ network. Note - DMZ is not supported in 1550 appliances.
Allow LAN-LAN DPI	Allow Deep Packet Inspection in traffic between internal networks.

Table: Stateful Inspection Attributes (continued)

Stateful Inspection Attribute	Description
Drop out of state ICMP packets	Drop ICMP packets which are not in the context of a "virtual session".
ICMP virtual session timeout	An ICMP virtual session is considered to have timed out after this time period (in seconds).
Log dropped out of state ICMP packets	Indicates if dropped out of state ICMP packets generate a log. See the "Drop out of state ICMP packets" parameter.
Log dropped out of state TCP packets	Indicates if dropped out of state TCP packets generate a log. See the "Accept out of state TCP packets" parameter.
Other IP protocols virtual session timeout	A virtual session of services which are not TCP, UDP or ICMP is considered to have timed out after this time period (in seconds).
TCP end timeout	Indicates the timeout (in seconds) for TCP session end. A TCP session is considered as "ended" following two FIN packets, one in each direction, or an RST packet.
TCP session timeout	Indicates the timeout (in seconds) for TCP sessions. A TCP session times out if the connection remains idle after this time period (in seconds).
TCP start timeout	Indicates the timeout (in seconds) for TCP session start. A TCP connection times out if the interval between the arrival of the first packet and establishment of the connection (TCP three-way handshake) exceeds this time period (in seconds).
UDP virtual session timeout	A UDP virtual session is timed out after this time period (in seconds).

Table: Streaming Engine Setting Attributes

Streaming Engine Settings Attribute	Description
Multiple parameters	<p>These settings determine how the TCP streaming engine used by the various deep inspection blades (IPS, Application Control, Anti-Bot, Anti-Virus, etc.) handles protocol violations and events that prevent the streaming engine from further inspection.</p> <p>We highly recommend that these settings always be in prevent mode. Using these settings in detect mode may significantly lower security as inspection stops when the event or violation occurs.</p> <p>When the configuration is set to log such events, the logs are shown in Logs & Monitoring > Security Logs under the IPS blade.</p> <p>For each violation or event configure the action and tracking mode.</p>
TCP Segment Limit Enforcement	<p>For every TCP segment that passes through the gateway, the gateway retains a copy of the segment until it receives an acknowledgment that the segment was received. This buffered data occupies space in the gateway's memory. This enforces a limit on the number and size of buffered segments per connection. When a connection reaches one of these limits, the gateway does not accept new segments for this connection until buffered segments are acknowledged.</p>
TCP Out of Sequence	<p>The receiving host of a TCP stream buffers segments and retains only those segments within a specified window. Segments outside this window are not processed by the receiving host. TCP segments which are outside the TCP receiving window should not be processed by the gateway. All data from TCP segments that are outside of the window is either dropped or removed. If the segment is near the window, data is stripped. If the segment is far from the window, the segment is dropped.</p>
TCP Invalid Retransmission	<p>For every TCP segment that passes through the gateway, the gateway retains a copy of the segment until the gateway receives an acknowledgment that the segment was received. If no acknowledgment is received, the source machine resends the segment, which the gateway compares to its copy to verify that the new packet matches the original. Passing a retransmission that differs from the original allows uninspected data to reach the destination application. This can block segment retransmissions which differ from the original segments, and this assures that the gateway inspects all data that is processed by the receiving application. When set to detect, such retransmissions causes the traffic to bypass deep inspection blades.</p>
TCP Invalid Checksum	<p>The gateway does not need to inspect packets with an invalid TCP checksum because these packets are dropped by the receiving host's TCP stack. This blocks TCP packets with an invalid checksum. Due to malfunctioning networking equipment, it is normal to see some packets with an incorrect checksum on the network. This does not indicate an attempted attack and for this reason, the default is to NOT log such events.</p>

Table: Streaming Engine Setting Attributes (continued)

Streaming Engine Settings Attribute	Description
TCP SYN Modified Retransmission	A TCP SYN packet may be retransmitted with a changed sequence number in an attempt to initiate a connection that IPS does not inspect. This blocks a SYN retransmission where the sequence number has been modified. When set to detect, such retransmissions cause the traffic to bypass deep inspection blades.
TCP Urgent Data Enforcement	Some TCP protocols, such as Telnet, send out-of-band data using the TCP URG bit as part of the protocol syntax, whereas most protocols don't use the TCP out-of-band functionality. Allowing packets with the URG bit may prevent the gateway from determining what data would be processed by the receiving application. This could lead to a situation where the data inspected by the gateway is not what the receiving application processes, thus allowing IPS protections to be bypassed. When a packet with the URG bit is received in a protocol that does not support out-of-band functionality, the gateway cannot determine whether the receiving application processes the data. This removes the URG bit from TCP segments with the URG bit set in protocols which do not support the TCP out-of-band functionality. When set to detect, usage of the URG bit causes the traffic to bypass deep inspection blades.
Stream Inspection Timeout	A connection being inspected by a dedicated process may be delayed until inspection is completed. If inspection is not completed within a time limit, the connection is dropped so that resources are not kept open. This blocks connections whose inspection timeout has expired. When set to detect, exceeding the timeout causes the traffic to bypass deep inspection blades.

Table: Threat Prevention Anti-Bot Policy Attributes

Threat Prevention Anti-Bot Policy Attribute	Description
Resource classification mode	<p>Indicates the mode used by the Anti-Bot engine for resource classification:</p> <ul style="list-style-type: none"> ■ Hold - Connections are blocked until classification is complete. When a connection cannot be classified with the cached responses, it remains blocked until the Check Point Online Web Service completes classification. ■ Background - Connections are allowed until classification is complete. When a connection cannot be classified with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the classification procedure. The response is then cached locally for future requests. This option reduces latency in the classification process.

Table: Threat Prevention Anti-Virus Policy Attributes

Threat Prevention Anti-Virus Policy Attribute	Description
File scan size limit	Indicates the size limit (in KB) of a file scanned by Anti-Virus engine. To specify no limit, set to 0.
MIME maximum nesting level	For emails that contain nested MIME content, set the maximum number of levels that the ThreatSpect engine scans in the email.
MIME nesting level exceeded action	If there are more nested levels of MIME content than the configured amount, select to Block or Allow the email file.
Priority scanning	Scan according to security and performance priorities for maximum optimization.
Resource classification mode	Indicates the mode used by the Anti-Virus engine for resource classification: <ul style="list-style-type: none"> ■ Hold - Connections are blocked until classification is complete. When a connection cannot be classified with the cached responses, it remains blocked until the Check Point Online Web Service completes classification. ■ Background - Connections are allowed until classification is complete. When a connection cannot be classified with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the classification procedure. The response is then cached locally for future requests. This option reduces latency in the classification process.

Table: Threat Prevention Threat Emulation Policy Attributes

Threat Prevention Threat Emulation Policy Attribute	Description
Emulation connection handling mode - IMAP	Indicates the strictness mode of the Threat Emulation engine over IMAP: <p>Background - Connections are allowed while the file emulation runs (if needed) until emulation handling is complete.</p> <p>Hold - Connections are blocked until the file emulation is completed</p>

Table: Threat Prevention Threat Emulation Policy Attributes (continued)

Threat Prevention Threat Emulation Policy Attribute	Description
Emulation connection handling mode - POP3	<p>Indicates the strictness mode the Threat Emulation engine over POP3:</p> <p>Background - Connection are allowed while the file runs (if needed)</p> <p>Hold - Connections are blocked until the file emulation is completed.</p>
Emulation connection handling mode - SMTP	<p>Indicates the strictness mode of the Threat Emulation engine over SMTP:</p> <p>Background - Connections are allowed while the file emulation runs (if needed)</p> <p>Hold - Connections are blocked until the file emulation is completed.</p>
Emulation location	Indicates if emulation is done on Public ThreatCloud or on remote (private) SandBlast.
Primary emulation gateway	The IP address of the primary remote emulation gateway.

Table: Threat Prevention Policy Attributes

Threat Prevention Policy Attribute	Description
Block when service is unavailable	Block web requests traffic when the Check Point ThreatCloud online web service is unavailable.
Fail mode	Indicates the action to take (Allow all requests or Block all requests) on traffic in case of an internal system error or overload.
File inspection size limit	<p>Indicates the size limit (in KB) of a file inspected by Threat Prevention engines.</p> <p>Note - A limit too low may have an impact on the functionality of the Application Control blade. To specify no limit, set to 0.</p>

Table: Threat Prevention Policy Attributes (continued)

Threat Prevention Policy Attribute	Description
Method for skipping HTTP inspection	<p>Warning: Changing the setting to <i>Full</i> has a severe security impact.</p> <p>An HTTP connection can be made up of many sessions. A file that is part of an HTTP connection passes in one HTTP session.</p> <p>If a non-zero File inspection size limit is configured, the <i>Default</i> setting of Method for skipping HTTP inspection is that file inspection is skipped to the end of the session, and resumes in the next HTTP session.</p> <p>If a non-zero File inspection size limit is configured and the Method for skipping HTTP inspection is changed to <i>Full</i>, file inspection is skipped to the end of the connection and resumes in the next connection. This improves performance because the remaining part of the connection is fully accelerated. However, changing the setting to <i>Full</i> is not recommended because of a severe security impact: The remaining sessions of the connection are not inspected.</p>

Table: Update services schedule Attributes

Update Services Schedule Attribute	Description
Maximum number of retries	Indicates the maximum number of retries for a single update when the cloud is unavailable
Timeout until retry	Indicates the timeout (in seconds) until update retry.

Table: User Awareness Attributes

User Awareness Attribute	Description
Active Directory association timeout	Indicates the timeout (in minutes) for caching an association between a user and an IP address.
Allow DNS for unknown users	<p>Indicates that DNS traffic from unauthenticated users is not be blocked when Block unauthenticated users when the captive portal is not possible is selected in Users & Objects > User Awareness > Browser-Based Authentication > Identification tab.</p> <p>Without DNS traffic, the browsers of end users, may not show the Captive Portal.</p>

Table: User Awareness Attributes (continued)

User Awareness Attribute	Description
Assume single user per IP address	When Active Directory Queries is enabled in Users & Objects > User Awareness the parameter indicates that only one user can be identified from a single device. When two or more users connect from a device, only the last user to log on is identified.
Log blocked unknown users	Indicates if unauthenticated users that are blocked are logged when Block unauthenticated users when the captive portal is not possible is selected in Users & Objects > User Awareness > Browser-Based Authentication > Identification tab.

Table: User Management Attributes

User Management Attribute	Description
Automatically delete expired local users	Automatically delete all expired local users every 24 hours (after midnight).

Table: VPN Remote Access Attributes

VPN Remote Access Attribute	Description
Allow clear Traffic while disconnected	Indicates if traffic to the VPN domain is handled when the Remote Access VPN client is not connected to the site is sent without encryption (clear) or dropped.
Allow simultaneous login	Indicates if a user can log in to multiple sessions. If the option is disabled, and a user logs in a second time with the same credentials, the previous session is disconnected.
Authentication timeout	Indicates the amount of time (in minutes) the remote client's password remains valid if timeout is enabled.
Authentication timeout enable	Indicates if the remote client's password remains valid only for a configured amount of time (Authentication timeout attribute).
Auto-disconnect in VPN domain	Indicates if the client disconnects automatically to save resources when it connects from inside the secured internal network (local encryption domain).
Back connections enable	Enable back connections from the encryption domain behind the gateway to the client.

Table: VPN Remote Access Attributes (continued)

VPN Remote Access Attribute	Description
Back connections keep-alive interval	Indicates the interval (in seconds) between keep-alive packets to the gateway required for gateway to client back connections.
Enable Visitor Mode on All Interfaces	This dialog box lets you configure a specified interface for visitor mode. Visitor mode allows the appliance to listen for TCPT traffic on a specified port (by default port 443) as backup to IKE connections from the remote access client.
Enable Visitor Mode on This Interface	<p>This mode is normally used to allow VPN remote access connections from behind restrictive environments such as hotels.</p> <p>Modifying visitor mode to be enabled only on a specific interface is not recommended.</p>
Encrypt DNS traffic	Indicates if DNS queries sent by the remote client to a DNS server located in the encryption domain are passed through the VPN tunnel.
Encryption Method	Indicates which IKE encryption method (version) is used for IKE phase 1 and 2.
Endpoint Connect re-authentication timeout	Indicates the time (in minutes) until the Endpoint Connect user's credentials are resent to the gateway to verify authorization.
IKE IP Compression Support	Indicates if IPSec packets from remote access clients is compressed.
IKE Over TCP	Enables support of IKE over TCP.
IKE restart recovery	When dealing with Remote Access clients, the appliance cannot initiate an IKE phase 1 negotiation because the client address is unknown. If the appliance has an active SA with a Remote Access client and it restarts, the SA is lost, and the appliance cannot initiate IKE phase 1. But, if the restart option is selected, the appliance saves the tunnel details every minute. When the first encrypted packet arrives after the appliance restarts, the appliance sends a Delete SA message. This causes the remote client to discard the old SA and initiate IKE phase 1 to reopen the tunnel.
Legacy NAT traversal	Indicates if the Check Point proprietary NAT traversal mechanism (UDP encapsulation) is enabled for SecureClient.
Minimum TLS version support in the SSL VPN portal	Indicates the minimum TLS protocol version which the SSL VPN portal supports. For security reasons, we recommend to support TLS 1.2 and above.

Table: VPN Remote Access Attributes (continued)

VPN Remote Access Attribute	Description
Office Mode Enable With Multiple Interfaces	Indicates if a mechanism (with a performance impact) to improve connectivity between remote access client and an appliance with multiple external interfaces is enabled.
Office Mode Perform Anti-Spoofing Single Office Mode Per Site	<p>Office Mode Perform Anti-Spoofing - If this option is selected, VPN verifies that packets whose encapsulated IP address is an Office Mode IP address are indeed coming from an address of a client working in Office Mode. If the addresses are allocated by a DHCP server, VPN must know the range of allocated addresses from the DHCP scope for the Anti-Spoofing feature to work. Define a Network object that represents the DHCP scope and select it here.</p> <p>Single Office Mode Per Site - After a remote user connects and receives an Office Mode IP address from a gateway, every connection to that gateway's encryption domain goes out with the Office Mode IP as the internal source IP. The Office Mode IP is what hosts in the encryption domain recognize as the remote user's IP address. The Office Mode IP address assigned by a specific gateway can be used in its own encryption domain and in neighboring encryption domains as well. The neighboring encryption domains should reside behind gateways that are members of the same VPN community as the assigning gateway. As the remote hosts connections are dependent on the Office Mode IP address it received, should the gateway that issued the IP become unavailable, all the connections to the site terminate.</p>
Office Mode allocate from RADIUS	Indicates if the Office Mode allocated IP addresses are taken from the RADIUS server used to authenticate the user.
Office Mode disable	Indicates if Office Mode (allocating IP addresses for Remote Access clients) is disabled. This is not recommended.
Passwords caching on client	Indicates if password caching is used. This means that re-authentication is not necessary when the client tries to access more than one gateway.
Prevent IP NAT Pool	Prevent IP Pool NAT configuration from being applied to Office Mode users. This is needed when using SecureClient as well as other VPN clients (see sk20251).
Radius retransmit timeout	Timeout interval (in seconds) for each RADIUS server connection attempt.

Table: VPN Remote Access Attributes (continued)

VPN Remote Access Attribute	Description
Remote Access port Reserve port 443 for port forwarding	The default remote access port is port 443. If there is a conflict with another server using this port number, configure a different Remote access port . You must change the default remote access port if the Check Point VPN client, Mobile client, or SSL VPN remote access methods are enabled as they use port 443 by default. If you change the default port number 443, make sure to select Reserve port 443 for port forwarding .
SNX keep-alive interval	Indicates the time (in seconds) between the SSL Network Extender client keep-alive packets.
SNX re-authentication timeout	Indicates the time (in minutes) between re-authentication of SSL Network Extender remote access users.
SNX support 3DES	Indicates if the 3DES encryption algorithm will be supported in SSL clients as well as the default algorithms.
SNX support RC4	Indicates if the RC4 encryption algorithm is supported in SSL clients as well as the default algorithms.
SNX uninstall	This parameter lets you configure under which conditions the SSL Network Extender client uninstalls itself. The options are: Do not uninstall automatically (recommended default), always uninstall upon disconnection, and ask the user upon disconnection.
SNX upgrade	This parameter lets you configure under which conditions the SSL Network Extender client installs itself. The options are: Do not upgrade automatically, always upgrade, and ask the user (default).
Topology updates manual interval	Indicates the manually configured interval (in hours) for topology updates to the clients. Applicable only if the override settings is set to true.
Topology updates override	Indicates if the configured topology updates settings override the default 'once a week' policy.
Topology updates upon startup only	Indicates if topology updates occur only when the client starts. Applicable only if the override settings is set to true.
Verify device certificate	The remote access client verifies the device's certificate against revocation list.

Table: VPN Site to Site Global Setting Attributes

VPN Site to Site Global Settings Attribute	Description
Accept NAT Traversal	Indicates if industry standard NAT traversal (UDP encapsulation) is enabled. This enables VPN tunnel establishment even when the remote site is behind a NAT device.
Administrative notifications	Indicates how to log an administrative event (for example, when a certificate is about to expire)
Check validity of IPSec reply packets	Indicated whether to check the validity of IPSec reply packets.
Cluster SA sync packets threshold	Sync SA with other cluster members when the number of packets reaches this threshold.
Copy DiffServ mark from encrypted /decrypted IPSec packet	Copy DiffServ mark from encrypted/decrypted IPSec packet.
Copy DiffServ mark to encrypted/ decrypted IPSec packet	Copy DiffServ mark to encrypted/decrypted IPSec packet.
DPD triggers new IKE negotiation	DPD triggers new IKE negotiation.
Delete IKE SAs from a dead peer	Delete IKE SAs from a dead peer.
Delete IPsec SAs on IKE SA delete	Delete IPsec SAs on IKE SA delete.
Delete tunnel SAs when Tunnel Test fails	When permanent VPN tunnels are enabled and a Tunnel Test fails, delete the relevant peer's tunnel SAs.
Do not encrypt connections originating from the local gateway	Packets whose original source or destination IP address is the local gateway's Internet Connection IP address will not go through a VPN tunnel. This parameter may be useful when the gateway behind hide NAT.
Do not encrypt local DNS requests	When enabled, DNS requests originating from the appliance will not be encrypted. Relevant when a configured DNS server is in a VPN peer's encryption domain.
Enable encrypted packets rerouting	Indicates if encrypted packets are rerouted through the best interface according to the peer's IP address or probing. We do not recommend to change this value to false.

Table: VPN Site to Site Global Setting Attributes (continued)

VPN Site to Site Global Settings Attribute	Description
Grace Period after CRL is no longer valid	<p>CRL grace period is required to resolve the issue of differing clock times between the appliance and the remote CA.</p> <p>A grace period permits a wider window for CRL validity.</p> <p>Indicates the time (in seconds) after which a revoked certificate of a remote site remains valid.</p>
Grace Period before CRL is valid	<p>CRL grace period is required to resolve the issue of differing clock times between the appliance and the remote CA.</p> <p>A grace period permits a wider window for CRL validity.</p> <p>Indicates the time window (in seconds) where a certificate is considered valid prior to the time set by the CA.</p>
IKE DoS from known sites protection	Indicates if the IKE DoS from known IP addresses protection is active and the method by which it detects potential attackers.
IKE DoS from unknown sites protection	Indicates if the IKE DoS from unidentified IP addresses protection is active and the method by which it detects potential attackers.
IKE Reply From Same IP	Indicates if the source IP address used in IKE session is based on destination when replying to incoming connections, or based on the general source IP address link selection configuration.
Join adjacent subnets in IKE Quick Mode	Indicates if to join adjacent subnets in IKE Quick Mode.
Keep DF flag on packet	Indicates if the 'Don't Fragment' flag is kept on the packet during encryption/decryption.
Keep IKE SA Keys	Keep IKE SA keys.
Key exchange error tracking	Indicates how to log VPN configuration errors or key exchange errors.
Maximum concurrent IKE negotiations	Indicates the maximum number of concurrent VPN IKE negotiations.
Maximum concurrent tunnels	Indicates the maximum number of concurrent VPN tunnels.
Open SAs limit	Indicates the maximum number of open SAs per VPN peer.
Outgoing link tracking	Indicates how to log the outgoing VPN link: Log, don't log, or alert.

Table: VPN Site to Site Global Setting Attributes (continued)

VPN Site to Site Global Settings Attribute	Description
Override 'Route all traffic to remote VPN site' configuration for admin access to the device	Select this option to prevent admin access to this appliance from being routed to the remote site even when the "Route all traffic to remote VPN site" is configured.
Packet handling errors tracking	Indicates how to log the VPN packet handling errors: Log, don't log, or alert.
Perform Tunnel Tests using an internal IP Address	<p>A Tunnel Test makes sure that the VPN tunnel between peer VPN Gateways is up.</p> <p>By default, the test is done by making sure there is a connection between all the external IP addresses of the peer VPN Gateways.</p> <p>You can configure this option to do the tunnel tests using the internal IP addresses of the Gateways that are part of the local encryption domain.</p> <p>You can see the status of the VPN tunnel in the Logs and Monitoring tab.</p>
Permanent tunnel down tracking	Indicates how to log when the tunnel goes down: Log, don't log, or alert.
Permanent tunnel up tracking	Indicates how to log when the tunnel is up: Log, don't log, or alert.
RDP packet reply timeout	Timeout (in seconds) for an RDP packet reply.
Reply from incoming interface	When tunnel is initiated from remote site, reply from the same incoming interface when applicable (IKE and RDP sessions).
Successful key exchange tracking	Indicates how to log when there is a successful key exchange: Log, don't log, or alert.
Use cluster IP address for IKE	Indicates if IKE is performed using cluster IP address (when applicable).
Use internal IP address for encrypted connections from local gateway	Encrypted connections originating from the local gateway will use an internal interface's IP address as the connection source.
VPN tunnel sharing	Indicates under what conditions new tunnels are created: per host pair, per subnet (industry standard), or a single tunnel per remote site/gateway. This controls the number of tunnels that are created.

Table: VoIP Attributes

VoIP Attribute	Description
Accept MGCP connections to registered ports	Indicates if deep inspection over MGCP traffic automatically accepts MGCP connections to registered ports.
Accept SIP connections to registered ports	Indicates if deep inspection over SIP traffic automatically accepts SIP connections to registered ports.

Table: Web Interface Settings and Customization Attributes

Web Interface Settings and Customizations Attribute	Description
Multiple parameters	<p>Select Use a company logo in the appliance's web interface to display a different logo (not the Check Point default logo).</p> <p>In Company logo, click the Upload company logo link, browse to the logo file, and click Apply.</p> <p>In Company URL, enter the company's URL. When you click the company logo in the web interface it opens this URL.</p>

Managing the Access Policy

This section describes how to set up and manage your Check Point Appliance access policy.

Configuring the Firewall Access Policy and Blade

In the **Access Policy > Firewall Blade Control** page you can set the default Access Policy control level, set the default applications and URLs to block and allow secure browsing, and configure User Awareness.

The Access Policy is a set of rules that defines the security requirements for your appliance for incoming, internal, and outgoing traffic.

The Access Policy includes:

- **Firewall Policy** - Defines how to inspect packets.
- **Application & URL Filtering** - Defines how to control Internet browsing and application usage.

The **Access Policy > Firewall Blade Control** page lets you easily define the default policy for your organization. In addition, you can define and view the rule based policy in the **Access Policy > Firewall Policy** page. Configurations in the **Firewall Blade Control** page are shown as automatically generated system rules at the bottom of the Rule Base. We recommend you use the **Access Policy > Firewall Policy** page to define manual rules that are exceptions to the default policy defined in this page.

The **Access Policy > Firewall Blade Control** page defines the default policy for incoming, internal, and outgoing traffic to and from your organization. In addition, the **Access Policy > Firewall Servers** page lets you easily define the default access policy for specific servers within your organization and automatically generated system rules are also defined.

Firewall Policy

Select one of these options to set the default Access Policy:

- **Strict**

Blocks all traffic, in all directions, by default. In this mode, your policy can only be defined through the Servers page and by manually defining access policy rules in the **Access Policy > Firewall Policy** page.
- **Standard**
 - Allows outgoing traffic to the Internet on configured services. You can click the **services** link to configure all or only specified services that are allowed.
 - Allows traffic between internal networks and trusted wireless networks (in applicable devices).
 - Blocks incoming unencrypted traffic from the Internet (traffic from outside your organization to it).

The Standard policy option is the default level and is recommended for most cases. Keep it unless you have a specified need for a higher or lower security level.
- **Off**

Allows all traffic. When the firewall is deactivated, your network is not secured. Manually defined rules are not applied.

Note - When the blade is managed by Cloud Services, a lock icon shows. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

To set specified outgoing services in a standard Firewall policy:

1. When the Access Policy control level is set to **Standard**, click **allservices**.
2. Select **Block all outgoing services except the following**.
3. Select which services to allow.
4. To allow all services, select **Allow all outgoing services**.
5. Click **Apply**.

To manually configure Access Policy rules:

Go to the **Access Policy > Policy** page.

In the **Access Policy > Blade Control** page:

- When no manual rules are configured, you can click the **Firewall Policy** link to add manual rules to the Firewall policy.
- When manual rules are configured, it shows the number of rules that are added. Click **manual rules** to see them in the Access Policy.

Click **Servers** to see how many servers are defined in the appliance. If no servers are configured, click **Add aserver** to add one. A server object is a defined IP address to which you can also define a specific access policy and also incoming NAT rules if necessary. For example, Port forwarding NAT. Automatically generated access rules to servers are created above the default policy rules and can be seen in the **Access Policy > Firewall Policy** page. You can create exception rules for servers as well in the **Access Policy > Firewall Policy** page.

Application & URL Filtering

The Application & URL Filtering section lets you define how to handle applications and URL categories on traffic from your organization to the Internet.

Application & URL Filtering are service based features and require Internet connectivity to download the latest signature package for new applications and to contact the Check Point cloud for URL categorization. This page lets you define the default policy for Application & URL Filtering control. It is recommended by default to block browsing to security risk categories and applications. You can also configure additional applications and categories to block by default according to your company's policy. In addition, you can also select to limit bandwidth consuming applications for better bandwidth control.

In addition to the **On** and **Off** buttons, you can select the **URL Filtering Only** mode. When you select this option, only URLs and custom applications defined by URLs are blocked. Predefined applications initially installed on your computer or added with automatic updates are not blocked.

When you select the **URL Filtering Only** mode:

- Rules that contain URLs are enforced. Any applications inside rules are not enforced.
- Rules that contain custom URLs and custom applications are enforced.
- Rules that contain application groups with both predefined applications and URLs are enforced only for the URLs and custom applications. They are not enforced for the predefined applications.
- Applications are not updated through the automatic updates.

The default policy defined here is viewed as automatically generated rules in the bottom of the Outgoing traffic Rule Base in the **Access Policy > Policy** page.

Select one or more of these options:

- **Block security risk categories** - Lets you block applications and URLs that can be a security risk and are categorized as spyware, phishing, botnet, spam, anonymizer, or hacking. This option is selected by default.
- **Block inappropriate content** - Lets you control content by blocking Internet access to websites with inappropriate content such as sex, violence, weapons, gambling, and alcohol.
- **Block file sharing applications** - Lets you block file-sharing from usually illegal sources using torrents and peer-to-peer applications.
- **Block other undesired applications** - Lets you manually add and block applications or categories of URLs to a group of undesired applications. You can also create a new URL or application if it is not in the database. Click this option to manage your basic Application & URL Filtering policy that sets what to block. For a more granular policy, go to the **Access Policy > Firewall Blade Control** page.
- **Limit bandwidth consuming applications** - Applications that use a lot of bandwidth can decrease performance necessary for important business applications. This option gives accelerated QoS (bandwidth control) for applications. When you select this option, P2P file sharing, media sharing, and media streams are selected by default but you can edit the group to add applications or categories that you think should have a limit with regards to the amount of bandwidth they consume. Note that it is very important to indicate the maximum bandwidth limit according to your Internet connection upload and download bandwidth. Consult your ISP for this information. For the limit to be effective, it has to be lower than the actual bandwidth supplied by your ISP. Upload and download bandwidths are usually not the same.

Updates

As a service based feature, this page also shows you the update status:

- Up to date
- Updated service unreachable - This usually results from a loss in Internet connectivity. You must check your Internet connection in the **Device > Internet** page and contact your ISP if the problem persists.
- Not up to date - A new update package is ready to be downloaded but the scheduled hour for updates has not occurred yet. Updates are usually scheduled for off-peak hours (weekends or nights).

To schedule updates:

1. Hover over the icon next to the update status and select the **Schedule Updates** link.
2. Select the blades for which to schedule updates. You must manually update the rest of the blades when new updates packages are available and a not up to date message is shown in the status bar at the bottom of the WebUI application.

3. Select a **Recurrence** time frame:

- **Hourly** - Enter the time interval for **Every x hours**.
- **Daily** - Select the **Time of day**.
- **Weekly** - Select the **Day of week** and **Time of day**.
- **Monthly** - Select the **Day of month** and **Time of day**.

4. Click **Apply**.

User Awareness

User Awareness lets you configure the Check Point Appliance to enforce access control for individual users and groups and show user-based logs instead of IP address based logs.

Initially, click **Configure** to set up how User Awareness recognizes users. When this is configured, you can see users in logs and also configure user based Access Policy rules. User recognition can be done seamlessly by the appliance using your organization's AD server. The user database and authentication are all done through the AD server. When a user logs in to the AD server, the appliance is notified. Users from the AD server can be used as the Source in Access Policy rules.

Alternatively or in addition, users can be defined locally in the **Users & Objects > Users** page with a password. For the appliance to recognize the traffic of those users, you must configure Browser-Based Authentication and the specific destinations to which they must be identified first before accessing. Normally, Browser-Based Authentication is not used for all traffic, but rather for specific destinations because it requires manual login by the end user through a dedicated portal.

If User Awareness has been configured, the **Enable User Awareness** checkbox is shown. To disable User Awareness, clear the checkbox. To make changes to the configuration, click **Edit settings**.

At any time, you can also click **Active Directory servers** to define an AD server that the gateway can work with. Creating an AD server is also available in the Edit settings wizard.

Tracking

Select which traffic to log:

For blocked traffic

- All
- Outgoing
- Incoming and internal

For allowed traffic

- All
- Outgoing
- Incoming and internal

These settings apply to all the incoming and outgoing traffic blocked or accepted by the default Firewall and Application & URL Filtering automatically generated rules.

These settings do not apply to automatically generated rules for VPN, DMZ, and wireless networks.

More Information

The Check Point Application Database contains more than 4,500 applications and about 96 million categorized URLs.

Each application has a description, a category, additional categories, and a risk level. You can include applications and categories in your Application Control and URL Filtering rules. If your appliance is licensed for the Application Control & URL Filtering blades, the database is updated regularly with new applications, categories and social networking widgets. This lets you easily create and maintain an up to date policy.

You can see the Application Database from:

- The Block **other undesired applications** link.
- The **Applications & URLs** link - This opens the **Users & Objects > Applications & URLs** page.
- The **Check Point AppWiki** link - The AppWiki is an easy to use tool that lets you search and filter the Application & URL Filtering Database.

Working with the Firewall Access Policy

In the **Access Policy > Firewall Policy** page you can manage the Firewall Access Policy Rule Base. You can create, edit, delete, enable or disable rules. In the **Access Policy > Firewall Blade Control** page you determine the basic firewall policy mode.

In **Standard** mode, this page shows you both automatically generated rules based on the configuration of your default policy and manually defined rules as exceptions to this default policy.

In **Strict** mode, all access is blocked by default and this page is the only way to configure access rules for your organization.

The Rule Base is divided into two sections. Each of the two sections represent a different security policy - how your organization browses to the Internet (the world outside your organization) and the security policy to access your organization's resources (both from within and from outside your organization). At the top of the page there are three links that let you see both or only one of the sections.

- **Outgoing access to the Internet** - For all outgoing traffic rules. In this Rule Base you determine the policy to access the Internet outside your organization. Commonly the policy here is to allow the basic traffic, but you can block applications and URLs based on your company's discretion. In the **Access Policy > Firewall Blade Control** page you can configure the default policy to block applications and URLs. This page lets you add manual rules as exceptions to the default policy. You can also **customize messages** that are shown to users for specified websites when they are blocked or accepted by the Rule Base (see below). You can also use an **Ask** action for applications or URLs that lets the end user determine whether browsing is for work related purposes or not. For example, we recommend you add a rule that asks the users before browsing to uncategorized URLs. Such a rule can disrupt possible bot attacks.
- **Incoming, internal and VPN traffic** - For all incoming, internal and VPN traffic rules. In this Rule Base, you determine the policy to access your organization's resources. All internal networks, wireless networks, **and** external VPN sites are considered part of your organization and traffic to them is inspected in this Rule Base. Commonly the policy here is to block traffic from outside your organization into it and allow traffic within your organization.

In Standard mode, you can configure in various pages a more granular default policy:

- **Traffic from specific sources into your organization** can be blocked or accepted by default. This configuration can be found in each specific sources' edit mode:
 - External VPN sites - Configure default access from/to **VPN > Site to Site Blade Control** page.
 - Remote Access VPN users - Configure default access from **VPN > Remote Access Blade Control** page.
 - Wireless networks - Configure default access for each wireless network from the Access tab in each wireless network's edit window in the **Device > Wireless Network** page.
 - DMZ network - Configure default access from the DMZ object's edit window in the **Device > Local Network** page.
- Note** - DMZ is not supported in 1550 appliances.
- **Traffic to defined server objects** as configured in each server's edit window in the **Access Policy > Firewall Servers** page.

This page lets you add manual rules as exceptions to the default policy. In Strict mode, the default policy blocks everything and you configure access only through manual rules.

Within each section there are these sections:

- **Manual Rules** - Rules that you manually create.
- **Auto Generated Rules** - Rules that the system determines based on the initial Firewall Policy mode (Strict or Standard) as explained above. These rules are also influenced by other elements in the system. For example, when you add a server, a corresponding rule is added to the Incoming, internal and VPN traffic section.

These are the fields that manage the rules for the Firewall Access Policy.

Rule Base Field	Description
No.	Rule number in the Firewall Rule Base.
Source	IP address, network object, or user group that initiates the connection.
Destination	IP address or network object that is the target of the connection.
Application	<p>Applications or web sites that are accepted or blocked. You can filter the list by common applications, categories, custom defined applications, URLs or groups. For more information, see "Managing Applications & URLs" on page 225.</p> <p>This field is only shown in the Outgoing access to the Internet section.</p>
Service	Type of network service that is accepted or blocked.
Action	<p>Firewall action that is done when traffic matches the rule.</p> <p>For outgoing traffic rules, you can use the Customize messages option to configure "Ask" or "Inform" actions in addition to the regular Block or Accept actions.</p> <p>The messages shown can be set for these action types: Accept and Inform, Block and Inform, or Ask. Ask action lets the end user decide if this traffic is for work purposes or personal. See the Customize messages section below. Users are redirected to a portal that shows a message or question.</p> <p>If a time range is set for the rule, a clock icon is shown.</p>
Log	The tracking and logging action that is done when traffic matches the rule.
Comment / Auto generated rule	<p>Details shown immediately below the above fields for:</p> <ul style="list-style-type: none"> ■ Comments you enter when you create a rule. ■ Rules that the system automatically generates. You can click the object name link in the comment to open its configuration tab.

The "Ask" action

The outgoing Rule Base gives the option to set an Ask action instead of just allow or block for browser based applications. There are several commonly used cases where this is helpful:

- This action can be used for traffic that is normally not allowed in your organization, but you do want it to be available for work-related purposes. End users are asked if they need to browse for work-related purposes and can continue without requiring the administrator to make changes to the access policy for this single event. For example, traffic to Facebook is generally blocked but you want your HR department to be able to access it for work-related purposes.
- This action for traffic to uncategorized URLs can also give security against malware that managed to be installed inside your organization. Such malware is blocked by the Ask action.

To create a new manually defined access rule:

1. Click the arrow next to **New**. When the page shows both Rule Bases, click **New** in the appropriate table.
2. Click one of the available positioning options for the rule: **On Top**, **On Bottom**, **Above Selected**, or **Under Selected**.

The Add Rule window opens. It shows the rule fields in two ways:

- A rule summary sentence with default values.
 - A table with the rule base fields in a table.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the rule base fields. See the descriptions above.

Note - The Application field is relevant only for outgoing rules.

In the **Source** field, you can optionally select between entering a manual IP address (network), a network object, or user group (to configure a user based policy, make sure the User Awareness blade is activated). Users can be defined locally on the appliance or externally in an Active Directory. For more details, see the **Access Policy > User Awareness Blade Control** page.

4. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in the Access Policy.
5. To limit the rule to a certain time range, select **Apply only during this time** and select the start and end times.
6. In outgoing rules, to limit the download traffic rate, select **Limit download traffic of applications to** and enter the **Kpbs** rate.
7. In outgoing rules, to limit the upload traffic rate, select **Limit upload traffic of applications to** and enter the **Kpbs** rate.
8. In incoming rules, to match only for encrypted VPN traffic, select **Match only for encrypted traffic**.
9. Click **Apply**.

The rule is added to the outgoing or incoming section of the Access Policy.

To clone a rule:

Clone a rule to add a rule that is almost the same as the one that already exists.

1. Select a rule and click **Clone**.
2. Edit the fields as necessary.
3. Click **Apply**.

To edit a rule:

Note - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**.

To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

To enable or disable a rule:

- To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
- To enable a manually defined rule that you previously disabled, select the rule and click **Enable**.

To change the rule order:

1. Select the rule to move.
2. Drag and drop it to the necessary position.

Note - You can only change the order of manually defined rules.

Customize messages

You can customize messages to let the Security Gateway communicate with users. This helps users understand that some websites are against the company's security policy. It also tells users about the changing Internet policy for websites and applications. When you configure such messages, the user's Internet browser shows the messages in a new window when traffic is matched on a rule using one of the message related actions.

These are the Action options and their related notifications:

Rule Base action	Notifications
Accept and Inform	Shows an informative message to users. Users can continue to the application or cancel the request.
Block and Inform	Shows a message to users and blocks the application request.
Ask	Shows a message to users and asks them if they want to continue with the request or not. See above for more details.

To customize messages:

1. Click **Customize messages** in the **Outgoing access to the Internet** section.
2. Configure the options in each of these tabs:
 - **Accept and Inform**
 - **Block and Inform**
 - **Ask**
3. Configure the applicable fields for each of the notifications:
 - **Title** - Keep the default or enter a different title.
 - **Subject** - Keep the default or enter a different subject.
 - **Body** - Keep the default or enter different body text. You can click **Optional keywords** for a list of keywords that you can add in the body text to give the user more information.
 - **Ignore text** (only for Ask) - This is the confirmation message for the Ask user message. Keep the default text or enter different text
 - **User must enter a reason** (only for Ask) - Select this checkbox if users must enter an explanation for their activity. The user message contains a text box for entering the reason.
 - **Fallback action** - Select an alternative action (Block or Accept) for when the notification cannot be shown in the browser or application that caused the notification, most notably in non-web applications. If it is determined that the notification cannot be shown in the browser or application, the behavior is:
 - If the Fallback action is **Accept** - The user can access the website or application.
 - If the Fallback action is **Block** - The Security Gateway tries to show the notification in the application that caused the notification. If it cannot, the website or application is blocked, and the user does not see a notification.
 - **Frequency** - You can set the number of times that users get notifications for accessing applications that are not permitted by the policy. The options are:
 - **Once a day**
 - **Once a week**
 - **Once a month**

For example, in a rule that contains in the Application - Social Networking category, if you select **Once a day** as the frequency, a user who accesses Facebook multiple times get one notification.
 - **Redirect the user to URL** - You can redirect the user to an external portal, not on the gateway. In the **URL** field, enter the URL for the external portal. The specified URL can be an external system. It gets authentications credentials from the user, such as a user name or password. It sends this information to the gateway. Only applicable for the Block and Inform notification.
4. Click the **Customize** tab to customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness). Click **Upload**, browse to the logo file and click **Apply**. If necessary, you can revert to the default logo by clicking **Use Default**.
5. Click **Apply**.

Defining Firewall Servers

In the **Servers** page you can see a list of servers defined in your system. You can create, edit, delete or search for server objects. Server objects are network objects that are defined with their access and NAT (if applicable) policies.

New server objects are created using a wizard:

- Step 1 - Select the server type.
- Step 2 - Define the server's details.
- Step 3 - Set up the server's access policy properties.
- Step 4 - NAT configuration (if relevant)

After you create a server, one or more corresponding rules are automatically generated and added to the Access Policy automatically and shown in the **Access Policy > Firewall Policy** page. The comment in the rule shows the object name. You can click the object name link in the comment to open the Access tab in the Server Properties.

An easier way to define server objects is by detecting them in the **Home > Active Devices** page and saving them as servers. For example, this option automatically detects the MAC address of the server making configuration easier.

During the wizard:

- Click **Cancel** to quit the wizard.
- Click **Next** to move to the next page of the wizard.
- Click **Back** to go to an earlier page of the wizard.
- Click **Finish** to complete the wizard.

To create a new object:

Click **New**. The New Server Wizard opens and shows Step1: Server Type.

Step 1: Server Type

1. Select the server type. There are built-in types for common servers. You can manually define a server that listens to any configured ports and you can also change a common server type's ports.
2. When selecting built-in types, you can optionally click Edit to edit the protocol ports.
3. When you select Other Server:
 - Select the Protocol (TCP, UDP, or both).
 - Enter the TCP/UDP Ports (enter port numbers and/or port ranges separated by commas, for example, 1,3,5-8,15).

Step 2: Server Definitions

1. Enter a Name, IP address, and Comments (optional).
2. Select the options that apply to the server. For more information see **Users & Objects > Network Objects**.
 - **Allow DNS server to resolve this object name** - When the gateway is the DNS server for your internal networks the name of the server/network object will be translated to its IP address if this option is selected.
 - **Exclude from DHCP service** - The internal DHCP service will not distribute the configured IP address of this server/network object to anyone.
 - Reserve IP address in DHCP service for MAC - The internal DHCP service will distribute the configured IP address only to this server/network object according to its MAC address.
 - Enter the MAC address - This is required for IP reservation. When you create the object from the Active Devices page, the MAC address is detected automatically.

Step 3: Access

1. Select the zones from which the server is accessible:
 - **All zones (including the Internet)** - Select this option to create a server that anyone from outside the organization can access. This option requires configuring how the server is accessible through NAT (in the next step).
 - **Only trusted zones (my organization)** - Select the applicable checkboxes. You can override these settings by adding manual access rules.
 - LAN - Physical internal networks.
 - Remote Access VPN users - Users that connect from their homes/mobile devices to the office.
 - Secure wireless networks - Password protected networks, not including guest networks.
 - DMZ - The network physically connected to the DMZ port when it is not used for a secondary Internet connection.
Note - DMZ is not supported in 1550 appliances.
 - Remote VPN sites - Networks defined behind gateways to remote VPN sites.
2. If you do not want the server to be accessible to pings, clear the Allow access to server in the ICMP (ping) checkbox.
3. Select the logging policy of traffic to the server:
 - Log blocked connections
 - Log accepted connections

Step 4: NAT (when server is accessible from the Internet)

Select the relevant option:

- **The server's configured IP address (x.x.x.x) is public** - This option is only relevant if the **Hide internal networks behind the Gateway's external IP address** checkbox in the **Access Policy > NAT Control** page is cleared (see above for details). It means there are no NAT rules on the server.

When you complete the wizard, the server is added to the list of servers on the page and the automatically generated access rules are added to the **Access Policy > Firewall Policy** Rule Base.

Note - This page is available from the **Firewall** and **NAT** sections on the **Access Policy** tab.

Defining NAT Control

In the **Access Policy > Firewall NAT** page you can configure NAT for outgoing traffic and see how many servers are defined in the system. Servers are defined in the **Access Policy > Servers** page and are network objects configured with their access and NAT settings. This lets you configure servers that are accessible from the Internet even if they do not have a routable IP address. You can also configure servers with NAT settings from this page.

To disable NAT for outgoing traffic (hide NAT):

By default, NAT is configured for outgoing traffic. If it is necessary to disable NAT, make sure **Hide internal networks behind the Gateway's external IP address** is set to **OFF**.



Important - In most cases, if you turn off the hide NAT feature, you cause Internet connectivity issues. If your appliance is the gateway of your office to the Internet DO NOT set to off without consulting with networking experts.

To configure a server that is routable from the Internet (server with NAT):

1. Click **New Server (forwarding rule)**.
2. See the **Access Policy > Servers** page for instructions on how to use the server wizard.
3. In the Access step of the server wizard, select one of the options when asked from where this server is accessible.
4. In the NAT step of the server wizard, select the relevant option:
 - The gateway's external (public) IP address - This configures access through Port Forwarding. The appliance has an external routable IP address which is configured in its Internet connections (on the Device > Internet page). Traffic to the appliance to the ports configured for the server object in step 1 of the wizard is forwarded to the server. This allows traffic from the Internet into the organization (public servers) while still using one external routable IP address.
 - A different (public) IP address - This configures access through Static NAT. If a routable IP address was purchased for the server, enter it in the address field. While the rest of the internal network is hidden behind the gateway's external IP address, this specified server will use its own accessible IP address. Traffic to the specified IP address on relevant ports as configured in step 1 of the wizard will be forwarded to this server.
 - The server's configured IP address (x.x.x.x) is public - This option is only relevant if the Hide internal networks behind the Gateway's external IP address checkbox in the **Access Policy > NAT Control** page is cleared (see above for details). It means there are no NAT rules on the server.
5. When you have multiple internal servers that use the same port, select **Redirect from port** and enter a different port number that is used when you access this server from the Internet. Traffic to the server on the port you entered is forwarded to the server's port.
6. By default, the **Force translated traffic to return to the gateway** checkbox is selected. This allows access from internal networks to external IP addresses of servers through the local switch. The source is translated to "This Gateway". When the checkbox is cleared, the source is "Any" and there is no access from the internal network to external IP addresses through the switch.
7. Click **Finish**.

After you create a server with NAT settings, one or more corresponding rules are automatically generated and added to the NAT rules under the Auto Generated Forwarding Rules section. Click **View NAT rules** to see them. The comment in the rule shows the server object name. You can click the object name link to open the Access tab of the server's properties or click the Servers page link to go to the Firewall Servers page.

Advanced - Manual NAT Rules

Note - For the majority of cases, manual NAT rules are not necessary. There is no need to use this option unless you are an experienced network administrator.

A more advanced way to configure address translation is by defining manual NAT rules. If servers with NAT are configured, the manual NAT rules do not apply to them. However, they apply even when Hide NAT is activated.

These are the fields that manage the NAT rules.

Rule Base Field	Description
Original Source	The network object (a specified IP address) or network group object (a specified IP address range) that is the original source of the connections to translate.
Original Destination	The network object (a specified IP address) or network group object (a specified IP address range) that is the original destination of the connections to translate.
Original Service	The original service used for the connections to translate.
Translated Source	The network object or network group object that is the new source to which the original source is translated.
Translated Destination	The network object or network group object that is the new destination to which the original destination is translated.
Translated Service	The new service to which the original service is translated.

To create a new NAT rule:

1. If the NAT rules table is not shown on the page, click the **View NAT rules** link.
2. Click the arrow next to **New**.
3. Click one of the available positioning options for the rule: On Top, On Bottom, Above Selected, or Under Selected.

The Add Manual NAT Rule window opens. It shows the rule fields in two manners:

- A rule summary sentence with default values.
- A table with the Rule Base fields in a table.

4. Click the links in the rule summary or the table cells to select network objects or options that fill out the Rule Base fields. See the descriptions above.
5. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in NAT Manual Rules.
6. Select the **Hide multiple sources behind the translated source addresses** if you want the original source to contain multiple IP addresses, IP ranges, networks, etc. and the translated source to be a single IP address.

When this option is not selected, you can still use an IP range in the Original Source and a different IP range **of the same size** in the Translated Source. This rule does the IP address translation from one range to another, respectively (the first IP in the first range is translated to the first IP in the second range, and so on).

7. Select **Serve as an ARP Proxy for the original destination's IP address** for the gateway to reply to ARP requests sent to the original destination's IP address. Note that this does not apply to IP ranges or networks.
8. Click **Apply**.

After you create manual rule, it is added to the NAT rules table under the Manual NAT Rules section.

To edit a rule:

Note for Access Policy rules - you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**.

To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

To enable or disable a rule:

1. To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
2. To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

To change the rule order:

Note - You can only change the order of manually defined rules.

1. Select the rule to move.
2. Drag and drop it to the necessary position.

Advanced - Creating and Editing NAT Rules

In the **Access Policy > NAT Manual Rules** page you can create and edit custom NAT rules. If servers with NAT are configured the manual NAT rules do not apply to them. However, they do apply even when Hide NAT is activated.

Note - For the majority of cases, manual NAT rules are not necessary. There is no need to use this option unless you are an experienced network administrator. See the **AccessPolicy > NAT Control** page for the commonly used options.

These are the fields that manage the NAT rules.

Rule BaseField	Description
Original Source	The network object (a specified IP address) or network group object (a specified IP address range) that is the original source of the connections to translate.
Original Destination	The network object (a specified IP address) or network group object (a specified IP address range) that is the original destination of the connections to translate.
Original Service	The original service used for the connections to translate.
Translated Source	The network object or network group object that is the new source to which the original source is translated.
Translated Destination	The network object or network group object that is the new destination to which the original destination is translated.
Translated Service	The new service to which the original service is translated.

To create a new NAT rule:

1. Click the arrow next to **New**.
2. Click one of the available positioning options for the rule: **On Top**, **On Bottom**, **Above Selected**, or **Under Selected**.

The Add Rule window opens. It shows the rule fields in two manners:

- A rule summary sentence with default values.
 - A table with the rule base fields in a table.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the Rule Base fields. See the descriptions above.
 4. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule in NAT Manual Rules.

5. Select the **Hide multiple sources behind the translated source address/es** if you want the original source to contain multiple IP addresses, IP ranges, networks, etc. and the translated source to be a single IP address.

When this option is not selected, you can still use an IP range in the Original Source and a different IP range **of the same size** in the Translated Source. This rule does the IP address translation from one range to another, respectively (the first IP in the first range is translated to the first IP in the second range, etc.).

6. Click **Apply**.

To edit a rule:

Note for Access Policy rules - you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**.

To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

To enable or disable a rule:

- To disable a manually defined rule that you have added to the rule base, select the rule and click **Disable**.
- To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

To change the rule order:

1. Select the rule to move.
2. Drag and drop it to the necessary position.

Note - You can only change the order of manually defined rules.

Working with User Awareness

In the **User Awareness** page you can turn the blade on or off and use the configuration wizard to configure sources to get user identities, for logging and configuration purposes.

User Awareness lets you configure the Check Point Appliance to show user based logs instead of IP address based logs and enforce access control for individual users and user groups.

To use User Awareness, you must configure identification methods to get information about users and user groups. After the gateway acquires the identity of a user, user-based rules can be enforced on the network traffic in the Access Policy.

User Awareness can use these sources to identify users:

- **Active Directory Queries** - Seamlessly queries the AD (Active Directory) servers to get user information.
- **Browser-Based Authentication** - Uses a portal to authenticate either locally defined users or as a backup to other identification methods.

AD Query

The Check Point Appliance registers to receive security event logs from the AD domain controllers when the security policy is installed. This requires administrator privileges for the AD server. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The Check Point Appliance can then identify the user based on the AD security event log.

Browser-Based Authentication

Browser-Based Authentication uses a web interface to authenticate users before they can access network resources or the Internet. When users try to access a protected resource, they must log in to a web page to continue. This is a method that identifies locally defined users or users that were not successfully identified by other methods. You can configure the Browser-Based Authentication to appear for all traffic but because this method of identification is not seamless to the end users, it is commonly configured to appear when you access only specific network resources or the Internet to avoid the overhead required from end users when they identify themselves. For traffic that is not HTTP based, you can also configure that all unidentified are blocked from accessing the configured resources or Internet until they identify themselves first through the Browser-Based Authentication.

To turn on User Awareness on or off:

Select the **On** or **Off** option.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

Use the User Awareness configuration wizard to enable and configure the blade. You can configure the basic details of the identity sources. After initial configuration, you can select the **Active Directory Queries** or **Browser-Based Authentication** checkboxes under Policy Configuration and click **Configure** to configure more advanced settings.

To configure User Awareness with the wizard:

1. Click the **configuration wizard** link.

The User Awareness Wizard opens.

2. Select one or more user identification methods (see above for descriptions of methods) and click **Next**.

For Active Directory Queries:

If you have an existing Active Directory server, click **Use existing Active Directory servers**.

To add a new Active Directory Domain:

1. Select **Active Directory Queries** and click **Configure**.

The **Active Directory Queries** window opens.

2. Select **Define a new Active Directory** server.
3. Enter:
 - **Domain**
 - **IPv4 address**
 - **User name**
 - **Password**
 - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.
4. To select user groups from specific branches, select the checkbox **Use user groups from specific branch only**. Click **Add** and enter a branch path in the **AD Branch** field.
5. Click **Apply**.

You can also add a new AD Domain in the **Users & Objects > Authentication Servers** page.

For Browser-Based Authentication:

1. To block access for unauthenticated users when the portal is not available, select **Block unauthenticated users when the captive portal is not applicable**. This configuration option forces users using non-HTTP traffic to login first through Browser-Based Authentication.
2. Select if unidentified users are redirected to Captive Portal for **All traffic** or **Specific destinations**. In most cases, all traffic is not used because it is not a seamless identification method.
3. Under Specific destinations, select **Internet** or **Selected network objects**. If you select **Selected network objects**, select the objects from the list or create new objects.
4. Click **Finish**.

To edit settings and configure portal customization for Browser-Based Authentication:

1. Under **Policy Configuration**, select **Browser-Based Authentication** and click **Configure**.
2. In the **Identification** tab, you can edit settings configured in the wizard if necessary.

3. In the **Customization** tab, select the relevant options:

- **Users must agree to the following conditions** - You can require that users agree to legal conditions. In the text box, enter the conditions that are shown to the user.
- **Upload** - Lets you upload a company logo. **Browse** to the logo file and click **Apply**. The logo is shown in the **Displayed Logo** section.
- **Use Default** - Uses the default logo.

4. In the **Advanced** tab:

- **Portal Address** - Keep the default setting which is the address the Captive Portal runs on the Check Point Appliance or enter a different portal address.
- **Session timeout** - Sets for how long an authenticated user can access the network or Internet before they have to authenticate again.
- **Enable Unregistered guests login** - Allow an unregistered, guest user to be identified in the logs by name and not only by IP address. An unregistered user is an unmanaged non-AD user, typically a partner or a contractor. To gain access, guests enter their company name, email address, phone number (optional), and name.

Configure the **Guest Session timeout**. This is the number of minutes for which a guest user can access network resources. The default timeout is 180 minutes.

Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.

- **Force quick cache timeout if user closes portal window** - When the portal is closed, the user is logged out.

5. Click **Apply**.

Note - This page is available from **Access Policy > User Awareness Blade Control** and **Users & Objects > User Awareness**.

Configuring the QoS Blade

In the **Access Policy > QoS Blade Control** page you can activate QoS, define the QoS default policy, and add manual rules.

The QoS (bandwidth control) policy is a set of rules that lets you set bandwidth parameters to control the flow of communication to and from your network. These rules make sure that important traffic is prioritized so your business can work with minimum disruption when there is network congestion.

QoS can be activated on Internet connections and requires at least one Internet connection to be configured with the maximum download and/or upload speeds provided by your ISP. For more information about your download and upload speeds, contact your local ISP.

This page lets you configure a default simplified QoS policy. You can configure a more advanced policy in the **Access Policy > QoS Policy** page.

QoS policy applies to traffic over external interfaces only.

QoS

Select one of the options to set the Access Policy control level:

- **On** - Enforces the default QoS policy.
- **Off** - QoS default policy is not enforced.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

QoS default policy

Select the options for your default QoS policy. Alternatively, you can define your entire QoS policy through the **Access Policy > QoS Policy** page by clearing all of the checkboxes on this page.

- **Ensure low latency priority for Delay Sensitive Services (e.g. VoIP)** - Select this option to make sure that traffic that is very sensitive to delay is prioritized. For example, IP telephony, videoconferencing, and interactive protocols that must have a short response time, such as Telnet.

Click the **Delay Sensitive Services** link to see the default services included and add new ones or remove existing if necessary. QoS tries to send these packets before other packets. This option adds a rule to the QoS Policy Rule Base.

- **Guarantee X% of the bandwidth to VPN/all traffic on all services** - Select this option to guarantee a minimum bandwidth for the specified traffic on all services or selected services.

Enter the bandwidth percentage, change the type of traffic if needed, and if necessary click the **all services** link to edit a list of selected guaranteed services. This option adds a rule to the QoS Policy Rule Base.

- **Limit Bandwidth Consuming Applications** - Applications that use a lot of bandwidth can decrease performance necessary for important business applications.

Click the **Bandwidth Consuming Applications** link to see the default applications/categories included and add new ones or remove existing if necessary.

Select the **Limit Bandwidth Consuming Applications** checkbox and select **Download** and/or **Upload** to determine where the limit is enforced and the maximum bandwidth in each of the selected options. Bandwidth consuming applications control can also be configured in the **Access Policy > Firewall Blade Control** and **Policy** pages.

To add a guaranteed service to the default policy:

1. Select the **Guarantee X% of the bandwidth to X traffic on all/selected services** option and click the **services** link.
The Edit guaranteed services window opens.
2. Select **Selected services**.
3. Click **Select** to show the full list of available services and select the relevant checkboxes.
4. Click **New** if the existing list does not contain the service you need. For information on creating a new service, see the **Users & Objects > Services** page.
5. Click **Apply**.

Working with QoS Policy

In the **Access Policy > QoS Policy** page you can manage the QoS default policy and add manual rules if necessary.

The top of the page shows information about these limits:

- **Bandwidth Consuming Applications** - If you set download and upload rates in the **Access Policy > QoS Blade Control** page or **Access Policy > Firewall Blade Control** page. If you see the **disabled** link, click it to configure the rates here.
- **Low latency traffic** - Shows the maximum percentage of bandwidth that can be reserved for low latency traffic. If you do not set a maximum percentage, traffic that does not require low latency might be starved (might not be handled at all). To change the value, click the **percentage** link.

You can view the QoS Policy Rule Base on this page. For each rule, you see these fields:

Rule Base Field	Description
No.	Rule number in the QoS policy.
Source	Network object that starts the connection.
Destination	Network object that completes the connection.
Service	Type of network service for which bandwidth is adjusted based on weight, limit, and guarantee.
Guarantee/Limit	Lets you set a percentage that limits the bandwidth rate of traffic and/or guarantees the minimum bandwidth for traffic. Another option is to mark the traffic as low latency. This guarantees that it is prioritized accordingly.
Weight	The unit used to divide available bandwidth when traffic exceeds the maximum bandwidth configured for the Internet connection. See below.
Track	The tracking and logging action that is done when traffic matches the rule.
Comment	An optional field that shows a comment if you entered one. For system generated rules of the default policy a Note is shown.

Weight

QoS divides available bandwidth across the QoS policy rules based on *weight*. The use of weights instead of specified percentages is a flexible way for the QoS engine to allocate bandwidth if the maximum bandwidth is exceeded based on the specified traffic at that point. This maximizes the usage of the bandwidth.

For example, in an organization, Web traffic is deemed three times as important as FTP traffic. Rules with these services are assigned weights of 30 and 10 respectively. If the lines are congested, QoS keeps the ratio of bandwidth allocated to Web traffic and FTP traffic at 3 to 1.

You can set options for the default policy or you can manually define rules for the QoS policy. If a rule does not use all of its bandwidth, the leftover bandwidth is divided with the remaining rules, based on their relative weights. In the above example, if only one Web and one FTP connection are active and they compete, the Web connection receives 75% (30/40) of the leftover bandwidth, and the FTP connection receives 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection receives 100% of the bandwidth.

In the **Weight** field, enter a value that shows the services importance relative to other defined services. For example, if you enter a weight of 100 for a service and set 50 for a different service, the first service is allocated two times the amount of bandwidth as the second when lines are congested.

To create a QoS rule:

1. Click the arrow next to **New**.
2. Click one of the available positioning options for the rule: **On Top**, **On Bottom**, **Above Selected**, or **Under Selected**.

The **Add Rule** window opens. It shows the rule fields in two manners:

- A rule summary sentence with default values.
 - A table with the rule base fields in a table.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the rule base fields. See the descriptions above.
- Note** - You can select for a specified rule to have a specified guarantee and/or limit or be marked as low latency traffic. In case of the latter, there is a single maximum limit percentage for ALL low latency traffic which can be configured globally. See above.
4. To match only for encrypted (VPN) traffic, select **Match only for encrypted traffic**. The Service column shows "encrypted" if selected.
 5. To limit the rule to a specified time range, select **Apply only during this time** and select the start and end times. Only connections that begin during this time range are inspected.
 6. DiffServ Mark is a way to mark connections so a third party handles it. To mark packets that are given priority on the public network based on their DSCP, select **DiffServ Mark (1-63)** and select a value. To use this option, your ISP or private WAN must support DiffServ. You can get the DSCP value from your ISP or private WAN administrator.
 7. In the **Write a comment** field, enter optional text that describes the rule. This is shown as a comment below the rule.
 8. Click **Apply**.

Note - You can drag and drop rules to change the order of rules in the QoS Rule Base.

To edit a rule:

Note - For Access Policy rules, you can only edit the tracking options for automatically generated rules.

1. Select a rule and click **Edit**.
2. Edit the fields as necessary.
3. Click **Apply**.

To delete a rule:

1. Select a rule and click **Delete**.
2. Click **Yes** in the confirmation message.

To enable or disable a rule:

- To disable a manually defined rule that you have added to the Rule Base, select the rule and click **Disable**.
- To enable a manually defined rule that you have previously disabled, select the rule and click **Enable**.

To change the rule order:

1. Select the rule to move.
2. Drag and drop it to the necessary position.

Note - You can only change the order of manually defined rules.

SSL Inspection Policy

SSL Inspection

The **Access Policy > SSL Inspection Policy** page lets you enable and configure SSL inspection. When you turn on this setting, you allow different Software Blades that support SSL inspection to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol. To allow the gateway to inspect the secured connections, all hosts behind the gateway must install the gateway CA certificate.

Software Blades that support SSL traffic inspection:

- Application & URL Filtering
- IPS
- Anti-Virus
- Anti-Bot
- Threat Emulation

Deploying SSL Inspection

To deploy SSL inspection:

1. Select **SSL Traffic Inspection**.
2. Click **Download CA Certificate** to download the gateway's internal CA certificate.

Note - The certificate is available for all users on the gateway. You do not need admin credentials. If you do not have admin credentials, connect from an internal or wireless network to `http://my.firewall/ica` or `https://<IP_Address_of_Appliance>/ica`.

You must install this certificate on every client behind the gateway.

To install the certificate:

1. Manually copy the certificate file to your PC.
2. In the Windows PC, click the file and follow the wizard instructions to add the certificate to the Trusted Root Certification Authorities repository.

Note - This is not the default repository in the Certificate Import Wizard.

Certificate installation varies according to the OS. To learn how to install the certificate in your machine, see your OS vendor instructions.

SSL inspection uses the existing internal CA by default. To use your own certificate, you must replace the internal CA.

To replace the internal CA:

1. Go to **Certificates > Internal Certificate**.
2. Click **Replace Internal CA**.

The **Upload a P12 Certificate** window opens.

3. Click **Browse** to select the certificate file.
4. Enter the **Certificate name** and **Password**.

5. Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.
6. Click **Apply**.

SSL Inspection Bypass Policy

You can select categories that are bypassed for all possible traffic regardless of its source and destination. To configure more advanced exceptions, go to the **SSL Inspection Exceptions** page.

To set the SSL inspection bypass policy:

- **Wireless networks to bypass** - Select or clear which wireless networks to bypass. **Untrusted networks** are selected by default.
Note - Wireless networks must be assigned to **Separate Network**, not switch or bridge.
- **Categories** - Select or clear the privacy related categories that are not inspected. All categories except for **Media Streams** are selected by default.
- **Tracking** - Select to enable logs to indicate that the SSL inspection policy decision was inspect or bypass.
Note - These logs are generated in addition to the logs generated by the Software Blades.

To add other categories:

Note - The **Bypass** checkbox is selected by default.

1. Click **other categories and sites**.
The **SSL Inspection Bypass Other** window opens.
2. Select the desired items.
3. **Optional** - Click **New** to add URLs or custom applications.
4. Click **Apply**.

HTTPS Categorization

As an alternative to SSL inspection, you can enable HTTPS categorization. HTTPS categorization allows filtering specified HTTPS URLs and applications without activating SSL traffic inspection.

For more information, see the [HTTPS Inspection video](#) on the [Small Business Security video channel](#).

To enable HTTPS categorization:

1. Select **HTTPS Categorization**.
Note - When you enable HTTPS categorization, the SSL options are not available.
2. Click **Configure**.
The **Access Policy > Firewall Blade Control** page opens.
3. Configure the settings for URL Filtering.
Note - HTTPS categorization only applies when the URL Filtering blade is turned on.

To disable SSL inspection and HTTPS categorization:

Select **Off**.

IMAPS

Internet Message Access Protocol (IMAP) is an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAPS refers to IMAP over SSL.

SSL traffic inspection must be activated to scan HTTP and IMAP encrypted traffic.

SSL Inspection Exceptions

On the **SSL Inspection Exceptions** page, you can define manual rules to configure exceptions to bypass SSL inspection for specific traffic. You can configure more advanced exceptions with specific scope, category, and tracking options.

To add bypass exceptions:

1. Click **New**.
2. For each exception, enter:
 - **Source**
 - **Destination**
 - **Category/Custom Application**
 - **Track**

SSL Inspection Advanced

To enable SSL web traffic inspection, you must first establish trust between the clients and the gateway.

An important part of the HTTPS inspection support is the validation of the server's certificate. This requires validating the signing CA of the server certificates.

On the **SSL Inspection Advanced** page, you can manage trusted certificate authorities. The gateway has a built-in predefined list of trusted CAs, based on the Mozilla/LibCurl Trusted CA list. Only a server certificate signed by one of those CAs is recognized as a valid certificate. The table shows the list of trusted CAs.

Trusted CA types:

- Default from the gateway - These CAs can be disabled but not deleted.
- Added by user - These CAs can be deleted.

To manually add a CA to the trusted CA list:

1. Click **Add**.
The **Add a Trusted CA** window opens.
2. Click **Browse** to select a trusted CA file.
3. **Optional** - Click **Preview** to view the CA.
4. Click **Apply**.

To delete a trusted CA:

1. Click the icon next to the CA.
2. Click **Delete**.
Note - You can only delete a CA that was added by a user.

To disable/enable a trusted CA:

1. Click the icon next to the CA.
2. Click **Disable/Enable**.

Managing Threat Prevention

This section describes how to set up and manage the Intrusion Prevention System (IPS), Anti-Virus, Anti-Bot, Threat Emulation, and Anti-Spam blades.

Configuring Threat Prevention Blade Control

In the **Threat Prevention > Threat Prevention Blade Control** page you can activate:

- **Intrusion Prevention System (IPS).** Blocks potentially malicious attempts to exploit known vulnerabilities in files and network protocols.
- **Anti-Virus.** Blocks potentially malicious files that are infected with viruses.
- **Anti-Bot.** Detects bots, prevents communication between the bot and its Command & Control center, and gives threat visibility. A *bot* is malicious software that can infect your computer with malware. A bot infected device can then be used by a Command & Control server to execute different types of attacks (send out SPAM messages or Denial-of-Service attacks against web sites). There are many infection methods. These include if you open attachments that exploit a vulnerability or access a web site that results in a malicious download.
- **Threat Emulation.** Gives networks protection against unknown threats in files that are downloaded from the Internet or attached to emails. In emulation, the file is opened on more than one virtual computer with different operating system environments. These virtual computers are closely monitored for unusual and malicious behavior. Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network. Information about malicious files is shared with Check Point ThreatCloud.

You configure all the settings for these blades in the same place and set a single profile for all of them.

To turn a blade on or off:

Move the slider.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

The update status is displayed next to each blade:

- Up to date
- Update available
- Update service unreachable

You can activate the blades to prevent attacks/infection or set them to detect-mode only on the **Threat Prevention Engine Settings** page. A warning message shows if a blade is in detect-only mode.

The top of the page shows the number of infected devices. For more information, click **More details**.

One policy is configured for all the blades:

- **Strict** - Focuses on security.
- **Recommended** - The default option, which gives the best mixture of security and performance for small/medium sized business.

Note - The performance impact for the "Suspicious Mail Activity" protection in Anti-Bot was changed to High and is now **off** by default. To enable this protection, you must configure it in a custom policy.

- **Custom** - Manually defined by the user.

To create a custom policy for Threat Prevention:

1. In the **Threat Prevention Blade Control** page, under **Policy**, select **Custom**.
2. For **Tracking options**, select one of these options:
 - **None** - Do not log.
 - **Log** - Create a log.
 - **Alert** - Log with an alert.
3. Under **Protection Activation**, for each confidence level (**High confidence**, **Medium confidence**, and **Low confidence**), select the applicable action from the list:
 - **Ask** - Traffic is blocked until the user confirms it is allowed.
 - **Prevent** - Blocks identified virus or bot traffic, or identified malicious files, from passing through the gateway.
 - **Detect** - Allows identified virus or bot traffic, or identified malicious files, to pass through the gateway. This traffic is detected and logged.
 - **Inactive** - The protection is deactivated.
4. For **Severity**, select the level:
 - **Low or above**
 - **Medium or above**
 - **High or above**
 - **Critical**
5. For **Performance impact**, select the allowed impact level:
 - **Low**
 - **Medium or lower**
 - **High or lower**
6. To load the policy default values, click **Load default settings**:
 - **Recommended**
 - **Strict**
7. To save all settings on the **Threat Prevention Blade Control** page, click **Apply**.

To schedule updates:

1. Click **Schedule**.

The **Activate Automatic Updates** window opens.

2. Select the Software Blades to receive automatic updates:

- IPS
- Anti-Virus
- Anti-Bot
- Application Control

3. Select the **Recurrence** and **Time of day**.

4. Click **Apply**.

Configuring Threat Prevention Policy Exceptions

In the **Threat Prevention > Threat Prevention Exceptions** page you can configure exception rules for traffic which the IPS engine and malware engine for Anti-Virus and Anti-Bot do not inspect.

Threat Prevention Exceptions

To add a new Threat Prevention exception rule:

1. In the **IPS Exceptions** section, click **New > Add**.
2. Configure these fields:
 - **Scope** - For Threat Prevention blades only. Threat Prevention inspects traffic to and/or from all objects specified in the Scope, even when the specified object did not open the connection. Can include network object, network object groups, IP address ranges and local users.

Select either Any or a specific scope from the list. If necessary, you can create a New network object, network object group, or local user.

If it is necessary to negate a specified scope, select the scope and select the Any Scope except checkbox.

For example, if the scope of the exception should include all scopes except for the DMZ network, select DMZ network and select the Any Scope except checkbox.
 - **Source** - Network object that initiates the connection.
 - **Destination** - Network object that is the target of the connection.
 - **Protection** - In the Blades tab, select Any for all or for a specific blade. In the IPS protections tab, select a specific IPS protection from the list.
 - **Service/Port** - Type of network service. If you make an exception for a specified protection on a specific service/port, you might cause the protection to be ineffective.
 - **Action** - Select the applicable action to enforce on the matching traffic: **Ask**, **Prevent**, **Detect** or **Inactive**. See the Threat Prevention > **Threat Prevention Blade Control** page for a description of the action types.
 - **Log** - Select the tracking option: **None**, **Log**, or **Alert**. Logs are shown on the **Logs & Monitoring > Security Logs** page. An alert is a flag on a log. You can use it to filter logs.
3. **Optional** - Add a comment in the Write a comment field.
4. Click **Apply**.

Whitelists

You can set specified files and URLs that the Anti-Virus, Anti-Bot and Threat Emulation blades do not scan or analyze. For example, if there are files that you know are safe but can create a false positive when analyzed, add them to the Files Whitelist.

Threat Emulation only: You can set specified email addresses that the blade does not scan and add them to the Email Addresses Whitelist.

To add a file or URL to the whitelist:

1. Select **Files Whitelist** or **URLs Whitelist**.
2. Click **New**.

The **Add File** or **Add URL** window opens.

3. For a file, enter the **MD5 checksum** that gives the digital signature for a specified file.
4. For a URL, enter the **URL**.
5. Click **Apply**.

To add an email address to the whitelist:

1. Select **Email Addresses Whitelist**.
2. Click **New**.

The **Add Email Address** window opens.

3. Enter the email address.
4. For **Type**, select Sender or Recipient.
5. Click **Apply**.

To edit or delete an exception rule:





1. Select the relevant rule.
2. Click **Edit** or **Delete**.

Viewing Infected Devices

In the **Infected Devices** page you can see information about infected devices and servers in the internal networks. You can also directly create an exception rule for a specified protection related to an infected or possibly infected device or server.

The Infected Devices table shows this information for each entry:

- Icon - Shows icons for the different classifications of infected devices and servers.

Description	Host Icon	Server Icon
Infected device or server - When the Anti-Bot blade detects suspicious communication between the host or server and an external Command & Control center due to a specified triggered protection		
Possibly infected device or server - When the Anti-Virus blade detects an activity that <i>may</i> result in host or server infection. For example: <ul style="list-style-type: none"> • When you browse to an infected or a potentially unsafe Internet site, there is a possibility that malware was installed. • When you download an infected file, there is a possibility that the file was opened or triggered and infected the host or server. 		

- Object name - Shows the object name if the host or server was configured as a network object.
- IP/MAC address
- Device/User Name - Shows a device or user name if the information is available to the Check Point Appliance through DHCP or User Awareness.
- **Incident type - Shows the detected incident type:**
 - Found bot activity
 - Downloaded a malware
 - Accessed a site known to contain malware
- **Severity - Shows the severity of the malware:**
 - Low
 - Medium
 - High
 - Critical
- Protection name - Shows the Anti-Bot or Anti-Virus protection name.
- Last incident - The date of the last incident.

- **Incidents** - Shows the total number of incidents on the device or server in the last month. If there is a large amount of records, the time frame may be shorter.

To filter the infected devices list:

1. Click **Filter**.
2. Select one of the filter options:
 - **Servers only** - Shows only machines that were identified as servers (and not any machine/device). Servers are defined as server objects in the system from the **Access Policy > Servers** page.
 - **Possibly infected only** - Shows only devices or servers classified as possibly infected.
 - **Infected only** - Shows only devices or servers classified as infected.
 - **High and above severity only** - Shows devices and servers that are infected or possibly infected with malwares that have a severity classification of high or critical.

To add a malware exception rule for a specified protection:

1. Select the list entry that contains the protection for which to create an exception.
2. Click **Add Protection Exception**.
3. Click the links in the rule summary or the table cells to select network objects or options that fill out the exception rule fields.
 - **Scope** - Select either Any or a specific scope from the list. If necessary, you can create a **New** network object, network object group, or local user.
If it is necessary to negate a specified scope, select the scope and select the **Any Scope except** checkbox.
For example, if the scope of the exception should include all scopes *except* for the DMZ network, select DMZ network and select the Any Scope except checkbox.
 - Note** - DMZ is not supported in 1550 appliances.
 - **Action** - Select the applicable action to enforce on the matching traffic: **Ask**, **Prevent**, **Detect** or **Inactive**. See the **Threat Prevention > Threat Prevention Blade Control** page for a description of the action types.
 - **Log** - Select the tracking option: **None**, **Log**, or **Alert**. Logs are shown on the **Logs & Monitoring > Security Logs** page. An alert is a flag on a log. You can use it to filter logs.
4. **Optional** - Add a comment in the **Write a comment** field.
5. Click **Apply**.

The rule is added to Malware Exceptions on the **Threat Prevention > Exceptions** page.

To view the logs of a specified entry:

1. Select the list entry for which to view logs.
2. Click **Logs**.

The **Logs & Monitoring > Security Logs** page opens and shows the logs applicable to the IP/MAC address.

Note - This page is available from the **Home** and **Logs & Monitoring** tabs.

Viewing the IPS Protections List

In the **Threat Prevention > IPS Protections List** page you can monitor specific protections, or manually configure a specific protection to override the general policy.

To search for a specified protection:

1. Enter a name in the **filter** box.
2. Scroll the pages with the next and previous page buttons at the bottom of the page.

To configure the IPS policy, go to the **Threat Prevention > Threat Prevention Blade Control** page. You can see the details of each protection and also configure a manual override for individual protections' action, and tracking options.

Advanced Threat Prevention Engine Settings

In the **Threat Prevention > Threat Prevention Engine Settings** page you can configure advanced configuration settings for the Anti-Virus, Anti-Bot, Threat Emulation, and IPS engines.

Note - Many of the configurations below are advanced and should only be used by experienced administrators.

IPS

Configure the settings for newly downloaded protections:

- Active
- Detect
- Inactive

To configure the IPS engine to bypass mode when the appliance is under heavy load:

1. Select the **Bypass under load** checkbox to activate the feature.
2. Click **Configure** to select the thresholds upon which IPS engine toggles between bypass and inspection modes. Follow the instructions in the window that opens and click **Apply**.

Thresholds are configured for CPU Usage and Memory Usage. There is always a high watermark and a low watermark. Bypass occurs when the high watermark is exceeded and the IPS engine continues inspection when the load drops below the low watermark. In this way when under load, the IPS engine does not toggle between modes too frequently.

3. In **Bypass under load tracking**, to configure tracking options for this feature, select what type of log to issue.

To enable Detect-only mode:

Click the checkbox.

To import IPS protections:

Click the link.

Anti-Virus

To configure the Anti-Virus settings:

1. Select one of the protected scope options:
 - **Scan incoming files from** - Select one of these interfaces from which to scan incoming files:
 - **External and DMZ** - Files that originate from external and the DMZ interfaces are inspected.

Note - DMZ is not supported in 1550 appliances.

- **External** - Files that originate from external interfaces are inspected.
 - **All** - Files transferred between all interfaces are inspected.
- **Scan both incoming and outgoing files** - Files that originate from outside the organization and from within the organization to the Internet are inspected.
2. Select the protocols to scan for the selected scope:
 - **HTTP (on any port)**
 - **Mail (SMTP, POP and IMAP)**
 - **FTP**

SSL traffic inspection must be activated to scan HTTP and **IMAP** encrypted traffic. To activate, click the link or go to **Access Policy > SSL Inspection Policy**.
 3. Select one of the file type policy options:
 - **Process file types known to contain malware**
 - **Process all file types**
 - **Process specific file type families** - Click **Configure** for a list of file types and set prescribed actions to take place when these files pass through the Anti-Virus engine. To edit an action for a specified file type, right-click the row and click **Edit**.

The available actions are:

 - **Scan** - The Anti-Virus engine scans files of this type.
 - **Block** - The Anti-Virus engine does not allow files of this type to pass through it.
 - **Pass** - The Anti-Virus engine does not inspect files of this type and lets them pass through.

You cannot delete system defined file types. System defined file types are recognized by built-in signatures that cannot be edited. Manually defined file types are recognized by their extension and are supported through the web and mail protocols.
 4. You can set **policy overrides** to override the general policy setting defined on the Threat Prevention Blade Control page. For each of the below protection type options, you can set the applicable override action: Ask, Prevent, Detect, Inactive, or According to policy (no override). See the **Threat Prevention > Threat Prevention Blade Control** page for a description of the action types.
 - **URLs with malware** - Protections related to URLs that are used for malware distribution and malware infection servers.
 - **Viruses** - Real-time protection from the latest malware and viruses by examining each file against the Check Point ThreatCloud database.

To enable Detect-only mode:

Click the checkbox.

Anti-Bot

You can set **policy overrides** to override the general policy settings defined on the **Threat Prevention Blade Control** page. For each of the below protection type options, you can set the applicable override action: Ask, Prevent, Detect, Inactive, or According to policy (no override). See the **Threat Prevention > Threat Prevention Blade Control** page for a description of the action types.

- **Malicious activity** - Protections related to unique communication patterns of botnet and malware specified families.
- **Reputation domains** - Protections related to Command & Control (C&C) servers. Each host is checked against the Check Point ThreatCloud reputation database.
- **Reputation IPs** - Protections related to Command & Control (C&C) servers. Each IP is checked against the Check Point ThreatCloud reputation database.
- **Reputation URLs** - Protections related to Command & Control (C&C) servers. Each URL is checked against the Check Point ThreatCloud reputation database.
- **Unusual activity** - Protections related to the behavioral patterns common to botnet and malware activity.

To enable Detect-only mode:

Click the checkbox.

Threat Emulation

To configure the Threat Emulation settings:

1. Select one of the protected scope options:

- **Scan Incoming files from - Select one of these interfaces from which to scan incoming files:**

- **External and DMZ** - Files that originate from external and the DMZ interfaces are inspected.

Note - DMZ is not supported in 1550 appliances.

- **External** - Files that originate from external interfaces are inspected.
- **All** - Files transferred between all interfaces are inspected.

Note - LAN to LAN scanning is not supported.

- **Scan both incoming and outgoing files** - Files that originate from outside the organization and from within the organization to the Internet are inspected.

2. Select the protocols to scan for the selected scope:

- HTTP (on any port)
- Mail (SMTP, POP3 and IMAP).

SSL traffic inspection must be activated to scan HTTP and IMAP encrypted traffic. To activate, click the link or go to **Access Policy > SSL Inspection Policy**.

3. For file type policy:

- **Process specific file type families** - Click **Configure** for a list of file types and set prescribed actions to take place when these files pass through the Threat Emulation engine.

To edit an action for a specified file type, right-click the row and click **Edit**. You can also click the file type so it is selected and then click **Edit**.

The available actions are:

- **Inspect** - The Threat Emulation engine inspects files of this type.
- **Bypass** - The Threat Emulation engine does not inspect files of this type and lets them pass through.

You cannot delete system defined file types. System defined file types are recognized by built-in signatures that cannot be edited.

4. Select the HTTP connection emulation handling mode:

- **Background** - Connections are allowed until emulation is complete.
- **Hold** - Connections are blocked until emulation is complete.

In Threat Emulation, each file is run in the Check Point Public ThreatCloud to see if the file is malicious. The verdict is returned to the gateway.

To configure multiple remote emulators, you must use CLI commands.

For more information on Threat Emulation, see the [Threat Emulation video](#) on the [Small Business Security video channel](#).

To enable Detect-only mode:

Click the checkbox.

User Messages

You can customize messages for protection types set with the Ask action. When traffic is matched for a protection type that is set to Ask, the user's internet browser shows the message in a new window.

These are the Ask options and their related notifications:

Option	Anti-Virus Notification	Anti-Bot Notification
Ask	Shows a message to users and asks them if they want to continue to access a site or download a file that was classified as malicious.	Shows a message to users and notifies them that their computer is trying to access a malicious server.
Block	Shows a message to users and blocks the site.	Anti-Bot blocks background processes. If a specified operation from a browser to a malicious server is blocked, a message is shown to the user.

To customize messages:

1. Click **Customize Anti-Virus user message** or **Customize Anti-Bot user message**.
2. Configure the options in each of these tabs:
 - Ask
 - Block
3. Configure the applicable fields for the notifications:
 - **Title** - Keep the default or enter a different title.
 - **Subject** - Keep the default or enter a different subject.
 - **Body** - Keep the default or enter different body text. You can click **Optional keywords** for a list of keywords that you can add in the body text to give the user more information.
 - **Ignore text** (only for Ask) - If the user decides to ignore the message, this is the text that is shown next to the checkbox. Keep the default text or enter different text.
 - **User must enter a reason** (only for Ask) - Select this checkbox if users must enter an explanation for their activity. The user message contains a text box to enter the reason.
 - **Fallback action** (only for Ask) - Select an alternative action (Block or Accept) for when the notification cannot be shown in the browser or application that caused the notification, most notably in non-web applications.
 - If the Fallback action is **Accept** - The user can access the website or application.
 - If the Fallback action is **Block** - The website or application is blocked, and the user does not see a notification.
 - **Frequency** - You can set the number of times that the Anti-Virus, Anti-Bot, or Threat Emulation Ask user message is shown.
 - **Once a day**
 - **Once a week**
 - **Once a month**
 - **Redirect the user to a URL (only for block) -**
 You can redirect the user to an external portal, not on the gateway. In the URL field, enter the URL for the external portal. The specified URL can be an external system. It gets authentications credentials from the user, such as a user name or password. It sends this information to the gateway.
4. Click the **Customize** tab to customize a logo for all portals shown by the appliance (Hotspot and captive portal used by User Awareness). Click **Upload**, browse to the logo file and click **Apply**. If necessary, you can revert to the default logo by clicking **Use Default**.
5. Click **Apply**.

Configuring the Anti-Spam Blade Control

In the **Threat Prevention > Anti-Spam Blade Control** page you can activate the Anti-Spam engine to block or flag emails that are contain known or suspected spam content.

On this page you can activate the blade to identify, block or flag such emails or set it to detect mode only and use the logs to understand if your system is experiencing spam attacks.

Check Point can identify spam emails by their source address (most spam emails) and also the email content itself. You can configure the system to simply flag emails with spam content instead of blocking them and then configure your internal email server to use this flag to decide how to handle them. Flag is a common use case if you do not want to lose emails that are suspected of spam. The content of emails is inspected in the cloud and the appliance is notified how to handle the emails.

You can handle suspected spam the same way as known spam, or select the checkbox to handle suspected spam separately (see below).

To enable/disable the Anti-Spam blade:

1. Select **On** or **Off**.
2. Click **Apply**.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

To configure the Anti-Spam engine to work in detect only mode:

1. Select the **Detect-only mode** checkbox.
2. Click **Apply**.

In Detect-only mode, only logs appear and the blade does not block any emails.

To configure the Anti-Spam Policy:

The spam filter is always based on inspecting the senders' source address. This is a quick way to handle the majority of spam emails. In addition, you can configure to filter the rest of the spam emails by inspecting the email content. Make sure the **Email content** checkbox is selected. Select the action to perform on emails whose content was found to contain spam:

- **Block spam emails**
- **Flag spam email subject with X** - Replace X with manually defined text to add to the subject line for spam emails.
- **Flag spam email header** - This option identifies email as spam in the email message header.

Select the relevant **tracking option** - Log or Alert (shown as a highly important log).

To handle suspected spam separately from known spam:

1. Click **Handle suspected spam separately**.
2. Select an option: block, flag email subject, or flag email header.

When selecting a *flag* option, it is possible to modify the text string used to flag the suspected spam emails. The default is "[SUSPECTED SPAM]". You can choose the flag option for Spam and for Suspected Spam. Use this option to have a different string for the flag action.

3. Select a tracking option.
4. Click **Apply**.

Configuring Anti-Spam Exceptions

In the **Threat Prevention > Anti-Spam Exceptions** page you can configure:

- Safe senders (email addresses) and/or domains or IP addresses from which emails are not inspected.
- Specific senders and/or domains or IP addresses that Anti-Spam engine blocks regardless of its own classification.

To block or allow by senders requires the Anti-Spam engine to be configured to filter based on **Email content** in the **Threat Prevention > Anti-Spam Blade Control** page.

Note - IP address exceptions are ignored for POP3 traffic.

To add a new sender/domain/IP address to the Allow or Block list:

1. Click **Add** or **New** in the Allow or Block list.
2. Enter the **IP address** or **Sender/Domain**.
3. Click **Apply**.

To edit or delete a sender/domain/IP address from the Allow or Block list:

1. Select the relevant row in the Allow or Block list.
2. Click **Edit** or **Delete**. If the options are not visible, click the arrows next to the filter box.

Managing VPN

This section describes how to set up and manage Remote Access and Site to Site VPN.

Configuring the Remote Access Blade

In the **VPN > Remote Access Blade Control** page you can establish secure encrypted connections between devices such as mobile devices, home desktops and laptops, and the organization through the Internet.

For remote access, you must define users in the system with credentials and set permissions for specified users. The appliance must be accessible from the Internet.

Note - Remote Access applies to traffic from IPv4 addresses only.

These are supported remote access connection methods:

- Install a VPN client on the home desktops or laptops.
- Browse from home devices (using secure HTTPS) to the appliance and download a thin client when necessary. This method is known as SSL Network Extender.

We highly recommend that you first configure DDNS or a static IP Internet connection on the appliance. If you do not use a static IP, your appliance's IP address can vary based on to your Internet Service Provider. DDNS lets home users connect to the organization by name and not IP address that can change. See **Device > DDNS** for more details.

To configure DDNS, click the **DDNS** link or the **Internet** link for static IP.

To enable or disable VPN Remote Access:

1. Select **On** or **Off**.
2. Click **Apply**.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

To configure the default access policy through remote access:

1. Select or clear the **Allow traffic from Remote Access users (by default)** checkbox. When cleared, access from Remote Access users to resources in the organization must be defined for each resource using the **Access Policy > Servers** page or by manually defining access rules in the **Access Policy > Firewall Policy** page.
2. Select or clear the **Log traffic from Remote Access users (by default)** checkbox.
3. Click **Apply**.

VPN Remote Access methods:

- **Check Point VPN clients** - To connect laptops and desktops
- **Mobile client** - To connect smartphones and tablets
- **SSLVPN** - To connect through SSL VPN

- **Windows VPN Client** - To connect through native VPN client (L2TP)

By default, **Check Point VPN clients** is enabled.

To configure VPN remote access methods:

1. Select the checkbox next to the desired method and click **How to connect...**
The Usage window opens.
2. Follow the instructions. You can also receive these instructions by email.
3. Close the window and click **Apply**.

To manage SSL VPN bookmarks:

1. Select the **SSL VPN** checkbox.
2. Click **Apply**.
3. Click **Manage SSL VPN bookmarks**.
The **VPN > Advanced** page opens.
4. In **SSL VPN bookmarks**, click **New** to create new bookmarks.
A new window opens.
5. Enter these details:

- **URL**

Note - If you select Global bookmark, all users see this bookmark.

- **Type** - Link or RDP (remote desktop protocol)
- **Label** - The bookmark name
- **Tooltip** - Description

6. Click **Apply**.

If you select RDP as the bookmark type, you must enter the user name and password in the **RDP Advanced Settings**. These credentials are sent to the end user.

Note - If you select **Show characters**, the password characters are visible.

You can also specify the screen size of the remote desktop. The default mode is full screen.

To manage bookmarks:

1. Click on a bookmark.
2. Click **Edit** or **Delete**.
3. Click **Apply**

To assign a VPN certificate:

1. Select the **SSL VPN** check box.
2. Click **Certificate authentication**.

The Certificate authentication window opens. The list of uploaded certificates shows in the drop down menu.

3. Select the certificate name.

Note - You cannot select the default Web portal certificate.

4. Click **Apply**.

To send users remote access usage instructions:

1. Click the **How to connect** link next to the relevant remote access method.
2. Click the **E-mail these instructions** to automatically open a pre-filled email that contains the instructions.
3. Click **Close**.

To change the Remote Access port settings:

If the default remote access port (port 443) and a server use the same port, a conflict message shows. You must change the default remote access port if the Check Point VPN client, Mobile client, or SSL VPN remote access methods are enabled as they use port 443 by default.

1. Click the **Change port** link.
The Remote Access Port Settings window opens.
2. In **Remote Access port**, enter a new port number.
3. Make sure **Reserve port 443 for port forwarding** is selected.
4. Click **Apply**.

Configuring Remote Access Users

In the **VPN > Remote Access Users** page you can configure remote access permissions for users and groups.

Users and user groups can be configured in other pages as well (**Users & Objects > Users**). This page is dedicated to those with remote access permissions. You can add through it:

- New local users
- New users groups
- Active Directory group
- Active Directory permissions
- RADIUS group

You can also set SSL VPN bookmarks by user, user group, RADIUS users and Active Directory group.

If no authentication servers are defined, click the **Active Directory / RADIUS** server link to define them.

Note that when User Awareness is turned off, there is no user identification based on Browser-Based Authentication and Active Directory Queries.

To add a new local user with remote access permissions:

1. Click **Add > New Local User**.
2. In the **Remote Access** tab in the window that opens, enter this information:
 - **User name**
 - **Password** - Enter this again in the **Confirm** field.
Note - The password can be up to 100 characters.
 - **Comments** (optional)
3. For temporary or guest users, click **Temporary user**.
Enter the expiration date and time.
4. Do not clear the **Remote Access permissions** checkbox.
5. In the **SSL VPN Bookmarks** tab, configure the SSL VPN bookmarks (see below).
6. Click **Apply**.
The user is added to the table on the page.

To add a new local users group with remote access permissions:

1. Click **Add > New Users Group**.
2. In the **Remote Access** tab, enter the group name.
3. Do not clear the **Remote Access permissions** checkbox.

4. Select initial users to add to the group by clicking the relevant checkboxes from the user list or click **New** to create new users.

You can see a summary of the group members above the user list. You can remove members by clicking the **X** next to the relevant user name.

5. In the **SSL VPN Bookmarks** tab, configure the SSL VPN bookmarks (see below).
6. Click **Apply**.

The group is added to the table on the page.

To add remote access permissions to an existing Active Directory group:

1. Click **Add > Active Directory Group**.
2. If no Active Directory was defined, you are prompted to configure one. For more information on configuring Active Directory see **VPN > Authentication Servers**.
3. When an Active Directory has been defined, you see a list of available user groups defined in the server.
4. Select one of the user groups.
5. Click **Apply**.

The Active Directory group is added to the table on the page.

To add remote access permissions to all users in defined in an Active Directory:

1. Click **Edit Permissions** or **Add > Active Directory Permissions**.
2. Select **All users in Active Directory**. With this option, it is not necessary to use the **VPN > Remote Access Users** page to select specific users.

Note that most Active Directories contain a large list of users and you might not want to grant them all remote access permissions to your organization. Usually you keep the **Selected Active Directory user groups** option.

3. Click **Apply**.

The Active Directory is added to the table on the page.

To add remote access permissions for users defined in the RADIUS group:

1. Click **Add > RADIUS Group**.
2. If no RADIUS group was defined, you are prompted to configure one.
3. Select or clear the **Enable RADIUS authentication for remote access users** checkbox.

4. When selected, choose which users are given remote access permissions:
 - To allow all users defined in the RADIUS server to authenticate - Select **All users defined on RADIUS server**
 - Specific user groups defined in the RADIUS server - Select **For specific RADIUS groups only** and enter in the text field the names of the user groups separated by commas
 - To allow administrators with read-only permissions to authenticate - **Select Read-only Administrators**
5. Click **Apply**.

The RADIUS server or specific users from the RADIUS server are added to the table on the page.

To configure SSL VPN bookmarks:

1. Click **Add > New Local User/Users Group/Active Directory Group > SSL VPN Bookmarks** tab.
A new window opens.
2. Enter new bookmarks or select existing bookmarks.
Note - If you select **Global bookmark**, this bookmark is always shown.
3. Click **Apply**.

To edit a user or group:

1. Select the user or group from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete a user or group:

1. Select the user or group from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

The user or group is deleted.

Remote Access Connected Remote Users

The **VPN Remote Access > Connected Remote Users** page shows the currently connected remote users:

- Username
- IP address
- Connection Time
- Next Authentication Time

Configuring Remote Access Authentication Servers

In the **Authentication Servers** page you can define and view different authentication servers where users can define both an external user database and the authentication method for users in that database.

You can define these types of authentication servers:

- **RADIUS server** - Define the details of a primary and secondary RADIUS server. The Check Point Appliance can connect to these servers and recognize users defined in them and authenticated by them.
- **Active Directory domain** - Define the details of the Active Directory domain that contains your organization's user information. The User Awareness feature can use these details to provide seamless recognition of users for logging purposes and user based policy configuration. This can be used for VPN remote access user authentication. When this is the case, additional configuration is necessary in the **VPN > Remote Access Users** page.

To add a RADIUS server:

1. Click **Configure**.
2. In the Primary tab, enter this information:
 - **IP address** - The IP address of the RADIUS server.
 - **Port** - The port number through which the RADIUS server communicates with clients. The default is 1812.
 - **Shared secret** - The secret (pre-shared information used for message "encryption") between the RADIUS server and the Check Point Appliance. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ` " # + \
 - **Show** - Displays the shared secret.
 - **Timeout** (seconds) - A timeout value in seconds for communication with the RADIUS server. The timeout default is 3 seconds.
3. Repeat step 2 for a Secondary RADIUS server if applicable.
4. Click **Apply**.

Note - if you want to remove information you entered in IP address and shared secret, you can click **Clear**.

The primary and secondary servers (if defined) are added to the RADIUS section on the page.

RADIUS servers can be used for:

- Defining a database of users with remote access privileges. Such users are both defined and authenticated by the RADIUS server.
- Defining administrators. See the **Users & Objects > Administrators** page.

To edit a RADIUS server:

1. Click the IP address link of the RADIUS server you want to edit.
2. Make the necessary changes.

3. Click **Apply**.

The changes are updated in the RADIUS server.

To delete a RADIUS server:

Click the **Remove** link next to the RADIUS server you want to delete.

To configure remote access permissions for users defined in the RADIUS server:

1. Click **permissions for RADIUS users**.
2. Select or clear the **Enable RADIUS authentication for remote access users** checkbox.
3. When selected, choose which users are given remote access permissions:
 - To allow all users defined in the RADIUS server to authenticate - Select **All users defined on RADIUS server**
 - Specific user groups defined in the RADIUS server - Select **For specific RADIUS groups only** and enter in the text field the names of the user groups separated by commas.
 - To allow administrators with Read-only permissions to authenticate - Select **Read-only Administrators**
4. Click **Apply**.

To add an Active Directory domain:

1. In the Active Directory section, click **New**.
The **Add new Domain** window opens.
2. Enter this information:
 - **Domain** - The domain name.
 - **IP address** - The IP address of one of the domain controllers of your domain.
 - **User name** - The user must have administrator privileges to ease the configuration process and create a user based policy using the users defined in the Active Directory.
 - **Password** - The user's password. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ' " # + \
 - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually. For example: CN=John James,OU=RnD,OU=Germany,O=Europe,DC=Acme,DC=com
3. Select **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory. Enter the branch in the Branch full DN in the text field.
4. Click **Apply**.

When an Active Directory is defined, you can select it from the table and choose **Edit** or **Delete** when necessary.

When you edit, note that the Domain information is read-only and cannot be changed.

When you add a new Active Directory domain, you cannot create another object using an existing domain.

To configure remote access permissions for all users defined in Active Directory:

By default, users defined in the Active Directory are not given remote access permissions. Instead, in the **VPN > Remote Access Users** page all users defined locally or in Active Directories can be selected to be granted remote access permissions per user.

1. Click **permissions for Active Directory users**.
2. Select **All users in the Active Directory**. With this option, it is not necessary to go to the **VPN > Remote Access Users** page and select specific users.

Note that most Active Directories contain a large list of users and you might not want to grant them all remote access permissions to your organization. Usually you keep the **Selected Active Directory user groups** option and configure remote access permissions through **VPN > Remote Access Users** page.

3. Click **Apply**.

To change synchronization mode with the defined Active Directories:

1. Click **Configure** in the toolbar of the Active Directory table.
2. Select one of the options - **Automatic synchronization** or **Manual synchronization**.

When Manual synchronization is selected, you can sync the user database known to the appliance in all locations that this user database can be viewed. For example, the **Users & Objects > Users** page or the Source picker in the Firewall Rule Base in the **Access Policy > Firewall Policy** page.

Note - You cannot select a user from the Active Directory, only an Active Directory user group. You can select a local user.

3. Click **Apply**.

To edit an Active Directory:

1. Select the Active Directory from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete an Active Directory:

1. Select the Active Directory from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

Note - This page is available from the **VPN** and **Users & Objects** tabs.

Configuring Advanced Remote Access Options

In the **VPN > Remote Access Advanced** page you can configure more advanced settings to determine VPN remote access users' behavior.

You can also add bookmarks (HTML links or RDP links) for specified URLs or computers when you connect through SSL VPN (see below). The next time you log in, your bookmarks are shown.

What is Office Mode?

Remote access VPN clients connect through a VPN tunnel from their homes to the appliance and from there they can gain access into the organization's resources.

The appliance assigns each remote access user an IP address from a specified network so that the traffic inside the organization is not aware that it originated from outside the organization.

This technology is called Office Mode and the network used for supplying the IP addresses is configurable.

To configure the Office Mode network:

1. Enter the **Office Network address** and **Office Subnet Mask**.
2. Click **Apply**. The default setting for office mode is 172.16.10.0\24.

To assign a VPN certificate:

1. Click the downward arrow next to the **VPN Remote Access certificate** field.
The list of uploaded certificates shows.
2. Select the desired certificate.
Note - You cannot select the default Web portal certificate.
3. Click **Apply**.

To route all traffic from VPN remote access clients through the gateway:

1. Select the **Route Internet traffic from connected clients through this gateway** checkbox.
2. Click **Apply**.

Normally, only traffic from the VPN clients into the organization's encryption domain is encrypted and sent through the VPN tunnel to the gateway. Selecting the above checkbox causes all traffic from the VPN clients to be encrypted and sent to the gateway. Traffic to locations outside the organization are enforced in this case by the outgoing access Policy. For more information, see **Access Policy Firewall Blade Control** and **Policy** pages.

Note - This setting does not apply to traffic from SSL Network Extender clients.

To manually configure a local encryption domain for remote access users only:

The local encryption domains are the internal networks accessible by encrypted traffic from remote access VPN users. By default, the local encryption domain is determined automatically by the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local encryption domain.

Optionally, you can manually create a local encryption domain to be used by remote access users only instead. It is possible to configure a different manual local encryption domain for VPN remote access and VPN site to site. See **VPN > Site to Site Blade Control** page.

1. Click on the local encryption domain link: **automatically according to topology** or **manually**. The link shown is a reflection of what is currently configured.
2. Select **Define local network topology manually**.
3. Click **Select** to show the full list of available networks and choose the relevant checkboxes.
4. Click **New** if the existing list does not contain the networks you need. For information on creating a new network object, see the **Users & Objects > Network Objects** page.
5. Click **Apply**.

The Remote Access Local Encryption Domain window opens and shows the services you selected.

DNS Servers for Remote Access users

You can define up to three DNS servers for Remote Access clients. By default, the **Office mode first DNS for clients** is set to this gateway.

To use a different DNS Primary server:

1. Click **Configure manually**.
2. In **Office mode first DNS for clients**, enter the IP address of a server to use as the DNS server.
3. Click **Apply**.

DNS domain name

You can set a DNS domain name that the Remote Access clients' devices automatically use to attempt to resolve non-FQDN domains. By default, the suffix is automatically configured to take the DNS domain name configured in the DNS page.

To configure a manual DNS domain name:

1. Click **Configure manually**.
2. In **DNS domain name**, enter the DNS domain name suffix to use.
3. Click **Apply**.

To configure the DNS domain name to be the same as the defined DNS domain name:

1. Click **Configure automatically**.
2. Click **Apply**.

The DNS domain name shows the text "Same as DNS domain name".

To configure SSL VPN bookmarks:

1. Click **Add > New Local User/Users Group/Active Directory Group > SSL VPN Bookmarks** tab.
A new window opens.
2. Enter new bookmarks or select existing bookmarks.
Note - If you select **Global bookmark**, this bookmark is always shown.
3. Click **Apply**.

To set SSL VPN bookmarks:

1. In **SSL VPN bookmarks**, click **New** to create new bookmarks.

A new window opens.

2. Enter these details:

- **URL**

Note - If you select **Global bookmark**, this bookmark is shown to all users.

- **Type** - Link or RDP (remote desktop protocol)

- **Label** - The bookmark name

- **Tooltip** - Description

3. Click **Apply**.

If you select RDP as the bookmark type, you must enter the user name and password in the **RDP Advanced Settings**. These credentials are sent to the end user.

Note - If **Show characters** is selected, the password characters are shown.

You can also specify the screen size of the remote desktop. The default mode is full screen.

To manage bookmarks:

1. Click on a bookmark.
2. Click **Edit** or **Delete**.
3. Click **Apply**.

Configuring the Site to Site VPN Blade

In the **VPN > Site to Site Blade Control** page you can activate the appliance's ability to create VPN tunnels with remote sites. Site to Site VPN can connect two networks separated by the Internet through a secure encrypted VPN tunnel. This allows for seamless secure interaction between the two networks within the same organization even though they are physically distant from each other.

On this page you can activate the blade to allow site to site connectivity. You can view how many sites are already defined and configure basic access policy from the remote sites into the specific network accessible by this gateway.

The remote site can be accessible through another Check Point appliance (recommended) or a 3rd party VPN solution.

Once defined, access to the remote site is determined by the incoming/internal/VPN traffic Rule Base as seen in the **Access Policy > FirewallPolicy** page. This is due to the fact that the remote site's encryption domain is considered part of the organization even though traffic to it is technically outgoing to the Internet (since it is now VPN traffic).

To enable/disable the VPN Site to Site blade:

1. Select **On** or **Off**.
2. Click **Apply**.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally will be overridden in the next synchronization between the gateway and Cloud Services.

A warning icon is shown if the blade is active but no VPN sites are defined. Click **VPN Sites** to add a VPN site or see how many VPN sites are defined. The full list of the sites is located in **VPN > Site to Site VPN Sites**.

To configure the default access policy from remote VPN sites:

1. Select or clear the **Allow traffic from remote sites (by default)** checkbox. It is not recommended to clear this checkbox, as the remote site is usually part of your organization.
2. Select or clear the **Log remote sites traffic (by default)** checkbox.
3. Click **Apply**.

Local Encryption Domain

The local encryption domain defines the internal networks accessible by encrypted traffic from remote sites and networks, that traffic from them to remote sites is encrypted. By default, the local encryption domain is determined automatically by the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local encryption domain. Optionally, you can manually create a local encryption domain instead. See the **VPN > Site to Site Advanced** page for instructions.

Configuring VPN Sites

In the **VPN > Site to Site VPN Sites** page you can configure remote VPN sites. For more on how to configure site to site VPN, go to **VPN > Site to Site Blade Control**.

When you add a new VPN site, these are the tabs where you configure these details:

- **Remote Site** - Name, connection type, authentication method (preshared secret or certificate), and the Remote Site Encryption Domain.
- **Encryption** - Change the default settings for encryption and authentication details.
- **Advanced** - Enable permanent tunnels, disable NAT for this site, configure encryption method, and additional certificate matching.

To add a new VPN site:

1. Click **New**.

The **New VPN Site** window opens in the **Remote Site** tab.

2. Enter the **Site name**.

3. **Select the Connection type:**

- **Host name or IP address** - Enter the **IP address** or **Host name**. If you select IP address, and it is necessary to configure a static NAT IP address, select **Behind static NAT** and enter the IP address.

Note - Behind static NAT applies to IPv4 addresses only.

- **High Availability or Load Sharing** - Configure a list of backup IP addresses in case of failure (High Availability) or to distribute data (Load Sharing). The appliance uses probing to monitor the remote site's IP addresses. In High Availability, you can configure one of the IP addresses as the primary.

When you select this option, you must configure a probing method on the **Advanced** tab. The probing method monitors which IP addresses to use for VPN: ongoing or one at a time. Click **New** to add an **IP address** and set a **Primary IP address** if necessary for High Availability.

- **Only remote site initiates VPN** - Connections can only be initiated from the remote site to this appliance. For example, when the remote site is hidden behind a NAT device. In this scenario, this appliance only responds to the tunnel initiation requests. This requires a secure method of remote site authentication and identification.

4. Select an authentication method. This must match the authentication you used to configure this appliance as the other gateway's remote site.

- **Preshared secret** - If you select this option, enter the same **password** as configured in the remote gateway and **confirm** it. **Note** - You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | \ " # + \
- **Certificate** - The gateway uses its own certificate to authenticate itself. For more information, see **VPN > Internal Certificate**.

5. Select the **Remote Site Encryption Domain**. Configure the conditions to encrypt traffic and send to this remote site.
 - **Define remote network topology manually** - Traffic is encrypted when the destination is included in the list of network objects. Click **Select** to select the networks that represent the remote site's internal networks. Click **New** to create network objects.
 - **Route all traffic through this site** - All traffic is encrypted and sent to this remote site. You cannot configure more than one remote site.
 - **Encrypt according to routing table** - If you use dynamic routing, encrypts traffic based on source or service and destination. You must create a virtual tunnel interface (VTI) in the **Device > Local Network** page and associate it with this remote site. You can then use this VTI to create routing rules. Traffic that matches these routing rules is encrypted and routed to the remote site.
 - **Hidden behind external IP of the remote gateway** - If the remote site is behind NAT and traffic is initiated from behind the remote site to this gateway. When you select this option, it is not necessary to define an encryption domain.
6. **Exclude networks** - Select this option to exclude networks from the specified encryption domain. This may be useful if two gateways are in the same community and protect the same parts of the network.
7. Click **Apply**.

In the **Encryption** tab you can change the default settings. There are built in encryption settings' groups that only need to match in this configuration and in the remote site.

- **Default (most compatible)**
- **VPN A** - According to RFC4308.
- **VPN B** - According to RFC4308.
- **Suite-B GCM-128 or 256** - According to RFC6379.
- **Custom** - Select this option to manually decide which encryption method is used (optional).

In the **Advanced** tab:

- **Settings**
 - Select to configure if the remote site is a Check Point Security Gateway. To enable permanent VPN tunnels, click the checkbox.
 - Select to disable NAT for this site. The original IP addresses are used even if hide NAT is defined.
- **Encryption method**

Select the IKE version:

 - IKEv1
 - IKEv2
 - Prefer IKEv2, support IKEv1

If you select **IKEv1**:

The modes for IKE negotiation are main mode and aggressive mode. For IKE negotiation, main mode uses six packets and aggressive mode uses three packets. We recommend you use main mode which is more secure. By default, **Enable aggressive mode** is *not* selected and main mode is used. Enable aggressive mode only if necessary and the other side of the VPN tunnel does not support main mode. (Third party gateways primarily do not work in main mode.)

Aggressive mode is used to create a tunnel and one of the gateways is behind NAT. In this case, a pre-shared secret does not provide enough data for authentication in main mode. Authentication must be done using a certificate and a gateway (peer) ID, or a secondary identifier couple that is available in aggressive mode. The secondary identifier method is also available in IKEv2.

If you select **Enable aggressive mode for IKEv1**:

- **Use Diffie-Hellman group** - Determines the strength of the shared DH key used in IKE phase 1 to exchange keys for IKE phase 2. A group with more bits ensures a stronger key but lower performance.
- **Initiate VPN tunnel using this gateway's identifier** - When this gateway's IP address is dynamic and the authentication method is the certificate and the peer ID, you must enter the **Gateway ID**. For **Type**, select domain name or user name.

For more information on installing the certificate, see ["Managing Installed Certificates" on page 95](#).

Notes:

- The initiator's gateway ID must be set in the responder gateway as the peer ID.
- The Remote Access blade must be enabled for peer ID to work.
- On the gateway that is not behind NAT, for **Connection type**, select **Only remote site initiates VPN**.
- When you configure the remote site, do not select behind static NAT.

If you select **IKEv2**:

When you create a tunnel and one of the gateways is behind NAT without a certificate (uses a pre-shared secret), with IKEv2 protocol you can use a secondary identifier couple to allow authentication. In this case, the pre-shared secret is not enough.

Select to **Create IKEv2 VPN tunnel using these identifiers**:

- **Peer ID** - Enter the identifier.
- **Gateway ID** - Select **Use global identifier** or **Override global identifier** (enter the new identifier).

If you select **Prefer IKEv2, support IKEv1**, configure the fields as explained for the first two options.

- **Additional Certificate Matching** (does not apply when you use a pre-shared secret):

When you select certificate matching in the **Remote Site** tab, you first need to add the CA that signed the remote site's certificate in the **VPN > Certificates Trusted CAs** page. In the **Advanced** tab, you can select to match the certificate to **Any Trusted CA** or an **Internal CA**. You can also configure more matching criteria on the certificate.

■ Probing Method

This section is shown only when you select High Availability or Load Sharing for the connection type in the **Remote Site** tab. When the remote site has multiple IP addresses for VPN traffic, the correct address for VPN is discovered through one of these probing methods:

- **Ongoing probing** - When a session is initiated, all possible destination IP addresses continuously receive RDP packets until one of them responds. Connections go through the first IP to respond (or to a primary IP if a primary IP is configured and active for High Availability), and stay with this IP until the IP stops responding. The RDP probing is activated when a connection is opened and continues a background process.
- **One time probing** - When a session is initiated, all possible destination IP addresses receive an RDP session to test the route. The first IP to respond is chosen, and stays chosen until the VPN configuration changes.

When you finish the new VPN site configuration, click **Apply**.

An initial tunnel test begins with the remote site. If you have not yet configured it, click **Skip**. The VPN site is added to the table.

Locally managed gateways can be part of these site to site communities:

- **VPN mesh community** - All gateways are connected to each other, and each gateway handles its own internet traffic. Encrypted traffic is passed from networks in the encryption domain of one gateway to the networks in the encryption domain of the second gateway.
- **VPN star community** - One gateway is the center and routes all traffic (encrypted and internet traffic of the remote peer) to the internet and back to the remote peer. The peer gateway is a satellite and is configured to route all its traffic through the center.

To configure a gateway as the center:

1. Select the VPN site from the list.
2. Click **Edit**.

The **Edit VPN Site** window opens.

3. In the **Remote Site** tab:
 - For **Connection type**, enter the IP address which is the public IP of the remote peer (satellite gateway).
 - In the **Encryption domain**, select the networks of the satellite gateway that will participate in the VPN.
4. In the **Advanced** tab, select **Allow traffic to the internet from remote site through this gateway**.
5. Click **Apply**.

This gateway is now designated as the center. Hide NAT is done automatically in the center gateway.

To configure a gateway as a satellite:

1. Select the VPN site from the list.
2. Click **Edit**.

The **Edit VPN Site** window opens.

3. **In the Remote Site tab:**

- For **Connection type**, enter the IP address which is the public IP of the remote peer (center gateway).
- In the **Encryption domain**, select **Route all traffic through this site**.

4. Click **Apply**.

This gateway is now designated as a satellite.

You can configure more than one satellite gateway to route all traffic through the center gateway.

If you try to configure two gateways to be the center, an error message shows.

If you do not configure one gateway as a center, the site to site VPN acts like a mesh community and each gateway continues to handle its own traffic.

To run a tunnel test with a remote site:

Check Point uses a proprietary protocol to test if VPN tunnels are active. It supports any site-to-site VPN configuration. Tunnel testing requires two Security Gateways and uses UDP port 18234. Check Point tunnel testing protocol does not support 3rd party Security Gateways.

1. Select an existing site from the list.
2. Click **Test**.

To edit a VPN site:

1. Select the VPN site from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete a VPN site:

1. Select the VPN site from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

The VPN site is deleted.

To disable or enable the VPN site:

1. Select the VPN site from the list.
2. Click **Disable** or **Enable**.

VPN Community Use Cases

Q1: A system administrator is responsible for 6 gateways and wants to share network resources between the satellite branches. Which type of VPN community is preferable?

A1: A star VPN community is preferable as every gateway does not have to create a VPN tunnel with all of the others. Instead, the 5 satellite peer gateways will each create one site to site star VPN community to the center gateway. Only the star gateway (center) must create a site to site from itself to each of the remote peers.

Q2: A center gateway handles all the traffic in the VPN community. When the gateway reboots, all the other gateways' internet traffic is affected, and they lose access to the remote peer encryption domain until the center gateway comes back up. How can the administrator avoid this downtime?

A2: In this case, a mesh community is better as each gateway can handle its own internet traffic and is not affected by any other gateway.

Configuring Advanced Site to Site Community Settings

Note - This page is relevant only if Cloud Services is turned on.

In the **VPN > Site to Site Community** page you can see details of the community members configured for this appliance by Cloud Services. The information here is read-only and you cannot update details. The settings configured by Cloud Services for the **VPN > Site to Site** software blade are used by the community members.

The Community page shows:

- The name of the community configured by the Cloud Services Provider.
- A table with the sites that are part of the community.

To test the VPN connection for a site:

1. Select the site.
2. Click **Test**.

If the test succeeds, a success message is shown. Click **OK** to close it.

If the test does not succeed, click **Details** for more information. If applicable, click **Retry**.

To see the details of a site configured by Cloud Services:

Select a site and click **View Details**.

The View Site Details window opens and shows:

- Remote site details - Name, host or IP address, authentication method (preshared secret or certificate), and the Remote Site Encryption Domain
- Encryption settings - IKE (Phase 1) and IPSec (Phase 2) settings
- Advanced settings - Encryption method and certificate matching

For descriptions of the fields in the site details tabs, see ["Configuring VPN Sites" on page 195](#).

Viewing VPN Tunnels

In the **VPN Tunnels** page you can see current VPN tunnels opened between this gateway and remote sites. Some sites are configured so tunnels are established only when necessary and some are configured with permanent tunnels. When the appliance is managed by Cloud Services, this table also shows the tunnels for the gateways in the community.

This page is commonly used to see the permanent tunnels. The table shows each tunnel's details when there is an active VPN tunnel.

Field	Description
From	Host name or IP address of the tunnel's source gateway.
Site Name	Name of the VPN site name.
Peer Address	Host name or IP address of the tunnel's destination gateway.
Community Name	If the gateways are part of a community configured by Cloud Services, the community name with which the tunnel is associated.
Status	VPN tunnel status indication.

To filter the list:

In the **Type to filter** box, enter the filter criteria.

The list is filtered.

To refresh the list:

Click **Refresh** to manually refresh this page with updated tunnel information.

Note - This page is available from the **VPN** and **Logs & Monitoring** tabs.

Configuring Advanced Site to Site Settings

In the **VPN > Site to Site Advanced** page you can configure global advanced options that define how the appliance connects to remote sites.

The configuration options on this page answer these configuration questions:

- When to open a connection with a remote site - See "Configuring a Local Encryption Domain" below. In addition, the remote site's encryption domain is configured per site. See the **VPN > Site to Site VPN Sites** page.
- How the appliance connects to remote sites - See "Configuring the Appliance's Outgoing Interfaces for VPN usage below.

Configuring a Local Encryption Domain

In domain based VPN, traffic is encrypted when it originates in one encryption domain and is transmitted to a different domain.

The local encryption domain defines:

- The internal networks that encrypted traffic from remote sites and networks can get access.
- That traffic from the encryption domain to remote sites is encrypted.

By default, the local encryption domain is determined automatically by the appliance. Networks behind LAN interfaces and trusted wireless networks are part of the local encryption domain. Optionally, you can manually create a local encryption domain if necessary.

To manually configure a local encryption domain:

1. Click the **automatically according to topology** link.
2. Select **Define local network topology manually**.
3. Click **Select** to show the full list of available networks and select the applicable checkboxes.
4. Click **New** if the existing list does not contain the necessary networks required. For information on how to create a new network object, see the **Users & Objects > Network Objects** page.
5. Click **Apply**.

The Site to Site Local Encryption Domain window opens and shows the services you selected.

Configuring the Appliance's Interfaces

Link Selection is a method used to:

- Specify which interface is used for incoming and outgoing VPN traffic.
- Determine the best possible path for the traffic.

In addition, with the Link Selection mechanisms, the administrator can select which source IP addresses are used for VPN traffic.

The default configuration to select an outgoing interface and source IP address is for the device to determine them automatically. Alternatively, you can change the default settings and select other means to determine:

- The appliance's outgoing interface
- The appliance's source IP address

To configure the appliance's outgoing interfaces and source IP address for VPN:

1. In the **Link Selection > Outgoing interface selection** section, select a method to specify the outgoing interface:
 - **According to the routing table** - The OS's routing table finds the interface link with the lowest metric (highest priority) through which to send traffic based on the remote site's IP addresses.
 - **Route based probing** - This method also consults the routing table for the link with the lowest metric. But, before choosing an interface link to send traffic, all routing possibilities are examined. This is to make sure that the link is active. The gateway selects the best match (highest prefix length) active route with the lowest metric (highest priority). This method is recommended when there is more than one external interface.
2. In the **Source IP address selection** section, select an option to configure the source IP address used by the Security Gateway, when it initiates or responds to VPN traffic. This IP address is normally used by the remote sites to connect to this Security Gateway:
 - **Automatically chosen according to outgoing interface.**
 - **Manually configured** - Enter an IP address that is always used as the source IP address of a VPN tunnel.

Tunnel Health Monitoring

Dead Peer Detection (DPD) is an additional keepalive mechanism supported by the Check Point Security Gateway to test if VPN tunnels are active. DPD uses IPsec traffic to minimize the number of messages required to confirm the availability of a peer and requires an IPsec established tunnel. The DPD mechanism is based on IKE encryption keys only.

The feature also allows you to monitor permanent tunnels based on DPD for both IKEv1 and IKEv2.

In **active mode**, a peer that is configured as DPD receives DPD Hello requests at regular intervals if there is no incoming IPsec traffic for 10 seconds.

To test if a VPN tunnel is active:

Select a Tunnel health monitoring method

- **Tunnel test (Check Point Proprietary)** - Works only between Check Point gateways.
- **DPD (Dead Peer Detection)**

In **DPD responder mode**, the Check Point gateway sends the IKEv1 Vendor ID to peers from which the DPD Vendor ID was received and answers incoming DPD packets.

To enable DPD responder mode:

Click the checkbox.

Managing Trusted CAs

In the **VPN > Certificates Trusted CAs** page you can add CAs used by remote sites' certificates to enable a VPN or WebUI certificate. A certificate shown by the remote site must be signed by a CA that is trusted by the appliance. Trusted CAs include both intermediate and root CAs.

This page also shows the built in Internal CA that by default creates the certificates for this appliance. It can also be used to sign remote sites' certificates. You can also export the internal CA to add it to a remote site's trusted CA list.

When Cloud Services is turned on and the appliance is configured by a Cloud Services Provider, the CA of the Cloud Services Provider is downloaded automatically to the appliance. The Cloud Services Provider CA is used by community members configured by Cloud Services. Note that if you turn Cloud Services off, the Cloud Services Provider CA is removed.

Recommended configurations

When you use certificate based site to site VPN with only one remote site, we recommend you export each site's Internal CA and add it to the other site's Trusted CA list.

When you use certificate based site to site VPN with multiple remote sites, in a mesh configuration, we recommend for all sites to use one CA to sign their internally used certificates on appliances that support creating signing requests. You must also add the same CA to all sites' Trusted CAs list. That CA can be an external CA service like Verisign (for a fee) or simply use this appliance's Internal CA. See below how to use it to sign external requests.

To add a trusted CA:

1. Click **Add**.
2. Click **Browse** to upload a CA's identifier file (a .CRT file).
3. A **CA name** is suggested, but you can enter another name if preferred. Click **Preview CA details** to see further information from the .CRT file.
4. Click **Apply**. The CA is added to the Trusted CA list.

To edit a trusted CA's configuration:

1. Select the CA from the list.
2. Click **Edit**. The Edit window opens.
3. **Select the necessary options regarding CRL (Certificate Revocation List):**
 - **Retrieve CRL from HTTP Server(s)** - HTTP can be used to access the CA for CRL retrieval. When cleared, this appliance does not attempt to validate the remote site's certificate's CRL.
 - **Cache CRL on the Security Gateway - Select how often is a new updated CRL is retrieved.**
 - **Fetch new CRL when expires** - Upon expiration of the CRL.
 - **Fetch new CRL every X hours** - Regardless of CRL expiration.

4. Click **Details** to see full CA details.
5. Click **Apply**.

To delete a trusted CA:

1. Select the trusted CA from the list and click **Delete**.
2. Click **OK** in the confirmation message.

To export the Internal CA (or other previously imported CAs):

1. Select the Internal CA in the table.
2. Click **Export**. The Internal CA's identifier file is downloaded through your browser and is available to be imported to the remote site's trusted CA list.
3. You can also export other trusted CAs you've added to the list if necessary by selecting them and clicking Export.

To sign a remote site's certificate request by the Internal CA:

1. Click **Sign a Request**. A file upload window opens.
2. Click **Browse** to upload the signing request file as created in the remote site. In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.
3. Click **Download**. The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

Managing Installed Certificates

On the **Installed Certificates** page, you can create and manage appliance certificates or upload a P12 certificate. Uploaded certificates and the default certificates are displayed in a table. To see certificate details, click the certificate name.

You can upload a certificate signed by an intermediate CA or root CA. All intermediate and root CAs found in the P12 file are automatically uploaded to the trusted CAs list.

Note - This page is available from the **Device** and **VPN** tabs.

On the **VPN Remote Access Blade Control** page, after you enable the SSL VPN feature, you can select and assign a certificate from the list of the installed certificates (with the exception of the Default Web Portal certificate). You can also do this on the **Remote Access Advanced** tab.

On the **Device > Device Details** page, you can select and assign a Web portal certificate from the list of installed certificates (with the exception of the Default certificate).

Installed certificates are used in site-to-site VPN, SSL VPN, and the Web portal.

When Cloud Services is turned on and the appliance is configured by Cloud Services, the Cloud Services Provider certificate is downloaded automatically to the appliance. The Cloud Services Provider certificate is used by community members configured by Cloud Services. **Note** - If you turn Cloud Services off, the Cloud Services Provider certificate is removed.

These are the steps to create a signed certificate:

1. Create a signing request.
2. Export the signed request (download the signing request from the appliance).
3. Send the signing request to the CA.
4. When you receive the signed certificate from the CA, upload it to the appliance.

To create a new certificate to be signed by a CA:

1. Click **New Signing Request**. The New Certificate Request window opens.
2. Enter a **Certificate** name.
3. In the **Subject DN** enter a distinguished name (e.g. CN=myGateway).
4. **Optional** - to add alternate names for the certificate, click **New**. Select the **Type** and enter the **Alternate name** and click **Apply**.
5. Click **Generate**.

The new signing request is added to the table and the status shows "Waiting for signed certificate".

Note - You cannot edit the request after it is created.

If the new signing request is signed by the Internal CA and the Organization Name is not defined in the DN, the Internal CA automatically generates the Organization Name.

To export the signing request:

Click **Export**.

To upload the signed certificate when you receive the signed certificate from the CA:

1. Select the signing request entry from the table.
2. Click **Upload Signed Certificate**.
3. Browse to the signed certificate file (*.crt).
4. Click **Complete**.

The status of the installed certificate record changes from "Waiting for signed certificate" to "Verified".

To upload a P12 file:

1. Click **Upload P12 Certificate**.
2. Browse to the file.
3. Edit the **Certificate name** if necessary.
4. Enter the certificate **password**.
5. Click **Apply**.

Managing Internal Certificates

In the **Certificates Internal Certificate** page you can view details of an internal VPN certificate. You can also view and reinitialize the certificate used by the internal CA that signed the certificate and can be used to sign external certificates.

Note - This page is available from the **Device** and **VPN** tabs.

When you create an internal VPN certificate, when a certificate that is signed by the internal CA is used, the CA's certificate must be reinitialized when the Internet connection's IP addresses change.

To avoid constant reinitialization, we recommend you use the DDNS feature. See **Device > DDNS**. When DDNS is configured, you only need to reinitialize the certificate once. Changes in the DDNS feature configuration by default automatically reinitialize certificates.

To reinitialize certificates:

1. Click **Reinitialize Certificates**.

The Reinitialize Certificates window opens.

2. Enter the **Host/IP address**.

Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.

3. Select the number of years for which the Internal VPN Certificate is valid. The default is 3. The maximum value allowed is 20.
4. Click **Apply**.

Note - The internal VPN certificate expiration date cannot be later than the CA expiration date.

To replace an internal CA certificate:

1. Click **Replace Internal CA Certificate**.

The Upload a P12 Certificate window opens.

2. Click **Browse** to select the CA certificate file that includes the private key.
3. Enter the **Certificate name** and private key's password to allow the device to sign certificates with the uploaded CA.
4. Enter the **Host/IP address**.

Normally, the device suggests its own host name (when DDNS is configured) or its external IP address. If you have multiple Internet connections configured, in load sharing mode, you can manually enter an accessible IP address for this appliance. This is used by remote sites to access the internal CA and check for certificate revocation.

5. Click **Apply**.

To export an internal CA certificate:

Click **Export Internal CA Certificate** to download the internal CA certificate.

To sign a remote site's certificate request by the internal CA:

1. Click **Sign a Request**. A file upload window opens.
2. Click **Browse** to upload the signing request file as created in the remote site. In third party appliances, make sure to look in its Administration Guide to see where signing requests are created.

The file must be in a path accessible to the appliance. After you click **OK** in the file browsing window, the file is uploaded. If it is correctly formatted, it is signed by the Internal CA and the **Download** button is available.
3. Click **Download**. The signed certificate is downloaded through your browser and is available to be imported to the remote site's certificates list.

Managing Users and Objects

This section describes how to set up and manage users (User Awareness, users, administrators, and authentication servers) and network resources.

Working with User Awareness

In the **User Awareness** page you can turn the blade on or off and use the configuration wizard to configure sources to get user identities, for logging and configuration purposes.

User Awareness lets you configure the Check Point Appliance to show user based logs instead of IP address based logs and enforce access control for individual users and user groups.

To use User Awareness, you must configure identification methods to get information about users and user groups. After the gateway acquires the identity of a user, user-based rules can be enforced on the network traffic in the Access Policy.

User Awareness can use these sources to identify users:

- **Active Directory Queries** - Seamlessly queries the AD (Active Directory) servers to get user information.
- **Browser-Based Authentication** - Uses a portal to authenticate either locally defined users or as a backup to other identification methods.

AD Query

The Check Point Appliance registers to receive security event logs from the AD domain controllers when the security policy is installed. This requires administrator privileges for the AD server. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The Check Point Appliance can then identify the user based on the AD security event log.

Browser-Based Authentication

Browser-Based Authentication uses a web interface to authenticate users before they can access network resources or the Internet. When users try to access a protected resource, they must log in to a web page to continue. This is a method that identifies locally defined users or users that were not successfully identified by other methods. You can configure the Browser-Based Authentication to appear for all traffic but because this method of identification is not seamless to the end users, it is commonly configured to appear when you access only specific network resources or the Internet to avoid the overhead required from end users when they identify themselves. For traffic that is not HTTP based, you can also configure that all unidentified are blocked from accessing the configured resources or Internet until they identify themselves first through the Browser-Based Authentication.

To turn on User Awareness on or off:

Select the **On** or **Off** option.

Note - When the blade is managed by Cloud Services, a lock icon is shown. You cannot toggle between the on and off states. If you change other policy settings, the change is temporary. Any changes made locally are overridden in the next synchronization between the gateway and Cloud Services.

Use the User Awareness configuration wizard to enable and configure the blade. You can configure the basic details of the identity sources. After initial configuration, you can select the **Active Directory Queries** or **Browser-Based Authentication** checkboxes under Policy Configuration and click **Configure** to configure more advanced settings.

To configure User Awareness with the wizard:

1. Click the **configuration wizard** link.
The User Awareness Wizard opens.
2. Select one or more user identification methods (see above for descriptions of methods) and click **Next**.

For Active Directory Queries:

If you have an existing Active Directory server, click **Use existing Active Directory servers**.

To add a new Active Directory Domain:

1. Select **Active Directory Queries** and click **Configure**.
The **Active Directory Queries** window opens.
2. Select **Define a new Active Directory** server.
3. Enter:
 - **Domain**
 - **IPv4 address**
 - **User name**
 - **Password**
 - **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.
4. To select user groups from specific branches, select the checkbox **Use user groups from specific branch only**. Click **Add** and enter a branch path in the **AD Branch** field.
5. Click **Apply**.

You can also add a new AD Domain in the **Users & Objects > Authentication Servers** page.

For Browser-Based Authentication:

1. To block access for unauthenticated users when the portal is not available, select **Block unauthenticated users when the captive portal is not applicable**. This configuration option forces users using non-HTTP traffic to login first through Browser-Based Authentication.
2. Select if unidentified users are redirected to Captive Portal for **All traffic** or **Specific destinations**. In most cases, all traffic is not used because it is not a seamless identification method.
3. Under Specific destinations, select **Internet** or **Selected network objects**. If you select **Selected network objects**, select the objects from the list or create new objects.
4. Click **Finish**.

To edit settings and configure portal customization for Browser-Based Authentication:

1. Under **Policy Configuration**, select **Browser-Based Authentication** and click **Configure**.
2. In the **Identification** tab, you can edit settings configured in the wizard if necessary.

3. In the **Customization** tab, select the relevant options:

- **Users must agree to the following conditions** - You can require that users agree to legal conditions. In the text box, enter the conditions that are shown to the user.
- **Upload** - Lets you upload a company logo. **Browse** to the logo file and click **Apply**. The logo is shown in the **Displayed Logo** section.
- **Use Default** - Uses the default logo.

4. In the **Advanced** tab:

- **Portal Address** - Keep the default setting which is the address the Captive Portal runs on the Check Point Appliance or enter a different portal address.
- **Session timeout** - Sets for how long an authenticated user can access the network or Internet before they have to authenticate again.
- **Enable Unregistered guests login** - Allow an unregistered, guest user to be identified in the logs by name and not only by IP address. An unregistered user is an unmanaged non-AD user, typically a partner or a contractor. To gain access, guests enter their company name, email address, phone number (optional), and name.

Configure the **Guest Session timeout**. This is the number of minutes for which a guest user can access network resources. The default timeout is 180 minutes.

Guest access is logged. The name of the guest shows in the **User** column of the **Logs and Monitoring** tab. The other details show in the full log entry.

- **Force quick cache timeout if user closes portal window** - When the portal is closed, the user is logged out.

5. Click **Apply**.

Note - This page is available from **Access Policy > User Awareness Blade Control** and **Users & Objects > User Awareness**.

Configuring Local Users and User Groups

In the **Users & Objects > Users** page you can create local users and user groups. To use these objects in the Access Policy, make sure to activate User Awareness.

User objects are used to define the different terms under which users can operate. These include:

- The time frame during which users are allowed to access the network.
- If users can work remotely.

To add a new local user:

1. Click **New > Local User**.
2. Enter a **User name**, **Password**, and **Comments** (optional). You cannot use these characters when you enter a password or shared secret: { } [] \ ~ | ` " # + \

The password can be up to 100 characters.
3. For temporary or guest users, click **Temporary user**.

Enter the expiration date and time.
4. To give the user remote access permissions, select **Remote Access permissions**.
5. Click **Apply**.

The user is added to the table on the page.

To add a new local users group with remote access permissions:

1. Click **New > Users Group**.
2. Enter a **Group name**.
3. To give the group remote access permissions, select **Remote Access permissions**.
4. To select initial users to add to the group, click the relevant checkboxes from the user list or click **New** to create new users.

You can see a summary of the group members above the user list.
5. To remove a user, click the X next to the user name.
6. Click **Apply**.

The group is added to the table on the page.

To automatically delete expired local users:

1. Go to **Device > Advanced Settings**.
2. Select **User Management**.
3. Click **Edit**.

The **User Management** window opens.
4. Click the checkbox for **Automatically delete expired local users**.

5. Click **Apply**.

Expired local users are automatically deleted every 24 hours (after midnight).

To edit a user or group:

1. Select the user or group from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete a user or group:

1. Select the user or group from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

The user or group is deleted.

Configuring Local and Remote System Administrators

The **Device > Administrators** page lists the Check Point Appliance administrators and lets you:

- Create new local administrators.
- Configure the session timeout.
- Limit login failure attempts.
- Generate a QR code to connect the mobile application with the appliance for the first time.

Administrators can also be defined in a remote RADIUS server and you can configure the appliance to allow them access. Authentication of those remotely defined administrators is done by the same RADIUS server.

Administrator Roles:

- **Super Administrator** - All permissions. Super Administrators can create new locally defined administrators and change permissions for others.
- **Read Only Administrator** - Limited permissions. Read Only Administrators cannot update appliance configuration but can change their own passwords or run a traffic monitoring report from the Tools page.
- **Networking Administrator** - Limited permissions. Networking Administrators can update or modify operating system settings. They can select a service or network object but cannot create or modify it.
- **Mobile Administrator** - Mobile administrators are allowed all networking operations on all interfaces. They can change their own passwords, generate reports, reboot, change events and mobile policy, active hosts operations and pairing. They cannot login from or access the WebUI.

Two administrators with write permissions cannot log in at the same time. If an administrator is already logged in, a message shows. You can choose to log in with Read-Only permission or to continue. If you continue the login process, the first administrator session ends automatically.

The correct Administrator Role must be configured to perform the operations listed below. If not, a **Permission Error** message shows.

To create a local administrator:

1. Click **New**.

The **Add Administrator** page opens.

2. Configure the parameters (name, password, and password confirmation). The hyphen (-) character is allowed in the administrator name. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ' " # + \
3. Select the **Administrator Role**.
4. Click **Apply**.

The name and Administrator Role is added to the table. When logged in to the WebUI, the administrator name and role is shown at the top of the page.

To edit the details of locally defined administrators:

1. Select the administrator from the table and click **Edit**.
2. Make the relevant changes.
3. Click **Apply**.

To delete a locally defined administrator:

1. Select an administrator from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

Note - You cannot delete an administrator who is currently logged in.

To allow access for administrators defined in a remote RADIUS server:

1. Make sure administrators are defined in the remote RADIUS server.
2. Make sure a RADIUS server is defined on the appliance. If there is no server, click the **RADIUS configuration** link at the top of this page. You must configure the IP address and shared secret used by the RADIUS server.
3. When you have a configured RADIUS server, click **edit permissions**.

The **RADIUS Authentication** window opens.

4. Click the **Enable RADIUS authentication for administrators** checkbox.

Use roles defined on RADIUS server is selected by default.

5. Configure the role for each user on the RADIUS server. See additional details below.

Note - A user without role definition will get a login error.

6. If you select **Use default role for RADIUS users**, select the **Administrators Role**:
 - Super Admin
 - Read only
 - Networking Admin
 - Mobile Admin
7. To define groups, click **Use specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
8. Click **Apply**.

To set the Session Timeout value for both local and remotely defined administrators:

1. Click **Security Settings**.

The **Administrators Security Settings** window opens.

2. Configure the session timeout (maximum time period of inactivity in minutes). The maximum value is 999 minutes.
3. To limit login failure attempts, click the **Limit administrators login failure attempts** checkbox.
4. Enter the number of **Maximum consecutive login attempts** allowed before an administrator is locked out.
5. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.
6. To enforce password complexity on administrators, click the checkbox and enter the number of days for the password to expire.
7. Click **Apply**.

Note - This page is available from the **Device** and **Users & Objects** tabs.

To connect the mobile application with the appliance for the first time:

1. Click **Mobile Pairing Code**.

The **Connect Mobile Device** window opens.

2. Select an administrator from the pull down menu.
3. Click **Generate**.

This generates a QR code to connect the Check Point WatchTower mobile application with the appliance for the first time.

For more information about the mobile application, see the [Check Point SMB WatchTower App User Guide](#).

Configuring a RADIUS Server for non-local Check Point Appliance users:

Non-local users can be defined on a RADIUS server and not in the Check Point Appliance. When a non-local user logs in to the appliance, the RADIUS server authenticates the user and assigns the applicable permissions. You must configure the RADIUS server to correctly authenticate and authorize non-local users.

Note - The configuration of the RADIUS Servers may change according to the type of operating system on which the RADIUS Server is installed.

Note - If you define a RADIUS user with a null password (on the RADIUS server), the appliance cannot authenticate that user.

To configure a Steel-Belted RADIUS server for non-local appliance users:

1. Create the dictionary file `checkpoint.dct` on the RADIUS server, in the default dictionary directory (that contains `radius.dct`). Add these lines to the file:

```
@radius.dct

MACRO CheckPoint-VSA(t,s) 26 [vid=2620 type1=%t% len1=+2
data=%s%]

ATTRIBUTE CP-Gaia-User-RoleCheckPoint-VSA(229, string) r
ATTRIBUTE CP-Gaia-SuperUser-AccessCheckPoint-VSA(230,
integer) r
```

2. Add the following lines to the `vendor.ini` file on RADIUS server (keep in alphabetical order with the other vendor products in this file):

```
vendor-product = Check Point Appliance
dictionary = nokiaipso
ignore-ports = no
port-number-usage = per-port-type
help-id = 2000
```

3. Add to the `dictionary.dcm` file the line:
"`@checkpoint.dct`"
4. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

CP-Gaia-User-Role = *<role>*

Where *<role>* allowed values are:

Administrator Role	Value
Super Admin	adminRole
Read only	monitorrole
Networking Admin	networkingrole
Mobile Admin	mobilerole

To configure a FreeRADIUS server for non-local appliance users:

1. Create the dictionary file `dictionary.checkpoint` in `/etc/freeradius/` on the RADIUS server:

```
#Check Point dictionary file for freeradius AAA server

VENDORCheckPoint2620
ATTRIBUTE CP-Gaia-User-Role 229 string
CheckPoint
ATTRIBUTE CP-Gaia-SuperUser-Access 230 integer
CheckPoint
```

2. Add to `/etc/freeradius/dictionary` the line:
`"$INCLUDEdictionary.checkpoint"`
3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

CP-Gaia-User-Role = *<role>*

Where *<role>* is the name of the administrator role that is defined in the WebUI.

Administrator Role	Value
Super Admin	adminRole
Read only	monitorrole
Networking Admin	networkingrole
Mobile Admin	mobilerole

To configure an OpenRADIUS server for non-local appliance users:

1. Create the dictionary file `dict.checkpoint` in
`/etc/openradius/subdicts/`
on the RADIUS server:

```
# Check Point Gaia vendor specific attributes
# (Formatted for the OpenRADIUS RADIUS server.)
# Add this file to etc/openradius/subdicts/ and add the line
# "$include subdicts/dict.checkpoint" to
etc/openradius/dictionaries
# right after dict.ascend.

$add vendor 2620 CheckPoint

$set default vendor=CheckPoint
    space=RAD-VSA-STD
    len_ofs=1 len_size=1 len_adj=0
    val_ofs=2 val_size=-2 val_type=String
    nodec=0 noenc=0

$add attribute 229CP-Gaia-User-Role
$add attribute 230CP-Gaia-SuperUser-Accessval_type=Integer
val_size=4
```

2. Add the line
`$include subdicts/dict.checkpoint`
to
`/etc/openradius/dictionaries`
immediately after `dict.ascend`

3. Add this Check Point Vendor-Specific Attribute to users in your RADIUS server user configuration file:

`CP-Gaia-User-Role = <role>`

Where `<role>` is the name of the administrator role that is defined in the WebUI.

Administrator Role	Value
Super Admin	<code>adminRole</code>
Read only	<code>monitorrole</code>
Networking Admin	<code>networkingrole</code>
Mobile Admin	<code>mobilerole</code>

To log in as a Super User:

A user with super user permissions can use the Check Point Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Check Point Appliance platform using an SSH client or serial console client.
2. Log in to the Clish shell using your user name and password.
3. Run `Expert`
4. Enter the expert password.

Managing Authentication Servers

In the **Authentication Servers** page you can define and view different authentication servers where users can define both an external user database and the authentication method for users in that database.

You can define these types of authentication servers:

- **RADIUS server** - Define the details of a primary and secondary RADIUS server. The Check Point Appliance can connect to these servers and recognize users defined in them and authenticated by them.
- **Active Directory domain** - Define the details of the Active Directory domain that contains your organization's user information. The User Awareness feature can use these details to provide seamless recognition of users for logging purposes and user based policy configuration. This can be used for VPN remote access user authentication. When this is the case, additional configuration is necessary in the **VPN > Remote Access Users** page.

To add a RADIUS server:

1. Click **Configure**.
2. In the Primary tab, enter this information:
 - **IP address** - The IP address of the RADIUS server.
 - **Port** - The port number through which the RADIUS server communicates with clients. The default is 1812.
 - **Shared secret** - The secret (pre-shared information used for message "encryption") between the RADIUS server and the Check Point Appliance. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ` " # + \
 - **Show** - Displays the shared secret.
 - **Timeout (seconds)** - A timeout value in seconds for communication with the RADIUS server. The timeout default is 3 seconds.
3. Repeat step 2 for a Secondary RADIUS server if applicable.

Note - If you want to remove information you entered in IP address and shared secret, you can click **Clear**.

4. Click **Apply**.

The primary and secondary servers (if defined) are added to the RADIUS section on the page.

RADIUS servers can be used for:

- Defining a database of users with remote access privileges. Such users are both defined and authenticated by the RADIUS server.
- Defining administrators. See the **Users & Objects > Administrators** page.

To edit a RADIUS server:

1. Click the IP address link of the RADIUS server you want to edit.
2. Make the necessary changes.

3. Click **Apply**.

The changes are updated in the RADIUS server.

To delete a RADIUS server:

Click the **Remove** link next to the RADIUS server you want to delete.

The RADIUS server is deleted.

To configure remote access permissions for users defined in the RADIUS server:

1. Click **permissions for RADIUS users**.
2. Select or clear the **Enable RADIUS authentication for User Awareness, Remote Access and Hotspot** checkbox.

When selected, for **Remote Access**, select or clear to use specific RADIUS groups only.

3. Click **Apply**.

Note - Configure remote access permissions for RADIUS users in the **VPN > Remote Access Users** page.

To add an Active Directory domain:

1. In the Active Directory section, click **New**.

The Add new Domain window opens.

2. Enter this information:

- **Domain** - The domain name.
- **IP address** - The IP address of one of the domain controllers of your domain.
- **User name** - The user must have administrator privileges to ease the configuration process and create a user based policy using the users defined in the Active Directory.
- **Password** - The user's password. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | ' " # + \
- **User DN** - Click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually. For example: CN=John James, OU=RnD, OU=Germany, O=Europe, DC=Acme, DC=com

3. Select **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory. Enter the branch in the Branch full DN in the text field.
4. Click **Apply**.

When an Active Directory is defined, you can select it from the table and choose **Edit** or **Delete** when necessary.

When you edit, note that the Domain information is read-only and cannot be changed.

When you add a new Active Directory domain, you cannot create another object using an existing domain.

To configure remote access permissions for all users defined in Active Directory:

By default, users defined in the Active Directory are not given remote access permissions. Instead, in the **VPN > Remote Access Users** page all users defined locally or in Active Directories can be selected to be granted remote access permissions per user.

1. Click **permissions for Active Directory users**.
2. Select **All users in the Active Directory**. With this option, it is not necessary to go to the **VPN > Remote Access Users** page and select specific users. Note that most Active Directories contain a large list of users and you might not want to grant them all remote access permissions to your organization. Usually you keep the **Selected Active Directory user groups** option and configure remote access permissions through **VPN > Remote Access Users** page.
3. Click **Apply**.

To change synchronization mode with the defined Active Directories:

1. Click **Configure** in the toolbar of the Active Directory table.
2. Select one of the options - **Automatic synchronization** or **Manual synchronization**.

When Manual synchronization is selected, you can sync the user database known to the appliance in all locations that this user database can be viewed. For example, the **Users & Objects > Users** page or the Source picker in the Firewall Rule Base in the **Access Policy > Firewall Policy** page.

Note - You cannot select a user from the Active Directory, only an Active Directory user group. You can select a local user.

3. Click **Apply**.

To edit an Active Directory:

1. Select the Active Directory from the list.
2. Click **Edit**.
3. Make the relevant changes and click **Apply**.

To delete an Active Directory:

1. Select the Active Directory from the list.
2. Click **Delete**.
3. Click **OK** in the confirmation message.

Note - This page is available from the **VPN** and **Users & Objects** tabs.

Managing Applications & URLs

In the **Users & Objects > Applications & URLs** page you can define application groups, custom applications, and view the full list of available applications. You can then use them in the access policy together with the applications and URLs that are in the Application Database. A custom application group lets you define multiple categories and/or sites to use in the access policy Rule Base.

To configure the access policy, click the **applications default policy** link or click the **Applications Blade Control page** link.

For more information about all built in applications and categories, click the **Check Point AppWiki** link at the top of the page.

Note - When URL Filtering is selected in the **Access Policy > Firewall Blade Control** page, rules containing URLs and custom applications are enforced.

What is a custom application?

Most applications are browser based. A custom application can be defined using a string or regular expression search on URLs.

What is a category?

Each URL is inspected by the Check Point Cloud using the URL Filtering and can be matched to one or more built in categories (for example, phishing sites, high bandwidth, gambling, or shopping, etc.).

The Application and Categories List

A list of applications and categories is shown according to a filter that is shown above the list. There are 4 filters:

- **Common** - Commonly used applications, custom applications, and categories.
- **Custom** - Only custom applications.
- **Categories** - Only categories.
- **All**

A tag icon is shown next to categories and dedicated application icons are shown next to applications.

In the Application Database, each application is assigned to one primary category based on its most defining aspect. It also has additional categories which are characteristics of the application. For example, Pinterest - its primary category is social networking and its additional categories are share photos and SSL protocol. If a category is in a rule, the rule matches all applications that are marked with the category.

If new applications are added to an additional category that is in the access policy Rule Base, the rule is updated automatically when the database is updated.

To search for a category or application:

1. Filter the list to show the required view.
2. Enter the text of the category of application in the Filter box.

As you type, the list is filtered.

To create a custom URL:

1. Select **New > URL**.
2. Enter the URL.
3. Click **Apply**.

You can use the URL in a rule.

To create a custom application:

1. Select **New > Application**.
2. Enter a name for the custom application.
3. Select a **Primary category** from the list.
4. Select **All URLs are regular expressions** if you want to use regular expressions instead of partial strings. Regular expressions use **PCRE syntax** (for example, to block www.malicioussite.com using a regular expression you can use `.*\malicioussite\com`)
5. Click **New** to add a partial string or regular expression that the appliance will detect in the URL and then click **OK**.
6. Do step 5 to add more related strings or regular expressions. The custom application will be matched if one of the strings or expressions is found.
7. Click the **Additional Categories** tab to select more categories if necessary.
8. Click **Apply**.

You can use the application in a rule.

To create a custom applications group:

1. Select **New > Applications Group**.
2. Enter a **Group name**.
3. Select the applications and categories to add as group members. To filter the selection list by common, categories, custom, or all, click the link.

The group members window shows a quick view of the selected items. You can quickly remove a selected item by clicking the x next to it.

4. If necessary, click **New** to add a custom application or URL to the list. For information on creating a custom application, see above.
5. Click **Apply**.

You can use the custom application group in a rule.

Managing System Services

The **Users & Objects > Services** page lists the system services configured in the system. In this page you can add new services, edit services, and delete services.

You use service objects to easily define the different network protocols. This is usually with IP protocol and ports (used by the TCP and UDP IP protocols).

These objects can be used to define your security policy, as well as policy based routing rules. Many service objects are predefined with the system and cannot be deleted. Those predefined "system services" represent the appliance's ability to perform deep inspection on those services for connectivity and security reasons. The system services sometimes have additional configuration options.

To create a new service:

1. Click **New**.
2. In the **Service** tab, enter information in the fields that apply to the type of service you select. Note that not all fields may show:
 - **Name** - Enter the service's name.
 - **Type** - Select the service type from the list:
 - **TCP**
 - **UDP**
 - **ICMP** - Select this option if it is necessary to represent a specific option within the ICMP protocol. Note that this is an advanced option.
 - **Other** - Select this option to represent any IP protocol other than TCP or UDP.
 - **Ports** - Enter the port(s) if you selected Type - TCP or UDP. Port numbers and/or ranges can be entered by separating with commas.
 - **IP Protocol** - Enter the IP protocol if you selected Type - Other.
 - **ICMP type** and **ICMP code** - Enter the ICMP type and code that you want the service object to represent as listed in RFC 792. This option is only relevant if you selected Type - ICMP.
 - **Comments** - Enter an optional comment.
 - **Disable inspection for this service** - Select this checkbox to disable deep inspection of traffic matching this service. This option is only available for built-in services.

3. In the **Advanced** tab, enter information in the fields that apply to the type of service you selected. Note that not all fields may show depending on the service type.

General

- **Session timeout (in seconds)** - Time in seconds before the session times out.
- **Use source port** - Select this option and enter a port number for the client side service. If specified, only those source port numbers are accepted, dropped, or rejected when inspecting packets of this service. Otherwise, the source port is not inspected.
- **Accept replies** (relevant for non-TCP services) - When cleared, server to client packets are treated as a different connection.
- **Match** (a highly advanced option to be used only by Check Point Support)

Connection handling

- **Keep connections open after policy has been installed** - Even if they are not allowed under the new policy. If you change this setting, the change does not affect open connections, but only future connections.
- **Synchronize connections on cluster** - Enables state-synchronized High Availability or Load Sharing on a cluster. Of the services allowed by the Rule Base, only those with Synchronize connections on cluster are synchronized as they pass through the cluster. By default, all new and existing services are synchronized.
- **Start synchronizing X seconds after the connection was initiated** - For TCP services, enable this option to delay telling the Check Point Appliance about a connection so that the connection is only synchronized if it still exists in X seconds after the connection is initiated. Some TCP services (HTTP for example) are characterized by connections with a very short duration. There is no point in synchronizing these connections because every synchronized connection consumes gateway resources, and the connection is likely to have finished by the time a failover occurs.

Aggressive aging

This feature can be configured from the **Device > Advanced** page. When the appliance is under load, older connections are removed from memory faster to make room for new connections.

- **Enable aggressive aging** - Select this option to manage connections table capacity and reduce gateway memory consumption to increase durability and stability.
- **Aggressive aging timeout (in seconds)** - Time in seconds before the session times out.

4. Click **Apply**.

To edit a service:

1. Select a service from the list.
2. Click **Edit**.
3. Make the necessary changes. Note that not all fields can be edited.
4. Click **Apply**.

To delete a service:

1. Select the service from the list. Note that you can only delete a user defined service.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified service:

1. In the **Type to filter** box, enter the service name or part of it.
2. As you enter text, the list is filtered and shows matching results.

Built-in System Services

Some built-in services represent Check Point's ability to perform deep inspection of the specific protocol. These system services cannot be deleted. When you edit them, the ports which you configure decide when the deep inspection occurs and you can add or change default ports. Some system services have additional configuration which affect the way the deep inspection is performed.

- **HTTP** - The IPS settings tab lets you configure how and when HTTP deep inspection is performed. Select the relevant options.
- **HTTPS** - The URL Filtering settings tab lets you categorize HTTPS sites by information in certificates.
- **FTP** - The Firewall settings tab lets you configure how the firewall automatically detects data connections. You can select one of these options:
 - Any - The Firewall detects and allows FTP data connections in all modes.
 - Active - The Firewall detects and allows FTP data connections in active mode only.
 - Passive - The Firewall detects and allows FTP data connections in passive mode only.
- **PPTP_TCP** - The IPS settings tab lets you configure how PPTP deep inspection is performed.
 - Action on malformed connections - Choose the action to perform on connections when parsing has failed.
 - Tracking - Choose the type of log to issue when parsing fails.
 - Enforce strict PPTP parsing - Select this to enforce strict adherence to the protocol.
- **SNMP** - The Firewall settings tab lets you configure the firewall to enforce a read-only mode in SNMP.
- **SSH** - The Firewall settings tab lets you configure the firewall to block older version of the SSH protocol (1.x).
- **Citrix** - The Firewall settings tab lets you configure which protocol to support on the configured ports. The default port 1494 is commonly used by two different protocols - Winframe or Citrix ICA.

Managing Service Groups

The **Users & Objects > Service Groups** page lists the service groups defined in the system. In this page you can add new service groups, and edit or delete existing service groups.

We recommend you define service groups to configure the security policy. If the security policy is configured with groups and not specified objects, it is much easier to maintain the policy over time. If you decide to add new service objects to the system, you only need to add them to the relevant groups and your policy automatically applies.

There are built in service groups for common services.

Some of these service groups also contain additional configuration for the inspection of the specific protocol.

To create a new service group:

1. Click **New**.

The New Service Group window opens.

2. Enter a **Name** for the group and **Comments** (optional).
3. Click **Select** to show the full list of available services and select the relevant checkboxes.
4. Click **New** if the existing list does not contain the services you need. For information on creating a new service object, see the **Users & Objects > Services** page.
5. Click **Apply**.

The New Service Group window opens and shows the services you selected.

6. You can also click **New** from the New Service Group window.
7. To remove a service object from the group list, select it and click **Remove**.
8. Click **Apply**.

The service group is added to the list of groups.

To edit a service group:

1. Select a group from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.

To delete a service group:

1. Select the group from the list. Note that you can only delete a user defined service group.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified service group:

1. In the **Type to filter** box, enter the service group name or part of it.
2. As you enter text, the list is filtered and shows matching results.

Built-in System Service Groups

Some built-in service groups represent Check Point's ability to perform deep inspection of a specific protocol. Such system service groups cannot be deleted. They contain a list of built in services which you can restore if you edit the content of such groups by clicking **Reset**.

Some system service groups have additional configuration which affect the way the deep inspection is performed.

DNS - The Firewall settings tab lets you configure NAT support over DNS. Note that this option affects the performance of DNS traffic and is normally not needed unless your organization uses both NAT and an internal DNS server accessible to the Internet. The IPS settings tab lets you configure how and when DNS deep inspection is performed. Select the relevant options.

Managing Network Objects

The **Users & Objects > Network Objects** page lists the network objects defined in the system. In this page you can add new network objects, edit network objects, and delete network objects. In most cases, the most common use for these objects is to define a security policy and exceptions to it. These objects can be used as hosts for the internal DNS service and their IP addresses can be configured as fixed for the internal DHCP service.

These are the available network object types:

- **Single IP** - A network object that represents a device with a single IP address.
- **IP Range** - A network object that represents a range of IP addresses.
- **Network** - A network object that represents a network.

To create a **Single IP** network object:

1. Click **New**.
The New Network Object window opens.
2. In **Type**, select **Single IP**.
3. Enter an **IP address** and **Object name**.
4. Select or clear these options as necessary:
 - **Allow DNS server to resolve this object name** - When the gateway is the DNS server for your internal networks, the name of the server/network object is translated to its IP address.
 - **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP address of this server/network object to anyone.
 - **Reserve IP address in DHCP service for MAC** - The internal DHCP service distributes the configured IP address only to this server/network object based on its MAC address.
 - Enter the **MAC address** - This is required for IP reservation. When you create the object from the **Active Devices** page, the MAC address is detected automatically.
5. Click **Apply**.

To create an **IP Range** network object:

1. Click **New**.
The New Network Object window opens.
2. In **Type**, select **IP Range**.
3. In the **Start IP** and **End IP** fields, enter the IP addresses that represent the start of the IP range and end of the IP range.
4. Enter the **Object name**.
5. Select or clear this option as necessary:
 - **Exclude from DHCP service** - The internal DHCP service does not distribute the configured IP range to anyone.
6. Click **Apply**.

Note - Wildcard network objects that represent a series of non-sequential IP addresses are supported.

To create a Network type network object:

1. Click **New**.
The New Network Object window opens.
2. In **Type**, select **Network**.
3. Enter a **Network address** and **Subnet mask**.
4. Enter the **Object name**.
5. Click **Apply**.

To edit a network object:

1. Select a network object from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.

To delete a network object:

1. Select the network object from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified network object:

1. In the **Type to filter** box, enter the name of the network object or part of it.
2. As you enter text, the list is filtered and shows matching results.

Managing Network Object Groups

The **Users & Objects > Network Object Groups** page lists the network object groups defined in the system. In this page you can add new network object groups, edit network object groups, and delete network object groups.

We recommend you define groups for network objects to configure the security policy. If you configure security policy with groups and not specified objects, it is much easier to maintain the policy over time. When new network objects are added to the system, you only need to add them to the relevant groups and your policy automatically applies.

To create a new network object group:

1. Click **New**.

The New Network Object Group window opens.

2. Enter a **Name** for the group and **Comments** (optional).
3. Click **Select** to show the full list of available network objects and choose the relevant checkboxes.
4. Click **New** if the existing list does not contain the network object you need. For information on creating a new network object, see the **Users & Objects > Network Objects** page.
5. Click **Apply**.

The New Network Object Group window opens and shows the services you selected

6. You can also click **New** from the New Network Object Group window.
7. To remove a network object from the group list, select it and click **Remove**.
8. Click **Apply**.

The network object group is added to the list of groups.

To edit a network object group:

1. Select a group from the list.
2. Click **Edit**.
3. Make the necessary changes.
4. Click **Apply**.

To delete a network object group:

1. Select the group from the list.
2. Click **Delete**.
3. Click **Yes** in the confirmation message.

To filter for a specified service group:

1. In the **Type to filter** box, enter the network object group name or part of it.
2. As you enter text, the list is filtered and shows matching results.

Logs and Monitoring

This section describes the security and system logs. It also describes various monitoring tools.

Viewing Security Logs

The **Logs & Monitoring > Logs > Security Logs** page shows the last 100 log records.

To load more records, continue scrolling down the page. The log table is automatically refreshed.

To search for a security log:

Enter your query in the **Enter search query** box. You can only search one field at a time (AND/OR operators are not supported).

Use this syntax:

`<IP_address>`

or

`<column_name>:<value>`

For example:

`203.0.113.64`

or

`action:drop`

or

`source port:22`

For more details, click **Query Syntax** in the table header.

To see the security log record:

1. Select a log entry from the list.
2. Click **View Details** or double-click the entry.

The log record opens.

To refresh the security log data:

Click the **refresh** icon .

To stop local logging:

When necessary, you can stop local logging for better performance. This removes the overhead of creating and maintaining logs. No new logs are generated until you set the resume option.

1. Select **Options > Stop local logging**.
2. To resume, select **Options > Resume local logging**.

Storing Logs

Logs can be stored locally on the appliance's non-persistent memory or on an external SD card (persistent). Logs can also be sent to an externally managed log server (see **Log Servers** page).

When you insert an SD card, it mounts automatically and then local logs are saved to it. Before you eject an SD card, make sure to unmount it. Select **Options > Eject SD card safely**.

Note - From R77.20.85 and higher, SD cards are formatted with ext4. Older versions are formatted as FAT32. If you upgrade from a lower version to R77.20.85 or higher, the SD card will remain with FAT32 for backward compatibility.

To delete logs from local log storage:

1. In **Logs & Monitoring > Logs > Security Logs** page, click **Clear logs**.

A confirmation window opens.

2. Click **Yes** to delete logs.

The logs are deleted, and the logs grid reloads automatically.

Note - Logs are deleted from the external SD card (if inserted) or from the local logs storage. Logs are not deleted from the remote logs server.

The logs are deleted, and the logs grid reloads automatically.

Viewing System Logs

The **Logs & Monitoring > System Logs** page shows up to 500 systems logs (syslogs) generated from the appliance at all levels except for the debug level. These logs should be used mainly for troubleshooting purposes and can also give the administrator notifications for events which occurred on the appliance.

These are the syslog types:

- **Info** - Informative logs such as policy change information, administrator login details, and DHCP requests.

Audit logs show each operation of the admin from the WebUI/clish/mobile/SMP.

CPOSD logs show new configurations.

- **Notice** - Notification logs such as changes made by administrators, date, and time changes.
- **Warning** - Logs that show a connectivity or possible configuration failure. The problem is not critical but requires your attention.
- **Error** - System errors that alert you to the fact that a specific feature is not working. This can be due to misconfiguration or connectivity loss which requires the attention of your Internet Service Provider.

To download the full log file:

1. Click **Download Full Log File**.
2. Click **Open** or **Save**.

To save a snapshot of the syslogs to the flash disk:

1. Select **Save a snapshot of system logs to flash**.
2. Enter a minute value for the interval. The default is 180 minutes (3 hours). The minimum value is 30 minutes.
3. Click **Apply**.

This is an effort to keep syslogs persistent across boot, but not 100% guaranteed.

To refresh the system logs list:

Click **Refresh**. The list is refreshed.

To clear the log list:

1. Click **Clear Logs**.
2. Click **OK** in the confirmation message.

Configuring External Log Servers

The **Logs & Monitoring > Log Servers** page lets you configure external log servers for security and system logs for additional logging storage.

Note - You cannot configure external log servers when Cloud Services is turned on.

External Check PointLog Server

You can use an external Check PointLog Server that is managed by a Security Management Server for storing additional logs.

Use cases for an external Check PointLog Server:

- Extend the log retention time. For example, currently, when your gateway is managed by SMP, you can retain logs for 3 months. If you configure an external Log Server, you can retain the logs for a year.
- Export the logs format to a 3rd party mechanism for data mining.

Do these steps before you configure an external Check PointLog Server from this page in the WebUI:

1. Identify the Log Server you want to send logs to.
2. Identify the Security Management Server that manages the Log Server.
3. Open SmartConsole on this Security Management Server.
4. Run the Security Gateway wizard to define and create a Security Gateway object that represents this Check Point Appliance with the these details:

In the **General Properties** window, select:

- **Gateway platform** - Select your appliance
- **Gateway IP address** - Dynamic IP address

In the **Trusted Communication** window, from **Gateway Identifier** select **MAC address** or **First to connect**.

5. Install the database on the Security Management Server and other related objects.

To configure an external Check Point log server:

1. Under **Check PointLog Server**, click **Configure**.

The External Check PointLog Server window opens.

2. Enter the **Management Server IP address**. This IP address is used only to establish trusted communication between the Check Point Appliance and the Security Management Server.

3. In **SIC name**, enter the SIC name of the ILog Server object defined in SmartConsole. To get this name:
 - Connect with GuiDBedit Tool (see [sk13009](#)) to the Security Management Server - From the **Tables** tab, expand **Table > Network Objects**. In the right pane, locate the Log Server object. In the bottom pane, locate **sic_name**.
 - or
 - Run this CLI command on the Log Server (use SSH or console connection):


```
$CPDIR/bin/cpprod_util CPPROD_GetValue SIC MySICname 0
```

Copy the SIC name value and paste it into the SIC name field on this page.
4. In **Set SIC One-time Password**, enter the same password that was entered for the Security Management Server and then enter it again in the **Confirm SIC One-time Password** field. You cannot use these characters when you enter a password or shared secret: { } [] ` ~ | \ " # + \
5. If the Log Server is not located on the Security Management Server, select **Log server uses different IP address** and enter the IP address.
6. Click **Apply**.

Important - After successful configuration of the external log server, any changes you make in the WebUI configuration on this page requires reinitialization of the SIC in SmartConsole. If you do not reinitialize SIC in SmartConsole, connectivity to the log server can fail.

To configure a new external Check PointLog Server when the gateway is connected to SMP (Cloud):

1. In the WebUI, connect to **Cloud Services**.
2. Go to **Logs and Monitoring > External Log Server**.
3. Click **New** to add a new Log Server.
4. In the **Add External Log Server** window, enter the **IP address** and the **SIC name** of the Log Server.
5. Click **Apply**.
6. To fetch the policy from the cloud, go to **Home > Cloud Services** and click **Fetch now**.

After you initiate traffic from resources behind the gateway, open the Check PointLog Server to verify that you see the logs. For more information, see [sk145614](#).

External Syslog Server Configuration

You can configure a gateway to send logs to multiple external syslog servers.

To configure an external syslog server:

1. Under **Syslog Servers**, click **Configure**.
The External Syslog Server window opens.
2. Enter a **Name** and **IP address**.
3. Enter a **Port**.
4. Select **Enable log server**.

5. **Optional** - Select **Show Obfuscated Fields**. Obfuscated packets are shown as plain text.
6. Select logs to forward:
 - System logs
 - Security logs
 - Both system and security logs
7. Click **Apply**.

To configure additional syslog servers:

Click **Add Syslog Server**.

You can send security logs to syslog servers. The security logs show in the syslog format, not in the security logs format.

To edit the external syslog server:

1. Click the **Edit link** next to the server's IP address.
2. Edit the necessary information.
3. Click **Apply**.

Note - When more than one server is defined, the syslog servers show in a table. Select the syslog server you want to edit and click **Edit**.

To delete the external syslog server:

1. Select the syslog server.
2. Click **Delete**.

The server is deleted.

Notifications

See ["Notifications" on page 41](#).

Managing Active Devices

See ["Managing Active Devices" on page 42](#).

Wireless Active Devices

The **Logs & Monitoring > Wireless Active Devices** page shows the devices connected to your gateway's wireless network.

Relevant information for each connected device's network usage includes:

- SSID - Name of the WiFi network
- Channel
- Frequency
- Signal Strength

- RSSI - Received Signal Strength
- Bandwidth

Paired Mobile Devices

The **Logs & Monitoring > Paired Mobile Devices** shows the mobile devices paired to the gateway.

To revoke a pairing:

1. Select the device name.
2. Click **Revoke**.
3. In the confirmation window that opens, click **Yes**.

Viewing Infected Devices

See ["Viewing Infected Devices" on page 169](#).

Viewing VPN Tunnels

In the **VPN Tunnels** page you can see current VPN tunnels opened between this gateway and remote sites. Some sites are configured so tunnels are established only when necessary and some are configured with permanent tunnels. When the appliance is managed by Cloud Services, this table also shows the tunnels for the gateways in the community.

This page is commonly used to see the permanent tunnels. The table shows each tunnel's details when there is an active VPN tunnel.

Field	Description
From	Host name or IP address of the tunnel's source gateway.
Site Name	Name of the VPN site name.
Peer Address	Host name or IP address of the tunnel's destination gateway.
Community Name	If the gateways are part of a community configured by Cloud Services, this column shows the community name with which the tunnel is associated.
Status	VPN tunnel status indication.

To filter the list:

In the **Type to filter** box, enter the filter criteria.

The list is filtered.

To refresh the list:

Click **Refresh** to manually refresh this page with updated tunnel information.

Note - This page is available from the **VPN** and **Logs & Monitoring** tabs.

Viewing Active Connections

The **Logs & Monitoring > Connections** page shows a list of all active connections.

The list shows these fields:

- Protocol
- Source Address
- Source Port
- Destination Address
- Destination Port

To filter the list:

In the **Type to filter** box, enter the filter criteria.

The list is filtered.

To refresh the list:

Click the **Refresh** link.

Access Points

The **Logs & Monitoring > Access Points** page shows the available access points around your gateway. The network information includes:

- Channel
- Frequency
- Security
- Signal strength
- Signal noise

Use case:

Use this information to help you decide which network to connect to, and switch according to your needs.

This page also displays the current wireless radio frequency and channel in use and the wireless networks configured.

Viewing Monitoring Data

See ["Viewing Monitoring Data" on page 44](#).

Viewing Reports

See ["Viewing Reports" on page 46](#).

Using System Tools

See ["Using System Tools" on page 48](#).

SNMP

In the **Logs & Monitoring > SNMP** page you can configure SNMP settings for this gateway.

You can do these actions:

- Turn the SNMP agent on or off
- Configure SNMP settings (system location, system contact, and community string for SNMP v1 and v2 authentication)
- Add SNMP v3 users
- Configure the settings for SNMP Trap receivers
- Enable or disable SNMP traps that are sent to the trap receivers

To turn **SNMP** on or off:

1. Change the SNMP On/Off slider position to **ON** or **OFF**.
2. Click **Apply**.

SNMP must be set to on to configure all SNMP settings (users, traps, and trap receivers).

To configure **SNMP** settings:

Click **Configure**.

The Configure SNMP General Settings window opens. You can enable SNMP traps, configure system location and contact details, and enable SNMP versions in addition to v3.

SNMP v3 Users

- To add a new SNMP v3 user, click **New**.
- To edit an existing SNMP v3 user, select the user from the list and click **Edit**.
- To delete an SNMP v3 user, select the user from the list and click **Delete**.

SNMP Traps Receivers

You can add, delete, or edit the properties of SNMP trap receivers.

- To add an SNMP trap receiver, click **New**.
Note - To add a new SNMP v3 trap receiver, there must be an SNMP v3 user defined for it.
- To edit an existing SNMP trap receiver, select the trap receiver from the list and click **Edit**.
- To delete an SNMP trap receiver, select the trap receiver from the list and click **Delete**.

SNMP Traps

You can enable or disable specified traps from the list and for some traps set a threshold value. The enabled traps are sent to the receivers.

To edit an SNMP trap:

1. Select the trap from the list and click **Edit**.
2. Select the **Enable trap** option to enable the trap or clear it to disable the trap.
3. If the trap contains a **value**, you can edit the threshold value when necessary.
4. Click **Apply**.

Advanced Configuration

This section contains information about advanced configuration, including upgrades and restoring factory defaults.

Note - Not all topics are relevant for all appliance models.

Upgrade Using a USB Drive

This section explains how you can upgrade the appliance with a USB drive without a console connection to the appliance. It is possible to manually choose from a console the specific file you wish to use for the upgrade. For more information, see ["Upgrade Using Boot Loader" on page 251](#).

Note - The USB drive must be formatted in FAT32.

Installing a new firmware image from a USB drive

Check Point releases new firmware images every so often. You can reburn the appliance using the image file and a USB drive. Note that you can also upgrade through the WebUI. If the new image supports it, you do not lose your previous settings. When you reburn a new image with a USB drive, the appliance deletes your previous settings and creates a new factory default image.

As this operation removes your previous settings, refer to the *Getting Started Guide* and reconfigure your appliance with the First Time Configuration Wizard.

Note - When you upgrade with a USB drive, you also replace the saved factory default image of the appliance as this method reburn the appliance.

Installing a new Boot-Loader from a USB drive

Check Point releases new Boot Loader rarely. This usually comes with a new image. To upgrade to a new U-Boot or Firmware image, you must boot the appliance.

Replace the Boot Loader before you upgrade to a new image.

To replace Boot-Loader:

1. Disconnect your Check Point appliance from the power source.
2. Place the Boot loader file on a USB drive in the top folder. Do not rename the file.
3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (`u-boot*.ubt` files or `fw1*.img` files).
4. Connect the USB drive to one of the appliance USB ports. If the operation does not succeed, this may be because the USB port does not recognize all USB drives. Some USB drives also use a different file system and those are not supported.
5. Connect the appliance to the power source. When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

When the LED turns a solid blue, the appliance is ready for login.

Note - The LED is red if there is an alert or error.

6. Remove the USB drive and disconnect the appliance from the power source.
7. If you need to install a new firmware image, refer to the firmware image installation section before you reconnect the appliance to the power source.

To upgrade to a new firmware image from a USB drive:

1. Disconnect the Check Point appliance from the power source.
2. Place the firmware image file on a USB drive in the top folder. Do not rename the file.
3. Make sure the top folder of the USB drive does not contain any previous Boot loader or Firmware images (`u-boot*.bin` files, or `fw1*.img` files).
4. Connect the USB drive to the USB port on the Check Point appliance.
5. **Connect the appliance to the power source.**

When the appliance is turned on, the Power LED on the front panel lights up in red for a short period.

The LED then turns blue and starts to blink. This shows a boot is in progress and firmware is being installed.

When the LED turns a solid blue, the appliance is ready for login.

Note - The LED is red if there is an alert or error.

6. Remove the USB drive.
7. As this operation removes your previous settings, refer to the *Getting Started Guide* and reconfigure your appliance with the First Time Configuration Wizard.

Note - When you upgrade with a USB drive, you also replace the saved factory defaults image of the appliance as this method reburns the appliance.

Note - Uboot update from a USB drive is currently not supported in 1500 appliances.

Upgrade Using an SD Card

In the 1590 appliances, you can use an SD card to upgrade to a new firmware image or auto-configuration file. When you install a new image with an SD card, the appliance deletes your previous settings and creates a new factory default image. Back up your settings so you can restore them after the installation is complete.

Note - The 1550 appliance does not support SD cards.

Note - SD cards are formatted with `ext4`. In earlier versions, SD cards are formatted as FAT32. If you upgrade from an earlier version to R77.20.85 or higher, the SD remains with FAT32 for backward compatibility.

To upgrade to a new firmware image from an SD card:

1. Disconnect the Check Point Appliance from the power source.
2. Place the firmware image on the SD card in the top folder. Do not rename the file.

Make sure the top folder of the SD card does not contain any previous Boot loader or firmware images (`u-boot*.bin` files or `fwl*.gz` files).
3. Insert the SD card into the SD card slot on the Check Point Appliance. If the operation does not succeed, this may be because the SD card slot does not recognize all devices.
4. Connect the appliance to the power source.

The installation begins with the image file. This takes several minutes.

If the file is valid, all LAN LEDs start to blink to show progress. The LEDs are different colors and blink at different speeds.

When the installation is complete, all LAN LEDs turn a constant green. The appliance is ready for your input.

Restore your settings. For more information, see ["Backup, Restore, Upgrade, and Other System Operations" on page 79](#).

To upgrade using Gaia Clish commands:

These are the file names that you can use:

- `autoconf.clish`
- `autoconf.<MAC address>.clish`

`<MAC address>` is the specified MAC address in this format: `XX-XX-XX-XX-XX`

You can create multiple configuration files for Check Point Appliance gateways. The gateways run both files or only one of them. First the `autoconf.clish` configuration file is loaded. If there is a configuration file with the same MAC address as the gateway, that file is loaded second.

Use the `#` symbol to add comments to the configuration file.

Boot Loader

The Gaia Embedded Boot Menu shows during boot and is available if you press **CTRL+C** while the appliance boots if you have a console connection. The menu contains the available options.

```
1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Restart Boot-Loader
7. Run Hardware diagnostics
8. Install DSL Firmware / Upload preset configuration file
Please enter your selection:
```

When you are in Boot Loader, all interfaces are down and you can only activate them for options that require connectivity. At this point Check Point's services are not active.

Options 1-3 start the appliance.

- Normal mode is the default boot mode for the appliance.
- Debug mode boot gives printouts of processes that are initialized during boot.
- Maintenance mode boots the machine and gives access only to the file system (network interfaces, Check Point processes and the appliance's services are down).

Note - During normal/debug boot, if there is an error and the appliance cannot boot properly, it reverts to maintenance mode and the Power LED turns a constant red.

Options 4-5 are explained in the subsequent sections.

Option 6 restarts the appliance.

Option 8 installs new firmware for the DSL modem (supported in DSL models only) or uploads a preset configuration file.

Upgrade Using Boot Loader

To upgrade the Check Point Appliance using U-boot (boot loader):

Note - In 1590, Bootloader is supported only through the DMZ port and is not available through the LAN ports.

1. Connect to the appliance with a console connection (use the serial console connection on the back panel of the appliance), boot the appliance and press **CTRL+C**. The Gaia Embedded Boot Menu is shown.
2. Press **5** to select **Install/Update Image/Boot-Loader from Network**.
3. You are asked if you want to manually load the image from a TFTP server, or if you want to use automatic mode with a bootp server.
4. If you select manual mode, you are asked to fill in the IP of the Check Point Appliance, the IP of the TFTP server, and the image name.
5. If you select automatic mode, the procedure starts automatically to search for the bootp server.
6. While in menu mode, press **CTRL+C** again to return to the Boot Loader menu.

During the upgrade, all LAN Link and Activity LEDs blink red and blue alternately to indicate progress. This takes up to a minute.

When all LAN Link and Activity is successfully completed, the LEDs light in blue, and the appliance waits for you to press a key. Error in the upgrade process is indicated by all LAN Link and Activity LEDs blinking red.

Restoring Factory Defaults

The Check Point Appliance contains a default factory image.

When the appliance is turned on for the first time, it loads with the default image.

As part of a troubleshooting process, you can restore the Check Point Appliance to its factory default settings if necessary.

You can restore a Check Point Appliance to the factory default image with the WebUI, Boot Loader, or a button on the back panel.



Important - When you restore factory defaults, you delete all information on the appliance and it is necessary to run the First Time Configuration Wizard.

To restore factory defaults with the WebUI:

1. In the Check Point Appliance WebUI, click **Device > System Operations**. The System Operations pane opens.
2. In the Appliance section, click **Factory Defaults**.
3. In the pop-up window that opens, click **OK**.
4. While factory defaults are restored, the Power LED blinks blue to show progress.

This takes some minutes. When this completes, the appliance reboots automatically.

To restore factory defaults with the button on the back panel:

1. Press the Factory Default button with a pin. Hold for at least 12 seconds.
2. When the Power LED is lit blue, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are restored, the Power LED blinks blue to show progress.

This takes some few minutes. When this completes, the appliance reboots automatically.

To restore the Check Point Appliance to its default factory configuration using U-boot (boot loader):

1. Connect to the appliance with a console connection (use the serial console connection on the back panel of the appliance).

2. Boot the appliance and press **CTRL+C**.

The Gaia Embedded Boot Menu is shown.

```
Welcome to Gaia Embedded Boot Menu:
1. Start in normal Mode
2. Start in debug Mode
3. Start in maintenance Mode
4. Restore to Factory Defaults (local)
5. Install/Update Image/Boot-Loader from Network
6. Restart Boot-Loader
7. Run Hardware diagnostics
8. Install DSL Firmware/Upload preset configuration file
Please enter your selection:
```

3. Enter **4** to select **Restore to Factory Defaults (local)**.
4. When you are prompted: "Are you sure? (y/n)" select **y** to continue and restore the appliance to its factory defaults settings.

While factory defaults are restored, the Power LED blinks blue to indicate progress. This takes up to a few minutes. When completed, the appliance boots automatically.

To disable the reset to default:

Use this CLI command:

```
>set additional-hw-settings reset-timeout 0
```

To enable the reset to default:

Use this CLI command:

```
>set additional-hw-settings reset-timeout 12
```