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.

**Check Point R77.20.10**
For more about this release, see the R77.20.10 home page [http://supportcontent.checkpoint.com/solutions?id=sk106957].

**Latest Version of this Document**
Download the latest version of this document [http://supportcontent.checkpoint.com/documentation_download?ID=43527].
To learn more, visit the Check Point Support Center [http://supportcenter.checkpoint.com].

**Feedback**
Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments [mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point 600 Appliance R77.20.10 Administration Guide].

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09 September 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Contents

Important Information ................................................................................................... 3
Introduction ................................................................................................................... 7
   Welcome ................................................................................................................... 7
   Check Point 600 Appliance Overview ................................................................. 7
Installation .................................................................................................................... 8
   Setting Up the Check Point 600 Appliance ............................................................ 8
   Connecting the Cables ............................................................................................ 8
Deploying from a USB Drive ......................................................................................... 9
   Sample Configuration File ..................................................................................... 9
   Preparing the Configuration Files ........................................................................... 10
   Deploying the Configuration File - Initial Configuration .................................... 10
   Deploying the Configuration File - Existing Configuration .................................. 11
Viewing Configuration Logs ....................................................................................... 12
Troubleshooting Configuration Files ......................................................................... 12
   Configuration File Error ....................................................................................... 12
   Suggested Workflow - Configuration File Error ...................................................... 12
   Sample Configuration Log with Error .................................................................... 13
Using the set property Command ............................................................................ 14
Common Configuration Scenarios .............................................................................. 15
   Configuring Cloud Services .................................................................................. 15
   Configuring a Guest Network .............................................................................. 16
   Configuring VPN .................................................................................................. 16
      Configuring Remote Access VPN .................................................................. 17
      Configuring Site to Site VPN with a Preshared Secret .................................. 18
      Configuring Site to Site VPN with a Certificate ............................................. 19
   Configuring QoS ................................................................................................... 20
   Configuring a Cluster ............................................................................................ 21
   Enabling VoIP Traffic ............................................................................................ 23
Appliance Configuration ............................................................................................... 24
   Introduction to the WebUI Application .................................................................. 25
The Home Tab ............................................................................................................. 26
   Viewing System Information ................................................................................ 26
   Controlling and Monitoring Software Blades ....................................................... 26
   Configuring Cloud Services .................................................................................. 28
   Viewing the Site Map ............................................................................................ 30
Managing Licenses ..................................................................................................... 31
Managing Active Computers in Internal Networks ................................................. 31
   Viewing Monitoring Data ..................................................................................... 32
   Viewing Reports .................................................................................................... 34
   Using System Tools .............................................................................................. 35
Managing the Device ................................................................................................. 37
   Configuring Internet Connectivity ...................................................................... 37
   Configuring Wireless Network Settings ............................................................... 40
   Configuring the Local Network ............................................................................ 43
   Configuring a Hotspot ......................................................................................... 49
   Configuring the Routing Table ............................................................................. 50
Introduction

In This Section:

Welcome..................................................................................................................................7
Check Point 600 Appliance Overview.......................................................................................7

Review these documents before doing the procedures in this guide:

- Version’s release notes
- Known limitations
- Resolved Issues
- Check Point 600 Appliance Getting Started Guide

See the R77.20.10 home page [http://supportcontent.checkpoint.com/solutions?id=sk106957].

Welcome

Thank you for choosing Check Point’s Internet Security Product Suite. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional and support services through a network of Authorized Training Centers, Certified Support Partners and Check Point technical support personnel to ensure that you get the most out of your security investment.

For additional information on the Check Point Internet Security Product Suite and other security solutions, refer to: http://www.checkpoint.com [http://www.checkpoint.com]. For technical assistance, contact Check Point 24 hours a day, seven days a week at: +1 972-444-6600 (Americas) +972 3-611-5100 (International). For additional technical information, refer to: http://support.checkpoint.com [http://supportcenter.checkpoint.com].

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application and management security needs.

Check Point 600 Appliance Overview

Check Point 600 Appliance delivers 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], Check Point 600 Appliance provides simplified deployment while delivering uncompromising levels of security.

Check Point 600 Appliance supports the Check Point Software Blade architecture that gives independent and modular security building blocks. Software Blades can be quickly enabled and configured into your solution based on specific security needs.
Installation

In This Section:

Setting Up the Check Point 600 Appliance ................................................................. 8
Connecting the Cables ............................................................................................... 8

Setting Up the Check Point 600 Appliance

1. Remove the Check Point 600 Appliance from the shipping carton and place it on a tabletop.
2. Identity 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 on the Check Point 600 Appliance:

1. Connect the power supply unit to the appliance and to a power outlet. The appliance is turned on once the power supply unit is connected to an outlet. The Power LED on the front panel (on page 174) turns on. This indicates that the appliance is turned on. The Notice LED on the front panel starts blinking. This indicates that the appliance is booting up. When the Notice LED turns off, the appliance is ready for login.
2. Connect the standard network cable to the network interface port (LAN1) on the appliance and to the network adapter on your PC.
3. Connect another standard network cable to the WAN interface on the appliance and to the external modem, external router, or network point.
You can deploy Check Point 600 Appliance configuration files using a USB drive and quickly configure many appliances without using the First Time Wizard. The configuration file lets you configure more settings and parameters than are available in the First Time Wizard.

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

Check Point 600 Appliance starts, automatically mounts the USB drive, and checks the root directory for a configuration file.

**Note** - The USB drive must be formatted in FAT32.

### Sample Configuration File

This is a sample Check Point 600 Appliance configuration file for USB deployment.
Preparing the Configuration Files

The Check Point 600 Appliance Massive Deployment configuration files are composed of C莉sh commands. These are the file names that can be used:

- `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 600 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 600 Appliance. The file must be correctly configured and formatted before being deployed. The USB drive can be inserted in the front or the rear USB port. Make sure it is formatted in FAT32.

You can deploy the configuration file to Check Point 600 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 Check Point 600 Appliance configuration script is running. Otherwise, it is possible that Check Point 600 Appliance does not configure and run correctly.
To deploy the configuration file from a USB drive for the initial configuration:

1. Insert the USB drive into Check Point 600 Appliance.
   - Check Point 600 Appliance is OFF - Turn on the appliance. The Power LED comes on and is green.
   - Check Point 600 Appliance is ON - The appliance automatically detects the USB drive. The USB LED comes on and is solid orange.

2. Check Point 600 Appliance locates the USB configuration file and begins running the script. The USB LED blinks green while the script is running.

3. The configuration script finishes and the Check Point 600 Appliance USB LED is solid green.

4. Remove the USB drive from Check Point 600 Appliance.

   **Note** - The USB LED is red when there is a problem running the configuration script. Turn off Check Point 600 Appliance and confirm that the configuration files are formatted correctly (“Preparing the Configuration Files” on page 10).

   For more information about errors with configuration files, see Troubleshooting Configuration Files (on page 12).

---

**Deploying the Configuration File - Existing Configuration**

This section describes how to deploy a configuration file on a USB drive to Check Point 600 Appliance to edit or update the existing configuration. 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 Check Point 600 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 600 Appliance configuration script is running. Otherwise, it is possible that Check Point 600 Appliance does not configure and run correctly.

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 USB LED comes on and is solid orange.

3. The appliance locates the USB configuration file and begins running the script. The USB LED blinks green while the script is running.

4. The configuration script finishes.
   The USB LED is solid green and the screen displays: `System Started`.

5. Remove the USB drive from the appliance.
Note - The USB LED is red when there is a problem running the configuration script. Turn off the appliance and confirm that the configuration files are formatted correctly ("Preparing the Configuration Files" on page 10).

For more information about errors with configuration files, see Troubleshooting Configuration Files (on page 12).

Viewing Configuration Logs

After Check Point 600 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 600 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 appear before the error are applied to the appliance. You can examine the configuration log to find where the error occurred.

When there is a not fully configured appliance, the First Time Wizard is displayed in the Web UI. However, not all of the settings from the failed configuration file are displayed in the First Time Wizard. Check Point recommends that you should not use the First Time Wizard to configure an appliance when the configuration file fails.

Note - You should restore the default settings to a partially configured appliance before using the First Time 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` ("Using the set property Command" on page 14) command when you are running a configuration file script on a configured appliance.

1. The USB drive with the configuration file is inserted into a USB port on Check Point 600 Appliance.
2. The USB 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 through
   sd 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.

5. If you cannot repair the configuration file:
   a) Remove the USB drive.
   b) Run the CLI command: `restore default-settings`.
   c) Connect to the Web UI and use the First Time Wizard to configure the appliance.

6. If you understand the error and know how to repair the configuration file:
   a) Remove the USB drive.
   b) Run the CLI command: `restore default-settings`.
   c) 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.

```plaintext
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 Check Point 600 Appliance runs configuration scripts from a USB drive. These commands do not change how the First Time Wizard in the Web UI configures the appliance.

- **set propert USB_auto_configuration off** - The appliance does not run configuration scripts from a USB drive.
- **set propert USB_auto_configuration once** - The appliance only runs the next configuration script from a USB drive.
- **set propert USB_auto_configuration any** - The appliance always runs configuration scripts from a USB drive.
Common Configuration Scenarios

**In This Section:**

- Configuring Cloud Services ................................................................. 15
- Configuring a Guest Network ............................................................... 16
- Configuring VPN ................................................................................ 16
- Configuring QoS .................................................................................. 20
- Configuring a Cluster ........................................................................... 21
- Enabling VoIP Traffic ........................................................................... 23

This chapter contains workflows for common configuration scenarios.
The workflow steps include links to the related appliance configuration sections when necessary.

### Configuring Cloud Services

**Introduction**

Cloud Services lets you connect your Check Point 600 Appliance to a Cloud Services Provider that uses a Web-based application to manage, configure, and monitor the appliance.

**Prerequisites**

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

- Received an email from your Cloud Services Provider that contains an activation link. Clicking the link automatically connects your Check Point 600 Appliance to Cloud Services.
  
  * Or

- The Service Center IP address, the Check Point 600 Appliance gateway ID, and the registration key. Use these details to manually connect your Check Point 600 Appliance to Cloud Services.

**To automatically connect to Cloud Services:**

1. Make sure the Check Point 600 Appliance has been configured with the First Time Configuration Wizard. See the Check Point 600 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 28].

**To manually connect to Cloud Services:**

1. In the WebUI, go to the **Home > Cloud Services** page.

2. Do the connect to Cloud Services procedure in Configuring Cloud Services [on page 28].
Configuring a Guest Network

In some situations, it is necessary to allow guest access to the Internet from within your organization. At the same time, it might be necessary to restrict access to internal network resources. Configuring a guest network with a Hotspot lets you 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 will redirect users to the Hotspot portal when they browse from those interfaces.

Configuration

1. Go to the Device > Wireless Network page.
2. Click the Guest link and follow the wizard instructions. See Configuring Wireless Network Settings (on page 40).
   a) Make sure that the Use Hotspot checkbox is selected in the wizard.
   b) Set the network protection (unprotected or protected network).
   c) Set the access and log policy options in the Access Policy tab.
3. Make sure you have defined the network interfaces for Hotspot. See Configuring the Local Network (on page 43).
4. Configure the Hotspot - Go to the Device > Hotspot page and set the options. See Configuring a Hotspot (on page 49).
5. 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 will see the customized Hotspot portal. Note that you will be shown the Hotspot portal one time in the given timeout period. The default timeout period is 4 hours.

User activity on this network will be 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
You can use these options for remote access:

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

Prerequisites

- On the VPN > Blade Control page, 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 125).
- If the gateway uses a dynamic IP address, it is recommended to use the DDNS feature. See Configuring DDNS Account Details ("Configuring DDNS and Access Services" on page 62).
- For the Check Point VPN client or Mobile client method, make sure that the applicable client is installed on the hosts. Click the How to connect link for more details.

Remote Access Configuration

There are 3 methods you can use to configure remote access users:

- Local users
- RADIUS users
- AD users

To allow only specified users to connect with a remote access client, set up group permissions for the applicable user type. Select the arrow next to the Add option and choose the relevant group option. See Configuring Remote Access Users (on page 127)

To configure local users:

1. For new users:
   a) Go to the VPN > Remote Access Users page.
   b) Use the Add option to add local users.
   c) Make sure that the Remote Access permissions checkbox is selected.
   d) For more details, see Configuring Remote Access Users (on page 127).
2. For existing users:
   a) Go to the VPN > Remote Access Users page.
   b) Use the Edit option to make sure that the Remote Access permissions checkbox is selected.
   c) For more details, see Configuring Remote Access Users (on page 127).
To configure RADIUS users:

1. Go to **VPN > Authentication Servers** and click **Configure** to add a RADIUS server. See Configuring Remote Access Authentication Servers (on page 129).
2. Set the access permissions for RADIUS users by clicking the **permissions for RADIUS users** link.

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 129).
2. Set the access permissions for Active Directory users by clicking the **permissions for Active Directory users** link.

**L2TP VPN Client configuration**

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

**Advanced Options**

For details regarding advanced Remote Access options, for example Office Mode network, see Configuring Advanced Remote Access Options (on page 132).

**Monitoring**

To make sure that Remote Access is working:

Connect from a remote host to an internal resource using the configured client.

### 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]** option is selected. See Configuring the Site to Site VPN Blade (on page 134).
- The peer device that you are connecting 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 details, see Configuring VPN Sites (on page 135).

**Monitoring**

To make sure the VPN is working:

1. Send traffic between the local and peer gateway.
2. Go to the **VPN > VPN Tunnels** page to monitor the tunnel status. See Viewing VPN Tunnels (on page 138).
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] option is selected. See Configuring the Site to Site VPN Blade (on page 134).
- The peer device that you are connecting 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 that 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 using the Custom encryption option.

Configuration
1. Reinitialize certificates - Use the Reinitialize certificates option described in Managing Internal Certificates (on page 143). Make sure this is done on both the local and peer gateway (if they are both using 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
   Do the corresponding steps for the applicable procedure listed in the Trust Procedures section below.
3. Create the VPN site using the certificate authentication.
   a) Follow the instructions in Configuring VPN Sites (on page 135).
   b) To make sure the specified certificate is used, in the Advanced tab > Certificate Matching section, fill in the peer gateway’s certificate details.

Trust Procedures

Exchange CAs between gateways
Make sure the CA is uploaded on both the local and peer gateways by adding the Trusted CA of the peer gateway. Use the Add option, see Managing Trusted CAs (on page 141).

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 142).
2. Export this request using the Export option.
3. Sign the request on the peer gateway using the peer gateway’s internal CA.
   If the peer gateway is a locally managed Check Point gateway, go to the VPN > Trusted CAs page and use the Sign a Request option. For more details, see Managing Trusted CAs (on page 141).
4. Upload the signed request to the local gateway.
   a) Go to the **VPN > Installed Certificates** page.
   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 142).

5. Make sure that the CA is installed on both of the gateways. Use the **Add** option in Managing Trusted CAs (on page 141).

**Authenticate by using a 3rd party CA**

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

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 the **VPN > Installed Certificates** page.
   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 142).

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 141).

**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 141).

**Monitoring**

To make sure the VPN is working:

1. Pass traffic between the local and peer gateway.
2. Go to the **VPN > VPN Tunnels** page to monitor the tunnel status. See Viewing VPN Tunnels (on page 138).

**Configuring QoS**

**Introduction**

The QoS (bandwidth control) policy is a set of rules that lets you set bandwidth parameters. These parameters control the flow of traffic to and from your network. These rules make sure that:

- Important traffic is prioritized.
- 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. You get the speed information from your ISP.
QoS policy rules apply separately on each configured Internet connection.

**Prerequisites**

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

**Configuration**

1. Go to the **Device > Internet** page, 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 calculating QoS weight. For more details, see Configuring Internet Connectivity (on page 37).
3. You can use these options:
   - A default QoS policy that requires defining only a number of parameters. See Configuring the Quality of Service (QoS) - Bandwidth Control Blade (on page 106)
   - Define manual rules for further granularity if necessary on the **Access Policy > QoS > Policy** page. See Working with the QoS Policy (on page 107).

### Configuring a Cluster

**Introduction**

You can configure two appliances in a cluster configuration for High Availability. **High Availability** makes sure to keep connections in the organization’s network working when there is a failure in a cluster member. Only one gateway is active during a given time. When there is a failover, the standby member becomes active.

Only Cluster High Availability is supported. There is no load sharing between the members of the cluster.

**Prerequisites**

- Bridge and switch configurations are not supported in cluster configuration. You must delete these before you start to configure a cluster (in the **WebUI > Device > Local Network** page).
- Both appliances that are designated for use as cluster members must have the same hardware, firmware, and licenses.
- It is recommended to designate the same LAN port for the Sync interface. The default Sync interface is LAN2/SYNC.
  
  **Note** - Connect the Sync cable only after completing the First Time Configuration Wizard and removing the switch on both appliances. No additional configuration is required on both members.

**Configuration**

1. Complete the First Time Configuration Wizard on both appliances. In Step 5 (the Local Network page of the wizard), clear the **Enable switch on LAN ports** checkbox. If you forgot to do this, you can delete the switch from the **WebUI > Device > Local Network** page.
2. Configure network settings on the appliance that will be the primary member.
3. Connect a sync cable between the appliances.
4. For the primary cluster member:
   a) Connect to the appliance that will be the primary cluster member.
b) In the WebUI, go to the **Device > High Availability** page and click **Configure Cluster**.

c) Do the wizard steps for the primary member option. For more details, see Configuring High Availability [on page 64].

5. For the secondary cluster member:

a) Connect to the appliance that will be the secondary cluster member.

b) Go to the **Device > High Availability** page and click **Configure Cluster**.

c) Do the wizard steps for the secondary member option. For more details, see Configuring High Availability [on page 64].

6. Complete other configuration requirements such as access policy, VPN, and Threat Prevention parameters. This will configure the active member and will be synchronized to the standby member. On failover, the standby member will become the active member.

**Monitoring**

After the cluster is successfully configured, it is recommended to connect to my.firewall. This redirects you to the active cluster member.

You can still log in to each appliance by connecting to http://<IP>:4434 where <IP> is the IP address of a specified member.

Note that the WebUI of the standby cluster member only has one tab, the Device tab. Not all options are available since all cluster configuration is done through the active member.

The WebUI **Device > High Availability** page shows the status of each member.
Enabling VoIP Traffic

Introduction
Do the below configuration procedures to fully allow SIP traffic to pass through the gateway when:

- The server is located on external networks.
- 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 the Users & Objects > Services page.
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 Managing System Services (on page 150).

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

2. Add a rule to the Incoming, Internal and VPN traffic Rule Base that allows SIP traffic.
   - For example:
     - Source - Any
     - Destination - Any
     - Service - SIP
     - Action - Accept
   - For more details, see Working with the Firewall Access Policy (on page 93).
3. If you know the IP address of the SIP server, you can use it as the source of this rule.
4. Optionally - you can configure if this rule will be logged or not.
Appliance Configuration

In This Section:

- Introduction to the WebUI Application ................................................................. 25
- The Home Tab ........................................................................................................ 26
- Managing the Device .......................................................................................... 37
- Managing the Access Policy .............................................................................. 89
- Managing Threat Prevention ............................................................................. 112
- Managing VPN .................................................................................................... 125
- Managing Users and Objects ............................................................................ 145
- Logs and Monitoring .......................................................................................... 157

This chapter contains instructions that help you configure the Check Point 600 Appliance and understand special Check Point 600 Appliance features.
Introduction to the WebUI Application

Check Point 600 Appliance uses a web application to configure the appliance.

After you use the First Time Configuration Wizard (see the Check Point 600 Appliance Getting Started Guide), when you connect to the appliance with a browser (with the appliance’s IP or, if using the appliance 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.

Logging in correctly opens the Home > System page of the WebUI application. 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 necessary 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 will be 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 will automatically load in the specified language. Only English is supported as the input language.
The Home Tab

Viewing System Information

The Home > System page shows an overview of Check Point 600 Appliance.

Check Point Check Point 600 Appliance requires only minimal user input of basic configuration elements, such as IP addresses, routing information, and blade configuration. The initial configuration of Check Point 600 Appliance can be done through a First Time Configuration Wizard. Once initial configuration has been completed, each subsequent entry using 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.
- **Network** - Shows Internet information and wireless network status. You can click the links to configure Internet and Wireless options (if applicable).
- **Statistics** - Shows live data graphs of packet rate and throughput.

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 regarding each blade (graph icon)
- Alerts you if there are some 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 hasn’t configured any sites). When applicable, there is a triangle in the upper right hand corner of the specified blade.

The software blades are shown in three groups on this page according to where they are configured in the WebUI:

- **Access Policy** - Contains the Firewall, Applications & URL Filtering, User Awareness, and QoS blades.
- **Threat Prevention** - Contains the Intrusion Prevention (IPS), Anti-Virus, Anti-Bot, 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:

Slide the lever of the specified blade to the necessary **ON** or **OFF** position. When turning 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 will be 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:
   a) View the graph and details.
   b) To go to other blade statistics, click the arrows in the header.
3. If the blade is turned off:
   a) Click View demo to see an example of the statistics shown.
   b) Click the X icon to close the demo.

To view an alert:
1. Hover over the alert triangle.
2. Click the relevant link if applicable.
Configuring Cloud Services

The **Home > Cloud Services** page lets you connect the Check Point 600 Appliance to Cloud Services. The Cloud Services Provider uses a Web-based application to manage, configure, and monitor your Check Point 600 Appliance.

You can connect the Check Point 600 Appliance to Cloud Services using one of these methods:

- Click the activation link in the email that the Security Gateway owner gets from the Cloud Services Provider. After you log in, a window opens and shows the activation details sent in the email. Make sure they are correct and click **Connect**. If the appliance is connected to a different Cloud Services Provider, you will be asked if you want to continue.

- Enter this page and use 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 600 Appliance.

- At the top of the WebUI application (near the search box) - The name of your Check Point 600 Appliance.

There are three 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.
  - Colorful icon - Shown for a blade that is remotely managed by Cloud Services. The blade is turned on in the plan.
  
  **Note** - A lock icon is shown on blade pages that are remotely managed. 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.

  - 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 Point 600 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 Point 600 Appliance and also an activation link
- Or
- The Service Center IP address, the Check Point 600 Appliance gateway ID, and the registration key

Connecting to Cloud Services includes these steps:

- Step 1 of 3
  - Connecting to Cloud Services Provider
  - Making sure the gateway registration information is correct
  - Establishing a secure connection
- Step 2 of 3
  - Preparing to get security policy and settings
  - Getting security policy and settings
- Step 3 of 3 Installing security policy and settings

When you connect for the first time, the appliance must make sure that 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 600 Appliance tries to connect to the Cloud Services Provider. The Cloud Services section shows a progress indicator and shows the connection steps.
4. If you are shown 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**. Clicking this widget opens the Cloud Services page.

**Note** - To test connectivity to the cloud service, open a console connection, login, and enter this CLI command:

```plaintext
test cloud-connectivity <service-center-addr> addr
```
To get an updated security policy, activated blades, and service settings:
Click **Fetch now**.

The Check Point 600 Appliance gets the latest policy, activated blades, and service settings from Cloud Services.

### 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.

You can open any of the pages directly from the Site Map page by clicking the link.

### 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 for service blades such as IPS and Anti-Virus.

**If you have Internet connectivity configured:**

1. Click the **Activate License** link on this page to be directed to the registration form in the User Center.
2. If registration information is not successfully retrieved, browse to the applicable URL:
   - For 1100 Appliances: http://register.checkpoint.com
   - For 600 Appliances: http://smbregistration.checkpoint.com
3. Complete the applicable fields in the User Center registration.
   - Appliance MAC address
   - Appliance registration key
   - From **Hardware Platform**, select **2012 Models**
   - From **Hardware Model**, select **600 Appliance**
4. Return to this page and click **Activate License**.
   You will be notified that you successfully activated the appliance. After initial activation, the Activate License button shows **Reactivate**. If changes are made to your license, click Reactivate to get the updated license information.

**If you are working offline while configuring the appliance:**

1. Browse to https://usercenter.checkpoint.com and fill out the requested information. You will have to enter the appliance’s credentials, MAC address and registration key, that can be found on the **Home > License** page.
2. After you complete the registration wizard, you will be prompted to download the activation file. Download it to a local location. This is needed for the next step.
3. In the **Home > License** page, click **Offline**.
   The Import Activation File window opens.
4. **Browse** to the activation file you downloaded and click **Import**. The activation process starts.
If there is a proxy between your appliance and the Internet, you must configure the proxy details before you can activate your license:

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

Managing Active Computers in Internal Networks

The Active Computers page shows a list of the devices that have been identified in internal networks. Information shown includes:

- Object name
- IP/MAC address
- Device/User Name - Shows a device/user name if the information is available to the Check Point 600 Appliance through DHCP or user awareness.
- Services - Shows incoming and outgoing services. Incoming services usually indicate servers.
- Zone - Shows if the appliance is connected physically or through a wireless connection.
- Traffic - Shows upload and download packet rates when traffic monitoring is active.

You can use these buttons:

- **Save as** - Lets you save a selected device as a network object or server. When you select this option, the New Network Object window or New Server Wizard 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 host 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** - Lets you filter the list according to servers, active devices, or known devices.
- **Details** - Select a row in the list and click Details to show additional properties of the device.
- **Refresh** - Refreshes the information in the list.
- **Start/Stop Traffic Monitor** - You can click Start Traffic Monitoring to gather upload and download packet rates for active computers. This information is shown in the added Traffic column in the table. This is an operation that may slightly affect performance. To stop, click Stop Traffic Monitoring. Note that the monitoring information is no longer available and the Traffic column not shown in the table.

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

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

There are two elements that 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 AM.
- 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 two hour intervals, starting with 00:00, 02:00, 04:00, 06:00 and so on. For example, if you generate a report at 09:55 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 2 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 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.

Therefore, the generation of reports after starting up an appliance will be possible:

- For hourly reports - 2-3 minutes from startup.
- For daily reports - 1-2 hours from startup.
- For weekly reports - 2-4 hours from startup.
- For 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 and Anti-Virus malwares 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 hosts, servers, and recently active infected hosts.

- 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 hosts 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.
Viewing Reports

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

There are two elements that 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 AM.
- 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 two hour intervals, starting with 00:00, 02:00, 04:00, 06:00 and so on. For example, if you generate a report at 09:55 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 2 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 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.

Therefore, the generation of reports after starting up an appliance will be possible:

- For hourly reports - 2-3 minutes from startup.
- For daily reports - 1-2 hours from startup.
- For weekly reports - 2-4 hours from startup.
- For 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 and Anti-Virus malwares 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 hosts, servers, and recently active infected hosts.
- 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 hosts 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**

The **Tools** page contains options for pinging or tracing an IP address, performing a DNS lookup, showing the routing table, generating a CPInfo file, capturing packets, and resource monitoring.

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 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 **Host 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 will overwrite 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.

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 600 Appliance.

Configuring Internet Connectivity

The Device > Internet page shows how Check Point 600 Appliance connects to the Internet. You can configure a single Internet connection or multiple connections in High Availability or Load Balancing configurations. Once multiple Internet connections are defined, the page shows them in a table, where 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.

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

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 changing 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** - Select WAN or DMZ for most types of Internet connections or USB/Serial for cellular or analog modems. In ADSL models, select ADSL.
   - **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 specific administrator-defined period.
     - **Static IP** - A fixed (non-dynamic) IP address.
     - **PPPoE** - A network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.
     - **PPTP** - The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. 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 used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it 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).
- **Cellular Modem** - Connect to the Internet using a cellular modem to the ISP via a 3G or 4G network. For this option select the USB/Serial option in Interface name.

- **Analog Modem** - Connect to the Internet using 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 will not be able to connect to the appliance using the serial port or get terminal server functionality. For more details regarding terminal server, see Device > Advanced Settings.

- **ADSL** - Connect to the Internet using ADSL. This option is only available in ADSL models.
  
  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: { } [ ] ` ~ | ' " # +

- **Use connection as VLAN** - Select this checkbox to add a virtual Internet interface. Relevant for WAN or DMZ interfaces only and static, DHCP, PPPoE, PPTP, and L2TP connection types.
  - **VLAN ID** - Enter a VLAN ID between 1 and 4094.

**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 selecting this option you can configure up to three servers by IP address or host name.
    - **Probe DNS servers** - When selecting this option the appliance probes the DNS servers as defined in the Internet connection and expects responses.

**Advanced tab**

For **PPPoE**

- **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**.

- **Service Provider Settings** - In **Service**, enter a service name (not mandatory) 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 PPPoA (only when ADSL is supported)**

- **IP Address Assignment** - Select if the local tunnel IP address is obtained automatically or manually configured. If manually configured, enter the **IP address**.

- **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 (not mandatory) 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 that for a DMZ interface the MTU value is applied to all LAN ports.

- **MAC address clone** - Choosing **Override default MAC address** lets you 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)**
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 has been turned on. You can do this from **Home > Security Dashboard > QoS > ON**.

**ISP Redundancy**
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 as according to the set mode.

- Clear the **Route traffic through this connection by default** checkbox when you want this Internet connection not to be used as a default route for this gateway. Such a connection will be used by the device only if specific, usually service-based, routing rules will be defined for it. This is commonly used when you have a connection that is used for dedicated traffic. When clearing 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 will only be used if higher priority connections are unavailable.
• **Load Balancing - Weight** - The traffic to the Internet is divided between all available connections according to their weights.

![Edit Internet Connection](image)

**Configuring Wireless Network Settings**

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 (Virtual Access Points (VAPs)).

- **Guest** wireless network - Uses hotspot by default and is unprotected (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 > Internet**.

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 have configured multiple VAPs, selecting **Off** will turn them all off.
  
  Note that if you turn off the wireless radio and then turn it back on, the VAPs will 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 customize Hotspot:**

- Click the **Hotspot** link. See the **Device > Hotspot** page for information.
To add or edit a wireless network:

1. Click **Edit wireless network settings** to edit the main wireless network.
2. To add an additional guest or standard network to the main network, click the **Guest** or **Standard** link on the page. Once defined, it shows in a table on the page where you can also create additional networks by clicking **New**. Editing one of the additional guest or standard networks (VAPs), can be done by selecting an entry from the table and clicking **Edit**.

The New/Edit Wireless Network window opens.

3. Configure the fields in these tabs:

**Configuration tab**

- **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.
- **Radio settings** - Select the correct **Operation mode**, **Channel**, **Channel width**, and **Transmitter power**. This configuration is global for all wireless networks. Some options may not be available or allowed depending on your country’s wireless standards.

**Configuration tab > 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.

**Configuration tab > 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 Configuration**

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

**Wireless Network tab > 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**

**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**

**DHCP Server Options tab**

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

This tab is only available when the wireless network is a separate network and a DHCP server is configured on it.

**DHCP Server Options tab > DNS Server**

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**.

**DHCP Server Options tab > 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.

**DHCP Server Options tab > 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.

**DHCP Server Options tab > Lease**

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

DHCP Server Options tab > 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.

The wireless client is shown as a link. Click **Edit Settings** to edit the settings. Click **Disable/Enable** to disable or enable the wireless client.

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).

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 neither monitored nor 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.
- Create and configure **VPN tunnels (VTI)** which can be used to create routing rules which determine which traffic will be 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 Network** page.

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.

Note the following:

- 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 will still be visible on this page, but can 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 will show 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 neither monitored nor inspected.
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 will not be shown at all 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 selecting a separate network, configure the settings for the switch

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 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**
DHCP Server Options tab
See DHCP Server Options tab below

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 creating a switch, the first interface within it cannot be removed from the switch unless the switch is deleted.

Advanced tab
The options that are shown vary according to 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 600 Appliance, the value is global for all physical LAN and DMZ ports.

• **Disable auto negotiation** - Choose this option to manually configure the link speed of the interface.

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**

DHCP Server Options tab
See DHCP Server Options tab below
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).

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 will be 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**

**DHCP Server Options tab**

See DHCP Server Options tab below

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 VPN site. See Configuring VPN Sites.
  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 IP 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.
  • **Local 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.
• Choose the **IP address** and **Subnet mask** the switch uses.
• **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

*DHCP Server Options tab*

See DHCP Server Options tab below
To create/edit a Virtual Access Point (VAP):

See the Device > Wireless Network help page.

**DHCP Server Options tab**

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

This tab is only available when the wireless network is a separate network and a DHCP server is configured on it.

**DHCP Server Options tab > DNS Server**

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.

**DHCP Server Options tab > 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.

**DHCP Server Options tab > 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.

**DHCP Server Options tab > Lease**

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

**DHCP Server Options tab > 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

**DHCP Server Options tab > 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 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.

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

Hotspot is automatically activated in the system. To turn it off, go to Device > Advanced Settings. Search for hotspot, double-click the entry, select **Disabled** and 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 will be 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 creating 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 either 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 will be redirected to the Check Point Hotspot portal and will have to 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. Configure the fields:
   - **Portal title** - Keep the default or enter a different title.
   - **Portal message** - Keep the default or enter a different message.
   - **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 will click the “terms and conditions” link, this text will be shown.
3. 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**.
4. Click **Apply**.

### Configuring the Routing Table

The **Device > Routing** page shows a routing table with the routes that have been added on your appliance. You can add new routes from here.

Default routes are not configured on this page. They are configured on the **Device > Internet** page, but can be viewed here. This page shows all the routing rules: manually configured on this page and defined automatically by the system. System defined routes cannot be edited.

You can create custom/new destination-based rules and policy-based routing rules, by source and by service.

To add a new route:

1. Click **New**.
   - The New Routing Rule window opens.
2. Click the links in the rule summary, or in the table cells, to select values for the routing rules. See the descriptions below. Note that for Service you can also create a new service or service group.
3. **Optional**: Enter a comment.
4. Enter a metric between 0 and 100. The default is 0.
5. Click **Apply**.

<table>
<thead>
<tr>
<th>Table Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The route rule applies only to traffic whose destination matches the destination IP address/network.</td>
</tr>
<tr>
<td>Source</td>
<td>The route rule applies only to traffic whose source matches the source IP address/network.</td>
</tr>
<tr>
<td>Service</td>
<td>The route rule applies only to traffic whose service matches the service IP protocol and ports or service group.</td>
</tr>
</tbody>
</table>
Table Columns | Description
---|---
Next Hop | The next hop gateway for this route. There are two available options: specific IP address of the next hop gateway or a specified Internet connection from the connections configured in the appliance.
Metric | Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.

The edit, delete, enable, and disable options only available for manually defined routing rules created on this page. You cannot edit, delete, enable, and disable routing rules created by the OS 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**.

**Important Notes**
- You cannot add a default route from this page. The default route of the system is inherited from Internet connection settings. To change the default route, edit an Internet connection. Then, set its default gateway (next hop) to a different IP address.
- For Internet Connection High Availability, the default route changes automatically on failover (according to the active Internet connection).
- When a network interface is disabled, all routes leading to this interface become "inactive". In such cases, the system routes traffic according to active routing rules (typically, to the default route). The route shows **inactive** in the routing page. It becomes active automatically when the interface is enabled.

When no default route is active (for example, when there is no Internet connection) this message shows: **Note: No default route is configured. Internet connections might be down or not configured.**

**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. Choose whether to define up to three DNS servers which will be 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 will be directed to these DNS servers.
The second option allows a more dynamic definition of DNS servers. The gateway will use 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 will switch automatically upon failover.

2. By default, the Check Point 600 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.

You can choose to get IP addresses directly from the DNS server(s) defined above, by clearing
the Enable DNS Proxy checkbox.

When DNS proxy is enabled, Resolve Network Objects controls whether or not the DNS proxy
will treat the local network objects as a hosts list. When selected the local DNS servers will
resolve 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

The Device > Proxy page, requires configuration when there is a proxy server between the
appliance and the Internet. This proxy server will be used when the appliance’s internal processes
must reach a Check Point server. For example, to get updates from update and license servers or
to reach the URL Filtering services.

This is not a common deployment as you usually deploy the proxy server for your organization in
the internal networks.

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:
• Click Reboot and then click OK in the confirmation message. The appliance will reboot.

To restore factory default settings:
• Click Default Settings and then click OK in the confirmation message. The factory default settings will be restored. The appliance will reboot itself to complete the operation.

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

To revert to the factory default image:
• Click Factory Defaults and then click OK in the confirmation message. The factory default settings will be restored. The appliance will reboot itself to complete the operation.

Note - This restores the default software image which the appliance came with and also the default settings (IP address 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 - 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.
4. Click Apply.

Note - When a new firmware upgrade is available, a note shows the version number and lets you upgrade it immediately by clicking Upgrade Now or you can click More Information to see what is new in the firmware version.
Note - 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:
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 will not allow restoring 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. Once the upload is complete, the wizard automatically validates the image. A progress indicator at the bottom of the page informs you the percentage completed. Upon successful image validation, an "Upload Finished" status appears.

**Upgrade Settings**

The system always performs an upgrade on a separate flash partition and your current-running partition is not affected. Consequently, you can always switch back to the current image in case of an immediate failure in the upgrade process. In the unexpected event that the appliance does not come up properly from the boot, disconnect the power cable and reconnect it. The appliance will automatically revert to the previous image.

You will be able to return to a previous image by clicking the **Revert to Previous Image** button on the System Operations page. 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 > Backup Settings** page do these steps:

1. To encrypt the backup file, select the **Use File Encryption** checkbox. Set and confirm a **password**.
   
   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.

2. You can add **Comments** about the specific backup file created.
   
   By default, system settings are always backed up.

3. Click **Create Backup**.

4. Click **Download Backup** to save the backup file. 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.
Important Notes

If you wish to replace an existing appliance with another one (for example, upon hardware failure) you can simply restore the settings saved on your previous appliance and re-activate your license (through License Page > Activate License).

If you wish 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.

Configuring Local and Remote System Administrators

The Device > Administrators page lists the Check Point 600 Appliance administrators and lets you create new local administrators, configure the session timeout, and limit login failure attempts. 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.

You can create administrators with read-only privileges. Read-only administrators cannot update appliance configuration, but some other operations are still available to them. For example, they can create new read-only users or run a traffic monitoring report from the Tools page.

To create a Check Point 600 Appliance local administrator:

1. Click New. The Add administrator page appears.
2. Configure the parameters in the page that opens (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. To set the administrator with read-only privileges, select Read-only Administrator.
4. Click Apply.

The name and permission information of the administrator is added to the table. When logging in to the WebUI, the administrator name and an icon that represents read or read/write permissions 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 that you cannot delete the administrator that 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 will be asked to configure the IP address and shared secret used by the RADIUS server.
3. Click **edit permissions** once you have a configured RADIUS server.
4. Click the **Enable RADIUS authentication for administrators** checkbox.
5. Select which user group defined in the RADIUS server will be granted administrator permissions:
   a) Select **All users defined on RADIUS server** (not recommended) or **Specific RADIUS groups only** and enter the RADIUS groups separated by a comma.
   b) To enable RADIUS authentication for read-only administrators, select the **Read-only Administrators** checkbox.
6. Click **Apply**.

**To set the Session Timeout value for both local and remotely defined administrators:**
1. Click **Session Timeout**.
2. Configure the session timeout in the page that opens (maximum time period of inactivity in minutes). The maximum value is 999 minutes.
3. Click **Apply**.

**To limit login failure attempts for both local and remotely defined administrators:**
1. Click **Session Timeout**.
2. Select **Limit administrators login failure attempts**.
3. Enter the number of **Maximum consecutive login attempts** allowed before a user is locked out.
4. In **Lock period**, enter the time (in seconds) that must pass before a locked out administrator can attempt to log in again.
5. Click **Apply**.

---

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

---

**Configuring a RADIUS Server for Non-Local Check Point 600 Appliance Users**

Non-local users can be defined on a RADIUS server and not in Check Point 600 Appliance. When a non-local user logs in to Check Point 600 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** - If you define a RADIUS user with a null password (on the RADIUS server), Check Point 600 Appliance cannot authenticate that user.
To configure a Steel-Belted RADIUS server for non-local Check Point 600 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-Role CheckPoint-VSA(229, string) r
   ATTRIBUTE CP-Gaia-SuperUser-Access CheckPoint-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 Check Point 600 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 = <group_name>
   ```

   Where `<group_name>` is the name of the RADIUS group that is defined in the Check Point 600 Appliance WebUI.

To configure a FreeRADIUS server for non-local Check Point 600 Appliance users

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

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

2. Add to `/etc/freeradius/dictionary` the line:

   ```
   "$INCLUDE dictionary.checkpoint"
   ```

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

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

   Where `<group_name>` is the name of the RADIUS group that is defined in the Check Point 600 Appliance WebUI.
To configure a OpenRADIUS server for non-local Check Point 600 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 229 CP-Gaia-User-Role
   $add attribute 230 CP-Gaia-SuperUser-Access val_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 = <group_name>`
   Where `<group_name>` is the name of the RADIUS group that is defined in the Check Point 600 Appliance WebUI.

To log in as a superuser

A user with super user permissions can use the Check Point 600 Appliance shell to do system-level operations, including working with the file system.

1. Connect to the Check Point 600 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` Enter the expert 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 600 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 and Wireless Network + ADSL models)
- **VPN** - Using encrypted traffic through VPN tunnels from a remote site or using 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. It is recommended to 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 will be able to access Check Point 600 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 **Add**. The Access Policy IP Address Configuration page appears.
3. Define the IPv4 address as either:
   - **Specific IP address** - manually enter the IP address or click **Get IP from My Computer**.
   - **Specific Network** - manually enter the **Network Address** and **Subnet Mask**.
4. Click **Apply**. The IP address is added to the table.
5. Change the **WEB Port (HTTPS)** and/or **SSH port** if necessary.
6. Click **Apply**. An administrator will be able to access Check Point 600 Appliance using the configured IP addresses through the allowed interface sources.

To allow administrator access from the Internet for specified IP addresses and from any IP address for other sources:
Select this option when it is necessary to allow administrator access from the Internet (you must define the specific 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 **Add**. The Access Policy IP Address Configuration page appears.
4. Define the IPv4 address as either:
   - **Specific IP address** - manually enter the IP address or click **Get IP from My Computer**.
   - **Specific Network** - manually enter the **Network Address** and **Subnet Mask**.
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 will be able to access Check Point 600 Appliance using the configured IP addresses through the allowed interface sources.
To delete administrator access from a specific IP address:
1. Select the IPv4 Address you want to delete from the IPv4 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.
- For your convenience, when you block the IP address or the interface group through which you are currently connected, you will not be disconnected immediately. The access policy is applied immediately, but your current session remains active until you log out.

Managing Device Details
In the Device > Device Details page, you can enter a name for the appliance.
- Enter an Appliance Name to identify the Check Point 600 Appliance.
  - The Appliance Name can only contain alphanumeric characters and the hyphen character.
  - The hyphen character should not be used as the first or last character.
- In wireless devices only - You can also configure the Country on this page. The allowed wireless radio settings vary according to the standards in each country.

Managing Date and Time Settings
The Device > Date and Time page shows the current system time and lets you define the Check Point 600 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 will be 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 Services**

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 will update the provider with its IP addresses. Users can then connect to the device using a host name given by 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)** to enable this service.
2. Enter the details of your account on the page:
   - **Provider** - Select the DDNS provider that you have already 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, reinitialization of internal certificates is necessary 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.
### How it works

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Register the Check Point 600 Appliance to the Check Point Cloud Service - When you first enter the <strong>Device &gt; DDNS &amp; Device Access</strong> page you see a link to register the appliance. Use the procedure below to register the appliance to the service.</td>
</tr>
</tbody>
</table>
| 2    | Upon successful registration - An outgoing tunnel to the Check Point Cloud Service is established with the appliance’s IP address. In the WebUI, the **Device > DDNS & Device Access** page shows:  
  - Validation token - A token you enter to make sure the host name is valid. This token is used to verify that an existing name actually belongs to this appliance owner.  
  - 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 is shown, enter the applicable user name and password.  
  - Shell link - Use this URL in a browser to open an SSH connection to the appliance in order to use CLI commands. For example: https://mygateway-shell.smbrelay.checkpoint.com Enter the administrator credentials. |
| 3    | When an administrator requires access to the WebUI or CLI, the applicable URL is entered in a browser and gets to the Web Service in the cloud. |
| 4    | The administrator gains access to the appliance WebUI or CLI through a pipe established by the Check Point Cloud Service to the appliance. |
To register to allow connections to the appliance when it is unreachable from the Internet:

1. Click **Register**.
   The Reach My Device window opens.
2. In **Host name**, use the default host name or enter a name for this Check Point 600 Appliance to enable remote access to it.
3. If the host name has already been defined, select **Register with an existing home name** and enter the **Validation token** of the gateway.
4. Click **Apply**.
   The validation token, web link, and shell link are shown on the **DDNS & Appliance Access** page.
5. Go to the **Device > Administrator Access** page and make sure to configure **Internet** as a source for administrator access and set specified IP addresses.

**Using System Tools**

See Using System Tools [on page 35].

**Configuring High Availability**

In the **Device > High Availability** page you can create a cluster of two Check Point 600 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.

If you change configuration details of the cluster members, click **Reinitialize Trust** to reestablish trust between the members.

**Reset Cluster Configuration** - Deletes all configuration settings. You will have to run the wizard again to configure the cluster.

**Force Member Down** - Use this option when it is necessary to failover to the other member. For example, when you want to test the functionality of the other member.

For troubleshooting, you can click the **diagnostics** button to see detailed information about the status of the cluster.

**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 has already been configured and this appliance will connect 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 will be used 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 will 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.

### Configuring 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**.
   The appliance attribute is configured.
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.

**Aggressive Aging**

<table>
<thead>
<tr>
<th>Aggressive Aging Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple parameters</td>
<td>Aggressive Aging helps manage the connections table capacity and memory consumption of the firewall to increase durability and stability.</td>
</tr>
</tbody>
</table>

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.

Aggressive Aging allows the gateway machine to handle large amounts of unexpected traffic, especially during a Denial of Service attack.

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.

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.

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.
Aggressive Aging Attributes | Description
--- | ---

**To configure Aggressive Aging:**

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**.

**To configure when the Aggressive Aging timeouts are enforced:**

1. Under **Aggressive Aging Timeouts are enforced when** section, select whether they will be 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.

---

**Anti-Spam policy**

| 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]. |
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. |
Transparent proxy | Use a transparent proxy for inspected email connections. When disabled, configuration of the proxy address and port is required on client machines. |
### Anti-Spoofing

<table>
<thead>
<tr>
<th>Anti-Spoofing Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable global anti-spoofing</td>
<td>Indicates if anti-spoofing is enabled automatically on all interfaces according to their zone.</td>
</tr>
</tbody>
</table>

### Application Control and URL Filtering

<table>
<thead>
<tr>
<th>Application Control and URL Filtering Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block when service is unavailable</td>
<td>Indicates if web requests are blocked when the Check Point categorization and widget definitions Online Web Service is unavailable.</td>
</tr>
<tr>
<td>Categorize cached and translated pages</td>
<td>Indicates if to perform URL categorization of cached pages and translated pages created by search engines.</td>
</tr>
<tr>
<td>Enforce safe search</td>
<td>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.</td>
</tr>
<tr>
<td>Fail mode</td>
<td>Indicates the action to take on traffic in case of an internal system error or overload.</td>
</tr>
<tr>
<td>Track browse time</td>
<td>Shows in logs the total time that users are connected to different sites and applications in an HTTP session</td>
</tr>
<tr>
<td>Use HTTP referer header</td>
<td>Indicates if the HTTP &quot;referer&quot; header (originally a misspelling of referrer) is used by the inspection engine to improved application identification.</td>
</tr>
<tr>
<td>Web site categorization mode</td>
<td>Indicates the mode that is used for website categorization:</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Hold</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Capacity Optimization

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

### Cloud Services Firmware Upgrade

<table>
<thead>
<tr>
<th>Cloud Services Firmware Upgrade Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service access maximum retries</td>
<td>Indicates the maximum number of retries when failing to upgrade using the service.</td>
</tr>
<tr>
<td>Service access timeout until retry</td>
<td>Indicates the time (in seconds) to wait when there is a connection failure to the service before the next retry.</td>
</tr>
</tbody>
</table>

### Cluster

<table>
<thead>
<tr>
<th>Cluster Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use virtual MAC                 | Indicates if a virtual MAC address will be used by all members to allow a quicker failover by the network’s switch. Using the virtual MAC address:  
  - Minimizes the potential traffic outage during fail-over.  
  - Removes the need to use G-ARPs for NATed IP addresses. |

### DHCP relay

<table>
<thead>
<tr>
<th>DHCP Relay Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use internal IP addresses as source</td>
<td>Select <strong>Use internal IP addresses as source</strong> if DHCP relay packets from the appliance will originate from internal IP addresses. This may be required if the DHCP server is located behind a remote VPN site.</td>
</tr>
</tbody>
</table>
**General Temporary Directory Size**

<table>
<thead>
<tr>
<th>General Temporary Directory Size Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General temporary directory size</td>
<td>Controls the size (in MB) of the general temporary directory.</td>
</tr>
<tr>
<td>System temporary directory size</td>
<td>Controls the size (in MB) of the temporary directory that is used by the system.</td>
</tr>
</tbody>
</table>

**Hardware Options**

<table>
<thead>
<tr>
<th>Hardware Options Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset to factory defaults timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Hotspot**

<table>
<thead>
<tr>
<th>Hotspot Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable portal</td>
<td>Select <strong>Disabled</strong> to disable the hotspot feature entirely.</td>
</tr>
</tbody>
</table>

**IP Fragments Parameters**

<table>
<thead>
<tr>
<th>IP Fragments Parameters Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple parameters</td>
<td>These parameters let you configure how the appliance handles IP fragments. It can either block fragmented IP packets or drop fragments once a configured threshold is reached. Select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forbid IP Fragments</strong> - Fragmented IP packets will be dropped.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow IP Fragments</strong> - 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.</td>
</tr>
</tbody>
</table>

**IPS Additional Parameters**

<table>
<thead>
<tr>
<th>IPS Additional Parameters Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max ping limit</td>
<td>Indicates the maximal ping packet size that will be allowed when the ‘Max Ping Size’ protection is active.</td>
</tr>
</tbody>
</table>
### IPS Engine Settings

<table>
<thead>
<tr>
<th>IPS Engine Settings Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure error page options for supported web protections - multiple parameters | Some web based protections can show an error page upon detection. This error page is configurable. The protections that support the error page:  
• 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  
Select one of these options that will apply to all such protections:  
• **Do not show**  
• **Show pre-defined HTML error page** - You can configure an HTML page that will open upon detection of an attack. 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 will be redirected upon detection of an attack. You can also choose 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. |
**IPS Engine Settings Attributes**

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML error page configuration - multiple parameters</td>
<td>These settings allow you to configure a pre-defined HTML error page that will be seen when the error page advanced settings are set to <strong>Show pre-defined HTML error page</strong>. Select one of these options:</td>
</tr>
<tr>
<td>- Logo URL - Optionally enter a URL that leads to your company logo.</td>
<td></td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>- Send detailed error code - You can enter manually defined text that will be shown in the HTML page. Enter the text in the Description box. For example, Access denied due to IPS policy violation.</td>
<td></td>
</tr>
</tbody>
</table>

**Managed Services**

<table>
<thead>
<tr>
<th>Managed Services Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow seamless administrator access from remote Management Server</td>
<td>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.</td>
</tr>
<tr>
<td>Show device details in Login</td>
<td>Indicates if appliance details are shown when an administrator accesses the appliance.</td>
</tr>
</tbody>
</table>

**NAT**

<table>
<thead>
<tr>
<th>NAT Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP manual file merge</td>
<td>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.</td>
</tr>
<tr>
<td>NAT Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multiple parameters - IP Pool NAT</td>
<td>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. When using IP Pool NAT, select an existing IP address range object. It must be previously defined in the Users &amp; Objects &gt; Networks Objects page. The IP Pool NAT mechanism will allocate IP addresses from this range. <strong>Use IP Pool NAT for VPN clients connections</strong> - Applies to connections from VPN remote access clients to the gateway. <strong>Use IP Pool NAT for gateway to gateway connections</strong> - Applies to site to site VPN connections. <strong>Prefer IP Pool NAT over Hide NAT</strong> - 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. <strong>Reuse IP addresses from the Pool for different destinations</strong> - Select this option to reuse IP addresses from the Pool for different destinations. <strong>Unused addresses interval</strong> - Configure in minutes the time interval it takes for unused addresses to return to the IP addresses pool. <strong>Address exhaustion tracking</strong> - Specifies the type of log to issue if the IP Pool is exhausted. <strong>Address allocation and release tracking</strong> - Specifies whether to log each allocation and release of an IP address from the IP Pool.</td>
</tr>
<tr>
<td>Automatic ARP detection</td>
<td>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.</td>
</tr>
<tr>
<td>Increase hide capacity</td>
<td>Indicates if hide-NAT capacity is given additional space.</td>
</tr>
<tr>
<td>NAT enable</td>
<td>Indicates if the device’s NAT capabilities are enabled.</td>
</tr>
<tr>
<td>NAT cache expiration</td>
<td>Indicates the expiration time in minutes for NAT cache entries.</td>
</tr>
<tr>
<td>NAT cache number of entries</td>
<td>Indicates the maximum number of NAT cache entries.</td>
</tr>
<tr>
<td>NAT hash size</td>
<td>Indicates the hash bucket size of NAT tables.</td>
</tr>
<tr>
<td>NAT limit</td>
<td>Indicates the maximum number of connections with NAT.</td>
</tr>
<tr>
<td>NAT Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Perform cluster hide fold</td>
<td>Indicates if local IP addresses will be hidden behind the cluster IP address when applicable, as opposed to being hidden behind each cluster member’s physical IP address.</td>
</tr>
<tr>
<td>Translate destination on client side</td>
<td>Translates destination IP addresses on client side (for automatically generated NAT rules).</td>
</tr>
<tr>
<td>Translate destination on client side (manual rules)</td>
<td>Translates destination IP addresses on client side (for manually configured NAT rules).</td>
</tr>
</tbody>
</table>

**QoS Blade**

<table>
<thead>
<tr>
<th>QoS Blade Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Indicates if the appliance logs QoS events when the QoS blade is enabled.</td>
</tr>
</tbody>
</table>

**Reach My Device**

<table>
<thead>
<tr>
<th>Reach My Device Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore SSL certificate</td>
<td>Indicates if the SSL certificate should be ignored when running the access service.</td>
</tr>
<tr>
<td>Server address</td>
<td>Indicates the address of the remote server that allows administration access to the appliance from the Internet even when behind NAT.</td>
</tr>
</tbody>
</table>
### Serial Port

<table>
<thead>
<tr>
<th>Serial Port Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Parameters</td>
<td>With the serial port parameters you can configure the console port on the back panel of the appliance. You can disable it completely <a href="#">clear the Enable serial port checkbox</a> if necessary and configure <strong>port speed</strong> and <strong>flow control</strong> settings. Note that these settings must match the configuration of the device connected to the console port. There are three modes for working with this port:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Console</strong> - This is the default mode configured. The port is used to access the appliance’s console.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong> - 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 <strong>Server TCP port</strong> of the telnet server and the IP address of the server. Two different IP server IP addresses can be configured (<strong>Primary server</strong> and <strong>Secondary server</strong>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Passive</strong> - 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 will be accessible through a telnet connection to a configured port on the appliance. In <strong>Listen on TPC port</strong>, enter the port number. To configure an implicit rule that allows traffic from any source to this port, make sure <strong>Implicitly allow traffic to this port</strong> is selected. If you do not create an implicit rule, you must manually define an access rule in the Firewall rule base.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Stateful Inspection

<table>
<thead>
<tr>
<th>Stateful Inspection Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept out of state TCP packets</td>
<td>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).</td>
</tr>
<tr>
<td>Accept stateful ICMP errors</td>
<td>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.</td>
</tr>
<tr>
<td>Accept stateful ICMP replies</td>
<td>Accept ICMP reply packets for ICMP requests that were accepted by the Rule Base.</td>
</tr>
<tr>
<td>Stateful Inspection Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accept stateful UDP replies for unknown services</td>
<td>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.</td>
</tr>
<tr>
<td>Accept stateful other IP protocols replies for unknown services</td>
<td>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 UDP/TCP connections which are not covered by the service objects.</td>
</tr>
<tr>
<td>Allow LAN-DMZ DPI</td>
<td>Allow Deep Packet Inspection in traffic between internal networks and the DMZ network.</td>
</tr>
<tr>
<td>Allow LAN-LAN DPI</td>
<td>Allow Deep Packet Inspection in traffic between internal networks.</td>
</tr>
<tr>
<td>Drop out of state ICMP packets</td>
<td>Drop ICMP packets which are not in the context of a &quot;virtual session&quot;.</td>
</tr>
<tr>
<td>ICMP virtual session timeout</td>
<td>An ICMP virtual session will be considered to have timed out after this time period (in seconds).</td>
</tr>
<tr>
<td>Log dropped out of state ICMP packets</td>
<td>Indicates if dropped out of state ICMP packets will generate a log. See the “Drop out of state ICMP packets” parameter.</td>
</tr>
<tr>
<td>Log dropped out of state TCP packets</td>
<td>Indicates if dropped out of state TCP packets will generate a log. See the “Accept out of state TCP packets” parameter.</td>
</tr>
<tr>
<td>Other IP protocols virtual session timeout</td>
<td>A virtual session of services which are not TCP, UDP or ICMP will be considered to have timed out after this time period (in seconds).</td>
</tr>
<tr>
<td>TCP end timeout</td>
<td>Indicates the timeout (in seconds) for TCP session end. A TCP session will be considered as &quot;ended&quot; following either two FIN packets, one in each direction, or an RST packet.</td>
</tr>
<tr>
<td>TCP session timeout</td>
<td>Indicates the timeout (in seconds) for TCP sessions. A TCP session will time out if the connection remains idle after this time period (in seconds).</td>
</tr>
<tr>
<td>TCP start timeout</td>
<td>Indicates the timeout (in seconds) for TCP session start. A TCP connection will time 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).</td>
</tr>
<tr>
<td>UDP virtual session timeout</td>
<td>A UDP virtual session will be considered to have timed out after this time period (in seconds).</td>
</tr>
</tbody>
</table>
## Streaming Engine Settings

<table>
<thead>
<tr>
<th>Streaming Engine Settings Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple parameters</td>
<td>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. It is highly recommended that these settings always be in prevent mode. Using these settings in detect mode may significantly lower security as inspection will stop when the event or violation occurs. When the configuration is set to log such events, the logs are shown in Logs &amp; Monitoring &gt; Security Logs under the IPS blade. For each violation or event configure the action and tracking mode.</td>
</tr>
<tr>
<td>TCP Segment Limit Enforcement</td>
<td>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 will not accept new segments for this connection until buffered segments are acknowledged.</td>
</tr>
<tr>
<td>TCP Out of Sequence</td>
<td>The receiving host of a TCP stream buffers segments and will retain only those segments within a specified window. Segments outside this window will not be 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 will be stripped. If the segment is far from the window, the segment will be dropped.</td>
</tr>
<tr>
<td>TCP Invalid Retransmission</td>
<td>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 will cause the traffic to bypass deep inspection blades.</td>
</tr>
<tr>
<td>Streaming Engine Settings Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TCP Invalid Checksum</td>
<td>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.</td>
</tr>
<tr>
<td>TCP SYN Modified Retransmission</td>
<td>A TCP SYN packet may be retransmitted with a changed sequence number in an attempt to initiate a connection that IPS will not inspect. This blocks a SYN retransmission where the sequence number has been modified. When set to detect, such retransmissions will cause the traffic to bypass deep inspection blades.</td>
</tr>
<tr>
<td>TCP Urgent Data Enforcement</td>
<td>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 will process 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 will cause the traffic to bypass deep inspection blades.</td>
</tr>
<tr>
<td>Stream Inspection Timeout</td>
<td>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 will cause the traffic to bypass deep inspection blades.</td>
</tr>
</tbody>
</table>
**Threat Prevention Anti-Bot Policy**

<table>
<thead>
<tr>
<th>Threat Prevention Anti-Bot Policy Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource classification mode</td>
<td>Indicates the mode used by the Anti-Bot engine for resource classification:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hold</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Background</strong> - 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.</td>
</tr>
</tbody>
</table>

**Threat Prevention Anti-Virus Policy**

<table>
<thead>
<tr>
<th>Threat Prevention Anti-Virus Policy Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File scan size limit</td>
<td>Indicates the size limit (in KB) of a file scanned by Anti-Virus engine. To specify no limit, set to 0.</td>
</tr>
<tr>
<td>MIME maximum nesting level</td>
<td>For emails that contain nested MIME content, set the maximum number of levels that the ThreatSpect engine scans in the email.</td>
</tr>
<tr>
<td>MIME nesting level exceeded action</td>
<td>If there are more nested levels of MIME content than the configured amount, select to <strong>Block</strong> or <strong>Allow</strong> the email file.</td>
</tr>
<tr>
<td>Priority scanning</td>
<td>Scan according to security and performance priorities for maximum optimization.</td>
</tr>
<tr>
<td>Resource classification mode</td>
<td>Indicates the mode used by the Anti-Virus engine for resource classification:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hold</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Background</strong> - 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.</td>
</tr>
</tbody>
</table>
### Threat Prevention Policy

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

**Method for skipping HTTP inspection**

**Warning:** Changing the setting to *Full* has a severe security impact.

An HTTP connection can be made up of many sessions. A file that is part of an HTTP connection passes in one HTTP session.

If a non-zero [File inspection size limit](#) is configured, the [Default](#) 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.

If a non-zero [File inspection size limit](#) is configured and the [Method for skipping HTTP inspection](#) is changed to *Full*, 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 *Full* is not recommended because of a severe security impact: The remaining sessions of the connection are not inspected.

---

### USB Modem Watchdog

<table>
<thead>
<tr>
<th>USB Modem Watchdog Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Indicates how often (in minutes) the USB modem watchdog probes the internet</td>
</tr>
</tbody>
</table>
| Mode                         | To enable USB modem watchdog when internet probing indicates there is no internet access, select one of these reset options:  
  - Hard reset - Shuts down the power for the USB modem and turns it on again.
  - Gateway reset - Restarts the appliance. |
### Update services schedule

<table>
<thead>
<tr>
<th>Update Services Schedule Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of retries</td>
<td>Indicates the maximum number of retries for a single update when the cloud is unavailable</td>
</tr>
<tr>
<td>Timeout until retry</td>
<td>Indicates the timeout (in seconds) until update retry.</td>
</tr>
</tbody>
</table>

### User Awareness

<table>
<thead>
<tr>
<th>User Awareness Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory association timeout</td>
<td>Indicates the timeout (in minutes) for caching an association between a user and an IP address.</td>
</tr>
<tr>
<td>Allow DNS for unknown users</td>
<td>Indicates that DNS traffic from unauthenticated users will not be blocked when <strong>Block unauthenticated users when the captive portal is not possible</strong> is selected in Users &amp; Objects &gt; User Awareness &gt; Browser-Based Authentication &gt; Identification tab. Without DNS traffic, the browsers of end users, may not show the Captive Portal.</td>
</tr>
<tr>
<td>Assume single user per IP address</td>
<td>When Active Directory Queries is enabled in Users &amp; Objects &gt; 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.</td>
</tr>
<tr>
<td>Log blocked unknown users</td>
<td>Indicates if unauthenticated users that are blocked will be logged when <strong>Block unauthenticated users when the captive portal is not possible</strong> is selected in Users &amp; Objects &gt; User Awareness &gt; Browser-Based Authentication &gt; Identification tab.</td>
</tr>
</tbody>
</table>

### VPN Remote Access

<table>
<thead>
<tr>
<th>VPN Remote Access Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow clear Traffic while disconnected</td>
<td>Indicates if traffic to the VPN domain is handled when the Remote Access VPN client is not connected to the site will be sent without encryption (clear) or dropped.</td>
</tr>
<tr>
<td>Allow simultaneous login</td>
<td>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 will be disconnected.</td>
</tr>
<tr>
<td>Authentication timeout</td>
<td>Indicates the amount of time (in minutes) the remote client’s password remains valid if timeout is enabled.</td>
</tr>
<tr>
<td>Authentication timeout enable</td>
<td>Indicates if the remote client’s password remains valid only for a configured amount of time (Authentication timeout attribute).</td>
</tr>
<tr>
<td><strong>VPN Remote Access Attributes</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Auto-disconnect in VPN domain</td>
<td>Indicates if the client disconnects automatically to save resources when it connects from inside the secured internal network (local encryption domain).</td>
</tr>
<tr>
<td>Back connections enable</td>
<td>Enable back connections from the encryption domain behind the gateway to the client.</td>
</tr>
<tr>
<td>Back connections keep-alive interval</td>
<td>Indicates the interval (in seconds) between keep-alive packets to the gateway required for gateway to client back connections.</td>
</tr>
<tr>
<td>Enable Visitor Mode on All Interfaces</td>
<td>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. This mode is normally used to allow VPN remote access connections from behind restrictive environments such as hotels. Modifying visitor mode to be enabled only on a specific interface is not recommended.</td>
</tr>
<tr>
<td>Encrypt DNS traffic</td>
<td>Indicates if DNS queries sent by the remote client to a DNS server located in the encryption domain are passed through the VPN tunnel.</td>
</tr>
<tr>
<td>Encryption Method</td>
<td>Indicates which IKE encryption method (version) is used for IKE phase 1 and 2.</td>
</tr>
<tr>
<td>Endpoint Connect re-authentication timeout</td>
<td>Indicates the time (in minutes) until the Endpoint Connect user’s credentials are resent to the gateway to verify authorization.</td>
</tr>
<tr>
<td>IKE IP Compression Support</td>
<td>Indicates if IPSec packets from remote access clients will be compressed.</td>
</tr>
<tr>
<td>IKE Over TCP</td>
<td>Enables support of IKE over TCP.</td>
</tr>
<tr>
<td>IKE restart recovery</td>
<td>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.</td>
</tr>
<tr>
<td>Legacy NAT traversal</td>
<td>Indicates if the Check Point proprietary NAT traversal mechanism (UDP encapsulation) is enabled for SecureClient.</td>
</tr>
<tr>
<td>Office Mode Enable With Multiple Interfaces</td>
<td>Indicates if a mechanism (with a performance impact) to improve connectivity between remote access client and an appliance with multiple external interfaces is enabled.</td>
</tr>
<tr>
<td><strong>VPN Remote Access Attributes</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Office Mode Perform Antispoofing</strong></td>
<td><strong>Office Mode Perform Antispoofing</strong> - 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.</td>
</tr>
<tr>
<td><strong>Single Office Mode Per Site</strong></td>
<td><strong>Single Office Mode Per Site</strong> - After a remote user connects and receives an Office Mode IP address from a gateway, every connection to that gateways encryption domain will go out with the Office Mode IP as the internal source IP. The Office Mode IP is what hosts in the encryption domain will recognize as the remote user’s IP address. The Office Mode IP address assigned by a specific 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. Since 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 will terminate.</td>
</tr>
<tr>
<td><strong>Office Mode allocate from RADIUS</strong></td>
<td>Indicates if the Office Mode allocated IP addresses will be taken from the RADIUS server used to authenticate the user.</td>
</tr>
<tr>
<td><strong>Office Mode disable</strong></td>
<td>Indicates if Office Mode (allocating IP addresses for Remote Access clients) is disabled. This is not recommended.</td>
</tr>
<tr>
<td><strong>Passwords caching on client</strong></td>
<td>Indicates if password caching is used. This means that re-authentication will not be necessary when the client tries to access more than one gateway.</td>
</tr>
<tr>
<td><strong>Prevent IP NAT Pool</strong></td>
<td>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 h_121870).</td>
</tr>
<tr>
<td><strong>Remote Access port Reserve port 443 for port forwarding</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>SNX keep-alive interval</strong></td>
<td>Indicates the time [in seconds] between the SSL Network Extender client keep-alive packets.</td>
</tr>
<tr>
<td><strong>SNX re-authentication timeout</strong></td>
<td>Indicates the time [in minutes] between re-authentication of SSL Network Extender remote access users.</td>
</tr>
<tr>
<td><strong>VPN Remote Access Attributes</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SNX support RC4</td>
<td>Indicates if the RC4 encryption algorithm will be supported in SSL clients as well as the default algorithms.</td>
</tr>
<tr>
<td>SNX uninstall</td>
<td>This parameter lets you configure under which conditions the SSL Network Extender client will uninstall itself. The options are: Do not uninstall automatically (recommended default), always uninstall upon disconnection, and ask the user upon disconnection.</td>
</tr>
<tr>
<td>SNX upgrade</td>
<td>This parameter lets you configure under which conditions the SSL Network Extender client will install itself. The options are: Do not upgrade automatically, always upgrade, and ask the user (default).</td>
</tr>
<tr>
<td>Topology updates manual interval</td>
<td>Indicates the manually configured interval (in hours) for topology updates to the clients. Will be applicable only if the override settings is set to true.</td>
</tr>
<tr>
<td>Topology updates override</td>
<td>Indicates if the configured topology updates settings will override the default ‘once a week’ policy.</td>
</tr>
<tr>
<td>Topology updates upon startup only</td>
<td>Indicates if topology updates will occur only when the client starts. Will be applicable only if the override settings is set to true.</td>
</tr>
<tr>
<td>Verify device certificate</td>
<td>The remote access client will verify the device’s certificate against revocation list.</td>
</tr>
</tbody>
</table>

**VPN Site to Site Global Settings**

<table>
<thead>
<tr>
<th><strong>VPN Site to Site Global Settings Attributes</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept NAT Traversal</td>
<td>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.</td>
</tr>
<tr>
<td>Administrative notifications</td>
<td>Indicates how to log an administrative event (for example, when a certificate is about to expire)</td>
</tr>
<tr>
<td>Check validity of IPSec reply packets</td>
<td>Indicated whether to check the validity of IPSec reply packets.</td>
</tr>
<tr>
<td>Cluster SA sync packets threshold</td>
<td>Sync SA with other cluster members when the number of packets reaches this threshold.</td>
</tr>
<tr>
<td>Copy DiffServ mark from encrypted/decrypted IPSec packet</td>
<td>Copy DiffServ mark from encrypted/decrypted IPSec packet.</td>
</tr>
<tr>
<td>Copy DiffServ mark to encrypted/decrypted IPSec packet</td>
<td>Copy DiffServ mark to encrypted/decrypted IPSec packet.</td>
</tr>
<tr>
<td><strong>VPN Site to Site Global Settings Attributes</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Enable encrypted packets rerouting</td>
<td>Indicates if encrypted packets will be rerouted through the best interface according to the peer’s IP address or probing. It is not recommended to change this value to false.</td>
</tr>
<tr>
<td>Grace Period after CRL is no longer valid</td>
<td>CRL grace period is required to resolve the issue of differing clock times between the appliance and the remote CA. A grace period permits a wider window for CRL validity. Indicates the time (in seconds) after which a revoked certificate of a remote site remains valid.</td>
</tr>
<tr>
<td>Grace Period before CRL is valid</td>
<td>CRL grace period is required to resolve the issue of differing clock times between the appliance and the remote CA. A grace period permits a wider window for CRL validity. Indicates the time window (in seconds) where a certificate is considered valid prior to the time set by the CA.</td>
</tr>
<tr>
<td>IKE DoS from known sites protection</td>
<td>Indicates if the IKE DoS from known IP addresses protection is active and the method by which it detects potential attackers.</td>
</tr>
<tr>
<td>IKE DoS from unknown sites protection</td>
<td>Indicates if the IKE DoS from unidentified IP addresses protection is active and the method by which it detects potential attackers.</td>
</tr>
<tr>
<td>IKE Reply From Same IP</td>
<td>Indicates if the source IP address used in IKE session will be according to destination when replying to incoming connections, or according to the general source IP address link selection configuration.</td>
</tr>
<tr>
<td>Join adjacent subnets in IKE Quick Mode</td>
<td>Indicates if to join adjacent subnets in IKE Quick Mode.</td>
</tr>
<tr>
<td>Keep DF flag on packet</td>
<td>Indicates if the ‘Don’t Fragment’ flag is kept on the packet during encryption/decryption.</td>
</tr>
<tr>
<td>Key exchange error tracking</td>
<td>Indicates how to log VPN configuration errors or key exchange errors.</td>
</tr>
<tr>
<td>Maximum concurrent IKE negotiations</td>
<td>Indicates the maximum number of concurrent VPN IKE negotiations.</td>
</tr>
<tr>
<td>Maximum concurrent tunnels</td>
<td>Indicates the maximum number of concurrent VPN tunnels.</td>
</tr>
<tr>
<td>Open SAs limit</td>
<td>Indicates the maximum number of open SAs per VPN peer.</td>
</tr>
<tr>
<td>Outgoing link tracking</td>
<td>Indicates how to log the outgoing VPN link: Log, don’t log, or alert.</td>
</tr>
</tbody>
</table>
## VPN Site to Site Global Settings Attributes

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Override 'Route all traffic to remote VPN site' configuration for admin access to the device</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Packet handling errors tracking</strong></td>
</tr>
<tr>
<td>Indicates how to log the VPN packet handling errors: Log, don’t log, or alert.</td>
</tr>
<tr>
<td><strong>Perform Tunnel Tests using an internal IP Address</strong></td>
</tr>
<tr>
<td>A Tunnel Test makes sure that the VPN tunnel between peer VPN Gateways is up.</td>
</tr>
<tr>
<td>By default, the test is done by making sure there is a connection between all the external IP addresses of the peer VPN Gateways.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>You can see the status of the VPN tunnel in the <strong>Logs and Monitoring</strong> tab.</td>
</tr>
<tr>
<td><strong>Permanent tunnel down tracking</strong></td>
</tr>
<tr>
<td>Indicates how to log when the tunnel goes down: Log, don’t log, or alert.</td>
</tr>
<tr>
<td><strong>Permanent tunnel up tracking</strong></td>
</tr>
<tr>
<td>Indicates how to log when the tunnel is up: Log, don’t log, or alert.</td>
</tr>
<tr>
<td><strong>RDP packet reply timeout</strong></td>
</tr>
<tr>
<td>Timeout (in seconds) for an RDP packet reply.</td>
</tr>
<tr>
<td><strong>Reply from incoming interface</strong></td>
</tr>
<tr>
<td>When tunnel is initiated from remote site, reply from the same incoming interface when applicable (IKE and RDP sessions).</td>
</tr>
<tr>
<td><strong>Successful key exchange tracking</strong></td>
</tr>
<tr>
<td>Indicates how to log when there is a successful key exchange: Log, don’t log, or alert.</td>
</tr>
<tr>
<td><strong>Use cluster IP address for IKE</strong></td>
</tr>
<tr>
<td>Indicates if IKE is performed using cluster IP address (when applicable).</td>
</tr>
<tr>
<td><strong>VPN tunnel sharing</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

## VoIP

<table>
<thead>
<tr>
<th>VoIP Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accept MGCP connections to registered ports</strong></td>
<td></td>
</tr>
<tr>
<td>Indicates if deep inspection over MGCP traffic will automatically accept MGCP connections to registered ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Accept SIP connections to registered ports</strong></td>
<td></td>
</tr>
<tr>
<td>Indicates if deep inspection over SIP traffic will automatically accept SIP connections to registered ports.</td>
<td></td>
</tr>
</tbody>
</table>
### Web Interface Settings and Customizations

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

### Wireless Networks

<table>
<thead>
<tr>
<th>Wireless Networks Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antenna control</td>
<td>Lets you select a single wireless antenna to use (<strong>left</strong> or <strong>right</strong>).</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>Lets you set an increased throughput through the wireless access point. Note that an increased throughput will affect the error rate.</td>
</tr>
<tr>
<td>Transmitter power</td>
<td>Lets you set different percentages for the transmitter power. Lower power can help reduce interference to nearby access points.</td>
</tr>
</tbody>
</table>
Managing the Access Policy

This section describes how to set up and manage your Check Point 600 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 Check Point 600 Appliance in regards to incoming, internal, and outgoing traffic.

The Access Policy includes:

- **Firewall Policy** - Defines how to inspect packets.
- **Applications & 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 will be shown as automatically generated system rules at the bottom of the Rule Base. It is recommended to 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.
To set specified outgoing services in a standard Firewall policy:
1. When the Access Policy control level is set to **Standard**, click the **all services** link.
2. Select **Block all outgoing services except the following**.
3. Select the checkboxes of the 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 have been configured, it shows the number of rules that has been added. Click on the **manual rules** link to see them in the Access Policy.

You can also see how many servers are defined in the appliance by clicking the **Servers** link. If you have no servers configured, you can click the **Add a server** link to easily 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.

Applications & URL Filtering

The Applications & URL Filtering section lets you define how to handle applications and URL categories on traffic from your organization to the Internet.

Applications and 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 Applications & URL Filtering control. It is recommended by default to block browsing to security risk categories and applications. But you can also configure additional applications and categories to block by default according to your company’s policy. In addition, you can also choose 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. Choose 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:
   - **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 600 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. Once this is configured, you will be able to 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**

You can log blocked and accepted traffic. By default, blocked traffic is logged. You can clear this setting if necessary. These settings apply to all traffic block or accepted by the default Firewall and Applications & URL Filtering policies.

**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 and 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 according to 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 for accessing 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 for accessing the Internet outside your organization. Commonly the policy here is to allow the basic traffic, but you can block applications and URLs according to your company's discretion. In the **Access Policy > Firewall Blade Control** page you can configure the default policy for blocking 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, it is recommended to 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 for accessing 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.

  - **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.

<table>
<thead>
<tr>
<th>Rule Base Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Firewall rule base.</td>
</tr>
<tr>
<td>Source</td>
<td>IP address, network object, or user group that initiates the connection.</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address or network object that is the target of the connection.</td>
</tr>
<tr>
<td>Application</td>
<td>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 Applications &amp; URLs (&quot;Defining Custom Applications &amp; URLs&quot; on page 110). This field is only shown in the Outgoing access to the Internet section.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of network service that is accepted or blocked.</td>
</tr>
</tbody>
</table>
Appliance Configuration

<table>
<thead>
<tr>
<th>Rule Base Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Firewall action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td></td>
<td>For outgoing traffic rules, you can use the <strong>Customize messages</strong> option</td>
</tr>
<tr>
<td></td>
<td>to configure “Ask” or “Inform” actions in addition to the regular Block or</td>
</tr>
<tr>
<td></td>
<td>Accept actions. The messages shown can be set for these action types:</td>
</tr>
<tr>
<td></td>
<td>Accept and Inform, Block and Inform, or Ask. Ask action lets the end user</td>
</tr>
<tr>
<td></td>
<td>decide if this traffic is for work purposes or personal. See the **Customize</td>
</tr>
<tr>
<td></td>
<td>messages** section below. Users will be redirected to a portal that shows a</td>
</tr>
<tr>
<td></td>
<td>message or question. If a time range is set for the rule, a clock icon is</td>
</tr>
<tr>
<td></td>
<td>shown.</td>
</tr>
<tr>
<td>Log</td>
<td>The tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Comment / Auto generated rule</td>
<td>Details shown immediately below the above fields for:</td>
</tr>
<tr>
<td></td>
<td>• Comments you enter when you create a rule.</td>
</tr>
<tr>
<td></td>
<td>• Rules that the system automatically generates. You can click the object</td>
</tr>
<tr>
<td></td>
<td>name link in the comment to open its configuration tab.</td>
</tr>
</tbody>
</table>

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.

- Using this action for traffic to uncategorized URLs, can also give security against malware that managed to be installed inside your organization as a common use case for such malware is to access uncategorized URLs and it 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**.
3. 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.
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.

**Note** - The Application field is relevant only for outgoing rules.

In the **Source** field, you can optionally choose 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...
Appliance Configuration

Active Directory. For more details, see the Access Policy > User Awareness Blade Control page.

5. 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.

6. To limit the rule to a certain time range, select **Apply only during this time** and select the start and end times.

7. In outgoing rules, to limit the download traffic rate, select **Limit download traffic of applications to** and enter the **Kpbs** rate.

8. In outgoing rules, to limit the upload traffic rate, select **Limit upload traffic of applications to** and enter the **Kpbs** rate.

9. In incoming rules, to match only for encrypted VPN traffic, select **Match only for encrypted traffic**.

10. 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 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.

**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:

<table>
<thead>
<tr>
<th>Rule base action</th>
<th>Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept and Inform</td>
<td>Shows an informative message to users. Users can continue to the application or cancel the request.</td>
</tr>
<tr>
<td>Block and Inform</td>
<td>Shows a message to users and blocks the application request.</td>
</tr>
<tr>
<td>Ask</td>
<td>Shows a message to users and asks them if they want to continue with the request or not. See above for more details.</td>
</tr>
</tbody>
</table>

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 will 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 Server Objects**

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 Computers 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 Computers 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.
- Remote VPN sites - Networks defined behind gateways to remote VPN sites.

- Manually configure access policy to this server - Select this option when you want to define an access policy using only manual access rules.

2. If you do not want the server to be accessible to pings, clear the Allow access to server using 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)

1. Select the relevant option:
   - Hide Behind Gateway (Port Forwarding) - 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.
   - Static NAT - 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.
     - Hide outgoing traffic from the server behind this IP address - Select this checkbox to create an outgoing NAT rule where the original source is the server (internal IP address) and the translated source is the server’s static IP address.
   - No NAT - This option is only relevant if the Hide internal networks behind the Gateway’s external IP address option in the Access Policy > NAT Control page is set to OFF (see above for details). It means there are no NAT rules on the server.

2. When you have multiple internal servers that use the same port, select Redirect from port and enter a different port number that will be used when accessing this server from the Internet. Traffic to the server on the port you entered will be forwarded to the server’s port.

3. 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.

   Note that this option is important for traffic originating from internal sources, however, currently, sources of all traffic to the server will be translated and hidden behind the gateway’s IP address.

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.
If NAT was defined for the server, automatically generated forwarding rules are added to the Access Policy > Firewall NAT page.

To change the Remote Access port settings:

If there is a conflict between the default remote access port (port 443) and a server defined with the same port, a message is shown. You must change the default remote access port if you want the server to use port 443.

1. Click the Change Remote Access 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.

Note - This page is available from the Firewall and NAT sections on the Access Policy tab.

Defining NAT

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 don’t 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, turning off the hide NAT feature will 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:
   - Hide Behind Gateway (Port Forwarding) - 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.
   - Static NAT - 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.

- **Hide outgoing traffic from the server behind this IP address** - Select this checkbox to create an outgoing NAT rule where the original source is the server [internal IP address] and the translated source is the server’s static IP address.

- **No NAT** - This option is only relevant if the **Hide internal networks behind the Gateway’s external IP address** option in the Access Policy > NAT Control page is set to OFF (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 will be used when accessing this server from the Internet. Traffic to the server on the port you entered will be 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 will not apply to them. However, they will apply even when Hide NAT is activated.

These are the fields that manage the NAT rules.

<table>
<thead>
<tr>
<th>Rule Base Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Source</td>
<td>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.</td>
</tr>
<tr>
<td>Original Destination</td>
<td>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.</td>
</tr>
<tr>
<td>Original Service</td>
<td>The original service used for the connections to translate.</td>
</tr>
<tr>
<td>Translated Source</td>
<td>The network object or network group object that is the new source to which the original source is translated.</td>
</tr>
<tr>
<td>Translated Destination</td>
<td>The network object or network group object that is the new destination to which the original destination is translated.</td>
</tr>
</tbody>
</table>
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 will do 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.).
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.

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 for getting user identities, for logging and configuration purposes.

User Awareness lets you configure Check Point 600 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

Check Point 600 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. Check Point 600 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. It is possible to 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 accessing only specific network resources or the Internet to avoid the overhead required from end users when identifying themselves. For traffic that is not HTTP based, it is also possible to configure that all unidentified users will be blocked from accessing the configured resources or Internet until they identify themselves first using 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 will be overridden in the next synchronization between the gateway and Cloud Services.
There is a User Awareness configuration wizard that helps you enable and configure the blade. You can use the configuration wizard to 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**.
3. For Active Directory Queries:
   a) If you have an existing Active Directory server, click **Use existing Active Directory servers**.
   b) To define a new Active Directory server, click **Define a new Active Directory server**.
      (i) Enter the **Domain**, **IP address**, **User name**, **Password**, and **User DN**. For the User DN, click **Discover** for automatic discovery of the DN of the object that represents that user or enter the user DN manually.
      (ii) You can optionally select, **Use user groups from specific branch only** if you want to use only part of the user database defined in the Active Directory. In **Branch**, enter the branch name.
   c) Click **Next**.
4. For Browser-Based Authentication:
   a) 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.
   b) Select if unidentified users should be 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.
   c) 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.
5. 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 will be 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 Check Point 600 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 Quality of Service (QoS) - Bandwidth Control 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. A more advanced policy can be configured 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 choose **Download** and/or **Upload** to determine where the limit will be 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 choose 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 the 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 regarding 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. Without setting 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.
The QoS Policy Rule Base can be viewed on this page. For each rule, you see these fields:

<table>
<thead>
<tr>
<th>Rule Base Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the QoS policy.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that starts the connection.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that completes the connection.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of network service for which bandwidth is adjusted according to weight, limit, and guarantee.</td>
</tr>
<tr>
<td>Guarantee/Limit</td>
<td>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 will be prioritized accordingly.</td>
</tr>
<tr>
<td>Weight</td>
<td>The unit used to divide available bandwidth once traffic has exceeded the maximum bandwidth configured for the Internet connection. See below.</td>
</tr>
<tr>
<td>Track</td>
<td>The tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that shows a comment if you entered one. For system generated rules of the default policy a Note is shown.</td>
</tr>
</tbody>
</table>

**Weight**

QoS divides available bandwidth across the QoS policy rules according to *weight*. Using weights instead of specific percentages is a flexible way for the QoS engine to allocate bandwidth if the maximum bandwidth has been exceeded according to the specific 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 is not using all of its bandwidth, the leftover bandwidth is divided with the remaining rules, in accordance with their relative weights. In the above example, if only one Web and one FTP connection are active and they are competing, the Web connection will receive 75% (30/40) of the leftover bandwidth, and the FTP connection will receive 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection will receive 100% of the bandwidth.

In the **Weight** field, enter a value that indicates 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 either choose for a specific 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 will show "encrypted" if chosen.

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 began during this time range are inspected.

6. DiffServ Mark is a way to mark connections so a third party will handle it. To mark packets that will be given priority on the public network according to 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:

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.
Defining Custom 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 blade 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 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:
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 Threat Prevention

This section describes how to set up and manage the Intrusion Prevention System (IPS), Anti-Virus, and Anti-Spam blades.

Configuring the Threat Prevention Blade

In the **Threat Prevention > Threat Prevention Blade Control** page you can activate:

- Intrusion Prevention System (IPS) to block potentially malicious attempts to exploit known vulnerabilities in files and network protocols.
- Anti-Virus to block potentially malicious files that are infected with viruses.
- Anti-Bot to detect bots, prevent communication between the bot and its Command & Control center, and give threat visibility. A *bot* is malicious software that can infect your computer with malware. A bot infected computer 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 opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

**Note** - Anti-Bot and Anti-Virus are configured in the same place.

On this page you can activate the blades to prevent such attacks/infections or set them to detect-mode only. The top of the page shows the number of infected hosts. For more information about them, click **More details**. The number of Anti-Bot and Anti-Virus malwares and the number of IPS attacks is shown next to the On/Off switch for each blade. You can also use logs to understand if your system is experiencing attack attempts. See the **Logs & Monitoring > Security Logs** page.

Check Point uses a large database of signature based protections and this page lets you use a default recommended policy. You can edit the policies and configure an IPS policy and Anti-Virus and Anti-Bot policy that will maximize connectivity and security in your environment. Each policy represents a different profile of protections according to their severity, performance impact, and confidence level.

To enable/disable the IPS, Anti-Bot, or Anti-Virus 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.

**IPS**

To configure the IPS Policy:

1. In the **IPS** section, click **Edit**.
2. Select one of these options:
   - **Strict** - A protection profile that focuses on security.
- **Typical** - A protection profile most suitable for small/medium sized businesses that gives the best mixture of security and performance. This is the default option.
- **Custom** - A protection profile that you can manually define.

**To configure a Custom IPS Policy:**

Each protection has three defining parameters whose levels are defined by the Check Point IPS service: **Severity** (how critical is the potential threat), **confidence-level** (protections with a lower confidence-level provide protection against a wide variety of attack vectors at the risk of more false-positives), and **performance impact** (how the appliance’s performance is affected by activating these protections).

In addition, protections are divided into those that protect servers and those that protect clients.

1. Select which type of protections to activate:
   - **Client protections**
   - **Server protections** - If your environment does not include any servers within the organization that are accessible from the Internet you might consider clearing this option.

2. Select which protections should be deactivated according to each of the protections parameters according to one or more of these levels:
   - **Disable protections with severity X or below** - You can decide the level of severity under which protections will not be activated. Choose between low, medium, high, critical.
   - **Disable protections with confidence-level X or below** - You can decide the level of confidence-level under which protections will not be activated. Choose between low, medium-low, medium, medium-high, and high.
   - **Disable protections with performance impact X or above** - You can decide the level of performance impact over which protections will not be activated. Choose between very low, low, medium, and high.

3. Select **Disable Protocol Anomalies** if you want to disable protections against protocol anomalies.

   Most of the IPS protections protect against malicious attempts to exploit vulnerabilities but there are two other types of protections:
   - **Protocol anomalies** - Protections of this type detect and block irregularities in protocols. Such irregularities are not necessarily indicative of a malicious attempt but many malicious attempts use such irregularities.
   - **Protocol control** - Protections of this type detect and block usage of protocol or files. They let you block those specific protocols or files according to your organization’s policy. This is a form of access control within the IPS blade. Protocol control protections are not activated automatically by the IPS policy. You can view them and manually activate each one according to your organization’s policy through the Threat Prevention > IPS Protections page.

4. Alternatively, you can set all the policy parameters to be the same as the built in strict or typical profiles and then make manual adjustments using the steps above. Choose **Load default settings** and the appropriate profile to do so.

5. Click **Apply**.

**Anti-Bot**

The Anti-Bot policy is based on a set of activated protections and instructions for how to handle traffic inspection that matches activated protections. **Protections** help manage the threats against
your network. For more information about protections, see the Check Point ThreatWiki. You can access it from a link on the Threat Prevention > Engine Settings page.

Set protection activation according to these protection criteria:

• Confidence level - The confidence level is how confident the Software Blade is that recognized attacks are actually bot traffic. Some attack types are more subtle than others and legitimate traffic can sometimes be mistakenly recognized as a threat. The confidence level value shows how well protections can correctly recognize a specified attack. The higher the Confidence level of a protection, the more confident Check Point is that recognized attacks are indeed attacks. Lower Confidence levels indicate that some legitimate traffic may be identified as an attack.

• Protection action - The action enforced on the matching traffic. Notification for these actions are set according to the defined tracking option (none, logged, or logged with an alert).
  • Prevent - Blocks identified bot traffic from passing through the gateway.
  • Detect - Allows identified bot traffic to pass through the gateway, but detects and logs it.
  • Ask - Traffic is blocked until the user confirms that it is allowed. To configure the Anti-Bot user message, see the Threat Prevention > Engine Settings page.
  • Inactive - The protection is deactivated.

• Performance impact - Indicates the impact level on Security Gateway performance

Anti-Virus

The Anti-Virus policy is also based on a set of activated protections and instructions for how to handle traffic inspection that matches activated protections.

Set protection activation according to these protection criteria:

• Confidence level - The confidence level is how confident the Software Blade is that recognized attacks are actually a virus. Some attack types are more subtle than others and legitimate traffic can sometimes be mistakenly recognized as a threat. The confidence level value shows how well protections can correctly recognize a specified attack. The higher the Confidence level of a protection, the more confident Check Point is that recognized attacks are indeed attacks. Lower Confidence levels indicate that some legitimate traffic may be identified as an attack.

• Protection action - The action enforced on the matching traffic. Notification for these actions are set according to the defined tracking option (none, logged, or logged with an alert).
  • Prevent - Blocks identified virus traffic from passing through the gateway.
  • Detect - Allows identified virus traffic to pass through the gateway, but detects it and logs it.
  • Ask - Traffic is blocked until the user confirms that it is allowed. To customize the Anti-Virus user message, see the Threat Prevention > Engine Settings page.
  • Inactive - The protection is deactivated.

• Performance impact - Indicates the impact level on Security Gateway performance

To configure the Anti-Bot or Anti-Virus Policy:

1. In the Anti-Bot or Anti-Virus section, click Edit.

2. For each confidence level (High confidence, Medium confidence, and Low confidence), select the applicable action from the list (prevent, detect, ask, or inactive).
3. In Performance impact, select the allowed impact level (Low, Medium or lower, or High or lower).
4. In Tracking options, select one of these options:
   - None - Do not log.
   - Log - Create a log.
   - Alert - Log with an alert.
5. If it is necessary to restore the policy default values, click Reset to defaults.

Click Apply.

Updates

As service based blades, it is necessary to schedule the interval at which updates are downloaded.

To schedule updates:
1. Click the Schedule link at the bottom of the page. You can also hover over the icon next to the update status and select the link from there.
2. Choose 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 the Recurrence time frame:
   - 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.

To toggle between block and detect-only modes:
1. Clear or select the applicable checkbox:
   - For IPS - Detect-only mode (IDS)
   - For Anti-Bot or Anti-Virus - Detect-only mode
2. Click Apply.

In detect-only mode, only logs will be shown and the blades will not block any traffic.

To import an IPS update offline:

On rare occasions, there are organizations where the gateway is without Internet connectivity, but IPS is still required. Please contact Check Point Support to receive an offline IPS update package.

1. Click import manually at the bottom of the page.
2. Browse to the offline package file you received from Check Point Support.
3. Click Import.

Configuring IPS 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 will not inspect.
IPS Exceptions

To add a new IPS exception rule:
1. In the IPS Exceptions section, click New.
2. Click the links in the rule summary or the table cells to select network objects or options that fill out the exception rule fields.
   - Protection - Select either All IPS protections or a specific IPS protection from the list.
   - Source - Network object that initiates the connection.
   - Destination - Network object that is the target of the connection.
   - Service/Port - Type of network service. Making an exception for a specific protection on a specific service/port might cause the protection to be ineffective.
3. Optionally add a comment in the Write a comment field.
4. Click Apply.

Malware Exceptions

Anti-Bot and Anti-Virus exception rules include a Scope parameter. Threat Prevention inspects traffic to and/or from all objects specified in the Scope, even when the specified object did not open the connection. This is an important difference from the Source object in Firewall rules, which defines the object that opens a connection.

For example, when a Scope includes a Network Object named MyWebServer. Threat Prevention inspects all files sent to and from MyWebServer (both directions) for malware threats, even if MyWebServer did not open the connection.

Scope objects can be:
- Network objects, such as Security Gateways, clusters, servers, networks
- Network object groups
- IP address ranges
- Local users

To add a new malware exception rule:
1. In the Malware Exceptions section, click New.
2. 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.
   - Protection - Select Any malware, Any Anti-Bot, or Any Anti-Virus. You cannot set a specific protection here. To set an exception for a specified protection, see the Threat Prevention > Infected Hosts page.
   - 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. Optionally add a comment in the Write a comment field.
4. Click Apply.

Files and URLs Whitelists
You can set specified files and URLs that the Anti-Bot and Anti-Virus 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.

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 edit or delete an exception rule:
1. Select the relevant rule.
2. Click Edit or Delete.

Viewing Infected Hosts
In the Infected Hosts page you can see information about infected hosts 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 host or server.

The Infected Hosts table shows this information for each entry:
• Icon - Shows icons for the different classifications of infected hosts and servers:

<table>
<thead>
<tr>
<th>Description</th>
<th>Host Icon</th>
<th>Server Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infected host or server - When the Anti-Bot blade detects suspicious</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>communication between the host or server and an external Command &amp; Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>center due to a specified triggered protection.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Possibly infected host or server - When the Anti-Virus blade detects an   | ![Icon]   | ![Icon]     |
| activity that may result in host or server infection. For example:         |           |             |
| • When browsing to an infected or a potentially unsafe Internet site,      |           |             |
| there is a possibility that malware was installed.                        |           |             |
| • When downloading 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 600 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 host or server in the last month. If there
  is a large amount of records, the time frame may be shorter.

To filter the infected hosts 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 hosts or servers classified as possibly infected.
   • Infected only - Shows only hosts or servers classified as infected.
   • High and above severity only - Shows hosts 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.
   • 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. Optionally 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 Protections List

In the Threat Prevention > IPS Protections List page you can view the signature based protections that the appliance has downloaded as part of the IPS service blade. You can see which of the protections are activated according to the policy you configured in the Threat Prevention > IPS Blade Control page.

You can see the details of each protection and also configure a manual override for individual protections’ action, and tracking options.

You can either search for a specific protection by entering a name in the filter box or by scrolling the pages using the next and previous page buttons at the bottom of the page.

These are the fields that manage IPS exceptions:

- **Protection** - Name of IPS protection
- **Protection Type** - Shows if the protection applies to servers, clients or both
- **Category** - Category of the protection
- **Action** - Firewall action for this protection, the word overridden indicates a manual override
- **Severity** - Probable severity of a successful attack to your environment
- **Confidence** - How confident IPS is that recognized attacks are actually undesirable traffic
- **Performance** - How much this protection and its resources affect gateway or server performance

To manually override a specific protection’s configuration:

1. Select a protection from the list.
2. Click Edit.

   The Protection Settings window opens.
3. Select the Override IPS policy action checkbox and select the relevant option:
   - Prevent
   - Detect
   - Inactive

   The protection’s action will not be affected anymore by the IPS policy configuration.
4. Select a Track option for the protection.
5. Click Apply.
Advanced IPS Configuration

In the Threat Prevention > Threat Prevention Engine Settings page you can configure advanced configuration settings for the Anti-Virus, Anti-Bot, and IPS engines.

Note - Many of the configurations below are advanced and should only be used by experienced administrators.

Anti-Virus

To configure the Anti-Virus settings:

1. Select one of the protected scope options:
   - Scan incoming files from X interfaces - These are the options for X:
     - External and DMZ - Files originating from external and the DMZ interfaces are inspected.
     - External - Files originating from external interfaces are inspected.
     - All - Files transferred between all interfaces are inspected.
   - Scan both incoming and outgoing files - Files originating 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 and POP3)
   - FTP

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.
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 specific 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.

Anti-Virus and Anti-Bot 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Anti-Virus Notification</th>
<th>Anti-Bot Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>Shows a message to users and asks them if they want to continue to access a site or download a file that was found to be classified as malicious.</td>
<td>Shows a message to users and notifies them that their computer is trying to access a malicious server.</td>
</tr>
<tr>
<td>Block</td>
<td>Shows a message to users and blocks the site.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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) - 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 for entering 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 or Anti-Bot 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**.

**IPS**

**To change the protection scope of the IPS engine:**

Select one of the options:

• **Protect internal hosts only** - The IPS engine will only protect against attacks targeted on clients and servers that are inside the organization. The IPS engine does not waste resources on protecting hosts outside your organization.

• **Perform IPS inspection on all traffic** - This option is less recommended as it consumes more resources.

**To configure the IPS engine to bypass mode when the appliance is under heavy load:**

1. Activate the feature by selecting the **Bypass under load** checkbox.

2. Click **Configure** to choose 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 manner, when under load, the IPS engine does not toggle between modes too frequently.

3. In **Bypass under load tracking**, configure tracking options for this feature by selecting what type of log to issue.

**To change the tracking setting:**

Select the relevant **Event tracking** option - **None**, **Log** or **Alert** (shown as a highly important log).
Configuring the Anti-Spam Blade

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 will appear and the blade will 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 will block regardless of its own classification.

Blocking or allowing 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 activate the device’s ability to establish secure encrypted connections between home desktops and laptops and the organization through the Internet.

Remote access requires the definition of users in the system with credentials and permissions for it can be set for specified users. It also requires the appliance to be accessible from the Internet.

There are numerous supported methods of remote access connection:
- Installing a VPN client on the home desktops or laptops.
- Browsing from home devices (using secure HTTPS) to the appliance and downloading a thin client when necessary. This method is known as SSL Network Extender.

It is highly recommended to work with remote access after configuring DDNS or a static IP Internet connection on the appliance. If you are not using a static IP, your appliance’s IP address may vary according to your Internet Service Provider. DDNS lets home users connect to the organization by name and not IP address that may 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 into the organization 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**.

To configure VPN remote access methods:

By default, Check Point VPN clients is enabled.

1. To connect through the Check Point Mobile VPN client (for smartphones and tablets), select the **Mobile client** checkbox.
2. To connect through **SSL VPN**, select the checkbox.
3. To connect through **Windows VPN client**, select the checkbox. Click the **L2TP Pre-Shared Key** link to enter the pre-shared key and click **OK**.
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**, this bookmark is shown to all users.
   - **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 **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**

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 there is a conflict between the default remote access port (port 443) and a server using the same port, a message is shown. 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, 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, enter the necessary details.
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 has been defined, you will be prompted to configure one. For more information on configuring Active Directory see **VPN > Authentication Servers**.
3. Once an Active Directory has been defined, you will 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 will 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 has been defined, you will be prompted to configure one.
3. Select or clear the **Enable RADIUS authentication for remote access users** checkbox.
4. When selected, choose which users will be granted 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:
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.

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 600 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 600 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 remote access users** checkbox.
3. When selected, choose which users will be granted 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.

Once 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 will 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 will be able to 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.

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.
   The Active Directory is deleted.
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 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 will be 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 domain 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 will 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 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**.

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 > Firewall Policy** 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 information on common configuration of site to site VPN, see VPN > Site to Site Blade Control.

When adding a new site you configure:

- Remote site details - Name, connection type, authentication method (preshared secret or certificate), and the Remote Site Encryption Domain
- Encryption settings

You can also configure advanced settings for the encryption method and certificate matching.

To add a new VPN site:

1. Click New.
   The New VPN Site window opens.
2. Fill in the fields in the Remote Site tab:
   - Site name
   - Connection type - Select the relevant type:
     - Host name or IP address - Select the relevant IP address or Host name option and enter the details. If you select IP address, and it is necessary to configure a static NAT IP address that the remote site is translated into, select Behind static NAT and enter the IP address.
     - High Availability or Load Sharing - Configure a list of IP addresses to create redundancy for backup purposes between them 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, one of the IP addresses can be configured as a primary IP address. When you select this option, you must configure a probing method on the Advanced tab. The probing method monitors which of the multiple 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.
Select one of the authentication methods. It must match the authentication configured when configured 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. You cannot use these characters when you enter a shared secret [ ] ‘-|`”

- **Certificate** - The gateway uses its own certificate to authenticate itself. For more information, see [VPN > Internal Certificate](#).

Select the remote site encryption domain. Configure here the conditions that when matched traffic will be encrypted and sent to this remote site.

- **Define remote network topology manually** - Traffic is encrypted when the destination is included in the list below this option. Click Select to select the networks in the list below that represent the remote site’s internal networks. Click New if you haven’t created such network objects already.

- **Route all traffic through this site** - All traffic is encrypted and sent to this remote site. You cannot configure more than one remote site with this option.

- **Encrypt according to routing table** - If you are using dynamic routing, encrypts traffic according to source or service and destination. You are required to create a virtual tunnel interface (VTI) in the [Device > Local Network](#) page and associate it with this remote site. You can then create routing rules using this VTI. Traffic that matches these routing rules will be 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.

3. Optionally you can change the default settings in the Encryption tab. There are built-in encryption settings’ groups that can be used and only need to match in both 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** - Optionally, you can select this option to manually decide which encryption method should be used.

4. Optionally you can change the default settings in the Advanced tab sections:

   **Settings**
   - Configure if the remote site is a Check Point gateway. This also enables configuration of permanent tunnels.
   - You can select to disable NAT for this site which is usually useful when your internal network contains a server.
   - There are two modes for IKE negotiation - main mode or aggressive mode. For IKE negotiation, main mode uses six packets and aggressive mode uses three packets. It is recommended to use main mode as it is more secure. By default, Enable aggressive mode is not selected and main mode is used. Enable aggressive mode only if it is necessary and the other side of the VPN tunnel does not support main mode.
- **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 preshared secret, the gateway must identify itself. Enter the **Gateway ID** to use for matching and in **Type** select domain name or user name.

- **Enable VPN access by peer identifier** - It is important to configure the peer identifier when you use the **Only remote site initiates VPN** connection type and the authentication method is preshared secret. In **Peer ID** enter the identifier and in **Type** select domain name or user name.

**Encryption Method**

Select the IKE version you want the appliance to support.

**Certificate Matching**

- When using preshared secret this section is not relevant. When selecting 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 known Trusted CA or a specific Trusted CA. You can also configure additional matching criteria on the certificate.

**Probing Method**

This section is shown when High Availability or Load Sharing is selected as the connection type. When the remote site has multiple IP addresses for VPN traffic, the correct address for VPN is discovered through one of the following 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.

5. Click **Apply**.
   
   An initial tunnel test will begin with the remote site. If you haven’t configured it yet, click **Skip**. The VPN site is added to the table.

**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.
   The VPN site is disabled or enabled accordingly.

Viewing VPN Community Details

Note - This page is applicable only if Cloud Services is turned on for your appliance.

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 regarding the fields in the site details tabs, see VPN Sites.

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Host name or IP address of the tunnel’s source gateway.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Name of the VPN site name.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Host name or IP address of the tunnel’s destination gateway.</td>
</tr>
<tr>
<td>Community Name</td>
<td>If the gateways are part of a community configured by Cloud Services, this column shows the community name with which the tunnel is associated.</td>
</tr>
<tr>
<td>Status</td>
<td>VPN tunnel status indication.</td>
</tr>
</tbody>
</table>

To filter the list:

In the **Type to filter** box, enter the filter criteria.

The list is filtered accordingly.

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. 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 below Configuring the Appliance’s Outgoing Interfaces for VPN usage.

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 choose the applicable checkboxes.
4. Click New if the existing list does not contain the necessary networks required. For information on creating 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, using the Link Selection mechanisms, the administrator can choose which source IP addresses are used for VPN traffic.

The default configuration for choosing an outgoing interface and source IP address is for the device to determine them automatically. Alternatively, it is possible to change the default settings and choose other means of determining:
- 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 according to 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 initiating or responding to VPN traffic. This IP address will normally be 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.
Managing Trusted CAs

In the VPN > Certificates Trusted CAs page you can add CAs used by remote sites’ certificates to enable certificate based site to site VPN. A certificate shown by the remote site must be signed by a CA that is trusted by the appliance.

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 using certificate based site to site VPN with only one remote site, it is recommended to export each site’s Internal CA and add it to the other site’s Trusted CA list.

When using certificate based site to site VPN with multiple remote sites, in a mesh configuration, it is recommended 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 either 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, 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 will 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 clicking OK, in the file browsing window, the file is uploaded and if it is correctly formatted, it will be signed by the Internal CA and the Download button will become 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
In the VPN > Certificates Installed Certificates page you can create and manage appliance certificates or upload a PKCS#12 (.p12, .pfx) file.

The installed certificates are used in site-to-site VPN authentication.

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 that if you turn Cloud Services off, the Cloud Services Provider certificate is removed.

These are the steps for creating 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:
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 that you cannot edit the request once it has been created.

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 PKCS#12 (.p12, .pfx) file:

1. Click **Upload P12 Certificate**.
2. Browse to the PKCS#12 file (*.p12 or *.pfx).
3. Edit the **Certificate name** if necessary.
4. Enter the certificate **password**.
5. Click **Apply**.

### Managing Internal Certificates

In the **VPN > Certificates Internal Certificate** page you can view details of the internal certificate used by the appliance in site to site VPN. 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.

When creating certificate based site to site VPN, once 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. This page lets you do that.

To avoid constant reinitialization it is recommended to use the DDNS feature. See **Device > DDNS**. Once DDNS is configured, it is only necessary to reinitialize the certificate once. Changes in the DDNS feature configuration, will automatically by default reinitialize certificates.

To reinitialize certificates:

1. Click **Reinitialize Certificates**. The Reinitialize Certificates window is shown.
2. 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 may choose to 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. Click **Apply**.

To export 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 clicking **OK**, in the file browsing window, the file is uploaded and if it is correctly formatted, it will be signed by the Internal CA and the **Download** button will become 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

See Working with User Awareness (on page 104).

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: { } [ ] ` ~ | ' “ # +
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. 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. Click Apply.
   The group is added to the table on the page.

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.
4. The user or group is deleted.

Configuring Local System Administrators

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 600 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 600 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.
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 remote access users checkbox.
3. When selected, choose which users will be granted 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.

Once 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 will 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 will be able to 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.
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.
   
   The Active Directory is deleted.

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

---

**Managing Applications and 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 blade 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 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:

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. Usually using 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
- Choose this option if it is necessary to represent a specific option within the TCP protocol.

### UDP
- Choose this option if it is necessary to represent a specific option within the UDP protocol.

### ICMP
- Choose this option if it is necessary to represent a specific option within the ICMP protocol. Note that this is an advanced option.
- Choose 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 will be 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 will 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 will be 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 Check Point 600 Appliance about a connection so that the connection will only be 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 type, 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. Such system services cannot be deleted. When editing them the ports which you configure decide when the deep inspection will occur 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.

Defining service groups is the recommended way to configure the security policy. If the security policy is configured using groups and not specific objects, then 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 will automatically apply to them.

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 choose 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 type, 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 choosing this option will affect 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 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 Computers 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 will not distribute the configured IP range to anyone.

6. Click **Apply**.

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 type, 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.

Defining groups for network objects is the recommended way to configure the security policy. If the security policy is configured using groups and not specific objects, then 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 will automatically apply to them.

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 type, 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 ejecting an SD card, make sure to unmount it. Select Options > Eject SD card safely.
To delete logs from local log storage:

   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 either the external SD card (if inserted) or from the local logs storage. Logs are not deleted from the remote logs server.

Viewing System Logs

The Logs & Monitoring > System Logs page shows up to 500 systems logs 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 system logs types:

- **Info** - Informative logs such as policy change information, administrator login details, and DHCP requests.
- **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 system logs 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 system logs 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 when necessary for additional logging storage.

*Note* - You cannot configure external log servers when Cloud Services is turned on.

### External Security Log Server

You can use an external Check Point log server that is managed by a Security Management Server for storing additional logs.

Before you can configure an external Check Point log server from this page in the WebUI, make sure to do these steps:

- Identify the Log Server you want to send logs to
- Identify the Security Management Server that manages the Log Server
- Open SmartDashboard on this Security Management Server
- Run the Security Gateway wizard to define and create a Security Gateway object that represents this Check Point 600 Appliance with the these details:
  - In the *General Properties* window, select:
    - **Gateway platform** - Check Point 600 Appliance
    - **Gateway IP address** - Dynamic IP address
  - In the *Trusted Communication* window, from **Gateway Identifier** select **MAC address** or **First to connect**.

For more information on using the Security Gateway wizard for object definition, see the *Check Point Check Point 600 Appliance Centrally Managed Administration Guide*.  

• Install the database on the Security Management Server and other related objects.

To configure an external security log server:


2. Enter the **Management Server IP address**. This IP address is used only for establishing trusted communication between the Check Point 600 Appliance and the Security Management Server.

3. In **SIC name**, enter the SIC name of the log server object that was defined in SmartDashboard. You can get this name by using one of these methods:
   - Open GuiDBedit on the Security Management Server - From the Tables tab, expand Table > Network Objects > locate the log server object > sic_name.
   - Run this CLI command on the log server (using SSH or running the command on the physical machine):
     ```bash
     $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. Select the **Log server uses different IP address** checkbox if the log server is not located on the Security Management Server.

6. Enter the **Log server IP address**.

7. Click **Connect**. A notification message is shown.

   **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 SmartDashboard. If you do not reinitialize SIC in SmartDashboard, connectivity to the log server can fail.
External System Log Server Configuration (for system logs)

To configure an external System Log server:
1. Click **Configure** next to the External System Log Server notification. The External System Log Server window opens.
2. Select the **Send system logs to an external System Log Server** checkbox.
3. Enter the **IP address**.
4. Enter the **Port**.
5. Click **Apply**.

To edit the external System Log server:
1. Click the server’s IP address.
2. Edit the necessary information.
3. Click **Apply**.

To delete the external System Log server:
Click **Delete**.
The server is deleted.

Managing Active Computers in Internal Networks
See Managing Active Computers in Internal Networks (on page 31).

Viewing Infected Hosts
In the **Infected Hosts** page you can see information about infected hosts 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 host or server.

The Infected Hosts table shows this information for each entry:
- **Icon** - Shows icons for the different classifications of infected hosts and servers:

<table>
<thead>
<tr>
<th>Description</th>
<th>Host Icon</th>
<th>Server Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infected host or server - When the Anti-Bot blade detects suspicious communication between the host or server and an external Command &amp; Control center due to a specified triggered protection.</td>
<td><img src="image" alt="Host Icon" /></td>
<td><img src="image" alt="Server Icon" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Possibly infected host or server - When the Anti-Virus blade detects an activity that <em>may</em> result in host or server infection. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- When browsing to an infected or a potentially unsafe Internet site, there is a possibility that malware was installed.</td>
</tr>
<tr>
<td>- When downloading an infected file, there is a possibility that the file was opened or triggered and infected the host or server.</td>
</tr>
</tbody>
</table>

| **Object name** - Shows the object name if the host or server was configured as a network object. |
| **IP/MAC address** |

Check Point 600 Appliance Administration Guide R77.20.10 | 161
- Device/User Name - Shows a device or user name if the information is available to the Check Point 600 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 host or server in the last month. If there is a large amount of records, the time frame may be shorter.

To filter the infected hosts 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 hosts or servers classified as possibly infected.
   - **Infected only** - Shows only hosts or servers classified as infected.
   - **High and above severity only** - Shows hosts 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.
   - **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. Optionally 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 VPN Tunnels**
See Viewing VPN Tunnels (on page 138).

**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 accordingly.

To refresh the list:
Click the **Refresh** link.

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

There are two elements that 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 AM.
- 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 two hour intervals, starting with 00:00, 02:00, 04:00, 06:00 and so on. For example, if you generate a report at 09:55 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 2 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 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.

Therefore, the generation of reports after starting up an appliance will be possible:

- For hourly reports - 2-3 minutes from startup.
- For daily reports - 1-2 hours from startup.
- For weekly reports - 2-4 hours from startup.
- For 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 and Anti-Virus malwares 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 hosts, servers, and recently active infected hosts.
- 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 hosts 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.

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

There are two elements that 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 AM.
- 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 two hour intervals, starting with 00:00, 02:00, 04:00, 06:00 and so on. For example, if you generate a report at 09:55 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 2 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 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.

Therefore, the generation of reports after starting up an appliance will be possible:

- For hourly reports - 2-3 minutes from startup.
- For daily reports - 1-2 hours from startup.
- For weekly reports - 2-4 hours from startup.
- For 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 and Anti-Virus malwares 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 hosts, servers, and recently active infected hosts.
- 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 hosts 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
See Using System Tools (on page 35).

Managing 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:
- Change the SNMP On/Off slider position to ON or OFF and 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.

Click **Apply**.
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. For more information, see Upgrade Using Boot Loader (on page 171).

**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 using the WebUI, in which case you will not lose your previous settings if the new image supports it. When you reburn a new image with a USB drive, the appliance deletes your previous settings and creates a new factory default image to which the appliance can return to.

**To upgrade to a new firmware image from a USB drive:**

1. Disconnect the Check Point 600 Appliance from the power source.
2. Place the firmware image file on a USB drive, in the top folder. The firmware image file is recognized by its name so do not rename it.
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 one of the USB ports on the Check Point 600 Appliance. If the operation does not succeed, this may be due to the fact that 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. The appropriate USB LED will light and blink several times as it recognizes the file and uploads it to the appliance. The LED turns off once the file uploads. This takes several seconds.
   - If the file is valid, all LAN LEDs will start to blink to show progress. Every other LED blinks at a different speed. The LAN LEDs blink in orange and green (Link LEDs blink orange and Activity LEDs blink green).
   - Upon successful installation all LAN LEDs will turn solid green and the appliance awaits your input.
6. Remove the USB drive and disconnect the appliance from the power source.
7. Reconnect the appliance to the power source. Allow the appliance to boot successfully. The first boot after an image reburn takes more time than a normal boot. Wait patiently for the Notice LED to stop blinking (this indicates that the boot is complete).

As this operation has removed your previous settings please 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. For more information, see Upgrade.

**Installing a new Boot-Loader from a USB drive**

Check Point releases new Boot Loader rarely. This usually comes together with a new image. To upgrade to a new U-Boot or Firmware image requires booting the appliance.

**To replace Boot-Loader (usually done before you upgrade to the new image, if one exists):**

1. Disconnect your Check Point 600 Appliance from the power source.
2. Place the Boot loader file on a USB drive, in the top folder. The Boot loader file is recognized by its name so do not rename it.
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 your Check Point 600 Appliance, to one of the USB ports. If the operation does not succeed, this may be due to the fact that 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. The appropriate USB LED will light and blink several times as it recognizes the file and uploads it to the appliance. The LED turns off once the file uploads. This takes several seconds.
   If the file is valid, all LAN LEDs will start to blink to show progress. Every other LED blinks at a different speed. The LAN LEDs blink in orange and green (Link LEDs blink orange and Activity LEDs blink green).
   Upon successful installation all LAN LEDs will turn solid green and the appliance awaits your input.
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 reconnecting the appliance to the power source.

**Boot Loader**

The Gaia Embedded Boot Menu shows during boot and is available by pressing **Ctrl+C** while the appliance is booting 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. Install/Update Image from USB
7. Install/Update Boot-Loader from USB
8. Restart Boot-Loader
9. 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 solid red.

Options 4-5 are explained in the subsequent sections.

Options 6-7 let you manually choose a specific file from a USB drive and install/update an image or a new boot loader. Once you choose the file and it is downloaded onto the appliance the rest of the procedure is the same as in Upgrade Using a USB Drive (on page 169).

Option 8 restarts the appliance.

Option 9 installs new firmware for the DSL modem (supported in DSL models only) or upload a preset configuration file.

---

**Upgrade Using Boot Loader**

To upgrade the Check Point 600 Appliance 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), 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 choose manual mode, you are asked to fill in the IP of the Check Point 600 Appliance, the IP of the TFTP server, and the image name.
5. If you choose automatic mode, the procedure starts automatically to search for the bootp server.
6. While in menu mode, pressing **Ctrl+C** again returns you to the Boot Loader menu.
   - During the upgrade, all LAN Link and Activity LEDs blink orange and green alternately to indicate progress. This takes up to a few minutes.
   - Upon successful completion all LAN Link and Activity will light in green, and the appliance waits for you to either press a key or to manually reboot [pull the power cable out and put it back in]. Error in the upgrade process is indicated by all LAN Link and Activity LEDs blinking red.
Restoring Factory Defaults

The Check Point 600 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 600 Appliance to its factory default settings if necessary.

You can restore a Check Point 600 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 600 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 being restored, all LAN Link and Activity LEDs blink orange and green alternately 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 defaults button with a pin and hold it for at least 3 seconds.
2. When the Power and Notice LEDs are lit red, release the button. The appliance reboots itself and starts to restore factory defaults immediately.
3. While factory defaults are being restored, all LAN Link and Activity LEDs blink orange and green alternately to show progress.
   This takes some few minutes. When this completes, the appliance reboots automatically.

To restore the Check Point 600 Appliance to its default factory configuration using U-boot (boot loader):
1. Connect to the appliance with a console connection (using 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. Install/Update Image from USB
   7. Install/Update Boot-Loader from USB
   8. Restart Boot-Loader
   Please enter your selection:
3. Enter 4 to select **Restore to Factory Defaults (local)**.

4. When you are prompted: "Are you sure? [y/n]" choose **y** to continue and restore the appliance to its factory defaults settings.

   While factory defaults are being restored, all LAN Link and Activity LEDs will blink orange and green alternately to indicate progress. This will take up to a few minutes. Upon completion, the appliance will boot automatically.
## Front Panel

### Wireless Network + ADSL Model

<table>
<thead>
<tr>
<th>Key</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Express Card</td>
<td>Express card slot that is used for cellular modems in Express Card form factor.</td>
</tr>
</tbody>
</table>
| 2   | USB1 port | USB1 port that is used for:  
- Cellular and analog modems.  
- Reinstalling the appliance with new firmware.  
- Running a first-time configuration script. |
| 3   | Power LED | Green when the appliance is turned on. |
| 4   | Notice LED | • Blinking green during boot.  
• Red when the appliance has a resource problem such as memory shortage. |
| 5   | LAN1 - LAN8, DMZ, WAN LEDs | **Link Indicator**  
- Orange when the port speed is 1000 Mbps.  
- Green when the port speed is 100 Mbps.  
- Not lit when the port speed is 10 Mbps.  
**Activity Indicator**  
- Blinking green when encountering traffic. |
|     | DSL LED | **Link Indicator**  
- Green when an ADSL connection is established.  
- Blinking green when establishing an ADSL connection.  
- Not lit when an ADSL connection is not established.  
**Activity Indicator**  
- Blinking green when encountering traffic.  
- Not lit when the ADSL line is idle.  
*(Only in the Wireless Network + ADSL model)* |
| 6   | Internet LED | • Green when connected to the Internet.  
• Blinking red when the Internet connection is configured but fails to connect. |
|     | WLAN LED | Blinking green when encountering traffic.  
*(Only in Wireless Network and Wireless Network + ADSL models)* |
|     | USB1, USB2 LEDs | Orange when a USB device is connected. |
## Back Panel

### Wireless Network + ADSL Model

<table>
<thead>
<tr>
<th>Key</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANT1 and ANT2</td>
<td>Ports for attaching wireless network antennas. (Only in Wireless Network and Wireless Network + ADSL models)</td>
</tr>
<tr>
<td>2</td>
<td>Power outlet</td>
<td>Connects to the power supply unit’s cable.</td>
</tr>
<tr>
<td>3</td>
<td>Reboot button</td>
<td>Lets you forcibly reboot the appliance. The button is recessed into the appliance chassis to prevent accidental reboot. The appliance reboots immediately after you press the button.</td>
</tr>
<tr>
<td>4</td>
<td>LAN1 - LAN8 ports</td>
<td>Built in Ethernet ports.</td>
</tr>
<tr>
<td></td>
<td>LAN2/SYNC port</td>
<td>In a cluster configuration, you must connect a cable between this port on both appliances that take part in the cluster. You can configure the cluster sync port to a port other than LAN2.</td>
</tr>
<tr>
<td>5</td>
<td>DMZ and WAN ports</td>
<td>Built in Ethernet ports.</td>
</tr>
<tr>
<td>6</td>
<td>USB2 port</td>
<td>Second USB port. Same functionality as the USB1 port on the Front Panel.</td>
</tr>
<tr>
<td>7</td>
<td>Console port</td>
<td>Serial connection configured to 115200 bps by default. You can also use this port to connect an analog modem.</td>
</tr>
<tr>
<td>8</td>
<td>Factory Defaults button</td>
<td>Lets you restore the appliance to its factory defaults. The button is recessed into the appliance chassis to prevent accidental restoring of factory default settings. See Restoring Factory Defaults (on page 172).</td>
</tr>
<tr>
<td>9</td>
<td>ADSL port</td>
<td>Port for attaching ADSL cable. (Only in Wireless Network + ADSL model)</td>
</tr>
</tbody>
</table>
Index

A
Advanced Configuration • 168
Advanced IPS Configuration • 119
Aggressive Aging • 65
Anti-Spam policy • 66
Anti-Spoofing • 67
Appliance Configuration • 23
Application Control and URL Filtering • 67

B
Back Panel • 175
Backing Up the System • 54
Backup, Restore, Upgrade, and Other System Operations • 51
Boot Loader • 169

C
Capacity Optimization • 68
Check Point 600 Appliance Overview • 7
Cloud Services Firmware Upgrade • 68
Cluster • 68
Common Configuration Scenarios • 14
Configuration File Error • 12
Configuring a Cluster • 20
Configuring a Guest Network • 15
Configuring a Hotspot • 47
Configuring Administrator Access • 58
Configuring Advanced Remote Access Options • 131
Configuring Advanced Settings • 64
Configuring Advanced Site to Site Settings • 138
Configuring Anti-Spam Exceptions • 123
Configuring Cloud Services • 14, 27
Configuring DDNS and Access Services • 60
Configuring External Log Servers • 158
Configuring High Availability • 62
Configuring Internet Connectivity • 36
Configuring IPS Exceptions • 114
Configuring Local and Remote System Administrators • 54
Configuring Local System Administrators • 145
Configuring Local Users and User Groups • 144
Configuring QoS • 19
Configuring Remote Access Authentication Servers • 128
Configuring Remote Access Users • 126
Configuring Remote Access VPN • 15
Configuring Site to Site VPN with a Certificate • 17
Configuring Site to Site VPN with a Preshared Secret • 17
Configuring the Anti-Spam Blade • 122
Configuring the DNS Server • 50
Configuring the Firewall Access Policy and Blade • 87
Configuring the Local Network • 42
Configuring the Proxy Server • 51
Configuring the Quality of Service (QoS) - Bandwidth Control Blade • 104
Configuring the Remote Access Blade • 124
Configuring the Routing Table • 49
Configuring the Site to Site VPN Blade • 133
Configuring the Threat Prevention Blade • 111
Configuring VPN • 15
Configuring VPN Sites • 134
Configuring Wireless Network Settings • 39
Connecting the Cables • 8
Controlling and Monitoring Software Blades • 25

D
Defining Custom Applications & URLs • 108
Defining NAT • 99
Defining Server Objects • 97
Deploying from a USB Drive • 9
Deploying the Configuration File - Existing Configuration • 11
Deploying the Configuration File - Initial Configuration • 10
DHCP relay • 68

E
Enabling VoIP Traffic • 21

F
Front Panel • 173

G
General Temporary Directory Size • 68

H
Hardware Options • 69
Hotspot • 69

I
Important Information • 3
Installation • 8
Introduction • 7
Introduction to the WebUI Application • 24
IP Fragments Parameters • 69
IPS Additional Parameters • 69
IPS Engine Settings • 70

L
Logs and Monitoring • 156

M
Managed Services • 71
Managing Active Computers in Internal Networks • 30, 160
Managing Applications and URLs • 147