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.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=16261

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R75.40VS home page (http://supportcontent.checkpoint.com/solutions?id=sk76540).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 October 2012</td>
<td>Updated Creating an IPv6 Object (on page 59)</td>
</tr>
<tr>
<td>16 July 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 Firewall R75.40VS Administration Guide).
Contents

Important Information ........................................................................................................3
Access Control ................................................................................................................... 8
  Access Control Overview ................................................................................................. 8
    Application Control and Identity Awareness ............................................................... 9
  Rules and the Rule Base ................................................................................................. 9
    Rule Base Elements ...................................................................................................... 10
    Implied Rules ................................................................................................................ 11
    Order of Rule Enforcement .......................................................................................... 11
    Example Access Control Rule ..................................................................................... 11
    Special Considerations for Access Control ............................................................... 11
    SmartDashboard Toolbar ............................................................................................. 13
    Defining Access Control Rules .................................................................................... 13
    Defining an Access Control Policy ............................................................................. 14
    Hit Count ..................................................................................................................... 14
  Preventing IP Spoofing ................................................................................................. 16
    Configuring Anti-Spoofing .......................................................................................... 17
    Excluding Specific Internal Addresses ...................................................................... 18
    Legal Addresses ........................................................................................................... 18
  Multicast Access Control ............................................................................................. 19
    Multicast Routing Protocols ....................................................................................... 19
    Dynamic Registration Using IGMP ............................................................................ 19
    IP Multicast Group Addressing ................................................................................... 19
    Per-Interface Multicast Restrictions ........................................................................... 20
    Configuring Multicast Access Control ....................................................................... 21
  Microsoft Networking Services Security ....................................................................... 21
    Securing Microsoft Networking Services (CIFS) ......................................................... 21
    Restricting Access to Servers and Shares (CIFS Resource) ......................................... 21
Authentication ................................................................................................................ 23
  Identity Awareness ......................................................................................................... 23
    AD Query ..................................................................................................................... 25
    Browser-Based Authentication .................................................................................... 26
    Identity Agents ............................................................................................................ 28
    Deployment .................................................................................................................. 30
    Identity Awareness Scenarios ...................................................................................... 30
    Acquiring Identities for Active Directory Users ......................................................... 31
    Configuring Identity Awareness ................................................................................ 38
Network Address Translation ......................................................................................... 39
  NAT Modes .................................................................................................................... 39
    Static NAT .................................................................................................................... 39
    Hide NAT ..................................................................................................................... 40
  NAT Rule Base ............................................................................................................... 42
    Rule Match Order ....................................................................................................... 42
    Automatic and Manual NAT Rules ............................................................................. 43
    Bidirectional NAT ....................................................................................................... 43
    Understanding Automatically Generated Rules ......................................................... 43
  Planning Considerations for NAT ............................................................................... 44
    Hide Versus Static ...................................................................................................... 44
    Automatic Versus Manual Rules ............................................................................... 45
    Choosing the Hide Address in Hide NAT .................................................................... 45
    Specific Deployment Considerations .......................................................................... 45
  Configuring NAT ............................................................................................................ 46
    General Steps for Configuring NAT ........................................................................... 46
Chapter 1

Access Control

In This Chapter

Access Control Overview 8
Rules and the Rule Base 9
Preventing IP Spoofing 16
Multicast Access Control 19
Microsoft Networking Services Security 21

Access Control Overview

A Security Gateway at the network boundary inspects and provides access control for all traffic. Traffic that does not pass through the gateway is not controlled.

A security administrator is responsible for implementing company security policy. The Security Management Server enables administrators to enforce security policies consistently across multiple gateways. To do this, the administrator defines a company-wide security policy Rule Base using SmartDashboard and installs it to the Security Management Server. SmartDashboard is a SmartConsole client application that administrators use to define and apply security policies to gateways. Granular security policy control is possible by applying specific rules to specific gateways.

A Security Gateway provides secure access control because of its granular understanding of all underlying services and applications traveling on the network. Stateful Inspection technology provides full application level awareness and comprehensive access control for predefined applications, services and protocols as well as the ability to specify and define custom services.
Application Control and Identity Awareness

For effective access control, the administrator must also:

- Control how applications access and use network resources
- Be aware of the identities of users and computers behind the IP addresses

The Need for Application Control

The wide adoption of social media and Web 2.0 applications changes the way people use the Internet. More than ever, businesses struggle to keep up with security challenges.

The use of internet applications present the administrator with a new set of challenges. For example:

- **Malware threats** - Application use can open networks to threats from malware. Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. File sharing can easily cause malware to be downloaded into your network.

- **Bandwidth hogging** - Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available for important business applications.

- **Loss of Productivity** - Employees can spend time on social networking and other applications that can seriously decrease business productivity.

Employers do not know what employees are doing on the internet and how that really affects them.

For more on Application Control, see the R75.40VS Application and URL Filtering Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

The Need for Identity Awareness

Traditionally, firewalls use IP addresses to monitor traffic and are unaware of the user and machine identities behind those IP addresses. Identity Awareness removes this notion of anonymity since it maps users and machine identities. This lets you enforce access and audit data based on identity.

Identity Awareness is an easy to deploy and scalable solution. It is applicable for both Active Directory and non-Active Directory based networks as well as for employees and guest users. It is currently available on the Firewall blade and Application Control blade and will operate with other blades in the future.

Identity Awareness lets you easily configure network access and auditing based on network location and:

- The identity of a user
- The identity of a machine

When Identity Awareness identifies a source or destination, it shows the IP address of the user or machine with a name. For example, this lets you create firewall rules with any of these properties. You can define a firewall rule for specific users when they send traffic from specific machines or a firewall rule for a specific user regardless of which machine they send traffic from.

In SmartDashboard, you use Access Role objects to define users, machines and network locations as one object.

For more on Identity Awareness, see the R75.40VS Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

Rules and the Rule Base

A **Security Policy** consists of an ordered set of rules, collectively known as the **Rule Base**. A well-defined security policy is essential to any effective security solution. The fundamental principle of the Rule Base is that all actions that are not explicitly permitted are prohibited.

Each rule in the Rule Base specifies the source, destination, service, and action to be taken for each session. A rule also specifies how the events are tracked. Events can be logged, and then trigger an alert message. Reviewing traffic logs and alerts is a crucial aspect of security management.
### Rule Base Elements

A rule is made up of the following Rule Base elements (not all fields are relevant to a given rule):

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hits</strong></td>
<td>Hit Count tracks the number of connections that each rule matches. For each rule in the Rule Base, the Hits column shows by default a visual indicator of matching connections together with the number of hits in K (thousands), M (millions), G (billions), or T (trillions). You can configure to show the percentage of the rule's hits from total hits, the indicator level (very high, high, medium, low, or zero) and set a timeframe for the data that is shown. These options are configured from the Firewall Rule Base by right-clicking the Hits column header or the rule number. See Hit Count (on page 14).</td>
</tr>
<tr>
<td><strong>Source and Destination</strong></td>
<td>Refers to the originator and recipient of the connection. For applications that work in the client server model, the source is the client and the destination is the server. Once a connection is allowed, packets in the connection pass freely in both directions. You can negate source and destination parameters, which means that a given rule applies to all connection sources/destinations except the specified location. You may, for example, find it more convenient to specify that the a rule applies to any source that is not in a given network. To negate a connection source or destination, right click on the appropriate rule cell and select Negate Cell from the options menu.</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Allows you to configure whether the rule applies to any connection (encrypted or clear) or only to VPN connections. To limit a rule to VPN connections, double-click on the rule and select one of the two VPN options.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>Allows you to apply a rule to specific predefined protocols or services or applications. You can define new, custom services.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Determines whether a packet is accepted, rejected, or dropped. If a connection is rejected, the firewall sends an RST packet to the originator of the connection and the connection is closed. If a packet is dropped, no response is sent and the connection eventually times out. For information on actions that relate to authentication, see Authentication (&quot;Appendix B: Legacy Authentication&quot; on page 102).</td>
</tr>
<tr>
<td><strong>Track</strong></td>
<td>Provides various logging options (see the R75.40VS Security Management Administration Guide (<a href="http://supportcontent.checkpoint.com/solutions?id=sk76540">http://supportcontent.checkpoint.com/solutions?id=sk76540</a>)).</td>
</tr>
<tr>
<td><strong>Install-On</strong></td>
<td>Specifies the Security Gateway on which the rule is installed. There may be no need to enforce certain rules on every Security Gateway. For example, a rule may allow certain network services to cross only one particular gateway. In this case, the specific rule need not be installed on other gateways (see the R75.40VS Security Management Administration Guide (<a href="http://supportcontent.checkpoint.com/solutions?id=sk76540">http://supportcontent.checkpoint.com/solutions?id=sk76540</a>)).</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Specifies the time period (for Activate On and Expire On), the time of day, and the days (every day, day of week, day of month) that the rule is enforced.</td>
</tr>
</tbody>
</table>
Implied Rules

Apart from rules explicitly defined by an administrator, the Security Gateway also creates implied rules, which are derived from Global Properties definitions. Implied rules enable certain connections to occur to and from the gateway using a variety of different services. The firewall places implied rules either first, last, or immediately before last rule in the Rule Base.

Examples of implied rules include rules that enable Security Gateway control connections and outgoing packets originating from the Security Gateway.

To view implied rules:
1. Add at least one rule to the rule base.
2. Click View > Implied Rules.
   The Firewall tab displays the Implied Rules in addition to the user-defined rules.

Order of Rule Enforcement

The Security Gateway inspects packets and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it inspects the packet and applies the first rule in the Rule Base, then the second rule and so on.

Once all elements in a given rule match the information contained the packet (source, destination, service, etc.), the Security Gateway stops the inspection and immediately applies that rule. If no applicable rule is found in the Rule Base, the traffic is automatically blocked.

It is essential that you understand the concept of rule processing. The firewall always enforces the first matching rule to any given packet. This may not necessarily the rule that best applies to the traffic.

It is important to carefully plan your Rule Base and place rules in the appropriate order. The best practice is to put rules that apply to very specific conditions at the beginning of the Rule Base. General rules should be put toward the end of the Rule Base.

Rules are processed in the following order:
1. **First Implied Rule**: This rule cannot be modified or overwritten in the Rule Base. No rules can be placed before it.
2. **Explicit Rules**: These are administrator-defined rules, which may be located anywhere between the first and the next to last implied rules.
3. **Next to Last Implied Rules**: These are more specific implied rules that are applied before the last implied rule is enforced.
4. **Last Implied Rule**: This is the default rule, which typically rejects all packets without logging.

Example Access Control Rule

This table shows a typical access control rule, as seen in the Firewall tab of SmartDashboard. This rule states that HTTP connections that originate from the branch office that are directed to any destination, will be accepted and logged.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch-Office-gw</td>
<td>Any</td>
<td>Any Traffic</td>
<td>http</td>
<td>accept</td>
<td>log</td>
</tr>
</tbody>
</table>

Special Considerations for Access Control

This section describes Access Control scenarios.

Simplicity

The key to effective firewall protection is a simple Rule Base. One of the greatest dangers to the security of your organization is misconfiguration. For example, a user may try to sneak spoofed, fragmented packets past your firewall if you have accidentally allowed unrestricted messaging protocols. To keep your Rule Base simple, ensure that it is concise and therefore easy to understand and maintain. The more rules you have, the more likely you are to make a mistake.
Basic Rules

When creating rules, ensure that you allow only traffic that you want. Consider traffic initiated and crossing the firewall from both the protected and unprotected sides of the firewall.

The following basic access control rules are recommended for every Rule Base:

- A Stealth Rule to prevent direct access to the Security Gateway.
- A Cleanup Rule to drop all traffic that is not permitted by the previous rules. There is an implied rule that does this, but the Cleanup Rule allows you to log such access attempts.

Remember that the fundamental concept behind the Rule Base is that actions that are not explicitly permitted are prohibited.

Rule Order

Rule order is a critical aspect of an effective Rule Base. Having the same rules, but putting them in a different order, can radically alter the effectiveness of your firewall. It is best to place more specific rules first and more general rules last. This order prevents a general rule from being applied before a more specific rule and protects your firewall from misconfigurations.

Topology Considerations: DMZ

If you have servers that are externally accessible from the Internet, it is recommended to create a demilitarized zone (DMZ). The DMZ isolates all servers that are accessible from untrusted sources, such as the Internet, so that if one of those servers is compromised, the intruder only has limited access to other externally accessible servers. Servers in the DMZ are accessible from any network, and all externally accessible servers should be located in the DMZ. Servers in the DMZ should be as secure as possible. Do not allow the DMZ to initiate connections into the internal network, other than for specific applications such as UserAuthority.

X11 Service

The X11 (X Window System Version 11) graphics display system is the standard graphics system for the Unix environment. To enable X11, you must create a specific rule using the X11 service. If you select Any as the Source or Destination, the X11 service is not included because when using the X11 service, the GUI application acts as the server rather than the client.

Editing Implied Rules

Implied rules are defined in the Global Properties window > Firewall Implied Rules page. In general, there is no need to change predefined implied rules. It is often best to leave some of the rules unselected so that the property can be controlled with greater granularity through the Rule Base. For example, you may want to allow ICMP pings across certain gateways only.

Recommended Settings for Firewall Implied Rules

<table>
<thead>
<tr>
<th>Implied Rule</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept control connections</td>
<td>First</td>
</tr>
<tr>
<td>Accept Remote Access control connections</td>
<td>First</td>
</tr>
<tr>
<td>Accept SmartUpdate connections</td>
<td>First</td>
</tr>
<tr>
<td>Accept outbound packets originating from the gateway</td>
<td>Unselected</td>
</tr>
<tr>
<td>Accept RIP</td>
<td>Unselected</td>
</tr>
<tr>
<td>Accept Domain Name Over UDP (Queries)</td>
<td>Unselected</td>
</tr>
</tbody>
</table>
### SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🏛️</td>
<td>Open the SmartDashboard menu. When you are instructed to selected menu options, click this button first. For example, if you are instructed to select <strong>Manage &gt; Users and Administrators</strong>, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td>📝</td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td>🔄</td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td>✗</td>
<td>Change global properties.</td>
</tr>
<tr>
<td>📦</td>
<td>Verify rule base consistency.</td>
</tr>
<tr>
<td>👾</td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td>🛡️</td>
<td>Open SmartConsoles.</td>
</tr>
</tbody>
</table>

### Defining Access Control Rules

**To define access control rules, perform the following steps using SmartDashboard:**

1. Define network objects for each network and host using SmartDashboard.
2. Click the **Firewall** tab in SmartDashboard.
3. From the SmartDashboard menu, select **Rules > Add Rule** and then select either **Bottom**, **Top**, **Below**, or **Above**.
4. In the rule, define the
   - Name
   - Source
   - Destination
   - VPN
   - Service
   - Action (Accept, Drop, or Reject)
   - Track
   - Install On
   - Time
Defining an Access Control Policy

The Access Control policy is required to:

- Allow internal users to access the Internet.
- Allow all users access to the servers on the DMZ network.
- Protect the network from outsiders.

The policy also requires two basic rules: a Stealth rule and a Cleanup rule.

Hit Count

Hit Count tracks the number of connections that each rule matches. For each rule in the Rule Base, the Hits column shows by default a visual indicator of matching connections together with the number of hits.

You can configure to show the percentage of the rule’s hits from total hits, the indicator level (very high, high, medium, low, or zero) and set a timeframe for the data that is shown. These options are configured in the Firewall Rule Base and affect the display in other supported Software Blades.

When you enable Hit Count, the Security Management Server collects the data from supported gateways (from version R75.40). Hit Count works independently from logging. It is not necessary to set the Track option for each rule to Log. Hit count works even if the Track option is None.

With the data you see in the Rule Base Hits column, you can:

- Make the Rule Base more efficient - You can delete rules that have no matching connections. Note that if you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. Other gateways can possibly have matching connections.
- Improve Rule Base performance - In the Firewall Rule Base you can move a rule that has a high hit count to a higher position (one of the first rules) in the Rule Base.
- Better understand the behavior of the policy.

Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable the Hit Count feature for one or more Security Gateways.

After you enable or disable Hit Count you must install the policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally:
1. From the Policy menu, select Global Properties.
2. Select Hit Count from the tree.
3. Select the options:
- **Enable Hit Count** - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.

- **Keep Hit Count data up to** - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

4. Click **OK**.
5. Install the policy.

**To enable or disable Hit Count on each Security Gateway:**
1. From the Gateway Properties of the Security Gateway, select **Hit Count** from the tree.
2. Select **Enable Hit Count** to enable the feature or clear the checkbox to disable it.
3. Click **OK**.
4. Install the policy.

**Configuring the Hit Count Display**

These are the options you can configure for how matched connection data is shown in the **Hits** column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported (versions before R75.40)
  - Security Gateways that have disabled the hit count feature

The values are shown with these letter abbreviations:

- K = 1,000
- M = 1,000,000
- G = 1,000,000,000
- T = 1,000,000,000,000

For example, 259K represents 259 thousand connections and 2M represents 2 million connections.

- **Percentage** - Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded and can be off by a tenth a percent.

- **Level** - The hit count level is a label for the range of hits according to the table.

  The hit count range = Maximum hit value - Minimum hit value (does not include zero hits)

<table>
<thead>
<tr>
<th>Hit Count Label</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>![Zero Icon]</td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td>![Low Icon]</td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td>![Medium Icon]</td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td>![High Icon]</td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td>![Very High Icon]</td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>

**Hits column showing all display options**

- 3M (15.6%, Medium)
- 7M (31.3%, Very High)
- 63K (0.3%, Low)
To configure the Hit Count display:
1. Right-click the **Hits** column header or the rule number in the row.
2. From the menu, select **Display**.
3. Select one or more options:
   - Percentage
   - Value
   - Level

**Configuring the Hit Count Timeframe**

The values shown in the Hits column are based on the Timeframe setting. By default, the timeframe is cumulative according to the **Keep Hit Count data up to** parameter in the Global Settings. For example, if the parameter is configured to 6 months, the available timeframe options are 1 month, 3 months, and 6 months.

You can change the timeframe according to intervals based on the Global Settings parameter.

To configure the hit count timeframe:
1. Right-click the **Hits** column header or the rule number in the row.
2. From the menu, select **Timeframe**.
3. Select the timeframe.

**Refreshing the Hit Count Data**

Hit count data is transferred from the Security Gateways to the Security Management Server once every three hours for each rule. When you refresh the hit count data, you are getting updated data from the data in the Security Management Server database and not directly from the Security Gateways.

After you install a policy, the hit count is updated from each Security Gateway in the policy to the Security Management Server database. This is done once a minute for the first 3 minutes after the policy is installed.

To refresh hit count data in the Firewall Rule Base:
1. Right-click the **Hits** column header or the rule number in the row.
2. From the menu, select **Hit Count > Refresh**.

**To refresh hit count data in the Application and URL Filtering Rule Base:**
- Click **Refresh Hits** in the policy toolbar.

**Preventing IP Spoofing**

If your network is not protected against IP address spoofing, your access control rules are ineffective and it is easy for attackers to gain access by changing the source address of the packet. For this reason, ensure that you configure anti-spoofing protection on every interface of the Security Gateway, including internal interfaces.

IP spoofing occurs when an intruder attempts to gain unauthorized access by changing a packet's IP address to appear as though it originated from network node with higher access privileges.

*Note* - It is important to ensure that all communication originates from its apparent source.

Anti-spoofing protection verifies that packets originate from and are destined to the correct interfaces on the gateway. It confirms which packets actually come from the specified internal network interface. It also verifies that once a packet is routed, it goes through the proper interface.
A packet coming from an external interface, even if it has a spoofed internal IP address, is blocked because the firewall anti-spoofing feature detects that the packet arrived from the wrong interface.

On Alaska_GW, the firewall ensures that:
- All incoming packets to interface IF1 come from the Internet.
- All incoming packets to interface IF2 come from Alaska_LAN or, Alaska_RND_LAN or Florida_LAN.

On Alaska_RND_GW, the firewall ensures that:
- All incoming packets to interface IF3 come from Alaska_LAN, Florida_LAN or the Internet.
- All incoming packets to interface IF4 come from Alaska_RND_LAN.

When configuring anti-spoofing, you need to specify in the interface topology definitions whether the interfaces lead to the Internet (defined as External) or an internal network (defined as Internal).

**Configuring Anti-Spoofing**

It is important to configure anti-spoofing protection on every interface of every Security Gateway, including internal interfaces.

**Configuring Anti-Spoofing for External Interfaces**

To define a valid address for external interfaces:
1. In SmartDashboard, select Manage > Network Objects.
2. Select a gateway and click Edit.
3. From the list of pages, click Topology.
4. Click Get > Interfaces to obtain interface information of the gateway machine.
5. Click Accept.
   - If SmartDashboard cannot retrieve the topology information, check that the gateway General Properties are listed correctly and that the gateway, the Security Management server, and the SmartDashboard all have functioning communications.
6. In the Topology page, select the interface to the Internet and click Edit.
7. In the Interface Properties window, open the Topology tab.
8. Select External (leads out to the Internet).
9. Select Perform Anti-Spoofing based on interface topology.
10. Under Anti-Spoofing action is set to, select one of the following:
    - Prevent - to block packets that have been spoofed.
- **Detect** - to allow packets that have possibly been spoofed. This option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually rejecting packets.

11. **Don't check packets from** is used to ensure anti-spoof checks do not take place for addresses from certain internal networks coming into the external interface.

   To use this option, select the checkbox and select from the drop-down list a network object that represents those internal networks with valid addresses. If the network object that you need is not in the list, click **New** and define the Internal Network object that you need.

   Objects selected in the drop-down list are disregarded by the anti-spoofing enforcement mechanism.

12. In the **Spoof Tracking** option, select **Log** and then click **OK**.

### Configuring Anti-Spoofing for Internal Interfaces

**To define a valid address for internal interfaces:**

1. In SmartDashboard, select **Manage > Network Objects**.
2. Select the Check Point gateway and click **Edit**.
3. In the gateway window, select **Topology**.
4. In the Topology window, click **Get > Interfaces** to obtain interface information of the gateway machine.
5. Under the **Name** column, select the internal interface and click **Edit**.
6. In the **Interface Properties** window, click **Topology**, and then select **Internal (leads to the local network)**.
7. Under **IP Addresses behind this interface**, do one of the following:
   - If there is only one network behind the interface, select **Network defined by the interface IP and Net Mask**.
   - If there is more than one network behind the interface, define a group network object that consists of all the networks behind the interface by selecting **Specific** and the group.
8. Select **Perform Anti-Spoofing based on interface topology**.
9. Under **Anti-Spoofing action is set to**, select one of the following:
   - **Prevent** - to block packets that have been spoofed.
   - **Detect** - to allow packets that have possibly been spoofed. This option is used for monitoring purposes and should be used in conjunction with one of the tracking options. It serves as a tool for learning the topology of a network without actually rejecting packets.
10. Under **Spoof Tracking**, select **Log** and click **OK**.
11. Repeat step 1 to step 8 for all internal interfaces.
12. Install the security policy: **Policy > Install**.

### Excluding Specific Internal Addresses

In some cases, it may be necessary to allow packets with source addresses that belong to an internal network to enter the gateway through an external interface. This may be useful if an external application assigns internal IP addresses to external clients. In this case, you can specify that anti-spoofing checks are not made on packets from specified internal networks.

### Legal Addresses

Legal addresses are those addresses that are permitted to enter a Security Gateway interface. Legal addresses are determined by the network topology. When configuring the firewall anti-spoofing protection, the administrator specifies the legal IP addresses behind the interface. The **Get Interfaces with Topology** option automatically defines the interface and its topology and creates network objects. The firewall obtains this information by reading routing table entries.
Multicast Access Control

Multicast IP transmits a single message to a predefined group of recipients. An example of this is distributing real-time audio and video to a set of hosts that have joined a distributed conference.

Multicast is similar to radio and TV where only those people who have tuned their tuners to a selected frequency receive the information. With multicast you hear the channel you are interested in, but not the others.

IP multicasting applications send one copy of each datagram (IP packet) and address it to a group of computers that want to receive it. This technique sends datagrams to a group of recipients (at the multicast address) rather than to a single recipient (at a unicast address). The routers in the network forward the datagrams to only those routers and hosts that want to receive them.

The Internet Engineering Task Force (IETF) has developed multicast communication standards that define:

- Multicast routing protocols
- Dynamic registration
- IP multicast group addressing

**Multicast Routing Protocols**

Multicast routing protocols communicate information between multicast groups. Examples of multicast routing protocols include Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).

**Dynamic Registration Using IGMP**

Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know if they want to belong to a particular multicast group. Hosts can leave or join the group at any time. IGMP is defined in RFC 1112.

**IP Multicast Group Addressing**

The IP address area has four sections: Class A, Class B, Class C, and Class D. Class A, B, and C addresses are used for unicast traffic. Class D addresses are reserved for multicast traffic and are allocated dynamically.

The multicast address range 224.0.0.0 through 239.255.255.255 is used only for the group address or destination address of IP multicast traffic. Every IP datagram whose destination address starts with 1110 is an IP multicast datagram.

```
+-----+-----+-----+-----+
| 4 bits | 28 bits |
+-----+-----+-----+-----+
| Class D | Multicast group ID |
+-----+-----+-----+-----+
 1 1 1 0   224.0.0.0 — 239.255.255.255
```

Just as a radio is tuned to receive a program that is transmitted at a certain frequency, a host interface can be tuned to receive datagrams sent to a specific multicast group. This process is called joining a multicast group.

The remaining 28 bits of the multi-case address range identify the multicast group to which the datagram is sent. Membership in a multicast group is dynamic (hosts can join and leave multicast groups). The source address for multicast datagrams is always the unicast source address.

**Reserved Local Addresses**

Multicast group addresses in the 224.0.0.0 through 224.0.0.255 range are assigned by the Internet Assigned Numbers Authority (IANA) for applications that are never forwarded by a router (they remain local on a particular LAN segment).

These addresses are called permanent host groups. The following table shows examples of reserved Local Network Multicast Groups.
## Local Network Multicast Groups Examples

<table>
<thead>
<tr>
<th>Multicast Address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.1</td>
<td>All hosts. An ICMP Request (ping) sent to this group should be answered by all multicast capable hosts on the network. Every multicast capable host must join this group at start up on all of its multicast capable interfaces.</td>
</tr>
<tr>
<td>224.0.0.2</td>
<td>All routers. All multicast routers must join this group on all of its multicast capable interfaces.</td>
</tr>
<tr>
<td>224.0.0.4</td>
<td>All DVMRP routers.</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>All OSPF routers.</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>All PIM routers.</td>
</tr>
</tbody>
</table>

For additional information on reserved multicast addresses, refer to the IANA website (http://www.iana.org/assignments/multicast-addresses).

### Per-Interface Multicast Restrictions

A multicast enabled router forwards multicast datagrams from one interface to another. When you enable multicast on a Security Gateway running on SecurePlatform, you can define multicast access restrictions on each interface. These restrictions specify which multicast groups (addresses or address ranges) to allow or to block. Enforcement is performed on outbound multicast datagrams.

When access is denied to a multicast group on an interface for outbound IGMP packets, inbound packets are also denied.

When access restrictions for multicast datagrams are not defined, inbound multicast datagrams entering a gateway from one interface are allowed out of all other interfaces.

In addition to defining per interface access restrictions, you must define a rule in the Rule Base that allows multicast traffic and services, and the destination defined in this rule must allow the required multicast groups.

### VPN Connections

Multicast traffic can be encrypted and sent across VPN links defined using multiple VPN tunnel interfaces (virtual interfaces associated with the same physical interface).
Configuring Multicast Access Control

To configure multicast access control:
1. Select a gateway object in SmartDashboard.
2. On General Properties page, ensure that the gateway version is specified correctly.
3. On the Topology page, select an interface and click Edit.
4. On the Multicast Restrictions tab of the Interface Properties page, select Drop Multicast packets by the following conditions.
5. Select a multicast policy for the interface:
   - Drop multicast packets whose destination is in the list
   - Drop all multicast packets except those whose destination is in the list
6. Click Add to add a multicast address range. The Add Object window opens, with the Multicast Address Ranges object selected in the list.
7. Click New > Multicast Address Range. The Multicast Address Range Properties window opens.
8. Provide a name for this range.
9. Define either an IP address Range or a Single IP Address that are in the 224.0.0.0 to 239.255.255.255 range.
10. Click OK. The named Multicast Range appears in the Add Object window.
11. Click OK. The named Multicast Range appears in the Interface Properties > Multicast Restrictions window.
12. Click OK to close the Interface Properties window and again to close the gateway window.
13. In the Rule Base, add a rule that allows the multicast address range. As the Destination of the rule, specify the range defined in step 5.
14. Save and install the security policy: Policy > Install.

Microsoft Networking Services Security

Securing Microsoft Networking Services (CIFS)

CIFS (Common Internet File System) is a protocol used to request file and print services from server systems over a network. CIFS is an extension of the Server Message Block (SMB) protocol. CIFS is used as the underlying transport layer for the NETBIOS session (nbsession) service over TCP using port 139. In Windows networking, CIFS is used over the Microsoft-DS protocol (port 445) for networking and file sharing. More information on CIFS can be found at http://samba.org/cifs/.

By default, a Windows server has default shares open for administrative purposes (C$, ADMIN$, PRINT$) and is therefore an easy target for internal attacks, such as brute-force password attacks on file servers.

A Security Gateway secures Microsoft Networking Services in the Inspection Module, without requiring a Security server. This meets the high performance requirements of LAN security (Fast Ethernet and Gigabit Ethernet).

The CIFS resource can be used to enforce the following security checks on CIFS connections:

- Verifying the correctness of the protocol.
- Preventing CIFS and NETBIOS messages issued by the client from pointing to beyond message boundaries.
- Restricting access to a list of CIFS servers and disk shares.
- Logging disk share access.

Restricting Access to Servers and Shares (CIFS Resource)

To restrict access to servers and shares:
1. Define a new CIFS Resource.
2. Configure the CIFS Resource. Allowed Disk/Print Shares is a list of allowed CIFS servers and disk shares. Note that the use of wildcards is allowed. Select Add, Edit or Delete to modify the list.
For example, to allow access to the disk share PAUL on the CIFS server BEATLES:

a) Click **Add** and type BEATLES in the **Server Name** field and IPC$ in the **Share Name** field. Click **OK**.

b) Click **Add** again and type BEATLES in the **Server Name** field and PAUL in the **Share Name** field. Click **OK**.

3. Add a new rule. Under **Service**, add either nbsession or Microsoft-DS, together with the configured Resource.

   **Important** - Do not delete or change the protocol type of the service objects that perform content inspection. If the service is altered in this way, the protection will not work.

4. Install the security policy: **Policy > Install**.
Chapter 2

Authentication

In This Chapter

- Identity Awareness 23
- Deployment 30
- Identity Awareness Scenarios 30
- Configuring Identity Awareness 38

Identity Awareness

Check Point Identity Awareness is an easy to deploy and scalable authentication solution, applicable for Active Directory and non-Active Directory based networks. Identity Awareness lets you control network access for employees and guest users and audit data based on identity.

Currently only available on the firewall blade and the Application Control and URL Filtering blade, Identity Awareness will operate with other blades in the future.

Identity Awareness lets you easily configure network access and auditing based on network location and:

- The identity of a user
- The identity of a machine

When Identity Awareness identifies a source or destination, it shows the IP address of the user or machine with a name. For example, this lets you create firewall rules with any of these properties. You can define a firewall rule for specific users when they send traffic from specific machines or a firewall rule for a specific user regardless of which machine they send traffic from.

In SmartDashboard, you use Access Role objects to define users, machines and network locations as one object.

![SmartDashboard Access Role](image-url)
Identity Awareness also lets you see user activity in SmartView Tracker and SmartEvent based on user and machine name and not just IP addresses.

Identity Awareness gets identities from these acquisition sources:

- **AD Query**
- **Browser-Based Authentication**
- **Identity Agent**
- **Terminal Servers Identity Agent**
- **Remote Access**

The table below shows how identity sources are different in terms of usage and deployment considerations. Depending on these considerations, you can configure Identity Awareness to use one identity source or a combination of identity sources.

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
<th>Recommended Usage</th>
<th>Deployment Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AD Query</strong></td>
<td>Gets identity data seamlessly from Microsoft Active Directory (AD)</td>
<td>• Identity based auditing and logging</td>
<td>• Easy configuration (requires AD administrator credentials). For organizations that prefer not to allow administrator users to be used as service accounts on third party devices there is an option to configure AD Query without AD administrator privileges, see sk43874 (<a href="http://supportcontent.checkpoint.com/solutions?id=sk43874">http://supportcontent.checkpoint.com/solutions?id=sk43874</a>).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Leveraging identity in Internet application control</td>
<td>• Preferred for desktop users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Basic identity enforcement in the internal network</td>
<td>• Only detects AD users and machines</td>
</tr>
<tr>
<td>Source</td>
<td>Description</td>
<td>Recommended Usage</td>
<td>Deployment Considerations</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Browser-Based</strong></td>
<td>Captive Portal sends unidentified users to a Web portal for authentication</td>
<td>Captive Portal</td>
<td>Used for identity enforcement (not intended for logging purposes)</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>If Transparent Kerberos Authentication is configured, the browser attempts to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>authenticate users transparently by getting identity information before the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Captive Portal Username/password page is shown to the user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Identity Agent</strong></td>
<td>A lightweight endpoint agent that authenticates securely with Single Sign-On</td>
<td>• Leveraging identity for Data Center protection</td>
<td>See the chapter on Choosing Identify Sources in the R75.40VS Identity Awareness Administration Guide (<a href="http://supportcontent.checkpoint.com/solutions?id=sk76540">http://supportcontent.checkpoint.com/solutions?id=sk76540</a>).</td>
</tr>
<tr>
<td></td>
<td>(SSO)</td>
<td>• Protecting highly sensitive servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When in detecting identity is crucial</td>
<td></td>
</tr>
<tr>
<td><strong>Terminal Servers</strong></td>
<td>To identify multiple users that connect from one IP address, a Terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Identity Agent</strong></td>
<td>Server Identity agent is installed on the application server that hosts</td>
<td>• Identify users that use a Terminal Servers or Citrix environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terminal/Citrix services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Remote Access</strong></td>
<td>Users that gain access through IPSec VPN Office Mode are seamlessly</td>
<td>• Identify and apply identity-based security policy on users that access the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authenticated.</td>
<td>organization through VPN.</td>
<td></td>
</tr>
</tbody>
</table>

Identity aware gateways can share the identity information that they acquire with other identity aware gateways. Users that need to pass through several enforcement points are only identified once. See Advanced Deployment for more information.

**AD Query**

AD Query is an easy to deploy, clientless identity acquisition method. It is based on Active Directory integration and it is completely transparent to the user.

The AD Query option operates when:

- An identified asset (user or machine) tries to access an Intranet resource that creates an authentication request. For example, when a user logs in, unlocks a screen, shares a network drive, reads emails through Exchange, or accesses an Intranet portal.
AD Query is selected as a way to acquire identities. The technology is based on querying the Active Directory Security Event Logs and extracting the user and machine mapping to the network address from them. It is based on Windows Management Instrumentation (WMI), a standard Microsoft protocol. The Security Gateway communicates directly with the Active Directory domain controllers and does not require a separate server.

- No installation is necessary on the clients or on the Active Directory server.

How AD Query Operates - Firewall Rule Base Example

1. The Security Gateway registers to receive security event logs from the Active Directory domain controllers.
2. A user logs in to a desktop computer using his Active Directory credentials.
3. The Active Directory DC sends the security event log to the Security Gateway. The Security Gateway extracts the user and IP information (user name@domain, machine name and source IP address).
4. The user initiates a connection to the Internet.
5. The Security Gateway confirms that the user has been identified and lets him access the Internet based on the policy.

Browser-Based Authentication

Browser-Based Authentication acquires identities from unidentified users. You can configure these acquisition methods:

- Captive Portal
- Transparent Kerberos Authentication

Captive Portal is a simple method that authenticates users through a web interface before granting them access to Intranet resources. When users try to access a protected resource, they get a web page that must fill out to continue.
With Transparent Kerberos Authentication, the browser attempts to authenticate users transparently by getting identity information before the Captive Portal username/password page opens. When you configure this option, the Captive Portal requests authentication data from the browser. Upon successful authentication, the user is redirected to its original destination. If authentication fails, the user must enter credentials in the Captive Portal.

The Captive Portal option operates when a user tries to access a web resource and all of these apply:

- The Captive Portal is selected as a way to acquire identities and the redirect option has been set for the applicable rule.
- Unidentified users cannot access that resource because of rules with access roles in the Firewall / Application Rule Base. But if users are identified, they might be able to access the resource.
- Transparent Kerberos Authentication was configured, but authentication failed.

When these criteria are true, Captive Portal acquires the identities of users.

From the Captive Portal users can:

- Enter an existing user name and password if they have them.
- For guest users, enter required credentials. Configure what is required in the Portal Settings.
- Click a link to download an Identity Awareness agent. Configure this in the Portal Settings.

How Captive Portal Operates - Firewall Rule Base

The steps listed in the example align with the numbers in the image below.

1. A user wants to access the Internal Data Center.
2. Identity Awareness does not recognize him and redirects the browser to the Captive Portal.
3. The user enters his regular office credentials. The credentials can be AD or other Check Point supported authentication methods, such as LDAP, Check Point internal credentials, or RADIUS.
4. The credentials are sent to the Security Gateway and verified in this example against the AD server.
5. The user can now go to the originally requested URL.
How Transparent Kerberos Authentication Operates

1. A user wants to access the Internal Data Center.
2. Identity Awareness does not recognize the user and redirects the browser to the Transparent Authentication page.
3. The Transparent Authentication page asks the browser to authenticate itself.
4. The browser gets a Kerberos ticket from the Active Directory and presents it to the Transparent Authentication page.
5. The Transparent Authentication page sends the ticket to the Security Gateway which authenticates the user and redirects it to the originally requested URL.
6. If Kerberos authentication fails for some reason, Identity Awareness redirects the browser to the Captive Portal.

Identity Agents

There are two types of Identity Agents:

- **Identity Agents** - dedicated client agents installed on users’ computers that acquire and report identities to the Security Gateway.
- **Terminal Servers Identity Agent** - an agent installed on an application server that hosts Citrix/Terminal services. It identifies individual users whose source is the same IP address.
Using Identity Agents gives you:

- **User and machine identity**
- **Minimal user intervention** - all necessary configuration is done by administrators and does not require user input.
- **Seamless connectivity** - transparent authentication using Kerberos Single Sign-On (SSO) when users are logged in to the domain. If you do not want to use SSO, users enter their credentials manually. You can let them save these credentials.
- **Connectivity through roaming** - users stay automatically identified when they move between networks, as the client detects the movement and reconnects.
- **Added security** - you can use the patented packet tagging technology to prevent IP Spoofing. Identity Agents also gives you strong (Kerberos based) user and machine authentication.

These are the types of Identity Agents you can install:

- **Full** - requires administrator permissions for installation. If installed by a user without administrator permissions, it will automatically revert to installing the Light agent. The Full agent performs packet tagging and machine authentication.
- **Light** - does not require administrator permissions for installation. Cannot be configured with packet tagging or machine authentication. The light agent supports Microsoft Windows and Mac OS X. For supported version information, see the R75.40VS Release Notes (http://supportcontent.checkpoint.com/solutions?id=sk76540).
- **Custom** - a customized installation package.
  
  For more information, see Prepackaging Identity Agents.

Users can download and install Identity Agents from the Captive Portal or you can distribute MSI/DMG files to computers with distribution software or any other method (such as telling them where to download the client from).

**How You Download an Identity Agent - Example**

This is how a user downloads the Identity Agent from the Captive Portal:

1. A user logs in to his PC with his credentials and wants to access the Internal Data Center.
2. The Security Gateway enabled with Identity Awareness does not recognize him and sends him to the Captive Portal.
3. The Security Gateway sends a page that shows the Captive Portal to the user. It contains a link that he can use to download the Identity Agent.
4. The user downloads the Identity Agent from the Captive Portal and installs it on his PC.
5. The Identity Agent client connects to the Security Gateway. If SSO with Kerberos is configured, the user is automatically connected.

6. The user is authenticated and the Security Gateway sends the connection to its destination according to the Firewall Rule Base.

**Deployment**

Identity Awareness is commonly enabled on the perimeter gateway of the organization. It is frequently used in conjunction with Application Control and URL Filtering.

To protect internal data centers, Identity Awareness can be enabled on an internal gateway in front of internal servers, such as data centers. This can be in addition to on the perimeter gateway but does not require a perimeter gateway.

Identity Awareness can be deployed in Bridge mode or Route mode.

- In Bridge mode it can use an existing subnet with no change to the hosts' IP addresses.
- In Route mode the gateway acts as a router with different subnets connected to its network interfaces.

For redundancy, you can deploy a gateway cluster in Active-Standby (HA) or Active-Active (LS) modes. Identity awareness supports ClusterXL HA and LS modes.

If you deploy Identity Awareness on more than one gateway, you can configure the gateways to share identity information. Common scenarios include:

- Deploy on your perimeter gateway and data center gateway.
- Deploy on several data center gateways.
- Deploy on branch office gateways and central gateways.

You can have one or more gateways acquire identities and share them with the other gateways.

You can also share identities between gateways managed in different Multi-Domain Servers.

**Identity Awareness Scenarios**

This section describes scenarios in which you can use Identity Awareness to let users access network resources.

The first 3 scenarios describe different situations of acquiring identities in a Firewall Rule Base environment. The last scenario describes the use of Identity Awareness in an Application Control and URL Filtering environment.
Acquiring Identities for Active Directory Users

Organizations that use Microsoft Active Directory as a central user repository for employee data can use AD Query to acquire identities.

When you set the AD Query option to get identities, you are configuring clientless employee access for all Active Directory users. To enforce access options, make rules in the Firewall Rule Base that contain access role objects. An access role object defines users, machines and network locations as one object.

Active Directory users that log in and are authenticated will have seamless access to resources based on Firewall Rule Base rules.

Let's examine a scenario to understand what AD Query does.

Scenario: Laptop Access

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.

He received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19).

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jadams to HR Server</td>
<td>Jadams_PC</td>
<td>HR_Web_Server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>Log</td>
</tr>
</tbody>
</table>

He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator does these steps:

1. Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources and installs the policy.
2. Checks SmartView Tracker to make sure the system identifies John Adams in the logs.
3. Adds an access role object to the Firewall Rule Base that lets John Adams access the HR Web Server from any machine and from any location.
4. Sees how the system tracks the actions of the access role in SmartView Tracker.

User Identification in the Logs

The SmartView Tracker log below shows how the system recognizes John Adams as the user behind IP 10.0.0.19.
This log entry shows that the system maps the source IP to the user John Adams from CORP.ACME.COM. This uses the identity acquired from AD Query.

**Note** - AD Query maps the users based on AD activity. This can take some time and depends on user activity. If John Adams is not identified (the IT administrator does not see the log), he should lock and unlock the computer.

### Using Access Roles

To let John Adams access the HR Web Server from any machine, it is necessary for the administrator to change the current rule in the Rule Base. To do this, it is necessary to create an access role for John Adams that includes the specific user John Adams from any network and any machine.

Then the IT administrator replaces the source object of the current rule with the HR_Partner access role object and installs the policy for the changes to be updated.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR Partner</td>
<td>HR_Partner</td>
<td>HR_Web_Server</td>
<td>Any Traffic</td>
<td>Any</td>
<td>accept</td>
<td>None</td>
</tr>
</tbody>
</table>

The IT administrator can then remove the static IP from John Adam's laptop and give it a dynamic IP. The Security Gateway lets the user John Adams access the HR Web server from his laptop with a dynamic IP as the HR_Partner access role tells it that the user John Adams from any machine and any network is permitted access.

### Acquiring Identities with Browser-Based Authentication

Browser-Based Authentication lets you acquire identities from unidentified users such as:

- Managed users connecting to the network from unknown devices such as Linux computers or iPhones.
- Unmanaged, guest users such as partners or contractors.

If unidentified users try to connect to resources in the network that are restricted to identified users, they are automatically sent to the Captive Portal. If Transparent Kerberos Authentication is configured, the browser will attempt to identify users that are logged into the domain using SSO before it shows the Captive Portal.

Let's examine some scenarios to understand what Browser-Based Authentication does and the configuration required for each scenario.

**Scenario: Recognized User from Unmanaged Device**

The CEO of ACME recently bought her own personal iPad. She wants to access the internal Finance Web server from her iPad. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the Firewall Rule Base.

**Required SmartDashboard Configuration**

To make this scenario work, the IT administrator must:

1. Enable Identity Awareness on a gateway and select Browser-Based Authentication as one of the Identity Sources.
2. In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3. Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
4. Right-click the Action column and select Edit Properties.
   The Action Properties window opens.
5. Select the Redirect http connections to an authentication (captive) portal. Note: redirection will not occur if the source IP is already mapped to a user checkbox.
6. Click OK.
7. From the Source of the rule, right-click to create an Access Role.
a) Enter a **Name** for the Access Role.

b) In the **Users** tab, select **Specific users** and choose Jennifer McHanry.

c) In the **Machines** tab make sure that **Any machine** is selected.

d) Click **OK**.

The Access Role is added to the rule.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>Jennifer_McHanry</td>
<td>Finance_Server</td>
<td>Any</td>
<td>Traffic</td>
<td>http accept (display captive portal)</td>
<td>Log</td>
</tr>
</tbody>
</table>

**User Experience**

Jennifer McHanry does these steps:

1. Browses to the Finance server from her iPad.
   - The Captive Portal opens because she is not identified and therefore cannot access the Finance Server.
2. She enters her usual system credentials in the Captive Portal.
   - A **Welcome to the network** window opens.
3. She can successfully browse to the Finance server.

**User Identification in the Logs**

The SmartView Tracker log below shows how the system recognizes Jennifer McHanry from her iPad.

- This log entry shows that the system maps the source "Jennifer_McHanry" to the user name. This uses the identity acquired from Captive Portal.

**Scenario: Guest Users from Unmanaged Device**

Guests frequently come to the ACME company. While they visit, the CEO wants to let them access the Internet on their own laptops.
Amy, the IT administrator configures the Captive Portal to let unregistered guests log in to the portal to get network access. She makes a rule in the Firewall Rule Base to let unauthenticated guests access the Internet only.

When guests browse to the Internet, the Captive Portal opens. Guests enter their name, company, email address, and phone number in the portal. They then agree to the terms and conditions written in a network access agreement. Afterwards they are given access to the Internet for a specified period of time.

**Required SmartDashboard Configuration**

To make this scenario work, the IT administrator must:

1. **Enable Identity Awareness** on a gateway and select **Browser-Based Authentication** as one of the Identity Sources.
2. In the **Portal Settings** window in the **User Access** section, make sure that **Unregistered guest login** is selected.
3. Click **Unregistered guest login - Settings**.
4. In the **Unregistered Guest Login Settings** window, configure:
   - The data guests must enter.
   - For how long users can access the network resources.
   - If a user agreement is required and its text.
5. Create two new rules in the Firewall Rule Base:
   a) If it is not already there, create a rule that identified users can access the internet from the organization.
      (i) From the **Source** of the rule, right-click to create an **Access Role**.
      (ii) Enter a **Name** for the Access Role.
      (iii) In the Users tab, select **All identified users**.
      (iv) Click **OK**.
      (v) The Access Role is added to the rule.

   || Name | Source       | Destination | VPN  | Service | Action           |
   |-----|-------------|-------------|------|---------|------------------|
   | Internet | Identified_users | ExternalZone | Any Traffic | http | accept |

   b) Create a rule to let Unauthorized Guests access only the internet.
      (i) From the **Source** of the rule, right-click to create an **Access Role**.
      (ii) Enter a **Name** for the Access Role.
      (iii) In the Users tab, select **Specific users** and choose **Unauthenticated Guests**.
      (iv) Click **OK**. The Access Role is added to the rule.
      (v) Select **accept** as the **Action**.
      (vi) Right-click the **Action** column and select **Edit Properties**. The Action Properties window opens.
      (vii) Select **Redirect http connections to an authentication (captive) portal. Note: redirection will not occur if the source IP is already mapped to a user**.
      (viii) Click **OK**.

   || Name | Source | Destination | VPN  | Service | Action                              |
   |-----|--------|-------------|------|---------|-------------------------------------|
   | Guests | Guests | ExternalZone | Any Traffic | http | accept (display captive portal) |

**User Experience**

From the perspective of a guest at ACME, she does these steps:

1. Browses to an internet site from her laptop.
   The Captive Portal opens because she is not identified and therefore cannot access the Internet.
2. She enters her identifying data in the Captive Portal and reads through and accepts a network access agreement.
   A Welcome to the network window opens.
3. She can successfully browse to the Internet for a specified period of time.

**User Identification in the Logs**

The SmartView Tracker log below shows how the system recognizes a guest.

This log entry shows that the system maps the source IP address with the user’s identity. In this case, the identity is "guest" because that is how the user is identified in the Captive Portal.

**Acquiring Identities with Identity Agents**

**Scenario: Identity Agent Deployment and User Group Access**

The ACME organization wants to make sure that only the Finance department can access the Finance Web server. The current Rule Base uses static IP addresses to define access for the Finance department.

Amy, the IT administrator wants to leverage the use of Identity Agents so:

- Finance users will automatically be authenticated one time with SSO when logging in (using Kerberos which is built-in into Microsoft Active Directory).
- Users that roam the organization will have continuous access to the Finance Web server.
- Access to the Finance Web server will be more secure by preventing IP spoofing attempts.

Amy wants Finance users to download the Identity Agent from the Captive Portal. She needs to configure:

- **Identity Agents** as an identity source for Identity Awareness.
- Agent deployment for the Finance department group from the Captive Portal. She needs to deploy the Full Identity Agent so she can set the IP spoofing protection. No configuration is necessary on the client for IP spoofing protection.
- A rule in the Rule Base with an access role for Finance users, from all managed machines and from all locations with IP spoofing protection enabled.

After configuration and policy install, users that browse to the Finance Web server will get the Captive Portal and can download the Identity Agent.

**Required SmartDashboard Configuration**

To make this scenario work, the IT administrator must:

1. Enable Identity Awareness on a gateway and select Identity Agents and Browser-Based Authentication as Identity Sources.
2. Click the Browser-Based Authentication Settings button.
3. In the Portal Settings window in the Users Access section, select Name and password login.
4. In the Identity Agent Deployment from the Portal, select Require users to download and select Identity Agent - Full option.
   
   **Note** - This configures Identity Agent for all users. Alternatively, you can set Identity Agent download for a specific group.

5. Configure Kerberos SSO.
6. Create a rule in the Firewall Rule Base that lets only Finance department users access the Finance Web server and install policy:
   a) From the Source of the rule, right-click to create an Access Role.
   b) Enter a Name for the Access Role.
   c) In the Networks tab, select Specific users and add the Active Directory Finance user group.
   d) In the Users tab, select All identified users.
   e) In the Machines tab, select All identified machines and select Enforce IP spoofing protection (requires Full Identity Agent).
   f) Click OK.
g) The Access Role is added to the rule.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance Web Server</td>
<td>Finance_dept</td>
<td>Finance_web_server</td>
<td>Any Traffic</td>
<td>http, https</td>
<td>accept</td>
</tr>
</tbody>
</table>

7. Install policy.

**User Experience**

A Finance department user does this:

1. Browses to the Finance Web server.
   - The Captive Portal opens because the user is not identified and cannot access the server. A link to download the Identity Agent is shown.

2. The user clicks the link to download the Identity Agent.
   - The user automatically connects to the gateway. A window opens asking the user to trust the server.

   *Note:* The trust window opens because the user connects to the Security Gateway with Identity Awareness using the File Name based server discovery option. See Server Discovery and Trust for more details on other server discovery methods that do not require user trust confirmation.

3. Click **OK**. The user automatically connects to the Finance Web server.
   - The user can successfully browse to the internet for a specified period of time.

**What’s Next**

Other options that can be configured for Identity Agents:

- A method that determines how Identity Agents connect to a Security Gateway enabled with Identity Awareness and trusts it. See Server Discovery and Trust for more details. In this scenario, the File Name server discovery method is used.
- Access roles to leverage machine awareness.
- End user interface protection so users cannot access the client settings.
- Let users defer client installation for a set time and ask for user agreement confirmation. See User Access.

**Acquiring Identities in a Terminal Server Environment**

**Scenario: Identifying Users Accessing the Internet through Terminal Servers**

The ACME organization defined a new policy that only allows users to access the internet through Terminal Servers. The ACME organization wants to make sure that only the Sales department will be able to access Facebook. The current Rule Base uses static IP addresses to define access for Facebook, but now all connections are initiated from the Terminal Servers' IP addresses.

Amy, the IT administrator wants to leverage the use of the Terminal Servers solution so that:
- Sales users will automatically be authenticated with Identity Awareness when logging in to the Terminal Servers.
- All connections to the internet will be identified and logged.
- Access to Facebook will be restricted to the Sales department's users.

To enable the Terminal Servers solution, Amy must:
- Configure Terminal Server/Citrix Identity Agents as an identity source for Identity Awareness.
- Install a Terminal Servers Identity Agent on each of the Terminal Servers.
- Configure a shared secret between the Terminal Servers Identity Agents and the Identity Server.
- After configuration and installation of the policy, users that log in to Terminal Servers and browse to the internet will be identified and only Sales department users will be able to access Facebook.

**Acquiring Identities in Application Control and URL Filtering**

Identity Awareness and Application Control and URL Filtering can be used together to add user awareness, machine awareness, and application awareness to the Check Point gateway. They work together in these procedures:
- Use Identity Awareness Access Roles in Application and URL Filtering rules as the source of the rule.
- You can use all the types of identity sources to acquire identities of users who try to access applications.
- In SmartView Tracker logs and SmartEvent events, you can see which user and IP address accesses which applications.

**Scenario: Identifying Users in Application Control and URL Filtering logs**

The ACME organization wants to use Identity Awareness to monitor outbound application traffic and learn what their employees are doing. To do this, the IT administrator must enable Application Control and URL Filtering and Identity Awareness. The SmartView Tracker and SmartEvent logs will then show identity information for the traffic.

Next, the IT department can add rules to block specific applications or track them differently in the Application Control and URL Filtering policy to make it even more effective. For more, see the R75.40VS Application Control and URL Filtering Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

**Required SmartDashboard Configuration**

To make this scenario work, the IT administrator does these steps:

1. Enables the Application Control and URL Filtering blades on a Security Gateway.
   - This adds a default rule to the Application Control and URL Filtering Rule Base that allows traffic from known applications, with the tracking set to Log.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Application/Sites</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Internet</td>
<td>Any Recognized</td>
<td>Allow</td>
<td>Log</td>
</tr>
</tbody>
</table>

2. Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
3. Installs the policy.

User identification in the Logs

- Logs related to application traffic in SmartView Tracker and SmartEvent show data for identified users.
- SmartView Tracker log entries show that the system maps the source IP address with the user’s identity. It also shows Application Control and URL Filtering data.
- SmartEvent Intro log entries show details of an Application Control and URL Filtering event with Identity Awareness user and machine identity.

Configuring Identity Awareness

To configure Identity Awareness, see the R75.40VS Identity Awareness Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).
Chapter 3

Network Address Translation

Network Address Translation (NAT) involves replacing one IP address with another. NAT can change both the source and destination address inside the packet. This means that a packet that is sent from the internal (protected) side to the external (unprotected) side of the firewall appears to the destination as if it came from a different address, and the packet that is sent from the external to the internal side of the firewall arrives at the correct address.

NAT works with all Check Point network objects, nodes, networks, address ranges, and dynamic objects. You can define NAT automatically by means of the network object configuration, which automatically adds rules to the NAT Rule Base. You can also manually define rules in the NAT Rule Base.

Manually creating NAT Rules adds extra flexibility. For example, in addition to translating IP addresses, you can translate the service or the destination port numbers. Port number translation is a type of Static NAT, in which one port number is translated to another port number.

NAT Modes

The Security Gateway supports two types of NAT:

- **Static NAT**: Each individual private address is translated to a corresponding public address. Connections can originate from both sides of a Security Gateway, so that internal servers are accessible from external sources.

- **Hide NAT**: Maps all specified internal addresses to a single public IP address, thus hiding the internal IP structure from external sources. Connections can originate only from the internal, protected side of a Security Gateway. Internal resources are not accessible by external sources.

Static NAT

The following example illustrates a typical static NAT deployment. Static NAT on a node translates its private address to a unique public address. Static NAT on a network or address range translates each IP address in the network or range to a corresponding public IP address, starting from the defined Static IP address.
Hide NAT

In the Hide NAT mode, source port numbers of all packets are modified. When return packets enter a firewall, the Security Gateway uses the port number to determine which internal machines the packets are destined for. Port numbers are dynamically assigned from two pools of numbers: 600 to 1023 and 10,000 to 60,000.

Port numbers are normally assigned from the second pool. The first pool is used for only three services: rlogin (destination port 512), rshell (destination port 513) and rexec (destination port 514). If the connection uses one of these services, and the original source port is less than 1024, then a port number is assigned from the first pool. This behavior is configurable.

The Security Gateway keeps track of all port numbers assigned, so that the original port number is correctly restored for return packets and a port number that is currently in use is not assigned again to a new connection.

Hide NAT supports a maximum 50,000 connections per server. This capacity limit is only reached if more than 50,000 connections from Hide NATed internal clients are simultaneously directed at a single server on the unprotected side of the Security Gateway—a highly unlikely scenario.

The NAT gateway makes it possible to share a single public address with multiple computers that have private addresses on your intranet. The Internet is unaware of the division you have created between the Internet and your intranet, and treats your multiple computer connection as a single connection.

Hide NAT allows only connections that originate on the internal network. This lets an internal host initiate a connection to both inside and outside the intranet, however, a host outside the network cannot initiate a connection to an internal host.

The Hide Address is the address behind which the internal network, address range or node is hidden. You can opt to hide the internal address(es) either:

- Behind a virtual IP address, which is a routable, public IP address that does not belong to any physical machine, or
- Behind the IP address of the Security Gateway interface through which the packet is routed.

For example, assume the address range 10.1.1.2 to 10.1.1.10 is hidden behind the address of the external interface 192.168.0.1. A connection appears to originate from 10.1.1.3, and the source and destination original and reply packets are translated.
Port Translation

Port Translation allows multiple application servers in a hidden network to be accessed using a single IP address, based on the requested service (or destination port), which saves scarce public IP addresses. A typical implementation enables an FTP server (accessible via port 21), an SMTP server (port 25) and an HTTP server (port 80) to be accessed using a single IP public address.

To use Port Translation you need to create manual NAT rules.

Automatic Hide NAT for Internal Networks

You can use Hide NAT to allow Internet access for large and complex internal networks that contain many subnets, not all of which may be known.

Regular Hide NAT requires that all internal network addresses to be NATed must be specified, even though this may be impractical.

If this is the case, you can specify automatic Hide NAT for all internal networks. Every connection entering from an internal interface and exiting through an external gateway interface (as defined in the Topology page of the gateway object) is NATed behind the external gateway interface address.

For example, assume clients in internal networks initiate connections to servers on the Internet. The source addresses of internal clients are NATed to the address of the external interface, either 192.168.0.1 or 172.16.1.1, depending on the interface from which the connection emerges.
Note - Regular NAT rules take precedence over NAT-for-internal-networks rules. If a connection matches both NAT rule types, the connection is matched to the regular NAT rule. Access rules must also be defined in the Rule Base.

NAT Rule Base

Each rule specifies what happens to the first packet of a connection. Reply packets travel in the opposite direction to the original packet, but are matched to the same rule.

The NAT Rule Base is divided into two sections:

- **Original Packet**: Specifies the conditions when the rule is applied.
- **Translated Packet**: Specifies the action taken when the rule is applied.

Each section in the NAT Rule Base Editor is divided into Source, Destination, and Service. The following actions are performed:

- Translate Source under Original Packet, to Source under Translated Packet
- Translate Destination under Original Packet, to Destination under Translated Packet
- Translate Service under Original Packet, to Service under Translated Packet

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Alaska_W eb</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rule Match Order**

Rule matching in the NAT Rule Base follows the same principle as in the Rule Base. When the firewall receives a packet belonging to a connection, it first compares it against the first rule in the Rule Base, then the second rule, and then the third rule, and so on. When it finds a rule that matches, it stops checking and applies that rule.

The exception to this principle is when two automatic rules match a connection, in which case, bidirectional NAT is applied.
Automatic and Manual NAT Rules

NAT can be defined automatically through the network object (node, network or address range). When you define NAT this way, rules are automatically added to the NAT Rule Base.

You can manually specify NAT rules by adding or editing NAT rules in the NAT Rule Base. The firewall validates manual NAT rules, helping to avoid mistakes in the setup process. Creating manual NAT Rules gives maximum control over the way NAT functions. You can specify the source, destination and service separately for both the original and the translated packet.

When creating Manual NAT rules, you must define the translated network objects in addition to the original objects.

Bidirectional NAT

Bidirectional NAT applies to automatic NAT rules in the NAT Rule Base and allows two automatic NAT rules to match a connection. Without bidirectional NAT, only one automatic NAT rule can match a connection.

When NAT is defined for a network object, an automatic NAT rule is generated which performs the required translation. If there are two network objects, where one is the source of a connection and the other is the destination, using bidirectional NAT, both automatic NAT rules are applied and both objects are translated.

The logic behind bidirectional NAT is:

- If the first match of a connection is on a Manual NAT rule, no further checking of the NAT Rule Base is performed.
- If the first match of a connection is on an Automatic NAT rule, the rest of the NAT Rule Base is checked, one rule at a time, to verify whether another Automatic NAT rule matches the connection. If it finds another match, both rules are matched and no further checking is performed.

The operation of bidirectional NAT can be tracked using the SmartView Tracker and the NAT Rule Number and NAT Additional Rule Number fields. The additional rule is the rule that matches the automatic translation performed on the second object in bidirectional NAT.

Understanding Automatically Generated Rules

NAT can be defined automatically through a network object (node, network or address range), with rules added automatically to the NAT Rule Base.

Hide NAT on a node adds one rule to the NAT Rule Base. It specifies that the source address of the packet is translated for connections originating from the node in the internal network (Source Hide Rule).

Static NAT on a node adds two rules to the NAT Rule Base. In addition to the Source Hide rule, another rule specifies that for connections originating from the external network, the Destination address of the packet is translated (Destination Static Rule).

If NAT (Hide or Static) is performed on a network or an address range, an extra rule is added which specifies that communication within the network or address range is not translated (a packet sent from one machine to another in the same network is not changed).

Example of Automatically Generated Rule (Hide NAT)

This example shows automatically defined Hide NAT rules for the address range node.

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Range_Hide</td>
<td>Range_Hide</td>
</tr>
<tr>
<td>Range_Hide</td>
<td>Any</td>
</tr>
</tbody>
</table>
- Rule 1 states that for connections within the internal (unprotected) side of the firewall, no NAT takes place.
- Rule 2 states that for connections initiated on the internal (protected) side of the firewall, the source address of the packets is translated to the public Hide NAT address.

In automatic Hide NAT rules, the translated address is known as the Hiding Address and is used on the unprotected side of the Security Gateway. The actual addresses are private addresses that are used on the protected side of the Security Gateway.

**Example of Automatically Generated Rules (Static NAT)**

This example shows automatically generated Static NAT rules for an address range on a node.

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Range_static</td>
<td>Range_static</td>
</tr>
<tr>
<td>Range_static</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Range_static</td>
</tr>
</tbody>
</table>

In this example:
- Rule 1 states that for connections within the internal (unprotected) side of the firewall, no NAT takes place. A packet sent from one machine to another in the same network is not changed.
- Rule 2 states that for packets originating from the internal (protected) side of the firewall, source addresses are translated to valid (public) static NAT addresses.
- Rule 3 states that for packets originating from the external (unprotected) side of the firewall, valid (public) destination addresses are translated to static NAT addresses.

In automatic Static NAT rules, statically translated public addresses are called Valid Addresses and are used on the unprotected side of the Security Gateway. The actual addresses are private addresses that are used on the protected side of the Security Gateway.

**Order of Automatic Rules**

Automatic rules are placed in the NAT Rule Base in the following order:
1. Static NAT rules
2. Hide NAT rules.
3. NAT on a node
4. NAT on a network or an address range.

**Planning Considerations for NAT**

**Hide Versus Static**

For protocols where the port number cannot be changed, Hide NAT cannot be used.

When the external server must distinguish between clients based on their IP addresses, Hide NAT cannot be used because all clients share the same IP address under Hide NAT.

To allow connections from the external network to the internal network, only Static NAT can be used.
Automatic Versus Manual Rules

Automatic NAT rules are easy to configure and therefore are less prone to configuration errors. Automatic ARP configuration is only effective for automatic rules.

Manually defining NAT rules can be complicated, but it gives you complete control over NAT. The following operations can only be performed using manual NAT rules:

- Restricting rules to specified destination IP addresses and to specified source IP addresses.
- Translating both source and destination IP addresses in the same packet.
- Performing Static NAT in only one direction.
- Translating services (destination ports).
- Restricting rules to specified services (ports).
- Performing NAT on dynamic objects.

Choosing the Hide Address in Hide NAT

The Hide Address is the address behind which the network, address range or node is hidden.

It is possible to hide behind either the interface of the Security Gateway or a specified IP address.

Choosing a fixed public IP address is a good option if you want to hide the address of the Security Gateway, however, it means you have to use an extra publicly routable IP address.

Choosing to hide behind the address of the Security Gateway is a good option for administrative purposes, for example, if the external IP address of the firewall changes, there is no need to change the NAT settings.

Specific Deployment Considerations

This section presents considerations for using NAT in specific network deployments.

Automatic and Proxy ARP

Giving a machine in the internal network an external IP address using NAT makes that machine appear to the Internet to be on the external network, or the Internet side of the firewall. When NAT is configured automatically, the Security Gateway replies on behalf of translated network objects to ARP requests from the Internet router for the address of the internal machine.
If you are using manual rules, you must configure proxy ARPs to associate the translated IP address with the MAC address of the Security Gateway interface that is on the same network as the translated addresses.

**NAT and Anti-Spoofing**

NAT is performed after anti-spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT.

**Disabling NAT in a VPN Tunnel**

When communicating within a VPN, it is normally not necessary to perform NAT. You can disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule slows down the performance of the VPN.

**Configuring NAT**

**General Steps for Configuring NAT**

To configure NAT:

1. Determine the IP addresses to be used for translation.
2. Define the network objects.
3. Define the Access rules in the Rule Base. When defining Manual NAT rules, you must define network objects with translated addresses. If using Automatic NAT rules, you must define only one network object per real object. For example, if Static NAT is defined on an object called Alaska_Web, then the Rule Base only needs to refer to Alaska_Web, and there is no need to define a rule for Alaska_Web (Valid Address).
4. Define NAT rules (automatic and/or manual).
5. Install the security policy: Policy > Install.

**Basic Configuration - Network Node with Hide NAT**

For example, assume a basic configuration for a network node with Hide NAT. Its goal is to hide the IP address of the Alaska_Web Web server (10.1.1.10) from connections that originate on the Internet. Alaska_GW has three interfaces, one of which faces the network where Alaska_Web resides.
To configure a network node with Hide NAT:
1. Edit the node object for Alaska_Web, and in the NAT page, select Add Automatic Address Translation rules.

   ![NAT configuration interface]

2. Select Translation Method Hide and the Hide behind the interface of the Install on Gateway option.
3. Select Install on Gateway. In the above example, the NAT gateway is Alaska_GW, therefore, select either Alaska_GW or All.

   Packets originating from Alaska_Web, with the Internet as their destination, have their source address translated from 10.1.1.10 to 192.168.0.1. For example, packets originating from the Web server have their source address changed from 172.16.10.3 to 192.168.0.1.

Sample Configuration (Static and Hide NAT)

In this next example, the objective is to make the SMTP and the HTTP servers on the internal network available to the Internet using public addresses and to provide Internet access to all users on the internal network.

The Web and mail servers require static translation because incoming connections are made to them from the Internet. Two routable addresses are available. In this example, 192.168.0.5 is used for the Alaska.Web HTTP server and 192.168.0.6 is used for the Alaska.Mail SMTP server.

The internal clients require hide translation because they will initiate connections. No incoming connections are allowed to them from the Internet. They will hide behind the external interface of the Security Gateway.

To perform a sample configuration with Static and Hide NAT:
1. Define network objects for Alaska.Web (10.1.1.5), Alaska.Mail (10.1.1.6), Alaska_LAN (10.1.1.0 with Net Mask 255.255.255.0) and the Security Gateway (Alaska.GW).
2. Edit the Alaska.Web object and in the NAT page, select Add Automatic Address Translation Rules.
3. Select Static as the Translation Method and define the Translate to IP Address as 192.168.0.5.
4. For Alaska.Mail, select Static as the Translation Method and define the Translate to IP Address as 192.168.0.6.
5. Edit the Alaska_LAN object and in the NAT page:
   a) Select Hide as the Translation Method.
   b) Select Hide behind Gateway.

The effective Hide address for the internal clients on Alaska_LAN is therefore 192.168.0.1. The following screen shot shows the resulting NAT Rule Base.

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Alaska.Mail</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Alaska.Mail (Valid Addresses)</td>
</tr>
<tr>
<td>Alaska.Web</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Alaska.Web (Valid Addresses)</td>
</tr>
<tr>
<td>Alaska_LAN</td>
<td>Alaska_LAN</td>
</tr>
<tr>
<td>Alaska_LAN</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Sample Configuration (Using Manual Rules for Port Translation)**

In following example, the objective is to make both a Web server and a mail server in a DMZ network available from the Internet using a single IP address. Hide NAT is performed on all addresses in the DMZ.
To perform a sample configuration using manual rules for port translation:

1. Define network objects for the network Alaska.DMZ.LAN (172.16.0.0 with Net Mask 255.255.0.0), the Web server Alaska_DMZ_Web (172.16.1.7), the Mail server Alaska_DMZ_Mail (172.16.1.5) and the Security Gateway (Alaska.GW).

2. In the NAT tab on the Alaska.DMZ.LAN network object, select Add Automatic Address Translation Rules.

3. Select Hide as the Translation Method and then Hide behind Gateway. This step adds two automatic rules to the NAT Rule Base (Rules 1 and 2).

4. In the NAT Rule Base, define a Manual NAT rule that translates requests for the HTTP service to the Web server (Rule 3) and a Manual NAT rule to translate SMTP requests to the SMTP server (Rule 4).

<table>
<thead>
<tr>
<th>Original Packet</th>
<th>Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>Alaska.DMZ.LAN</td>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
<td>Alaska_GW</td>
</tr>
<tr>
<td>Any</td>
<td>Alaska_GW</td>
</tr>
</tbody>
</table>

---

**Advanced NAT Configuration**

**Connecting Translated Objects on Different Interfaces**

The following sections describe how to allow connections in both directions between statically translated objects (nodes, networks or address ranges) on different Security Gateway interfaces.

If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

**Internal Communication with Overlapping Addresses**

If two internal networks have overlapping (or partially overlapping) IP addresses, Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each of the overlapping internal networks.
Network Configuration

For example, assume both Network A and Network B share the same address space (192.168.1.0/24), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network A who want to communicate with users in Network B must use the 192.168.30.0/24 network as a destination. Users in Network B who want to communicate with users in Network A must use the 192.168.20.0/24 network as a destination.

The Security Gateway translates the IP addresses in the following way for each individual interface:

**Interface A**
- Inbound source IP addresses are translated to the virtual network 192.168.20.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.

**Interface B**
- Inbound source IP addresses are translated to the network 192.168.30.0/24.
- Outbound destination IP addresses are translated to the network 192.168.1.0/24.

**Interface C**
Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface's IP address (192.168.4.1).

**Communication Examples**
This section describes how to enable communication between internal networks, and between an internal network and the Internet

**Communication Between Internal Networks**
If user A, at IP address 192.168.1.10 in Network A, wants to connect to user B, at IP address 192.168.1.10 (the same IP address) in Network B, user A opens a connection to the IP address 192.168.30.10.
Communication Between Internal Networks

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface A — before NAT</td>
<td>192.168.1.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface A — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
</tbody>
</table>

Security Gateway enforces the security policy for packets from network 192.168.20.0/24 to network 192.168.30.0/24.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface B — before NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface B — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.1.10</td>
</tr>
</tbody>
</table>

Communication Between an Internal Network and the Internet

If user A, at IP address 192.168.1.10 in network A, connects to IP address 10.10.10.10 on the Internet.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface A — before NAT</td>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface A — after NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

Security gateway enforces the security policy for packets from network 192.168.20.0/24 to the Internet.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface C — before NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface C — after NAT Hide</td>
<td>192.168.4.1</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

Routing Considerations

To allow routing from Network A to Network B, routing must be configured on the firewall machine.

The following are routing command examples for Windows and Linux operating systems (for other operating systems, use the equivalent commands):

On Windows
- route add 192.168.30.0 mask 255.255.255.0 192.168.3.2
- route add 192.168.20.0 mask 255.255.255.0 192.168.2.2

On Linux
- route add -net 192.168.30.0/24 gw 192.168.3.2
- route add -net 192.168.20.0/24 gw 192.168.2.2

Object Database Configuration

To activate the overlapping NAT feature, use the dbedit database editor GUI (or command line utility). In the sample network configuration, the per interface values for interface A and interface B are set in the following way:
Sample Network Configuration: Interface Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_overlapping_nat</td>
<td>true</td>
</tr>
<tr>
<td>overlap_nat_dst_ipaddr</td>
<td>The overlapping IP addresses (before NAT). In the sample network configuration, 192.168.1.0 for both interfaces.</td>
</tr>
<tr>
<td>overlap_nat_src_ipaddr</td>
<td>The IP addresses after NAT. In the sample network configuration, 192.168.20.0 for interface A, and 192.168.30.0 for interface B.</td>
</tr>
<tr>
<td>overlap_nat_netmask</td>
<td>The net mask of the overlapping IP addresses. In the sample network configuration, 255.255.255.0.</td>
</tr>
</tbody>
</table>

Security Management Behind NAT

The Security Management server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

NAT (Static or Hide) for the Security Management server IP address can be configured in one click, while still allowing connectivity with managed gateways. All gateways can be controlled from the Security Management server, and logs can be sent to the Security Management server. NAT can also be configured for a Management High Availability server and a Log server.

Note - Security Management behind NAT is not supported for deployments where the Security Management server also acts as a gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management server is in a network on which Network Address Translation is performed (the "NATed network"). The Security Management server can control Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A Security Gateway. However, when using Hide NAT on the Security Management server, gateways can send logs to the Security Management server.

When using the Security Management behind NAT feature, the remote gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management server:

- From the NAT page of the Security Management server object, define NAT and select Apply for A Security Gateway control connections.
Non-Corresponding Gateway Addresses

Sometimes the gateway contacts the Security Management server with an address that does not correspond to the remote gateway's deployment, for example:

- When the gateway's automatic selection does not conform with the routing of the gateway's deployment. In this case, define the masters and loggers manually, to allow the remote gateway to contact the Security Management server using the required address. When an inbound connection from a managed gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management server.

To define masters and loggers, select Use local definitions for Log Servers and Use local definitions for Masters and specify the correct IP addresses on the gateway.

This solution encompasses different scenarios:

- The remote gateway addresses the NATed IP when you want it to address the real IP.
- The remote gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management server or as a Log server.
- Ensure that you properly define the Topology settings on all gateways. All workarounds required for previous versions still function with no changes in their behavior.

Configuring the Security Management server Object

To configure the Security Management server object:

1. From the NAT page on the Primary_Security_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select Hide behind IP Address, for example, 192.168.55.1. Do not select Hide behind Gateway (address 0.0.0.0).
2. Select Install on Gateway to protect the NATed objects or network. Do not select All.

Configuring the Gateway Object

To configure the gateway object:

1. From the Security Gateway Topology page, define the Interface.
2. In the General tab in the Interface Properties window, define the IP Address and the Net mask.
3. In the Topology tab of the Interface Properties window, select Network defined by the interface IP and Net Mask.

IP Pool NAT

An IP Pool is a range of IP addresses (an address range, a network or a group of one of these objects) that is routable to the gateway. IP Pool NAT ensures proper routing for encrypted connections for the following two connection scenarios:

- SecuRemote/SecureClient to MEP (Multiple Entry Point) gateways
- Gateway to MEP gateways

When a connection is opened from a SecuRemote/SecureClient or a client behind a gateway to a server behind the MEP Gateways, the packets are routed through one of the MEP gateways. Return packets in the connection must be routed back through the same gateway in order to maintain the connection. To ensure that this occurs, each of the MEP gateways maintains a pool of IP addresses that are 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.

The pool of IP addresses is configured in the IP Pool page of the gateway object. For additional information on how IP Pool NAT is used in MEP scenarios, see “Multiple Entry Point VPNs”.
IP Pool per Interface

You can define a separate IP address pool on one or more of the gateway interfaces instead of defining a single pool of IPs for the gateway.

Defining an IP pool per interface solves routing issues that occur when the gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the gateway through the same gateway interface. The following illustration shows one of the MEP Gateways in a SecuRemote/SecureClient to MEP (Multiple Entry Point) gateway deployment.

If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct gateway interface through the use of static IP pool NAT addresses.

The remote VPN client's IP address is NATed to an address in the IP pool on one of the gateway interfaces. The addresses in the IP pool can be routed only through that gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the gateway interface, the gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the gateway must be edited so that addresses from a gateway IP pool are returned to the correct gateway interface.

Switching between IP Pool NAT per gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

NAT Priorities

IP Pool NAT can be used both for encrypted (VPN) and non-encrypted (decrypted by the gateway) connections.

Note - To enable IP Pool NAT for clear connections through the gateway, configure INSPECT changes in the user.def file. For additional information, contact Check Point Technical Support.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPSec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify 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.

The order of NAT priorities are:
1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

**Reusing IP Pool Addresses For Different Destinations**

IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers. When reusing addresses from the IP Pool, back connections are supported from the original server only. This means that connections back to the client can be opened only from the specific server to which the connection was opened.

The default Do not reuse IP Pool behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in the following illustration). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client.
Switching between Reuse and Do not reuse modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

Configuring IP Pool NAT

To configure IP Pool NAT:
1. In the Global Properties > NAT page, select Enable IP Pool NAT and the required tracking options.
2. In the gateway General Properties page, ensure the gateway version is specified correctly.
3. For each gateway or gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range. For example, for an address range, do the following:
   a) In the network objects tree, right-click Network Objects branch and select New > Address Range
      The Address Range Properties window opens.
   b) In the General tab, enter the first and last IP of the address range.
   c) Click OK. The new address range appears in the Address Ranges branch of the network objects tree.
4. Select the gateway object, access the Gateway Properties window and select NAT > IP Pool NAT.
5. In the IP Pool NAT page, select one of the following:
   a) Allocate IP Addresses from and then select the address range you created to configure IP Pool NAT for the whole gateway, or
   b) Define IP Pool addresses on gateway interfaces to configure IP Pool NAT per interface.
6. If required, select one or more of the following options:
   a) Use IP Pool NAT for VPN client connections
   b) Use IP Pool NAT for gateway to gateway connections
   c) Prefer IP Pool NAT over Hide NAT to specify 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.
7. Click Advanced.
   a) Return unused addresses to IP Pool after: Addresses in the pool are reserved for t60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the timeout to prevent the IP Pool from being depleted.
   b) Reuse IP addresses from the pool for different destinations: This is a good option unless you need to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.
8. Click OK.
9. Edit the routing table of each internal router so that packets with an IP address assigned from the NAT pool are routed to the appropriate gateway or, if using IP Pools per interface, the appropriate gateway interface.

IP Pool NAT for Clusters

IP Pools for gateway clusters are configured in two places in SmartDashboard:
- In the gateway Cluster object NAT > IP Pool NAT page, select the connection scenario.
- In the Cluster member object IP Pool NAT page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.
Chapter 4

IPv6

In This Chapter

Supported Features

Supported Check Point Features

- Supported Platforms: Gaia, SecurePlatform and IPSO
- Access Control Rules - IPv6 Hosts and IPv6 networks can be configured in Firewall Rule base
- User defined ICMPv6 services
- Anti-Spoofing
- IPS protections:
  - Port Scan
  - Aggressive Aging
  - Max Ping Size Limit
  - Small PMTU
- Acceleration by SecureXL (SecurePlatform and Gaia only)
- ClusterXL High Availability (SecurePlatform and Gaia only)
- CoreXL (SecurePlatform and Gaia only)
- SmartView Tracker support with IPv6 filtering

IPv6 Specific Functionality

- IPv6 extension headers can be allowed or blocked
- IPv6 Fragmentation headers are fully inspected
- 6in4 tunnel traffic can be allowed or blocked
- IPv6 traffic in 6in4 tunnels can be inspected (SecurePlatform and Gaia only)

Non-Supported Features

All features and functionality not specifically shown above are not supported for IPv6. This includes, but is not limited to these items:
- IPS (except for protections shown above)
- NAT
- Application & URL Filtering
- IPSec VPN (This feature was previously supported R70 IPv6Pack)
- Anti-Spam & Mail
- Anti-Virus
- DLP
- QoS

**Enabling IPv6 on a Security Gateway**

This section shows you how to enable IPv6 on different platforms.

**SecurePlatform**

To enable IPv6 on a SecurePlatform Security Gateway:
1. Go to /etc/rc.d/rc3.d and create the file S11ipv6
2. Add these commands to the S11ipv6 file:
   ```
   #!/bin/sh
   modprobe ipv6
   /sbin/ifconfig <dev> inet6 add <IPv6-Address>/<Prefix-Length>
   ```
   **Note** - /sbin/ifconfig <dev> inet6 add <IPv6-Address>/<Prefix-Length> is required for each interface that is configured with an IPv6 address.
3. Configure the S11ipv6 file with executable permissions.
5. Run $FWDIR/scripts/fwipv6_enable on.

**IPSO Appliances**

To enable IPv6 on IPSO appliances:
1. Use Voyager or the CLI to enable and configure applicable interfaces for IPv6 traffic.
2. Use Voyager or the CLI to configure IPv6 static routes.
3. Run $FWDIR/scripts/fwipv6_enable on
4. Reboot the Security Gateway.

**Gaia**

To enable IPv6 on Gaia Security Gateways:
1. In the WebUI, go to the System Management > System Configuration page.
2. Select the IPv6 Support > On option.
4. Use the WebUI or the CLI to enable and configure the applicable interfaces for IPv6.
5. Use the WebUI or the CLI to configure IPv6 static routes.
Disabling IPv6 on a Security Gateway

This section shows you how to disable IPv6 on different platforms.

**SecurePlatform**

To disable IPv6 on an IPv6 enabled Security Gateway:
1. Run this command from the expert mode:
   
   ```bash
   $FWDIR/scripts/fwipv6_enable off
   ```
2. Delete the S11ipv6 file from `/etc/rc.d/rc3.d`.

To disable IPv6 functionality, disable IPv6 support on all Security Gateways.

**IPSO Appliances**

To disable IPv6 on IPSO appliances:
1. Run `$FWDIR/scripts/fwdir6_enable off`
2. Disable IPv6 support for each applicable interface using Voyager or the CLI.

**Gaia**

To disable IPv6 on Gaia Security Gateways:
1. In the WebUI, go to the System Management > System Configuration page.
2. Select the IPv6 Support > Off option.

**Working with IPv6 in SmartConsole**

IPv6 host and network objects can be created in SmartDashboard, and used in the Rule Base as source and destination. You can create rules that have IPv4 and IPv6 objects in the same column.

Creating and managing IPv6 objects is performed in a similar manner as for IPv4 network objects.

Two types of IPv6 objects are supported:
- Host
- Network

**Creating an IPv6 Object**

To create an IPv6 object in SmartDashboard:
1. From the menu bar, select Manage > Network Objects. The Network Objects window opens.
2. From Show, select IPv6.
3. Click New > IPv6 > IPv6 Host or IPv6 Network.
The General Properties window for the object opens.

4. For a Host object, enter the object Name and the IPv6 Address (for example, 2001:db8::11).
   For a Network object, enter the object Name, network IPv6 Address and Prefix length (for example, 2001:db8::11 and 64).

5. Click OK and click Close.
   The IPv6 object is shown in the Network Objects tree.

**IPv6 Rules**

To create an IPv6 rule, simply use IPv6 object(s) in the rule in the same way you would with an IPv4 object. For example, to accept and log IPv6 FTP connections from host alice_v6 to host bob_v6, define this rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>alice_v6</td>
<td>bob_v6</td>
<td>Any Traffic</td>
<td>http</td>
<td>accept</td>
<td>log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

Rules with Sources or Destinations defined as Any, apply to both IPv4 and IPv6 traffic. You can create rules that have IPv6 and IPv6 objects in the same column.

For example, this rule drops all IPv4 and IPv6 telnet packets:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>telnet</td>
<td>drop</td>
<td>None</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
Anti-Spoofing for IPv6 Addresses

Anti-spoofing fully supports IPv6 addresses.

To configure Anti-Spoofing for IPv6:
1. Double-click a Security Gateway object.
2. Open Topology.
3. In the Topology page, select an interface and click Edit. The Interface Properties window opens.
4. Add the IPv6 address information.
5. Open the Topology tab.
6. Configure the IPv6 topology for this interface.
   - If you select **External**, the topology includes all addresses not specified in Internal interface topologies.
   - If you select **Internal > Network defined by the Interface IP and Net Mask**, the topology is calculated using the specified IPv6 and IPv4 addresses.
   - If you select **Internal > Specific**, select the group that contains all network objects behind this interface.

7. Enable **Anti-Spoofing**.

8. Click **OK**.

**IPv6 in SmartView Tracker**

IPv6 logs can be viewed in SmartView Tracker and a predefined selection for IPv6 is also available. To see the IPv6 logs, select the IPv6 Source and IPv6 Destination addresses in the query properties.

**Working with ICMPv6**

These ICMPv6 services are defined by default under ICMP services.

**Predefined ICMPv6 Services:**
- ICMPv6 echo-request6
- ICMPv6 neighbor-advertisement
- ICMPv6 neighbor-solicitation
- ICMPv6 router-advertisement
- ICMPv6 router-solicitation

**Defining an ICMPv6 Service**

You can manually define ICMPv6 services

To report errors when processing packets and to do other Internet-layer functions, you must define the applicable ICMPv6 service.

**To define an ICMPv6 service:**
1. In the **Object List > Services** sub-tab, select **ICMP**.
   - In the **Objects List** pane, **Services** and actions are filtered for ICMP.
2. Click **Action > New > ICMPv6**.
3. In the ICMPv6 Service Properties window, enter a name and a value for **Type** (as listed in RFC 792).
4. Click **OK**.

You can use firewall rules to allow or block ICMP services with the ICMPv6 service type. This service type lets you filter ICMPv6 services based on the type and code specification. You can also define custom (unknown) ICMPv6 services for use in rules.

**Inspiration of Unknown ICMPv6 Codes**

By default, the Security Gateway inspects only a set of known ICMPv6 services. Inspection of unknown ICMPv6 codes can be enabled by setting the Security Gateway kernel parameter `fw_allow_unknown_icmpv6` to 1, then defining them in the rule base.

To change the global kernel parameter, see sk26202

**IPv6 with ClusterXL**

R75.40 ClusterXL supports High Availability clusters for IPv6. All IPv6 status information is synchronized and the IPv6 clustering mechanism is activated during failover.
When you use R75.40 ClusterXL (as with IPv4), ClusterXL does both state synchronization and clustering. In SmartDashboard, you must define IPv6 cluster addresses for each interface that is clustered.

To enable IPv6 functionality for an interface, define an IPv6 address for the applicable interface on the cluster and on each member. All interfaces configured with an IPv6 address must also have a corresponding IPv4 address. If an interface does not require IPv6, only the IPv4 definition address is necessary.

**Note** - You must configure synchronization interfaces with an IPv4 address only. This is because the synchronization mechanism works using IPv4 only. All IPv6 information and states are synchronized using this interface.

To configure IPv6 addresses for cluster interfaces and cluster members:
1. In SmartDashboard, create a new cluster object or double-click an existing cluster object.
2. Click ClusterXL in the navigation tree.
3. Select High Availability.
4. Click Topology > Edit.
   The Edit Topology window opens.
5. Click Add Network.
6. Enter the cluster interface and member information in the applicable fields (IPv4 address, Net Mask, IPv6 address, Prefix length).
   To enter information, select the cell and click Edit.

   **Note** - Cluster members must have the same IPv6 address prefix as the cluster interface. Different prefixes are not supported.

7. Click OK to save your changes.

The cphaprob stat or cphaprob -a only show IPv4 address information because the ClusterXL mechanism is based on IPv4. If cphaprob stat shows that an IPv4 address is up and active, this means that the IPv6 address is also up and active.

Advanced Features

**Defining Rules for IPv6 or IPv4 Only**

You can define rules that examine traffic for a specified IP protocol for one IP version, but not the other. For example, a rule can block traffic using IP protocol 42 for IPv6 but not for IPv4.

You use the IPV4_MATCH or IPv6_MATCH macros as rule parameters in the Match field to do this.

To create a rule for IPv6 or IPv4 only:
1. Define a rule or select an existing rule that uses an unknown service.
2. In the Service column, click the plus icon.
3. Click New and select Other.
4. In the Other Service Properties window, click Advanced.

5. In the Advanced Other Services Properties window, enter the applicable macro for the applicable protocol in the Match field:
- For IPv4, use IPv4_MATCH.
- For IPv6, use IPv6_MATCH.

For example, to block IP protocol 41 for IPv6 only, enter IPv6_MATCH in the match field.

**Traceroute IPv6**

The traceroute service is not predefined for IPv6 traffic. If it is necessary to use the traceroute service for IPv6 rules, you must create a user defined service.

**To create the traceroute service:**
1. In SmartDashboard, create a new service of type ‘other’.
2. In the Other Service Properties window, assign a name.
3. Set the IP protocol to 17.
4. Click Advanced.
5. In the Advanced Other Service Properties window, enter this text string in the Match field:
   
   IPv6_MATCH, uh_dport > 33000, ip_ttl6 < 30

6. Define other parameters as necessary.

**IPv6 Extension Headers**

By default, only packets containing fragmentation headers are allowed. Packets containing other headers are blocked without inspection.

You can also configure the system to allow these extension headers:

- EXTHDR_ROUTING 432.
- EXTHDR_HOPOPTS 0
- EXTHDR_DSTOPTS 60
- EXTHDR_AH 51
If you allow these headers, the IPv6 packet content is inspected.

**To allow any of these extension headers:**

1. Open the table.def file using a text editor:
   
   On a Security Management server, this file is located at $FWDIR/lib/table.def.

2. Remove the "/*" and "*/" characters from the following line:

   ```
   /* allowed_ipv6_extension_headers = { <EXTHDR_ROUTING>,
   <EXTHDR_HOPOPTS>, <EXTHDR_DSTOPTS>, <EXTHDR_AH>,
   <EXTHDR_MOBILE> }; */
   ```

3. Save the file and then Install a policy.

---

**Working with 6in4 Tunnels**

**Using 6in4 Tunnels (SIT) in Rules**

You can allow or block traffic in a 6in4 tunnel with security rules. To do this, you use the SIT service (IPv4 protocol 41) in the rule.

**Important** - Rules using the SIT service only look for IPv4 protocol 41. There is no inspection of encapsulated IPv6 content.

**IPv6 in IPv4 Intra Tunnel Inspection**

R75.40VS supports access control and IPS inspection of encapsulated IPv6 packets using the SIT_with_Intra_Tunnel_Inspection service. When using the SIT_with_Intra_Tunnel_Inspection service in a rule, the IPv6 packets are extracted and matched against all applicable rules in the Rule Base.

**Note** - The location of the rule that contains the SIT_with_Intra_Tunnel_Inspection rule is not important. The extracted packets are matched against all rules in the Rule Base.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>SIT_with_Intra_Tunnel_Inspection</td>
<td>accept</td>
<td>log</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>echo-request6</td>
<td>accept</td>
<td>log</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any Traffic</td>
<td>Any</td>
<td>drop</td>
<td>None</td>
</tr>
</tbody>
</table>

**Partial Address Based Filtering**

Partial Address Based filtering filters an IPv6 address according to part of the address. That is, an IPv6 address is filtered according to an address value within a defined bit range in the IPv6 address.

In order to use Partial Address Based Filtering, one or all of these type 'Other' services must be applied to the rules in the security policy:

- Partial-Source-v6
- Partial-Destination-v6

These services allow filtering of source and destination addresses, by defining the specification of an address, start offset and mask length in their advanced > match part.

**Partial Destination IPv6**

The following Inspect macro can be found in the advanced > match part:

```
PARTIAL_DST_ADDR_MATCH6(0x0,0x0,0x0,0x0,0x0,0,0)
```
The PARTIAL_DST_ADDR_MATCH6 macro receives 6 unsigned integers. The first 4 are the IPv6 address in Network Order (in hexadecimal notation). The 5th is the offset to the first bit of the partial address (starting from 0), and the 6th integer is the length of the partial address (in bits).

For example 2000:1::/64 (in Network Order) is written as:

PARTIAL_DST_ADDR_MATCH6(0x20000001, 0x0, 0x0, 0x0, 0, 64)

**Partial Source IPv6**

The following Inspect macro can be found in the `advanced > match` part:

PARTIAL_SRC_ADDR_MATCH6(0x0,0x0,0x0,0x0,0,0)

For example, if this specification is changed to

PARTIAL_SRC_ADDR_MATCH6(0x0,0x0,0x11aa22bb,0x0,64,32), the service will match connections with IP source addresses with the value 0x11aa22bb in bits 65-96.

**Accessing the IPv6 Kernel**

All regular fw commands communicate with the IPv4 kernel. To access the IPv6 kernel, use the `fw6` command. Examples of such commands are `fw6 ver`, and `fw6 tab`.

The following are examples of commands that support IPv6:

**fw6 ver**

**Description**
This command shows the major and minor version numbers as well as the build number.

**Syntax**
fw6 ver [-k][-f <filename>]

**fw6 tab**

**Description**
This command lets you see dynamic kernel table contents and change them.

**Syntax**
fw6 tab [-t <table>] [-s] [-c] [-f] [-o <filename>] [-r] [-u | -m <maxvals>] [-x | -a -e entry] [-y] [hostname]*
Chapter 5

ISP Redundancy

In This Chapter

ISP Redundancy Modes 67
Configuring ISP Redundancy 67

Make Internet connectivity more reliable with ISP Redundancy. This connects a Security Gateway or cluster member to the Internet through redundant Internet Service Provider (ISP) links.

ISP Redundancy Modes

ISP Redundancy monitors the ISP links and chooses the best current link. You can configure this choice to be for Load Sharing or Primary/Backup.

Item | Description
---|---
1 | Security Gateway
2 | Link A to the ISP
3 | Link B to the ISP

ISP Redundancy monitors the links and directs the connection. You can configure this choice to be for Load Sharing or Primary/Backup ("Configuring ISP Redundancy" on page 67).

- **Load Sharing**: Uses the two links with a distributed load of connections going out from the Security Gateway. Connections coming in are alternated. You can configure best relative loads for the links (set a faster link to handle more load). New connections are randomly assigned to a link. If one link fails, the other takes the load.

- **Primary/Backup**: Uses one link for connections going out from the Security Gateway and coming in. It switches to the backup if the primary link fails. When the primary link is restored, new connections are assigned to it. Existing connections continue on the backup link until they are complete.

Configuring ISP Redundancy

If you configure VPN Link Selection settings on the Security Gateway, ISP Redundancy settings override them.

**To enable ISP Redundancy:**
1. Open the network object properties of the Security Gateway or cluster.
2. Click **Topology > ISP Redundancy**.
3. Select **Support ISP Redundancy**.
4. Select **Load Sharing** or **Primary/Backup**.
5. Configure the links ("Configuring the ISP Links" on page 68).
6. Configure the Security Gateway to be the DNS server ("Configuring Security Gateway as DNS" on page 68).
7. Configure the policy for ISP Redundancy ("Configure the Firewall" on page 69).

### Configuring the ISP Links

Before you begin, make sure you have the ISP data - the speed of the link and next hop IP address. If the Security Gateway has only one external interface, configure two subnets on this interface. You will need routers and a switch.

If the Security Gateway has two external interfaces in the Topology page of the gateway object, you can configure the links automatically.

If the gateway is a ClusterXL cluster member, configure the two cluster members to the two ISPs. Use a LAN with two interfaces. Make sure the member interfaces are on the same subnet as the cluster external interfaces.

**To configure ISP links automatically:**
1. In the ISP Redundancy page, click **Set initial configuration**.
   The ISP Links are added automatically.
2. For **Primary/Backup**, make sure the primary interface is first in the list. Use the arrows to change the order.

**To configure ISP links manually:**
1. In the ISP Redundancy page, click **Add**.
2. In the ISP Link window, give the link a name.
   Note the names you give here. They are used in the ISP Redundancy script and commands.
3. Select the **interface** of the Security Gateway for this ISP link.
   - If the Security Gateway has two external interfaces, set each link to a different interface. If one of the ISP links is dialup connection to a backup ISP, configure the ISP Redundancy Script ("Editing the ISP Redundancy Script" on page 70).
   - If the Security Gateway has only one external interface, set each ISP link to connect to this interface.
4. Configure the **next hop**.
   - If the Security Gateway has two external interfaces, leave this field empty and click **Get from routing table**. The next hop is the default gateway.
   - If the Security Gateway has one external interface, set each ISP link to a different next hop router.
5. For Load Sharing, enter the **weight**. For equal weight distribution, enter **50**. If one link is faster, raise this value and lower it for the other link, so that the two equal 100.
6. Define hosts to be monitored, to make sure the link is working. Open the **Advanced** tab of the ISP Link window, and select hosts to add.

### Configuring Security Gateway as DNS

The Security Gateway, or a DNS server behind it, must respond to DNS queries. It resolves IP addresses of servers in the DMZ (or another internal network).

Get a routable IP address from each ISP. If routable IP addresses are not available, register the domain to make the DNS server accessible from the Internet.

**To enable DNS on the Security Gateway:**
1. Select **Enable DNS Proxy**.
   The gateway intercepts Type A DNS queries for the web servers in its domain, that come from external hosts. If the Security Gateway recognizes the external host, it replies:
   - In Load Sharing mode, the Security Gateway replies with two addresses, alternating their order.
   - In Primary/Backup mode, the Security Gateway replies with the addresses of the active link.
If the Security Gateway does not recognize the host, it passes the DNS query on to the original destination or to the domain DNS server.

2. Click **Configure**.
3. Add your DMZ or web servers. Give each two routable IP addresses, one for each ISP.
4. Enter a number of seconds in **DNS TTL**.
   This sets a Time To Live for each DNS reply. DNS servers in the Internet cannot cache your DNS data in the reply for longer than the TTL.
5. Configure Static NAT to translate the routable addresses to the real server address. External clients use one of the two addresses.

   **Note** - If the servers use different services (for example, HTTP and FTP), you can use NAT only for two routable IP addresses.

6. Define a firewall rule: **allow DNS traffic through the Security Gateway using the domain_udp service.**

**To register the domain and get IP addresses:**
1. Register your domain with the two ISPs.
2. Tell the ISPs the two addresses of the DNS server that respond to DNS queries for the domain.
3. For each server in the DMZ, get two routable IP addresses, one from each ISP.
4. In SmartDashboard, open Global Properties > **NAT** and select **Manual NAT rules - Translate destination on client side.**

**Configure the Firewall**

The Firewall must allow connections through the ISP links, with Automatic Hide NAT on network objects that start outgoing connections.

**To configure the firewall for ISP Redundancy:**
1. In the properties of the object for an internal network, select **NAT > Add Automatic Address Translation Rules.**
2. Select **Hide** and **Hide behind Gateway.**
3. Click **OK.**
4. Define rules for publicly reachable servers (web servers, DNS servers, DMZ servers).
   If you have one routable IP address from each ISP for the Security Gateway, define Static NAT. Allow specific services for specific servers. For example, make rules so that incoming HTTP connections from the two ISPs reach a Web server, and DNS traffic from the ISPs reach the DNS server.

**Example: Manual Static Rules for a Web Server and a DNS Server**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Source</th>
<th>Translated Destination</th>
<th>Serv.</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>IP of web server</td>
<td>http</td>
<td>=</td>
<td>10.0.0.2 (Static)</td>
<td>=</td>
<td>Incoming Web - ISP A</td>
</tr>
<tr>
<td>Any</td>
<td>IP of web server</td>
<td>http</td>
<td>=</td>
<td>10.0.0.2 (Static)</td>
<td>=</td>
<td>Incoming Web - ISP B</td>
</tr>
<tr>
<td>Any</td>
<td>IP of DNS server</td>
<td>domain_udp</td>
<td>=</td>
<td>10.0.0.3 (Static)</td>
<td>=</td>
<td>Incoming DNS - ISP A</td>
</tr>
<tr>
<td>Any</td>
<td>IP of DNS server</td>
<td>domain_udp</td>
<td>=</td>
<td>10.0.0.3 (Static)</td>
<td>=</td>
<td>Incoming DNS - ISP B</td>
</tr>
</tbody>
</table>

If you have a routable address from each ISP for each publicly reachable server (in addition to the Security Gateway), define NAT rules:

a) Give each server a non-routable address.
b) Use the routable addresses in the **Original Destination.**
c) Use the non-routable address in the **Translated Destination.**
d) Select **Any** as the **Original Service.**
Note - If using Manual NAT, automatic arp does not work for the NATed addresses. On Linux and SecurePlatform use local.arp. On IPSO set up Proxy ARP.

When done, install the policy.

**Configuring with VPN**

When ISP Redundancy is enabled, VPN encrypted connections survive a failure of an ISP link. The settings in the ISP Redundancy page override settings in the Link Selection page.

**To configure ISP Redundancy with VPN on one Security Gateway:**

1. In **Topology > ISP Redundancy**, select **Apply settings to VPN traffic**.
2. In **IPSec VPN > Link Selection**, see that **Use ongoing probing** shows the mode of the ISP Redundancy: **Load Sharing** or **High Availability** (for Primary/Backup).

   Link Selection now only probes the ISPs configured in ISP Redundancy.

**To configure for VPN with a third-party peer:**

If the Security Gateway’s peer is not a Check Point computer or appliance, the VPN may fail, or the third-party device may continue to encrypt traffic to a failed link.

- Make sure the device recognizes encrypted traffic from the secondary link as coming from the gateway.
- Change the configuration of ISP Redundancy to not use these Check Point technologies:
  - **Use Probing** - Make sure that Link Selection uses another option.
  - **Load Sharing, Service Based Link Selection, Route based probing** - Work only on Check Point Security Gateways. If used, the Security Gateway uses one link to connect to the third-party peer. The link with the highest prefix length and lowest metric is used.

**Force ISP Link State**

Use the `fw isp_link` command to force the ISP link state to Up or Down. Use this to test installation and deployment, or to force the Security Gateway to recognize the true link state if it cannot (the ISP link is down but the gateway sees it as up).

You can run this command on the Security Gateway or the Security Management server: `fw isp_link [target-gw] link-name up|down`

The `link_name` is the name in the ISP Link window.

**Editing the ISP Redundancy Script**

When the Security Gateway starts, or an ISP link state changes, the `$FWDIR/bin/cpisp_update` script runs. It changes the default route of the Security Gateway. For example, you can force the Security Gateway to change the state of a dialup interface to match that state of its ISP link.

Edit this script to enable a dialup connection for one of the ISP links.

**To configure dialup:**

1. In the script on the Security Gateway, enter the command to change the dialup interface state:
   - If the link goes down: `fw isp_link link_name down`
   - If the link goes up: `fw isp_link link_name up`
2. If you use PPPoE or PPTP xDSL modems, in the PPPoE or PPTP configuration of SecurePlatform, the **Use Peer Gateway** option must not be selected.
Chapter 6

Anti-Spam and Mail

In This Chapter

- Introduction to Anti-Spam and Mail Security
- Mail Security Overview
- Configuring Anti-Spam
- Configuring Anti-Virus Protection for Mail
- Configuring a Disclaimer
- Anti-Spam Logging and Monitoring
- Reporting False Positives to Check Point
- Anti-Spam Tracking and Reporting Options

Introduction to Anti-Spam and Mail Security

The relentless and unprecedented growth in unwanted email now poses an unexpected security threat to the network. As the amount of resources (disk space, network bandwidth, CPU) devoted to handling unsolicited emails increases from year to year, employees waste more and more time sorting through unsolicited bulk email commonly known as spam. Anti-Spam and Mail provides network administrators with an easy and central way to eliminate most of the spam reaching their networks.

Anti-Spam and Mail Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti-Spam</td>
<td>The core of the Anti-Spam functionality is the content based classification engine.</td>
</tr>
<tr>
<td>IP Reputation Anti-Spam</td>
<td>Using an IP reputation service, most of the incoming spam is blocked at connect time.</td>
</tr>
<tr>
<td>Block List Anti-Spam</td>
<td>Block specific senders based on IP address or sender's address.</td>
</tr>
<tr>
<td>Mail Anti-Virus</td>
<td>Scan and filter mail for malware.</td>
</tr>
<tr>
<td>Zero Hour Malware Protection</td>
<td>Filter mail using rapid response signatures.</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion prevention system for mail protection.</td>
</tr>
</tbody>
</table>
Mail Security Overview

On the Anti-Spam & Mail tab:

- Select gateways that enforce Anti-Virus checking
- Select gateways that enforce Anti-Spam protection
- Enable automatic updates
- View settings and logs

Anti-Spam

The Anti-Spam functionality employs unique licensed technology. Unlike many Anti-Spam applications that rely on searching for keywords and a lexical analysis of the content of an email message, Check Point Anti-Spam identifies spam by analyzing known and emerging distribution patterns. By avoiding a search for key words and phrases that might classify a legitimate email as spam and instead focusing on other message characteristics, this solution offers a high spam detection rate with a low number of false positives.

To preserve personal privacy and business confidentiality, only select characteristics are extracted from the message envelope, headers, and body (no reference to actual content or attachments are included). Hashed values of these message characteristics are sent to a Detection Center for pattern analysis. The Detection Center identifies spam outbreaks in any language, message format, or encoding type. Responses are returned to the enterprise gateway within 300 milliseconds.

Once identified, the network of spam generating machines is blacklisted. If the network changes its behavior, it is removed from the black list.
The following figure illustrates the Anti-Spam workflow:

1. Proxy SMTP server on the gateway receives incoming mail
2. The SMTP proxy forwards the mail to an Anti-Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. Using a special Anti-Spam protocol, the Anti-Spam daemon queries the Detection center. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The detection classifies the email as either spam or not spam, and returns the result to the gateway.
5. If the email has been classified as spam, the email is flagged as such (in the header or subject) and forwarded to the enterprise mail server.
6. The mail server forwards the email to its recipient on the network. Because the header or subject has been flagged as spam, recipients can use that tag or marker to set up filtering rules in their native mail program — for example in Microsoft Outlook a rule can be configured to delete all emails with the word SPAM in either the subject line or header.

To prevent delays while large email files are scanned for Spam, a feature known as Adaptive Continuous Download transfers email to the recipient while Anti-Spam detection takes place.

**Adaptive Continuous Download**

To avoid delays, Adaptive Continuous Download starts delivering the email to the recipient while Anti-Spam scanning is still in progress. If the email is designated as Spam, it is flagged as spam before it is completely transferred to the recipient. Both the SMTP and POP3 protocols support Adaptive Continuous Download for the entire email message.

**Configuring Anti-Spam**

**Configuring a Content Anti-Spam Policy**

A content Anti-Spam policy is set on the Anti-Spam & Mail tab of SmartDashboard > Anti-Spam > Content based Anti-Spam.

1. Use the slider to select an Anti-Spam policy protection level.
2. Select flagging options.
3. In the Security Gateway Engine settings section, set a maximum data size to scan.
4. In the **UTM-1 Edge Engine settings** section, set a confidence level for spam and suspected spam.

A spam confidence level is a grade or rating (usually between zero and a hundred) used to decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.

UTM-1 Edge devices contain their own Anti-Spam engines. Values entered in the **UTM-1 Edge Engine settings** section are used to correlate SofaWare Anti-Spam engine ratings with Check Point Anti-Spam engine ratings. For example, if a particular email message is rated by the SofaWare Anti-Spam engine as 90, and this value, once translated into Check Point ratings, means the email should be treated as spam, then the **Actions** defined for Spam or Suspected spam on the **Anti-Spam Policy** page are enforced.

5. Select **Tracking Options** for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include:

- None (no logging)
- Log
- Popup Alert
- Mail Alert
- SNMP trap alert
- Three custom user-defined scripts.

### Configuring an IP Reputation Policy

This window enables IP reputation, an Anti-Spam mechanism that checks the IP address of the message sender (contained in the opening SYN packet) against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. In this way, the IP reputation feature creates a list of trusted email sources.

1. Use the slider to select an IP Reputation Policy:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No IP Reputation service</td>
</tr>
<tr>
<td>Monitor Only</td>
<td>Monitors spam and suspected spam</td>
</tr>
<tr>
<td>Medium Protection</td>
<td>Rejects spam and monitors suspected spam</td>
</tr>
<tr>
<td>High Protection</td>
<td>Rejects spam and suspected Spam</td>
</tr>
</tbody>
</table>

2. Select tracking options for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include

- None (no logging)
- Log
- Popup Alert
- Mail Alert
- SNMP trap alert
- Three custom user-defined scripts.

### Configuring a Block List

A list of email sources to block can be configured according to the sender's name, domain name, or IP address.

1. Use the slider to select a Block Policy:

<table>
<thead>
<tr>
<th>Block Policy</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>No blocking</td>
</tr>
<tr>
<td>Block Policy</td>
<td>Result</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>Monitor Only</td>
<td>Monitors sends by IP and email address</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks senders by IP address and email address</td>
</tr>
</tbody>
</table>

2. In the **Blocked senders/domains** section, click **Add** and enter the name of a sender or domain to be rejected.
3. In the **Blocked IPs** section, click **Add** and enter an IP address that should be blocked.
4. From the drop-down list in the **Tracking** section, select a tracking option for blocked mail or non-spam.

**Configuring Anti-Spam SMTP**

SMTP traffic can be scanned according to direction.

1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download for further information.

**Configuring Anti-Spam POP3**

POP3 traffic can be scanned according to direction.

1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download for further information.

**Configuring Network Exceptions**

An Anti-Spam policy can be enforced on all email traffic or only on traffic that has not been deliberately excluded from the policy.

To exclude sources and destinations:

1. In the **Anti-Spam & Mail** tab, click **Anti-Spam > Advanced > Network Exceptions**.
2. Select **Enforce the Anti-Spam policy on all traffic except for traffic between the following sources and destinations**.
3. Click **Add**. The **Network Exception** window opens.
4. For **Source** and **Destination**, select **Any**, or select **Specific** and one gateway from each list.
5. Click **OK**.

**Configuring an Allow List**

A list of email sources to allow can be configured according to either the senders name and domain name, or IP address.

1. In the **Anti-Spam & Mail** tab, click **Anti-Spam > Advanced > Allow List**.
2. In the **Allowed Senders / Domains** section, click **Add** and enter the name of a sender or domain to be allowed.
3. In the **Allowed IPs** section, click **Add** and enter an allowed IP address.
4. From the drop-down list in the **Tracking** section, select a tracking option.
Selecting a Customized Server

You can select an alternative data center for Anti-Spam analysis.

To select a data center:
1. In the Anti-Spam & Mail tab, click Anti-Spam > Advanced > Customized Server.
2. Select Use Customized Server.
3. From the drop-down list, select a server.

Anti-Spam on UTM-1 Edge Devices

Anti-Spam protection is available on UTM-1 Edge devices.

To configure Anti-Spam on UTM-1 Edge devices:
1. Open the General Properties window of the UTM-1 Edge gateway.
2. Select the Anti-Spam option.

Bridge Mode and Anti-Spam

If an UTM-1 appliance is configured to run in bridge mode, Anti-Spam is supported providing that:

- The bridge interface has an IP address
- The bridge interface has a default gateway
Configuring Anti-Virus Protection for Mail

For detailed explanations regarding the options described in the procedures in this section, see Managing Traditional Anti-Virus in the R75.40VS Anti-Bot and Anti-Virus Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

Configuring Mail Anti-Virus

The Mail Anti-Virus policy prevents email from being used as a virus delivery mechanism.

To configure a mail Anti-Virus policy:
1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Anti-Virus.
2. Set the slider to Block.
3. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
   - Three custom user-defined scripts

Configuring Zero Hour Malware Protection

By proactively scanning the Internet, the Data Center identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection.
2. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block
3. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
4. Three custom user-defined scripts

Configuring SMTP and POP3

SMTP and POP3 traffic can be scanned according to direction or by IPs.

1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > SMTP or POP3.
2. Using the slider, select a protection level:
   - Off
   - Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   - Block
3. When scanning by File Direction, select a scanning direction for:
   - Incoming files
4. When scanning by IPs, create rules for the Rule Base to specify the source and destination of the data to be scanned.

5. For SMTP and HTTP, select the **Activate Proactive Detection (impacts performance)** checkbox to enable file-based Traditional Anti-Virus detection. Clear the checkbox to enable stream mode detection. See Understanding Proactive and Stream Mode Detection for further information. FTP and POP3 are set to Proactive Detection mode automatically.

6. If Proactive Detection has been configured, select the **Activate Continuous Download** checkbox to avoid client time-outs when large files are scanned. See Continuous Download for further information.

### Configuring File Types

You can set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

**File Types**

You can set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

*In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > File Types page and set the actions.*

### Configuring Settings

Define maximum sizes for files and archives that should be scanned. Configure actions to take if the set limits are exceeded, or when a scan fails.

*In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Settings page, configure the fields.*

### Configuring a Disclaimer

You can create your own custom disclaimer notice.

1. In the Anti-Spam & Mail tab, click Advanced > Disclaimer.
2. Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines.**
3. In the text box, type your disclaimer notice.
Anti-Spam Logging and Monitoring

Logs derived from Anti-Spam scanning are sent to Security Management server, and viewed using SmartView Tracker.

Anti-Spam status is monitored using SmartView Monitor. The Anti-Spam status appears under the Firewall product. The status contains information such as the Anti-Spam engine version. Anti-Spam status also includes statistics regarding scanned files. See also: Tracking and Reporting Options ("Anti-Spam Tracking and Reporting Options" on page 79).

Reporting False Positives to Check Point

A small number of genuine emails will inevitably be classified as spam. To help Check Point fine-tune the Anti-Spam service, please report them to Check Point support.

The sender of an email that is falsely classified as spam will receive an email notification that the email could not be delivered. This email contains an Email session ID.

1. Request the email session ID from the sender.
2. Open SmartView Tracker.
3. On the Log tab > Content-based Anti-Spam section locate the email session ID.
4. Open the Record Details and click Copy.
5. At the Check Point Support Center, open a Service Request and paste in the record details.
For more information on how to create and view Service Requests, refer to sk31615 (http://supportcontent.checkpoint.com/solutions?id=sk31615).

Anti-Spam Tracking and Reporting Options

Anti-Spam tracking and reporting options are available in:
- SmartView Tracker
- SmartView Monitor
- SmartReporter

**SmartView Tracker**

SmartView Tracker logs Anti-Spam activity. Record details exist for Number, Date, Time, Product, Interface, Origin, Type, Action, Service, Source, Source country, Destination, Sender, Original sender, Recipients, Original recipients, Spam category, Control, and Information.

Right-clicking on a row displays a new Follow Email Session ID option. Following the session provides granular information.

<table>
<thead>
<tr>
<th>No.</th>
<th>T Date</th>
<th>T Time</th>
<th>Y Type</th>
<th>Y Origin</th>
<th>Y Service</th>
<th>T Source</th>
<th>Y Destination</th>
<th>Y I</th>
</tr>
</thead>
<tbody>
<tr>
<td>5441</td>
<td>3Sep2007</td>
<td>9:17:20</td>
<td>spam-pl</td>
<td>chenlev checkpoint...</td>
<td>smtp</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5442</td>
<td>3Sep2007</td>
<td>9:17:20</td>
<td>spam-pl</td>
<td>chenlev checkpoint...</td>
<td>smtp</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5443</td>
<td>3Sep2007</td>
<td>9:17:20</td>
<td>spam-pl</td>
<td>chenlev checkpoint...</td>
<td>smtp</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SmartView Monitor**

SmartView Monitor reports on Anti-Spam and Anti-Virus activity.

**SmartReporter**

New express reports for content inspection have been added to SmartReporter:
- Anti-Virus
- Anti-Spam
Chapter 7

VoIP

IPS adds more than 80 IPS protections and VoIP settings to protect against malicious attacks. IPS protects by:

- Identifying attack signatures
- Identifying packets with protocol anomalies
- Ensuring RFC compliance
- Inspecting signaling protocols, verifying header formats and protocol call flow state

As part of IPS, VoIP Protections can be:

- Enforced for different gateways using IPS profiles
- Monitored using Detect Mode

IPS also lets you:

- Generate detailed logs with packet captures on VoIP security events
- Configure granular VoIP security for maximum flexibility in deployment and enforcement.
- Add exceptions to specified VoIP protections.
  
  For example, if you add an exception that allows non-RFC complaint SIP traffic on a specified VoIP server, security is not compromised for all other VoIP traffic.

The Security Gateway interoperates with VoIP devices from many leading vendors and supports the SIP, H.323, MGCP and SCCP (Skinny) protocols.

For more on VoIP, see the R75.40VS VoIP Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).
Chapter 8

ConnectControl - Server Load Balancing

In This Chapter
- Introduction to ConnectControl
- Load-Balancing Methods
- ConnectControl Packet Flow
- Logical Server Types
- Persistent Server Mode
- Server Availability
- Load Measuring
- Configuring ConnectControl

Introduction to ConnectControl

ConnectControl is Check Point’s solution for server load balancing. ConnectControl distributes network traffic among a number of servers, which reduces the load on a single machine and thereby improves network response time and provides high availability. In addition to the performance benefits, spreading the load over multiple machines creates redundancy for your application and reduces the risk of downtime.

Load-balanced servers are represented by a single virtual IP address, so clients are unaware that more than one server is serving their requests. This is accomplished using a Logical server, which is a network object defined in SmartDashboard that represents a group of physical servers. The Logical server fields service requests for the load-balanced application and directs them to the appropriate physical server.

ConnectControl runs on the gateway and does not impose any additional memory or processing requirements. It continuously checks the availability of each server and if a server fails or is unreachable, ConnectControl stops directing connections to that server until it becomes available.

Load-Balancing Methods

ConnectControl distributes network traffic to load-balanced servers according to predefined balancing methods, which include:

- **Server Load**: Measures the load on each server to determine which server has the most available resources to service a request. Each server in the group runs a load measuring agent that automatically reports the current system load to ConnectControl on the Security Gateway. Server Load is a good choice if your servers run other demanding applications in addition to supporting your load-balanced application. See also Load Measuring (on page 85).

- **Round Trip**: Ensures that incoming requests are handled by the server with the fastest response time. ConnectControl ascertains the response times of the servers in the group at a user-defined interval, whereupon the gateway executes a series of ICMP echo requests (pings) and reports which server has the shortest average round trip time. ConnectControl then directs the service request to that server. The round trip method is a good choice if there are large variations in the traffic load on your network or when load balancing over WAN connections.

- **Round Robin**: Assigns service requests to the next server in the sequence. The round robin method provides optimal load balancing when the load balanced servers all have similar RAM and CPU and are located on the same segment.
- **Random**: Assigns service requests to servers at random. The random method provides optimal load balancing when the load-balanced servers all have similar RAM and CPU and are located on the same segment.
- **Domain**: Directs service requests based on domain name.

### ConnectControl Packet Flow

When a client requests access to an application that is load balanced by ConnectControl, the following is the packet flow:

1. A client initiates a connection with the logical IP address of the application server, which is actually the address assigned to the Logical server.
2. The service request arrives at the gateway and is matched by the Logical server rule in the Rule Base. The firewall then directs the packet to the Logical server.
3. ConnectControl determines which of the servers in the group can best fulfill the request based on the load-balancing method.

![ConnectControl Packet Flow Diagram]

### Logical Server Types

When creating the Logical server object, you must identify the server type as either HTTP or Other. This distinction is important, as ConnectControl handles the connection to the client differently for each server type. To direct network traffic, the HTTP server type uses HTTP redirection, while the Other server type uses address translation.

#### HTTP

The HTTP Logical server type employs HTTP redirection to distribute network traffic and supports only HTTP services. The redirection mechanism ensures that all sessions comprising an HTTP connection are directed to a single server. This is critical for many Web applications, such as those using HTTP-based forms, which require that a single server process all user data.

The HTTP redirection mechanism works in conjunction with ConnectControl's load-balancing methods. The initial HTTP connection is directed to the proper server based on the selected load-balancing method. ConnectControl then notifies the client that subsequent connections should be directed to the IP address of the selected physical server, rather than to the IP address of the Logical server. The IP address can be the address of a server behind the firewall or of an offsite server. The remainder of the session is conducted without ConnectControl intervention and all operations are transparent to the user.
The Logical server may direct the client to an HTTP server behind the firewall or to an offsite HTTP server, depending on the result of ConnectControl’s load balancing.

All further communication between the client and the server takes place without the intervention of ConnectControl.

**Other**

The Other Logical server type can be used for all services supported by A Security Gateway including HTTP. It uses NAT to direct network traffic to the grouped servers. ConnectControl mediates each service request, even when clients continue a session. When you create an Other Logical server type, ConnectControl allows the connection by automatically placing entries in the Security Gateway kernel table. ConnectControl determines which server receives the request and uses NAT to modify the destination IP address of the incoming packet. If a return connection is opened, the connection is automatically established between the server and the client and the server’s source address in the packet is translated to that of the Logical server. The following illustration shows a connection being directed to a NATed FTP server inside the firewall.
On the packet's return, the firewall translates the packet's original address to that of the Logical server. You can also use an Other Logical server type to handle HTTP service requests. In contrast to the HTTP type, once a connection between the client and server has been established, the Other Logical server type does not disconnect. Instead, ConnectControl handles each HTTP service request from the client and multiple service requests from one client can be directed to different servers.

**Considering Logical Server Types**

When considering the proper implementation for your environment, there are three decisive criteria: use of HTTP forms, server location and servers configured for NAT. The HTTP type supports offsite HTTP servers and form based applications, but only works with the HTTP protocol. The Other type supports all protocols and may provide the most effectively balanced load, but requires servers to be NATed by the gateway.

**Persistent Server Mode**

Persistent server mode is a ConnectControl feature that maintains a client's connection to the server to which it was first directed. When using this feature, you must decide whether the persistency is by server or by service.

**Persistency By Server**

Persistency by server is useful for certain types of HTTP applications, such as forms support in a load-balanced environment comprised of multiple Web servers. When Persistency by server is enabled, ConnectControl directs an HTTP client to a specific server and each subsequent request by the client is directed to the same server. This mode allows clients to fill out forms without the data loss that occurs if separate service requests are directed to different servers. If you support forms, enable Persistent server mode (the default setting) and the Persistency by server option.

**Persistency By Service**

The persistency by service feature is useful if you are load balancing multiple services in your server group, for example, in a redundant environment of two machines, each running HTTP and FTP.
Using persistency by service, the client can be directed to one server for HTTP services and another for FTP services. This prevents you from being locked in to a server under a heavy load, as may occur if you opt for persistency by server in this configuration. **Persistency by service** directs previously load-balanced clients, which request a different service, to be load balanced and directed once again to the correct server.

### Persistent Server Timeout

The **Persistent server timeout** sets the amount of time that a client, once directed to a particular server, continues to be directed to that server. In the event that a server becomes unavailable, new connections are directed to an available server, even if Persistent server mode is enabled. For optimal load balancing between servers, disable **Persistent server mode** so that all application traffic is distributed according to the load-balance method. The **Persistent server timeout** is configured in the **ConnectControl** page of the **Global Properties** window.

### Server Availability

You can configure various properties of ConnectControl in order to check the availability of servers in the Logical server group. You can define how often the gateway pings the servers to ensure they are still active and the number of attempts it makes to contact a nonresponsive server after ConnectControl stops directing connections to it.

These settings are located in the **ConnectControl** page of the **Global Properties** window. The **Server availability check interval** option defines how often the servers are pinged. The **Server check retries** option defines the number of attempts to contact nonresponsive servers.

### Load Measuring

The server load-balancing method is unique because it requires a load-measuring agent to run on each server in the group. The agent is lightweight and does not add additional latency or system overhead to the server. It uses the UDP transport protocol to support communication between the load-measuring agent and ConnectControl.

Check Point provides a sample load-measuring agent application for installation on servers, as well as a load-measuring agent programming interface (API) for organizations who want to write their own agents. You can download the load agent application for your OS from the Check Point Support site (http://supportcontent.checkpoint.com/solutions?id=47.0.1569467.2530820). Sign in to view the solution.

You can configure certain properties of the load-measuring agent in the **ConnectControl** page of the **Global Properties** window. The **Load agents port** property determines the port that the load agent uses to communicate with the Security Gateway. All the load-measuring agents in a configuration must use the same port number. The **Load measurement interval** property defines the interval at which the agent returns information about the server's load to the firewall (the default is every 20 seconds).

For Windows servers, configure and enable the load-measuring agent using the **load_agent_nt <port_number> <load_value>** syntax.

The default port used by ConnectControl is 18212. The values for **load_value** are 0, 1, 2, where:

- 0 measures the load over a 1 minute interval
- 1 measures the load over a 5 minute interval
- 2 measures the load over a 15 minute interval

### Configuring ConnectControl

**To configure ConnectControl:**

1. In SmartDashboard, right-click **Network Objects** in the **Network Objects** tree and select **New > Node > Host**.
2. Define a server object that represents a load-balanced server.
3. Repeat step 2 for each server you place in the group.
4. In Security Management, right-click **Network Objects** and select **New > Group > Simple Group**.
5. Name the group (for example, HTTP_Server_Group).
6. Add the server objects to the group in the Group Properties box. It is recommended to add no more than 29 Logical servers to a group.
7. In SmartDashboard, right-click Network Objects in the Network Objects tree and select New > Logical Server. Ensure the IP address you assign is a routable IP address. All traffic to be load-balanced should be directed through the gateway.
8. Select the Server's Type.
9. Add the Group object you created in step 3 to the Servers Group.
10. To enable Persistent server mode, select either Persistency by service or server (the default mode is Persistency by service).
11. Select a load-balance method as the Balance Method.
12. Add the following rule to the Rule Base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Logical_Server</td>
<td>[load-balanced service(s)]</td>
<td>Accept or User Auth or Client Auth or Session Auth</td>
</tr>
</tbody>
</table>

13. For applications using HTTP redirection (HTTP Logical server type), add a second rule to allow the physical server group to communicate directly with clients after sessions have started.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>HTTP_Server_Group</td>
<td>http</td>
<td>Accept</td>
</tr>
</tbody>
</table>

14. From the Policy menu, select Global Properties > ConnectControl. Review the default settings and adjust according to your implementation. The following options are available:

- **Servers Availability**: Manages how often ConnectControl ensures that the load-balanced servers are running and responding to service requests and how many times ConnectControl attempts to contact a server before ceasing to direct traffic to it. The Server availability check interval option default value is 20 seconds. The Server check retries option default value is 3 times.
- **Servers Persistency**: Defines the amount of time that a client, once directed to a particular server, directs traffic to it. The Persistent server timeout option default value is 1800 seconds.
- **Servers Load Balancing**: Manages how often the load measuring agents (if employed) report their load status to ConnectControl and the port from which they communicate with ConnectControl. The Load agents port option default value is 18212. The Load measurement interval default value is 20 seconds.
Chapter 9
CoreXL Administration

In This Chapter
- Supported Platforms and Unsupported Features 87
- Default Configuration 87
- CoreXL for IPv6 88
- Performance Tuning 88
- Configuring CoreXL 91
- Command Line Reference 91

CoreXL is a performance-enhancing technology for Security Gateways on multi-core processing platforms. CoreXL enhances Security Gateway performance by enabling the processing cores to concurrently perform multiple tasks.

CoreXL provides almost linear scalability of performance, according to the number of processing cores on a single machine. The increase in performance is achieved without requiring any changes to management or network topology.

CoreXL joins ClusterXL Load Sharing and SecureXL as part of Check Point's fully complementary family of traffic acceleration technologies.

In a CoreXL gateway, the firewall kernel is replicated multiple times. Each replicated copy, or instance, of the firewall kernel runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel.

A CoreXL gateway works like a regular Security Gateway. All kernel instances work with traffic going through the same gateway interfaces and apply the same gateway security policy.

Supported Platforms and Unsupported Features

CoreXL is supported on SecurePlatform, IPSO, and Crossbeam platforms.

Unsupported Features:
CoreXL does not support Check Point Suite with these features:

- Check Point QoS (Quality of Service)
- Route-based VPN
- IPv6 on IPSO
- Overlapping NAT

To enable a non-supported feature in the Check Point Suite, disable CoreXL using cpconfig and reboot the gateway (see Configuring CoreXL (on page 91)).

Default Configuration

After installation of CoreXL, the number of kernel instances is taken from the total number of cores in the system.

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Kernel Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>


### CoreXL Administration

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Kernel Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>More than 12</td>
<td>Number of cores, minus 2</td>
</tr>
</tbody>
</table>

The default affinity setting for all interfaces is Automatic when Performance Pack is installed. See Processing Core Allocation (on page 88). Traffic from all interfaces is directed to the core running the Secure Network Distributor (SND).

### CoreXL for IPv6

R75.40VS XX Product XX supports multiple cores for IPv6 traffic. For each firewall kernel instance that works with IPv4 traffic, there is a corresponding firewall kernel instance that also works with IPv6 traffic. Both instances run on the same core.

To check the status of CoreXL on your Security Gateway, run:
```
fw6 ctl multik stat.
```

The `fw6 ctl multik stat` (multi-kernel statistics) command shows IPv6 information for each kernel instance. The state and processing core number of each instance is displayed, along with:
- The number of connections currently running.
- The peak number of concurrent connections the instance has used since its inception.

### Performance Tuning

The following sections are relevant only for SecurePlatform.

#### Processing Core Allocation

The CoreXL software architecture includes the Secure Network Distributor (SND). The SND is responsible for:
- Processing incoming traffic from the network interfaces
- Securely accelerating authorized packets (if Performance Pack is running)
- Distributing non-accelerated packets among kernel instances.

Traffic entering network interface cards (NICs) is directed to a processing core running the SND. The association of a particular interface with a processing core is called the interface's *affinity* with that core. This affinity causes the interface's traffic to be directed to that core and the SND to run on that core. Setting a kernel instance or a process to run on a particular core is called the instance's or process's *affinity* with that core.

The default affinity setting for all interfaces is Automatic. Automatic affinity means that if Performance Pack is running, the affinity for each interface is automatically reset every 60 seconds, and balanced between available cores. If Performance Pack is not running, the default affinities of all interfaces are with one available core. In both cases, any processing core running a kernel instance, or defined as the affinity for another process, is considered unavailable and will not be set as the affinity for any interface.

In some cases, which are discussed in the following sections, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This is done by changing the affinities of different NICs (interfaces) and/or processes. However, to ensure CoreXL's efficiency, all interface traffic must be directed to cores not running kernel instances. Therefore, if you change affinities of
interfaces or other processes, you will need to accordingly set the number of kernel instances and ensure that the instances run on other processing cores.

Under normal circumstances, it is not recommended for the SND and an instance to share a core. However, it is necessary for the SND and an instance to share a core when using a machine with exactly two cores.

**Allocating Processing Cores**

In certain cases, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This section discusses these cases.

Before planning core allocation, make sure you have read the Processing Core Allocation (on page 88).

**Adding Processing Cores to the Hardware**

Increasing the number of processing cores on the hardware platform does not automatically increase the number of kernel instances. If the number of kernel instances is not increased, CoreXL does not utilize some of the processing cores. After upgrading the hardware, increase the number of kernel instances using `cpconfig`.

Reinstalling the gateway will change the number of kernel instances if you have upgraded the hardware to an increased number of processing cores, or if the number of processing cores stays the same but the number of kernel instances was previously manually changed from the default. Use `cpconfig` to reconfigure the number of kernel instances.

In a clustered deployment, changing the number of kernel instances (such as by reinstalling CoreXL) should be treated as a version upgrade. Follow the instructions in the [R75.40VS Installation and Upgrade Guide](http://supportcontent.checkpoint.com/solutions?id=sk76540) in the "Upgrading ClusterXL Deployments" chapter, and perform either a Minimal Effort Upgrade (using network downtime) or a Zero Downtime Upgrade (no downtime, but active connections may be lost), substituting the instance number change for the version upgrade in the procedure. A Full Connectivity Upgrade cannot be performed when changing the number of kernel instances in a clustered environment.

**Allocating an Additional Core to the SND**

In some cases, the default configuration of instances and the SND will not be optimal. If the SND is slowing the traffic, and your platform contains enough cores that you can afford to reduce the number of kernel instances, you may want to allocate an additional core to the SND. This is likely to occur especially if much of the traffic is of the type accelerated by Performance Pack; in a ClusterXL Load Sharing deployment; or if IPS features are disabled. In any of these cases, the task load of the SND may be disproportionate to that of the kernel instances.

**To check if the SND is slowing down the traffic:**

1. Identify the processing core to which the interfaces are directing traffic using `fw ctl affinity -l -r`.
2. Under heavy traffic conditions, run the `top` command on the CoreXL gateway and check the values for the different cores under the 'idle' column.

It is recommended to allocate an additional core to the SND only if all of the following conditions are met:

- Your platform has at least eight processing cores.
- The 'idle' value for the core currently running the SND is in the 0%-5% range.
- The sum of the 'idle' values for the cores running kernel instances is significantly higher than 100%.

If any of the above conditions are not met, the default configuration of one processing core allocated to the SND is sufficient, and no further configuration is necessary.

Allocating an additional processing core to the SND requires performing the following two stages in the order that they appear:

1. Reduce the number of kernel instances using `cpconfig`.
2. Set interface affinities to the remaining cores, as detailed below.
3. Reboot to implement the new configuration.
Setting Interface Affinities

Check which cores are running the kernel instances. See also Allocating Processing Cores (on page 89). Allocate the remaining cores to the SND by setting interface affinities to the cores. The correct method of defining interface affinities depends on whether or not Performance Pack is running, as described in the following sections.

- When Performance Pack is Running
  
  If Performance Pack is running, interface affinities are handled by using Performance Pack’s sim affinity command.

  The default sim affinity setting is Automatic. In Performance Pack’s Automatic mode, interface affinities are automatically distributed among cores that are not running kernel instances and that are not set as the affinity for any other process.

  In most cases, you do not need to change the sim affinity setting. For further information on sim affinity settings, see the R75.40VS Performance Pack Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk76540).

- Setting Interface Affinities when Performance Pack is not Running

  If Performance Pack is not running, interface affinities are loaded at boot from a configuration text file called fwaffinity.conf, located under: $FWDIR/conf. In the text file, lines beginning with the letter i define interface affinities.

  If Performance Pack is running, interface affinities are defined by sim affinity settings, and lines beginning with i in fwaffinity.conf are ignored.

  If you are allocating only one processing core to the SND, it is best to have that core selected automatically by leaving the default interface affinity set to automatic, and having no explicit core affinities for any interfaces. To do this, make sure fwaffinity.conf contains the following line:

  i default auto

  In addition, make sure that fwaffinity.conf contains no other lines beginning with i, so that no explicit interface affinities are defined. All interface traffic will be directed to the remaining core.

  If you are allocating two processing cores to the SND, you need to explicitly set interface affinities to the two remaining cores. If you have multiple interfaces, you need to decide which interfaces to set for each of the two cores. Try to achieve a balance of expected traffic between the cores (you can later check the balance by using the top command).

  To explicitly set interface affinities, when Performance Pack is not running:

  1. Set the affinity for each interface by editing fwaffinity.conf. The file should contain one line beginning with i for each interface. Each of these lines should follow the following syntax:

     i <interfacename> <cpuid>

     where <interfacename> is the interface name, and <cpuid> is the number of the processing core to be set as the affinity of that interface.

     For example, if you want the traffic from eth0 and eth1 to go to core #0, and the traffic from eth2 to go to core #1, create the following lines in fwaffinity.conf:

     i eth0 0
     i eth1 0
     i eth2 1

     Alternatively, you can choose to explicitly define interface affinities for only one processing core, and define the other core as the default affinity for the remaining interfaces, by using the word default for <interfacename>.

     In the case described in the previous example, the lines in fwaffinity.conf would be:

     i eth2 1
     i default 0

  2. Run $FWDIR/scripts/fwaffinity_apply for the fwaffinity.conf settings to take effect.

The affinity of virtual interfaces can be set using their physical interface(s).

Allocating a Core for Heavy Logging

If the gateway is performing heavy logging, it may be advisable to allocate a processing core to the fwd daemon, which performs the logging. Like adding a core for the SND, this too will reduce the number of cores available for kernel instances.
To allocate a processing core to the `fwd` daemon, you need to do two things:

1. Reduce the number of kernel instances using `cpconfig`.
2. Set the `fwd` daemon affinity, as detailed below.

**Setting the fwd Daemon Affinity**

Check which processing cores are running the kernel instances and which cores are handling interface traffic using `fw ctl affinity -l -r`. Allocate the remaining core to the `fwd` daemon by setting the `fwd` daemon affinity to that core.

Note - Avoiding the processing core or cores that are running the SND is important only if these cores are explicitly defined as affinities of interfaces. If interface affinities are set to Automatic, any core that is not running a kernel instance can be used for the `fwd` daemon, and interface traffic will be automatically diverted to other cores.

Affinities for Check Point daemons (such as the `fwd` daemon), if set, are loaded at boot from the `fwaffinity.conf` configuration text file located at: `$FWDIR/conf`. Edit the file by adding the following line:

```
n fwd <cpuid>
```

where `<cpuid>` is the number of the processing core to be set as the affinity of the `fwd` daemon. For example, to set core #2 as the affinity of the `fwd` daemon, add to the file:

```
n fwd 2
```

Reboot for the `fwaffinity.conf` settings to take effect.

**Configuring CoreXL**

**To enable/disable CoreXL:**

1. Run the `cpconfig` command.
2. Select Configure Check Point CoreXL.
3. Choose whether to enable or disable CoreXL.
4. Reboot the gateway.

**To configure the number of instances:**

1. Run the `cpconfig` command.
2. Select Configure Check Point CoreXL.
3. If CoreXL is enabled, choose to change the number of firewall instances.
   - If CoreXL is disabled, choose to enable CoreXL and then set the required number of firewall instances.
4. Reboot the gateway.

Note - In a clustered deployment, changing the number of kernel instances should be treated as a version upgrade.

**Command Line Reference**

**Affinity Settings**

Affinity settings controlled by the `fwaffinity_apply` script file, which executes automatically at boot. When you make a change to affinity settings, the settings will not take effect until you either reboot or manually execute the `fwaffinity_apply` script.

`fwaffinity_apply` executes affinity definitions according to the information in the `fwaffinity.conf` text file. To change affinity settings, edit the text file.
Note - If Performance Pack is running, interface affinities are only defined by Performance Pack's sim affinity command. The fwaffinity.conf interface affinity settings are ignored.

fwaffinity.conf

fwaffinity.conf is located in the $FWDIR/conf directory.

Syntax

Each line in the text file uses the same format: <type> <id> <cpu>

<table>
<thead>
<tr>
<th>Data</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;type&gt;</td>
<td>i</td>
<td>interface</td>
</tr>
<tr>
<td></td>
<td>n</td>
<td>Check Point daemon</td>
</tr>
<tr>
<td></td>
<td>k</td>
<td>kernel instance</td>
</tr>
</tbody>
</table>

| <id> | interface name if <type> = i |
|      | daemon name if <type> = n   |
|      | instance number if <type> = k |
|      | default interfaces that are not specified in another line |

| <cpuid> | <number> | number(s) of processing core(s) to be set as the affinity |
|         |         | all all processing cores are available to the interface traffic, daemon or kernel instance |
|         |         | ignore no specified affinity (useful for excluding an interface from a default setting) |
|         |         | auto Automatic mode See also Processing Core Allocation (on page 88). |

Note - Interfaces that share an IRQ cannot have different cores as their affinities, including when one interface is included in the default affinity setting. Either set both interfaces to the same affinity, or use ignore for one of them. To view the IRQs of all interfaces, run: fw ctl affinity -I -V -A.

fwaffinity_apply

fwaffinity_apply is located in the $FWDIR/scripts directory. Use the following syntax to execute the command: $FWDIR/scripts/fwaffinity_apply <option> where <option> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-q</td>
<td>Quiet mode - print only error messages.</td>
</tr>
</tbody>
</table>
### fw ctl affinity

The *fw ctl affinity* command controls affinity settings. However, *fw ctl affinity* settings will not persist through a restart of the Security Gateway.

To set affinities, execute *fw ctl affinity* `-s`.

To list existing affinities, execute *fw ctl affinity* `-l`.

**fw ctl affinity -s**

Use this command to set affinities.

*fw ctl affinity* `-s` settings are not persistent through a restart of the Security Gateway. If you want the settings to be persistent, either use *sim affinity* (a Performance Pack command - see the *R75.40VS Performance Pack Administration Guide* (http://supportcontent.checkpoint.com/solutions?id=sk76540) for details) or edit the fwaffinity.conf configuration file.

To set interface affinities, you should use *fw ctl affinity* only if Performance Pack is not running. If Performance Pack is running, you should set affinities by using the Performance Pack *sim affinity* command. These settings will be persistent. If Performance Pack's *sim affinity* is set to Automatic mode (even if Performance Pack was subsequently disabled), you will not be able to set interface affinities by using *fw ctl affinity* `-s`.

#### Syntax

```
fw ctl affinity -s <proc_selection> <cpuid>
```

*<proc_selection>* is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;pid&gt;</code></td>
<td>Sets affinity for a particular process, where <code>&lt;pid&gt;</code> is the process ID#</td>
</tr>
<tr>
<td><code>-n &lt;cpdname&gt;</code></td>
<td>Sets affinity for a Check Point daemon, where <code>&lt;cpdname&gt;</code> is the Check Point daemon name (for example: <em>fwd</em>)</td>
</tr>
<tr>
<td><code>-k &lt;instance&gt;</code></td>
<td>Sets affinity for a kernel instance, where <code>&lt;instance&gt;</code> is the instance's number.</td>
</tr>
<tr>
<td><code>-i &lt;interfacename&gt;</code></td>
<td>Sets affinity for an interface, where <code>&lt;interfacename&gt;</code> is the interface name (for example: <em>eth0</em>).</td>
</tr>
</tbody>
</table>

*<cpuid>* should be a processing core number or a list of processing core numbers. To have no affinity to any specific processing core, `<cpuid>` should be: *all*.

#### Note

- Setting an Interface Affinity will set the affinities of all interfaces sharing the same IRQ to the same processing core.
- To view the IRQs of all interfaces, run:  
  
  *fw ctl affinity -l -v -a*

#### Example

To set kernel instance #3 to run on processing core #5, run:

```
fw ctl affinity -s -k 3 5
```
fw ctl affinity

Use this command to list existing affinities. For an explanation of kernel, daemon and interface affinities, see CoreXL Administration (on page 87).

Syntax

fw ctl affinity -l [<proc_selection>] [<listtype>]

If <proc_selection> is omitted, fw ctl affinity -l lists affinities of all Check Point daemons, kernel instances and interfaces. Otherwise, <proc_selection> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;pid&gt;</td>
<td>Displays the affinity of a particular process, where &lt;pid&gt; is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Displays the affinity of a Check Point daemon, where &lt;cpdname&gt; is the Check Point daemon name (for example: fwd).</td>
</tr>
<tr>
<td>-k &lt;instance&gt;</td>
<td>Displays the affinity of a kernel instance, where &lt;instance&gt; is the instance's number.</td>
</tr>
<tr>
<td>-i &lt;interfacename&gt;</td>
<td>Displays the affinity of an interface, where &lt;interfacename&gt; is the interface name (for example: eth0).</td>
</tr>
</tbody>
</table>

If <listtype> is omitted, fw ctl affinity -l lists items with specific affinities, and their affinities. Otherwise, <listtype> is one or more of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>All: includes items without specific affinities.</td>
</tr>
<tr>
<td>-r</td>
<td>Reverse: lists each processing core and the items that have it as their affinity.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose: list includes additional information.</td>
</tr>
</tbody>
</table>

Example

To list complete affinity information for all Check Point daemons, kernel instances and interfaces, including items without specific affinities, and with additional information, run:

fw ctl affinity -l -a -v

fw ctl multik stat

The fw ctl multik stat and fw6ctl multik stat (multi-kernel statistics) commands show information for each kernel instance. The state and processing core number of each instance is displayed, along with:

- The number of connections currently being handled.
- The peak number of concurrent connections the instance has handled since its inception.
Appendix A

Appendix A: Security Before Firewall Activation

Achieving Security Before Firewall Activation

There are several scenarios in which a computer does not yet have a security policy installed and is vulnerable. Two features provide security during these situations: Boot Security, which secures communication during the boot period, and Initial Policy, which provides security before a security policy is installed for the first time. As a result, there is no point in time when the computer is left unprotected.

Boot Security

During the boot process, there is a short period of time (measured in seconds) between the point when the computer is capable of receiving communication (and can be attacked) and the point when the security policy is loaded and is enforced. During this time, the firewall Boot Security feature protects both the internal networks behind the Security Gateway, and the computer itself. Boot Security is provided by two elements working together:

- Control of IP Forwarding on boot
- Default Filter

The Default Filter also provides protection in a scenario where firewall processes are stopped for maintenance.

Control of IP Forwarding on Boot

For networks protected by a Security Gateway, protection is available at boot by disabling IP forwarding in the OS kernel. This ensures that there will never be a time when IP Forwarding is active and no security policy is enforced. This ensures that networks behind the gateway are safe.

Disabling IP Forwarding protects networks behind the Security Gateway computer, but it does not protect the Security Gateway computer itself. For this purpose, the Security Gateway implements a Default Filter during the period of vulnerability.

The Default Filter

When a Security Gateway boots with the Default Filter, the following sequence is performed:

1. Computer boots up.
2. Boot security takes effect (Default Filter loads and IP Forwarding is disabled).
3. Interfaces are configured.
4. Security Gateway services start.
The computer is protected as soon as the Default Filter loads.

There are several Default Filters:

- General Filter accepts no inbound communication (this is the default option).
- Drop Filter accepts no inbound or outbound communication. This filter drops all communications into and out of the gateway during a period of vulnerability. Note, however, that if the boot process requires that the gateway communicate with other hosts, then the Drop Filter should not be used.
- Default Filter for IPSO allowing SSH incoming communication to support remote Administration.
- Default Filter for IPSO allowing HTTPS incoming communication to support remote Administration.
- Default Filter for IPSO allowing SSH and HTTPS incoming communication to support remote Administration.

The appropriate Default Filter should be selected based on platform and communication needs. The General Filter is selected by default.

The Default Filter also provides anti-spoofing protection for the Security Gateway. It ensures that packets whose source are the Security Gateway computer itself have not come from one of its interfaces.

**Changing the Default Filter to a Drop Filter**

For a typical setup there are two Default Filters: `defaultfilter.boot` and `defaultfilter.drop`. They are located in `$FWDIR/lib`.

To change the Default Filter:
1. Copy over and rename the relevant desired Default Filter Inspect file (`defaultfilter.boot` or `defaultfilter.drop`) to `$FWDIR/conf/defaultfilter.pf`
2. Compile the Default Filter by running the command:
   ```
   fw defaultgen
   ```
   The output will be in `$FWDIR/state/default.bin`
3. Run `fwboot bootconf get_def` to print the Default Filter file path.
4. Copy `default.bin` to the Default Filter file path.
5. If the security policy has not yet been installed, run `cpconfig` to regenerate the Initial Policy.

**Defining a Custom Default Filter**

For administrators with Inspect knowledge, you can define your own Default Filter.

To define a Default Filter:
1. Create an Inspect script named `defaultfilter pf` in `$FWDIR/conf`:
Important - Ensure that the script does not perform any of the following functions:

- Logging
- Authentication
- Encryption
- Content security

1. Continue from step 2 of Changing the Default Filter to a Drop Filter.
You must ensure that your security policy does not interfere with the boot process.

**Using the Default Filter for Maintenance**

It is sometimes necessary to stop firewall processes for maintenance, and it is impractical to disconnect the Security Gateway computer from the network (for example, the computer may be at a remote location).

The `cpstop-fwflag-default` and `cpstop-fwflag-proc` commands allow Security Gateway processes to be temporarily stopped for remote maintenance without exposing the computer to attack.

During maintenance, the Default Filter allows open connections to the gateway to remain open, without dropping them.

**The Initial Policy**

Until the Security Gateway administrator installs the security policy on the gateway for the first time, security is enforced by an Initial Policy. The Initial Policy operates by adding "implied rules" to the Default Filter. These rules forbid most communication yet allows the communication needed for the installation of the security policy. The Initial Policy also protects a gateway during Check Point product upgrades, when a SIC certificate is reset on the gateway, or in the case of a Check Point product license expiration.

Note - During a Check Point upgrade, a SIC certificate reset, or license expiration, the Initial Policy overwrites the user-defined policy.

The sequence of actions during boot of the Security Gateway computer until a security policy is loaded for the first time:

1. The computer boots up.
2. The Default Filter loads and IP Forwarding is disabled.
3. The Interfaces are configured.
4. Security Gateway services start.
5. The Initial policy is fetched from the local gateway.
6. SmartConsole clients connect or Trust is established, and the security policy is installed.

The Initial Policy is enforced until a user-defined policy is installed, and is never loaded again. In subsequent boots, the regular policy is loaded immediately after the Default Filter.

There are different Initial Policies for standalone and distributed setups. In a standalone configuration, where the Security Management server and the Security Gateway are on the same computer, the Initial Policy allows CPMI communication only. This permits SmartConsole clients to connect to the Security Management server.

In a distributed configuration, where the Primary Security Management server is on one computer and the Security Gateway is on a different computer, the Initial Policy allows the following:

- **Primary Security Management server computer** — allows CPMI communication for SmartConsole clients.
- **Security Gateway** — allows cpd and fwd communication for SIC communication (to establish trust) and for Policy installation.

In a distributed configuration, the Initial Policy on the Security Gateway does not allow CPMI connections. The SmartConsole will not be able to connect to the Security Management server if the SmartConsole must access the Security Management server through a gateway running the Initial Policy.

There is also an Initial Policy for a Secondary Security Management server (Management High Availability). This Initial Policy allows CPMI communication for SmartConsole clients and allows cpd and fwd communication for SIC communication (to establish trust) and for Policy installation.

### Managing Default Filter and Initial Policy

**Verifying Default Filter or Initial Policy Loading**

You can verify that the Default Filter and/or Initial Policy are loaded.
To verify loading of the Default Filter or Initial Policy:
1. Boot the system.
2. Before installing another security policy, type the following command:

   `FWDIR/bin/fw stat`

   The command’s output should show that `defaultfilter` is installed for the Default Filter status. It should show that `InitialPolicy` is installed for the Initial Policy.

**Unloading Default Filter or Initial Policy**

To unload a Default Filter or an Initial Policy from the kernel, use the same command that is used for unloading a regular policy. Do this only if you are certain that you do not need the security provided by the Default Filter or an Initial Policy.

**To unload the Default Filter locally:**
- Run the `fw unloadlocal` command.

**To unload an Initial Policy from a remote Security Management machine:**
- Run the following command on the Security Management server:

  `fwm unload <hostname>`

  where `hostname` is the SIC_name of the gateway.

**Troubleshooting: Cannot Complete Reboot**

In certain configurations the Default Filter may prevent the Security Gateway computer from completing the reboot following installation.

First, examine the Default Filter and verify that the Default Filter allows traffic that the computer needs in order to boot.

If the boot process cannot complete successfully, remove the Default Filter as follows:
1. Reboot in **single user** mode (for UNIX) or **Safe Mode With No Networking** (for Windows 2000).
2. Ensure that the Default Filter does not load in future boots. Use the command

   `fwbootconf bootconf Set_def`

3. Reboot.

**Command Line Reference**

**control_bootsec**

Enables or disables Boot Security. The command affects both the Default Filter and the Initial Policy.

**Usage**

```
$FWDIR/bin/control_bootsec [-r] [-g]
```

**options control_bootsec**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-r</code></td>
<td>Removes boot security</td>
</tr>
<tr>
<td><code>-g</code></td>
<td>Enables boot security</td>
</tr>
</tbody>
</table>

**fwboot bootconf**

Use the `fwboot bootconf` command to configure boot security options. This command is located in `$FWDIR/boot`. 
Appendix A: Security Before Firewall Activation

Usage

```
$FWDIR/bin/fwboot bootconf <command> [value]
```

**options fwboot bootconf**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get_ipf</td>
<td>Reports whether firewall controls IP Forwarding.</td>
</tr>
<tr>
<td></td>
<td>• Returns 1 if IP Forwarding control is enabled on boot.</td>
</tr>
<tr>
<td></td>
<td>• Returns 0 if IP Forwarding is not controlled on boot.</td>
</tr>
<tr>
<td>Set_ipf 0/1</td>
<td>Turns off/on control of IP forwarding for the next boot.</td>
</tr>
<tr>
<td></td>
<td>0 - Turns off</td>
</tr>
<tr>
<td></td>
<td>1 - Turns on</td>
</tr>
<tr>
<td>Get_def</td>
<td>Returns the full path to the Default Filter that will be used on boot.</td>
</tr>
<tr>
<td>Set_def &lt;filename&gt;</td>
<td>Loads &lt;filename&gt; as the Default Filter in the next boot. The only safe, and recommended, place to put the default.bin file is $FWDIR\boot. (The default.bin filename is a default name.)</td>
</tr>
</tbody>
</table>

**Note** - Do NOT move these files.

comp_init_policy

Use the `comp_init_policy` command to generate and load, or to remove, the Initial Policy.

This command generates the Initial Policy. It ensures that it will be loaded when the computer is booted, or any other time that a Policy is fetched, for example, at `cpstart`, or with the `fw fetch localhost` command. After running this command, `cpconfig` adds an Initial Policy if there is no previous Policy installed.

**Usage**

```
$FWDIR/bin/comp_init_policy [-u | -g]
```

**options comp_init_policy**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>Removes the current Initial Policy, and ensures that it will not be generated in future when <code>cpconfig</code> is run.</td>
</tr>
<tr>
<td>-g</td>
<td>Generates the Initial Policy and ensures that it is loaded the next time a policy is fetched (at <code>cpstart</code>, or at next boot, or via the <code>fw fetch localhost</code> command). After running this command, <code>cpconfig</code> adds an Initial Policy when needed.</td>
</tr>
</tbody>
</table>

The `comp_init_policy -g` command will only work if there is no previous policy. If there is a policy, make sure that after removing the policy, you delete the folder `$FWDIR\state\local\FW1`. The `$FWDIR\state\local\FW1` folder contains the policy that will be fetched when `fw fetch localhost` is run.

The `fw fetch localhost` command is the command that installs the local policy. `cpstart, comp_init_policy` creates the initial policy, but has a safeguard so that the initial policy will not overwrite a regular user policy (since initial policy is only used for fresh installations or upgrade). For this reason, you must delete the `$FWDIR\state\local\FW1` directory if there is a previous policy, otherwise `comp_init_policy` will detect that the existing user policy and will not overwrite it.

If you do not delete the previous policy, yet perform the following commands … … the original policy will still be loaded.
comp_init_policy -g + fw_fetch localhost
comp_init_policy -g + cpstart
comp_init_policy -g + reboot

cpstop -fwflag default and cpstop -fwflag proc

To stop all firewall processes but leave the Default Filter running, use `cpstop -fwflag -default`. To stop all Security Gateway processes but leave the security policy running, use `cpstop -fwflag -proc`.

To stop and start all Check Point processes, use `cpstop` and `cpstart`. These commands should be used with caution.

On Win32 platforms, use the Services applet in the Control Panel to stop and start Check Point Services.

**Usage**

`cpstop -fwflag [-default | -proc]`

**Options for fwflag**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-default</td>
<td>Kills firewall processes (fwd, fwm, vpnd, snmpd etc.). Logs, kernel traps, resources, and all security server connections stop working. The security policy in the kernel is replaced with the Default Filter.</td>
</tr>
<tr>
<td>-proc</td>
<td>Kills firewall processes (fwd, fwm, vpnd etc.). Logs, kernel traps, resources, and all security server connections stop working. The security policy remains loaded in the kernel. Therefore allow, reject, or drop rules that do not use resources, but only services, continue to work.</td>
</tr>
</tbody>
</table>
Appendix B

Appendix B: Legacy Authentication

This section covers how to work with legacy authentication methods.

In This Appendix

- Configuring Authentication: 102
- Authentication Schemes: 103
- Authentication Methods: 107
- Creating Users and Groups: 115
- Configuring Authentication Tracking: 115
- Configuring Policy for Groups of Windows Users: 116

Configuring Authentication

On the Security Gateway, you can configure authentication in one of two places:

- In the Gateway Properties window of a gateway in Authentication. In the Authentication page, you can allow access to users who authenticate with a Check Point Password, SecurID, OS Password, RADIUS server, or TACACS server. Authentication using Client Certificates from the Internal Certificate Authority is enabled by default in addition to the selected method.

- Some blades have their own authentication settings. Configure this in the Gateway Properties window of a gateway under <name of the blade> > Authentication. For example, configure the authentication method for IPsec VPN clients in Gateway Properties > IPsec VPN > Authentication. If you select an authentication method for the blade, that is the method that all users must use to authenticate to that blade. You can configure other authentication methods that users must use for different blades on different pages.

If you do not make a selection on the Authentication page for a specific blade, the Security Gateway takes authentication settings for the blade from the main gateway Authentication page.

Note - In previous releases there was no option to configure an authentication setting for a specific blade. But from R75 and higher, if you configure an authentication method for a specific blade, the settings on this page do not apply at all to that blade.

How the Gateway Searches for Users

If you configure authentication for a blade from the main Security Gateway Legacy Authentication page, the Security Gateway searches for users in a standard way when they try to authenticate. The gateway searches:

1. The internal users database.
2. If the specified user is not defined in this database, the gateway queries the User Directory (LDAP) servers defined in the Account Unit one at a time, and according to their priority.
3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

If you configure an authentication method for a specific blade, the gateway searches for users according to the user groups that are used for authorization in that blade.

For example, in Mobile Access, the gateway looks at the Mobile Access policy to see which user groups are part of the policy. When the gateway tries to authenticate a user, it starts to search for users in the databases related to those user groups.
In IPsec VPN, the gateway looks at the Remote Access VPN Community to see which user groups are included. It starts to search for users in the databases related to those user groups.

A search based on the authentication scheme is faster, with better results. You can have users with the same user name in unrelated groups. The gateway will know which user is relevant for the blade based on the user groups.

**Authentication Schemes**

Security Gateways authenticate individual users using credentials and manages them using different authentication schemes. All of the authentication schemes require the provision of a user name and password. While some schemes involve storing the passwords on the gateway, others are stored on external servers.

The following sections describe the various authentication schemes supported by Check Point.

**Check Point Password**

The Security Gateway can store a static password in the local user database of each user configured in Security Management server. No additional software is required.

**Operating System Password**

The Security Gateway can authenticate using the user name and password that is stored on the operating system of the machine on which the Security Gateway is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

**RADIUS**

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

Using RADIUS, the Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users.

The RADIUS protocol uses UDP to communicate with the gateway. RADIUS servers and RADIUS server group objects are defined in SmartDashboard.

**Configuring a Security Gateway to use RADIUS Authentication**

To configure a Security Gateway to use RADIUS authentication:

1. In SmartDashboard, create a RADIUS Host object by selecting Manage > Network Objects > New > Node > Host.
2. Name the Host object and assign it an IP address.
3. Create a RADIUS Server object by selecting Manage > Server and OPSEC Applications > New > RADIUS, and configure the following:
   a) Name the RADIUS Server object.
   b) Associate the RADIUS Server object with the RADIUS Host object created in step 1.
   c) Assign the Service by selecting either the RADIUS on port 1645 or NEW-RADIUS on port 1812 service. (The default setting is RADIUS, however the RADIUS standards group recommends using NEW-RADIUS, because port 1645 can conflict with the datametrics service running on the same port.)
   d) Assign the same Shared Secret that you configured on the actual RADIUS server.
   e) Select either RADIUS Ver. 1.0 Compatible, which is RFC 2138 compliant, or RADIUS Ver. 2.0 Compatible, which is RFC 2865 compliant.
   f) Assign the RADIUS server's Priority if you are employing more than one RADIUS Authentication server.
Appendix B: Legacy Authentication

4. Right-click the gateway object and select Edit > Authentication.
5. Enable RADIUS authentication.
6. Define a user group by selecting Manage > Users & Administrators > New > User Group (for example, RADIUS_Users).
8. Enable RADIUS authentication for users without Security Gateway user accounts by creating an External User Profile. Select Manage > Users and Administrators > New > External User Profile > Match all users or Match by domain. To support more than one external authentication scheme, define your External User Profiles with the Match By Domain setting.
9. For all User Profiles and Templates, configure the following:
   a) In the General tab, type the default login name for the RADIUS server. (When configuring Match all users as an External User Profile, the name "generic" is automatically assigned.)
   b) In the Personal tab, adjust the Expiration Date.
   c) In the Authentication tab, select RADIUS from the drop-down list.
   d) In the Groups tab, add the User Profile to the RADIUS group.
10. Verify that communication between the firewall and the RADIUS server are not defined in the Address Translation Rule Base.
11. Save, verify, and install the policy.

Granting User Access Using RADIUS Server Groups

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

To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, RAD_<group to which the RADIUS users belong>) to which the users belong. Although other RADIUS attributes can be used, by default the Class attribute is used (IETF RADIUS attribute number 25).

To grant access using RADIUS server groups:
2. Create an External User Profile by selecting Manage > Users and Administrators > New > External User Profile > Match all users. This is the generic user.
3. In the Authentication tab, select RADIUS as the Authentication Scheme and then select the created RADIUS server (not the node) from the drop-down list.
4. Define the required RADIUS user groups by selecting Manage > Users & Administrators > New > User Group. The name of the group must be in the format: RAD_<group to which the RADIUS users belong>. Ensure the group is empty.
5. Create the required Rule Base rules to allow access to RADIUS users.
6. Save the changes, and exit SmartDashboard.
8. On the Security Management server, use the Graphical Database Tool (GUIdbEdit) to change the value of the add_radius_groups attribute from false to true.
10. Install the policy.
11. On the RADIUS server, modify the RADIUS users to include a class RADIUS attribute on the users Return list that corresponds to the user group that they access.

To use a different attribute instead of the class attribute, do one of the following:
1. On the Security Gateway, use GUIdbEdit to modify the value of the firewall_properties attribute radius_groups_attr to the new RADIUS attribute.
2. On the RADIUS server, ensure that you use the same RADIUS attribute (on the users’ Return list that corresponds to the Firewall user group that they access).

**Associating a RADIUS Server with Security Gateway**

You can associate users with the Radius authentication server in the User Properties Authentication tab. You can also associate a gateway with a Radius server so that this overrides the User to Radius server association. This is performed by editing the database using the `dbedit` command.

**To associate one or more Radius servers to a gateway:**

1. Run the `dbedit` command as follows:
   
   ```
   modify network.objects <gw obj> radius_server
   servers:<radius obj>
   ```

2. To switch off the Radius to the Security Gateway association so that the user always authenticates to the Radius server specified in the User Properties Authentication tab, switch off another attribute in the database by running the `dbedit` command:
   
   ```
   modify users <user obj> use_fw_radius_if_exist false
   ```

**SecurID**

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

Using SecurID, the Security Gateway forwards authentication requests by remote users to the ACE/server. ACE manages the database of RSA users and their assigned hard or soft tokens. The gateway acts as an ACE/Agent 5.0 and directs all access requests to the RSA ACE/server for authentication. For additional information on agent configuration, refer to ACE/server documentation.

There are no specific parameters required for the SecurID authentication scheme.

**Configuring a Security Gateway to use SecurID Authentication**

**To configure a Security Gateway to use SecurID:**

1. Generate and copy the `sdconf.rec` file from the ACE/Server to:
   - `/var/ace/sdconf.rec` on UNIX, Linux or IPSO
   - `%SystemRoot%\System32\sdconf.rec` on Windows
2. In SmartDashboard, right-click the gateway object and select **Edit >Authentication** page.
3. Enable SecurID authentication.
4. Define a user group by selecting **Manage > Users & Administrators > New > User Group** (for example, SecurID_Users).
5. Enable SecurID authentication for Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.
6. Enable SecurID authentication for users without Security Gateway user accounts by creating an External User Profile. Select **Manage > Users and Administrators > New > External User Profile > Match all users** or **Match by domain**. If you support more than one external authentication scheme, set up your External User Profiles with the **Match By Domain** setting.
7. For all User Profiles and Templates, configure the following:
   a) In the **General** tab, enter the default login name for the ACE/Server. (When configuring **Match all users** as an External User Profile, the name "generic" is automatically assigned).
   b) In the **Personal** tab, change the **Expiration Date**.
   c) In the **Authentication** tab, select SecurID from the drop-down list.
   d) In the **Groups** tab, add the User Profile to the SecurID group.
8. **Verify that communication between the firewall and the ACE/Server are not NATed in the Address Translation Rule Base.**

9. **Save, verify, and install the policy.**

   **Note** - When a Security Gateway has multiple interfaces, the SecurID agent on the Security Gateway sometimes uses the wrong interface IP to decrypt the reply from the ACE/Server, and authentication fails.

   To overcome this problem, place a new text file, named `sdopts.rec`, in the same directory as `sdconf.rec`. The file should contain the `CLIENT_IP=<ip>` line, where `<ip>` is the primary IP address of the Security Gateway, as defined on the ACE/Server. This is the IP address of the interface to which the server is routed.

---

### TACACS

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication scheme that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. The TACACS server, which stores user account information, authenticates users. The system supports physical card key devices or token cards and Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

---

### Configuring a Security Gateway to use TACACS+ Authentication

**To configure a Security Gateway to use TACACS+:**

1. In SmartDashboard, create a TACACS Host object by selecting **Manage > Network Objects > New > Node > Host**

2. Name the Host object and assign it an IP address.

3. Create a TACACS server by selecting **Manage > Server and OPSEC Applications > New… > TACACS…**, and configure the following:

   a) **Name** the TACACS server object.
   
   b) Associate the TACACS server object with the TACACS Host object created in step 1.
   
   c) Select the **Type** of TACACS you want to run. (The default is TACACS, but TACACS+ is recommended).

   d) Assign the **Service**. Match the TACACS service (UDP or TCP) to the **Type** selected in step c.

4. Right-click the gateway object and select **Edit > Authentication**.

5. **Enable TACACS authentication.**

6. Define a user group by selecting **Manage > Users & Administrators > New > User Group** (for example, `TACACS_Users`).

7. Enable TACACS authentication for Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.

8. Enable TACACS authentication for users without Security Gateway user accounts by creating an External User Profile. Select either **Manage > Users and Administrators > New > External User Profile > Match all users** or **Match by domain**. If more than one external authentication scheme is supported, set up your External User Profiles using the **Match By Domain** setting.

9. For all User Profiles and Templates, configure the following:

   a) In the **General** tab, enter the default login name for the TACACS Server. (When configuring **Match all users** as an External User Profile, the name “generic” is automatically assigned).

   b) In the **Personal** tab, change the **Expiration Date**.

   c) In the **Authentication** tab, select **TACACS** from the drop-down list.

   d) In the **Groups** tab, add the User Profile to the TACACS group.

10. **Verify that communication between the firewall and the TACACS server is not NATed in the Address Translation Rule Base.**
11. Save, verify, and install the policy.

**Undefined**

The authentication scheme for a user can be defined as undefined. If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

**Authentication Methods**

Instead of creating a security rule that simply allows or denies connections, the firewall administrator can request that clients authenticate when they try to access specific network resources.

There are three authentication methods available: user, client and session. These methods differ in the services provided, the logon mechanism, and the overall user experience. Each method can be configured to connect and authenticate clients to the gateway before the connection is passed to the desired resource (a process known as nontransparent authentication). Alternatively, each method can be configured to connect clients directly to the target server (a process known as transparent authentication).

**User Authentication**

User Authentication provides authentication for Telnet, FTP, HTTP, and rlogin services. By default, User Authentication is transparent. The user does not connect directly to the gateway, but initiates a connection to the target server.

The following is a typical User Authentication method workflow:

1. The Security Gateway intercepts the communication between the client and server.  
2. The Security Gateway prompts the user for a user name and password.  
3. If the user successfully authenticates, the gateway passes the connection to the remote host. If incorrect credentials are presented, the user is prompted to re-enter the data. After a predefined number of unsuccessful connection attempts, the connection is dropped.  
4. The remote host prompts the user for a user name and password.

**Note** - When configuring user objects, you can set the locations that they are allowed to access, however, this can lead to a conflict with security rules that require some form of authentication. See also: Resolving Access Conflicts (on page 112)

**Configuring User Authentication**

**To configure user authentication:**

1. Configure authentication for required users and groups and install the user database. For detailed information, refer to Creating Users and Groups (on page 115).
2. Define a user authentication access rule as follows:
   a) Right-click in the **Source** column, select **Add object > Add legacy user access** and then select the group.
   b) To restrict the location of authenticating users, select **Restrict To** and the host, group of hosts, network or group of networks that users can access in the **Location** section of the same window.
   c) In the **Service** field, select the services you wish to authenticate.
   d) In the **Action** column, select **Legacy > User Auth**.
3. Double-click the **Action** column to edit the **User Authentication Action Properties**.
4. If required, adjust the **User Authentication session timeout** from the **Authentication** page of the Security Gateway object.
5. Install the security policy: **Policy > Install**.
Importance of Rule Order in User Authentication

When defining user authentication rules for Telnet, FTP, HTTP, and RLOGIN services, if there are other non-authentication rules that use these services, ensure that the user authentication rule is located last amongst these rules.

Session Authentication

Session Authentication can be used for any service, however, a Session Authentication agent is required to retrieve a user's identity. The Session Authentication agent is normally installed on the authenticating client, whereby the person who initiates the connection to the destination host, supplies the authentication credentials. Session authentication requires an authentication procedure for each connection, however, the Session Authentication agent can also be installed on the destination machine, or on some other machine in the network, thereby allowing the user at that machine to provide the user name and password.

The following is a typical Session Authentication workflow:

1. The user initiates a connection directly to the server.
2. The Security Gateway intercepts the connection.
3. The Session Authentication agent challenges the user for authentication data and returns this information to the gateway.
4. If the authentication is successful, the Security Gateway allows the connection to pass through the gateway and continue to the target server.

   Note - When configuring user objects, you can set the locations that they are allowed to access. This can lead to conflicts with security rules that require a form of authentication. See also Resolving Access Conflicts (on page 112)

Configuring Session Authentication

To configure session authentication:

1. If using the Session Authentication Agent, install and configure it for all machine desktops with Session Authentication enabled.
2. Configure the users and groups for authentication, and install the user database. Refer to Creating Users and Groups (on page 115) for more information.
3. From the Authentication page, edit the Check Point Gateway object that represents the gateway and enable the required authentication schemes. The gateway must support all of the user defined authentication schemes. For example, if some users must provide a Check Point password, and others RADIUS authentication, select both schemes.
4. Define a Session Authentication access rule by doing the following:
   a) Right-click in the Source column, select Add object > Add legacy user access and then the group. Do not close the window.
   b) To restrict the location of authenticating users, in the Location section of the same window, select Restrict To and the host, group of hosts, network or group of networks that users can access.
   c) In the Service field, select the services you want to authenticate.
   d) In the Action column, select Legacy > Session Auth.
5. Double-click the Action column to edit the User Authentication Action Properties.
7. Install the security policy.

Installing and Configuring Session Authentication Agent

To install and configure the Session Authentication Agent:

1. Install the Session Authentication agent from the DVD.
   - If the Session Authentication agent is installed on the authenticating client, users who want to connect to the destination host provide the authentication credentials.
Appendix B: Legacy Authentication

- If Session Authentication agent is installed on the destination machine or on some other machine in the network, the user at the machine on which the Agent is installed is prompted to provide authentication credentials.

2. On Windows machines, double-click the Session Authentication agent icon in the system tray. The Session Authentication window.

3. Click Configure. The Configuration window opens and displays the Passwords tab. Specify how often the user is prompted to provide their password. One-time passwords (such as SecurID) cannot be cached.

4. Select one of the following options:
   - **Every request**: The user is prompted for a password each time that the Security Gateway requests authentication. Each time that the user initiates a session for which a Session Authentication Rule applies, the user is prompted for the password. No password caching occurs.
   - **Once per session**: The user is prompted for the password once per Session Authentication Agent session. Once the user provides the password, the Session Authentication agent caches the password indefinitely. This option cannot be used with one-time passwords. If the Session Authentication Agent session is closed and then restarted, the user must provide the password again.
   - **After minutes of inactivity**: Similar to the Once per session option, however, the user is prompted again for the password if there has been no authentication request over a specified time interval.

5. In the Configuration window, select the Allowed FireWall-1 tab and specify the Security Gateways for which the Session Authentication agent can provide authentication services.

6. Select one of the following options:
   - **Any IP Address**: The Session Authentication agent can provide authentication services for any Security Gateway.
   - **IP Address**: The Session Authentication agent can provide authentication services for only a Security Gateway running on a user-specified IP address (you can specify up to three IP addresses).

7. In the Configuration window, select the Options tab and specify whether to allow clear passwords and to resolve addresses.

8. Select the appropriate option and click OK.

Starting the Session Authentication Agent

To start the Session Authentication Agent:
1. From the Windows system tray, select the minimized Session Authentication Agent icon.
2. Configure the Session Authentication Agent and/or receive authentication requests from a Security Gateway.

**Client Authentication**

Client Authentication can authenticate any service. It enables access from a specific IP address for an unlimited number of connections. The client user performs the authentication process, but it is the client machine that is granted access. Client Authentication is less secure than user authentication because it permits access for multiple users and connections from authorized IP addresses or hosts. Authorization is performed on a per machine basis for services that do not have an initial login procedure. The advantages of Client Authentication are that it can be used for an unlimited number of connections, for any service, and is valid for any length of time.

> **Note** - When configuring user objects, you can set the locations that users can access, however, this can cause problems with security rules that require some form of authentication. See also Resolving Access Conflicts (on page 112)

Client Authentication works with all sign on methods. The following table shows how different sign on methods provide choice when selecting an authentication method for authenticated and other services. For sign on methods other than Manual Client Authentication, the gateway is transparent to the users and they authenticate directly to the destination host.
## Client Authentication Sign On Methods

<table>
<thead>
<tr>
<th>Client Authentication Sign On Method</th>
<th>Authentication Method for authenticated services: Telnet, FTP, HTTP, RLOGIN</th>
<th>Authentication Method for other services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Telnet to port 259 on gateway HTTP to port 900 on gateway</td>
<td>Telnet to port 259 on gateway HTTP to port 900 on gateway</td>
</tr>
<tr>
<td>Partially automatic</td>
<td>User Authentication</td>
<td>Not available</td>
</tr>
<tr>
<td>Fully automatic</td>
<td>User Authentication</td>
<td>Session Authentication</td>
</tr>
<tr>
<td>Agent automatic</td>
<td>Session Authentication</td>
<td>Session Authentication</td>
</tr>
<tr>
<td>Single Sign on</td>
<td>UserAuthority</td>
<td>UserAuthority</td>
</tr>
</tbody>
</table>

The following are the two Client Authentication sign on options:

- **Standard Sign on**: Enables users to access all services permitted by the rule without authenticating for each service.
- **Specific Sign on**: Enables users to access only the services that they specify when they authenticate, even if the rule allows more than one service. If the user wants to use another service, they must re-authenticate for that specific service.

At the end of an authentication session, the user can sign off. When a user signs off, they are disconnected from all services and the remote host.

## Manual Sign On

Manual Sign On is available for any service that is specified in the Client Authentication rule. The user must first connect to the gateway and authenticate in one of the following two ways:

1. Through a Telnet session to the gateway on port 259.
2. Through an HTTP connection to the gateway on port 900 and a Web browser. The requested URL must include the gateway name and the port number, for example, `http://Gateway:900`.

   a) The following example shows Client Authentication using a Standard Manual Sign On method. In this example, before opening a connection to the destination host, the user `fbloggs` first authenticates to `london`, the Security Gateway.

   ```
tower 1% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: fbloggs
FireWall-1 Password: ********
User authenticated by FireWall-1 auth.
```

   Choose:
   - (1) Standard Sign On
   - (2) Sign Off
   - (3) Specific Sign On

   Enter your choice: 1

   User authorized for standard services (1 rules)
   Connection closed by foreign host.

   b) The following example shows Client Authentication using a Specific Manual Sign On method. In this example, two services are specified: `rstat` and `finger` (each one to a different host).
Wait Mode

Wait mode is a Client Authentication feature for Manual Sign On when the user initiates a client authenticated connection with a Telnet session on port 259 on the gateway.

Wait mode eliminates the need to open a new Telnet session in order to sign off and withdraw client authentication privileges. In Wait mode, the initial Telnet session connection remains open so long as client authentication privileges remain valid. Client authentication privileges are withdrawn when the Telnet session is closed.

The Security Gateway keeps the Telnet session open by pinging the authenticating client. If for some reason the client machine stops running, the gateway closes the Telnet session and client authentication privileges from the connected IP address are withdrawn.

Enable Wait mode works only with client authentication rules that specify Standard Sign On. In Enable Wait mode, client authentication rules that require Specific Sign On are not applied.

Partially Automatic Sign On

Partially Automatic Sign On is available for authenticated services (Telnet, FTP, HTTP and RLOGIN) only if they are specified in the client authentication rule. If the user attempts to connect to a remote host using one of the authenticated services, they must authenticate with User Authentication. When using Partially Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.

Fully Automatic Sign On

Fully Automatic Sign On is available for any service only if the required service is specified in the client authentication rule. If the user attempts to connect to a remote host using an authenticated service (Telnet, FTP, HTTP, and RLOGIN), they must authenticate with User Authentication. If the user attempts to connect to a remote host using any other service, they must authenticate through a properly installed Session Authentication agent. When using Fully Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.

Agent Automatic Sign On

Agent Automatic Sign On is available only if the required service is specified in the Client Authentication rule, and the Session Authentication agent is properly installed.

If a user attempts to connect to a remote host using any service, they must authenticate through a Session Authentication agent.
Single Sign On

Single Sign On is available for any service only if the required service is specified in the Client Authentication rule and UserAuthority is installed.

Single Sign On is a Check Point address management feature that provides transparent network access. The Security Gateway consults the user IP address records to determine which users are logged on to any given IP address. When a connection matches a Single Sign On enabled rule, the gateway queries UserAuthority with the packet's source IP. UserAuthority returns the name of the user who is registered to the IP. If the user's name is authenticated, the packet is accepted, if not, it is dropped.

Configuring Client Authentication

To configure basic client authentication:

1. Configure the required users and groups for authentication and install the user database. Refer to Creating Users and Groups (on page 115) for details.
2. From the Authentication page, edit the Check Point Gateway object that represents the Security Gateway and enable the required authentication schemes. The gateway must support all of the user defined authentication schemes. For example, if some users must provide a Check Point password, and others RADIUS authentication, select both schemes.
3. Define a Client Authentication access rule as follows:
   a) Right-click in the Source column, select Add object > Add legacy user access and then the group. Do not close the window.
   b) To restrict the location of authenticating users, in the Location section of the same window, select Restrict To and the host, group of hosts, network or group of networks that users can access.
   c) In the Service field, select the services you want to authenticate.
   d) In the Action column, select Legacy > Client Auth.
4. For Partially or Fully Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.
6. Place all Client Authentication Rules above the rule that prevents direct connections to the Security Gateway (the Stealth Rule) to ensure that they have access to the Security Gateway.
8. Install the security policy.

Enabling Client Authentication Wait Mode

When using Manual Sign On and the user authenticates with a Telnet session to port 259 on the gateway, Wait mode eliminates the need to open a new Telnet session in order to sign off and withdraw client authentication privileges.

To enable Wait mode:

1. From the Authentication page, edit the Check Point Gateway object that represents the Security Gateway and select Enable Wait Mode for Client Authentication. In Client Authentication Wait mode, the Security Gateway monitors the Telnet connection to port 259 of the gateway by pinging the user's host.
2. Define rules to enable pinging as follows:
   - Enable the echo-request service from the Security Gateway to the user's host.
   - Enable the echo-reply service from the user's host to the Security Gateway.

Resolving Access Conflicts

When configuring users, you define those locations that they can access. However, by doing so, you disallow access to all unspecified locations, which can cause conflicts with security rules that require authentication.
For example, if a rule grants authenticated access to users from Marketing_net to Finance_net, but in the user’s Location tab connections are only permitted within Marketing_net, the firewall does not know whether to allow the authentication request when the user tries to connect to Finance_net.

You can specify how to resolve this conflict by editing the Authentication Action Property of this rule. You can define this property for both the Source and Destination of the rule.

To resolve access conflicts:
1. Right-click the Action field of a rule using some form of authentication and select Edit Properties.
2. Do one of the following:
   - To apply the more restrictive access privileges specified in the rule and in the Location tab of each user’s User Properties window, select Intersect with User Database.
   - To allow access according to the location specified in the rule, select Ignore User Database.

**Authorizing All Standard Sign On Rules**

By default, the Partially or Fully Automatic sign on methods open one rule following successful authentication (the rule for which the sign on was initiated). For example, if a user successfully authenticates according an automatic sign on rule, the user can work with the services and destinations permitted only by that rule.

You can configure Security Gateway to automatically open all Standard Sign On rules following successful authentication using Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules that define that user and source are available. The user can then work with all of the services and destinations permitted by the relevant rules; the Security Gateway knows which user is at the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules following successful Partially or Fully Automatic authentication, use the GUIdbedit Database Tool to change a setting in the database.

**To authorize all standard sign on rules:**
1. Access the GUIdbedit Database Tool from the same directory on your local drive as where SmartConsole is installed.
2. Open GUIdbedit.
3. Search for the automatically_open_ca_rules field.
4. Set the value to true. The new value takes effect after you install the security policy.

**Changing the Client Authentication Port Number**

**To change the Client Authentication port number:**
1. Stop Check Point services by running the cpstop command.
2. Modify the port number in the Manage > Service > Show > TCP Services window for the following services:
   - To modify the port number for Telnet sign on, change the port number of the FW1_clntauth_telnet service.
   - To modify the port number for HTTP sign on, change the port number of the FW1_clntauth_http service.
   These are special Check Point services provided as part of the Client Authentication feature.
3. Use a simple text editor to edit the $FWDIR/conf/fwauthd.conf file. Change the port number of the Client Authentication application to the same port number defined in step 2.
4. Do one of the following:
   - For Telnet Sign On, modify the first column in the in.aclientd line.
   - For HTTP Sign On, modify the first column in the in.ahclientd line.
Appendix B: Legacy Authentication

Firewall Administration Guide R75.40VS | 114

21 fwssd in.aftpd wait 0
80 fwssd in.ahttpd wait 0
513 fwssd in.arlogindwait 0
25 fwssd in.asmtpd wait 0
23 fwssd in.atelnetd wait 0
259 fwssd in.aclientd wait 259
10081 fwssd in.ihhttpd wait 0
900 fwssd in.ahclientdwait 900
0 fwssd in.pingd respawn 0
0 fwssd in.asessiond respawn 0
0 fwssd in.aufpd respawn 0
0 vpn vpnd respawn 0
0 fwssd mdq respawn 0
0 xrm xrmrespawn0-pr

Important - Do not change anything else in these lines.

5. Ensure that there is no rule that blocks the connection to the new port.
6. Restart Check Point services by running the cpstart command.

Allowing Encrypted Client Authentication

To configure Encrypted Client Authentication for HTTPS Connections:
2. Edit fwauthd.conf, located in the $FWDIR/conf directory. Add :defaultCert to the following line:

   ```
   900 fwssd in.ahclientd wait 900 ssl:defaultCert
   ```

   Note - defaultCert is a nickname included in the Certificate List on a Security Gateway. To check the nickname of your gateway, open the VPN page of the Gateway Properties window and see the Certificates List.

3. Save and close the file.
4. Run cpstart.
5. Open SmartDashboard.
6. Create this rule (which also permits HTTPS traffic between the client and the Web server):

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any user group</td>
<td>Internal Web server</td>
<td>https</td>
<td>Client Auth (Partially automatic or Manual mode)</td>
</tr>
</tbody>
</table>

7. Install the policy.

Continue with the following procedure using the client browser.
1. Using the client browser, enter: https://<gateway URL>:900
2. Click Yes to trust the Security Gateway certificate.
3. Type the Security Gateway user name.
4. Click OK.
5. Click Yes.
6. Enter the gateway password.
7. Click Submit.
8. Enter the URL address: https://<Internal_Web_Server_IP_address>
9. Click Yes.

You are authenticated on the Security Gateway and your internal Web server.
Creating Users and Groups

Authentication rules are defined by user groups, rather than individual users. Therefore, you must first define users and then add them to groups to define authentication rules. You can define users with the Security Gateway proprietary user database or with an LDAP server.

Creating User Groups

To create a user group:
1. In SmartDashboard, select **User Groups** from the **Users and Administrators** tab of the **Objects** tree.
2. Right-click and select **New Group**. The **Group Properties** window opens.
3. Assign the group a name.

Creating a User Template

With a template, a user inherits the template's properties, including membership in groups. If you modify a template's properties, changes only affect future users. Users previously created with that template are not affected.

To create a user template:
1. In the SmartDashboard **Objects** tree, open the **Users and Administrators** tab.
2. Right-click **Templates** and select **New Template**. The **User Template Properties** window opens.
3. Assign the template a name.
4. In the **Groups** tab, add user groups.
   All users in these groups will get the properties of this template.
5. In the **Authentication** tab, select an authentication scheme.
6. In the remaining tabs, enter the properties of the user template.

Creating Users

To create users:
1. In the **Users** branch of the objects tree, right-click and select **Edit**. The **User Properties** window opens.
2. Enter the user data. You can change the properties that the user inherited from the template for that user only without changing the template.

Installing User Information in the Database

Users and groups can be installed separately from the Rule Base, meaning that you can update users and groups without reinstalling the Rule Base.

To install the user database, select **Policy > Install Database** from the SmartDashboard menu.

Configuring Authentication Tracking

Successful and unsuccessful authentication attempts can be monitored in SmartView Tracker or using other tracking options, for example, email and alerts. Authentication tracking can be configured for the following types of authentication attempts:

- **Failed authentication attempts**: Can be tracked for all forms of authentication.
  
  To track failed authentication attempts:

- In the **Authentication** page of a gateway object, set the **Authentication Failure Track** property to define the tracking option when authentication failures occur.

- **Successful authentication attempts**: Can be tracked for Client Authentication.
To track successful authentication attempts:
1. In the Client Authentication Action Properties window, set the Successful Authentication Tracking property to define the tracking option for all successful Client Authentication attempts.
2. To set this option, right-click in the Action column of the Client Authentication rule. The default setting is Log.

To track all authentication attempts:
1. Select an option in the Track column of any rule that uses some form of authentication. The Set by Rule tracking option can only be added to the tracking policy set in the gateway object.
   For example, if the gateway object is set to log all failed authentication attempts, setting a rule to None has no effect and failed authentication attempts are still logged in SmartView Tracker. However, setting the rule to Alert causes an Alert to be sent for each failed authentication attempt.

Configuring Policy for Groups of Windows Users

You can create policy rules for groups of users that are not defined on the Security Management Server, but are defined either on the Windows-based gateway host or in the Windows trusted domain.

To configure policy for groups of Windows users:
1. Enable this feature using the Graphical Database Tool (GUIdbEdit).
2. Change the value of the add_nt_groups attribute to true. (This attribute is located under the firewall_properties object in the properties table.)
3. Ensure that the user belongs to a Windows user group.
4. In the SmartDashboard, create a user group with the name: Windows_<Windows user group>. The group may be empty.
5. Define a Generic User Profile for each user that uses an operating system password as its authentication scheme.
Appendix C: Cooperative Enforcement

Cooperative Enforcement works with Check Point Endpoint Security servers. This feature utilizes the Endpoint Security server compliance capability to verify connections arriving from various hosts across the internal network.

Endpoint Security server is a centrally managed, multi-layered Endpoint Security solution that employs policy-based security enforcement for internal and remote PCs. Easily deployed and managed, the Endpoint Security server mitigates the risk of hackers, worms, spyware, and other security threats.

Features such as predefined policy templates, an intuitive Web-based management interface, and PC firewall and application privilege controls, enable administrators to develop, manage, and enforce Cooperative Enforcement quickly and easily.

Using Cooperative Enforcement, any host initiating a connection through a gateway is tested for compliance. This increases the integrity of the network because it prevents hosts with malicious software components from accessing the network.

This feature acts as a middle-man between hosts managed by an Endpoint Security server and the Endpoint Security server itself. It relies on the Endpoint Security server compliance feature, which defines whether a host is secure and can block connections that do not meet the defined prerequisites of software components.

The following is a typical Cooperative Enforcement workflow:

1. A host opens a connection to the network through a firewall gateway. The first packet from the client to the server is allowed. It is only on the first server’s reply to the client that the Cooperative Enforcement feature begins to perform.
2. The firewall checks for host compliance in its tables and queries the Endpoint Security server, if required.
3. Upon receiving a reply, connections from compliant hosts are allowed and connections from non-compliant hosts are blocked.

When activating the cooperative enforcement feature on a gateway, the following implied rules are automatically enabled:

1. Allow all firewall GUI clients to connect to the Endpoint Security server via HTTP or HTTPS (port 80 or 443).
2. Allow all internal clients to access the Endpoint Security server via the firewall for heartbeats.
3. Allow the firewall to communicate with the Endpoint Security server on port 5054.

If additional access permissions are required (such as allow external clients to connect to the Endpoint Security server, or for other machines to access the administration portion of the Endpoint Security server), explicit rules should be defined.

In This Appendix

- Enforcement Mode 118
- NAT Environments 118
- Monitor Only Deployment Mode 118
- Configuring Cooperative Enforcement 118
Enforcement Mode

When in Enforcement Mode, non-compliant host connections are blocked by the firewall endpoint security feature. For HTTP connections, the host is notified that it is non-compliant. The user can then perform appropriate actions to achieve compliance. For example, the user may upgrade the version of the Endpoint Security client.

NAT Environments

Cooperative Enforcement feature is not supported by all the NAT configurations. For Cooperative Enforcement to work in a NAT environment, the gateway and the Endpoint Security Server must relate to the same IP address of a specific client. Therefore, when NAT is used, if NAT is causing the Client IP received by gateway to be different than the Client IP received by the Endpoint Security Server, Cooperative Enforcement will not work properly.

Monitor Only Deployment Mode

In the Monitor Only deployment mode, the firewall requests authorization statuses from the Endpoint Security server but, regardless of the received statuses, connections are not dropped. In addition (if configured by the administrator) the Cooperative Enforcement feature generates logs regardless of the deployment mode.

Configuring Cooperative Enforcement

To configure Cooperative Enforcement:

From the gateway's Cooperative Enforcement page, select Authorize clients using Endpoint Security Server to enable Cooperative Enforcement.

1. Select Monitor Only for traffic to pass successfully and to track only connections that would otherwise have been dropped.
2. Track unauthorized client status allows you to set the appropriate track or alert option. The default setting is Log.
3. In the Endpoint Security Server Selection section, select which Endpoint Security server will be used:
   - To use this machine, select Use Endpoint Security Server installed on this machine.
   - To use another machine, select a server from the Select Endpoint Security Server drop down menu. Click New to create a new server.
4. In the Client Authorization section, select one of the following methods:
   - Check authorization of all clients: Inspects all clients.
   - Bypass authorization of the following clients: Permits all clients in the selected groups drop-down list to pass without inspection.
   - Check authorization only of the following clients: Verifies the authorization of clients from the selected groups drop-down list.
Index

A
Access Control • 8
Access Control Overview • 8
Accessing the IPv6 Kernel • 66
Achieving Security Before Firewall Activation • 95
Acquiring Identities for Active Directory Users • 31
Acquiring Identities in a Terminal Server Environment • 37
Acquiring Identities in Application Control and URL Filtering • 37
Acquiring Identities with Browser-Based Authentication • 32
Acquiring Identities with Identity Agents • 35
AD Query • 25
Adaptive Continuous Download • 73
Adding Processing Cores to the Hardware • 89
Advanced Features • 63
Advanced NAT Configuration • 49
Affinity Settings • 91
Agent Automatic Sign On • 111
Allocating a Core for Heavy Logging • 90
Allocating an Additional Core to the SND • 89
Allocating Processing Cores • 89
Allowing Encrypted Client Authentication • 114
Anti-Spam • 72
Anti-Spam and Mail • 71
Anti-Spam Logging and Monitoring • 79
Anti-Spam on UTM-1 Edge Devices • 76
Anti-Spam Tracking and Reporting Options • 79
Anti-Spoofing for IPv6 Addresses • 61
Appendix A
  Security Before Firewall Activation • 95
Appendix B
  Legacy Authentication • 102
Appendix C
  Cooperative Enforcement • 117
Application Control and Identity Awareness • 9
  Associating a RADIUS Server with Security Gateway • 105
Authentication • 23
Authentication Methods • 107
Authentication Schemes • 103
Authorizing All Standard Sign On Rules • 113
Automatic and Manual NAT Rules • 43
Automatic and Proxy ARP • 45
Automatic Hide NAT for Internal Networks • 41
Automatic Versus Manual Rules • 45
B
Basic Configuration - Network Node with Hide NAT • 46
Basic Rules • 12
Bidirectional NAT • 43
Boot Security • 95
Bridge Mode and Anti-Spam • 76
Browser-Based Authentication • 26
C
Changing the Client Authentication Port Number • 113
Changing the Default Filter to a Drop Filter • 96
Check Point Password • 103
Choosing the Hide Address in Hide NAT • 45
Client Authentication • 109
Command Line Reference • 91, 99
Communication Between an Internal Network and the Internet • 51
Communication Between Internal Networks • 50
Communication Examples • 50
comp_init_policy • 100
Configure the Firewall • 69
Configuring a Block List • 74
Configuring a Content Anti-Spam Policy • 73
Configuring a Disclaimer • 78
Configuring a Security Gateway to use RADIUS Authentication • 103
Configuring a Security Gateway to use SecurID Authentication • 105
Configuring a Security Gateway to use TACACS+Authentication • 106
Configuring an Allow List • 75
Configuring an IP Reputation Policy • 74
Configuring Anti-Spam • 73
Configuring Anti-Spam POP3 • 75
Configuring Anti-Spam SMTP • 75
Configuring Anti-Spoofing • 17
Configuring Anti-Spoofing for External Interfaces • 17
Configuring Anti-Spoofing for Internal Interfaces • 18
Configuring Anti-Virus Protection for Mail • 77
Configuring Authentication • 102
Configuring Authentication Tracking • 115
Configuring Client Authentication • 112
Configuring ConnectControl • 85
Configuring Cooperative Enforcement • 118
Configuring CoreXL • 91
Configuring File Types • 78
Configuring Identity Awareness • 38
Configuring IP Pool NAT • 56
Configuring ISP Redundancy • 67
Configuring Mail Anti-Virus • 77
Configuring Multicast Access Control • 21
Configuring NAT • 46
Configuring Network Exceptions • 75
Configuring Policy for Groups of Windows Users • 116
Configuring Security Gateway as DNS • 68
Configuring Session Authentication • 108
Configuring Settings • 78
Configuring SMTP and POP3 • 77
Configuring the Gateway Object • 53
Configuring the Hit Count Display • 15
Configuring the Hit Count Timeframe • 16
Configuring the ISP Links • 68
Configuring the Security Management server Object • 53
Configuring User Authentication • 107
Configuring with VPN • 70
Configuring Zero Hour Malware Protection • 77
ConnectControl - Server Load Balancing • 81
ConnectControl Packet Flow • 82
Connecting Translated Objects on Different Interfaces • 49
Considering Logical Server Types • 84
Control of IP Forwarding on Boot • 95
control_bootsec • 99
CoreXL Administration • 87
CoreXL for IPv6 • 88
cpstop -fwflag default and cpstop -fwflag proc • 101
Creating a User Template • 115
Creating an IPv6 Object • 59
Creating User Groups • 115
Creating Users • 115
Creating Users and Groups • 115
Default Configuration • 87
Defining a Custom Default Filter • 96
Defining Access Control Rules • 13
Defining an Access Control Policy • 14
Defining an ICMPv6 Service • 62
Defining Rules for IPv6 or IPv4 Only • 63
Deployment • 30
Disabling IPv6 on a Security Gateway • 59
Disabling NAT in a VPN Tunnel • 46
Dynamic Registration Using IGMP • 19
Editing Implied Rules • 12
Editing the ISP Redundancy Script • 70
Enabling Client Authentication Wait Mode • 112
Enabling IPv6 on a Security Gateway • 58
Enabling or Disabling Hit Count • 14
Enforcement Mode • 118
Example • 93, 94
Example Access Control Rule • 11
Example of Automatically Generated Rule (Hide NAT) • 43
Example of Automatically Generated Rules (Static NAT) • 44
Excluding Specific Internal Addresses • 18
Force ISP Link State • 70
Fully Automatic Sign On • 111
fw ctl affinity • 93
fw ctl affinity -l • 94
fw ctl affinity -s • 93
fw ctl multik stat • 94
fwaffinity.conf • 92
fwaffinty_apply • 92
fwboot bootconf • 99
Gaia • 58, 59
General Steps for Configuring NAT • 46
Granting User Access Using RADIUS Server Groups • 104
Hide NAT • 40
Hide Versus Static • 44
Hit Count • 14
How AD Query Operates - Firewall Rule Base Example • 26
How Captive Portal Operates - Firewall Rule Base • 27
How the Gateway Searches for Users • 102
How Transparent Kerberos Authentication Operates • 28
How You Download an Identity Agent - Example • 29
HTTP • 82
Identity Agents • 28
Identity Awareness • 23
Identity Awareness Scenarios • 30
Implied Rules • 11
Importance of Rule Order in User Authentication • 108
Important Information • 3
Inspection of Unknown ICMPv6 Codes • 62
Installing and Configuring Session Authentication Agent • 108
Installing User Information in the Database • 115
Interface A • 50
Interface B • 50
Interface C • 50
Internal Communication with Overlapping Addresses • 49
Introduction to Anti-Spam and Mail Security • 71
Introduction to ConnectControl • 81
IP Multicast Group Addressing • 19
IP Pool NAT • 53
IP Pool NAT for Clusters • 56
IP Pool Per Interface • 54
IPSO Appliances • 58, 59
IPv6 • 57
IPv6 Extension Headers • 64
IPv6 in IPv4 Intra Tunnel Inspection • 65
IPv6 in SmartView Tracker • 62
IPv6 Rules • 60
IPv6 with ClusterXL • 62
ISP Redundancy • 67
ISP Redundancy Modes • 67
Legal Addresses • 18
Load Measuring • 85
Load-Balancing Methods • 81
Logical Server Types • 82
Mail Security Overview • 72
Managing Default Filter and Initial Policy • 98
Manual Sign On • 110
Microsoft Networking Services Security • 21
Monitor Only Deployment Mode • 118
Multicast Access Control • 19
Multicast Routing Protocols • 19
NAT and Anti-Spoofing • 46
NAT Environments • 118
NAT Modes • 39
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Priorities</td>
<td>54</td>
</tr>
<tr>
<td>NAT Rule Base</td>
<td>42</td>
</tr>
<tr>
<td>Network Address Translation</td>
<td>39</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>50</td>
</tr>
<tr>
<td>Non-Corresponding Gateway Addresses</td>
<td>53</td>
</tr>
<tr>
<td>Object Database Configuration on Linux</td>
<td>51</td>
</tr>
<tr>
<td>Object Database Configuration on Windows</td>
<td>51</td>
</tr>
<tr>
<td>Operating System Password</td>
<td>103</td>
</tr>
<tr>
<td>Order of Automatic Rules</td>
<td>44</td>
</tr>
<tr>
<td>Order of Rule Enforcement</td>
<td>11</td>
</tr>
<tr>
<td>Other</td>
<td>83</td>
</tr>
<tr>
<td>Partial Address Based Filtering</td>
<td>65</td>
</tr>
<tr>
<td>Partial Destination IPv6</td>
<td>65</td>
</tr>
<tr>
<td>Partial Source IPv6</td>
<td>66</td>
</tr>
<tr>
<td>Partially Automatic Sign On</td>
<td>111</td>
</tr>
<tr>
<td>Performance Tuning</td>
<td>88</td>
</tr>
<tr>
<td>Per-Interface Multicast Restrictions</td>
<td>20</td>
</tr>
<tr>
<td>Persistency By Server</td>
<td>84</td>
</tr>
<tr>
<td>Persistency By Service</td>
<td>84</td>
</tr>
<tr>
<td>Persistent Server Mode</td>
<td>84</td>
</tr>
<tr>
<td>Persistent Server Timeout</td>
<td>85</td>
</tr>
<tr>
<td>Planning Considerations for NAT</td>
<td>44</td>
</tr>
<tr>
<td>Port Translation</td>
<td>41</td>
</tr>
<tr>
<td>Preventing IP Spoofing</td>
<td>16</td>
</tr>
<tr>
<td>Processing Core Allocation</td>
<td>88</td>
</tr>
<tr>
<td>RADIUS</td>
<td>103</td>
</tr>
<tr>
<td>Refreshing the Hit Count Data</td>
<td>16</td>
</tr>
<tr>
<td>Reporting False Positives to Check Point</td>
<td>79</td>
</tr>
<tr>
<td>Required SmartDashboard Configuration</td>
<td>32, 34, 35, 37</td>
</tr>
<tr>
<td>Reserved Local Addresses</td>
<td>19</td>
</tr>
<tr>
<td>Resolving Access Conflicts</td>
<td>112</td>
</tr>
<tr>
<td>Restricting Access to Servers and Shares (CIFS Resource)</td>
<td>21</td>
</tr>
<tr>
<td>Reusing IP Pool Addresses For Different Destinations</td>
<td>55</td>
</tr>
<tr>
<td>Routing Considerations</td>
<td>51</td>
</tr>
<tr>
<td>Rule Base Elements</td>
<td>10</td>
</tr>
<tr>
<td>Rule Match Order</td>
<td>42</td>
</tr>
<tr>
<td>Rule Order</td>
<td>12</td>
</tr>
<tr>
<td>Rules and the Rule Base</td>
<td>9</td>
</tr>
<tr>
<td>Sample Configuration (Static and Hide NAT)</td>
<td>47</td>
</tr>
<tr>
<td>Sample Configuration (Using Manual Rules for Port Translation)</td>
<td>48</td>
</tr>
<tr>
<td>Scenario</td>
<td></td>
</tr>
<tr>
<td>Guest Users from Unmanaged Device</td>
<td>33</td>
</tr>
<tr>
<td>Identifying Users Accessing the Internet through Terminal Servers</td>
<td>37</td>
</tr>
<tr>
<td>Identifying Users in Application Control and URL Filtering logs</td>
<td>37</td>
</tr>
<tr>
<td>Identity Agent Deployment and User Group Access</td>
<td>35</td>
</tr>
<tr>
<td>Laptop Access</td>
<td>31</td>
</tr>
<tr>
<td>Recognized User from Unmanaged Device</td>
<td>32</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>58, 59</td>
</tr>
<tr>
<td>SecurID</td>
<td>105</td>
</tr>
<tr>
<td>Securing Microsoft Networking Services (CIFS)</td>
<td>21</td>
</tr>
<tr>
<td>Security Management Behind NAT</td>
<td>52</td>
</tr>
<tr>
<td>Selecting a Customized Server</td>
<td>76</td>
</tr>
<tr>
<td>Server Availability</td>
<td>85</td>
</tr>
<tr>
<td>Session Authentication</td>
<td>108</td>
</tr>
<tr>
<td>Setting Interface Affinities</td>
<td>90</td>
</tr>
<tr>
<td>Setting the fwd Daemon Affinity</td>
<td>91</td>
</tr>
<tr>
<td>Simplicity</td>
<td>11</td>
</tr>
<tr>
<td>Single Sign On</td>
<td>112</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>13</td>
</tr>
<tr>
<td>SmartReporter</td>
<td>79</td>
</tr>
<tr>
<td>SmartView Monitor</td>
<td>79</td>
</tr>
<tr>
<td>SmartView Tracker</td>
<td>79</td>
</tr>
<tr>
<td>Special Considerations for Access Control</td>
<td>11</td>
</tr>
<tr>
<td>Specific Deployment Considerations</td>
<td>45</td>
</tr>
<tr>
<td>Starting the Session Authentication Agent</td>
<td>109</td>
</tr>
<tr>
<td>Static NAT</td>
<td>39</td>
</tr>
<tr>
<td>Supported Features</td>
<td>57</td>
</tr>
<tr>
<td>Supported Platforms and Unsupported Features</td>
<td>87</td>
</tr>
<tr>
<td>Syntax</td>
<td>92, 93, 94</td>
</tr>
<tr>
<td>TACACS</td>
<td>106</td>
</tr>
<tr>
<td>The Default Filter</td>
<td>95</td>
</tr>
<tr>
<td>The Initial Policy</td>
<td>97</td>
</tr>
<tr>
<td>Topology Considerations</td>
<td></td>
</tr>
<tr>
<td>DMZ</td>
<td>12</td>
</tr>
<tr>
<td>Traceroute IPv6</td>
<td>64</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Cannot Complete Reboot</td>
<td>99</td>
</tr>
<tr>
<td>Undefined</td>
<td>107</td>
</tr>
<tr>
<td>Understanding Automatically Generated Rules</td>
<td>43</td>
</tr>
<tr>
<td>Unloading Default Filter or Initial Policy</td>
<td>99</td>
</tr>
<tr>
<td>Usage</td>
<td>99, 100, 101</td>
</tr>
<tr>
<td>User Authentication</td>
<td>107</td>
</tr>
<tr>
<td>User Experience</td>
<td>33, 34, 36</td>
</tr>
<tr>
<td>User Identification in the Logs</td>
<td>38</td>
</tr>
<tr>
<td>User Identification in the Logs</td>
<td>31, 33, 35</td>
</tr>
<tr>
<td>Using 6in4 Tunnels (SIT) in Rules</td>
<td>65</td>
</tr>
<tr>
<td>Using Access Roles</td>
<td>32</td>
</tr>
<tr>
<td>Using the Default Filter for Maintenance</td>
<td>97</td>
</tr>
<tr>
<td>Verifying Default Filter or Initial Policy Loading</td>
<td>98</td>
</tr>
<tr>
<td>VoIP</td>
<td>80</td>
</tr>
<tr>
<td>VPN Connections</td>
<td>20</td>
</tr>
<tr>
<td>Wait Mode</td>
<td>111</td>
</tr>
<tr>
<td>What's Next</td>
<td>36</td>
</tr>
<tr>
<td>Working with 6in4 Tunnels</td>
<td>65</td>
</tr>
<tr>
<td>Working with ICMPv6</td>
<td>62</td>
</tr>
<tr>
<td>Working with IPv6 in SmartConsole</td>
<td>59</td>
</tr>
</tbody>
</table>
X
X11 Service • 12