Important Information

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

Check Point R77
For more about this release, see the R77 home page http://supportcontent.checkpoint.com/solutions?id=sk92965.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=24836.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Gateway R77 Versions Technical Administration Guide).

Searching in Multiple PDFs
To search for text in all the R77 PDF documents, download and extract the complete R77 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=26770.
Use Shift-Control-F in Adobe Reader or Foxit reader.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 August 2015</td>
<td>Updated BPDU procedure in Special Protocols (on page 52)</td>
</tr>
<tr>
<td></td>
<td>Updated Configuring a Security Gateway to use SecurID Authentication (on page 77) for Windows 64-bit</td>
</tr>
<tr>
<td>22 September 2014</td>
<td>Added Using Monitor Mode (on page 61)</td>
</tr>
<tr>
<td></td>
<td>Added Managing Ethernet Protocols (on page 49)</td>
</tr>
<tr>
<td></td>
<td>Updated Supported Software Blades: Gateway and Virtual Systems (on page 37)</td>
</tr>
<tr>
<td></td>
<td>Added Confirming the High Availability Configuration (on page 44)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3 July 2014</td>
<td>Updated for R77.20.</td>
</tr>
<tr>
<td></td>
<td>Updated Rate Limiting for DoS Mitigation (on page 14) to include support for VSX. This feature is supported from R77.20 and higher.</td>
</tr>
<tr>
<td></td>
<td>Updated Adding One Rule at a Time (on page 15) with new parameters. These parameters are supported from R77.10 and higher.</td>
</tr>
<tr>
<td></td>
<td>Updated information for the asterisk character in Regular Expression Syntax (on page 105).</td>
</tr>
<tr>
<td></td>
<td>Updated Bridge Mode (&quot;Bridge Mode&quot; on page 37).</td>
</tr>
<tr>
<td></td>
<td>Removed content for Load Measuring Agent. This feature is supported from R70 and lower.</td>
</tr>
<tr>
<td>13 January 2014</td>
<td>Updated layout and formatting.</td>
</tr>
<tr>
<td></td>
<td>Updated Management over Bridge (R77.10 and Higher) (&quot;Security Gateways R77.10 and Higher&quot; on page 47).</td>
</tr>
<tr>
<td></td>
<td>Added Configuring Monitor Mode (on page 62).</td>
</tr>
<tr>
<td>29 August 2013</td>
<td>First release of this document.</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Start Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Advanced Access Control</td>
<td>9</td>
</tr>
<tr>
<td>Multicast Access Control</td>
<td>9</td>
</tr>
<tr>
<td>Multicast Routing Protocols</td>
<td>9</td>
</tr>
<tr>
<td>Dynamic Registration Using IGMP</td>
<td>9</td>
</tr>
<tr>
<td>IP Multicast Group Addressing</td>
<td>9</td>
</tr>
<tr>
<td>Per-Interface Multicast Restrictions</td>
<td>10</td>
</tr>
<tr>
<td>Configuring Multicast Access Control</td>
<td>11</td>
</tr>
<tr>
<td>Microsoft Networking Services Security</td>
<td>12</td>
</tr>
<tr>
<td>Securing Microsoft Networking Services (CIFS)</td>
<td>12</td>
</tr>
<tr>
<td>Restricting Access to Servers and Shares (CIFS Resource)</td>
<td>12</td>
</tr>
<tr>
<td>Rate Limiting for DoS Mitigation</td>
<td>14</td>
</tr>
<tr>
<td>Overview</td>
<td>14</td>
</tr>
<tr>
<td>VSX and Rate Limiting for DoS Mitigation</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Rate Limiting for DoS Mitigation</td>
<td>15</td>
</tr>
<tr>
<td>Adding One Rule at a Time</td>
<td>15</td>
</tr>
<tr>
<td>Adding Rules in Batch Mode</td>
<td>19</td>
</tr>
<tr>
<td>Deleting a Rule</td>
<td>20</td>
</tr>
<tr>
<td>Configuring Rules with VSX</td>
<td>20</td>
</tr>
<tr>
<td>Configuring Global Parameters</td>
<td>21</td>
</tr>
<tr>
<td>Monitoring Events Related to DoS Mitigation</td>
<td>23</td>
</tr>
<tr>
<td>ISP Redundancy</td>
<td>24</td>
</tr>
<tr>
<td>ISP Redundancy Modes</td>
<td>24</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>25</td>
</tr>
<tr>
<td>Configuring ISP Redundancy</td>
<td>25</td>
</tr>
<tr>
<td>Configuring the ISP Links</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Security Gateway as DNS</td>
<td>26</td>
</tr>
<tr>
<td>Configure the Firewall</td>
<td>27</td>
</tr>
<tr>
<td>Configuring with VPN</td>
<td>28</td>
</tr>
<tr>
<td>Force ISP Link State</td>
<td>29</td>
</tr>
<tr>
<td>Editing the ISP Redundancy Script</td>
<td>29</td>
</tr>
<tr>
<td>ConnectControl - Server Load Balancing</td>
<td>30</td>
</tr>
<tr>
<td>Introduction to ConnectControl</td>
<td>30</td>
</tr>
<tr>
<td>Load-Balancing Methods</td>
<td>30</td>
</tr>
<tr>
<td>ConnectControl Packet Flow</td>
<td>31</td>
</tr>
<tr>
<td>Logical Server Types</td>
<td>31</td>
</tr>
<tr>
<td>HTTP</td>
<td>31</td>
</tr>
<tr>
<td>Other</td>
<td>33</td>
</tr>
<tr>
<td>Considering Logical Server Types</td>
<td>33</td>
</tr>
<tr>
<td>Persistent Server Mode</td>
<td>34</td>
</tr>
<tr>
<td>Persistency By Server</td>
<td>34</td>
</tr>
<tr>
<td>Persistency By Service</td>
<td>34</td>
</tr>
<tr>
<td>Persistent Server Timeout</td>
<td>35</td>
</tr>
<tr>
<td>Server Availability</td>
<td>35</td>
</tr>
<tr>
<td>Configuring ConnectControl</td>
<td>35</td>
</tr>
<tr>
<td>Bridge Mode</td>
<td>37</td>
</tr>
<tr>
<td>Introduction to Bridge Mode</td>
<td>37</td>
</tr>
</tbody>
</table>
Regular Expressions .................................................................................. 105
Using Non-Printable Characters ............................................................... 106
Using Character Types ............................................................................. 106
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.

![Multicast Address Diagram]

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/](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 Server(s) 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:
  - Click **Add** and type BEATLES in the **Server Name** field and IPC$ in the **Share Name** field. Click **OK**.
  - 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.
Rate Limiting for DoS Mitigation

In This Section:

Overview .......................................................................................................................... 14
VSX and Rate Limiting for DoS Mitigation ................................................................. 14
Configuring Rate Limiting for DoS Mitigation ......................................................... 15

Overview

Rate Limiting is a defense against DoS (Denial of Service) attacks. A rule-based policy limits traffic coming from specific sources and using specific services.

Rate limiting is enforced on:

- Bandwidth and packet rate
- Number of concurrent connections
- Connection rate

Rate Limiting for DoS Mitigation is scalable and can support a large number of rules. You can define policies that limit bandwidth for the traffic coming from geographic sources that are outside of normal business profiles. It also provides monitoring and whitelisting bypass capabilities.

Note -

- Rate Limiting for DoS Mitigation is supported on SecurePlatform and Gaia gateways with Performance Pack installed
- During the installation of the Firewall policy on the gateway, the rate limiting policy is not enforced

VSX and Rate Limiting for DoS Mitigation

This feature is supported in R77.20 and higher.

VSX supports all the Rate Limiting features and functionality. You can configure different settings for the Virtual Systems or global parameters for all of them.

For R77.10 and lower, you can configure only the VSX Gateway (VS0).
Configuring Rate Limiting for DoS Mitigation

To prevent Denial of Service (DoS) attacks, add rules to a policy one at a time ("Adding One Rule at a Time" on page 15), or in batch mode ("Adding Rules in Batch Mode" on page 19).

If this gateway is a cluster member, configure Rate Limiting for DoS Mitigation on all of the cluster members.

Note - By default, the rules are loaded only on the local gateway, unless you specify a different gateway with the -S <server> parameter.

Adding One Rule at a Time

To add a rule to the policy:

```
fw samp add -a d|n|b [-l r] [-t TIMEOUT] [-n NAME] [-c COMMENT] [-o ORIGINATOR] quota KEY VALUE [KEY VALUE ...KEY VALUE]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Action: on the incoming packets that match the rule:</td>
</tr>
<tr>
<td></td>
<td>• d - drops the packet</td>
</tr>
<tr>
<td></td>
<td>• n - notify: logs the packet and lets it through</td>
</tr>
<tr>
<td></td>
<td>• b - bypass: lets the packet through without checking it against the policy rules</td>
</tr>
<tr>
<td></td>
<td>Note - Rules set to bypass cannot have a log or limit specification. Bypassed packets and connections do not count towards overall number of packets and connection for limit enforcement of type ratio.</td>
</tr>
<tr>
<td>-l</td>
<td>Log (optional) - turns on logging:</td>
</tr>
<tr>
<td></td>
<td>- l r - regular logging</td>
</tr>
<tr>
<td>-t</td>
<td>Timeout (optional) - the number of seconds after which the rule expires.</td>
</tr>
<tr>
<td></td>
<td>- t INTEGER</td>
</tr>
<tr>
<td></td>
<td>If not set, the rule does not expire.</td>
</tr>
<tr>
<td>-n</td>
<td>Name (optional) - adds a name label to the rule.</td>
</tr>
<tr>
<td></td>
<td>- n NAME</td>
</tr>
<tr>
<td>-c</td>
<td>Comment (optional) - adds comment to the rule.</td>
</tr>
<tr>
<td></td>
<td>- c COMMENT</td>
</tr>
<tr>
<td>-o</td>
<td>Originator (optional) - specifies the originator.</td>
</tr>
<tr>
<td></td>
<td>- o ORIGINATOR_NAME</td>
</tr>
<tr>
<td>-s</td>
<td>Server (optional) - specifies the IP address of a target gateway for policy installation.</td>
</tr>
<tr>
<td></td>
<td>- s IP_ADDRESS</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description and Values</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| source       | Defines packet sources as a list of comma separated expressions in this format:  
  
  source TYPE:VALUE [,TYPE:VALUE,  
  TYPE:VALUE,...TYPE:VALUE]  
  
  Valid TYPES and VALUES:  
  
  - any  
    The rule is applied to packets from any source.  
    This value is supported in R77.10 and higher.  
  
  - range:IP_ADDRESS or range:IP_ADDRESS-IP_ADDRESS  
    IP addresses can be IPv4 addresses (x.y.z.w) or IPv6 addresses ([x:x[:y:y:...:z]).  
  
  - cidr:IP_ADDRESS/NETMASK  
    IPv4 or IPv6 address, NETMASK 0 to 32 for IPv4, 0 to 128 for IPv6.  
  
  - cc:COUNTRY_CODE  
    Two-letter code defined in ISO 3166-1 alpha-2  
    http://www.iso.org/iso/iso-3166-1_decoding_table.html. The rule matches the country code to the addresses assigned to this country, based on the Geo IP database.  
  
  - asn:AUTONOMOUS_SYSTEM_NUMBER  
    Valid value syntax is ASnnnn, where nnnn is a number unique to the specific organization. The rule matches the AS number of the organization to the IP addresses that are assigned to this organization, based on the Geo IP database.                                                                                                                                                                                                                                                                                         |
| destination  | This parameter is supported in R77.10 and higher.  
  The options for this parameter are the same as the source parameter.                                                                                                                                                                                                                                                                                                                                                     |
| source-negated | true or false (default):  
  
  source-negated true|false  
  
  If true, the rule matches the packet or the connection to the complement set of the values defined as the source.                                                                                                                                                                                                                                                                                                                                 |
| destination-negated | This parameter is supported in R77.10 and higher.  
  The options for this parameter are the same as the source-negated parameter.                                                                                                                                                                                                                                                                                                                                                     |
| service      | Service protocols, ports, or ranges of protocols or ports:  
  
  service  
  PROTO|PROTO-PROTO|PROTO/PORT|PROTO/PORT-PORT  
  
  Valid values:  
  
  - PROTO - IP protocol number in the range 1-255.  
  
  - PORT - TCP or UDP port number in the range 1-65535.  
  
  Source: Security Gateway Technical Administration Guide R77 Versions |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Values</th>
</tr>
</thead>
</table>
| service-negated    | **true** or **false** (default):  
  
  `service-negated true|false`  
  
  - If **true**, the rule matches the packet or the connection to the complement set of the values defined as the `service`. |
| new-conn-rate      | Maximum (per second) number of connections that match the rule:  
  
  `new-conn-rate <seconds>` |
| new-conn-rate-ratio| Maximum ratio of the `new-conn-rate` value to the rate of all connections per second through the gateway, expressed in parts per 65536:  
  
  `new-conn-rate-ratio n` |
| concurrent-conns   | Maximum number of concurrent active connections that match the rule:  
  
  `concurrent-conns n` |
| concurrent-conns-ratio | Maximum ratio of the `concurrent-conns` value to the total number of active connections through the gateway, expressed in parts per 65536.  
  
  `concurrent-conns-ratio n` |
| pkt-rate           | Maximum per second number of packets that match the rule:  
  
  `pkt-rate n` |
| pkt-rate-ratio     | Maximum ratio of the `pkt-rate` value to the rate of all connections through the gateway, expressed in parts per 65536.  
  
  `pkt-rate-ratio n` |
| byte-rate          | Maximum total number of bytes per second in packets that match the rule:  
  
  `byte-rate n` |
| byte-rate-ratio    | Specifies the maximum ratio of the `byte-rate` value to the bytes per second rate of all connections through the gateway, expressed in parts per 65536.  
  
  `byte-rate-ratio n` |

**track**  

Criteria for counting connections, packets, and bytes:  

- `track source` connections, packets, and bytes are counted per specific source IP address, and not cumulatively for the rule.  
- `track source-service` connections, packets, and bytes are counted per specific source IP address and specific IP protocol and destination port, and not cumulatively for the rule.
Note -

- The quota rules are not immediately applied to the gateway. They are only registered in the Suspicious Activity Monitoring policy database. To apply all the rules from the policy database immediately, add `flush true` in the `fw samp add` command.
- The new rules apply only to the new connections, not to the existing ones.

Here are some rule examples.

**Example of a rule with a range:**

```
fw samp add -a d -l r -t 3600 quota service any source
range:172.16.7.11-172.16.7.13 new-conn-rate 5 flush true
```

- Limits the rate of creation of new connection for the IP addresses in the range 172.16.7.11-172.16.7.13 to 5 per second. Drops all other attempted connections (`-a d`).
- Logs packets that exceed the quota set by the rule. **Note:** The limit of the total number of log entries per second is set through the global parameter `sim_dos ctl -l LOG-LIMIT`. Refer to the Global Parameters ("Configuring Global Parameters" on page 21) section for more information.
- The rule will expire in one hour (3600 seconds).
- This rule will be compiled and loaded on the Performance Pack, together with other rules in the Suspicious Activity Monitoring policy database, immediately because this rule includes the `flush true` parameter.

**Example of a rule with a service specification:**

```
fw samp add -a n -l r quota service 1,50,51,6/443,17/53
service-negated true source cc:QQ byte-rate 0
```

- Logs all packets (`-a n`) coming from IP addresses that are assigned to the country with specified country code (`cc:QQ`).
- Does not let any traffic through (`byte-rate 0`) except for the packets (`service-negated` `true source`) that match the IP protocols on the list:
  - 1 - ICMP
  - 50-51 - IPsec
  - 6/443 - HTTPS
  - 17/53 - DNS
- The rule will not expire (`TIMEOUT` parameter is not specified). To cancel it, you must delete it explicitly.
- This rule will not be compiled and installed on the Performance Pack immediately because it does not include the `flush true` parameter.

**Example of a rule with ASN:**

```
fw samp -a d quota source asn:AS64500,cidr:[::ffff:c0a8:1100]/120
service any pkt-rate 0
```

- Drops all packets (`-a d`) with the source IP address in the IPv6 address block (`cidr:[::ffff:c0a8:1100]/120`), from the autonomous system number 64500 (`asn:AS64500`)
The rule will not expire (TIMEOUT parameter is not specified). To cancel it, you must delete it explicitly.

This rule will not be compiled and installed on the Performance Pack immediately because it does not include the flush true parameter.

Example of a whitelist rule:

```
fw samp add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
```

- Ignores all other quota type of rules that match the traffic (-a b), and lets through all HTTP traffic (service 6/80) from the specified address range (source range:172.16.8.17-172.16.9.121).
  
  **Note:** the Firewall and other types of security policy rules still apply.

- The rule will not expire (TIMEOUT parameter is not specified). To cancel it, you must delete it explicitly.

- This rule will not be compiled and installed on the Performance Pack immediately because it does not include the flush true parameter.

Example of a tracked rule:

```
fw samp add -a d quota service any source negated true source cc:QQ concurrent-conns-ratio 655 track source
```

- Drops (-a d) new connections for every IP address that already has more than approximately 1% (655/65536) of all existing connections (concurrent-conns-ratio 655).

- Defines IP addresses that are assigned to a specific country (source-negated true source cc:QQ) as exception to the rule.

- Does not log any entries (does not include -l parameter).

- The rule will not expire (TIMEOUT parameter is not specified). To cancel it, you must delete it explicitly.

- This rule will not be compiled and installed on the Performance Pack immediately because it does not include the flush true parameter.

Adding Rules in Batch Mode

**To add rules in batch mode:**

1. Type this command to start `fw samp` batch:

   `fw samp [-S IP_ADDRESS] batch <<EOF`

   **Note:** if you include the -s parameter, all the commands in this batch will apply to the specified gateway.

2. Enter one add or delete command per line on as many lines as necessary. Start each line with add or del parameter, and not with `fw samp`. Use the same set of parameters and values as for the individual rules ("Adding One Rule at a Time" on page 15). Terminate each line with a Return (ASCII 10 - Line Feed) character:

   add -a d|n|b [-l r] [-t TIMEOUT] [-n NAME] [-c COMMENT] [-o ORIGINATOR] quota KEY VALUE KEY VALUE.
   del UID

3. To end the batch, type: EOF.
Example:

```
fw samp -S 192.168.37.5 batch <<EOF
add -a d -l r -t 3600 -c a\ comment quota service any source
range:172.16.7.13-172.16.7.13 new-conn-rate 5
del <501f6ef0,00000000,cb38a8c0,0a0afffe>
add -a b quota source range:172.16.8.17-172.16.9.121 service 6/80
EOF
```

This batch applies two `add` commands and one `delete` command to a gateway with the IP address 192.168.37.5. For details on `add` command syntax, see Adding One Rule at a Time (on page 15).

**Note** - A space or a backslash in comments must be each preceded by a backslash:

```
c this\ is\ a\ comment\ with\ a\ backslash\ \\```

### Deleting a Rule

**To delete a rule:**

1. List all the rules in the Suspicious Activity Monitoring policy database:
   
   ```
   fw samp get
   ```

   The rules show in this format:

   ```
   ... operation=add uid=<501f6ef0,00000000,cb38a8c0,0a0afffe> target=all
timeout=... action=... ... ...
   ```

2. Delete a rule from the list:

   ```
   fw samp del '<501f6ef0,00000000,cb38a8c0,0a0afffe>'
   ```

3. Enter this flush-only `add` rule:

   ```
   fw samp add -t 2 quota flush true
   ```

   This immediately deletes the rule, and times out in 2 seconds. It is a good practice to specify a short timeout period for the flush-only rules. This prevents accumulation of rules that are obsolete in the database.

   The `fw samp del` command removes a rule from the persistent database only. The deleted rule continues to be enforced until the next time a policy is compiled and loaded. To force the rule deletion immediately, you must enter a flush-only `add` rule right after the `fw samp del` command.

### Configuring Rules with VSX

This feature is supported in R77.20 and higher.

Use the `fw samp` command to add rules to a Virtual System. You can run the command on the local gateway, or remotely configure the rules.

**To configure rules on a local gateway:**

1. Log in to the gateway CLI.
2. Set the environment for the specified Virtual System, run `set virtual-system <vsid>`
3. Run `fw samp` and configure one or more Rate Limiting rules.

The previous sections explain how to add or delete rules.
To configure rules on a remote gateway:
1. Log in to the server CLI.
2. Run `fw samp` and with these parameters and configure one or more Rate Limiting rules.
   - `-S <server_IP>` - Use the IP address of the VSX Gateway
   - `-s <VS_SIC_name>` - Use the name of the Virtual System that established SIC

Run `fw vsx showncs -vs <VSID>` to show the SIC name for the Virtual System.

The previous sections explain how to add or delete rules.

Configuring Global Parameters

There are several global parameters that you can configure with `sim_dos ctl` command for IPv4 addresses and with `sim6_dos ctl` for IPv6 addresses. They apply to all the policy rules.

**Note** - `sim_dos ctl` and `sim6_dos ctl` are only available as CLI commands on the gateways. Remote command option is not available.

Use the `sim_dos ctl` or `sim6_dos ctl` command with the parameters and values below:

<table>
<thead>
<tr>
<th>Parameter and Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-m 1</td>
<td>0`</td>
</tr>
</tbody>
</table>
| `-x 1|0`               | When set to 1 (default), the rules are only applied to traffic that arrives on the external interfaces of the gateway. When set to 0, the rules are applied to traffic regardless of the interface on which it arrives.  
  **Note**: This does not apply to other security policies on the gateway. They still get enforced. |
| `-l n`              | Sets the limit for the number of log entries per second (the default is 100). All the entries that exceed the limit are suppressed. The number of suppressed messages shows in the following period summary. |
| `-a 1|0`               | Turns the quota policy rules enforcement on (1) and off (0). When the rule enforcement is turned off, no traffic is matched against the quota rules.  
  **Note**: The quota rule enforcement is on automatically, when a policy with rules is loaded, and is off, when an empty policy is loaded. |

The global parameters return to their default values every time the DoS in the Performance Pack module is initialized. This happens on every reboot. To keep the changes to global parameters until you decide to change them again, include the `sim_dos ctl` (or `sim6_dos ctl`) command in the `dospreload` script:
For IPv4:

```
$ cat >$PPKDIR/bin/dospreload4 <<EOF
#!/bin/bash
$PPKDIR/bin/sim_dos ctl -m 1 -x 0 -l 30
EOF
$ chmod +x $PPKDIR/bin/dospreload4
```

For IPv6:

```
$ cat >$PPKDIR/bin/dospreload6 <<EOF
#!/bin/bash
$PPKDIR/bin/sim6_dos ctl -m 1 -x 0 -l 30
EOF
$ chmod +x $PPKDIR/bin/dospreload6
```

For VSX:

Rate Limiting for VSX is supported in R77.20 and higher.

- `$PPKDIR/bin/` is shared by all the Virtual Systems
- `$FWDIR/scripts/` is specific for each Virtual System

Run these commands from Expert mode to apply monitor only mode (`-m 1`) to all Virtual Systems.

```
# cat > $PPKDIR/bin/dospreload4 << EOF
#!/bin/bash
sim_dos ctl -m 1
if test -x $FWDIR/scripts/dospreload4; then
  $FWDIR/scripts/dospreload4
fi
EOF
# chmod +x $PPKDIR/bin/dospreload4
```

Run similar commands to create `$PPKDIR/bin/dospreload6` and a `$FWDIR/scripts/dospreload6` script for each Virtual System. 

Run these commands from Expert mode to limit the number of log entries (`-l 40`) for the Virtual System with VSID 2.

```
# vsenv 2
Context is set to Virtual Device myVS-2 (ID 2).
# cat > $FWDIR/scripts/dospreload4 << EOF
#!/bin/bash
sim_dos ctl -l 40
EOF
# chmod +x $FWDIR/scripts/dospreload4
```
Monitoring Events Related to DoS Mitigation
To see some useful information related to DoS Mitigation, run these commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat /proc/ppk/dos</td>
<td>Shows memory utilization, DoS policy rules, and global parameter configuration.</td>
</tr>
<tr>
<td>cat /proc/ppk6/dos  (for IPv6)</td>
<td></td>
</tr>
<tr>
<td>fw samp get -l</td>
<td>grep '^[0-9a-f,]*$'</td>
</tr>
<tr>
<td></td>
<td>Shows details of active policy rules in long format. It only show rules loaded in IPv4 kernel. To see the rules in IPv6 kernel, use sim6_dos get command.</td>
</tr>
<tr>
<td>cat /proc/ppk/&lt;VSID&gt;/dos</td>
<td>VSX is supported in R77.20 and higher.</td>
</tr>
<tr>
<td></td>
<td>&lt;VSID&gt; is the VSID for the Virtual System.</td>
</tr>
</tbody>
</table>
ISP Redundancy

In This Section:

| ISP Redundancy Modes ................................................................. | 24 |
| SmartDashboard Toolbar ........................................................................ | 25 |
| Configuring ISP Redundancy .............................................................. | 25 |

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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>Link A to the ISP</td>
</tr>
<tr>
<td>3</td>
<td>Link B to the ISP</td>
</tr>
</tbody>
</table>

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 25).

- **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.
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><img src="image" alt="Icon" /></td>
<td>Open the SmartDashboard menu. When instructed to select menu options, click this button to show the menu. For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Change global properties.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Open SmartConsole.</td>
</tr>
</tbody>
</table>

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 Other > ISP Redundancy.
4. Select Load Sharing or Primary/Backup.
5. Configure the links ("Configuring the ISP Links" on page 26).
6. Configure the Security Gateway to be the DNS server ("Configuring Security Gateway as DNS" on page 26).
7. Configure the policy for ISP Redundancy ("Configure the Firewall" on page 27).
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 ISP. 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 29).
   - 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 ISP.
2. Tell the ISP 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 ISP reach a Web server, and DNS traffic from the ISP reach the DNS server.
Example: Manual Static Rules for a Web Server and a DNS Server

<table>
<thead>
<tr>
<th>Source</th>
<th>Original Destination</th>
<th>Service</th>
<th>Translated Source</th>
<th>Translated Destination</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>IP of web server</td>
<td>http</td>
<td>10.0.0.0.2 (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>10.0.0.0.2 (Static)</td>
<td>=</td>
<td>Incoming Web - ISP B</td>
</tr>
<tr>
<td>Any</td>
<td>IP of DNS server</td>
<td>domain_</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>udp</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 ISP configured in ISP Redundancy.
To configure for VPN with a third-party peer:

If the Security Gateway 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}`

`<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 a dialup connection:

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.
ConnectControl - Server Load Balancing

In This Section:

Introduction to ConnectControl ................................................................. 30
Load-Balancing Methods ............................................................................ 30
ConnectControl Packet Flow ..................................................................... 31
Logical Server Types .................................................................................. 31
Persistent Server Mode .............................................................................. 34
Server Availability ....................................................................................... 35
Configuring ConnectControl ...................................................................... 35

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:

- **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.

**Note** - Make sure that rules that allow traffic for services to ConnectControl logical servers and server groups are before Firewall rules that allow traffic for those services.

**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.

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:
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.

Server Group Connection Rule

<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 Persistence**: 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.
Introduction to Bridge Mode

Bridge Interfaces

Bridge interfaces connect two different interfaces (bridge ports). Bridging two interfaces causes every Ethernet frame that is received on one bridge port to be transmitted to the other port. Thus, the two bridge ports participate in the same Broadcast domain (which is different from router ports behavior).

Only two interfaces can be connected by a single Bridge interface. These two interfaces can then be thought of as a two-ports switch. Each port can be a physical, VLAN, or bond device.

Bridge interfaces can be configured on Check Point Security Gateway, and can be used for different deployments. The Firewall inspects every Ethernet frame that passes through the bridge.

Supported Software Blades: Gateway and Virtual Systems

These Software Blades support bridge mode (unless stated they do not) for single Security Gateway deployment, cluster with one switch in Active/Active and Active/Standby deployment, and cluster with four switches.

<table>
<thead>
<tr>
<th>Supported Blade</th>
<th>Supports Gateways in Bridge Mode</th>
<th>Supports Virtual Systems in Bridge Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DLP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Bridge Mode

<table>
<thead>
<tr>
<th>Supported Blade</th>
<th>Supports Gateways in Bridge Mode</th>
<th>Supports Virtual Systems in Bridge Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Inspection</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Threat Emulation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Client Authentication</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User Authentication</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Supported Software Blades: Management

Bridge-mode for a Security Management Server is supported only for Standalone configurations, and it supports all management Software Blades.

#### Unsupported for Bridge Mode

These features, Software Blades and deployments are not supported in Bridge Mode:

- Mobile Access Software Blade
- IPsec VPN Software Blade
- Full High Availability deployment
- NAT on Gateways
- Access to Portals from bridged networks, if the bridge does not have an assigned IP address
- Anti-Virus Traditional Mode
- Identity Awareness authentication other than AD Query (AD Query is the only supported authentication)

#### Supported Operating Systems

These operating systems support Bridge Mode configurations:

- Gaia and SecurePlatform - All Supported Software Blades ("Supported Software Blades: Gateway and Virtual Systems" on page 37)
- IPSO - Only supports the Firewall Software Blade

For more about configuring Bridge Mode for an IPSO Security Gateway, see How To Setup a Bridge Mode Firewall on an IP Appliance with IPSO [http://supportcenter.checkpoint.com/file_download?id=15361](http://supportcenter.checkpoint.com/file_download?id=15361).
Configuring Bridge Interfaces

Using the Gaia WebUI

To configure a bridge interface with the WebUI:

1. In the WebUI navigation tree, select **Network Interfaces**.

2. Click **Add Bridge**.

   The **Add Bridge** window opens.

3. On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 0 and 1024).

4. Select the interfaces from the **Available Interfaces** list and then click **Add**.

5. Click **OK**.
Using the CLI

Bridge interfaces are known as **Bridging Groups** in Gaia clish commands. You can optionally assign an IPv4 or IPv6 address to a bridge interface.

To create a new bridging group:
Run:
> add bridging group <Group ID>
  
  <Group Name> - Bridging Group ID (unique integer between 0 and 1024)

To add an interface to the bridging group:
Run:
> add bridging group <Group ID> interface <interface>
  
  <interface> - Physical interface name

Run this command once for each physical interface included in the bridge interface.

To delete an interface from the bridging group:
Run:
> delete bridging group <Group ID> interface <IF>.

Run this command once for each physical interface included in the bridge interface.

To delete a bridging group:
Run:
> delete bridging group <Group ID>.

To add or change a bridge interface IP address:

- For an IPv4 IP address, run
  
  > set interface <interface> ipv4-address <IP> subnet-mask <Mask>.

- For an IPv6 IP address, run
  
  > set interface <interface> ipv6-address <IP> mask-length <Prefix>.

  <interface> - Bridge interface name
  
  <IP> - IP address - IPv4 or IPv6 address
  
  <Mask> - IPv4 subnet mask in dotted decimal format
  
  <Prefix> - IPv6 prefix length

Example:

set interface br1 ipv6-address 3000:40::1 mask-length 64
**Bridging group commands**

This is a quick reference for bridge interface commands.

**Description** - Use these commands to configure bridge interfaces.

**Syntax**

```plaintext
add bridging group <Group ID> [interface <interface>]
delete bridging group <Group ID> interface <interface>
show bridging group <Group ID>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Group ID&gt;</td>
<td>ID of bridging group</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name</td>
</tr>
</tbody>
</table>

**Example** - add bridging group 56 interface eth1

⚠️ **Important** - After using CLI commands to add, configure or delete features, you must run the `save config` command. This makes sure that the new configuration settings remain after reboot.

---

**Configuring Bridge Mode for Gateways**

You can configure bridge mode with a single gateway or with a cluster. VSX bridge deployments are explained later ("Virtual System in Bridge Mode" on page 54).

The bridge can work without an assigned IP address.

SmartDashboard helps you configure the topology for the bridge ports. There is a separate network or group object that represents the networks or subnets that connect to each port.

**Configuring Single Gateway in Bridge Mode**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 and 2</td>
<td>Switches</td>
</tr>
<tr>
<td>3</td>
<td>Security Gateway Firewall bridging Layer-2 traffic over the one IP address, with a subnet on each side using the same address.</td>
</tr>
</tbody>
</table>

Before you begin, configure a dedicated management interface.

First you configure the bridge interface ("Bridging group commands" on page 41). Then you define the bridge topology in SmartDashboard.
To define the bridge topology:

Use SmartDashboard to manually configure the topology for the bridge ports:

- If one of the bridge ports connects to the Internet, set the topology to **External**
- If the topology uses Anti-Spoofing, for the internal port (interface), make sure that you:
  - Set the topology to **Internal**
  - Select the specific network that connects to the port
- If the topology does not use Anti-Spoofing, make sure that you disable Anti-Spoofing on the bridge port

⚠️ **Note** - When you use Internet objects in a rule with a Security Gateway, make sure that the bridge interface is defined as **External**.

### Configuring an IP Address for the Bridge

In a Security Gateway bridge deployment, you can configure an IP address for the bridge. The IP address of the bridge must be in the bridged subnet. The bridge IP address can be used for gateway management and access to the gateway portals.

When you assign an IP address to the bridge, the **Topology** window shows that both bridge ports have the same IP address as the bridge.
Configuring Gateway Cluster in Bridge Mode

You can configure cluster gateways for bridge mode in different deployments:

- Active/Standby mode
- Active/Active mode

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 and 2</td>
<td>Switches</td>
</tr>
<tr>
<td></td>
<td>Security Gateway Firewall bridging Layer-2 traffic</td>
</tr>
<tr>
<td>3</td>
<td>eth1</td>
</tr>
<tr>
<td>4</td>
<td>eth2</td>
</tr>
<tr>
<td>5</td>
<td>eth3 - the ClusterXL Sync interface</td>
</tr>
</tbody>
</table>

Configuring Active/Standby Mode

This is the preferred mode in topologies that support it.

In Active-Standby mode, ClusterXL decides the cluster state. The standby member drops all packets. It does not pass any traffic, including STP/RSTP/MSTP. If there is a failover, the switches are updated by the Security Gateway to forward traffic to the new active member.

If you use this mode, it is best to disable STP/RSTP/MSTP on the adjacent switches.

To configure Active/Standby mode:

1. Configure the cluster ("Configuring Active/Active Mode" on page 44).
2. Run: `cpconfig`
3. Enter 8, to select Enable Check Point ClusterXL for Bridge Active/Standby.
4. Confirm: y
5. Reboot the cluster member.
6. Install Policy.
7. Test the cluster state: `cphaprojb stat`

The output should be similar to:

```
Cluster Mode: High Availability (Active Up, Bridge Mode) with IGMP Membership
Number   Unique Address     Firewall State (*)
1 (local) 2.2.2.3             Active
2          2.2.2.2            Standby
```
Configuring Active/Active Mode

When you define a bridge interface on a Security Gateway cluster, Active/Active mode is activated by default.

Before you begin, install ClusterXL High Availability on a Gaia appliance or open server.

To configure Active/Active mode, do these steps on each member of the cluster:

1. Configure dedicated management and Sync interfaces.
2. Add a bridge interface, as in a single gateway deployment ("Configuring Single Gateway in Bridge Mode" on page 41).
   Do not configure an IP address on the newly created bridge interface.
3. In SmartDashboard, add the cluster object:
   a) Open Topology of the cluster object.
   b) Get the cluster topology.
   c) Make sure the dedicated management and Sync interfaces are configured.
   d) Make sure the bridge interface and bridge ports are not in the topology.

   Bridge port topology cannot be defined. It is external by default.

4. Install Policy.
5. Test the cluster state: `cphaprob stat`
   The output should be similar to:

   Cluster Mode: High Availability (Active Up, Bridge Mode) with IGMP Membership
   Number   Unique Address     Firewall State (*)
   1 (local) 2.2.2.3            Active
   2          2.2.2.2            Active

6. Make sure that cluster is configured as High Availability in SmartDashboard ("Confirming the High Availability Configuration" on page 44).

Confirming the High Availability Configuration

When you finish configuring Active/Active mode, the output for `cphaprob stat` shows that the Firewall State is Active/Active. Make sure that the cluster is configured as High Availability in SmartDashboard.
To confirm the High Availability configuration:

1. From SmartDashboard, double-click the cluster object. The cluster window opens and shows the General Properties page.
2. From the navigation tree, click ClusterXL.
3. In the Cluster Mode section, make sure that High Availability is selected.
4. Click OK.

Cluster Between Four Switches
You can configure a bridged cluster between four switches, in Active/Active mode. Active/Standby mode is not supported.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, 4</td>
<td>Switches</td>
</tr>
<tr>
<td>5</td>
<td>eth1</td>
</tr>
<tr>
<td>6</td>
<td>eth2</td>
</tr>
<tr>
<td>7</td>
<td>eth3 - the ClusterXL Sync interface</td>
</tr>
</tbody>
</table>

See also: Link Aggregation with ClusterXL in Layer-2

Routing and Bridges

Security Gateways with a bridge interface can support Layer 3 routing over non-bridged interfaces. If you configure a bridge interface with an IP address for one Security Gateway (not a cluster), the bridge functions as a regular Layer 3 interface. It participates in IP routing decisions on the gateway and supports Layer 3 routing.

- Cluster deployments do not support this configuration.
- You cannot configure the bridge to be the route gateway.
• One Security Gateway can support multiple bridge interfaces, but only one bridge can have an IP address.

• The Security Gateway cannot filter or transmit packets on a bridge interface that it inspected before (double-inspection).

Management over Bridge

The following diagram shows a sample topology:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switch</td>
</tr>
<tr>
<td>2</td>
<td>Router</td>
</tr>
<tr>
<td>3</td>
<td>Security Gateway Firewall bridging Layer-2 traffic</td>
</tr>
<tr>
<td>4</td>
<td>Management interface (inspects first packet)</td>
</tr>
<tr>
<td>5</td>
<td>eth1 (inspects first packet again)</td>
</tr>
<tr>
<td>6</td>
<td>eth2</td>
</tr>
<tr>
<td>7</td>
<td>Bridge interface - Management traffic drops</td>
</tr>
<tr>
<td></td>
<td>Security Management Server</td>
</tr>
</tbody>
</table>

When a Layer-3 management interface sends traffic through the firewall, the traffic is dropped because it cannot inspect the same packet again.

• The first packet is inspected and then goes from the management interface to the router.

• The router sends the packet to the bridge interface, and the firewall inspects the first packet again. The firewall concludes that this packet is a retransmission and then drops it.

Use the procedure for the applicable Security Gateway version.
Security Gateways R77.10 and Higher

This feature is supported in R77.10 and higher.

You can configure the Security Gateway to recognize that the first packet is from the management interface. The firewall makes sure that the MD5 hash of the packet that leaves the management interface and enters the bridge interface is the same. Other packets in this connection are handled by the bridge interface without using the router.

To enable management over the bridge:

1. Edit $FWDIR/boot/modules/fwkern.conf.
   If necessary, create this file.
2. Add the appropriate line to the file:
   - For IPv4 traffic - `fwx_bridge_reroute_ipv4=<management>
   - For IPv6 traffic - `fwx_bridge_reroute_ipv6=<management>
   
   `<management>` is the IP address of the management interface.

Security Gateways R77 and Earlier

Incoming and outgoing traffic from a Layer-3 management interface is dropped if traversed over a bridge interface. You can make this traffic pass. Disable inspection on the management interface and disable local Anti-Spoofing.

Note: This removes inspection from the management interface and could compromise gateway security. If you are unsure whether your environment is safe to use this method, contact CheckPoint Solution Center.

To configure management over the bridge:

1. Open $PPKDIR/boot/modules/simkern.conf and add:
   `simlinux_excluded_ifs_list=interface name`
   (Create this file if not found.)
   Where the value (interface name) is the management interface name.
   This excludes the management interface from SecureXL.
2. Edit $FWDIR/modules/fwkern.conf.
   (Create this file if not found.)
   Add these lines:
   `fwx_bridge_use_routing=0`
   `fw_local_interface_anti_spoofing=0`
   `fwlinux_excluded_ifs_list=interface name`
   Where the value (interface name) is the management interface name.
   This disables local Anti-Spoofing and bridge routing, and excludes the management interface from security inspection.
3. Reboot.
IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol. ICMPv6 Neighbor Discovery Protocol must be explicitly allowed for all bridged networks in your Firewall rules. This is different from ARP, for which traffic is always allowed regardless of the Rule Base.

This is an example of a rule that allows ICMPv6 Neighbor Discovery protocol:

```
Policy

<table>
<thead>
<tr>
<th>No.</th>
<th>Hits</th>
<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>1</td>
<td>0</td>
<td>Network Discovery</td>
<td>Bridged Network</td>
<td>Bridged Network</td>
<td>Any Traffic</td>
<td>neighbor-advertisement, neighbor-solicitation, router-advertisement, router-solicitation</td>
<td>accept</td>
<td>None</td>
</tr>
</tbody>
</table>
```

Configuring Link State Propagation

You can bind two ports together, so that when the link state for one port goes down, the other port also goes down. This lets a switch detect and react to a link failure on the other side of a bridge or another part of the network.

This feature is available in one of these modes:

- **Automatic port detection and port pair creation** - All bridge ports are assigned to a port pair (the pair in the bridge).
- **Manual port pair creation** - Up to four port pairs are supported.

Link state propagation is supported on these Check Point appliance line cards:

- CPAC-4-1C/CPAC-8-1C – Copper line cards with IGB driver
- CPAC-4-1F – 1Gbe fiber line card with an IGB driver
- CPAC-4-10F – 10Gbe fiber line card with an IXGBE driver

For example:

```
fw_lsp_pair1="eth1,eth2"
```

**Note** - You can add up to four lines to this file, one for each pair.

**Note:** The below procedures are applicable to R77.20 and higher.

**To configure Link State Propagation for automatic port detection:**

1. Open `FWDIR/modules/fwkern.conf` in a text editor. If there is no `fwkern.conf` file, create a new one.
2. Add this line:
   `fw_link_state_propagation_enabled=1`
3. Reboot the computer.
To create port pairs automatically:

1. **Open** `FWDIR/modules/fwkern.conf` in a text editor.
   If there is no `fwkern.conf` file, create a new one.

2. **Add** these lines:
   ```
   fw_link_state_propagation_enabled=1
   fw_manual_link_state_propagation_enabled=1
   fw_lsp_pair<1-4>="<interface_name1,interface_name2>"
   ```

3. **Reboot** the computer.

   **Note** - Link State Propagation is a Firewall Software Blade feature. It is supported for Security Gateways and clusters. You must configure Link State Propagation for each cluster member.

### Managing Ethernet Protocols

This feature is supported in R77.10 and higher.

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.

By default, these protocols are allowed by the Security Gateway.

**To manage the traffic of Ethernet protocols:**

1. **Change** the value of global parameter `fwaccept_unknown_protocol` in `FWDIR/modules/fwkern.conf`. The default value is 1.

2. **Create** user defined tables in `FWDIR/conf/user.def`:
   ```
   ifndef __user_def__
   define __user_def__
   
   /* User defined INSPECT code */
   
   allowed_ethernet_protocols={ <0x44,0x44> );
   dropped_ethernet_protocols={ <0x4,0x4> );
   
   fendif /*__user_def__*/
   ```

   Traffic is allowed if:
   - `fwaccept_unknown_protocol` is enabled
   - OR protocol is in `allowed_ethernet_protocols` table
   - AND NOT in `dropped_ethernet_protocols` table
VLANs

When switches are configured with VLANs, VLAN traffic can pass through our bridge in Access mode or in Trunk mode:

- **Access mode** (VLAN translation) – Bridge is constructed from two VLAN interfaces.
- **Trunk mode** – Bridge is constructed from two non-VLAN interfaces. The VLAN tag is not removed, and the firewall processes the tagged packet. The traffic passes with the original tag to its destination.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>Switch</td>
</tr>
<tr>
<td>3</td>
<td>Access mode bridge 1 with VLAN translation</td>
</tr>
<tr>
<td>4</td>
<td>Access mode bridge 2 with VLAN translation</td>
</tr>
<tr>
<td>5</td>
<td>VLAN 3 (eth 1.3)</td>
</tr>
<tr>
<td>6</td>
<td>VLAN 33 (eth 2.33)</td>
</tr>
<tr>
<td>7</td>
<td>VLAN 2 (eth 1.2)</td>
</tr>
<tr>
<td>8</td>
<td>VLAN 22 (eth 2.22)</td>
</tr>
</tbody>
</table>
Access Mode VLAN

When the switch is configured in Access Mode, create the bridge from two VLAN interfaces as the slave ports of the bridge. For VLAN translation, use different numbered VLAN interfaces to create the bridge. You can build multiple VLAN translation bridges on the same Security Gateway.

Note - VLAN translation is not supported over bridged FONIC (Fail open NIC) ports. See sk85560 http://supportcontent.checkpoint.com/solutions?id=sk85560.

To configure VLAN translation:

1. Add the VLANs. In the WebUI: Network Management > Network Interfaces > Add > VLAN. The Add VLAN window opens. Configure the interfaces of the VLAN.

2. Open the Add Bridge window and select the VLAN interfaces in the Bridge tab.

VLAN ID 2 traffic will be translated into VLAN ID 22, and vice versa.
Special Protocols

**PVST** - Per-VLAN Spanning Tree. PVST is a proprietary Cisco version of STP and maintains a spanning tree instance for each VLAN. It uses ISL Trunking and lets a VLAN trunk be forwarded for some VLANs and blocked for others. Because PVST treats each VLAN as a separate network, it can load balance traffic at layer-2. It forwards some VLANs on one trunk and other VLANs on another trunk without causing a Spanning Tree loop.

**BPDU** - Bridge Protocol Data Unit. BPDU frames are data messages that are exchanged across the switches within an extended LAN that uses STP topology.

When VLAN translation is configured, BPDU frames can arrive with the wrong VLAN number to the ports through the bridge. This mismatch can cause the switch port to enter blocking mode. In Active-Standby mode only, there are options to avoid blocking mode.

**To disable BPDU forwarding:**

1. Edit the file `/etc/rc.d/init.d/network`
2. After the line:
   ```bash
   . /etc/init.d/functions
   ```
   Add this line:
   ```bash
   /sbin/sysctl -w net.bridge.bpdu_forwarding=0
   ```
3. Save the file.
4. Reboot the Security Gateway.

**To configure the gateway to allow only IPv4, IPv6, and ARP traffic:**

1. Add to `$FWDIR/modules/fwkern.conf` the line: `fwaccept_unknown_protocol=0`
2. Reboot the Security Gateway.

**Trunk Mode**

If you configure the switch ports as VLAN trunk, the Check Point bridge should not interfere with the VLANs. To configure bridge with VLAN trunk, create the bridge from two interfaces (no VLAN).

- **Note** - VLAN translation is not supported in Trunk mode.

**Configuring a DLP Gateway in Bridge Mode**

When setting up a dedicated DLP gateway, Check Point recommends that you configure the DLP gateway as a bridge, so that the DLP gateway is transparent to network routing.

You can deploy DLP in bridge mode, with the requirements described in this section for routing, IP address, and VLAN trunks.

Note the current limitations:

- In an environment with more than one bridge interface, the DLP gateway must not see the same traffic twice on the different interfaces. The traffic must not run from one bridged segment to another.
- Inter-bridge routing is not supported. This includes inter-VLAN routing.
- If the bridge interface is connected to a VLAN trunk, all VLANs will be scanned by DLP. You cannot exclude specific VLANs.

- Routing from the bridge interface to a Layer3 interface, and from Layer3 interface to the bridge, is not supported. Traffic on the bridge interface must run through the bridge or be designated to the DLP gateway.

- From R76, the DLP gateway in bridge mode can be in a cluster, in High Availability mode. But the Ask User action and the UserCheck Agent are not supported.

- If the DLP gateway in bridge mode is behind a cluster, the cluster must be in High Availability mode.

- Bond High Availability (HA) or Bond Load Sharing (LS) (including Link Aggregation) are not supported in combination with bridge interfaces.

### Required Routing in Bridge Mode

There must be routes between the DLP gateway and the required servers:

- Security Management Server
- DNS server
- Mail server, if an SMTP Relay server is configured to work with the gateway
- Active Directory or LDAP server, if configured to work with the gateway

There must be a default route. If this is not a valid route, it must reach a server that answers ARP requests.

If UserCheck is enabled, configure routing between the DLP gateway and the network.

### Configuring Bridge IP Address

The bridge interface can be configured without an IP address, if another interface is configured on the gateway that will be used to reach the UserCheck client and the DLP Portal.

If you do add an IP address to the bridge interface after the Security Gateways are started, run the `cpstop` and `cpstart` commands to apply the change.

### Required VLAN Trunk Interfaces

- A single bridge interface must be configured to bind the DLP gateway for a VLAN trunk.
- If an IP address is configured on the bridge, the IP address must not belong to any of the networks going through the bridge. Users must have routes that run traffic through the bridge interface of the DLP gateway. The gateway handles this traffic and answers to the same VLAN of the original traffic.
- In a VLAN trunk interface, another interface must be configured as the management interface for the required bridge routing.
Virtual System in Bridge Mode

A Virtual System in bridge mode implements native layer-2 bridging. A typical bridge mode scenario incorporates an 802.1q compatible VLAN switch on either side of the VSX Gateway. The Virtual System interfaces do not have IP addresses.

A Virtual System in bridge mode:
- Simplifies virtual network management
- Does not segment an existing virtual network
- Requires manual topology configuration to enforce anti-spoofing

To configure a Virtual System to use bridge mode, define it as a **Virtual System in bridge mode** when you first create it. You cannot reconfigure a non-Bridge mode Virtual System to use bridge mode later.
Core Network Security

Many Enterprise environments are based on core networks. Situated adjacent to core network backbone switches, VSX protects the internal network by providing security at layer-2, layer-3 or both. VSX communicates with the core network using the existing infrastructure. With Virtual Systems in the Bridge Mode, VSX can protect departmental networks, while simultaneously preventing network segmentation. In this case, switches are located at the entrance to each department's network.

VSX ensures connectivity between the core network and the Internet or external networks, while providing perimeter security. Security can be configured on a per VLAN basis.

Three Layer Hierarchical Model

A three-layer hierarchical model is used in large, high-traffic network environments.

1. A core network, with high-speed backbone switches that direct traffic to and from the Internet and other external networks.
2. A distribution layer, with routers, for connectivity between the core and the access layer.
3. An access layer, with redundant LAN switches, that forward traffic to and from internal networks.

VSX in Active/Standby Bridge Mode is incorporated in the distribution layer, enforcing the security policy.

The routers direct external traffic to the appropriate Virtual System through a segregated VLAN. Inspected traffic exits the Virtual System through a separate segregated VLAN, to the routers and then to internal destinations.

Configuring Virtual Systems for Active/Standby Bridge Mode

To configure a Virtual System to use bridge mode, define it as such when you first create the object.
To configure a Virtual System for the Active/Standby Bridge Mode:

1. In the Virtual System General Properties page of the new Virtual System object, select **Bridge Mode**.
2. Click **Next**.
   The Virtual System Network Configuration window opens.
3. Configure the external and internal interfaces for the Virtual System.
4. **Optional**: Select **Enable Layer-3 Bridge Interface Monitoring**.
   The IP address must be unique and on the same subnet as the protected network.
5. Click **Next** and then click **Finish**.

Enabling Active/Standby Bridge Mode for a New Member

When you create a new cluster member, enable the cluster options during the first configuration.

1. In the Gaia First Time Configuration Wizard **Products** page, select **ClusterXL**.
2. From the VSX Gateway CLI, run: `cpconfig`
   - If you enable the **Per Virtual System State** feature, (required for VSLS), Active/Standby Bridge Mode is enabled automatically.
   - If you chose not to enable Virtual System Load Sharing, an option to enable **Active/Standby Bridge Mode** appears. Enter `y` and continue with the gateway configuration.

Enabling Active/Standby Bridge Mode for Existing Members

To enable the Active/Standby Bridge Mode on existing Virtual Systems:

1. Run: `cpconfig`
2. Enable **ClusterXL for Bridge Active/Standby**.
3. Reboot the member.

Enabling Active/Active Bridge Mode when Creating Member

When you create a new VSX Gateway to use as a cluster member, configure it as a cluster member when you first define the gateway.

1. Run: `cpconfig`
2. At *Would you like to install a Check Point clustering product, enter:* y
3. If prompted to disable Active/Standby Bridge Mode, enter: n
4. Continue with the `cpconfig` options as usual.

Enabling Active/Active Bridge Mode for Existing Members

To enable the Active/Active Bridge mode for existing cluster members:

1. Run: `cpconfig`
2. Enable **cluster membership for this member**.
   (If a numerical value appears here, cluster membership has already been enabled).
3. Disable **ClusterXL for Bridge Active/Standby**.
4. Reboot the member.
Custom or Override in Bridge Mode

You must manually define network interfaces, if:

- You used the Custom Configuration template when you created the VSX Gateway
- You selected Override Creation Template and this is a Virtual System in bridge mode

In the Virtual System wizard > Virtual System Network Configuration, add the external and internal interfaces and links to devices.

If the Virtual System is on IPSO, select Enable Layer-3 Bridge Interface Monitoring. Define the IP address and net mask. Make sure the IP address to be monitored is on a different subnet than the subnet that handles bridge traffic.

VLAN Shared Interface Deployment

In this deployment, each member connects to pair of redundant switches through a VLAN trunk. All Virtual Systems in a given member share the same VLAN trunk.

VSX Clusters

A VSX cluster has two or more identical, interconnected VSX Gateways for continuous data synchronization and transparent failover. Virtual System Load Sharing (VSLS) enhances throughput by distributing Virtual Systems, with their traffic load, among multiple, redundant machines.
Configuring Clusters for Active/Standby Bridge Mode

To enable the Active/Standby Bridge Mode for a cluster:
1. Open SmartDashboard.
2. From the Network Objects tree, double-click the VSX Cluster object.
   The VSX Cluster Properties window opens.
3. Select Other > VSX Bridge Configuration.
4. Select Check Point ClusterXL.
   The Active/Standby Bridge Mode loop detection algorithms in ClusterXL is enabled.

Configuring Clusters for Active/Active Bridge Mode

To enable the Active/Active Bridge mode for a cluster:
1. Open SmartDashboard.
2. From the Network Objects tree, double-click the VSX Cluster object.
   The VSX Cluster Properties window opens.
3. Select Other > VSX Bridge Configuration.

Separate Interfaces in Bridge Mode

The Virtual System Network Configuration page for the Separate Interfaces template in the Bridge Mode opens.

To configure the external and internal interfaces:
1. Select the desired interfaces for the internal and external networks from the appropriate list.
   If the selected Interface is a VLAN interface, enter the same VLAN tag in both the external and internal VLAN Tag fields. This field is not available for non-VLAN interfaces.
2. Define the topology for the internal interface:
   - Select Not Defined if you do not wish to define an IP address.
   - Select Specific and then select an IP address definition from the list. IP address definitions can be based on object groups or predefined networks that define the topology.
3. To create a new IP address definition:
   a) Select Specific, and click New.
   b) Select Group to define an object group, or Network to define network properties.
4. Enable Layer-3 bridge interface monitoring to enable layer 3 network fault detection for this Virtual System.
   Enter an IP address and subnet mask, which continuously monitors the specified network for faults or connectivity issues. The IP address/subnet define the network on which the Virtual System resides.
5. Complete the definition process.
Virtual System Load Sharing (VSLS)

VSX clusters can efficiently balance network traffic load by distributing active Virtual Systems amongst cluster members. This capability is known as **Virtual System Load Sharing (VSLS)**.

In a deployment scenario with three cluster members, each with three Virtual Systems: an equalized Load Sharing deployment might have one active Virtual System on each cluster member.

A different member hosts the active peer for each Virtual System. This distribution spreads the load equally amongst the members. When you create a Virtual System, VSX automatically assigns standby and backup states to the appropriate peers and distributes them among the other cluster members.

In the event that a cluster member fails, VSLS directs traffic destined to affected Virtual Systems to their fully synchronized standby peers, which then become active. At the same time, a backup Virtual Systems switches to standby, and synchronizes with the newly active Virtual System.

In the event that an individual active Virtual System fails, it immediately fails over to its standby peer and one of its backup peers becomes the standby, synchronizing with the newly active peer.

**Converting from High Availability to VSLS**

To convert an existing High Availability cluster to VSLS Load Sharing:

1. Close SmartDashboard.
2. On each member:
   a) Run `cpconfig`
   b) Enable the **Per Virtual System State**.
   c) Enable **ClusterXL for Bridge Active/Standby**.
3. Restart the members: `cpstop` and `cpstart`
4. On the management server, enter Expert mode.
5. Run: `vsx_util convert_cluster`
7. Enter the administrator user name and password.
8. Enter the VSX cluster name.
9. Enter: `ls`
10. At the "Proceed with conversion?" prompt, enter: `y`
11. Select an option to distribute Virtual Systems among members:
   a) Distribute all Virtual Systems equally.
   b) Set all Virtual Systems as **Active** on the same member.

   **Note** - You cannot convert a VSX cluster to the VSLS mode if it contains Virtual Systems in the Active/Active Bridge mode or Virtual Routers.
Using Monitor Mode

In This Section:

Introduction to Monitor Mode ...........................................................61
Configuring Monitor Mode ................................................................62

Introduction to Monitor Mode

Monitor Mode can be configured on Check Point Security Gateway interfaces. It lets Check Point Security Gateways monitor traffic from a mirror port or span port on a switch. Use Monitor Mode to analyze network traffic without changing the production environment. The mirror port on a switch duplicates the network traffic and sends it to the monitor interface on the gateway to record the activity logs.

You can use mirror ports in these scenarios:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Application Control and IPS blades before you buy them

The mirror port does not enforce a policy or do any active operation (prevent/drop/reject) on network traffic. It can be used only to evaluate the monitoring and detecting capabilities of the Software Blades.

All duplicated packets that arrive at the monitor interface of the gateway are terminated and will not be forwarded.

The Security Gateway does not send traffic through the monitor interface.

Supported Software Blades for Monitor Mode

These Software Blades support Monitor mode for Security Gateway deployment:

<table>
<thead>
<tr>
<th>Supported Blade</th>
<th>Supports Gateways in Monitor Mode</th>
<th>Supports VS in Monitor Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DLP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Threat Emulation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Monitor Mode - Software Blades Not Supported

These features, Software Blades and deployments are not supported in Monitor mode:

- NAT
- IPsec VPN
- HTTPS Inspection
- Mobile Access
- DLP with FTP
- HTTP/HTTPS proxy
- Anti-Spam and Email Security
- QoS
- Traditional Anti-Virus
- User Authentication
- Client Authentication

Unsupported Monitor Mode Deployments

These are deployments do not support Monitor Mode:

- Access to Portals
- Multiple TAP interfaces when the same traffic is monitored

Configuring Monitor Mode

You can configure a mirror or TAP port to duplicate network traffic that is sent to a Security Gateway. The gateway inspects the traffic but does not drop packets.

Connect the Security Gateway to a mirror port on the switch that duplicates the appropriate ports and VLANs.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switch with mirror port</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Servers</td>
</tr>
<tr>
<td>3</td>
<td>Computers</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway in monitor mode</td>
</tr>
<tr>
<td>5</td>
<td>Management for Security Gateway</td>
</tr>
</tbody>
</table>

**Note** - Make sure that one mirror port on the switch is connected to one interface on the Security Gateway.

To enable monitor mode on the Security Gateway from the WebUI:

1. From the navigation tree, click **Network Interfaces**.
2. Select the interface and click **Edit**.
3. Click the **Ethernet** tab.
4. Click **Monitor Mode**.
5. Click **OK**.

To enable monitor mode on the Security Gateway from the clish:

Run this command:

```bash
> set interface <int name> monitor-mode on
```
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 is 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
   ```
2. 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>-r</td>
<td>Removes boot security</td>
</tr>
<tr>
<td>-g</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`.

**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>
</tbody>
</table>
### Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<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.)&lt;br&gt;Note - Do NOT move these files.</td>
</tr>
</tbody>
</table>

---

**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 <em>(fwd, fwm, vpnd, snmpd</em> 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 <em>(fwd, fwm, vpnd</em> 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>
Legacy Authentication

In This Section:

- Configuring Authentication ................................................................. 72
- Authentication Schemes ......................................................................... 73
- Authentication Methods ........................................................................ 79
- Creating Users and Groups .................................................................... 88
- Configuring Authentication Tracking ....................................................... 89
- Configuring Policy for Groups of Windows Users ..................................... 90

This section covers how to work with legacy authentication methods.

Configuring Authentication

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

- **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.
   g) Click OK.

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 give users access to specified 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 give access through RADIUS server groups:

1. In SmartDashboard, go to Manage > Server and OPSEC Applications.
   Servers and OPSEC Applications window opens.
2. Click New > RADIUS.
   The RADIUS Server Properties window opens.
3. Configure new server properties:
   a) Name the RADIUS Server object.
   b) Click New to create a new Host Object.
      Host Node window opens.
   c) Enter the Name and the IP Address of the new RADIUS Host object, and click OK.
   d) Select the Service - RADIUS (on port 1645) or NEW-RADIUS (on port 1812 service).
      Note - 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.
   e) Enter the Shared Secret that you configured on the RADIUS server.
   f) Select the version - RADIUS Ver. 1.0 Compatible (RFC 2138 compliant) or RADIUS Ver. 2.0 Compatible (RFC 2865 compliant).
   g) Select the Priority, if you use more than one RADIUS Authentication server.
   h) Click OK.
   i) Click Close.
4. Create a generic* External User Profile:
   a) Go to Manage > Users and Administrators.
      Users and Administrators window opens.
   b) Go to New > External User Profile > Match all users.
      External User Profile Properties window opens.
   c) In the Authentication tab, select RADIUS as the Authentication Scheme.
   d) Select the created RADIUS server (not the node) from the drop-down list.
   e) Click OK.
   f) Click Close.
5. Define the RADIUS user groups:
   a) Go to Manage > Users & Administrators.
      Users and Administrators window opens.
   b) Go to New > User Group.
      Group Properties window opens.
   c) Enter the name of the group in this format: RAD_ <group to which the RADIUS users belong>. Make sure the group is empty.
d) Click **OK**.
e) Click **Close**.

6. Create the required Rule Base rules to allow access to RADIUS users.
7. Save the changes.
8. Close all SmartConsole windows.
9. On the Security Management Server, use GuIDBedit to change the value of the `add_radius_groups` attribute from false to true.
10. Save.
12. Open SmartDashboard.
13. Install the policy.
14. On the RADIUS server, edit the RADIUS users to include a `class` RADIUS attribute on the users' `Return` list that corresponds to the user group that they access.

**To use a different attribute instead of the class attribute:**
1. Close all SmartConsole windows
2. On the Security Gateway, use GuIDBedit to modify the value of the `firewall_properties` attribute `radius_groups_attr` to the new RADIUS attribute.
3. Save.
5. Open SmartDashboard.
6. Install the policy.
7. On the RADIUS server, make sure that you use the same RADIUS attribute on users' `Return` lists that corresponds to the Firewall user group that they access.

**Associating a RADIUS Server with Security Gateway**

You can associate users with the Radius authentication server in the **User PropertiesAuthentication** 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 32-bit Windows
   - `%SystemRoot%\SysWOW64\sdconf.rec` on 64-bit Windows

2. In SmartDashboard, right-click the gateway object and select **Edit >Authentication** page.
3. Enable SecurID authentication.
4. Define a user group. Select **Manage > Users & Administrators > New > User Group** (for example, SecurID_Users).
5. Enable SecurID authentication for Security Gateway users. Select **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 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. Make sure that connections 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).
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 86)

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 88).
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 86)

**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 88) 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.
   - 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 86)

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 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).

   ```
tower 3% telnet london 259
Trying 191.23.45.67 ... 
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: jim
FireWall-1 Password: ********
User authenticated by Internal auth.

Choose:
(1) Standard Sign On
(2) Sign Off
(3) Specific Sign On
```
Enter your choice: 3
Service: rstat
Host: palace
Client Authorized for service
Another one (Y/N): Y
Service: finger
Host: thames
Client Authorized for service
Another one (Y/N): n
Connection closed by foreign 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 88) for details.
2. From the Authentication page, edit the 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.
5. Double-click in the Action column to edit the Client Authentication Action Properties. The settings for Requires Sign On and Sign On Method are described in Client Authentication (on page 82).
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.

```
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.1httpd 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 xrmdrespawn0-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.
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.
Cooperative Enforcement

In This Section:

- Enforcement Mode ......................................................... 92
- NAT Environments ............................................................ 92
- Monitor Only Deployment Mode .......................................... 92
- Configuring Cooperative Enforcement .................................. 92

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.
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 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.
Content Security

In This Section:

Introduction to Content Security .......................................................... 93
Configuring Content Security ................................................................. 98
Advanced CVP Configuration: CVP Chaining and Load Sharing ............. 102

Introduction to Content Security

The firewall integrates Content Security capabilities with best-of-breed, OPSEC-certified applications. OPSEC applications enable organizations to select content screening applications that best meet their needs, while managing Content Security centrally. These applications:

- Protect against network viruses, by scanning data and URLs to prevent viruses, malicious Java and ActiveX components, and other malicious content from entering your organization.
- Prevent users from browsing to undesirable websites, by filtering URLs.
- Provide auditing capabilities and detailed reports.

For details, see the list of OPSEC Content Security solutions (http://www.opsec.com/solutions/sec_content_security.html).

Content security applications, like virus scanners, inspect the content of individual packets for specific services.

The Content Vectoring Protocol (CVP) is an API specification developed by Check Point used for integration with Anti-Virus servers. This API defines an asynchronous interface to server applications that validate file content. An important feature of CVP is scanning files for viruses or harmful applets as they pass through firewalls. CVP defines a client/server relationship that enables different Security Gateways to share a common content validation server.

In Service Provider environments, it can be offered as an add-on to Internet services, where it may be used for parental restriction of child Web surfing or on behalf of businesses that have an inherent distrust of Internet content.

Security Servers

Security servers are Check Point processes that are integrated into the firewall. They are user mode processes that provide content security for:

- HTTP
- FTP
- SMTP

There is also a generic TCP Security server. Security servers employ many ways of enforcing Content Security, including, checking whether the connections for these protocols are well formed, stripping script tags for HTTP, email address translation for SMTP, and file name matching for FTP.
In addition to Content Security, Security servers also perform authentication. For additional information on the authentication functions of the Security servers, refer to Authentication ("Legacy Authentication" on page 72).

**How a Server Mediates Connections**

The HTTP Security server is used as an example, but the method is the same for all Security servers.

When a packet is matched to a rule that contains a resource, the Inspection Module on a Security Gateway diverts a connection to a Security server. The Security server performs the Application Security checks, and, if necessary, diverts the connection to a Content Vectoring Protocol (CVP) server application. The Security server then returns the connection to the Inspection Module, which opens a second connection that is sent on the destination HTTP server.

The source IP address that appears to the destination server is the IP address of the client that originally opened the connection. The connection leaves the Security server with the source IP address of the Security Gateway, and the outbound kernel performs NAT so that the source IP address is that of the original client.

**Deploying OPSEC Servers**

OPSEC solutions, such as CVP and UFP servers, are deployed on dedicated servers. These servers are typically placed in the DMZ or on a private network segment. This allows fast secure connections between the CVP servers and the Security Gateway.
Performing scanning at the network perimeter is both safer and more efficient than performing the scanning at the desktop or on the application servers.

CVP Servers for Anti-Virus and Malicious Content Protection

**CVP and Anti-Virus Protection for SMTP and HTTP Traffic**

To perform virus scanning, the HTTP or SMTP security server transfers packets from the Security Gateway to another server running an OPSEC certified virus scanner. This method uses the Content Vectoring Protocol (CVP) to transfer packets to and from an OPSEC virus scanning server.

The virus scanning CVP server determines if there is a virus. If it finds a virus, it can:

- Return the file to the Security Gateway with the offending content removed (if the CVP server is configured to modify content), or
- Drop the file (if the CVP server is not allowed to modify content).

CVP uses TCP port 18181, by default.

**How a Connection is Handled by the HTTP Security Server**

This section describes how the HTTP Security server handles a connection where CVP checking is performed. The Security Gateway that runs the HTTP Security server acts as a proxy, and so is not an active participant in the connection.
The connection request/response process without a CVP server is:

1. HTTP client to HTTP server (request)
2. HTTP server to HTTP client (response)

The data that needs to be checked is carried in the response that comes from the Web server. Therefore, when a CVP server is used, the response is always checked. In that case, the connection request/response process is:

1. HTTP client to HTTP server (request)
2. HTTP server to CVP server (response)
3. CVP server to HTTP client (response)

Normally, only HTTP responses, which come from the Web server, are sent to the CVP server for checking. However, you also may wish to protect against undesirable content in the HTTP request, for example, when inspecting peer-to-peer connections. In this case, the connection request/response process is:

1. HTTP client to CVP server (request)
2. CVP server to HTTP server (request)
3. HTTP server to CVP server (response)
4. CVP server to HTTP client (response)

The HTTP Security server can be configured to send HTTP headers to the CVP server, as well as the HTTP message data.

**Improving CVP Performance for Web Traffic**

HTTP Security server performance can be significantly improved by ensuring that safe traffic is not sent to the CVP server. This reduces the number of connections opened with the CVP server. Nonetheless, sending all content for CVP checking provides better protection.

The Security Gateway considers non-executable picture and video files to be safe because they do not normally contain viruses.

The HTTP Security server identifies safe content by actually examining the contents of a file. It does not rely on examining the URL (for file extensions such as *.GIF) nor does it rely on checking the MIME type (such as image/gif) in the server response.

For configuration details, refer to Configuring CVP for Web Traffic Performance (on page 100).
Using CVP for Virus Scanning on FTP Connections

Virus scanning on FTP connections can be performed by transferring the file to a third-party Anti-Virus application using the CVP protocol.

The relevant rule for the connection specifies a resource that includes Content Vectoring Protocol (CVP) for Anti-Virus checking.

1. The FTP client establishes a connection via port 21 to the FTP server.
2. The Inspection Module monitors port 21 for GET and PUT commands, and determines that the CVP server must be invoked.
3. When the client initiates data transfer over port 20, the gateway diverts the connection into the FTP Security server.
4. The FTP Security server sends the file to be inspected to the CVP server.
5. The CVP server scans the FTP files and returns a Validation Result message, notifying the FTP Security server of the result of the scan.
6. The CVP server returns a clean version of the file to the FTP Security server.
7. Based on the Validation Result message, the FTP Security server determines whether to transfer the file, and takes the action defined for the resource, either allowing or disallowing the file transfer.
8. If allowed, the FTP Security server relays the FTP file on to the FTP server.

TCP Security Server

Malicious content can potentially be carried in any TCP service, not only SMTP, HTTP and FTP.
The TCP Security server is used to perform CVP or UFP Content Security by a third-party, OPSEC-compliant application, on any TCP Service.

For configuration details, refer to Performing CVP/UFP Inspection on any TCP Service (on page 101).

Configuring Content Security

Resources: What They Are and How to Use Them

To perform Content Security via the Security Rule Base, an object called a Resource is defined in SmartDashboard. Resources are used to match a specific kind of application layer content, (in other words, to specify what content you are looking for,) and to perform some action on the content.

Using a Resource turns on either kernel inspection or the Security servers, depending on what the resource is used for.

For instance, a rule can be created that will drop the connection and generate an alert if there are GETs or PUTs in an FTP transfer or if a specifically named file is part of the transfer. Another rule can drop email addresses or attachments while allowing the rest of the content through.

To specify the content you are looking for, regular expressions ("Regular Expression Syntax" on page 105) and wildcards can be used in the Resource.

The Resource is triggered when a rule includes the Resource, and a packet matching that rule is encountered. A Resource is applied per Service. If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the action in the rule and the action in the Resource are applied.
Creating a Resource and Using it in the Rule Base

To create a resource:

1. Select the Resources tab in the objects tree. Select the Resource Type, right-click, select a resource type, such as New URI or New SMTP.
2. Define the resource parameters in the General tab, and in the other tabs as required.
3. To use a service with a resource in a rule, right-click in the Service column of the rule, right-click, and select Add with Resource. In the Service with Resource window, select the service, and then select the Resource that will operate on the service. Click OK.

If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the action in the rule and the action in the Resource are applied.

Configuring Anti-Virus Checking for Incoming Email

The goal is to check incoming mail for viruses, as illustrated below. SMTP mail arrives from the Internet to a mail relay server (Mail_relay) in a DMZ segment. Before the mail is forwarded to the internal mail server (Mail_server), it undergoes virus checking by the Anti-Virus server (Anti_virus_server). Outgoing mail is sent from the mail server to the Internet.

To configure Anti-Virus checking for incoming email:

1. Create a host object for the machine on which the third-party, OPSEC server application is installed.
2. Create an OPSEC Application object to represent the OPSEC Application server, and associate it with the host object created in step 1.
3. Define an SMTP resource that uses the OPSEC Application object, and associate it with the OPSEC Application object created in step 2. Specify the matching, and the content checking to be performed.
4. Define rules that use the resource.

To implement Anti-Virus checking for incoming email:

1. Create a host object (e.g. Anti_virus_server) for the machine on which the third-party OPSEC Server application is installed.
2. Create an OPSEC Application object to represent the OPSEC application server, and associate it with the host object created in step 1. Initialize Secure Internal Communication between the
OPSEC Application and the Security Management Server. In the CVP Options tab, verify that FW1_cvp is selected, and click OK.

3. Define an SMTP resource that uses the OPSEC object, and associate it with the OPSEC Application object created in step 2. Specify the matching and the content checking to be performed.

   a) In the General Tab, give the Resource a Name (such as virus_check). Select both the Mail Delivery and the Error Mail Delivery options, as well as Exception Tracking.

   b) In the Match tab, for the Sender put *, and for the Recipient put *@your_domain, (for example *@company.com).

   c) In the Action1 tab, define the Rewriting Rules, if any.

   d) In the Action2 tab, define the Attachment handling, if any. Define the largest allowed email attachment.

4. In the CVP tab, check Use CVP (Content Vectoring Protocol), select the CVP server defined in step 1, and define the CVP Server Options and Reply Order.

5. Click OK. A message may appear regarding stripping MIME of type "message/partial". Accepting the MIME strip of type "message/partial" changes configuration to the Action2 tab. The Strip MIME of Type field will contain message/partial. Stripping the Multipurpose Internet Mail Extension (MIME) type of message/partial will not allow multiple-part messages to be accepted for scanning.

6. Define a pair of rules that will perform virus checking on incoming mail, and a rule to allow outbound email.

7. Install the security policy: Policy >Install.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>mail_relay</td>
<td>smtp</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Incoming to mail relay</td>
</tr>
<tr>
<td>mail_relay</td>
<td>mail_server</td>
<td>smtp-&gt;virus_check</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Incoming virus scan</td>
</tr>
<tr>
<td>mail_server</td>
<td>Any</td>
<td>smtp</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Outgoing email</td>
</tr>
</tbody>
</table>

**Configuring CVP for Web Traffic Performance**

The performance of the CVP server when inspecting HTTP connections can be enhanced by ensuring that only unsafe file types are sent to the CVP server for inspection. For background information, refer to Improving CVP Performance for Web Traffic (on page 96).

**To configure CVP checking for Web traffic:**

1. Create a host object for the machine on which the CVP Server application is installed.
2. Create an OPSEC Application object to represent the CVP server, and associate it with the host object created in step 1.
3. Define a URI resource that uses the OPSEC Application object, and associate it with the OPSEC Application object created in step 2. Give it a name (such as Internal.HTTP.CVP), specify the matching, and the content checking to be performed.

4. In the CVP tab, select **Send only unsafe file types to the CVP server**, and the other required CVP options.

5. Associate the Resource with the HTTP Service, and place it in a rule in the Security Rule Base. Refer to the sample rule shown below.

**Sample URI Resource in a Rule Base**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal_LAN</td>
<td>Any</td>
<td>http-Internal.HTTP.CVP</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**Performing CVP/UFP Inspection on any TCP Service**

In this procedure, you will create and configure a TCP service and a TCP resource. These steps are done with the Firewall tab open, by selecting different tabs in the left panel.

**To configure CVP or UFP inspection on any TCP service:**

1. Open the **Services** tab.
2. Right-click TCP and choose **NewTCP**. Fill in the general properties of the new TCP service.
3. Click **Advanced**.
4. In the **Advanced TCP Service Properties** window, check **Enable for TCP Resource** and then click **OK**.
5. Open the **Servers and OPSEC Applications** tab, right-click **OPSEC Applications**, and choose **New > OPSEC Applications**.
6. In the **OPSEC Application Properties** window, name the server and select **Server Entities > CVP and UFP**.
7. Select a host to act as the CVP and UFP server.
8. In the **UFP Options** and **CVP Options** tabs, select the TCP service configured in the Services tab.
9. Click **OK**.
10. Open the **Resources** tab, right-click **Resources**, and choose **New > TCP**.
11. In the **TCP Resource Properties** window, provide a name for the resource and choose **UFP** or **CVP**.
12. The tab that appears in this window depends on whether you chose UFP or CVP. In this tab, select the CVP/UFP server you configured in OPSEC Applications.
13. Click **OK**.
14. Add a rule to the Rule Base: in the **Service** column, select **Add with Resource**.
15. In the **Service with Resource** window, select the configured TCP service.
16. In the **Resource** drop-down list, select the configured TCP resource.
17. Install the security policy: **Policy > Install**.
Advanced CVP Configuration: CVP Chaining and Load Sharing

Introduction to CVP Chaining and Load Sharing
Traffic that crosses the Security Gateway can be checked using CVP servers. CVP checking is available for Web, Mail, FTP and TCP traffic. For detailed explanations, see:

- CVP and Anti-Virus Protection for SMTP and HTTP Traffic (on page 95)
- Using CVP for Virus Scanning on FTP Connections (on page 97)

It is possible to chain CVP servers in order to combine functionality, and to perform Load Sharing between CVP servers, in order to speed up CVP checking.

CVP Chaining

CVP servers can be chained for the purpose of combining functionality. Chaining is useful when each of the CVP servers performs a different task, such as scanning for viruses, or blocking large email attachments. In the configuration shown below, the Security Gateway server invokes the first, second, and third CVP servers in turn.

Chained CVP servers are invoked in the order set by the administrator in the CVP Group object. When choosing a chaining order, consider whether there are any security or connectivity issues.

The order in which the chained servers are called is relative to the response of the server. This is the case whether the server is on the unprotected (external interface) side or on the protected (internal interface) side.

Consider a user at an internal FTP client who is downloading a file from an external FTP server. CVP checking is performed on the response from the FTP server (that is, on the downloaded file) in the order defined in the CVP Group object.

There is one exception to this order. The HTTP Security server allows CVP checking to be performed on the HTTP request. CVP checking of HTTP requests is performed by the CVP servers in the reverse of the order specified in the CVP Group object.

CVP chaining works only if all servers in the chain are available. If one or more of the servers is unavailable, the whole CVP session is dropped. This is because skipping one of the servers may
contradict the Security Policy. For example, the Security Policy may specify that both virus scanning and blocking of large attachments are mandatory.

CVP Load Sharing

Identical CVP servers can be configured to share the load among themselves. Load Sharing can speed up CVP checking by allowing many CVP sessions to run simultaneously on more than one CVP server.

Two Load Sharing methods are available:

- **Round robin**: The Security server sends each new CVP session to a different CVP server in turn.
- **Random**: The Security server sends each new CVP session to a randomly chosen CVP server.

It is possible to configure a Load Sharing suspension period for a CVP server that does not respond. During that period of time, that CVP server does not take part in the Load Sharing group.

CVP Load Sharing is implemented by defining a Resource that invokes a group of CVP servers. The order in round robin mode is configured in the CVP Group object.

Combining CVP Chaining and Load Sharing

It is possible to combine CVP chaining and Load Sharing. The following diagram shows three CVP servers. Two perform Load Sharing between themselves, and the Load Sharing group is chained with another CVP server.
It is possible to put a Load Sharing group into a CVP chain, but it is not possible to perform Load Sharing between chained CVP groups.

Configuring CVP Chaining and Load Sharing

1. For each CVP server, define a CVP server object. To define a CVP server object, right-click in the Servers and OPSEC Application tree, and select New > OPSEC Application. In the OPSEC Application Properties window, General tab, make sure that the selected Server Entities include CVP.

2. Define a CVP Group object. A CVP Group object contains CVP server objects, and is used in the same way as an OPSEC Application object for a CVP server. To define a CVP Group object, right-click the Servers and OPSEC Application tree, and select New > CVP Group.

3. In the CVP Group Properties window, add the CVP servers to the group.

4. Select the Work distribution method: Either Load Sharing or Chaining.

5. If you select Load Sharing, define the Load Sharing method, and the Load Sharing suspend timeout, if any.

6. Create a Resource object. In the Resources tree, right-click and select one of the following: New > URI, New > SMTP, New > FTP, or New > TCP. Define the content security capabilities.

7. In the CVP Server field in the CVP tab of the Resource object, select the CVP Group defined in step 2.

8. In the Security Rule Base, define a rule that uses the Resource.

9. Save and install the security policy: Policy > Install.
Regular Expressions

In This Appendix

Regular Expression Syntax ................................................................. 105
Using Non-Printable Characters ......................................................... 106
Using Character Types ........................................................................ 106

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Backslash</td>
<td>escape metacharacters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>non-printable characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>character types</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square Brackets</td>
<td>character class definition</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>subpattern, to use metacharacters on the enclosed string</td>
</tr>
<tr>
<td>{min[,max]}</td>
<td>Curly Brackets</td>
<td>min/max quantifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n} - exactly n occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,m} - from n to m occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,} - at least n occurrences</td>
</tr>
<tr>
<td>.</td>
<td>Dot</td>
<td>match any character</td>
</tr>
<tr>
<td>?</td>
<td>Question Mark</td>
<td>zero or one occurrences (equals {0,1})</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>zero or more occurrences of preceding character</td>
</tr>
<tr>
<td>+</td>
<td>Plus Sign</td>
<td>one or more occurrences (equals {1,})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vertical Bar</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex</td>
<td>anchor pattern to beginning of buffer (usually a word)</td>
</tr>
<tr>
<td>$</td>
<td>Dollar</td>
<td>anchor pattern to end of buffer (usually a word)</td>
</tr>
<tr>
<td>-</td>
<td>hyphen</td>
<td>range in character class</td>
</tr>
</tbody>
</table>
Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>&quot;control-x&quot;, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>

Using Character Types

To specify types of characters in patterns, escape the reserved character.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit [0-9]</td>
</tr>
<tr>
<td>\D</td>
<td>any character that is not a decimal digit</td>
</tr>
<tr>
<td>\s</td>
<td>any whitespace character</td>
</tr>
<tr>
<td>\S</td>
<td>any character that is not whitespace</td>
</tr>
<tr>
<td>\w</td>
<td>any word character (underscore or alphanumeric character)</td>
</tr>
<tr>
<td>\W</td>
<td>any non-word character (not underscore or alphanumeric)</td>
</tr>
</tbody>
</table>
Defining a Custom Default Filter • 66
Deleting a Rule • 20
Deploying OPSEC Servers • 94
Dynamic Registration Using IGMP • 9

Editing the ISP Redundancy Script • 29
Enabling Active/Active Bridge Mode for Existing Members • 56
Enabling Active/Active Bridge Mode when Creating Member • 56
Enabling Active/Standby Bridge Mode for a New Member • 56
Enabling Active/Standby Bridge Mode for Existing Members • 56
Enabling Client Authentication Wait Mode • 85
Enforcement Mode • 92

Force ISP Link State • 29
Fully Automatic Sign On • 84
fwboot bootconf • 69

Granting User Access Using RADIUS Server Groups • 74

How a Connection is Handled by the HTTP Security Server • 95
How a Server Mediates Connections • 94
How the Gateway Searches for Users • 72
HTTP • 31

Importance of Rule Order in User Authentication • 80
Important Information • 3
Improving CVP Performance for Web Traffic • 96
Installing and Configuring Session Authentication Agent • 81
Installing User Information in the Database • 89
Introduction to Bridge Mode • 37
Introduction to ConnectControl • 30
Introduction to Content Security • 93
Introduction to CVP Chaining and Load Sharing • 102
Introduction to Monitor Mode • 61
IP Multicast Group Addressing • 9
IPv6 Neighbor Discovery • 48
ISP Redundancy • 24
ISP Redundancy Modes • 24

Legacy Authentication • 72
Load-Balancing Methods • 30
Logical Server Types • 31

Management over Bridge • 46
Managing Default Filter and Initial Policy • 68
Managing Ethernet Protocols • 49
Manual Sign On • 83
Microsoft Networking Services Security • 12
Monitor Mode - Software Blades Not Supported • 62
Monitor Only Deployment Mode • 92
Monitoring Events Related to DoS Mitigation • 23
Multicast Access Control • 9
Multicast Routing Protocols • 9

NAT Environments • 92

Operating System Password • 73
Other • 33
Overview • 14

Partially Automatic Sign On • 84
Performing CVP/UFP Inspection on any TCP Service • 101
Per-Interface Multicast Restrictions • 10
Persistency By Server • 34
Persistency By Service • 34
Persistent Server Mode • 34
Persistent Server Timeout • 35

RADIUS • 73
Rate Limiting for DoS Mitigation • 14
Regular Expression Syntax • 105
Regular Expressions • 105
Required Routing in Bridge Mode • 53
Required VLAN Trunk Interfaces • 53
Reserved Local Addresses • 10
Resolving Access Conflicts • 86
Resources
What They Are and How to Use Them • 98
Restricting Access to Servers and Shares (CIFS Resource) • 12
Routing and Bridges • 45

SecurID • 76
Securing Microsoft Networking Services (CIFS) • 12