13 March 2017

Security Gateway

R80.10

Technical Administration Guide

Check Point
SOFTWARE TECHNOLOGIES LTD.

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 R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

Latest Version of this Document

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

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 R80.10 Technical Administration Guide.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=TBD.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

Revision History

Date	Description
13 March 2017	First release of this document

Contents

About This Guide

This Technical Administration Guide is a collection of advanced, less-frequently used Security Gateway features. Each section is an independent feature.

Multicast Access Control

Multicast IP transmits one copy of each datagram (IP packet) to a multicast address, where each recipient in the group takes their copy. The routers in the network forward the datagrams only to routers and hosts with access to receive the multicast packets.

To configure multicast access control:

1. Open a gateway object.
2. On the **Network Management** page, select an interface and click **Edit**.
3. On **Interface** > **Advanced**, click **Drop Multicast packets by the following conditions**.
4. 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**

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

   If you do not define access restrictions for multicast packets, multicast datagrams to one interface of the gateway are allowed out of all other interfaces.
5. Click **Add**.

   The **Add Object** window opens, with the **Multicast Address Ranges** object selected.
6. Click **New** > **Multicast Address Range**.

   The **Multicast Address Range Properties** window opens.
7. Enter a name for this range.
8. Define an **IP address Range** or a **Single IP Address** in the range: **224.0.0.0** - **239.255.255.255**.

   Class D IP addresses are reserved for multicast traffic and are allocated dynamically. The multicast address range `224.0.0.0 - 239.255.255.255` is used only for the destination address of IP multicast traffic.

   Every IP datagram whose destination address starts with `1110` is an IP multicast datagram. The remaining 28 bits of the multicast address range identify the group to which the datagram is sent.

   The `224.0.0.0 - 224.0.0.255` range is reserved for LAN applications that are never forwarded by a router. These addresses are permanent host groups. For example: an ICMP request to `224.0.0.1` is answered by all multicast capable hosts on the network, `224.0.0.2` is answered by all routers with multicast interfaces, and `224.0.0.13` is answered by all PIM routers. To learn more, see the IANA website (http://www.iana.org/assignments/multicast-addresses).

   The source address for multicast datagrams is always the unicast source address.

9. Click **OK**.
10. In the **Add Object** window, click **OK**.
11. In the **Interface Properties** window, click **OK**.
12. In the gateway window, click **OK**.
13. In the Rule Base, add a rule that allows the multicast address range as the **Destination**.
14. In the **Services** of the rule, add the multicast protocols.
    - **Multicast routing protocols** - For example: Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).
    - **Dynamic registration -** Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know they want to belong to a specified multicast group. Hosts can leave or join the group at any time.
15. Install the policy.

Rate Limiting for DoS Mitigation

Rate Limiting is a defense against DoS (Denial of Service) attacks. A policy limits traffic coming from specified sources and 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 traffic from geographic sources that are not in your business profile. You can configure white-list bypasses.

Important: During the installation of the Access Control policy on the gateway, the rate limiting policy is not enforced.

Rate Limiting Support

Rate Limiting for DoS Mitigation is supported on:

- Gaia gateways with Performance Pack installed.
- VSX. On R77.20 and higher, you can configure different settings for the Virtual Systems or global parameters for all of them. On 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, or in batch mode ("Adding Rules in Batch Mode" on page 13).

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.

Creating Quota Rules

To prevent Denial of Service (DoS) attacks, add **quota** rules to a policy.

Syntax:

```
fw samp add {-a {d | n | b}} [-l r] [-t <timeout>] [-n <name>] [-c <comment>]
[-o <originator>] [-S <IP>] source {any | range:<IP>[-<IP>] | cidr:<IP>/<netmask>
| cc:<country_code> | asn:<sys_number>} [destination {<property>:<value>}]
[source-negated {true | false}] [destination-negated {true | false}]
[service <protocol> | <protocol>-<protocol> | <protocol>/<port> |
<protocol>/<port>-<port>] [service-negated {true | false}] quota
```

```
{[new-conn-rate <seconds>] [new-conn-rate-ratio <number>] [concurrent-conns
<number>] [concurrent-conns-ratio <number>] [pkt-rate <number>]
[pkt-rate-ratio <number>] [byte-rate <number>] [byte-rate-ratio <number>]
[track {track source | track source-service}]} [flush true]
```

Parameter	Description and Values
`-a`	Required action on the incoming packets that match the rule. Valid values: • `d` - drops the packet • `n` - notify: logs the packet and lets it through • `b` - bypass: lets the packet through without checking it against the policy rules. If this is the action you set, there are no logs or limits. Bypassed packets and connections are not added to total number of packets or connections for limit enforcement of type ratio.
`-l r`	If given, regular logging is done on matching traffic.
`-t`	The number of seconds (integers) after which the rule expires. If not given, the rule does not expire.
`-n`	Name of the rule.
`-c`	Optional free-text comment for the rule. Escape spaces and backslashes with a backslash. Do not use other special characters.
`-o`	Name of the originator.
`-s`	IP address of a target gateway for policy installation. By default, the rules are loaded only on the local gateway, unless you specify a different gateway with this parameter.
`source`	Definition of the source, from which to limit traffic. You can add multiple properties and sources, delimited by a comma: `source TYPE:VALUE [,TYPE:VALUE, TYPE:VALUE,...TYPE:VALUE]` Valid values: • `any` - The rule is applied to packets from any source. • `range:`*IP ADDRESS* or `range:`*IP ADDRESS–IP ADDRESS* - IPv4 or IPv6 addresses • `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` – `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`	Definition of a specific destination, to limit inbound traffic. Properties are the same as the `source`.

Parameter	Description and Values
`source-negated`	To ignore the action on traffic from the specified source, use `source-negated true`
`destination-negated`	To ignore the action on traffic from the specified destination, use `destination-negated true`
`service`	Service protocols, ports, or ranges of protocols or ports. Valid values: • `any` • *PROTOCOL* - IP protocol number in the range 1 - 255 (see http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml) • *PORT* - TCP or UDP port number in the range 1 - 65535 (see http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)
`service-negated`	To ignore the action on traffic using the specified services, use `service-negated true`
`quota`	Indicates that the next parameters describe the Rate Limiting quota.
`new-conn-rate`	Maximum (per second) number of connections that match the rule.
`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
`concurrent-conns`	Maximum number of concurrent active connections that match the rule.
`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.
`pkt-rate`	Maximum per second number of packets that match the rule.
`pkt-rate-ratio`	Maximum ratio of the `pkt-rate` value to the rate of all connections through the gateway, expressed in parts per 65536.
`byte-rate`	Maximum total number of bytes per second in packets that match the rule.
`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.
`track`	Criteria for counting connections, packets, and bytes: • `track source` - Count for each source IP address. • `track source-service` - Count for each source IP address and service (protocol and destination port).

Parameter	Description and Values
`flush`	These 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, use: `flush true`

Notes:

New rules apply only to new connections, not to existing connections.

Example of a rule with a range:

```
fw samp add -a d -l r -t 3600 -c rule\ for\ IPs\\SE 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 connections from the IP addresses in the range 172.16.7.11-172.16.7.13 to 5 connection per second. Drops all other attempted connections (`-a d`).
- Logs packets that exceed the quota set by the rule. The limit of the total number of log entries per second is set through the global parameter `sim_dos ctl -l LOG-LIMIT`.
- Expires after one hour (3600 seconds).
- This rule is immediately compiled and loaded with other rules in the Suspicious Activity Monitoring policy database, because this rule includes `flush true`.

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:SE byte-rate 0
```

- Logs all packets (-a n) coming from IP addresses from the country with country code SE.
- Does not let any traffic through (`byte-rate 0`), except for the packets (`service-negated true`) that match the IP protocols on the list (ICMP, IPSec, HTTPS, DNS).
- Does not expire (to cancel this rule, delete it explicitly), and is not enforced until you install the policy.

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`)
- Does not expire, and is not enforced until you install the policy.

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 (other policy rules still apply) that match the traffic (`-a b`). Lets through all HTTP traffic (`service 6/80`) from the specified address range (`source range:172.16.8.17-172.16.9.121`).
- Does not expire, and is not enforced until you install the policy.

Example of a tracked rule:

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

- Drops (-a d) new connections for every IP address that 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:SE`) as exception to the rule.
- Tracks the count of connections, packets, and bytes from the source.

Adding Rules in Batch Mode

To add rules in batch mode:

1. Enter this command:

   `fw samp [-s <IP_ADDRESS>] batch << EOF`

   Note: If you include the `-s` parameter, all the commands in this batch apply to the specified gateway.
2. Enter one *add* or *delete* command for each 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. 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 quota {[new-conn-rate <seconds>] [new-conn-rate-ratio <number>] [concurrent-conns <number>] [concurrent-conns-ratio <number>] [pkt-rate <number>] [pkt-rate-ratio <number>] [byte-rate <number>] [byte-rate-ratio <number>] [track {track source | track source-service}]}`

   `del <UID>`
3. To end the batch, enter: `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.

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: `set virtual-system <vsid>`
3. Run the `fw samp` command ("Creating Quota Rules" on page 9).

To configure rules on a remote gateway:

1. Log in to the server CLI.
2. Run: `fw vsx showncs -vs <VSID>`

   Record the output, the name of the Virtual System that established SIC.
3. Run: `fw samp -S <VSX_IP> -s <SIC_name> [options]` ("Creating Quota Rules" on page 9)

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 these parameters and values.

Parameter and Values	Description
`-m {1 | 0}`	Turns on the monitor-only mode, when set to 1. In this mode, rules do not drop any packets, regardless of the action specified. Each rule only does logging, as specified in it.

Parameter and Values	Description
`-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 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
```

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

Monitoring Events Related to DoS Mitigation

To see some useful information related to DoS Mitigation, run these commands:

Command	Command Output
`cat /proc/ppk/dos` `cat /proc/ppk6/dos` (for IPv6)	Shows memory utilization, DoS policy rules, and global parameter configuration.
`fw samp get -l | grep '^<[0-9a-f,]*>$' | xargs sim_dos get`	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.
`cat /proc/ppk/<VSID>/dos` `cat /proc/ppk6/<VSID>/dos (for IPv6)`	VSX is supported in R77.20 and higher. Shows memory utilization, DoS policy rules, and global parameter configuration for Virtual Systems. `<VSID>` is the VSID for the Virtual System.

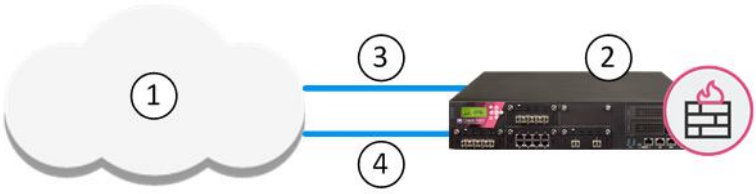
ISP Redundancy

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.

R80.10 supports two ISPs.

ISP Redundancy Modes

ISP Redundancy monitors the ISP links and chooses the best current link.



Item	Description
1	ISP in the Internet
2	Security Gateway
3	Link A to the ISP
4	Link B to the ISP

You can configure the ISP preference to be for Load Sharing or Primary/Backup.

- **Load Sharing -** Uses the two links with a distributed load of connections going out from the Security Gateway. Connections coming in are alternated. You can configure best relative loads for the links (set a faster link to handle more load). New connections are randomly assigned to a link. If one link fails, the other takes the load.
- **Primary/Backup -** Uses one link for connections going out from the Security Gateway and coming in. It switches to the backup if the primary link fails. When the primary link is restored, new connections are assigned to it. Existing connections continue on the backup link until they are complete.

Configuring ISP Redundancy

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

To enable ISP Redundancy:

1. Open the network object properties of the Security Gateway or cluster.
2. Click **Other** > **ISP Redundancy**.
3. Select **Support ISP Redundancy**.

4. Select **Load Sharing** or **Primary/Backup**.
5. Configure the links ("Configuring the ISP Links" on page 18).
6. Configure the Security Gateway to be the DNS server ("Configuring Security Gateway as DNS" on page 19).
7. Configure the policy for ISP Redundancy ("Configuring the Firewall" on page 19).

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 **Network Management** 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 Security Gateway object go to the **Other** > **ISP Redundancy** page.
2. Click **Set initial configuration**.
   The ISP Links are added automatically.
3. 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 Security Gateway object go to the **Other** > **ISP Redundancy** page.
2. Click **Add**.
3. 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.
4. 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 21).
   - If the Security Gateway has only one external interface, set each ISP link to connect to this interface.
5. Configure the **Next hop IP Address**.
   - 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.
6. 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.
7. Define hosts to be monitored, to make sure the link is working. Open the **Advanced** tab of the **ISP Link** window, and add **Selected hosts**.

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. In the Security Gateway object **ISP Redundancy** page, 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 for only two routable IP addresses.
6. Define an Access Control Policy 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 SmartConsole, click **Menu** > **Global Properties** > **NAT** and select **Manual NAT rules** - **Translate destination on client side**.

Configuring 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 behind the 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 NAT 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

Original Source	Original Destination	Original Service	Original Source	Translated Destination	Translated Services	
Any	IP of web server	http	=	10.0.0.2 (Static)	=	Incoming Web - ISP A
Any	IP of web server	http	=	10.0.0.2 (Static)	=	Incoming Web - ISP B
Any	IP of DNS server	domain_udp	=	10.0.0.3 (Static)	=	Incoming DNS - ISP A
Any	IP of DNS server	domain_udp	=	10.0.0.3 (Static)	=	Incoming DNS - ISP B

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 use local.arp.

When done, install the Access Control 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.

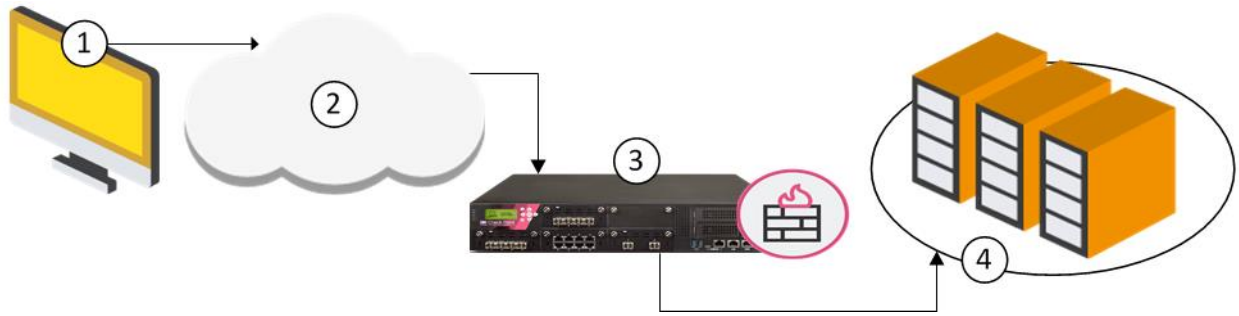
ConnectControl - Server Load Balancing

ConnectControl is a solution for server load balancing. ConnectControl distributes network traffic between a number of servers, to improve network response time and to provide High Availability.

ConnectControl runs on the gateway and does not require more memory or processing power.

ConnectControl Packet Flow

Load-balanced servers are represented by one virtual IP address. Define a *Logical server*, a network object that represents a group of physical servers. The Logical server takes service requests for the load-balanced application and directs the requests to the applicable physical server.



When a client requests access to an application that is load balanced by ConnectControl, the request goes through the Security Gateway.

Item	Description
1	**Client request** - A client starts a connection with the logical IP address of the application server (the address assigned to the Logical server).
2	**Internet** - The service request goes through the Internet.
3	**Security Gateway** - The service request arrives at the destination public IP address of the Logical Server, which is on the Security Gateway. The request is matched to the Logical Server rule in the Rule Base. The gateway directs the request to the internal IP address of the Logical Server group.
4	**Logical Server** - ConnectControl determines which server in the Logical Server group is best for the request, based on the selected load-balancing method.

Note - Make sure that rules that allow traffic for services to ConnectControl Logical Servers and that server groups are before Access Control Policy Firewall rules that allow traffic for those services.

To define a Logical Server:

1. In the Object Explorer, click **New** > **Network Object** > **More** > **Logical Server**.
2. In the **New Logical Server** window, enter a name for the ConnectControl Logical server.
3. Enter a virtual IP address.
4. Select the **Server type** ("Logical Server Types" on page 23).
5. Select the **persistent server mode**.
6. Select the Load **Balance method**.
7. Select a server group, or define a new group (**Servers group** > **New**).
   The members of the group must be hosts, gateways, or OSE devices.
8. Click **OK**.

Logical Server Types

When you create the Logical server object, configure the server type as **HTTP** or **Other**. This distinction is important. ConnectControl handles the connection to the client differently for each server type.

The **HTTP** server type uses HTTP redirection. This type supports offsite HTTP servers and form-based applications, but only works with the HTTP protocol. An HTTP Logical server makes sure that all HTTP-connection sessions are directed to one server, which is a requirement for many Web applications. ConnectControl finds the correct physical server, behind the firewall or offsite, based on the selected load-balancing method ("Load-Balancing Methods" on page 24). The session connections continue to go to that one server.

The **Other** server type uses NAT (address translation) to send traffic to the grouped servers. This Logical server supports all protocols (including HTTP) and gives the most effectively balanced load. It requires servers to be NATed by the gateway. ConnectControl mediates each service request and then selects the server to get that request. It uses NAT to change 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. The server's source address in the packet is translated to the IP address of the Logical server. On the packet's return, the firewall translates the packet's original address to the IP address of the Logical server.

Persistent Server Mode

Persistent server mode maintains a client's connection to the server that ConnectControl first selected.

- **Persistency by server** is useful for HTTP applications, such as forms, in a load-balanced environment with multiple Web servers. ConnectControl directs an HTTP client to one server for all requests. This allows clients to fill forms without the data loss that occurs if different servers take the requests.
- **Persistency by service** is useful if you are load balancing multiple services in your server group. For example, in a redundant environment of two servers, each running HTTP and FTP, ConnectControl directs traffic from one client to the server of the correct service. This prevents heavy load on one server, which can happen with **Persistency by server**.

Item	Description
1	Multiple client requests for HTTP and FTP.

2	**Internet**
3	**Security Gateway** - The service requests arrive at the destination public IP address of the Logical Server, which is on the Security Gateway. The gateway directs the requests to the internal IP address of the Logical Server group.
4	**Logical Server** group with two servers, each with FTP and HTTP services. ConnectControl balances the load between the servers.

Persistent Server Timeout

If you enable Persistent server mode, you can set a timeout for a client to use one server. If a server becomes unavailable, ConnectControl directs new connections to a new, available server. This bypasses the persistency and optimizes load balancing.

To set persistent server mode timeout:

1. Open **Global Properties**.
2. Click **ConnectControl**.
3. In **Persistent server timeout**, enter the timeout in seconds.

Load-Balancing Methods

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

- **Round Trip**: Directs incoming requests to the server with the fastest response time. ConnectControl calculates the fastest server from average round-trip time to respond to ICMP echo requests. 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**: Directs service requests to the next server in the sequence. The round robin method is a good choice when all the load balanced servers have similar RAM and CPU and are on the same segment.
- **Random**: Directs service requests to servers at random. The random method is a good choice when all the load-balanced servers have similar RAM and CPU and are located on the same segment.
- **Domain**: Directs service requests based on domain name.

Server Availability

You can configure how ConnectControl finds available servers.

To set server availability configurations:

1. Open **Global Properties**.
2. Click **ConnectControl**.

3. In **Server availability check interval**, enter the number of seconds between pings from the gateway to the servers.
4. In **Server check retries**, enter the number of attempts to contact a nonresponsive server after ConnectControl stops directing connections to it.

End to End ConnectControl

This procedure explains the steps to set up ConnectControl in your environment.

To configure ConnectControl:

1. In the SmartConsole open the **Object Explorer** (Ctrl+E)
2. Click **New** > **Host**.
3. Define the objects for the servers that will be load-balanced.
4. In the **Object Explorer**, click **New** > **Network Group**.
5. Name the group (for example, HTTP_Server_Group).
6. Add the server objects to the group.

   We recommend to add no more than 29 Logical servers to a group.
7. In the **Object Explorer**, click **New** > **Network Object** > **More** > **Logical Server**.
8. Define the Logical server (on page 23).

   Make sure the IP address you assign is a routable IP address. All traffic to be load-balanced is directed through the gateway.
9. Select the **Server type** ("Logical Server Types" on page 23).
10. Select the server group that you defined in these steps.
11. Select the **Persistent Server Mode** (on page 23) that fits your environment.
12. Select a **Balance Method** ("Load-Balancing Methods" on page 24).
13. Add the Load Balancing rule to the Access Control Policy Rule Base:

    Source = `Any`

    Destination = *<Logical Server>*

    Services & Applications = *<load-balanced services>*

    Action = `Accept`, `User Auth`, or `Client Auth`
14. For applications using HTTP redirection, add a rule to allow the server group to communicate directly with clients:

    Source = `Any`

    Destination = `HTTP_Server_Group`

    Services & Applications = `http`

    Action = `Accept`
15. Click **Menu** > **Global Properties** > **ConnectControl**.
16. Set the Persistent Server Timeout (on page 24) and Server Availability (on page 24) controls for your environment.

Bridge Mode

You can configure bridge mode with one gateway or with a cluster. 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.

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.

Supported Blade	Supports Gateways in Bridge Mode	Supports Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot and Anti-Virus	Yes	Yes
Application Control	Yes	Yes
HTTPS Inspection	Yes	No
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes

Supported Blade	Supports Gateways in Bridge Mode	Supports Virtual Systems in Bridge Mode
QoS	Yes	No
Client Authentication	Yes	No
User Authentication	Yes	No

Configuring Bridge Mode with the Gaia WebUI

To configure a bridge interface with the WebUI:

1. In the WebUI navigation tree, click **Network Management** > **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**.

Configuring Bridge Mode with the CLI

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

To see the interfaces of an existing bridge:

`show bridging group` *<Group ID>*

Where *Group ID* is the unique identifier of the bridge, an integer between 0 and 1024

To create a new bridging group:

`add bridging group` *<Group ID>* [interface *<Bridge Interface Name>*]

To add an interface to the bridging group:

`add bridging group` *<Group ID>* `interface` *<Physical interface Name>*

Run this command one time for each physical interface.

To remove an interface from the bridging group:

`delete bridging group` *<Group ID>* `interface` *<Physical interface Name>*

Run this command one time for each physical interface.

To delete a bridging group:

`delete bridging group` *<Group ID>*

To add or change a bridge interface IP address:

- IPv4: `set interface` *<Bridge interface Name>* `ipv4-address` *<IP>* `subnet-mask` *<Mask>*

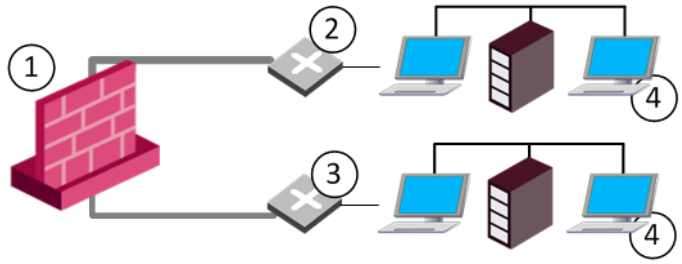
- IPv6: `set interface` *<Bridge interface Name>* `ipv6-address` *<IP>* `mask-length` *<Prefix>*

Examples:

```
add bridging group 56 interface eth1
set interface br1 ipv6-address 3000:40::1 mask-length 64
```

Important - After you add, configure, or delete features, run the `save config` command to keep settings after reboot.

Configuring One Gateway in Bridge Mode



Item	Description
1	Security Gateway bridges Layer-2 traffic over one IP address, with a subnet on each side, using the same address
2	Switch from a bridged interface to a subnet
3	Switch from a second bridged interface to a second subnet
4	Internal network

To define the bridge topology:

1. Configure a dedicated management interface.
2. Configure the bridge interface. It must be in the bridged subnet. Only the bridge interface has an IP address. The bridge ports must not have IP addresses.
3. Configure the bridge topology in the properties of the network object:
   - If a bridge port connects to the Internet, set the interface to **External**.
   - If the Security Gateway is in rules with Internet objects, set the interface to **External**.
   - If the topology uses Anti-Spoofing for the internal port (interface), set the interface to **Internal** and select the network that connects to the port.
   - If the topology does not use Anti-Spoofing, disable Anti-Spoofing on the bridge port.

   For example:

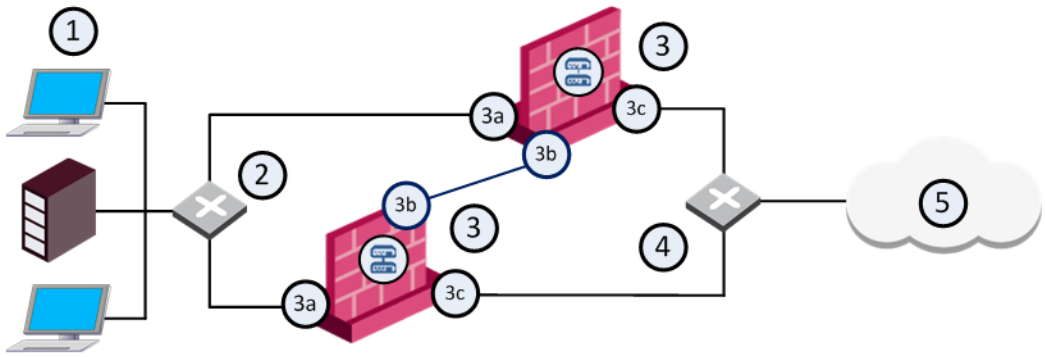
   Bridge Interface - **eth0** - **External** - **192.0.2.0.208/24**

   Bridge Port to Internet - **eth1** - **External** - **0.0.0.0/0**

   Bridge Port with Anti-Spoofing - **eth2** - **Internal to** *CP_default_Office* **network** - **0.0.0.0/0**

Configuring Gateway Cluster in Bridge Mode

You can configure cluster gateways for bridge mode in different deployments Active/Standby mode or Active/Active mode.



Item	Description
1	Internal network
2	Switch for internal network
3	Security Gateway bridging Layer-2 traffic
3a	eth1 - connects to the internal network
3b	eth3 - ClusterXL Sync interface
3c	eth2 - connects to the external network (192.168.10.1)
4	Switch for external network
5	Internet

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 30).
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: `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            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 one-gateway deployment ("Configuring One Gateway in Bridge Mode" on page 28).

   Do not configure an IP address on the newly created bridge interface.
3. In SmartDashboard, add the cluster object:

   a) Open the **Network Management** page of the of the cluster object.

   b) Get the cluster Interfaces with 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. See the cluster state: `cphaprob stat`

   Example of expected output:

   ```
   Cluster Mode: High Availability (Active Up, Bridge Mode) with IGMP
   Membership
   Number     Unique Address     Firewall State (*)
   1 (local>  192.0.2.3            Active
   2          192.0.2.2            Active
   ```
6. Make sure that cluster is configured for High Availability ("Confirming the High Availability Configuration" on page 30).

Confirming the High Availability Configuration

After you configure Active/Active mode, the output for `chpaprob stat` shows that the `Firewall State` is `Active/Active`. Make sure that the cluster is configured for High Availability.

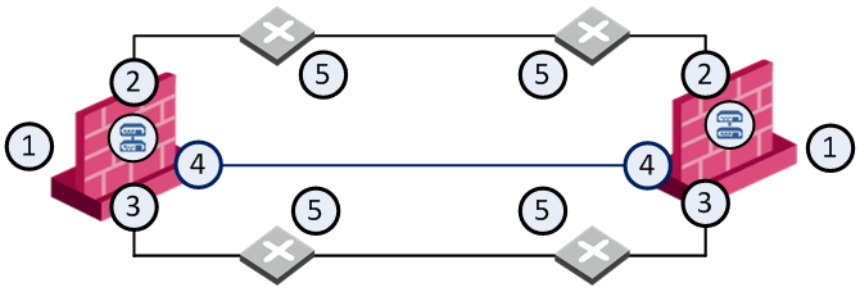
To confirm the High Availability configuration:

1. Open the cluster object.
2. In the cluster **Properties** window, 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.



Item	Description
1	Security Gateway bridging Layer-2 traffic
2	eth1
3	eth2
4	eth3 - ClusterXL Sync interface
5	Switch

See also: Link Aggregation with ClusterXL in Layer-2
http://supportcontent.checkpoint.com/documentation_download?ID=23341

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.

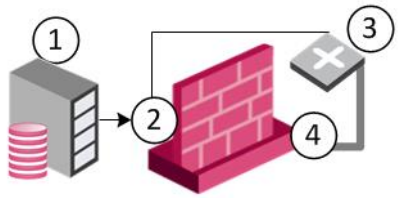
- Cluster deployments do not support this configuration.
- You cannot configure the bridge to be the route gateway.
- One Security Gateway can support multiple bridge interfaces, but only one bridge can have an IP address.
- The Security Gateway cannot filter or transmit packets on a bridge interface that it inspected before (*double-inspection*).

Management over Bridge

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

- The first packet is inspected and goes from the management interface to the router.
- The router sends the packet to the bridge interface.

- The firewall concludes that this packet is a retransmission and drops it.



Item	Description
1	Security Management Server sends management packet to management interface
2	Management interface on Security Gateway Firewall bridging Layer-2 traffic inspects the packet and sends it to the router
3	Router sends the packet to the bridge interface
4	Bridge interface drops the packet as a retransmission

Configure the Security Gateway to handle management packets properly.

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.
3. Reboot the Security Gateway.

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 Check Point 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:

- **Source** - *Bridged_Network*
- **Destination** - *Bridged_Network*
- **Services & Applications** - **neighbor-advertisement**, **neighbor-solicitation**, **router-advertisement**, **router-solicitation**, **redirect6**
- **Action** - **Accept**

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__*/
```

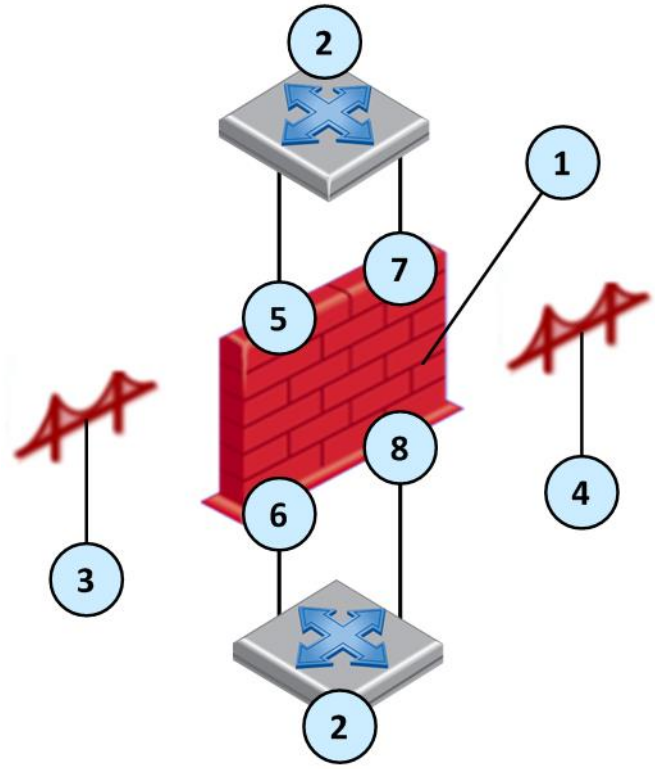
Traffic is allowed if:

- `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.



Item	Description
1	Security Gateway
2	Switch
3	Access mode bridge 1 with VLAN translation
4	Access mode bridge 2 with VLAN translation
5	VLAN 3 (eth 1.3)
6	VLAN 33 (eth 2.33)
7	VLAN 2 (eth 1.2)

Item	Description
8	VLAN 22 (eth 2.22)

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**.
2. The **Add VLAN** window opens. Configure the interfaces of the VLAN: **IPv4**, **IPv6**, **VLAN ID**, and add the VLAN interface to a physical interface.

   When you set a VLAN ID to be a member of a physical interface, the VLAN interface name *<physical_interface>.<vlan_id>*. For example, if **VLAN ID 2** is a member of **eth1**, the VLAN interface is **eth1.2.**
3. Open the **Add Bridge** window and select the VLAN interfaces in the **Bridge** tab.

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. BPDUs 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:
   `./etc/init.d/functions`

   Add this line:
   `/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

Best Practice - When you set 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.

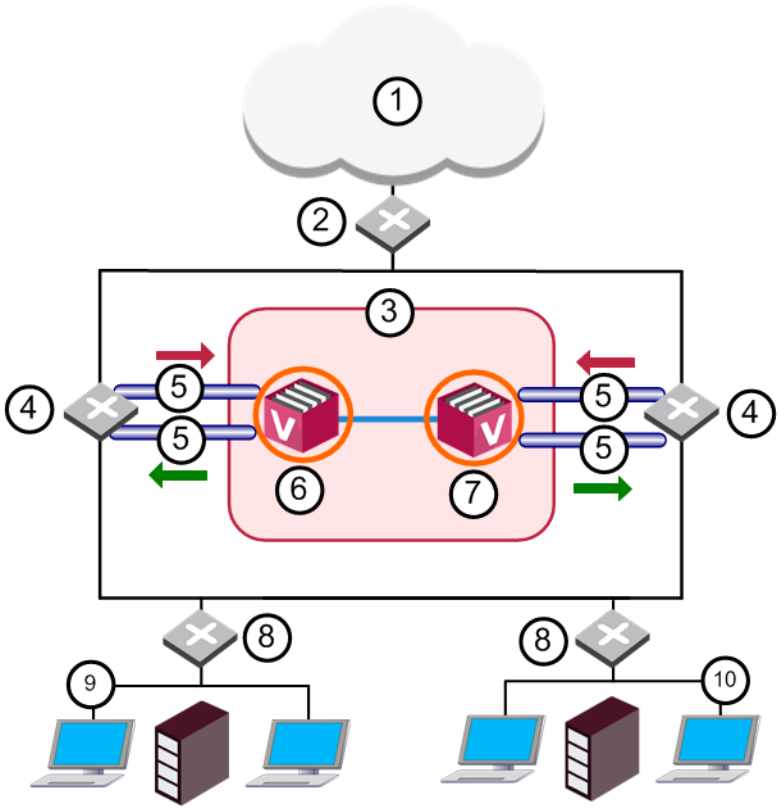
Required VLAN Trunk Interfaces

- 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

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.



Item	Description
1	Internet
2	Core Network Backbone switch
3	VSX Cluster
4	Router
5	VLAN
6	Member 1
7	Member 2

Item	Description
8	LAN Switches
9	Sales
10	Finance
	Sync Network
	Physical Interface
	VLAN Trunk

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 Configuration or Override in Bridge Mode

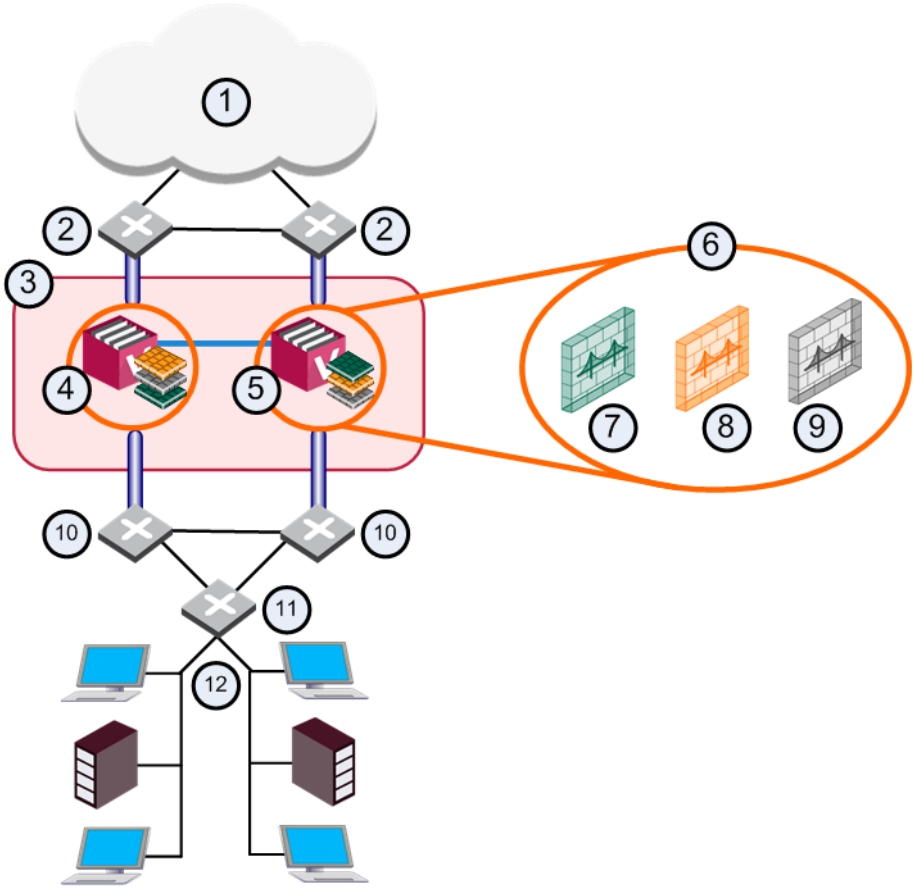
If you used the **Custom Configuration** template when creating the VSX Gateway, or if you selected the **Override Creation Template** option, and are creating a Virtual System in the Bridge Mode, manually define the network interfaces.

Interfaces: To configure the external and internal interfaces, define interfaces and links to devices in the **Interfaces** table. You can add new interfaces as well as delete and modify existing interfaces.

To add an interface, click **Add**. The **Interface Properties** window opens. Select an interface from the list and define is properties. Click **Help** for details regarding the various properties and options.

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.



Item	Description
1	Internet
2	Redundant switches (external)
3	VSX Cluster
4	Member 1
5	Member 2
6	Virtual Systems in Bridge Mode
7	VS 1 Active
8	VS 2 Standby

Item	Description
9	VS 3 Backup
10	Redundant switches (internal)
11	VLAN Switch
12	Internal Networks
	Sync Network
	Physical Interface
	VLAN Trunk

With Active/Standby Bridge Mode in High Availability mode, ClusterXL directs traffic to members according to administrator -defined priorities and status. In Virtual System Load Sharing

deployments, the system distributes the traffic load amongst members according to your Virtual System Load Sharing configuration.

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**.
4. Select **Standard Layer-2 Loop Detection Protocols**.

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.

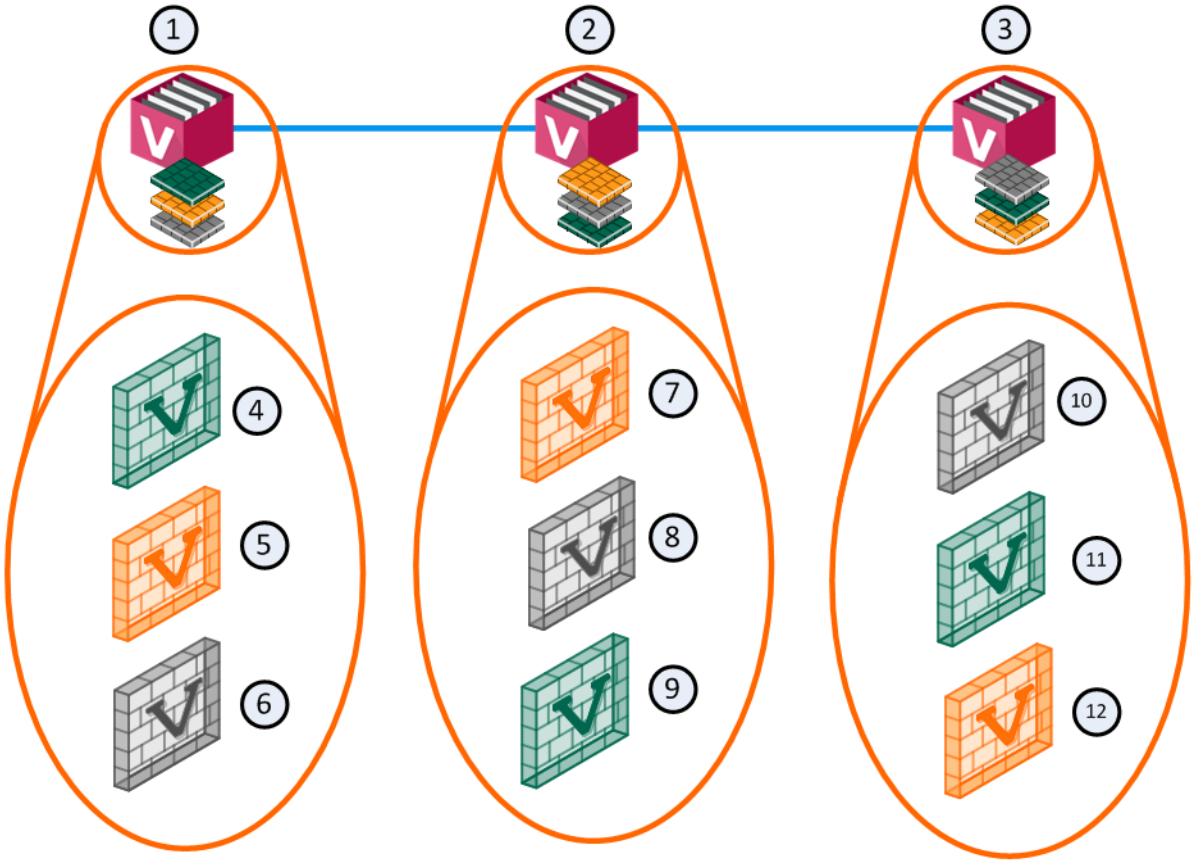
   Enter an IP address and subnet mask, which continuously monitors the specified network for faults or connectivity issues. The IP address/subnet define the network on which the Virtual System resides.

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.



Item	Description
1	Member 1
2	Member 2
3	Member 3
4	VS 1 Active
5	VS 2 Standby
6	VS 3 Backup

Item	Description
8	VS 2 Backup
9	VS 3 Active
10	VS 1 Backup
11	VS 2 Active
12	VS 3 Standby
———	Sync Network

Item	Description
7	VS 1 Standby

Item	Description

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`
6. Enter the Security Management Server or Multi-Domain Security Management Domain Management Server IP address.
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.
12. Reboot the members.

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

Configure Monitor Mode on Security Gateway interfaces, to 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:

- 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 run active operations (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:

Supported Blade	Supports Gateways in Monitor Mode	Supports Virtual System in Monitor Mode
Firewall	Yes	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot	Yes	Yes
Application Control	Yes	Yes
Identity Awareness	Yes	No
Threat Emulation	Yes	Yes

Unsupported Software Blades for Monitor Mode

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 Deployments for Monitor Mode

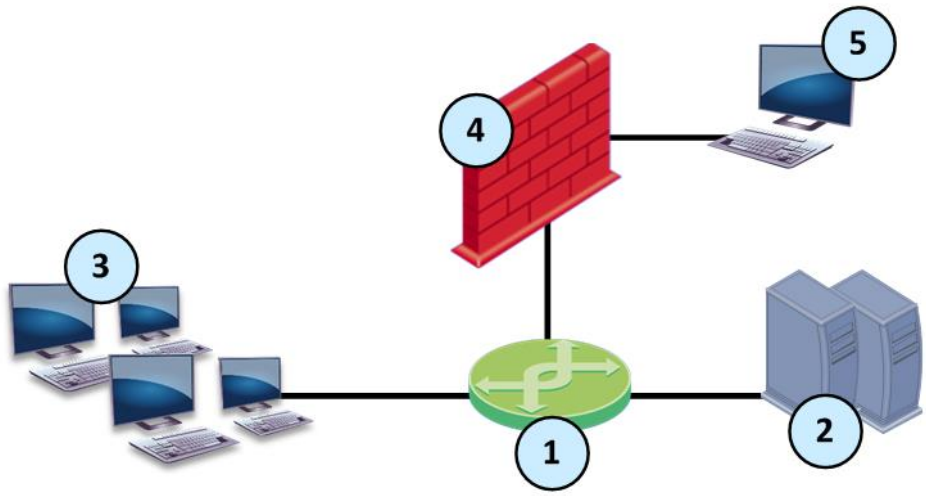
These are deployments do not support Monitor Mode:

- 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 ports and VLANs.



Item	Description
1	Switch with mirror port
2	Servers
3	Computers
4	Security Gateway in monitor mode
5	Management for Security Gateway

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:

```
set interface <interface name> monitor-mode on
```

Security Before Firewall Activation

There are different reasons for a computer to not have a security policy installed and to be vulnerable. To protect the computer and network, Check Point has baseline security:

- **Boot Security -** Security during boot process
- **Initial Policy -** Security before a policy is installed for the first time

Boot Security

During the boot process, there are a few seconds after the computer can receive communication (and can be attacked) and before the security policy is loaded and enforced. firewall Boot Security protects the computer, and its networks, during this time. Boot Security works through *control of IP Forwarding* on boot and the *Default Filter*.

The Default Filter also provides protection if firewall processes are stopped for maintenance.

Control of IP Forwarding on Boot

Boot Security disables IP forwarding in the OS kernel. There is never a time when IP Forwarding is active without a security policy. This protects the networks behind the Security Gateway.

The Default Filter

Boot Security loads the Default Filter when it disables IP Forwarding, after bootup and before interfaces are configured. You can configure the Default Filter to work in different modes:

- *General Filter* accepts no inbound communication (this is the default option).
- *Drop Filter* accepts no inbound or outbound communication. This filter drops all communications in and out of the gateway during a period of vulnerability.

  Best Practice: If the boot process requires that the gateway communicate with other hosts, do not use the Drop Filter.

The Default Filter also provides Anti-Spoofing protection for the Security Gateway.

Changing the Default Filter

There are two filter files in **$FWDIR/lib**: **defaultfilter.boot** and **defaultfilter.drop**

To change the Default Filter:

1. Copy the Default Filter file (**defaultfilter.boot** or **defaultfilter.drop**) to: `$FWDIR/conf/defaultfilter.pf`
2. Compile the Default Filter: `fw defaultgen`

   The output is `$FWDIR/state/default.bin`
3. Get the Default Filter file path: `fwboot bootconf get_def`
4. Copy `default.bin` to the Default Filter file path.
5. Generate the Initial Policy: `cpconfig`

Defining a Custom Default Filter

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

Make sure your security policy does not interfere with the boot process.

To define a Default Filter:

1. Create an Inspect script named: `$FWDIR/conf/defaultfilter.pf`

   Important - The script must not do these functions:
   - Logging
   - Authentication
   - Encryption
   - Content security
2. Run: `fw defaultgen`
3. Run: `fwboot bootconf get_def`
4. Copy `$FWDIR/state/default.bin` to the Default Filter file path.
5. Generate the Initial Policy from: `cpconfig`

Using the Default Filter for Maintenance

It is sometimes necessary to stop firewall processes for maintenance. It is not always practical to disconnect the Security Gateway from the network (for example, if the gateway is on a remote site).

Run the `cpstop` command with the `-fwflag` *<value>* to make sure the Security Gateway is protected when Check Point processes are stopped.

```
> cpstop -fwflag {-proc|-default}
```

Parameter	Description
`-fwflag -proc`	Maintains the active Security Policy running in the kernel when Check Point daemons and services are stopped. Rules with generic allow, reject, or drop rules based on services continue to work.
`-fwflag -default`	The active Security Policy running in the kernel is replaced with the Default Filter, which allows open connections to the gateway to remain open.

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.

Monitoring Security

You can see that the Default Filter or the Initial Policy are loaded on a non-production Security Gateway. Restart the computer before Install Policy and run:
`$FWDIR/bin/fw stat`

If the output shows **defaultfilter** for the Default Filter status and **InitialPolicy** for the installed policy, the computer is running on the default, pre-firewall security.

Unloading Default Filter or Initial Policy

To unload a Default Filter or an Initial Policy from the kernel, use the command to unloading a regular policy. Do this only if you are sure that the security of the Default Filter or Initial Policy is not required.

To unload the Default Filter locally: `fw unloadlocal`

To unload an Initial Policy from a remote Security Management server: `fwm unload` *<gateway>*

Where *gateway* is the SIC_name of the gateway.

Troubleshooting: Cannot Complete Reboot

In some configurations, the Default Filter prevents the Security Gateway from completing the reboot after installation.

First, look at the Default Filter. Does the Default Filter allow traffic required by the boot procedures? If the boot process cannot complete successfully, remove the Default Filter.

1. Reboot in **single user** mode.
2. Set the Default Filter to not load again: `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.

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

Options	Description
-r	Removes boot security
-g	Enables boot security

fwboot bootconf

Configure boot security options. This command is in `$FWDIR/boot`.

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

Commands	Values	Description
Get_ipf	none	Reports if firewall controls IP Forwarding. • Returns 1 if IP Forwarding control is enabled on boot. • Returns 0 if IP Forwarding is not controlled on boot.
Set_ipf	0 | 1	Turns off/on control of IP forwarding for the next boot. **0 -** Turns off **1 -** Turns on
Get_def	none	Returns the full path to the Default Filter that will be used on boot.

Set_def	<*filename*>	Loads the file as the Default Filter in the next boot. The only safe and recommended directory is `$FWDIR\boot`**.** (The `default.bin` filename is a default name.) **Note -** Do NOT move these files.

comp_init_policy

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

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

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

Options	Description
-u	Removes the Initial Policy, and makes sure that it will not be generated in the future when **cpconfig** is run.
-g	Generates the Initial Policy and makes sure that it is loaded the next time a policy is fetched (`cpstart`, `reboot`, `fw fetchlocalhost`). After running this command, **cpconfig** adds an Initial Policy when needed.

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, the original policy will be loaded.

cpstop -fwflag default and cpstop -fwflag proc

To stop all firewall processes but leave the Default Filter running, run: `cpstop -fwflag -default`

To stop all Security Gateway processes but leave the security policy running, run: `cpstop -fwflag -proc`

To stop and start all Check Point processes, run: `cpstop` and `cpstart`

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

Options	Description
-default	Kills firewall processes (such as `fwd`, `fwm`, `vpnd`**,** `snmpd`). Logs, kernel traps, resources, and security server connections stop. The security policy in the kernel is replaced with the Default Filter.

-proc	Kills firewall processes. Logs, kernel traps, resources, and security server connections stop. The security policy remains loaded in the kernel. Allow, reject, and drop rules that do not use resources, only services, continue to work.

Legacy Authentication

Check Point supports different methods of authenticating end users and administrators. Security Gateways authenticate individual users. The Security Management Server authenticates administrators. Users and Administrators authenticate with username and password credentials.

Users and administrators can be stored in the Check Point User Database or on an LDAP server.

Session Authentication is not supported with an R80 Security Management Server.

Check Point Password

Check Point password is a static password that is configured in SmartConsole. For administrators, the password is stored in the local database on the Security Management Server. For users, it is stored on the local database on the Security Gateway. No additional software is required.

Operating System Password

OS Password is stored on the operating system of the computer on which the Security Gateway (for users) or Security Management Server (for administrators) 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 method that provides security and scalability by separating the authentication function from the access server.

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

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

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

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**).
7. Enable RADIUS authentication for Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.
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 lets you control access privileges for authenticated RADIUS (on page 54) 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.

Use these RADIUS attributes (refer to RFC 2865):

- For SecurePlatform - attribute "Class" (25)

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

Sample workflow for RADIUS authentication configuration:

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

Associating a RADIUS Server with Security Gateway

You can associate users with the RADIUS authentication server in the **User Properties > Authentication** tab. You can override that association and associate a gateway with a RADIUS server.

To associate one or more Radius servers to a gateway, run this **dbedit** command:

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

To turn off the RADIUS-gateway association:

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

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. For administrators, it is the Security Management Server that forwards the requests. ACE manages the database of RSA users and their assigned hard or soft tokens. The gateway or the Security Management Server act as an ACE/Agent 5.0 and direct 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 method.

Configuring a Security Gateway to use SecurID Authentication

Sample workflow for SecurID (on page 56) authentication configuration:

1. Configure gateways for SecurID authentication.
2. Define user groups.
3. Configure SecurID authentication settings for users.

The procedure for doing this is different for Internal Users (that are defined in the internal User Database on the Security Management Server) and for External Users.

4. Complete the SecurID authentication configuration.

To configure a Security Gateway to use SecurID:

1. Generate the *sdconf.rec* file on the ACE/Server and copy it 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

   On a Virtual System, follow the instructions in sk97908 http://supportcontent.checkpoint.com/solutions?id=sk7908.
2. In SmartConsole, go to the **Gateways & Servers** view, right-click a Security Gateway object and select **Edit**.
3. In the gateway property window that opens, select **Other > Legacy Authentication**.
4. In the **Enabled Authentication Schemes** section, select **SecurID**.
5. Click **OK**.

To define a user group:

1. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New > More > User > User Group**.

   The **New User Group** window opens.
3. Enter the name of the group, for example *SecurID_Users*.

   Make sure the group is empty.
4. Click **OK**.
5. Publish the changes and install the policy.

To configure SecurID authentication settings for Internal Users:

Internal users are users that are defined in the internal User Database on the Security Management Server.

1. Create a new user. In SmartConsole, open the **Objects Bar (F11)**.
2. Click **New > More > User > User**.

   The **New User** window opens.
3. Choose a template.
4. Click **OK**.
5. In the **General** page:
   - Enter a default **Name**. This name will be used to authenticate users on the ACE/Server.
   - Set the **Expiration** date.
6. In the **Authentication** page, from the **Authentication Method** drop-down list, select **SecurID.**
7. Click **OK**.

To configure SecurID authentication settings for External Users:

External users are users that are not defined in the internal Users Database on the Security Management Server.

1. Create a new user profile. In SmartConsole, click **Manage & Settings** > **Blades**.

2. In the **Mobile Access** section, click **Configure in SmartDashboard**.
   SmartDashboard opens.
3. Go to the objects pane, and click **Users**.
4. Right-Click and select **New > External User Profile**.
5. If you support more than one external authentication scheme, select **Match By Domain**.
   In the **External User Profile Properties** window, **General Properties** page:
   - Enter an **External User Profile Name**. This name will be used to authenticate users on the ACE/Server.
   - Set the **Expiration Date**.

   If you support one external authentication scheme, select **Match all users**.
   In the **External User Profile Properties** window, **General Properties** page, set the **Expiration Date**.
6. In the **Authentication** page, from the **Authentication Scheme** drop-down list, select **SecurID.**
7. Click **OK**.
8. Click **Update** (Ctrl + S).
9. Close SmartDashboard.

To complete the SecurID authentication configuration:

1. Make sure that connections between the gateway and the ACE/Server are not NATed in the Address Translation Rule Base.
   On a Virtual System, follow the instructions in sk107281 http://supportcontent.checkpoint.com/solutions?id=sk107281.
2. Save, verify, and install the policy in SmartConsole.

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 method that provides verification services. Using TACACS, the Security Gateway forwards authentication requests by remote users to the TACACS server. For administrators, it is the Security Management Server that forwards the requests. 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 TACACS+ Authentication

To configure a Security Gateway to use TACACS+ authentication, you must set up the server and enable its use on the Security Gateway.

To define a TACACS+ server:

1. Define a TACACS Host object: **Object Explorer** > **New** > **Host**
2. Enter a name and IP address.
3. Define a TACACS server: **Object Explorer** > **New** > **Server** > **More** > **TACACS**.
4. Enter a name.
5. In **Host**, select the TACACS host.
6. Select the **Type**.

   Best Practice: The default is **TACACS**, but **TACACS+** is recommended.
7. In **Service**, select the **TACACSplus** service (or **TACACS** UDP service if you selected **TACACS** type).
8. Enter a **Secret key**. (If you selected **TACACS** type, this is not available. If you selected **TACACS+**, it is required.)
9. Click **OK**.

To enable TACACS on the Security Gateway:

1. Right-click the gateway object and select **Edit**.
2. Click **Other** > **Legacy Authentication**.
3. In the **Enabled Authentication Schemes** section, click **TACACS**.
4. Click **OK**.

To enable TACACS authentication for users:

1. In the Object Explorer, click **Users** > **User Templates**.
2. Edit the **Default** user template.
3. In the **User Template** > **Authentication** tab, **Authentication method** list, select **TACACS**.
4. When **TACACS server** shows, select the TACACS server you defined.
5. Click **OK**.

   When you create a new user account, TACACS is the default selected authentication.

Undefined

The authentication scheme for a user can be set to **Undefined**. If a user with an undefined authentication scheme is matched to a Security Rule with authentication requirements, access is always denied.

Authentication Methods

You can define an Access Control Policy Rule Base action that requires clients or users to authenticate before they access specified network resources. Authentication actions are transparent or nontransparent.

- Transparent authentication - Clients connect to known servers.

- Nontransparent authentication - Users or client services send credentials when they request a resource.

User and Client authentication are supported on layers that have only Firewall enabled. If other layers (such as Applications) are enabled, the **User Auth** and **Client Auth** options are not available.

User Authentication

User Authentication is authentication for Telnet, FTP, HTTP, and RLOGIN services. By default, User Authentication is transparent. The user does not connect directly to the gateway. The user starts a connection to the target server.

The Security Gateway intercepts the start of the traffic between the user's client and the target server. The Security Gateway prompts the user for a user name and password.

- If the user successfully authenticates, the gateway passes the connection to the server. The remote server also prompts the user for a user name and password.
- Otherwise, the user is prompted to enter the data again. After a number of unsuccessful attempts, the connection is dropped.

Best Practice - When you configure user accounts, you can predefine the locations users are allowed to access. But this can create a mismatch with security rules that require authentication. To prevent Rule Base issues, make sure the Authentication Action of these rules defines the correct resolution. (see "Resolving Access Conflicts" on page 65)

Configuring User Authentication

Before you begin:

- Make sure you have user groups.
- Make sure the user groups each have a defined Authentication scheme.
- Make sure the policy has only the Firewall layer enabled.

To configure user authentication in a rule:

1. Right-click in the **Source** column, select **Add legacy user access** and then select the user group.
2. To configure the location of authentic users, select **Location** and the object that defines their location.
3. Click **OK**.
4. In **Services & Applications**, select the services to authenticate. These services are supported for user authentication: http, ftp, rlogin, and telnet.
5. In the **Action** column, select **More.**
6. In the **Action Settings** window, select **User Auth**.
7. Click the pencil icon.
8. In the **User Auth** window, configure the **User Auth** options (on page 61).

   Best Practice - If the Authentication scheme of the user group is not a static password (*Check Point Password* or *Operating System Password*), set the **User Authentication session timeout**. This timeout closes inactive Telnet, FTP and login connections. It ends HTTP sessions that are authenticated with a One Time Password (such as SecurID), and makes the server request a new password.

Note - If a static password scheme is used with HTTP, this setting is ignored, because web browsers cache passwords.

To set the **User Authentication session timeout**: open the Security Gateway object > **Other** > **Legacy Authentication**.

9. Install the Access Control Policy: Click **Install Policy** (Ctrl+Shift+Enter).

User Auth Options

Source/Destination

- **Intersect with User Database** - The more restrictive access privileges of the rule and the user account properties are applied. If the **User Properties** > **Location** for a user does not allow this location, the user will be denied. If the rule blocks the user, the user will be denied, even if the Location is allowed.
- **Ignore User Database** - Access is given or denied according to the rule. The user account properties are ignored.

HTTP

- **Allow Predefined Servers Only** - Activates the Reauthentication options defined for the HTTP servers, and allows users to access only the servers in **Global Properties** > **Security Servers** > **HTTP servers**.
- **Allow All Servers** - Ignores Reauthentication options. If you are in transparent mode, it is not necessary to define the servers.

Best Practice - Use *Allow All Servers* with caution. It allows users to continue to any port.

Importance of Rule Order in User Authentication

For user authentication rules for Telnet, FTP, HTTP, and RLOGIN services:

If there are other non-authentication rules that use these services, make sure that the user authentication rule is after those rules.

Client Authentication

Client Authentication gives access according to the IP address. Client Authentication is not as secure as user authentication. It gives access for unlimited users, connections, and time, until the user signs off. Select client authentication only if this access is required.

Best Practice - When you configure user accounts, you can predefine the locations they are allowed to access. But this can create a conflict with security rules that require authentication. To prevent conflicts, make sure the Authentication Action of these rules defines the correct resolution. (see "Resolving Access Conflicts" on page 65)

Client Authentication works with all sign-on methods, with different behavior and options.

Client Auth Sign-On Method	Authentication Method for authenticated services: Telnet, FTP, HTTP, RLOGIN	Authentication Method for other services
Manual	Telnet to port 259 on gateway HTTP to port 900 on gateway	Telnet to port 259 on gateway HTTP to port 900 on gateway

Client Auth Sign-On Method	Authentication Method for authenticated services: Telnet, FTP, HTTP, RLOGIN	Authentication Method for other services
Partially automatic	User Authentication on destination server	Not available
Fully automatic	User Authentication on destination server	Not available
Single Sign on	UserAuthority	UserAuthority

Client Authentication sign-on options:

- **Standard Sign on**: Users can access all services permitted by the rule without authenticating for each service.
- **Specific Sign on**: Users can access only the services that they specify when they authenticate (ignores the rule if it allows more services). If the user wants to use a different allowed service, they must authenticate again for that service.

Manual Sign On

Manual Sign On is available for any service in the Client Authentication rule. The client must first connect to the Security Gateway and authenticate.

- The client can connect through a Telnet session to the gateway on port 259.
- The client can connect with a Web browser, through an HTTP connection to the gateway on port 900, with this syntax in the URL: `http://<gateway name>:900`

Through Telnet or HTTP, the client can use the **Standard Manual Sign On** method or the **Specific Manual Sign On** method.

Standard Manual Sign On Example:

In this example, before the client opens a connection to the destination server, the user (`fbloggs`) authenticates to the Security Gateway (`london`).

```
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.
```

Specific Manual Sign On Example:

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.
```

Partially Automatic Sign On

With Partially Automatic Sign On, when users connect to remote hosts with an authenticated service, they must also authenticate with User Authentication. To make a rule that allows Partially Automatic Sign On:

- Specify a supported service: Telnet, FTP, HTTP or RLOGIN
- Enable Client Authentication
- Open port 80 on the Security Gateway

Fully Automatic Sign On

With Fully Automatic Sign On, the rule does not block for service. But if the remote host uses authenticated services, users must also authenticate with User Authentication. To make a rule that allows Fully Automatic Sign On:

- Specify the service to allow for transparent authentication to a remote host without authentication services.
- Enable Client Authentication
- Open port 80 on the Security Gateway

Single Sign On

Single Sign On is available for all services, if the required service is specified in the Client Authentication rule, and if UserAuthority is installed.

Single Sign On is a Check Point address management feature for transparent network access. The Security Gateway matches the user IP address records against users logged on to an 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 registered to the IP address. If the user's name is authenticated, the packet is accepted. If not, the packet is dropped.

Configuring Client Authentication

Before you begin:

- Make sure you have user groups.
- Make sure the user groups each have a defined Authentication scheme.
- Make sure the policy has only the Firewall layer enabled.

To configure basic client authentication:

1. In the gateway properties > **Other** > **Legacy Authentication**, click **Enable 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.
2. In the Rule Base, right-click the **Source** and select **Add legacy user access**.
3. Select the group.

   Best Practice - Set the location of allowed resources. Select **Location** and the host, group of hosts, network, or group of networks that users can access.
4. Select the services to authenticate.
5. In **Action**, click **More.**

   The **Action Setting** window opens.
6. Select **Client Auth** and then edit (pencil icon).

   The **Client Auth** window opens.
7. Configure the settings for **Requires Sign On** and **Sign On Method** ("Client Authentication" on page 61).

   If you select **Partially** or **Fully Automatic Client Authentication**, make sure that port 80 is open on the Security Gateway.

   If you select **Manual**, configure the gateway for Wait Mode (on page 64).
8. Make sure the Rule Base does not block all access to the Security Gateway. Put all Client Authentication Rules above the rule that prevents direct connections to the Security Gateway (the Stealth Rule).

   Best Practice - Make sure the **Failed Authentication Attempts** settings for Client Authentication are applicable for your environment. Open **Global Properties** > **Authentication**.
9. Install policy.

Wait Mode

Wait mode is a Client Authentication feature for Standard Sign On with a Telnet session on gateway port 259. With Wait mode, the user can sign off and remove client authentication privileges without a new Telnet session. The Security Gateway keeps the Telnet session open with pings to the client. If the client stops running, the gateway closes the Telnet session and removes authentication privileges from the client's IP address. The Telnet session stays open until the user manually closes the session or stops the client.

Enabling Client Authentication Wait Mode

To enable Wait mode:

1. From the SmartConsole Gateways & Servers view, edit the Gateway object.
2. In the **Other** > **Legacy Authentication** page, 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 with pings to the user's host.
3. Define rules to enable ping:
   - Accept the **echo-request** service, from the Security Gateway to the user's host.
   - Accept the **echo-reply** service, from the user's host to the Security Gateway.

Resolving Access Conflicts

When you configure users, you can define locations that they can access without more authentication. This blocks access to all other locations, which can cause conflicts with security rules that require authentication.

For example: A rule allows authenticated access to users from *Marketing_net* to *Finance_net.* John Smith is in Marketing_net, but in the **Location** tab of his account, connections are permitted only in Marketing_net. If John Smith tries to connect to Finance_net, the firewall cannot resolve the conflict.

You can specify how to resolve this conflict with the **Authentication Action Property** of the rule's source, destination, or both.

To resolve access conflicts:

1. Right-click the **Action** of a rule using **User Auth** or **Client Auth** and click **More**.
2. In the **Action Settings** window, click **Edit**.
3. Select a resolution action:
   - To apply the more restrictive access privileges of the rule and the user account, select **Intersect with User Database**.
   - To allow access according to 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

There are Check Point services available for Client Authentication. You can change the default ports and other settings.

To change the Client Authentication port number:

1. Open Object Explorer and select **Services** > **TCP**.
2. Search for the service to change.
   - To change the settings for Telnet sign on, search for **FW1_clntauth_telnet**.
   - To change the settings for HTTP sign on, search for **FW1_clntauth_http**.
3. Double-click the service, to open its properties window.
4. Click **Advanced**.
5. Configure the service settings.
6. Click **OK**.
7. Install policy.

TCP - Advanced Options

Advanced - sets the advanced options for this service.

- **Source Port** - Enter a port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected when inspecting packets of this service. Otherwise, the source port is not inspected.
- **Protocol Signature** - A unique signature created by Check Point for each protocol and stored on the gateway. The signature identifies the protocol as genuine. Select this option to limit the port to the specified protocol.
- **Enable for TCP resource** - Enables the TCP service for a TCP Resource, if checked.
- **Match for Any -** Indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol.

  When there is a rule whose **Service** cell contains **Any**, and a connections protocol and source port match more than one service object, then the service object with the selected **'Match for Any'** option will be used and its properties will be taken for handling this connection
- **Keep connections open after policy has been installed** even if they are not allowed under the new policy. This overrides the settings in the Connection Persistence page. If you change this property, the change will not affect open connections, but only future connections.

Virtual session timeout - Time (in seconds) before the session times out. Select one of the following options:

- **Default** - Use the default value defined on the **Stateful Inspection** page in the **Global Properties** window.
- **Specific -** Manually define a timeout period specifically for this service.

Aggressive aging

- **Enable Aggressive Aging -** Enable to manage the connections table capacity and memory consumption of the firewall to increase durability and stability.

Cluster and Synchronization

- **Synchronize connections on cluster -** Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster.

  Of the services allowed by the Rule Base, only those with **Synchronize connections on cluster** will be synchronized as they pass through the cluster. By default, all new and existing services are synchronized.

- **Start Synchronizing X seconds after connection initiation -** For all TCP services whose Protocol Type is *HTTP* or *None*, enable this option to delay telling the Security Gateway about a connection, so that the connection will only be synchronized if it still exists x seconds after the connection is initiated. Note that delayed synchronization is disabled if the log or account are enabled.

  Some TCP services (HTTP for example) are characterized by connections with a very short duration. There is no point in synchronizing these connections because every synchronized connection consumes gateway resources, and the connection is likely to have finished by the time a failover occurs.

  This capability is only available if a SecureXL-enabled device is installed on the Security Gateway through which the connection passes. The setting is ignored if connection templates are not off-loaded from the SecureXL-enabled device. See the Performance Pack documentation for additional information.

Allowing Encrypted Client Authentication

Client authentication on HTTPS connections requires explicit rules and gateway configuration.

To configure encrypted Client Authentication for HTTPS Connections:

1. On the Security Gateway, stop Check Point services: `cpstop`
2. Open the configuration file: `$FWDIR/conf/fwauthd.conf`
3. Search for `900 fwssd in.ahclientd wait 900 ssl`
4. Add this parameter: `:defaultCert`
   `900 fwssd in.ahclientd wait 900 ssl:defaultCert`

   Note - **defaultCert** is a nickname in the Certificate List on a Security Gateway. To see the nickname of your gateway, open the **IPsec VPN** page of the Gateway object, and see the **Repository of Certificates**.
5. Save and close the file.
6. On the Security Gateway, start Check Point services: `cpstart`
7. Open SmartConsole.

8. Create this rule, to allow HTTPS traffic between the client and the Web server:

Source	Destination	Services & Applications	Action
<user group>	*<Internal Web server>*	https	Client Auth (Partially automatic or Manual mode)

9. Install the Access Control Policy.

To make sure encrypted authentication is configured:

1. From a client in the supported user group, open a browser to: `https://` *<gateway URL>*`:900`
2. Click **Yes** to trust the Security Gateway certificate.
3. Enter 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**.

Cooperative Enforcement

Cooperative Enforcement works with Check Point Endpoint Security servers. This feature uses the Endpoint Security server compliance to authenticate connections in the internal network.

Endpoint Security server is a centrally managed, multi-layered Endpoint Security solution that uses policy-based security enforcement for internal and remote computers. Easily deployed and managed, the Endpoint Security server mitigates the risk of hackers, worms, spyware, and other security threats. You can quickly develop, manage, and enforce Cooperative Enforcement with it easy-to-use features: predefined policy templates, an intuitive Web-based management interface, PC firewall, and application privilege controls.

Using Cooperative Enforcement, a host that starts a connection through a gateway is tested for compliance. This increases the integrity of the network, because it blocks hosts with malicious software components.

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. Compliance defines if a host is secure, according to the defined prerequisites of software components and blade activation. If a host is not compliant, the gateway blocks connections.

This 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.
2. The firewall checks for host compliance in its tables and queries the Endpoint Security server, if required.
3. On the first server's reply to the client, Cooperative Enforcement begins. Connections from compliant hosts are allowed, and connections from non-compliant hosts are blocked.

When you enable Cooperative Enforcement on a gateway, these implied rules are automatically enabled:

1. Allow all firewall GUI clients to connect to the Endpoint Security server through HTTP or HTTPS (port 80 or 443).
2. Allow all internal clients to access the Endpoint Security server through the firewall for heartbeats.
3. Allow the firewall to communicate with the Endpoint Security server on port 5054.

If you require more access permissions (such as *allow external clients to connect to the Endpoint Security server*, or *allow computers to access Endpoint Security server administration*), define explicit rules.

NAT Environments

Cooperative Enforcement 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 recognize the same IP address of a client. If NAT causes the IP address received by gateway to be different than the IP address received by the Endpoint Security Server, Cooperative Enforcement will not work.

Configuring Cooperative Enforcement

To configure Cooperative Enforcement:

From the gateway **Cooperative Enforcement** page, click **Authorize clients using Endpoint Security Server** to enable Cooperative Enforcement.

- **Monitor Only** - The firewall requests authorization from the Endpoint Security server, but connections are not dropped. Hosts can connect while the gateway grants authorization. The Firewall generates logs for unauthorized hosts. You can add unauthorized hosts to the host's exception list or make those hosts compliant in other ways.

  If Monitor Only is not selected, Cooperative Enforcement works in **Enforcement mode**. The Endpoint Security Firewall blocks non-compliant host connections. For HTTP connections, the client is notified that its host is non-compliant. The user can change the computer to make compliant. For example, the user can upgrade the version of the Endpoint Security client.
- **Track unauthorized client status** - Set a log, or alert option for the hosts that would be dropped if not in Monitor Only mode.
- 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 **Select Endpoint Security Server**. Click **New** to create a new server.
- In the **Client Authorization** section, define exceptions for client authorization.
  - **Check authorization of all clients -** Get authorization from all clients.
  - **Bypass authorization of the following clients -** Allow clients in the selected groups to always connect, without authorization inspection. All other clients are inspected.
  - **Check authorization only of the following clients -** Inspect authorization of clients from the selected groups. All other clients bypass authorization.

Content Security

The Firewall integrates Content Security capabilities with best-of-breed, OPSEC-certified applications. OPSEC applications let you select content screening applications that best meet your needs, while managing Content Security centrally:

- 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

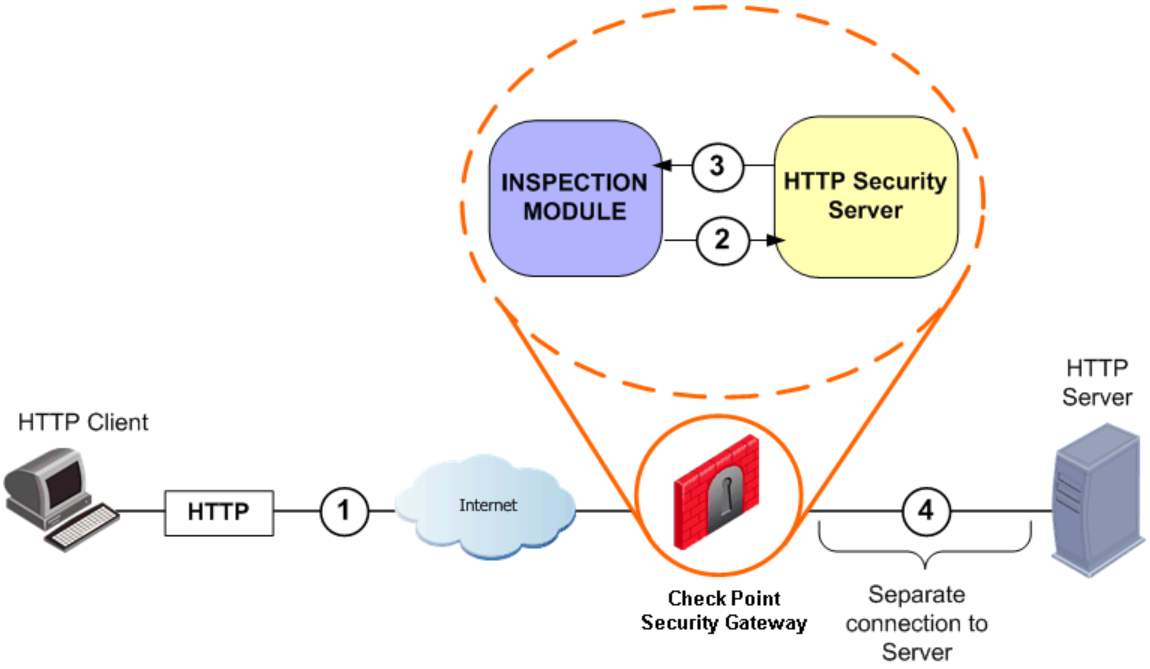
There is also a generic TCP Security server. Security servers employ many ways of enforcing Content Security, including, checking whether the connections for these protocols are well formed, stripping script tags for HTTP, email address translation for SMTP, and file name matching for FTP.

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 54).

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.

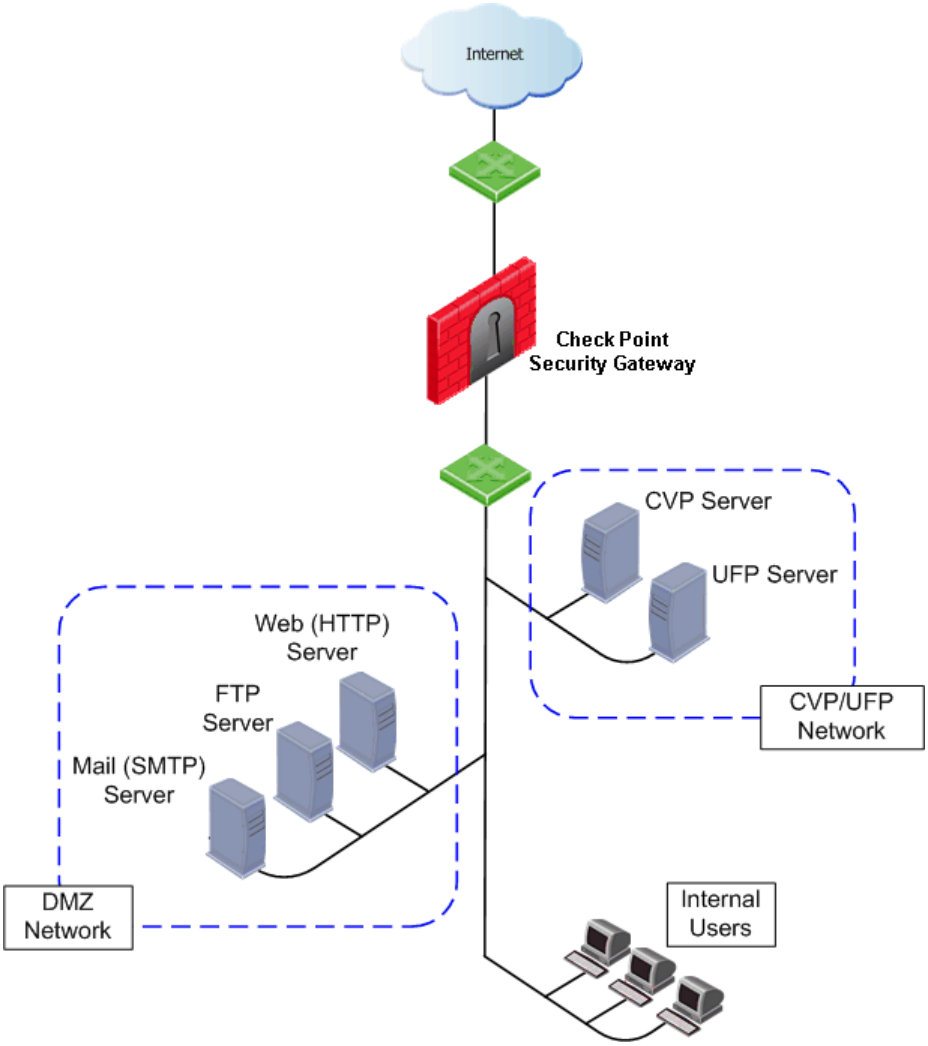


The source IP address that appears to the destination server is the IP address of the client that originally opened the connection. The connection leaves the Security server with the source IP address of the Security Gateway, and the outbound kernel performs NAT so that the source IP address is that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

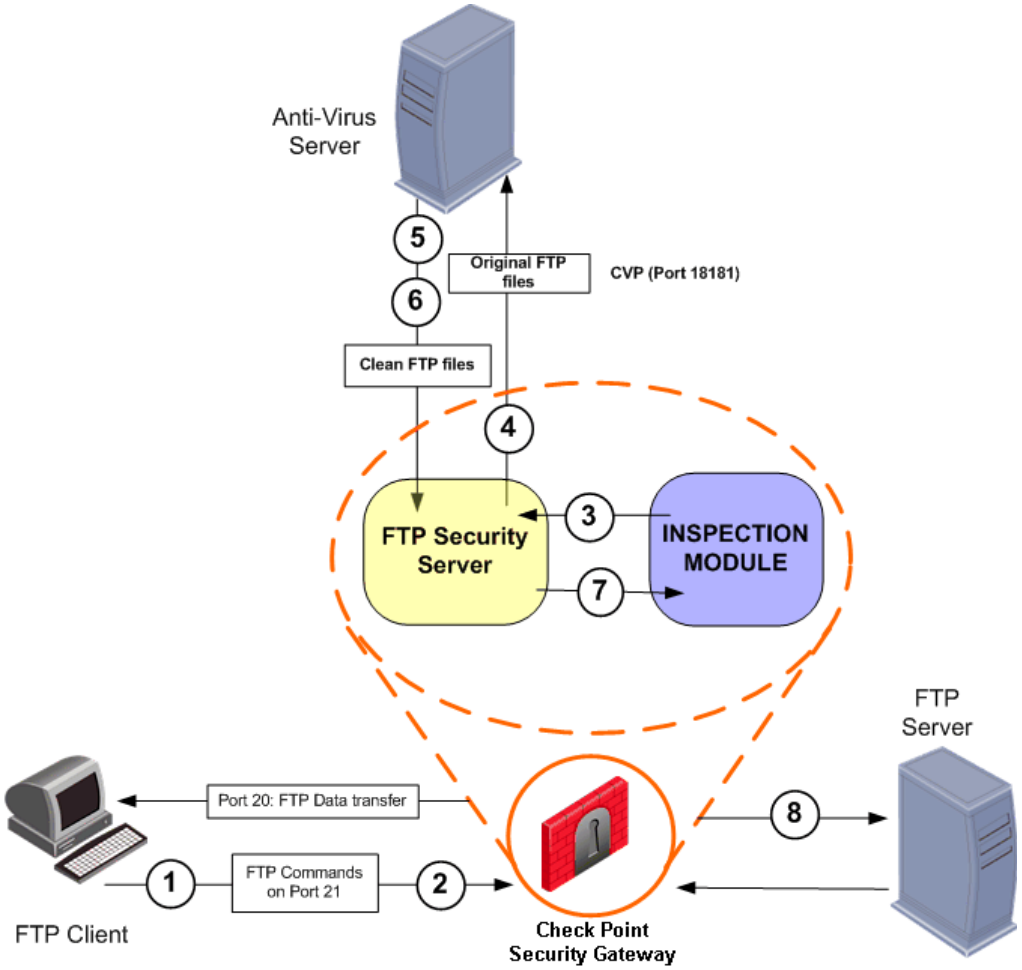
The Security Gateway considers non-executable picture and video files to be safe because they do not normally contain viruses.

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 78).

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 79).

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 SmartConsole. 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 83) 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:

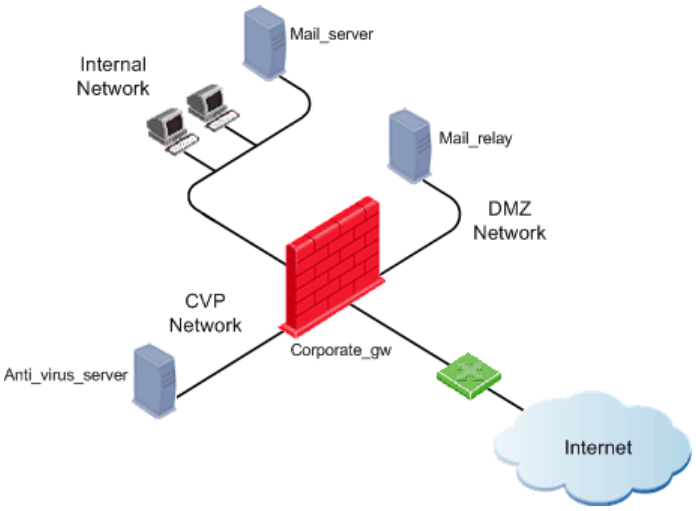
1. In SmartConsole, click **Open Object Explorer** (Ctrl+E).
2. Click **New** > **Resource** and select the resource type. For example **URI** or **SMTP**.
3. Define the resource parameters in the **General** tab, and in the other tabs as required.
4. To use a service with a resource in an Access Control Policy rule,
   a) Right-click in the **Services & Applications** column (that has the value **Any*)
   b) Select **Add with Resource**.
   c) In the **New Service with Resource** window, select the **Service**.
   d) Select the **Resource** that will operate on the service.
   e) Click **OK**.

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

The Policy must have only the Firewall Layer enabled.

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.



Workflow for configuring 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
   a) In SmartConsole, click **Open Object Explorer** (Ctrl+E).
   b) Click **New** > **Server** > **OPSEC Application** > **Application**.
   c) In the **General** tab, give the OPSEC Application object a **Name**.
   d) Associate it the with the **Host** object created in step 1.
   e) Initialize **Secure Internal Communication** between the OPSEC Application and the Security Management Server.
   f) Select the **Vendor** and **Product**. For an Anti-Virus product, one of the selected **Server Entities** must be *CVP*
   g) 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 **Object Explorer**, click **New** > **Resource** > **SMTP**.

b) In the **General** page, 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**.

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

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

e) 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 Access Control policy. Click **Install Policy**.

Source	Destination	Services & Applications	Action	Track	Install On	Comments
Any	mail_relay	smtp	Accept	Log	Corporate_gw	Incoming to mail relay
mail_relay	mail_server	smtp-> virus_check	Accept	Log	Corporate_gw	Incoming virus scan
mail_server	Any	smtp	Accept	Log	Corporate_gw	Outgoing email

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 74).

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

Source	Destination	Services & Applications	Action
Internal_LAN	Any	http->Internal.HTTP.CVP	Accept

Performing CVP/UFP Inspection on any TCP Service

In this procedure, you will create and configure a TCP service and a TCP resource. Do these steps in the Firewall Layer of the Access Control Policy.

To configure CVP or UFP inspection on any TCP service:

1. Open the **Object Explorer** (Ctrl+E)
2. Select **New** > **Service** > **TCP**.
3. Fill in the general properties of the new TCP service.
4. Click **Advanced**.
5. In the **Advanced** window, check **Enable for TCP Resource** and then click **OK**.
6. In the **Object Explorer**, select **New** > **Servers > OPSEC Applications** > **Applications**.
7. In the **OPSEC Application Properties** window, name the server and select **Server Entities** > **CVP** and **UFP**.
8. Select a host to act as the CVP and UFP server.
9. In the **UFP Options** and **CVP Options** tabs, select the TCP service configured in the Services tab.
10. Click **OK**.
11. In the **Object Explorer**, select **New** > **Resource** > **TCP**.
12. In the **TCP Resource Properties** window, provide a name for the resource and choose **UFP** or **CVP**.
13. 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.
14. Click **OK**.
15. Add a rule to the Rule Base: in the **Service** column, right click and select **Add with Resource.**
16. In the **Service with Resource** window, select the configured TCP service.
17. In the **Resource** drop-down list, select the configured TCP resource.
18. Install the security policy: **Policy** > **Install**.

Advanced CVP Configuration: CVP Chaining and Load Sharing

Introduction to CVP Chaining and Load Sharing

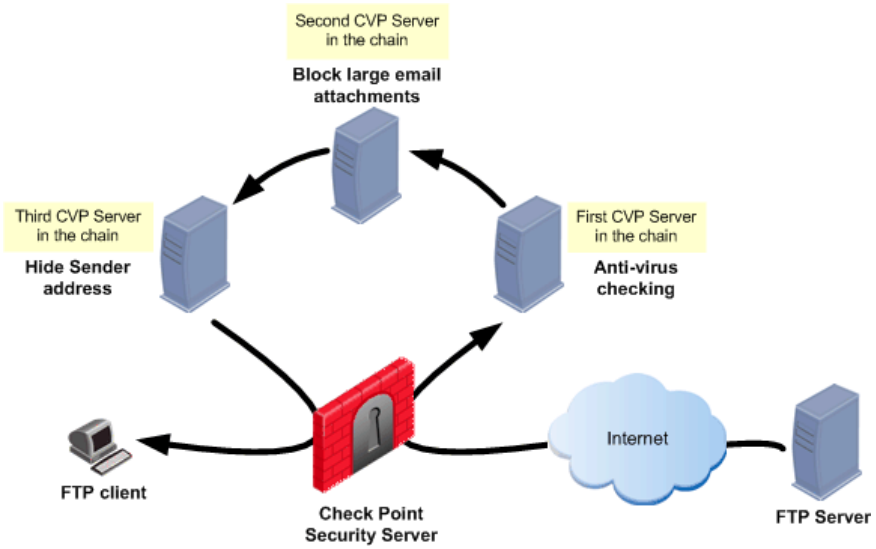
Traffic that crosses the Security Gateway can be checked using CVP servers. CVP checking is available for Web, Mail, FTP and TCP traffic. For detailed explanations, see:

- CVP and Anti-Virus Protection for SMTP and HTTP Traffic (on page 73)
- Using CVP for Virus Scanning on FTP Connections (on page 75)

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 of the Security Gateway 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

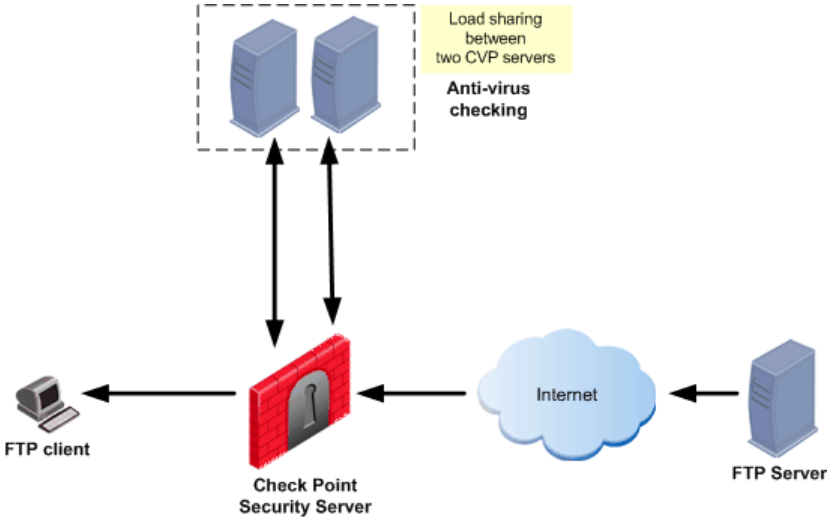
Identical CVP servers can be configured to share the load among themselves. Load Sharing can speed up CVP checking by allowing many CVP sessions to run simultaneously on more than one CVP server.

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.

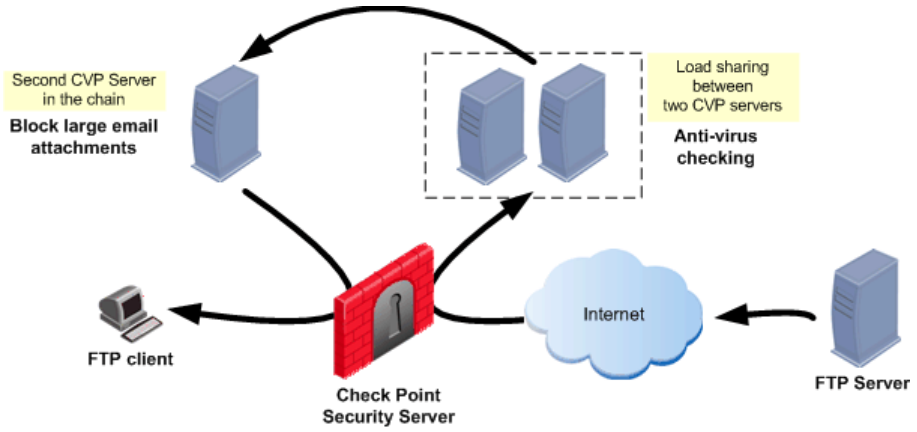
CVP Load Sharing is implemented by defining a Resource that invokes a group of CVP servers. The order in round robin mode is configured in the CVP Group object.



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:
   a) In SmartConsole, click **Open Object Explorer** (Ctrl+E).
   b) Click **New** > **Server** > **OPSEC Application** > **Application**.
   c) 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. In **Object Explorer**, select **New** > **Server** > **OPSEC Application** > **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:
   a) In the **Object Explorer**, click **New** > **Resource** > **URI** or **SMTP** or **FTP** or **TCP**.
   b) Define the content security capabilities.
7. In the **CVP Server** field in the **CVP** page of the Resource object, select the CVP Group defined in step 2.
8. In the Access Control Policy Rule Base, define a rule that uses the Resource.
9. Install the Access Control policy: Click **Install Policy**.

Appendix: Regular Expressions

In This Section:

Regular Expression Syntax

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

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

Using Non-Printable Characters

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

Character	Description
\a	alarm; the BEL character (hex 07)
\cx	"control-x", where x is any character
\e	escape (hex 1B)
\f	formfeed (hex 0C)
\n	newline (hex 0A)
\r	carriage return (hex 0D)
\t	tab (hex 09)
\ddd	character with octal code ddd
\xhh	character with hex code hh

Using Character Types

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

Character	Description
\d	any decimal digit [0-9]
\D	any character that is not a decimal digit
\s	any whitespace character
\S	any character that is not whitespace
\w	any word character (underscore or alphanumeric character)
\W	any non-word character (not underscore or alphanumeric)