Security Gateway Virtual Edition
Hypervisor Mode
Administration Guide

R75.40

15 November 2012
Important Information

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

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=21381
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 November 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Security Gateway Virtual Edition Overview</td>
<td>6</td>
</tr>
<tr>
<td>Glossary</td>
<td>7</td>
</tr>
<tr>
<td>Key Benefits</td>
<td>8</td>
</tr>
<tr>
<td>Hypervisor Mode Overview</td>
<td>8</td>
</tr>
<tr>
<td>Basic Deployment with Hypervisor Mode</td>
<td>8</td>
</tr>
<tr>
<td>Hypervisor Connector</td>
<td>9</td>
</tr>
<tr>
<td>IP Anti-Spoofing</td>
<td>10</td>
</tr>
<tr>
<td>Network Mode Overview</td>
<td>11</td>
</tr>
<tr>
<td>Basic Deployment with Network Mode</td>
<td>11</td>
</tr>
<tr>
<td>Cluster Support</td>
<td>12</td>
</tr>
<tr>
<td>Licensing Security Gateway Virtual Edition</td>
<td>12</td>
</tr>
<tr>
<td>ESX Host Security Considerations</td>
<td>12</td>
</tr>
<tr>
<td>Installing and Uninstalling</td>
<td>13</td>
</tr>
<tr>
<td>Installing Security Gateway Virtual Edition Virtual Machine</td>
<td>13</td>
</tr>
<tr>
<td>Saving Hypervisor Connector Settings</td>
<td>13</td>
</tr>
<tr>
<td>Getting the Template</td>
<td>14</td>
</tr>
<tr>
<td>Deploying the Security Gateway Virtual Edition Virtual Machine</td>
<td>14</td>
</tr>
<tr>
<td>Mapping Interfaces and Completing the Procedure</td>
<td>15</td>
</tr>
<tr>
<td>Completing the Deployment</td>
<td>16</td>
</tr>
<tr>
<td>Configuring the Virtual Machine Settings</td>
<td>16</td>
</tr>
<tr>
<td>Memory</td>
<td>16</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>16</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>17</td>
</tr>
<tr>
<td>Configuring the Network</td>
<td>17</td>
</tr>
<tr>
<td>Installing Check Point Products</td>
<td>18</td>
</tr>
<tr>
<td>Selecting the Installation Mode</td>
<td>19</td>
</tr>
<tr>
<td>Completing the Installation</td>
<td>20</td>
</tr>
<tr>
<td>Cluster Support</td>
<td>20</td>
</tr>
<tr>
<td>Licensing Security Gateway Virtual Edition</td>
<td>20</td>
</tr>
<tr>
<td>Uninstallation</td>
<td>21</td>
</tr>
<tr>
<td>Removing Hypervisor Connector</td>
<td>21</td>
</tr>
<tr>
<td>Uninstalling Security Gateway Virtual Edition</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Hypervisor Mode</td>
<td>22</td>
</tr>
<tr>
<td>Configuring a User for Hypervisor Mode</td>
<td>22</td>
</tr>
<tr>
<td>Configuring a Local ESX Connection</td>
<td>23</td>
</tr>
<tr>
<td>Enabling or Disabling Clusters</td>
<td>23</td>
</tr>
<tr>
<td>Configuring Global Options</td>
<td>23</td>
</tr>
<tr>
<td>Default Security Settings</td>
<td>23</td>
</tr>
<tr>
<td>Global Failure Setting</td>
<td>24</td>
</tr>
<tr>
<td>Cluster Anti-Spoofing</td>
<td>24</td>
</tr>
<tr>
<td>MAC Address Anti-Spoofing</td>
<td>25</td>
</tr>
<tr>
<td>Configuring Hypervisor Connector Policy</td>
<td>25</td>
</tr>
<tr>
<td>The Virtual Object Hierarchy</td>
<td>25</td>
</tr>
<tr>
<td>Understanding Security Setting Precedence</td>
<td>26</td>
</tr>
<tr>
<td>Configuring vSwitches</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Port Groups</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Virtual Machines</td>
<td>28</td>
</tr>
<tr>
<td>Hypervisor Mode Operations</td>
<td>29</td>
</tr>
<tr>
<td>Configuring the Communication Channel</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Hypervisor Mode for Routers</td>
<td>30</td>
</tr>
<tr>
<td>Configuring IP Anti-Spoofing</td>
<td>31</td>
</tr>
</tbody>
</table>
Check Point Security Gateway Virtual Edition protects dynamic virtual environments and external networks from internal and external threats by securing virtual machines and applications. This solution uses proven Check Point security technologies: Software Blade architecture, Firewall with content inspection, IPS, central management, and more.

Security Gateway Virtual Edition has different operation modes. Hypervisor Mode and Network Mode. Hypervisor Mode enforces VM security within the VMware Hypervisor by inspecting inter-VM traffic, without changing the virtual network topology.

**Important** -
- Only Hypervisor Mode is supported in this release.
- Unless otherwise stated, all references to ESX throughout this document relate to ESXi 5.0 / 5.1. *This release supports ESXi 5.0 and 5.1 only.*
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter</td>
<td>Collection of hosts and their associated Virtual Machines and datastores.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Host-independent storage location for Virtual Machine files in ESX environments. This is typically a system volume located on a physical disk, RAID, SAN, or network file system.</td>
</tr>
<tr>
<td>Data Resource Scheduler (DRS)</td>
<td>Monitors resource utilization across resource pools and allocates resources amongst virtual machines to maximize throughput.</td>
</tr>
<tr>
<td>ESX/ESXi Host</td>
<td>Physical server using VMware to host one or more Virtual Machines and other virtual objects. All references to ESX are also relevant for ESXi unless specifically noted otherwise.</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>Software system running on the ESX host that monitors and controls guest operating systems. In vSphere environments, the VMkernel is the hypervisor.</td>
</tr>
<tr>
<td>Hypervisor Connector (cpdvfilter)</td>
<td>Check Point kernel module that directs Virtual Machine traffic to and from the Security Gateway Virtual Edition for inspection. This module is loaded into the hypervisor when working in hypervisor mode.</td>
</tr>
<tr>
<td>Port Group</td>
<td>One or more vSwitch ports sharing common options, such as bandwidth limitations and VLAN tagging policies. Virtual Machines connect to vSwitches via port groups.</td>
</tr>
<tr>
<td>Security Gateway Virtual Edition (VE)</td>
<td>Check Point virtual Security Gateway that protects dynamic virtual environments from internal and external threats.</td>
</tr>
<tr>
<td>Virtual Network Interface (vNIC)</td>
<td>A software based abstraction of a physical interface that supplies network connectivity for Virtual Machines.</td>
</tr>
<tr>
<td>Virtual Machine (VM)</td>
<td>A software abstraction of a physical computer.</td>
</tr>
<tr>
<td>Virtual Network</td>
<td>A network of VMs running on an ESX host. The individual VMs are logically connected to each other. Virtual networks do not depend on physical network interfaces.</td>
</tr>
<tr>
<td>Virtual Switch (vSwitch)</td>
<td>A software abstraction of a physical Ethernet switch. vSwitches can connect to physical switches, via physical network adapters, to join virtual networks with physical networks.</td>
</tr>
<tr>
<td>VMotion</td>
<td>VMware technology that allow running VMs to migrate from one ESX host to the other.</td>
</tr>
<tr>
<td>VMSafe</td>
<td>VMware API technology that lets 3rd party software integrate with the hypervisor. Security Gateway Virtual Edition in Hypervisor mode uses VMSafe APIs to secure virtual networks.</td>
</tr>
<tr>
<td>vSphere Client</td>
<td>VMware GUI client used to manage VMs and associated objects. It manages VMs much in the same way that SmartDashboard manages Security Gateways.</td>
</tr>
</tbody>
</table>
Key Benefits

**Hypervisor Mode:**
- Protects VMs and traffic between VMs.
- Secures dynamic virtual environments without network topology changes.
- Leverages VMware VMsafe for tight integration with the ESX environment.
- Protects against security breaches caused by configuration errors.
- Gives out-of-the-box protection with easy configuration.
- Supports R75.40 Software Blade architecture.
- Maximizes security granularity at the vSwitch, port group, and VM levels.
- Supports ESX clusters for VM high availability and load sharing.
- Enforces security with no downtime during and after vMotion migration.
- Lets growing enterprises protect expanding virtual networks while reducing hardware investment, maintenance, energy, and site costs.
- Optimizes performance for virtual environments.

**Network Mode:**
- Operates as a layer-2 or layer-3 Security Gateway for virtual network environments.
- Supports ClusterXL for high availability and load sharing.
- Enforces security with no downtime during and after vMotion migration.
- Supports vMotion of the Security Gateway Virtual Edition virtual machine.
- Lets growing enterprises protect expanding virtual networks while reducing hardware investment, maintenance, energy, and site costs.
- Optimizes performance for virtual environments.

**Hypervisor Mode Overview**

Ensures the security of virtual machines by inspecting all VM traffic. Security Gateway Virtual Edition utilizes VMware's VMsafe technology to seamlessly enforce security within the hypervisor. Hypervisor Mode does not require changes to the VM network topology.

To install Security Gateway Virtual Edition in Hypervisor Mode, the ESX or ESXi host must have a license that includes VMsafe and dvfilter.

**Basic Deployment with Hypervisor Mode**

In this basic Hypervisor Mode deployment, one VM on an ESX host has a standalone Security Gateway Virtual Edition with a Security Management Server. This standalone Security Gateway Virtual Edition is connected to a vSwitch with an ESX Service Console or with an ESXi Host Management Network port. The standalone Security Gateway Virtual Edition protects all of the other VMs on the ESX host, even though it is not connected to them by a switch or router. This works using a Hypervisor Connector. The Hypervisor Connector attaches to each vNIC of each VM automatically when you install Hypervisor mode on the Security Gateway Virtual Edition.
The Security Gateway Virtual Edition inspects all traffic that goes to or leaves from the VMs. For example, Security Gateway Virtual Edition inspects traffic between the different server VMs.


**Hypervisor Connector**

Security Gateway Virtual Edition with Hypervisor Mode is an "out of the box" security solution for VMware virtual environments, protecting your environment after only a few steps. The secret of this solution is the Hypervisor Connector, which automatically attaches itself to VM vNICs.
The Hypervisor Connector inspects traffic on vNICs without configuration on the ESX host or the VM. Administrators configure security settings using a simple command line interface integrated into the familiar Check Point sysconfig utility.

The Hypervisor Connector uses default security settings together with object hierarchy and security setting inheritance for maximum granularity. It is not necessary to define explicit settings for all virtual objects (VMs, port groups, and vSwitches).

**Note** - You must install Security Gateway Virtual Edition in Hypervisor Mode to use the Hypervisor Connector.

### Automatic Attachment

After installation, Security Gateway Virtual Edition does these actions to initialize the Hypervisor Mode:

1. Installs and loads the Hypervisor Connector.
2. Attaches the Hypervisor Connector to all vNICs.
3. Creates a new vSwitch named `_cp_private_vSwitch` connected to a new port group called `_cp_private`.
5. Defines an IP address for the new bridge interface. This IP address is used to communicate with the Hypervisor Connector.

After installation, the Hypervisor Connector is in the bypass mode until you install a policy on the Security Gateway Virtual Edition. In the bypass mode, all traffic is allowed without inspection.

### Security Options

You can configure the Hypervisor Connector enforcement behavior for each vNIC using these settings:

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secured</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition, which allows or blocks traffic according to the security policy.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>All traffic is allowed and no inspection occurs.</td>
</tr>
<tr>
<td>Monitored-only</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition. The Hypervisor Connector does not block any traffic. But traffic is still passed to the Security Gateway Virtual Edition, which can block traffic according to the Firewall Security Policy. All events are logged.</td>
</tr>
<tr>
<td>Blocked</td>
<td>All traffic is blocked and no inspection occurs.</td>
</tr>
</tbody>
</table>

### IP Anti-Spoofing

Security Gateway Virtual Edition Hypervisor Mode enforces IP Anti-Spoofing for vNICs on an ESX host. Protection setting granularity lets you define IP Anti-Spoofing protection for individual vSwitches, port groups, VMs and individual vNICs.


You cannot use the physical Security Gateway IP Anti-Spoofing feature when using the Hypervisor Mode.

Hypervisor Mode makes sure that packets with a VM source IP address actually come from a vNIC connected to that VM.
Hypervisor Mode enforces IP Anti-Spoofing for each vNIC according to a hierarchy of objects connected to the vNIC:

1. **Virtual Machine**: The Hypervisor Connector enforces IP Anti-Spoofing as defined for the VM object.
2. **Port Group**: If IP Anti-Spoofing is not defined for the VM object, the Hypervisor Connector enforces IP Anti-Spoofing as defined for the port group object.
3. **vSwitch**: If IP Anti-Spoofing is not defined for the VM or port group object, the Hypervisor Connector enforces IP Anti-Spoofing as defined for the vSwitch object.
4. If IP Anti-Spoofing is not defined for any VM, port group, or vSwitch objects, the Hypervisor Connector does not enforce IP Anti-Spoofing for the vNIC. However, packets going through an unprotected vNIC cannot spoof IP addresses for other protected vNICs.

## Network Mode Overview

Secures virtual environments and perimeter networks by deploying the Security Gateway Virtual Edition as a virtual network device (layer 2 or layer 3). This mode requires changing the network topology to include:

- Explicit routing or
- Layer-2 bridging

## Basic Deployment with Network Mode

In this basic Network Mode deployment, one VM has a standalone Security Management Server with a Security Gateway Virtual Edition to protect three networks. These networks connect using vSwitches.

<table>
<thead>
<tr>
<th>Callout</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physical Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>SmartDashboard and vSphere client</td>
</tr>
<tr>
<td>3</td>
<td>LAN</td>
</tr>
</tbody>
</table>

---

Security Gateway Virtual Edition Administration Guide Hypervisor Mode | 11
The Security Gateway Virtual Edition inspects all traffic between virtual networks. For example, Security Gateway Virtual Edition inspects traffic between the Web server and database server VMs.

Administrators manage network security using SmartDashboard, which connects to the Security Management Server VM.

## Cluster Support

### Hypervisor Mode

Hypervisor Mode adds enhanced functionality to VMware clusters. VMware VMotion lets you migrate running VMs from one ESX host in a VMware cluster to the other. Hypervisor Mode gives continuous service availability and full transaction integrity during VM migration.

The security policy distributes across all the Security Gateway Virtual Edition members within the cluster. In this mode you must install a Security Gateway Virtual Edition on every ESX cluster member.

### Network Mode

Network Mode uses ClusterXL High Availability or Load Sharing to support VMware ESX clusters.

## Licensing Security Gateway Virtual Edition

Each Security Gateway Virtual Edition instance requires its own license. You must purchase a license according to the number of physical cores on the local ESX host. Security Gateway Virtual Edition licenses are assigned to IP addresses.

Each Security Gateway and Security Management server installed on a VM must have a license.

## ESX Host Security Considerations

We recommend that you read the *VMware Best Practices - Security Hardening* document for suggestions on how to secure your ESX host.

Check Point recommends the following practices:

- Always use different, secured networks for the VMkernel and ESX service console/ESXi Host Management Network, because this traffic is not automatically inspected by Security Gateway Virtual Edition. You can configure Security Gateway Virtual Edition to protect the ESX host and VMkernel.

- Grant users only the necessary privileges. For example, only VMware security administrators have access to the Security Gateway Virtual Edition.

  This recommendation applies to Check Point and VMware permissions. To learn more about VMware roles and permissions, see the best practices in the *VMware Managing VMware Virtual Center Roles and Permissions Guide*. 
Chapter 2

Installing and Uninstalling

In This Chapter

Installing Security Gateway Virtual Edition Virtual Machine .................................................. 13
Configuring the Virtual Machine Settings ................................................................................. 16
Initial Configuration ....................................................................................................................... 17
Uninstallation ................................................................................................................................. 21

The installation procedure lets you quickly deploy Security Gateway Virtual Edition on your ESX hosts.
Security Gateway Virtual Edition is distributed as a VMware OVF template preconfigured for most common
deployments.

Installing Security Gateway Virtual Edition Virtual Machine

The installation of a new Security Gateway Virtual Edition VM includes these tasks:

• Importing the OVF template and starting the **Deploy OVF Template** wizard.
• Configuring the Security Gateway Virtual Edition VM in the ESX inventory.
• Mapping the Security Gateway Virtual Edition VM interfaces to your network.

For VMware cluster deployments, repeat these procedures for each cluster member.

**Saving Hypervisor Connector Settings**

Although you cannot upgrade from R75.20VE to R75.40VE, you can save Hypervisor Connector settings
from ESX to ESXi 5.0 / 5.1.

**To save Hypervisor Connector settings:**

On the ESX host:

1. Log on to the R75.20 VE gateway.
3. Turn off VMs, or migrate the VMs to a different ESX host.
   **Important!** If the ESX that will host the migrated VMs does not have a VE in Hypervisor mode installed,
you must configure Fail-Open *before* you migrate the VMs. If you do not, the VMs will not have network
connectivity.
4. Uninstall R75.20 VE.
   • Uninstall Hypervisor Mode
   • Uninstall Security Gateway Virtual Edition
5. Upgrade your ESX host to ESXi 5.0 or 5.1.
6. Install R75.40 VE.
7. Copy `virt_conf.C` saved in step 2 to `$CPVIRTDIR/conf/` on the newly installed R75.40VE.
8. If you changed your ESX host password during the ESX upgrade, reset your local ESX connection. On
   the Virtual Edition gateway:
   a) Run: `sysconfig`
   b) Select: 7. Hypervisor mode
   c) Select: 1. Local ESX Connection
7. In SmartDashboard, reset SIC with the gateway.
Getting the Template

To get the Security Gateway Virtual Edition OVF Template:
1. Download Check_Point_Security_Gateway_R75.40_VE.tgz to your vSphere Client computer.
2. Extract the template OVF file to a temporary folder.

Deploying the Security Gateway Virtual Edition Virtual Machine

To deploy the VM and save it in the inventory:
1. In the VMware vSphere client, select an ESX host.
2. Select File > Deploy OVF Template. The Deploy OVF Template wizard opens.
3. In the Source window, select Deploy from file.
4. Enter or select the .ovf file and then click Next.
5. In the OVF Template Details window, click Next.
6. If the Name and Location window opens, select an inventory location for the VM.
7. If the Disk Format window opens, select Thick provisioned format.
8. If the Host/Cluster window opens, select a host. This window only opens if there are multiple hosts or clusters.
9. If the Datastore window opens, select a datastore. This window only opens if there is more than one datastore associated with the host or cluster.

Note - We recommend that you deploy the Security Gateway Virtual Edition on ESX Host local storage instead of external storage.
Mapping Interfaces and Completing the Procedure

To map the Security Gateway Virtual Edition interfaces and complete the import procedure:

1. In the Network Mapping window, configure the default network adapters and destination networks as shown in this example.

   Security Gateway Virtual Edition is pre-configured with four network adapters.

   **Note** - This configuration table is only relevant for Hypervisor Mode deployments. If you are deploying the Network Mode, you can connect the vNICs to internal and external networks as necessary. You can also add and delete vNICs as necessary.

<table>
<thead>
<tr>
<th>Source Network</th>
<th>Description</th>
<th>Destination Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ESX Management</td>
<td>vSphere Host connection</td>
<td>Port group connected to the ESX service console/ESXi Host Management Network.</td>
</tr>
<tr>
<td>2 Check Point Management</td>
<td>Check Point management connection (optional)</td>
<td>Port group connected to the Check Point management network. This can be the same network as the ESX Management.</td>
</tr>
<tr>
<td>3 Check Point Sync</td>
<td>Cluster synchronization connection</td>
<td>Port group connected to the Check Point cluster synchronization network.</td>
</tr>
<tr>
<td>4 Check Point reserved for auto-attachment</td>
<td>Reserved for inspection traffic and Hypervisor Connector auto-attachment (Hypervisor Mode only)</td>
<td>Do not change the default value assigned by the ESX host. The destination network is assigned automatically. <strong>Do not assign an IP address to the vNIC connected to this network.</strong></td>
</tr>
</tbody>
</table>

2. For each source network, select a destination network from the list. (The destination network names are examples and will be different for your deployment.)
Completing the Deployment

To complete the VM deployment:

1. In the Ready to Complete window, click Finish. It may take a while to add your new Security Gateway Virtual Edition VM to the inventory.
2. Select the Security Gateway Virtual Edition from the inventory and power it on.

Important
- When using the Hypervisor Mode, you cannot use VMotion to migrate a Security Gateway Virtual Edition VM to a different ESX host.
- When working in Network Mode, you can use VMotion to migrate Security Gateway Virtual Edition VM to a different ESX host.
- If you are going to install the Hypervisor Mode, disable DRS for the Security Gateway Virtual Edition VM.

Configuring the Virtual Machine Settings

To see the Security Gateway Virtual Edition settings:

- Right-click the VM and select Edit Settings.

The Virtual Machine Properties window opens.

Memory

A minimum 512 Mb of memory is necessary to run Security Gateway Virtual Edition. Add additional memory as necessary to increase connection capacity.

Network Adapters

Security Gateway Virtual Edition is pre-configured with four network adapters, as shown in this table.

Note - This configuration table is only relevant for Hypervisor Mode deployments. If you are deploying the Network Mode, you can connect the vNICs to internal and external networks as necessary. You can also add and delete vNICs as necessary.
### Source Network | Description | Destination Network
--- | --- | ---
1 | ESX Management | Port group connected to the ESX service console/ESXi Host Management Network.
2 | Check Point Management | Port group connected to the Check Point management network. This can be the same network as the ESX Management.
3 | Check Point Sync | Port group connected to the Check Point cluster synchronization network.
4 | Check Point reserved for auto-attachment | Do not change the default value assigned by the ESX host. The destination network is assigned automatically. Do not assign an IP address to the vNIC connected to this network.

**Important** - For Hypervisor Mode installations only, you must read this list and make sure it is true in your environment to ensure connectivity:

- You must leave one network adapter undefined and available for inspection traffic. Do not configure an IP address to this network adapter. Typically this is the Check Point reserved for inspection source network, which is automatically assigned to the `cp_private` destination network.
- Make sure that one vNIC (typically **ESX Management**) connects to a port group connected to the ESX service console/ESXi Host Management Network.
- Do not delete the **ESX management** or the Check Point reserved for inspection vNICs.
- If you are not using the **Check Point Management** or the **Check Point Sync** vNICs, you can safely delete them.

### Initial Configuration

**Configuring the Network**

To configure the network and set the system date and time:

1. Power on the Security Gateway Virtual Edition VM.
2. Log in using **admin** as the user name and password.
3. When prompted, change the password and, optionally, the user name. The new password must contain at least six characters.
4. Run `sysconfig`. The **Configuration** window opens and shows a welcome message. Enter 'n' to continue.
5. Select the keyboard language and then enter 'n' to continue. The default language is US English.
6. From the **Network Configuration** menu, configure these parameters:

```
Network Configuration
-----------------------------------------------
1) Host Name  3) Domain Name Servers  5) Routing
2) Domain Name 4) Network Connections
-----------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
-----------------------------------------------
Your choice:
```

- **a)** Define a host name if necessary.
b) Set the domain name and DNS server (if required).

c) Define IP addresses for the network connections (vNICs) as necessary.

**Important** - For Hypervisor Mode deployments:
- You must configure an IP Address for the ESX Host connection. We recommend that you use **eth0** for this purpose.
- You must always keep one vNIC with no defined IP address. Hypervisor Mode uses this vNIC for inspecting traffic sent by the Hypervisor Connector. If this vNIC is not available, Virtual machines can have connectivity problems.

a) Define a default gateway (if required).

7. In the **time and date configuration** menu, use the menu options to configure these parameters:

```
Choose a time and date configuration item:
------------------------------------------
1) Set time zone                        3) Set local time
2) Set date                             4) Show date and time settings
------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
------------------------------------------
Your choice:
- Time zone
- Date
- Local time
```

8. Select **Show date and time settings** to make sure that the information is correct.

If the date and time are correct, press **n** to continue.

**Installing Check Point Products**

To install Check Point products:

1. In the **Import Check Point Products configuration** window, press **n** to continue.
2. In the **Check Point Suite Welcome** window press **N** to continue.
3. Press **Y** to accept the **End User License Agreement**.
4. In the next window, select **New Installation** (default option) and press **N** to continue.

```
Please select one of the following options

1 (*) New Installation
2 ( ) Installation Using Imported Configuration
```

5. Select Check Point products to install.

```
The following products are available in this version
Please select product(s)

1 [*] Security Gateway
2 [*] Performance Pack
3 [*] Security Management
4 [ ] Smart Event and Smart Reporter Suite
5 [ ] Endpoint Security
6 [ ] Management Portal
7 [ ] Mobile Access
```

To install a product, enter the number to the left of the product. An asterisk indicates products selected for installation. This example shows the default choices.

To cancel installation of a selected product, enter its related number.
Note -
Endpoint Security is not currently supported.
Mobile Access is only supported in Network Mode installations.

- You must install a Security Gateway.
- To install a stand-alone deployment that includes a Security Management Server, make sure that Security Management (3) is selected.
- To install a distributed deployment (without a Security Management Server), enter 3 to clear the selection.
- We recommend that you install the Performance Pack (2) for enhanced performance.

6. If prompted, select the Security Management installation type.

Please specify the Security Management type you are about to install

1 (*) Primary Security Management
2 ( ) Secondary Security Management
3 ( ) Log Server

Note - Management High Availability and Log Server are not supported on a standalone Security Gateway Virtual Edition.

Selecting the Installation Mode

In the VE Installation window, select an installation mode and configure Security Gateway Virtual Edition.

Important
- After you select an installation mode, you cannot change it. To change the installation mode, you must deploy the Security Gateway Virtual Edition OVF again
- If you select Hypervisor mode, make sure that at least one virtual switch exists on the ESX host.

Please choose VE installation mode:

1 (*) Hypervisor*
2 ( ) Network**

* Hypervisor Mode:
Ensure virtual machines security by inspecting all VM traffic. Security Gateway VE seamlessly enforces security within the hypervisor without changing the VM network topology.

** Network Mode:
Secure virtualized environment and perimeter networks by deploying the Security Gateway VE as a virtual network device. Requires explicit routing or bridging network configuration.

To install and configure the Security Gateway Virtual Edition:

1. In the VE Installation window, enter 1 or 2.

2. In the Validation window, press N to continue.
   The selected products are installed.
   If you see the Is this a Dynamically Assigned IP Address installation prompt, enter y or n.
   If you see the Would you like to install a check Point clustering product? prompt, enter y to install a cluster or n to continue without installing a cluster.

3. When Hypervisor Mode is selected, enter the local ESX Host IP address.
Installing and Uninstalling

4. When prompted, enter `y` to confirm the certificate.
5. Enter the local ESX host administrator name and password.
   See Configuring a User for Hypervisor Mode (on page 22) to learn how to configure the ESX user.
   You can use a different user after the installation completes.

```
Enter user name: root
Enter password:
```

- If the user name and password are incorrect, a message shows. Correct and enter again.
- When you install Hypervisor Mode, if a Hypervisor Connector currently exists on the ESX host, a
  warning message shows. We recommend that you enter `y` to replace the Hypervisor Connector.

Completing the Installation

After `sysconfig` completes installing Security Gateway Virtual Edition, complete the configuration.

To complete the installation:
1. You can add a permanent license at this time. By default, Security Gateway Virtual Edition installs with a
   15 day trial license. We recommended that you add a license at a later time using the GUI client. Enter `n` to continue.
2. If prompted, enter `y` to add an administrator for the Security Management Server. Enter the user name
   and password as required.
3. If prompted, add one or more GUI clients. Follow the instructions on the screen.
4. If prompted, enter and confirm a SIC activation code.
5. Optionally, save the Certificate Authority fingerprint.
6. Reboot the Security Gateway Virtual Edition VM.

Note - For Hypervisor Mode deployments only:
- The IPsec VPN Software Blade is not supported in Hypervisor Mode. Do not select this product when you configure the Security Gateway Virtual Edition object in SmartDashboard.
- By default, the Hypervisor Connector is configured with Bypass mode activated until you install a policy.

You can change the configuration settings as necessary at a later time.

Note - You must have SmartDashboard installed on a Windows computer that is defined as a GUI client on the Security Management Server. To get the `<cp_version>` SmartDashboard:

Browse to `https://<IP address of the Virtual Edition Gateway>` > Select **Product Configuration** > **Download SmartConsole**.

Cluster Support

Hypervisor Mode

Hypervisor Mode adds enhanced functionality to VMware clusters. VMware VMotion lets you migrate running VMs from one ESX host in a VMware cluster to the other. Hypervisor Mode gives continuous service availability and full transaction integrity during VM migration. The security policy distributes across all the Security Gateway Virtual Edition members within the cluster. In this mode you must install a Security Gateway Virtual Edition on every ESX cluster member.

Network Mode

Network Mode uses ClusterXL High Availability or Load Sharing to support VMware ESX clusters.

Licensing Security Gateway Virtual Edition

Each Security Gateway Virtual Edition instance requires its own license. You must purchase a license according to the number of physical cores on the local ESX host. Security Gateway Virtual Edition licenses are assigned to IP addresses.

Each Security Gateway and Security Management server installed on a VM must have a license.
Uninstallation

To uninstall Security Gateway Virtual Edition, first remove Hypervisor Connector. Then uninstall this release.

Removing Hypervisor Connector

To remove Hypervisor Connector:
1. On the Security Gateway Virtual Edition use the sysconfig menu to disable the hypervisor connector:
   ```bash
   sysconfig > Hypervisor mode > Operations > Disable Hypervisor Connector policy settings
   ```
2. On the Security Gateway Virtual Edition, run:
   ```bash
   cpv disable_attachment.
   ```
3. On the ESX server:
   a) Remove the Check Point VIB. Run:
      ```bash
      esxcli software vib remove -n cp-esx-cpdvfilter --maintenance-mode
      ```
      To make sure the VIB was removed, run:
      ```bash
      esxcli software vib list
      ```
   b) Make sure `cp-esx-cpdvfilter` is not in the command’s output.
4. Reboot the ESX host.

To make sure the Check Point kernel module is not loaded:

Run:
```bash
esxcfg-module -l
```

# esxcfg-module -l | grep cpdvfilter_kern
```
cpdvfilter_kern Not loaded
```

Uninstalling Security Gateway Virtual Edition

To uninstall Security Gateway Virtual Edition:
1. In the vSphere client, power off the Security Gateway Virtual Edition VM.
2. Delete the Security Gateway Virtual Edition from your inventory.
3. Delete Security Gateways, cluster objects and other network objects in SmartDashboard that were used with Security Gateway Virtual Edition.
Chapter 3

Configuring Hypervisor Mode

In This Chapter
- Configuring a User for Hypervisor Mode
- Configuring a Local ESX Connection
- Enabling or Disabling Clusters
- Configuring Global Options
- Configuring Hypervisor Connector Policy
- Hypervisor Mode Operations
- Configuring the Communication Channel
- Configuring Hypervisor Mode for Routers
- Configuring IP Anti-Spoofing

Configuring a User for Hypervisor Mode

When using Hypervisor Mode, a VMware user is required for authenticating the connection to the ESX host. Use the root user of the ESX host, or configure a dedicated user that has the Assigned Role of Administrator.

To define a user for the Security Gateway Virtual Edition:

1. Log in to the ESX host with the vSphere client.
2. In the Users & Groups tab of the ESX host, right-click in an empty space and select Add.
3. In the Add New User window:
a) Enter the Login name.
b) Optionally enter a user name and UID in the applicable fields.
c) Enter and confirm the user password.
d) Click OK to complete the definition.

4. In the Permissions tab of the ESX host, right-click in an empty space and select Add Permission.
   a) Click Add.
   b) Select the newly defined user from the list and click OK.
   c) Select Administrator from the Assigned Role list.
   d) Click OK to complete the definition.

Configuring a Local ESX Connection

You defined the local ESX connection during installation and initial setup. You can change the IP address, user name, and password for the connection to the local ESX host. Use the same procedure for all deployments.

To reconfigure the connection to the local ESX host:

1. Run sysconfig.
2. Select Hypervisor Mode.
3. From the Hypervisor Mode menu, select Local ESX connection.
4. If the ‘You are about to reset your vSphere connection’ prompt appears, enter y to continue.
5. Enter the local ESX host’s IP address.
6. When prompted to confirm the certificate, enter y. The Local ESX user name and password confirmation window opens.
7. Make sure that the user has the Administrator Role permissions before continuing.
8. Enter the ESX user name and password.
9. If an error occurs, re-enter the information. Otherwise, press any key to continue.
10. Exit sysconfig.

Enabling or Disabling Clusters

You can always activate or deactivate clusters with the cpconfig command line utility.

To activate or deactivate clusters:

1. Log in to the Security Gateway Virtual Edition VM.
2. Run cpconfig.
3. Select Enable [or Disable] cluster membership for this gateway.
4. Exit cpconfig.

Configuring Global Options

The Global Configuration menu lets you configure settings that control global security behavior for the Security Gateway Virtual Edition.

Default Security Settings

The default security settings define the Hypervisor Connector behavior, which applies to virtual objects by default. When you define a new VM, port group, or vSwitch, the global setting applies automatically. You can define explicit security settings to override the default settings for individual VMs, port groups, and vSwitches.
To define the default security settings:
1. Run `sysconfig` and select Hypervisor Mode from the Main menu.
2. Select Hypervisor Connector Policy > Global configuration > Default security.
3. Select one of these options:

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secured</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition, which allows or blocks traffic according to the security policy.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>All traffic is allowed and no inspection occurs.</td>
</tr>
<tr>
<td>Monitored-only</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition. The Hypervisor Connector does not block any traffic. But traffic is still passed to the Security Gateway Virtual Edition, which can block traffic according to the Firewall Security Policy. All events are logged.</td>
</tr>
<tr>
<td>Blocked</td>
<td>All traffic is blocked and no inspection occurs.</td>
</tr>
</tbody>
</table>

In a cluster deployment, these settings apply to all members.

**Global Failure Setting**

The Global Failure setting controls system behavior if the Hypervisor Connector or the Security Gateway Virtual Edition fails.

To define the global failure settings:
1. Run `sysconfig` and select Hypervisor Mode from the Main menu.
2. Select Hypervisor Connector Policy > Global configuration > Global Failure.
3. Select one of these options:

<table>
<thead>
<tr>
<th>Global Failure Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail-Open</td>
<td>If the Hypervisor Connector or the firewall fails, all traffic is allowed and no inspection occurs (the Virtual NIC is &quot;open&quot;).</td>
</tr>
<tr>
<td>Fail-Close</td>
<td>If either the Hypervisor Connector or the firewall fails, all traffic is blocked (the Virtual NIC is &quot;closed&quot;). This is the default option.</td>
</tr>
</tbody>
</table>

In a cluster deployment, these settings apply to all members.

*Note* - The "Fail-Open" and "Fail-Close" terms are conceptually different from similar terms used in IPS protection definitions.

**Cluster Anti-Spoofing**

Cluster anti-spoofing prevents the malicious spoofing of VM IP addresses between cluster members. These settings apply to all members.

If your network uses routers to direct traffic between ESX host members in a cluster, you must deactivate cluster anti-spoofing. This is because the Hypervisor Connector treats the router as a spoofed source IP address and blocks the traffic.

This setting only activates or deactivates anti-spoofing protection between cluster members. To configure anti-spoofing for vNIC IP addresses, see IP address anti-spoofing ("Configuring IP Anti-Spoofing" on page 31).

To activate or deactivate cluster anti-spoofing:
1. Run `sysconfig` and select Hypervisor Mode from the Main menu.
2. Select Hypervisor Connector Policy > Global configuration > Cluster anti-spoofing.
3. Select **Enable** or **Disable**.

**MAC Address Anti-Spoofing**

MAC address anti-spoofing prevents malicious spoofing of Virtual Machine vNIC MAC addresses.

**To Enable or Disable MAC anti-spoofing:**
1. Run `sysconfig` and select **Hypervisor Mode** from the Main menu.
2. Select **Hypervisor Connector Policy > Global configuration > MAC Enforcement**.
3. Select **Enabled** or **Disabled**.

In a cluster deployment, changes to these settings apply to all members.

**Configuring Hypervisor Connector Policy**

The **Local ESX Objects** menu lets you to work with global default settings and settings for individual vSwitches, port groups, and VMs.

**To configure the Hypervisor Connector policy:**
1. Run `sysconfig` and then select **Hypervisor Mode**.
2. Select **Hypervisor Connector Policy**.

The **Hypervisor Connector Policy and Settings** window opens.

<table>
<thead>
<tr>
<th>Hypervisor Connector Policy and Settings ('e' to exit):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Global configuration 3) Port Groups</td>
</tr>
<tr>
<td>2) Virtual Switches 4) Virtual Machines</td>
</tr>
</tbody>
</table>

(Note: configuration changes are automatically saved and applied when you exit the Hypervisor mode menu)

**The Virtual Object Hierarchy**

The Hypervisor Mode applies security settings according to an object hierarchy.
Configuring Hypervisor Mode

List of Callouts

<table>
<thead>
<tr>
<th>Callout</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virtual machine</td>
</tr>
<tr>
<td>2</td>
<td>vNIC</td>
</tr>
<tr>
<td>3</td>
<td>Hypervisor Connector</td>
</tr>
<tr>
<td>4</td>
<td>Port Group</td>
</tr>
<tr>
<td>5</td>
<td>vSwitch</td>
</tr>
</tbody>
</table>

The highest level is the virtual machine. Each VM contains one or more vNICs to connect to the internal networks and the Internet.

Understanding Security Setting Precedence

The Hypervisor Connector assigns the first applicable security setting to vNIC traffic according to the object hierarchy:

1. The security setting explicitly defined for a Virtual Machine.
2. The security setting explicitly defined for a port group.
3. The security setting explicitly defined for a vSwitch.
4. If a security setting is not explicitly defined for the vNIC, the default security setting applies ("Default Security Settings" on page 23).

Configuring vSwitches

To configure security for vSwitches:

1. In the Hypervisor Connector Policy and Settings window, select Virtual Switches.
2. Select a Virtual Switch from the list and follow the instructions on the screen.

<table>
<thead>
<tr>
<th>Virtual switch</th>
<th>Current Security state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) vSwitch0</td>
<td>Default (Secured)</td>
</tr>
<tr>
<td>2) vSwitch1</td>
<td>Default (Secured)</td>
</tr>
<tr>
<td>3) vSwitch2</td>
<td>Default (Secured) *</td>
</tr>
</tbody>
</table>

* One or more related virtual objects have explicitly defined settings and will not inherit the global setting

(Nota: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

Your choice:

⚠️ Important - An asterisk to the right of a VSwitch indicates that one or more Port Groups or VMs connected to this vSwitch have explicitly defined security settings and will not inherit the vSwitch security setting.

3. Select one of these options:
   - Change security definition: Change the security setting for the selected item.
   - Reset Security to default: Reset the selected item to the default security setting.
Virtual switch name: vSwitch0

Choose item to configure ('e' to exit):
------------------------------------------------------------------
1) Change security definition
2) Reset Security to default
------------------------------------------------------------------
(Note: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

Your choice:

4. If you selected the Change security definition option, select one of these security options:

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secured</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition, which allows or blocks traffic according to the security policy.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>All traffic is allowed and no inspection occurs.</td>
</tr>
<tr>
<td>Monitored-only</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition. The Hypervisor Connector does not block any traffic. But traffic is still passed to the Security Gateway Virtual Edition, which can block traffic according to the Firewall Security Policy. All events are logged.</td>
</tr>
<tr>
<td>Blocked</td>
<td>All traffic is blocked and no inspection occurs.</td>
</tr>
</tbody>
</table>

**Configuring Port Groups**

To configure port groups:

1. In the Hypervisor Connector Policy and Settings window, select Port Groups.
2. Select a port group from the list and follow the instructions on the screen.

    Port group settings are synchronized with all cluster members.
    Choose a port group to configure ('e' to exit):
    ------------------------------------------------------------------
    | Port group      | Current Security state |
    |-----------------|------------------------|
    | VM Network      | Default (Secured) *    |
    | Service Console | Default (Secured)      |
    | VMkernel        | Default (Secured)      |
    | sync            | Default (Secured)      |
    | LAN_10.0.0.0    | Default (Secured)      |
    ------------------------------------------------------------------
    * One or more related virtual objects have explicitly defined settings and will not inherit the global setting

    (Note: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

    Your choice:

    **Important** - An asterisk to the right of a port group indicates that one or more vSwitches or VMs connected to this port group have explicitly defined security settings and the VM will not inherit the port group security setting.

3. Select one of these options:
   - **Change security definition**: Change the security setting for the selected item.
   - **Reset Security to default**: Reset the selected item to the default security setting.
Port group name: VM Network

Choose item to configure ('e' to exit):

1) Change security definition
2) Reset Security to default

(Note: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

Your choice:

4.

If you selected the **Change security definition** option, select one of these security options:

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secured</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition, which allows or blocks traffic according to the security policy.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>All traffic is allowed and no inspection occurs.</td>
</tr>
<tr>
<td>Monitored-only</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition. The Hypervisor Connector does not block any traffic. But traffic is still passed to the Security Gateway Virtual Edition, which can block traffic according to the Firewall Security Policy. All events are logged.</td>
</tr>
<tr>
<td>Blocked</td>
<td>All traffic is blocked and no inspection occurs.</td>
</tr>
</tbody>
</table>

In a cluster deployment, these settings apply to all members.

### Configuring Virtual Machines

**To configure virtual machines:**

1. In the **Hypervisor Connector Policy and Settings** window, select **Virtual Machine**.
2. Select a VM from the list and follow the instructions on the screen.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Current Security state</th>
</tr>
</thead>
<tbody>
<tr>
<td>ubuntu-server-05</td>
<td>Default (Secured) *</td>
</tr>
<tr>
<td>windows-xp-01</td>
<td>Default (Secured) *</td>
</tr>
<tr>
<td>ubuntu-server-01</td>
<td>Default (Secured)</td>
</tr>
<tr>
<td>ubuntu-server-02</td>
<td>Default (Secured)</td>
</tr>
</tbody>
</table>

* One or more related virtual objects have explicitly defined settings and will not inherit the global setting

(Note: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

Your choice:

**Important** - An asterisk to the right of a VM indicates that one or more Port Groups or vSwitches associated with this VM have explicitly defined security settings and some of the vNICs of this VM will not inherit the default security.

3. Select one of these options:
   - **Change security definition**: Change the security setting for the selected item.
   - **Reset Security to default**: Reset the selected item to the default security setting.
VM name: windows-xp-01

Choose item to configure ('e' to exit):

1) Change security definition
2) Reset Security to default

(Note: configuration changes are automatically saved and applied when you exit the Security Gateway Virtual Edition menu)

Your choice:

4. If you selected the **Change security definition** option, select one of these security options:

<table>
<thead>
<tr>
<th>Security Option</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secured</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition, which allows or blocks traffic according to the security policy.</td>
</tr>
<tr>
<td>Bypassed</td>
<td>All traffic is allowed and no inspection occurs.</td>
</tr>
<tr>
<td>Monitored-only</td>
<td>All traffic is inspected by the Hypervisor Connector and Security Gateway Virtual Edition. The Hypervisor Connector does not block any traffic. But traffic is still passed to the Security Gateway Virtual Edition, which can block traffic according to the Firewall Security Policy. All events are logged.</td>
</tr>
<tr>
<td>Blocked</td>
<td>All traffic is blocked and no inspection occurs.</td>
</tr>
</tbody>
</table>

In a cluster deployment, these settings apply to all members.

**Hypervisor Mode Operations**

The **Operations** menu lets you manage Hypervisor Mode operations. To open the **Operations** menu, run `sysconfig` and from the **Main** menu, select **Hypervisor Mode > Operations**.

Select options from the menu by number.

1. **Apply configuration to this local Gateway**
   - Apply configuration settings made during the current `sysconfig` session without exiting the **Hypervisor Mode** menu. This is applicable to the local Security Gateway Virtual Edition.

2. **Apply configuration to all cluster members**
   - Apply configuration settings made during the current `sysconfig` session to all cluster members without exiting the **Hypervisor Mode** menu. Normally, configuration settings are automatically applied when you exit the **Hypervisor Mode** menu.

3. **Reset Hypervisor Connector to default policy**
   - Resets all VMs, port groups, and vSwitches to the default security settings. This action applies to all cluster members.

4. **Reset entire settings and policy to default**
   - Resets all global default settings to their original settings (after installation). This also resets all VMs, port groups, and vSwitches to these default settings. This action applies to all cluster members.

5. **Logging configuration**
   - Lets you control the events recorded in the Check Point logs.
     - **Security Gateway Virtual Edition Logs**: Include Hypervisor Mode logs in SmartView Tracker (On/Off)
     - **vSphere Events Logs**: Include VMware ESX events logs in SmartView Tracker (On/Off)
     - **Configuration Logs**: Include Hypervisor Mode configuration changes logs in SmartView Tracker (On/Off)

6. **Re-install Hypervisor Connector**
• Lets you re-install the Hypervisor Connector kernel module on this ESX host. Follow the instructions on the screen.
• If the Hypervisor connector is already installed on this ESX host, before selecting this option you must uninstall the hypervisor connector.
• To complete the procedure, reboot the ESX host.

7. Enable/Disable Hypervisor Connector policy settings
Activates or deactivates Hypervisor Mode protection.
• When disabled, all traffic goes through the Hypervisor Connector without inspection. This mode is useful when debugging network connectivity issues.
• When enabled, traffic is inspected and security settings are applied according to the policy.
• This option only applies to the currently selected ESX host.

Configuring the Communication Channel

Security Gateway Virtual Edition communicates with the Hypervisor Connector using a dedicated communication channel. This traffic goes through the Security Gateway Virtual Edition VM bridge interface (typically br0). The Hypervisor Mode installation procedure automatically assigns these default IP addresses for the bridge interface and the Hypervisor Connector:

| Bridge interface: 192.168.28.10 |
| Hypervisor Connector: 192.168.28.11 |

These addresses have no effect on any IP segments on your ESX host. However, you cannot use the communication channel IP addresses on your VMs. This can cause an IP collision.

You can change the communication channel IP addresses to any two addresses on the same class C subnet.

To change the communication channel IP addresses:
1. Log in to the Security Gateway Virtual Edition VM.
2. Run:
   ckp_regedit -a SOFTWARE\CheckPoint\FW1\6.0\reserved\CPVIRT\Comm
   fw_ip -s <new IP address for Bridge interface>.
3. Run:
   ckp_regedit -a SOFTWARE\CheckPoint\FW1\6.0\reserved\CPVIRT\Comm
   filter_ip -s <new IP address for Hypervisor Connector>.
4. Run:
   cpv comm_reset.

These settings are not synchronized between cluster members. You must manually configure the IP addresses for the communication channel on each member.

Configuring Hypervisor Mode for Routers

If you have physical or virtual routers for traffic between VMs, you must follow these configuration steps to secure more than one virtual network.

To configure Hypervisor Mode to work with physical or virtual routers:
1. On each cluster member, configure the MTU of the sync interface to 9000:
   a) Run: sysconfig > Network Connections > Configure connection
   b) Select sync interface
   c) Select: Change MTU settings
   d) Enter: 9000
2. For each cluster member:
   a) Edit $FWDIR/modules/fwkern.conf to include:
   fwha_vmotion_use_packet_encapsulation=1
b) Restart the cluster member.

3. On each ESX host configure the vSwitch (that has the VE sync interface connected to it) MTU value to 9000.
   a) Run `esxcfg-vswitch -l` (on the ESX host).
   b) Find the vswitch that has the sync interface connected to it.
   c) Change the MTU value of the vSwitch to 9000:
      ```bash
      esxcfg-vswitch -m 9000 vSwitch1
      ```
      (in this example the correct vswitch is vSwitch1).
   d) Verify the change: `esxcfg-vswitch -l`

4. If virtual routers are used to route the traffic, run `sysconfig` to configure their security setting to bypassed.

Configuring IP Anti-Spoofing

In this section:

- IP Anti-Spoofing Overview
- Creating Virtual Machine Host Objects
- Creating Port Group Objects
- Creating vSwitch Objects

IP Anti-Spoofing Overview

Security Gateway Virtual Edition Hypervisor Mode enforces IP Anti-Spoofing for vNICs on an ESX host. Protection setting granularity lets you define IP Anti-Spoofing protection for individual vSwitches, port groups, VMs and individual vNICs.


Hypervisor Mode makes sure that packets with a VM source IP address actually come from a vNIC connected to that VM.

Hypervisor Mode enforces IP Anti-Spoofing for each vNIC according to a hierarchy of objects connected to the vNIC:

1. **Virtual Machine**: The Hypervisor Connector enforces IP Anti-Spoofing as defined for the VM object.
2. **Port Group**: If IP Anti-Spoofing is not defined for the VM object, the Hypervisor Connector enforces IP Anti-Spoofing as defined for the port group object.
3. **vSwitch**: If IP Anti-Spoofing is not defined for the VM or port group object, the Hypervisor Connector enforces IP Anti-Spoofing as defined for the vSwitch object.
4. If IP Anti-Spoofing is not defined for any VM, port group, or vSwitch objects, the Hypervisor Connector does not enforce IP Anti-Spoofing for the vNIC. However, packets going through an unprotected vNIC cannot spoof IP addresses for other protected vNICs.

**Note** - IP Anti-Spoofing in Security Gateway Virtual Edition in Hypervisor Mode is configured in SmartDashboard. SmartDashboard does not recognize some special characters in objects, such as the space character. If an object name in the vSphere Client contains characters not recognized by SmartDashboard, replace them with three underscore ('___') characters.

For example, if a VM is named 'My VM' in vSphere, define the name as 'vmware_vm_MY___VM' (non-cluster) in SmartDashboard.
Creating Virtual Machine Host Objects

SmartDashboard uses a host object with a unique name to manage VMs. This host object name must agree with the specified naming convention. If the name is not unique, or does not agree with the correct naming convention, IP anti-spoofing might not be enforced.

To define a VM network object:

2. In the Network Objects tree, right-click Nodes and then select Node > Host.
3. In the Host Node window, enter a unique name that agrees with one of these naming conventions:
   - For VMs in a cluster: `vmware_<cluster name>_vm_<VM name>`
   - For non-cluster VMs: `vmware_vm_<VM name>`
   - `<cluster name>`: Cluster name as defined in SmartDashboard
   - `<VM name>`: VM name as defined in the vSphere Client
4. In the Host Node window, enter the IP address for one of the vNICs used by this VM.
5. In the Topology window, click Add to define each vNIC.
   a) In the Interface Properties window, enter a vNIC name.
      - If you enter the name of a vNIC as defined in the vSphere client (Network adapter x), the policy is enforced for that vNIC only.
      - Alternatively, you can enter any name in this field. This will enforce the policy for all vNICs connected to this VM.
   b) Enter the IP address and net mask in the appropriate fields.
6. Install the policy.
Virtual Machine Naming Examples

- For a Check Point cluster object named **MyCluster** that protects a VM named **MyVM**, the name will be: `vmware_MyCluster_vm_MyVM`
- For a non-cluster environment that protects a VM entitled **MyVM**, the name will be: `vmware_vm_MyVM`

IP Anti-Spoofing Mapping

The Anti-Spoofing mapping table shows the current relationship between VMs and their related IP Anti-Spoofing objects in SmartDashboard.

When configuring IP Anti-Spoofing for a VM, you assign a name using a special naming convention that includes the VM name. After installing a policy, you can change the VM name without losing its IP Anti-Spoofing protection. This is because Hypervisor Mode uses the VM UUID for identification after installing the policy.

To see the object mapping table:
1. Run `sysconfig`.
2. Select Hypervisor Mode.
3. Select Anti-spoofing mapping from the Hypervisor Mode menu.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Smart Center Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) MyWebServer</td>
<td><code>vmware_MyCluster_vm_MyWebServer</code></td>
</tr>
<tr>
<td>2) MyEmailServer</td>
<td><code>vmware_MyCluster_vm_MyEmailServer</code></td>
</tr>
<tr>
<td>3) MyDatabase</td>
<td><code>vmware_MyCluster_vm_MyDatabase</code></td>
</tr>
<tr>
<td>4) NewVM_Name</td>
<td><code>vmware_MyCluster_vm_MyFTPServer</code></td>
</tr>
</tbody>
</table>

Select a VM to see more details or "e" to exit

Your choice

**Note:** The last VM name on the list is different from the SmartDashboard object name. This is because the VM name changed after the policy was installed.

Creating Port Group Objects

You enable IP anti-spoofing for port groups by creating either a new network or address range object in SmartDashboard with a unique name that conforms to a specific naming convention. If the name that you choose is not unique, or does not conform to the correct naming convention, IP anti-spoofing may not be enforced.

To enforce IP anti-spoofing for an entire specific network connected to a port group, define a network object. To enforce a specific range of IP addresses, define an address range object.

Port Groups as Address Range Objects

To create an address range object:
2. Right-click **Network Objects**, and select **New > Others > Address Ranges > Address Range**.
3. In the **Address Range Properties** window, enter a unique name conforming to these naming conventions:

   ![Address Range Properties](image)

   - For a **Cluster Port Group**: `vmware_<cluster name>_pg_<port group name>`
   - For a **non-cluster Port Group**: `vmware_pg_<port group name>`

   - `<cluster name>`: Cluster name as defined in SmartDashboard
   - `<port group name>`: Port group name as defined in the vSphere Client

4. Enter the first and last IP address for the range in the designated fields.
5. Click OK.
6. Install the policy.

**Port Group Naming Examples**

- For a Check Point cluster object named **MyCluster** that protects a port group named **MyPortGroup**, the name will be:
  
  `vmware_MyCluster_pg_MyPortGroup`

- For a port group entitled **MyPortGroup** in a non-cluster environment the name will be:
  
  `vmware_pg_MyPortGroup`

**Port Groups as Network Objects**

2. In the **Network Objects** tree, right-click **Networks > Network**.
3. In the **Network Properties** window, enter a unique name conforming to the below naming convention:

   ![Network Properties](image)

   - For a **cluster Port Group**: `vmware_<cluster name>_pg_<port group name>`
For non-cluster Port Group: `vmware_pg_<port group name>`
- `<cluster name>`: Cluster name as defined in SmartDashboard
- `<port group name>`: Port group name as defined in the vSphere Client

4. Enter the network IP address and net mask in the designated fields.
5. Click OK.
6. Install the policy.

**Port Group Naming Examples**

- For a Check Point cluster object named *MyCluster* that protects a port group named *MyPortGroup*, the name will be:
  
  `vmware_MyCluster_pg_MyPortGroup`

- For a port group entitled *MyPortGroup* in a non-cluster environment the name will be:
  
  `vmware_pg_MyPortGroup`

**Creating vSwitch Objects**

You enable IP anti-spoofing for vSwitches by creating either a new network or address range object in SmartDashboard with a unique name that conforms to a specific naming convention. If the name that you choose is not unique, or does not conform to the correct naming convention, IP anti-spoofing may not be enforced.

If you want to enforce IP anti-spoofing for an entire specific network connected to a vSwitch, define a network object. If you want to enforce IP anti-spoofing for a specific range of IP addresses, define an address range object.

**vSwitches as Address Range Objects**

⚠️ **Important** - When entering the name for an ESX host that uses a domain name format such as ‘MyHost@checkpoint.com’, you must substitute a ‘.’ (period) for the ‘@’ symbol.

**To create an address range object:**

2. Right-click **Network Objects**, and select **New > Address Ranges > Address Range**.
3. In the **Address Range Properties** window, enter a unique name conforming to the below naming convention:

![Address Range Properties](image)
For a Cluster vSwitch: `vmware_<cluster name>_<ESX host>_vs_<vSwitch name>

For non-cluster vSwitch: `vmware_<ESX host>_vs_<vSwitch name>

- `<cluster name>`: Cluster name as defined in SmartDashboard
- `<ESX host>`: ESX host name as defined in the vSphere Client
- `<vSwitch name>`: vSwitch name as defined in the vSphere Client

4. Enter the first and last IP address for the range in the designated fields.
5. Click OK.
6. Install the policy.

**vSwitch Naming Examples**

- For a Check Point cluster object named **MyCluster** that protects a vSwitch named **MyvSwitch**, and located on an ESX host named **MyHost** the name will be:
  `vmware_MyCluster_MyHost_vs_MyvSwitch`

- For a vSwitch entitled **MyvSwitch** that is located on an ESX host named **MyHost@checkpoint.com**, the name will be:
  `vmware_MyHost.checkpoint.com_vs_MyvSwitch`

**vSwitches as Network Objects**

To create a network object:
2. In the **Network Objects** tree, right-click **Networks** and select **Network**.
3. In the **Network Properties** window, enter a unique name conforming to the below naming convention:

   For a Cluster vSwitch: `vmware_<cluster name>_<ESX host>_vs_<vSwitch name>`

   For non-cluster vSwitch: `vmware_<ESX host>_vs_<vSwitch name>`

   - `<cluster name>`: Cluster name as defined in SmartDashboard
   - `<ESX host>`: ESX host name as defined in the vSphere Client
   - `<vSwitch name>`: vSwitch name as defined in the vSphere Client

4. Enter the network IP address and net mask in the designated fields.
5. Click OK.
6. Install the policy.
vSwitch Naming Examples

- For a Check Point cluster object named MyCluster that protects a vSwitch named MyvSwitch, and located on an ESX host named MyHost the name will be:
  vmware_MyCluster_MyHost_vs_MyvSwitch

- For a vSwitch entitled MyvSwitch that is located on an ESX host named MyHost@checkpoint.com, the name will be:
  vmware_MyHost.checkpoint.com_vs_MyvSwitch
Chapter 4

Clusters

In This Chapter

<table>
<thead>
<tr>
<th>Cluster Overview</th>
<th>38</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor Mode</td>
<td>38</td>
</tr>
<tr>
<td>Network Mode</td>
<td>41</td>
</tr>
</tbody>
</table>

Cluster Overview

ESX cluster support and behavior is different for each Security Gateway Virtual Edition mode.

- **Hypervisor Mode** - Hypervisor Mode adds enhanced functionality to VMware clusters. VMware VMotion lets you migrate running VMs from one ESX host in a VMware cluster to the other. Hypervisor Mode gives continuous service availability and full transaction integrity during VM migration. On Install Policy, all Security Gateway Virtual Edition cluster members get the updated policy. In this mode, you must install a Security Gateway Virtual Edition on every ESX cluster member.

  The challenge is to continue protection and service availability for open connections during and after migration. Hypervisor Mode resolves this challenge by synchronizing connection information between cluster members during and after migration. This ensures that packets for an open connection are sent automatically to the ESX host that originally hosted the Security Gateway Virtual Edition VM. Therefore, security enforcement continues.

- **Network Mode** - Network Mode uses ClusterXL High Availability or Load Sharing to support VMware ESX clusters.

Hypervisor Mode

Security Gateway Virtual Edition in Hypervisor Mode with VMware cluster solutions has these limitations:

- You cannot use ClusterXL High Availability or Load Sharing with Hypervisor Mode.
- You must install Security Gateway Virtual Edition on each member. If Security Gateway Virtual Edition is not installed on a member, that member will operate without security enforcement.
- You cannot install more than one Security Gateway Virtual Edition VM on a cluster member.

Cluster configuration includes these procedures:

- Installing Security Gateway Virtual Edition with Hypervisor Mode on each cluster member.
- Connecting the synchronization NICs.
- Configuring the cluster using SmartDashboard and cpconfig.

Defining a Cluster

To configure a cluster:

1. Install and configure ("Configuring Hypervisor Mode" on page 22) a Security Gateway Virtual Edition VM with Hypervisor Mode on each cluster member. Make sure that you enter **yes** when prompted to install the Check Point clustering product during the installation.

   **Important** - You must install Hypervisor Mode on all ESX cluster members to enforce security during vMotion migration.

2. Run cpconfig. Make sure that cluster support is activated.
3. Make sure that there is connectivity between the cluster members and the Security Management Server. Resolve connectivity issues before continuing.

4. Open SmartDashboard.

5. Select **Policy > Global Properties**.
   a) Select **SmartDashboard Customization** from the tree.
   b) Click **Configure**.
   c) In the **Advanced Configuration** window, select **FireWall-1 > General**.
   d) Activate the `cxl_is_bridge` option and then click **OK** twice.

   a) Right-click **Check Point** in the **Network Objects** tree.
   b) Select **Security Cluster**.
   c) Select the **Classic mode** option.

7. In the **General Properties** window:
   a) Enter a cluster name and the cluster IP address. We recommend that you assign an IP address in the same subnet as the members.
   b) In the **Network Security** section, deactivate the **ClusterXL** and the **IPSec VPN** blades. Make sure that neither of these blades appear in the **Cluster Properties** tree.
   c) Configure other options as required for your deployment.

8. On the **Cluster Members** page, define each Security Gateway Virtual Edition VM as a cluster member.
a) Click Add.

b) In the Cluster Member Properties window, enter a name and IP address.

c) Click Communication and enter the SIC internal communication password.

d) Configure other member properties as required for your deployment.

9. In the 3rd Party Configuration window, make sure that the Hide Cluster Members outgoing traffic behind Clusters IP address option is not activated.


11. On the Edit Topology page, click Get Topology for each member. Make sure that you configure the sync interface.
12. Install the policy.

## Network Mode

Network Mode uses ClusterXL High Availability and Load Sharing to support VMware ESX clusters. This section summarizes the procedures for defining a ClusterXL cluster with Security Gateways and a Security Management Server on VMs.

You can define a cluster, consisting of two or more members, each on the same or different ESX host. This makes sure that automatic failover occurs if an ESX host or a cluster member is unavailable. Load sharing lets you divide the traffic load amongst ESX hosts.

VMware High Availability and other VMware clustering solutions do not operate with state synchronization for Security Gateway clusters. You can, however, use VMware High Availability or other failover solutions for VMs.

### Defining a ClusterXL Cluster

**To define a ClusterXL cluster:**

1. Install and configure two or more Security Gateway Virtual Edition VMs.
2. Power on the VMs.
3. Run `cpconfig` on each member. Make sure that cluster support is active.
4. Make sure that there is connectivity between the cluster members and the Security Management Server. Resolve connectivity issues before continuing.
5. Make sure that there is connectivity between the cluster members and your internal networks, external networks, and other VMs. Resolve connectivity issues before continuing.
7. Define and install security policies.
Chapter 5

Working with R75.40 Software Blades

In This Chapter

- Configuring Security Policies Using VM Objects
- Configuring Identity Awareness in Hypervisor Mode
- Configuring DLP in Hypervisor Mode

This section covers how to configure the Identity Awareness and the DLP Software Blades to work in Hypervisor Mode.

Configuring Security Policies Using VM Objects

You can configure a security policy using VM objects, rather than using IP addresses. Enable the Identity Awareness Software Blade. You can use access role objects that represent VMs, or a group of VMs, and use these objects in the rulebase.

**Scenario 1: Using VM in the Rulebase**

A sensitive server that holds financial data requires a security policy with strict access. Add the server to the AD and create an access role. This role has the identity of the finance server. Use the access role in rules that Allow only the finance department to access this server.

**Scenario 2: Using Dynamic Groups in Rulebase**

An organization with many web servers (and new ones are created and deployed daily) requires special policy rules that apply to all the web servers. Create an access role object for an AD group with all web servers. When you create a new web server, add it to the AD group. The firewall rules that match the access role of the web server AD group, apply automatically on the new web server. You do not have to change the firewall or to install an updated policy.

Configuring Identity Awareness in Hypervisor Mode

**Note** - In Network mode, use the R75.40 Identity Awareness Administration Guide.

Use these procedures to add an AD server manually to the management server and to configure Identity Awareness.

To add an AD server to the management server:

1. Create a new LDAP Account Unit.
2. In the LDAP Account Unit Properties window:
   - **Profile** - Select **Microsoft_AD**.
   - **Domain** - Enter the AD Domain name.
   - Select **Active Directory Query**.
3. Open the **Servers** tab.
4. Add the AD server with the administrator login information.

5. Open the **Object Management** tab.
6. Click **Fetch branches**.
7. Double-click the branch. From the LDAP branch Definition window, copy the **Branch Path**.
8. Open the LDAP Server Properties window again.
9. In **Login DN**, enter: `cn=administrator,cn=users`, and then paste the Branch Path to complete the DN.
To configure Identity Awareness:
1. Open the properties window of the Security Gateway, and enable the Identity Awareness Software Blade.
2. In the Identity Awareness Configuration window, select **AD Query** and then click **Cancel**.
3. In the Security Gateway properties window, open **Identity Awareness**.
4. Select **Active Directory Query** and click **Settings**.
5. In the Active Directory Query, enter the domain name that you used in the LDAP Account Unit Properties window.
6. Click **OK** and install the policy.

**Configuring DLP in Hypervisor Mode**

These steps assume you are familiar with the DLP Software Blade. To learn more, see the *R75.20 Data Loss Prevention Administration Guide*.

**To configure DLP to work in Hypervisor Mode:**

1. In SmartDashboard, open the **General Properties** of the Gateway or Cluster object, and enable the **Data Loss Prevention** Software Blade.
2. Complete the Data Loss Prevention wizard.
   - If you do not have a cluster, install the policy and you are done.
   - If you have a cluster installed:
     (i) Save the database (File > Save)
     (ii) Close SmartDashboard
     (iii) Continue to step 3
3. Open **GuiDBEdit**.
5. In **Network Objects**, select **network_object**.
6. Click the cluster object.
7. Search for `CP_high_availability` and change its value to `false`.
8. Save your changes.
9. Close **GuiDBEdit**.
10. Open SmartDashboard and install the policy.
Chapter 6

Troubleshooting

In This Chapter

Hypervisor Mode Troubleshooting 47
General Troubleshooting 52

Hypervisor Mode Troubleshooting

Hypervisor Connector Installation Issues

If an error message appears during the Hypervisor Connector installation:
1. Log in to the local ESX host
2. Run: esxcli software vib list

   If you installed the Hypervisor Connector correctly, you will see output similar to this:

   ~# esxcli software vib list
   Name              Version        Vendor     Acceptance Level Install Date
   ----------------- ------------- -------- --------------- --------------
   cp-esx-cpdvfilter 5.75-976000014 CheckPoint VMwareAccepted 2012-09-04

3. If the Hypervisor Connector package did not successfully install:
   a) Log in to the Security Gateway Virtual Edition VM.
   b) Run sysconfig.
   c) Select Hypervisor Mode > Operations > Re-install Hypervisor Connector.
   d) Follow the on-screen instructions.

4. If the Hypervisor Connector installed successfully on the ESX host, make sure that the Hypervisor Connector kernel is loaded:
   a) Log in to the local ESX host.
   b) Run: vmkload_mod -l | grep cpdvfilter_kern

   ~# vmkload_mod -l | grep cpdvfilter_kern
   cpdvfilter_kern 0 716

5. To manually load the Hypervisor Connector kernel on the ESX Host:
   a) Log in to the local ESX host.
   b) Run: esxcfg-module cpdvfilter_kern

Security Gateway Virtual Edition Does not Inspect Traffic

If the Security Gateway Virtual Edition does not inspect ESX Server traffic:
2. Run sysconfig and confirm that all global and local settings (VMs, port groups, and vSwitches) are properly configured.
3. Run fw pstat on the ESX host.
Global configuration:
- Bypass mode: OFF
- Detect mode: OFF
- Mac anti spoofing: ON
- IP anti spoofing: ON
- Router configured: YES
- Assertions: OFF

Memory:
- Min Heap size: 4 Mb (4194304 Bytes)
- Max Heap size: 16 Mb (16777216 Bytes)
- Memory consumption: 48 Kb (49738 Bytes)
- Max memory consumption: 50 Kb (51612 Bytes)
- Allocations: 413512
- Frees: 413444
- Failed allocations: 0
- Current allocations: 68

Communication Channel:
- Communicating: YES
- Comm state: VIRT_COMM_STATE_INIT
- FW MAC: 00:0c:29:d1:9d:60
- FW IP: 192.168.1.1
- FW port: 37691
- My MAC: 00:0c:29:aa:a7:d8
- My IP: 192.168.1.2
- My port: 1234
- Messages received: 200519
- Bytes received: 4195568
- Messages sent: 200519
- Bytes sent: 4010380
- Comm breakdowns: 0
- Breakdown time: 4 Hr. 21 Min. 20 Sec.

Vmotion:
- Sync MAC address is not available

Filters:
- #Filters: 5
- #Machines: 2

a) Make sure that the Bypass Mode is set to OFF. If this is not the case:
   - (i) Make sure that you have installed a policy on the Security Gateway Virtual Edition.
   - (ii) Run sysconfig.
   - (iii) Select Hypervisor Mode and then select Operations. If the Enable hypervisor option shows, choose this option.

b) In the Communication Channel section, make sure that Communicating is set to YES. If not, do the procedure explained in Resolving Communication Channel Issues (on page 50).

4. Make sure that the bridge interface is available ("Security Gateway Virtual Edition Not Connected to _cp_private Port Group" on page 48) on the Security Gateway Virtual Edition VM and that it is configured correctly.

Security Gateway Virtual Edition Not Connected to _cp_private Port Group

Inspected traffic goes through the _cp_private port group. This port group is configured and controlled automatically using the local ESX connection. If you experience connectivity issues, make sure that the Security Gateway Virtual Edition is correctly configured to reach the ESX Service Console/ESXi Host Management Network.
To verify that Security Gateway Virtual Edition is connected to _cp_private port group:

1. Make sure that there is a bridge interface defined on the Security Gateway Virtual Edition VM.
   a) Run `ifconfig` on the Security Gateway Virtual Edition VM.
   b) Make sure a bridge interface (typically br0) shows in the list.

   ```
   [ava]# ifconfig
   br0   Link encap:Ethernet  HWaddr 00:50:56:94:13:C4
       UP  BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:602131 errors:0 dropped:0 overruns:0 frame:0
       TX packets:604350 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:28906908 (27.5 Mb)  TX bytes:42138542 (40.1 Mb)
   ```

2. Make sure that the bridge interface connects to the _cp_private port group.
   a) In the vSphere client, right-click the Security Gateway Virtual Edition VM.
   b) Select Edit Settings.
   c) In the Virtual Machine Properties window, make sure that one (and only one) network adapter is mapped to _cp_private.
      Verify that the MAC address assigned to this network adapter is the one assigned to the bridge interface.

   ! Important - Do not manually configure the bridge interface or change its settings. Security Gateway Virtual Edition configures it automatically.

If the Security Gateway Virtual Edition is not connected to the _cp_private port group, or the bridge interface is not defined:

1. Make sure that you have an available vNIC with no IP address assigned to it.
   If there is no available vNIC, add one in the vSphere client.
2. Ping the local ESX host from the Security Gateway Virtual Edition to verify connectivity.
3. Run `sysconfig` and make sure that the local ESX connection settings are correct.

**Verifying CPVIRTD**

The `cpvird` process needs connectivity between the Security Gateway Virtual Edition VM and the local ESX host. If it is not running, there will be connectivity issues between the VMs.
To verify CPVIRTD:
1. Log in to the Security Gateway Virtual Edition VM.
2. Run: cpwd_admin list
3. Make sure that the cpvird process is running.

<table>
<thead>
<tr>
<th>APP</th>
<th>PID</th>
<th>STAT</th>
<th>#START</th>
<th>START_TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPVIRTD</td>
<td>0</td>
<td>T</td>
<td>1</td>
<td>[14:36:56]</td>
<td>29/4/2010 cpvird</td>
</tr>
</tbody>
</table>

   In the STAT column, T indicates Terminated (not running) and E indicates Executing.
4. Ping the ESX Host from the Security Gateway Virtual Edition VM.
5. Run sysconfig.
6. Select Hypervisor Mode > Local ESX connections to make sure that the local ESX Connections are configured correctly.
7. Run cpstop and then cpstart.

Resolving Communication Channel Issues
To make sure that the communication channel is working:
1. On the Security Gateway Virtual Edition VM, run: cpv comm_is_up

   cpv comm_is_up
   UP

   Make sure that the command output is UP.
2. On the local ESX host, run: fw pstat

   fw pstat
   Communication Channel:
   Communicating: YES

   Make sure that the Communicating parameter in the Communication Channel section is YES.

If one or both of these conditions are false:
1. Make sure that CPVIRTD is running.

Resolving Connectivity Issues
To resolve connectivity issues:
2. Run sysconfig and make sure that you configured the global and local settings (VMs, port groups, and vSwitches) correctly.
3. Make sure that the communication channel is working ("Resolving Communication Channel Issues" on page 50).
4. Run fw pstat -f on the ESX host to show statistics for the relevant vNIC.
a) Identify the relevant vNIC by the VM UUID and the vNIC MAC address. To find the UUID, open the .vmx file, located in its datastore directory. Search for vc.uuid (UUID shown in the fw pstat output).

Alternatively, you can run cpv uuids on the Security Gateway Virtual Edition VM to query for the UUIDs of VMs running on the local ESX host.

b) The Security behavior line shows the security setting enforced on this vNIC.

- VIRTK_SEC_ENFORCE - The vNIC is secured as defined in the sysconfig policy.
- VIRTK_SEC_BLOCK - The vNIC is blocked for traffic as defined in the sysconfig policy.
- VIRTK_SEC_UNINITIALIZED - The Security Gateway Virtual Edition VM is not communicating with the ESX host. Make sure that there is properly configured bridge interface (“Security Gateway Virtual Edition Not Connected to _cp_private Port Group” on page 48) and that the local ESX connections are operating properly.

5. Read the log files using SmartView Tracker for dropped packets and other issues.

No ESX Objects in sysconfig

If no VMs, port groups, or vSwitches show in the sysconfig Hypervisor Connector Policy section, the cpvirtd process is not running, or not communicating with the local ESX host.

To find the cause:
1. Make sure that the cpvirtd process is running on Security Gateway Virtual Edition.
2. Make sure that Security Gateway Virtual Edition can connect to the IP address of the ESX Service Console/ESXi Host Management.
3. Make sure that you correctly configured the local ESX connection settings.

Connectivity Issues After Uninstalling Security Gateway Virtual Edition

If you experience connectivity issues after uninstalling Security Gateway Virtual Edition, one or more virtual machine vNICs may not have been reset to the failOpen state.

To reset the state of problematic vNICs on VMs:
1. Power off the VM.
2. In the vSphere client, open the Virtual Machine Properties window.
3. On the Options tab, select Advanced > General.
4. Click Configuration Parameters.
5. In the Configuration Parameters window:
   a) Find each ethernet<X>.filter14.onFailure (X=the Ethernet index 0-9) attribute.
   b) If its value is failClosed, change it to failOpen.
6. Repeat steps 1-5 for each problematic VM.
7. On the ESX host, make sure the Hypervisor Connector is not installed:
   a) Log in to the local ESX host and run: esxcli software vib list
b) If `cp-esx-cpdvfilter` shows in the output, remove it by running:

```
esxcli software vib remove -n cp-esx-cpdvfilter --maintenance-mode
```

8. Restart the ESX host.

**Issues when Reinstalling the Hypervisor Connector**

If you need to reinstall the Hypervisor Connector and the Reinstall Hypervisor procedure does not work, you can reinstall it manually.

To manually reinstall the Hypervisor Connector:
2. Locate the VIB file at:
   
   `$/CPVIRTDIR/data/cp-esx-cpdvfilter_ESX5.vib`
3. Copy the VIB file to this directory on the ESX host:
   
   `/var/log/vmware`
4. Uninstall the Hypervisor Connector:
   a) Power off all the VMs on the ESXi host (including the Security Gateway Virtual Edition VM).
   b) Log in to the ESXi host.
   c) Run:
      
      `esxcli software vib remove -n cp-esx-cpdvfilter --maintenance-mode`
   d) Run:
      
      `vmkload_mod -u cpdvfilter_kern`
5. Install the Hypervisor Connector:
   a) Log into the ESXi host.
   b) Run:
      
      `esxcli software vib install -v cp-esx-cpdvfilter_ESX5.vib --maintenance-mode`
6. Reboot the ESXi host and power on the VMs.

**General Troubleshooting**

**Policy Installation Issues**

If you have issues when you install a policy, such as:

- You get this error message:
  
  *Installation has failed due to connectivity issues with the vCenter/ESX host.*
- You see this log in SmartView Tracker after you install a policy:
  
  *Make sure you have connectivity to the vCenter/ESX host. Policy will be allowed for the next XX tries if connectivity issue is not resolved.*

Then do these steps to make sure that your environment can work correctly:


b) Make sure your vSphere connection configuration is correct. If not, change it as explained in Configuring a Local ESX Connection (on page 23) for Hypervisor Mode or in Configuring the vSphere Connection for Network Mode.
**Policy Installation Issues**

If you have issues when you install a policy, such as:

- You get this error message:
  
  *Installation has failed due to connectivity issues with the vCenter/ESX host.*

- You see this log in SmartView Tracker after you install a policy:
  
  *Make sure you have connectivity to the vCenter/ESX host. Policy will be allowed for the next XX tries if connectivity issue is not resolved.*

Then do these steps to make sure that your environment can work correctly:


b) Make sure your vSphere connection configuration is correct. If not, change it as explained in Configuring a Local ESX Connection (on page 23) for Hypervisor Mode.

**Increasing the Security Gateway Virtual Edition Disk Size**

You can increase the Security Gateway Virtual Edition VM disk size to give more space for logs, especially if the VM has a Security Management Server installed.

You can also add more disks to this VM. After you do this, format the new disk in SecurePlatform. You can then send logs to a directory on the disk.

**Creating a Second Hard Drive in VMware**

You cannot change the size of the hard disk in an existing VM. However, you can add an additional disk drive to a VM. This is useful for Security Management Server VMs with very large log files.

**To define a second hard drive:**

1. Power off the Security Gateway Virtual Edition VM.
2. Right-click the VM in your inventory and select *Edit Settings*.
3. Click *Add* and then select *Hard Disk* from the *Add Hardware Wizard*.
4. In the *Device Type* window, select *Create a new virtual disk*.
5. In the *Select a Disk* window, enter the disk size in gigabytes.
6. In the *Advanced Options* window, click *Next*.
7. In the *Ready to Complete* window, examine the settings and then click *Finish*.

You can now format the new drive and configure Security Management Server to send the log files to the new disk.

**Configure the New Hard Drive in SecurePlatform**

The process for configuring a new SecurePlatform hard drive includes these procedures:

1. Making a new partition.
2. Configuring the volume settings.
3. Formatting and mapping the disk.
4. Sending log files to the new disk.

**Creating a New Partition**

To make a new partition:

1. On the host console, log in to expert mode.
2. Create a new partition. Run: `fdisk /dev/sdb`
3. Enter `n` to add a new partition.
4. Enter `p` to choose a primary partition.
5. Enter for the partition number (1 for a second disk).
6. Accept the defaults for the first and last cylinder.
7. Enter t to change the partition’s system ID.
8. Enter the hex value: 83.
9. Enter w to write the partition table to disk and to exit.

**Defining the Volume Settings**

**To define the volume settings:**

1. Run this command:
   
   ```bash
   fdisk -l
   ```
   
   This command makes sure that the new hard disk is properly configured and that `dev/sdb1` was successfully created. The `l` parameter shows the parameter table.

2. Run this command to initialize the physical volume:
   
   ```bash
   pvcreate /dev/sdb1
   ```

3. Optionally, run this command to make sure that the physical volume was created by running:
   
   ```bash
   pvdisplay
   ```

4. Run this command to create a volume group:
   
   ```bash
   vgcreate mynew_vg /dev/sdb1
   ```
   
   Choose a name for the volume group, for example: `mynew_vg`

5. Run this command to create a logical volume:
   
   ```bash
   lvcreate -L 4000 -n vol2 mynew_vg
   ```
   
   - 4000 is the size of the hard drive in MB.
   - `vol2` is logical volume name.
   - `mynew_vg` is the volume group name, as defined in the previous step.

**Formatting and Mapping the Hard Drive**

**To format and map the hard drive:**

1. Run this command to format the hard disk:
   
   ```bash
   mkfs.ext3 -m 0 /dev/mynew_vg/vol2
   ```

2. Add the new hard disk to the SecurePlatform mapping tables.
   
   a) Run this command to change the `fstab` file:
      
      ```bash
      vi /etc/fstab
      ```
   
   b) Add this data to the end of the line:
      
      ```bash
      /dev/mynew_vg/vol2/ exvar ext3 defaults 1 2
      ```
      
      `exvar` is the name of the directory to which the disk is mapped in this example.

3. Run these commands to create the physical directory to which the disk is mapped
   
   ```bash
   mkdir /exvar
   mount -a
   ```
   
   `exvar` is the name of the directory to which the disk is mapped in this example.

**Moving Log Files to the New Disk**

**To redirect log files to the new disk:**

1. Run this command:
   
   ```bash
   cpstop
   ```

2. Save the current log directory by running:
   
   ```bash
   mv $FWDIR/log $FWDIR/log.old
   ```

3. Create a new log directory:
   
   ```bash
   mkdir /exvar/newlogs
   ```
   
   `newlogs` is the new directory name.

4. Map logs to the new directory:
5. Run this command:

   `cpstart`

   `ln -s /exvar/newlogs $FWDIR/log`