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=24540)
For additional technical information, visit the Check Point Support Center (Check Point Support Center - http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 May 2013</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
Chapter 1

Overview

In This Chapter
- Introduction 5
- Glossary 6
- Key Benefits 6
- Network Mode Overview 6
- Licensing Security Gateway Virtual Edition 8
- ESX Host Security Considerations 8

Introduction

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. Find which is best for your environment and plan the installation accordingly.

- **Hypervisor Mode** enforces VM security in the VMware Hypervisor with inter-VM traffic inspection, without virtual network topology changes.

- **The Network Mode** is deployed as a virtual network device to protect virtual networks and physical environments. You can configure it as a router or a bridge, with the same procedure as a physical gateway.

**Important Notes:**

- This release supports only Network Mode on Gaia.
- All references to ESX in the document are also for ESXi unless noted differently.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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. Trademark of VMware, Inc.</td>
</tr>
<tr>
<td>Port Group</td>
<td>Virtual Switch ports that share parameters, such as bandwidth limitations and VLAN tagging policies. Virtual Machines connect to vSwitches through 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 to migrate VMs between ESX hosts.</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

- 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.

## 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). To use Network Mode, the network topology must 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>
<tr>
<td>4</td>
<td>ESX host</td>
</tr>
<tr>
<td>5</td>
<td>Security Gateway Virtual Edition VM</td>
</tr>
<tr>
<td>6</td>
<td>Web Servers</td>
</tr>
<tr>
<td>7</td>
<td>Email Server</td>
</tr>
<tr>
<td>8</td>
<td>Database Servers</td>
</tr>
<tr>
<td>9</td>
<td>Physical switch</td>
</tr>
<tr>
<td>10</td>
<td>vSwitch</td>
</tr>
</tbody>
</table>

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.
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.

By default, Security Gateway Virtual Edition installs with a 15-day trial 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 Best Practices:

- Always use different, secured networks for the VMkernel and ESX service console/ESXi Host Management Network. This traffic is not automatically inspected by Security Gateway Virtual Edition. 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 Managing VMware Virtual Center Roles and Permissions Guide.
Chapter 2

Installing and Uninstalling

In This Chapter

- Installing Security Gateway Virtual Edition Virtual Machine
- Configuring the Virtual Machine Settings
- First Time Configuration Wizard
- Completing the Installation
- Uninstallation

You can quickly deploy Security Gateway Virtual Edition on your ESX hosts. It is distributed as a VMware OVF template, already configured 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.

Getting the Template

To get the Security Gateway Virtual Edition OVF Template:
1. Download Check_Point_Security_Gateway_R76_VE.tgz to your vSphere Client computer.
2. Extract the template OVF file to a temporary folder.

Deploying the Security Gateway Virtual Edition VM

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.

The next windows that you see depend on the template properties.
- Name and Location window - select an inventory location for the VM.
- Disk Format window - select Thick provisioned format.
• **Host/Cluster** window - select a host. This window only opens if there are multiple hosts or clusters.

6. If the **Datastore** window opens, select a datastore. This window opens only if there is more than one datastore related to the host or cluster.

---

**Mapping Interfaces and Completing Import**

To complete import of the OVF template, map the interfaces. Security Gateway Virtual Edition is already configured with four network adapters. You can add and delete vNICs.

**To complete import:**

In the **Network Mapping** window, configure the default network adapters and destination networks:

<table>
<thead>
<tr>
<th>Source Network</th>
<th>Description</th>
<th>Destination Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Check Point Management</td>
<td>Check Point management connection</td>
<td>Port group connected to the Check Point management network.</td>
</tr>
<tr>
<td>2 Check Point Sync</td>
<td>Cluster synchronization connection</td>
<td>Port group connected to the Check Point cluster synchronization network.</td>
</tr>
<tr>
<td>3 External Network</td>
<td>External connection</td>
<td>Port group connected to the external network.</td>
</tr>
<tr>
<td>4 Internal Network</td>
<td>Internal connection</td>
<td>Port group connected to the internal network.</td>
</tr>
</tbody>
</table>
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:

In the Ready to Complete window, click Finish.

It can take some time to add the Security Gateway Virtual Edition VM to the inventory.

Configuring the Virtual Machine Settings

Before you configure the Security Gateway Virtual Edition, make sure the VM has the minimum requirements.

To configure the VM:

1. Right-click the VM.
2. Select Edit Settings.
   - The Virtual Machine Properties window opens.
3. Configure memory:
   - Minimum to run Security Gateway Virtual Edition in 64-bit - 6 GB.

   See the table ("Mapping Interfaces and Completing Import" on page 10) for the network adapters that are already configured for Security Gateway Virtual Edition. You can change these, for other vNICs.

First Time Configuration Wizard

The First Time Configuration Wizard is part of the management console, on a WebUI. Open the management console from a VM or a remote host (virtual or physical).

- If the management console is a VM, it must be connected to the Check Point management port group.
- If the management console is a remote host, you will configure the network of the Security Gateway Virtual Edition to reach the host.

First, turn on the Security Gateway Virtual Edition VM.

To open the First Time Configuration Wizard from a different VM:
1. Open the VM console.
   The First Time Configuration Wizard starts.

To open the First Time Configuration Wizard from a remote host:
1. Open the console of the Security Gateway Virtual Edition VM.
2. Log in with the admin credentials (default is admin/admin).
3. In clish, run:
   ```
   set interface eth0 ipv4-address x.x.x.x subnet-mask x.x.x.x
   ```

Security Gateway Virtual Edition - Network Mode Administration Guide R76 | 12
4. If the remote host is not on the same subnet as the Security Gateway Virtual Edition, define a default gateway:
   `set static-route default nexthop gateway address x.x.x.x on`

   The First Time Configuration Wizard starts.

To configure the Security Gateway Virtual Edition with the First Time Configuration Wizard:
1. In the first step of the First Time Configuration Wizard, configure a new password.
2. Configure the date and time.
3. Configure the host name, domain name, and DNS server.
4. Review the network details of the management interface and correct, if necessary.
5. Select Check Point products to install.
6. Select deployment:
   - Standalone: Select Security Gateway and Security Management Server. In the next steps, configure the user name and password of the administrator, and the GUI clients.
   - Distributed: Select Security Gateway and not Security Management Server. In the next steps, configure the Security Gateway Virtual Edition IP address for static or dynamic, and configure the SIC activation key.
7. Click Finish.
   A message shows to restart the Security Gateway.
8. Click OK to restart the Security Gateway Virtual Edition now.

Completing the Installation

You must have a SmartDashboard installed on a Windows computer, and defined as a GUI client.

To install the R76 SmartDashboard:
1. Browse to: `https://<Security Gateway Virtual Edition IP address>`
2. At Manage Software Blades using SmartConsole, click Download Now.

After the SmartDashboard is installed, use the GUI client to install the 15-day trial license, or to add a permanent license. Open SmartDashboard and install a policy on the Security Gateway Virtual Edition.

Uninstallation

To uninstall Security Gateway Virtual Edition:
1. In the vSphere client, turn 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

Advanced Configuration

In This Chapter
- Changing Between 32-bit and 64-bit Gaia VM 14
- Installing Clusters 14
- Increasing the Security Gateway Virtual Edition Disk Size 15
- Changing Keyboard Layout 16

Changing Between 32-bit and 64-bit Gaia VM

When you install Security Gateway Virtual Edition on a Gaia computer or VM, a 32-bit kernel installs by default. You can change it to 64-bit with Edition.

Note: The ESX server hardware must support 64-bit.

To change to 64-bit Gaia:
1. Turn off the Security Gateway Virtual Edition VM.
2. Increase the Security Gateway Virtual Edition VM memory to 6 GB or more.
3. In the Gaia command line, run: `set edition 64-bit`
4. Turn on the Security Gateway Virtual Edition VM.

To see which edition is running:
In the Gaia command line, run: `show version os edition`

Installing Clusters

Security Gateway Virtual Edition supports clusters of two or more members. If you install cluster members on different ESX hosts, you can be sure of automatic failover if an ESX host is unavailable.

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

Defining a ClusterXL Cluster


To define a ClusterXL cluster:
1. Install and configure two or more Security Gateway Virtual Edition VMs.
2. Turn on the VMs.
3. Run the First Time Configuration Wizard 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 internal networks, external networks, and other VMs. Resolve connectivity issues before continuing.
6. Use SmartDashboard to define the cluster as an object and to configure its synchronization networks.
7. Define and install security policies.
Increasing the Security Gateway Virtual Edition Disk Size

The VE R76 Gaia OS is configured with this distribution:

- **Swap**: 2 GB
- **Root**: 7 GB
- **Logs**: 3 GB
- **Backup and upgrade**: 8 GB

Add a hard disk to the Security Gateway Virtual Edition VM to give space for backups.

**Creating a Second Hard Drive in VMware**

You cannot change the size of the hard disk in an existing VM. But you can add a disk drive to a VM.

**To define a second hard drive:**

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

**Configuring New Hard Drive in Gaia**

You can format the new drive and configure Security Management Server to send the log files to the new disk. First, create a new partition. Then, define the volume settings.

**To create a new partition:**

1. Log in to the host console in 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 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.

**To define volume settings, run these commands:**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fdisk -l</code></td>
<td>Makes sure that the new hard disk is properly configured and that <code>dev/sdb1</code> was successfully created. The option shows the parameter table.</td>
</tr>
<tr>
<td><code>pvcreate /dev/sdb1</code></td>
<td>Initializes the physical volume.</td>
</tr>
<tr>
<td><code>pvdisplay</code></td>
<td>See output to make sure that the physical volume was made.</td>
</tr>
</tbody>
</table>
### Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vgcreate &lt;group_name&gt; /dev/sdb1</code></td>
<td>Creates a volume group, with the name you give it.</td>
</tr>
<tr>
<td><code>lvcreate -L &lt;HD size&gt; -n &lt;vol_name&gt; &lt;group_name&gt;</code></td>
<td>Creates a logical volume, of the given size in MB, with the given volume name.</td>
</tr>
</tbody>
</table>

**Example:**

```
fdisk -l
pvcreate /dev/sdb1
vgcreate mynew_vg /dev/sdb1
lvcreate -L 4000 -n vol2 mynew_vg
```

### Changing Keyboard Layout

Security Gateway Virtual Edition is configured for United States English keyboard layout.

To change this, see sk73420 (http://supportcontent.checkpoint.com/solutions?id=sk73420).