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=25138)
To learn more, 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>13 February 2014</td>
<td>Added OVF installation (&quot;Installing Security Gateway Virtual Edition from OVF&quot; on page 9)</td>
</tr>
<tr>
<td>4 July 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 (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Gateway Virtual Edition Network Mode R77 Administration Guide).
Terms

Cluster
Two or more Security Gateways connected to each other for High Availability and/or Load Sharing.

Datastore
Host-independent storage (a system volume on a physical disk, RAID, SAN, or network file) for Virtual Machine files in ESX environments.

Deployment
1. Send an installation to multiple computers, appliances, or devices, to give the same configuration or policy. 2. A type of network topology.

ESX
A VMware physical server that hosts 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.

Port Group
Virtual Switch ports that share parameters, such as bandwidth limitations and VLAN tagging policies, and through which Virtual Machines connect to Virtual Switches.

Security Gateway
A computer or appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Gateway Virtual Edition
(Also: Security Gateway VE). A Security Gateway that protects virtual environments with policy enforcement. In hypervisor mode, it protects connections between virtual systems. In network mode, it protects connections between a virtual network and a physical network.

Security Management Server
The application that manages, stores, and distributes the security policy to Security Gateways.

Security Policy
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources through the use of packet inspection.

SmartDashboard
A SmartConsole client used to create and manage the security policy.

Virtual Network
An environment of logically connected VMs on an ESX host.

Virtual Switch
Also vSwitch. A software abstraction of a physical Ethernet switch that can connect to physical switches through physical network adapters, to join virtual networks with physical networks.

VLAN
Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

VLAN Trunk
A connection between two switches that contains multiple VLANs.

VM
Virtual Machine. A software abstraction of a physical computer. VMware, VMware VMotion and VMware vSphere are registered trademarks and trademarks of VMware, Inc. in the United States and other jurisdictions.

vNIC
Virtual Network Interface. A software based abstraction of a physical interface that supplies network connectivity for Virtual Machines.
Chapter 1

Introduction

In This Chapter

<table>
<thead>
<tr>
<th>Key Benefits</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Deployment with Network Mode</td>
<td>7</td>
</tr>
<tr>
<td>Network Mode Overview</td>
<td>8</td>
</tr>
<tr>
<td>Licensing Security Gateway Virtual Edition</td>
<td>8</td>
</tr>
<tr>
<td>ESX Host Security Considerations</td>
<td>8</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. 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.

**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 VMware vMotion migration.


- Protects expanding virtual networks while reducing hardware investment, maintenance, energy, and site costs.

- Optimizes performance for virtual environments.
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.
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.

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 from OVF 9
Installing Security Gateway Virtual Edition from ISO 12
First Time Configuration Wizard 13
Completing the Installation 14
Uninstallation 14

You can deploy Security Gateway Virtual Edition on your ESX hosts from an OVF template or from an ISO.
If you choose to install from an OVF template, the operating system for the VM is installed and configured for typical deployment. This option is faster.
If you choose to create a new Virtual Machine, you install the Security Gateway from the Check Point ISO. You install the operating system and then run the First Time Configuration Wizard.

Installing Security Gateway Virtual Edition from OVF

To install a new Security Gateway Virtual Edition VM from an OVF template:
1. Import the OVF template and start the Deploy OVF Template wizard.
4. Run the First Time Configuration Wizard ("First Time Configuration Wizard" on page 13).

Getting the Template

To get the Security Gateway Virtual Edition OVF Template:
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.

### Configuring Network Adapters - Mapping Interfaces

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.

In the **Network Mapping** window, configure the default network adapters and destination networks. These are the network adapters that are configured for Security Gateway Virtual Edition by the template.

<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>

**To complete the OVF import:**

1. For each source network, select a destination network from the list.
2. Click **Next**.
3. Click **Finish**.
   
   It can take some time to add the Security Gateway Virtual Edition VM to the inventory.
4. Continue with the First Time Configuration Wizard (on page 13).

**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.


**Configuring Storage**

When you deploy a Security Gateway Virtual Edition R77 on Gaia from OVF, it gets this configuration:

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

To add more storage, increase the disk size (*Increasing the Security Gateway Virtual Edition Disk Size* on page 16).

**Installing Security Gateway Virtual Edition from ISO**

Before you begin, download the ISO file with the R77 image for the Gaia operating system to your vSphere Client computer.

**To create a new R77 VM:**

1. In the VMware vSphere client, click **File > New > Virtual Machine**.
   - The **Create New Virtual Machine** wizard opens.
2. Select **Custom Configuration**.
3. Enter a name, inventory location, host, destination storage, and version for the VM.
5. In Version, select Other 2.6.x Linux (32-bit) or Other 2.6.x Linux (64-bit).
   The mode you select here must match the mode that you select during Gaia installation.
6. In the CPUs window, select the number of virtual CPUs for the virtual machine.
7. In the Memory window, set the memory size of the VM:
   - Minimum to run Security Gateway Virtual Edition in 64-bit - 6 GB.
8. In the Network window, select the number of NICs to connect to the VM.
9. Map the interfaces to the networks available to the ESX host.
   - Use E1000 adapters for the NICs.
   - Leave Connect at Power On selected.
10. In the SCSI Controller window, select LSI Logic Parallel.
11. In the Disk window, select Create a new virtual disk.
12. In the Create a Disk window:
   - Disk Size - 21 GB is required minimum
   - Disk Provisioning - select Thick Provision Lazy Zeroed
   - Location - select Store with virtual machine
13. In the Advanced Options window, do not change the default settings (Disk Provisioning = Flat Disk, Virtual Device Node = SCSI 0:0).
14. In the Ready to Complete window, select Edit the virtual machine settings before completion.
15. Click Continue.
   The Virtual Machine Properties window opens.

To configure the new VM with required settings:
1. Open the Resources Tab and select Memory.
2. Increase Memory Reservation to at least 1 GB.
   More reserved resources increase the performance of the Security Gateway VM.
3. Click Finish.
5. Attach the ISO file with the downloaded R77 image to the VM CD/DVD drive.
   a) With the Virtual Machine selected, click Connect/disconnect the CD/DVD devices of the virtual machine.
   b) Click Connect to ISO image on local disk.
   c) Browse to the location of the ISO file and click Open.
6. Right-click the VM and select Guest > Send Ctrl+Alt+Del.
7. With the Virtual Machine selected, open the Console tab.
8. Log in to the virtual machine console.
   The operating system installation begins automatically. See the R77 Installation and Upgrade Guide.
9. Continue with the First Time Configuration Wizard (on page 13).

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
   ```
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 host name, domain name, and DNS server.
3. Configure the date and time.
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. Configure the username of an administrator.
8. Click Finish.
   A message shows to restart the Security Gateway.
9. 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 R77 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 15
- Configuring VMXNET3 Network Adapters 16
- Installing Clusters 16
- Increasing the Security Gateway Virtual Edition Disk Size 16
- Changing Keyboard Layout 17

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
Configuring VMXNET3 Network Adapters

You can use the new VMXNET3 driver to get better performance and support for 10G network adapters. VMXNET3 comes as part of R77 VE OVF. It is not included with the ISO version of R77 VE.

If you want to change E1000 interfaces to VMXNET3, you must delete ALL interfaces and reinstall them with the VMXNET3 driver.

To change E1000 interfaces to VMXNET3:
2. Right-click the Virtual Machine in the inventory and select Edit Settings.
3. Select the applicable network adapters and then select Remove.
4. Click Add.
5. In the Add Hardware Wizard, select Ethernet adapter and click Next.
6. Select the VMXNET3 adapter and then choose network label.

Do steps 4 - 6 again for all of these networks:
- Check Point Management
- Check Point Sync
- External Networks
- Internal Networks

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

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 Security Gateway Virtual Edition 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>
<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).
Index

A
Advanced Configuration • 15

B
Basic Deployment with Network Mode • 7

C
Changing Between 32-bit and 64-bit Gaia VM • 15
Changing Keyboard Layout • 17
Cluster • 5
Completing the Installation • 14
Configuring Network Adapters - Mapping Interfaces • 10
Configuring New Hard Drive in Gaia • 17
Configuring Storage • 12
Configuring the Virtual Machine Settings • 11
Configuring VMXNET3 Network Adapters • 16
Creating a Second Hard Drive in VMware • 16

D
Datastore • 5
Defining a ClusterXL Cluster • 16
Deploying the Security Gateway Virtual Edition VM • 9
Deployment • 5

E
ESX • 5
ESX Host Security Considerations • 8

F
First Time Configuration Wizard • 13

G
Getting the Template • 9

I
Important Information • 3
Increasing the Security Gateway Virtual Edition Disk Size • 16
Installing and Uninstalling • 9
Installing Clusters • 16
Installing Security Gateway Virtual Edition from ISO • 12
Installing Security Gateway Virtual Edition from OVF • 9
Introduction • 6

K
Key Benefits • 6

L
Licensing Security Gateway Virtual Edition • 8

N
Network Mode Overview • 8

P
Port Group • 5

S
Security Gateway • 5
Security Gateway Virtual Edition • 5
Security Management Server • 5
Security Policy • 5
SmartDashboard • 5

U
Uninstallation • 14

V
Virtual Network • 5
Virtual Switch • 5
VLAN • 5
VLAN Trunk • 5
VM • 5
vNIC • 5