Important Information

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

**Check Point vSEC**
For more about this release, see the vSEC home page [http://supportcontent.checkpoint.com/solutions?id=sk109576](http://supportcontent.checkpoint.com/solutions?id=sk109576).

**Latest Version of this Document**

**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 vSEC Controller and vSEC Gateway R77.30 v2 Administration Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on vSEC Controller and vSEC Gateway R77.30 v2 Administration Guide).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 November 2016</td>
<td>General updates</td>
</tr>
<tr>
<td>17 November 2016</td>
<td>Upgrade information for vSEC for NSX (see &quot;Upgrading the vSEC Gateway for NSX&quot; on page 12) and installation and upgrade information for vSEC Management Controller (see “Installing the vSEC Controller” on page 10).</td>
</tr>
<tr>
<td>06 October 2016</td>
<td>Improved installation instructions (&quot;Installing the vSEC Controller&quot; on page 10) and general updates</td>
</tr>
<tr>
<td>01 June 2016</td>
<td>General updates</td>
</tr>
<tr>
<td>10 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
## Contents

- Important Information ................................................................................................... 2
- Terms ............................................................................................................................ 7
- Welcome to vSEC for NSX ............................................................................................. 9
- Installing the vSEC Controller ..................................................................................... 10
  - Upgrading the vSEC Management Controller ............................................................ 12
  - Upgrading the vSEC Gateway for NSX ................................................................. 12
  - Licensing vSEC ........................................................................................................ 13
  - Uninstalling the Hotfix ............................................................................................ 13
  - Uninstalling the SmartDashboard........................................................................... 14
- Configuring vSEC Controller ....................................................................................... 15
  - Connecting to a Data Center Server ........................................................................ 15
  - Creating Data Center Objects Group ....................................................................... 16
  - Creating Rules ........................................................................................................ 16
  - Threat Prevention Tagging ...................................................................................... 17
    - Threat Prevention Tagging for Upgrade to vSEC for NSX Gateway .................. 18
- vSEC Controller Monitoring and Troubleshooting .................................................. 19
  - No Servers and OPSEC > Data Center Option ......................................................... 19
  - Failed to Download Mapping to Target .................................................................. 19
  - Failed to Get Data from Data Center ...................................................................... 19
  - Database File not Updated .................................................................................... 20
  - Policy Installation Failed ....................................................................................... 20
  - Failed to Activate Threat Prevention Tagging ....................................................... 20
  - CPUSE Inconsistent Files ..................................................................................... 21
- Deploying vSEC Gateway ............................................................................................. 22
  - Basic Deployment with Hypervisor mode .............................................................. 23
  - ESX Host Security Considerations ...................................................................... 24
  - Configuring the VMware Components .................................................................. 24
    - Configuring Agent VM Host Settings ................................................................ 24
    - Adding the vCenter IP Address to the Runtime Settings ..................................... 25
    - Creating an ESX Cluster ..................................................................................... 25
  - Deploying the vSEC Gateway SVM ....................................................................... 25
    - Installing the OVF ............................................................................................ 25
    - Configuring the vSEC Management Server Properties ..................................... 26
    - Registering a vSEC Gateway Service ................................................................. 27
    - Deploying vSEC Gateway with the vSphere Web Client .................................... 27
    - Automatic Provisioning of vSEC Objects ........................................................... 29
    - Configuring NSX to Redirect traffic to the vSEC Gateway ................................. 30
  - Manual Configuration of the vSEC Gateway VM ................................................ 31
  - Manual Creation of vSEC Cluster Objects ............................................................. 32
  - Redirecting Traffic to the vSEC Gateway ............................................................. 33
  - Adding an ESX Host to a vSEC Protected ESX Cluster ....................................... 34
  - Removing a Host from a Cluster .......................................................................... 34
vMotion............................................................................................................................... 35
Configuring Check Point Blades and Management High Availability Failover ........ 35
  Configuring Application Control Policy................................................................. 35
  Configuring Threat Emulation.............................................................................. 35
  Configuring Identity Awareness in vSEC............................................................... 36
Management High Availability Failover ................................................................. 36
Uninstalling the vSEC Gateway Service................................................................. 38
Terms

Data Center
Virtual centralized repository, or group of physical networked hosts, VMs, and datastores, collected in a group for secured remote storage, management, distribution of data.

DRS
Data Resource Scheduler. Monitors resource use across resource pools and allocates resources between virtual machines to maximize throughput.

ESX
A VMware physical hypervisor 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.

Management Server
A Security Management Server or Multi-Domain Server that manages one or more Security Gateways and security policies.

NSX Manager
Basic network and security functionality for virtual computer environments. Previously known as vShield, a VMware product family for SDN of virtual machines on the cloud. Trademark of VMware, Inc.

OVF
Open Virtualization Format. Open standard (independent of processor architecture) for the distribution of software that runs on virtual machines.

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. Unless otherwise specified, this refers to both regular port groups (on one ESX host) and dvPGs (distributed virtual port groups, on multiple ESX hosts).

REST API
Representational State Transfer Application Programming Interface. The NSX API, for communication between the NSX Manager and the Service Manager.

SDDC
Software-Defined Data Center. Data center infrastructure components that can be provisioned, operated, and managed through an API for full automation.

SDN
Software-Defined Network. Virtualization of topology, traffic, and functionality.

Security Group
Collection of virtual objects that defines the NSX Distributed Firewall protection policy.

Service Composer
A VMWare NSX component that provisions and assigns network and security services to applications in a virtual infrastructure.

Service Manager
Component that manages the communication between Check Point products, the Controller, and the NSX, through VMWare REST API.

SVM
Service Virtual Machine. A virtual machine deployed as a service on the ESX and as part of NSX network. vSEC Gateway is an SVM.

Threat Prevention Tagging
A feature for tagging and quarantining VMs infected by a bot or a virus, to apply stricter policies to the tagged VMs.

vCenter Server
Centralized management tool for VMware vSphere. It manages many ESX servers and VMs from different ESX servers, from one console application.
**Virtual Network**
Environment of logically connected VMs on an ESX host.

**vMotion**
VMware technology for migration of active VMs between ESX hosts.

**vNIC**
Virtual Network Interface. Software based abstraction of a physical interface that supplies network connectivity for Virtual Machines.

**vSEC Controller**
Provisions software-defined data center services as virtual data centers that provide virtualized computer networking, storage, and security.

**vSEC Gateway**
Check Point virtual Security Gateway that protects dynamic virtual environments with policy enforcement. vSEC Gateway inspects traffic between VMs, to enforce security in VMware Hypervisor, without changing the virtual network topology.

**vSphere**
VMware cloud computing virtualization operating system. The vSphere Web Client is the GUI to manage VMs and their objects.
Welcome to vSEC for NSX

vSEC for NSX is an advanced security solution for the Software-Defined Data Center (SDDC). The Check Point vSEC solution enforces Advanced Threat Prevention within the NSX structure. It proactively stops malware and Zero Day attacks in the data center environment. The unified management of virtual and physical gateways simplifies security management across the data center.

vSEC Gateway for NSX is automatically deployed as a service VM in the VMware, virtual environment. It operates on a hypervisor level. It fully integrates with VMWare NSX components. vSEC Gateway secures data center traffic between Virtual Machines across the virtual network.

The vSEC Gateway for NSX secures data center traffic between virtual machines across the virtual network.

The vSEC Controller makes the Check Point Security Management Server SDDC aware, with VMware NSX and vCenter integration. This lets vSEC Controller make dynamic security policies, manage vSEC gateways and physical gateways, and provide complete visibility for data center security.
Installing the vSEC Controller

In This Section:

Upgrading the vSEC Management Controller ............................................................. 12
Upgrading the vSEC Gateway for NSX ................................................................. 12
Licensing vSEC ................................................................. 13
Uninstalling the Hotfix .................................................................................. 13
Uninstalling the SmartDashboard ................................................................. 14

Install the Hotfix on Gaia R77.30 Security Management Server and R77.20/R77.30 Security Gateways. It is required for the Security vSEC Gateway and the vSEC Controller. If you have previously installed hotfixes, consult with Check Point before you install this Hotfix.

To install a vSEC Controller, install this Hotfix.

<table>
<thead>
<tr>
<th>Install on:</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Server and Multi-Domain Server</td>
<td>R77.30 GA + R77.30 Add-on + R77.30 Jumbo Hotfix take 185 + vSEC Bundle Hotfix</td>
</tr>
<tr>
<td>Security Gateway</td>
<td>R77.30 GA + R77.30 Jumbo Hotfix take 185 + vSEC Bundle Hotfix</td>
</tr>
<tr>
<td></td>
<td>R77.20 GA + R77.20 Jumbo Hotfix take 169 +vSEC Hotfix (R77.20)</td>
</tr>
</tbody>
</table>

To install the SmartDashboard:

Install SmartDashboard to install the new hotfixes.

1. Uninstall the current R77.30 SmartDashboard.
2. Download the new SmartDashboard. See sk 114516
3. Install the .exe file.

To install the Security Management Server Hotfix with CPUSE:

1. Make sure the Security Management Server or Multi-Domain Server is prepared:
   - Make sure the Add-on and Jumbo Hotfix are installed.
   - Install the latest build of the CPUSE agent, sk92449
   - Make sure the server has sufficient disk space.
2. Take a snapshot of the server, to save a backup.
3. Open the Gaia portal > CPUSE > Status and Actions.
4. Click Add hotfixes from the cloud.
5. Select the vSEC Hotfix for Security Gateway, R77.30 or R77.20, see sk114516
6. Click Download.
   The Deployment Agent downloads the package from the Check Point cloud.
7. Click **Install**. Installation starts immediately.
8. Connect to the Management CLI.
9. Run: `vsec on`

**To install the Hotfix with CLI:**

1. Make sure the Security Management Server or Multi-Domain Server is prepared:
   - Make sure the Add-on and Jumbo Hotfix are installed.
   - In a Multi-Domain Security Management environment, make sure the Add-on is activated on the Domain Management Servers.
   - Make sure the server has sufficient disk space.
2. Take a snapshot of the server, to save a backup.
3. Download the CLI package of the **vSEC Bundle Hotfix for Security Management Server / Multi-Domain Security Management Server**, from sk114516
5. From the extracted folder, run: `./UnixInstallScript`
6. Follow the prompts.
7. Reboot the system.
8. Run: `vsec on`

**To install the Hotfix with CPUSE on Security Gateways to be managed by vSEC Controller:**

1. Make sure the Security Gateway is prepared:
   - Make sure the Jumbo Hotfix is installed.
   - Make sure the computer or appliance has sufficient disk space.
2. Take a snapshot of the gateway, to save a backup.
3. Open the Gaia portal > **CPUSE > Status and Actions**.
4. Install the latest build of the CPUSE agent from sk92449
5. Click **Add hotfixes from the cloud**.
6. Select **vSEC Hotfix for Security Gateway, R77.30 or R77.20**, see sk114516
7. Click **Download**. The Deployment Agent downloads the package from the Check Point cloud.
8. Click **Install**. Installation starts immediately.

**To install the Hotfix with CLI:**

1. Make sure the Security Gateway is prepared:
   - Make sure the Jumbo Hotfix is installed.
   - Make sure the computer or appliance has sufficient disk space.
2. Take a snapshot of the gateway, to save a backup.
3. Download the CLI package for **vSEC Hotfix for Security Gateway, R77.30 or R77.20**, see sk114516
4. Extract the package on the Security Gateway.
5. From the extracted folder, run:
   • R77.30: ./UnixInstallScript
   • R77.20: ./fw1_wrapper_HOTFIX_R77_20_JUMBO_169_VSEC_990606015_1
6. Follow the prompts.
7. Reboot the system.

Upgrading the vSEC Management Controller

If you have previously installed vSEC Controller Bundle on the Domain Management Server, upgrade to Jumbo Hotfix 185.

To upgrade the new vSEC bundle:
1. Download the Jumbo Hotfix package and the vSEC Bundle for it.
2. Download upgrade.sh to the Management Server from sk114516
3. Run: upgrade.sh backup
4. Uninstall the old vSEC Controller Bundle Hotfix ("Uninstalling the Hotfix" on page 13).
5. Install the latest build of the CPUSE agent, see sk92449
6. Install only the required Jumbo Hotfix Accumulator for R77.30.
8. Run: upgrade.sh restore

Upgrading the vSEC Gateway for NSX

There are different ways to upgrade your gateways. Install the Hotfix on all your gateways with CPUSE, or replace the OVF. If you replace the OVF, there is zero downtime.

**Best Practice** – Before you install the new Hotfix, migrate all the VMs to another ESX host. There is less downtime when you upgrade.

To install the Hotfix using CPUSE:
1. Install the latest build of the CPUSE agent from sk92449
2. Install vSEC Gateway for NSX R77.30VSEC v2 Hotfix package from sk114516
3. Reboot.
To change the gateway OVF:
1. Install the new OVF files (“Installing the OVF” on page 25).
2. Register a new vSEC Gateway service (“Registering a vSEC Gateway Service” on page 27).
3. Deploy the new vSEC Gateway service (“Deploying the Service” on page 28).
4. Install the policy on the dashboard of the Check Point gateway.
5. On the vSphere web UI, change the redirection policy from the old service to the new service.
6. Uninstall the old vSEC Gateway Service (“Uninstalling the vSEC Gateway Service” on page 38).

Licensing vSEC

When you attach the vSEC Gateway license to a cluster, every vSEC Gateway that is part of the cluster is licensed. You must purchase a license for the number of physical CPUs on the ESX clusters for the IP address of the vSEC Management Server.

To license vSEC:
1. Download your license from the User Center.
2. Attach your vSEC license to the Domain Management Server with SmartUpdate.
3. Attach the license to a cluster with the vsec config utility:
   a) Run: vsec config
   b) Select the Licensing option.
   c) Select Attach vSEC license.
   d) Select a cluster with vSEC.

By default, vSEC Gateway installs with a 15-day trial license. vSEC Controller is part of vSEC Management Server and does not require an additional license.

Uninstalling the Hotfix

To uninstall the Hotfix with CPUSE:
1. Open the Gaia portal > CPUSE > Status and Actions.
2. In the drop-down at the top of the list, select All.
3. Select the package you want to uninstall, see sk114516 https://supportcontent.checkpoint.com/solutions?id=sk114516.
   a) Security Management Server or Multi-Domain Server
   b) R77.30 Security Gateway
   c) R77.20 Security Gateway
4. Click Uninstall.
To uninstall the Hotfix with CLI from R77.20 or R77.30 Security Gateway:

1. Download the CLI package, see sk114516
2. Extract the package.
3. From the extracted folder, run: ./UnixInstallScript -u

**Uninstalling the SmartDashboard**

To uninstall the SmartDashboard:

1. After you uninstall the server Hotfix, remove the SmartDashboard of this Hotfix.
2. Install the SmartDashboard of the matching version.
Configuring vSEC Controller

In This Section:

- Connecting to a Data Center Server ................................................................. 15
- Creating Data Center Objects Group ................................................................. 16
- Creating Rules ................................................................................................. 16
- Threat Prevention Tagging ............................................................................... 17
- vSEC Controller Monitoring and Troubleshooting ............................................. 19

vSEC Controller integrates the virtual environment with Check Point security. The Check Point Data Center server connects to the SDDC (Software-Defined Data Center) and updates the IP addresses of the objects inside the Data Center Objects group.

vSEC Controller provides fast enforcement of dynamic topologies and policies. The virtual environment is automatically updated for new and changed appliances, computers, devices, and addresses. Your Data Center and its traffic are automatically secured.

vSEC Controller currently supports VMware I/S. More SDDCs will be supported in future releases.

Currently Supported Data Center Objects:
- Virtual Machines
- Security Groups
- vApps
- Resource Pools
- Hosts
- Clusters
- Data Center
- Cluster folders

Currently Supported Third Party Features:
- vCenter
- NSX

Connecting to a Data Center Server

Your vSEC Management Server connects to the SDDC through the Data Center Server object.

To create a connection to the SDDC:
1. In SmartDashboard Objects tree, click the Servers and OPSEC icon.
2. Right-click Data Center and select New Data Center.
3. Select the server type.
   The properties window of the selected server opens.
4. Enter your credentials.
5. Click **Test Connection**.
   
   If the server was not approved before, a certificate window opens.

6. If you did not confirm the certificate before, click **Trust**.

7. If **Connection Status** changes to **Connected**, click **OK**.
   
   If the Connection Status does not change to Connected, see Troubleshooting ["vSEC Controller Monitoring and Troubleshooting" on page 19].

### Creating Data Center Objects Group

Create a Data Center Objects Group object to easily manage rules related to the selected Data Center Servers. When you add a rule to a Data Center Objects Group, the rule is added to all the objects in the group.

**To create a Data Center Objects Group:**

1. In SmartDashboard open **Network Objects**.
2. Right-click **Groups** and select **Groups > Data Center Objects Group**.
   
   The Data Center Objects Group window opens.
3. Enter a name for the new group.
4. Click (+).
   
   The list shows the Data Center servers that are connected, and all the objects in that group.
5. In the window that opens, select the objects to add to this group.
   
   Make sure to select the Data Center object that you created.
6. Click **OK**.

### Creating Rules

After you create a group of the Data Center objects, you can assign rules to the groups. The SDDC automatically updates the rules for changes in IP addresses.

**To add a rule to a Data Center Objects Group:**

1. In SmartDashboard open the Rule Base.
2. Change the **Source** or **Destination** of the rule to be the Data Center Objects group.
3. Install policy.
Threat Prevention Tagging

With Threat Prevention Tagging, Anti-Bot and Anti-Virus services enabled, vSEC Gateway sends a tag command to the vSEC Management Server when a threat reaches the gateway. This threat is tagged and denied entry, and you can use this tag to apply stricter rules to the Threat Prevention service.

Enable the Anti-Bot or Anti-Virus Software Blade, or both, on the vSEC gateway, to apply the Threat Prevention Tagging service.

To enable the Anti-Bot or Anti-Virus Software Blade on the vSEC Gateway:

1. In SmartDashboard, click Gateways.
2. Right-click a gateway object and select Edit.
   The Gateway - General Properties window opens.
3. In the Network Security tab, select Anti-Bot or Anti-Virus, or both.
4. Click OK.
5. Click Policy.
6. In Action, click Recommended_Profile and make sure the threats are labeled Prevent.
7. Click Install Policy.

To check that the policy of the Software Blades is up to date, open the Threat Prevention tab and click Gateways. The status of each gateway shows.

After you enable the Anti-Bot and Anti-Virus Software Blade on the vSEC Gateway, add the vSEC Gateway or Cluster to the Threat Prevention Tagging service.

**Note** - Make sure you establish Internet connection, and configure the proxy server, if needed. To configure a proxy server, go to Firewall > Gateway Cluster Properties - General Properties > Topology > Proxy.
To add a vSEC Gateway or a Cluster to the Threat Prevention Tagging service:

1. Run: `vsec config`
2. From the menu, click Anti-Malware Configuration.
3. In the Gateway List Configuration, select Add a Gateway or a Cluster.
4. Select the vSEC Gateway or Cluster, to add to the list.
5. Select an NSX from the list.
6. In the Anti-Bot Security Tag Configuration or Anti-Virus Security Tag Configuration, either select a Security Tag or create a new one.
   To create a new Security Tag:
   a) Enter a new Security Tag name.
   b) Enter `y`.
   c) Enter a Security Tag description.
   Note - If you select Next without selecting or creating a Security Tag, the Tagging service is disabled.
7. Insert a white list of IP addresses. vSEC Gateway does not send tag commands for VMs with these IPs.
8. If you have secondary management, in the Primary Management SmartDashboard, click Launch Menu > Policy > Management High Availability > Synchronize.
   You will see: Gateway added successfully

### Threat Prevention Tagging for Upgrade to vSEC for NSX Gateway

Do this procedure in the Management CLI if you:

- Upgrade to vSEC for NSX gateway on the old vSEC gateway that you selected in the Threat Prevention Tagging Gateway list.
- Add a new ESX server to a cluster that is already in the Threat Prevention Tagging list. This makes sure that Threat Prevention Tagging is active on the gateway of the new ESX server.

To enable Threat Prevention Tagging on the vSEC Gateway:

1. Run: `vsec config`
2. Select Anti-Malware Configuration.
3. In the Gateway List Configuration, select Show Configured Gateways and Clusters.

Make sure all the Gateways in the list are successfully activated.
vSEC Controller Monitoring and Troubleshooting

No Servers and OPSEC > Data Center Option

Symptom
No Servers and OPSEC > Data Center Option. The new vSEC Controller options are not available.

Solution
1. Uninstall Hotfix ("Uninstalling the Hotfix" on page 13).
2. Confirm that the environment meets these requirements:
   - The R77.30 is the installed version of Security Management Server/Multi-Domain Server and SmartConsole.
   - The R77.30 add-on is installed on the Security Management Server/Multi-Domain Server.
   - The Security Gateways are R77.30 or R77.20.
3. Install missing requirements.
4. Install the R77.30 add-on on to your R77.30 gateway.
5. Install Hotfix again.

Failed to Download Mapping to Target

Symptom
You see the message Failed to Download Mapping to Target in the SmartView Tracker logs.

Solution
1. Confirm that there is SIC communication between the Security Management Server and the gateway.
2. If the SIC failed (there is no Trust), on the Security Gateway, run: cpconfig
3. Enter the number of Secure Internal Communication
4. Follow the instructions to reset SIC.

Failed to Get Data from Data Center

Symptom
You see the message Failed to Get Data from Data Center

Solution
Check if there are connectivity issues between the Management Server and the Data Center.
1. Open the Data Center object properties.
2. Click Test Connection.
Database File not Updated

Symptom
You see the message Database File not Updated and the gateway drops packets.

Solution
The database file on the gateway, which holds data of current virtual objects in the Rule Base, was not properly updated by the fwcloud process.

1. On the Security Gateway, review the last modified data and the contents of $FWDIR/database/virtual_objects.db
2. Reset SIC between the Security Gateway and the Management Server if you do not see the file. If this does not fix the error, the fwcloud process is not getting the data from the Data Center Server. Contact Check Point for further troubleshooting.
3. If you do see the file and it is newly updated, see if the file has all the Data Center object groups that you defined in the policy.
   Make sure that:
   • The Data Center objects are defined correctly
   • The Data Center Objects Group in Rules, is in the correct columns
   • The policy is installed on the correct gateway objects

Policy Installation Failed

Symptom
You see the message Installation failed. Reason: Load on Module failed - problem with the Commit Function.

Solution
Make sure the gateway protecting the Data Center objects is a vSEC Gateway, or a Security Gateway with this Hotfix.

Failed to Activate Threat Prevention Tagging

To confirm that all the gateways are successfully activated:

1. Run: vsec config
2. Select Anti-Malware Configuration.
3. In Gateway List Configuration, select Show Configured Gateways and Clusters.
4. Confirm that all the gateways in the list are activated.

Symptom
A gateway fails to activate in the Anti-Malware Tagging Gateway List.
Solution

1. There may be a SIC error or a Management / Gateway connectivity error.
   On the Multi-Domain Server, run: `tail -f $MDSDIR/log/cloud_tagger.elg`

2. The gateway policy is not installed.

CPUSE Inconsistent Files

Symptom

The CPUSE installation fails and you see this message: Check Point’s installer detected inconsistent files. To solve this, see sk97699

Solution

- Check Internet connections.
- Update the Deployment Agent.
  If you are not connected to the Internet, locally update the Deployment Agent. See sk92449
Deploying vSEC Gateway

In This Section:

- Basic Deployment with Hypervisor mode .......................................................... 23
- ESX Host Security Considerations ..................................................................... 24
- Configuring the VMware Components ............................................................... 24
- Deploying the vSEC Gateway SVM ................................................................. 25
- vMotion ............................................................................................................. 35
- Configuring Check Point Blades and Management High Availability Failover .... 35

Check Point vSEC Gateway enforces adaptive security across virtual environments. It applies advanced Threat Prevention to block threats inside the Data Center, and, micro-segmentation, for access control inside the virtual environment.

⚠️ Important - Unless otherwise stated, all references to ESX throughout this document relate to ESXi.
Basic Deployment with Hypervisor mode

vSEC Gateway inspects all traffic that goes to, from, or inside the protected Security Group.

<table>
<thead>
<tr>
<th>Item</th>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ESX host</td>
<td>Multiple ESX hosts in an ESX cluster make the physical infrastructure</td>
</tr>
<tr>
<td>2</td>
<td>NSX</td>
<td>NSX manager defines Security Groups and redirection policy</td>
</tr>
<tr>
<td>3</td>
<td>vCenter Server</td>
<td>vCenter manages ESX hosts</td>
</tr>
<tr>
<td>4</td>
<td>vSEC Gateway</td>
<td>Inspects traffic between VMs in the Security Group, and traffic coming in and going out of the Security Group.</td>
</tr>
<tr>
<td>5</td>
<td>VMs</td>
<td>Virtual Machines</td>
</tr>
<tr>
<td>6</td>
<td>Protected Security Group</td>
<td>Collection of objects from the vSphere inventory, protected by NSX</td>
</tr>
<tr>
<td>7</td>
<td>Data Center core</td>
<td>Switching and routing infrastructure of the Data Center</td>
</tr>
<tr>
<td>8</td>
<td>Physical Security Gateway</td>
<td>Physical enforcement point</td>
</tr>
<tr>
<td>9</td>
<td>Security Management Server</td>
<td>SDDC aware Security Management Server</td>
</tr>
</tbody>
</table>
ESX Host Security Considerations

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

Check Point Best Practices:

- Always use different and secured networks for your vSphere server management.

- Give users only the access they need to do their work. For example, only VMware security administrators have access to the vSEC Gateway.

  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*.

Configuring the VMware Components

Before you start these procedures, install and configure the required VMware components. You can install more than one ESXi host.

⚠️ **Important** - All references to ESX are for ESXi.

Configuring Agent VM Host Settings

To use a local Datastore for the vSEC Gateway on multiple ESX hosts (recommended), or to use a non-distributed vSwitch for vSEC Gateway communication to the vSEC Management Server, you must configure Agent VM settings.

To configure Agent VM settings for each ESXi host in the Cluster:

1. In the vSphere Web Client, select the **Manage** tab for each host.
2. Go to **Agent VM settings > Edit**.
3. In the **Agent VM Settings** window, select a Datastore to hold the files for the vSEC Gateway Service VM.
   
   **Note** - We recommend that you deploy the vSEC Gateway on ESX Host local storage, and not on external storage.

4. In the **Agent VM Settings** window, select the Port Group network that connects to the vSEC Gateway Service VM, by default.

   This Port Group will be used for communication with the Management Server.
Adding the vCenter IP Address to the Runtime Settings
VMware requires that you add the vCenter IP address to the Runtime Settings tab on the vCenter Server setting page.

To add the vCenter IP address to the Runtime Settings:
1. In the vSphere Web Client, click vCenter > vCenter Servers and select the server.
2. Click Manage > Settings > General > Runtime settings.
3. Click vCenter Server managed address > Edit > Runtime settings.
4. In the Virtual Center Server managed address field, enter the vCenter server IP address.

Creating an ESX Cluster
You can use an existing cluster, or create a new cluster and add your ESXi hosts to it.

To create a cluster and add ESXi hosts to it:
1. Open the vSphere Web Client.
2. Open the Hosts and Clusters page (Home > Hosts and Clusters).
3. Right-click the vCenter, select New Data Center and enter a name.
4. Right-click the new Data Center, select New Cluster and enter a name.
5. Select the Turn On vSphere DRS option.
6. Configure other cluster parameters as necessary.
7. Click OK.
8. Right-click the new cluster and select Add Host.
9. Enter the ESXi host IP address, user name, and password.

Deploying the vSEC Gateway SVM
The vSEC Management Server must have network connectivity to the vCenter server, and NSX Manager.
The ESX hosts must have full connectivity with the vCenter server during the deployment procedure.

Installing the OVF
The vSEC Gateway package includes these files:
- `<file_name>.ovf`
- `<file_name>.vmdk`
- `<file_name>.mf`

Notes:
Make sure that there is connectivity between the OVF URL and the NSX server.
We recommend that you use md5sum to validate copied files.
To install the files:

1. Download the TGZ package from the vSEC Home Page
2. Extract the package and make sure that you get the contained files (OVF, VMDK, and MF).
3. Copy the files to one of these locations. If there is no ve folder, create one.
   - **Security Management Server:** "$FWDIR/VE/jetty/ve/
   - **Multi-Domain Server:** "$MDS_TEMPLATE/VE/jetty/ve/
     Make sure you copy the files to the Multi-Domain Server and not to a Domain Management Server.
   - **Third-party HTTP Server:** Copy the files to an HTTP server that can access the vCenter server.

**Best Practice** - For the Management Server High Availability, install vSEC OVF files on a third-party Server.

Update the URL of the vSEC Gateway OVF. You must set this URL to the file name with the .ovf extension.

## Configuring the vSEC Management Server Properties

Run this procedure only when you enter the `vsec config` for the first time.

To configure the vSEC Management Server properties:

1. Make sure you are connected to the NSX and vCenter servers. For connection instructions see Data Center Server (see "Connecting to a Data Center Server" on page 15).
2. Connect to the vSEC Management Server or Multi-Domain Server with a console or SSH client.
3. Run: `vsec config`
4. From the menu, select **VMware Configuration**.
5. Click y to accept the default settings of these parameters or click n to configure manually.
6. Enter the Service Manager **IP Address** (IP Address of the vSEC Management Server that is routable from the NSX Manager).
7. Enter the Service Manager Port.
8. Enter the OVF URL.
   When you upload the OVF to the vSEC Domain Management Server, the default URL is defined as `https://<server_IP>:<server_port>/ve/<ovf_file_name>`.
   If you upload the OVF to a different location, you must enter the URL.
9. To change these parameters, run: `vsec config`
10. Select **Change Global configuration**.
11. Press y to accept the default settings or n to configure manually.
Registering a vSEC Gateway Service

To register the service:

1. Connect to the vSEC Management Server with a console or SSH client.
   In a Multi-Domain Security Management environment, you must run the shell from a Domain Management Server, not from the Multi-Domain Server. In the Domain Management Server, log in to `expert` mode.
2. Run: `vsec config`
3. From the menu, click `Register Service`.
4. Select the NSX you want to register to.
5. Click `y` for the default configuration or click `n` for manual configuration:
   a) Enter the Service Name.
      - **Note** - The name must be unique and have less than 34 characters. The default name is Check Point vSEC Service.
   b) Select the Failure Policy.
      - Based on this policy, packets are accepted, or dropped, if the ESX kernel cannot communicate with the vSEC Gateway agent. This can occur when the vSEC Gateway is down, restarts or has an unexpected error.
      - The options are:
        - **Fail open** - All packets are accepted
        - **Fail close** - All packets are dropped
      - The default is Fail Close.
      - Click `y` to automatically create vSEC Gateway objects on the vSEC Management Server ("Automatic Provisioning of vSEC Objects" on page 29) and automatically assign the IP gateway address from the NSX IP Pool
      - Click `n` to manually create vSEC Cluster objects ("Manual Creation of vSEC Cluster Objects" on page 32).
6. Enter and confirm the default administrator password for the vSEC Gateway.
7. Enter and confirm the SIC one-time password.
8. Click `y` to register the service.

Deploying vSEC Gateway with the vSphere Web Client

After you complete service registration, you can deploy the vSEC Gateway with the vSphere Web Client. See the VMware documentation to learn more about service deployment.

Installing NSX on all Hosts

You must install the NSX on all hosts before deployment.

To install the NSX on all hosts:

1. Log in to the vSphere Web Client.
2. Select the vCenter Home view.
3. Select Networking and Security from the left panel.
4. Select the **Installation tab** from the left panel.
5. Click **Host Preparation** in the central panel.
6. Click **Install** for the NSX clusters.

**Creating a vSEC Gateway IP Address Pool**

We recommend that you create an IP address pool for automatic assignment of management interface IP addresses.

To create an IP address pool:

1. Log in to the vSphere Web Client.
2. Click **Networking & Security > NSX Managers**.
3. Click an **NSX Manager** in the **Name** column.
4. Click the **Manage** tab.
5. Click the **Grouping Objects > IP Pool**.
6. Click **Add New IP Pool**.
7. Enter a name for the IP pool and its default gateway.
8. Enter the primary and secondary DNS, DNS suffix and prefix length.
9. Enter the IP address ranges to be included in the pool.
10. Click **OK**.

**Deploying the Service**

This procedure uses an Agent VM ["Configuring Agent VM Host Settings" on page 24], for an environment with a local Datastore. If you use an external Datastore, have its details ready before you begin.

To deploy the service:

1. Select the **Installation** from the left panel.
2. Select the **Service Deployments** tab in the central panel.
3. Click **New Service [+]**, and select the service you created ["Registering a vSEC Gateway Service" on page 27].
4. Select the cluster where the service is to be deployed.
5. Select one of these as the SVM’s Datastore:
   - Specified on-host, to install the SVM on the Datastore as defined in Configuring Agent VM Host Settings [see “Configuring Agent VM Host Settings” on page 24].
   - Specified Datastore, available to all ESX hosts in the Cluster.
6. Select one of these management interface port groups:
   - Specified on-host, to use the port group defined in the Agent VM Host Settings.
   - A distributed port group, if you did not configure an Agent VM.
7. If you enabled the Automatic IP Pool ("Registering a vSEC Gateway Service" on page 27) feature or the Automatic Provisioning ("Automatic Provisioning of vSEC Objects" on page 29) feature:
   a) Click **Change** in the IP Assignment column of the applicable service.
   b) In the **Select an Assignment Mode** window, select **Use IP Pool**.
   c) Select an existing IP pool or create a new one here.
   d) Click **OK**.

8. Click **Finish**.

The system copies the OVF to the vCenter, and deploys it to all ESX hosts on the selected clusters.

**Note** - See the **Installation Status** in the **Service Deployments** tab, to monitor the progress of the deployment from the vSphere client.

If the Installation Status did not succeed:

- Click **Failed** to see the reason for the failure
- Click **Resolve** to resolve the issues

**Notes:**

If the Enable Agent task shows an error with the message **Cannot complete the operation**, you can safely ignore it. This is a known VMware limitation.

After the installation completes, the vSEC Gateway automatically reboots.

### Automatic Provisioning of vSEC Objects

When enabled, the Automatic Provisioning feature performs these actions:

- Creates vSEC objects (Clusters or Gateways) on the vSEC Management Server when it receives a notification from the NSX Server.
- Automatically initializes SIC between the vSEC Gateway and the vSEC Management Server.
- Installs the policy if the vSEC Cluster Object already has a policy.

To enable Automatic Provisioning:

1. Enable Automatic Provisioning when you register the service ("Registering a vSEC Gateway Service" on page 27).
2. Deploy the vSEC Gateway ("Deploying vSEC Gateway with the vSphere Web Client" on page 27).

**Note** - To enable Automatic Provisioning of SmartDashboard objects, make sure that no other clients are connected to the vSEC Management Server.
Configuring NSX to Redirect traffic to the vSEC Gateway

This procedure shows the basic steps to configure a Security Group. See the VMware documentation for conceptual information, detailed procedures and explanations of the different objects and options.

Creating a Security Group

To create a Security Group:

1. In the vSphere Web Client, click Networking and Security > Service Composer > Security Groups.
3. Enter a name and description for the new Security Group and click Next to continue.
4. Define dynamic memberships and objects to include in this Security Group.
5. On the Select objects to include and Select objects to exclude pages, select object types:
   - Security Groups
   - Clusters
   - Logical Switches
   - Legacy Port Groups
   - Networks
   - Virtual Applications (vApps)
   - Data Centers
   - IP Sets
   - MAC Sets
   - Security Tags
   - vNICS
   - Virtual Machines
   - Resource Pools
   - Distributed Port Groups

Objects that you select in this step are always included in the Security Group, even if these objects do not match the dynamic membership criteria.

Note - You can include other Security Groups in your new Security Group.
NSX IP Mappings for VMs

NSX redirection policies based on VM names or other dynamic attributes require IP mapping of the VMs.

You can map IPs using one of these options:

- Install VMware Tools on each VM to confirm that all traffic goes through vSEC Gateway. Make sure that VMware tools are running correctly.
- Use NSX 6.2 SpoofGuard DHCP snooping or ARP snooping abilities. These features allow NSX to enforce IP address-based security rules on VMs with no VMware Tools installed. See sk109460 http://supportcontent.checkpoint.com/solutions?id=sk109460.
- Use an IP Set to redirect traffic from a VM, without VMware tools. To redirect traffic for IP Sets, enable SpoofGuard and add the Inactive Virtual NIC IP address to the Approved IP list.

To create an IP Set:

1. In the vSphere Web Client, click Home > Networking & Security > NSX Managers.
2. In the center panel, select the NSX Manager and click IP Sets.
3. Click Add new IP Set (+).
4. In the Add IP Addresses window, enter a name, description and IP address for the new Security Group.
   This IP address is redirected to the vSEC Gateway.
5. Add the new IP set to the Security Group.

To enable SpoofGuard for the Port Group:

2. In the SpoofGuard panel, add a new policy or select an existing policy.
3. In the Policy > Settings panel, enable SpoofGuard.
4. In the Policy > Select Networks panel, click the (+) icon.
5. Select the applicable Port Group from the list.
6. In the lower section of the SpoofGuard pane, from the View list, select Inactive Virtual NICs.
7. Select the applicable Virtual NIC.
8. Enter the Virtual NIC IP address in the Approved IP field.
   This creates a policy exception that enables traffic redirection to an approved IP address.

Manual Configuration of the vSEC Gateway VM

This procedure is not necessary if you configured the system for Automatic Provisioning of vSEC Objects or Automatic assignment of IP addresses to vSEC Gateways.

To enable the Service VM after installation:

1. Login to each vSEC Gateway instance with a console, and run these commands:
   # set interface eth0 ipv4-address <ip> mask-length <length>
   # set static-route default nexthop gateway address <default_gw_ip> on
   # save config
2. Connect to each vSEC gateway and run the First Time Wizard.
Manual Creation of vSEC Cluster Objects

This procedure is not necessary if you enabled Automatic Provisioning of vSEC objects.

Create a cluster object with vSEC Gateway members. Each gateway will automatically have the license attached to the cluster.

Step 1: Create a Network Object to represent the cluster:
1. In the SmartDashboard > Network Objects tree, right-click Check Point.
2. Click Security Cluster.
3. Select Classic mode.
4. In the cluster properties, enter a name for the cluster.
5. Enter the cluster IP address.
   The cluster IP address is only used to define the object.
6. In General Properties > Network Security, make sure the ClusterXL and IPSec VPN Software Blades are not selected.
7. In the 3rd Party Configuration window, make sure that the Hide Cluster Members outgoing traffic behind Clusters IP address and Use State Synchronization are not selected.
8. In the Topology window, make sure Enable Extended Cluster AntiSpoofing is not selected.
9. In the properties > Network Security and Management tabs, select the applicable Software Blades.

Step 2: Add vSEC Gateway instances as cluster members:
1. In the cluster properties, open Cluster Members.
2. Click Add > New Cluster Member.
3. In the Cluster Member Properties window, enter a name and IP address.
4. Click Communication and enter the SIC internal communication password.

Step 3: Configure the topology of cluster members:
1. In the cluster properties, open Topology.
2. Click Edit > Get > All Members Interfaces With Topology.
3. Click Add network.
4. For each vSEC Gateway member, right-click the new interface and select Edit Interface.
5. Enter these values: eth1 as Name, an IP Address and a Netmask.
   This IP address is used only to create the cluster object. It is not the real IP address of the gateway.
7. Select Network defined by the interface IP and Net Mask.
8. Perform Anti-Spoofing based on interface topology.
9. Select eth1 Network Objective as 1st Sync.
Redirecting Traffic to the vSEC Gateway

Configure the NSX security policy to redirect traffic to Check Point entities. Create the rules in this policy in pairs:

- Rule for traffic from the Security Group (Source = Security Group)
- Rule for traffic to the Security Group (Destination = Security Group)

**Note** - You can also configure redirection rules from partner security services > Firewall.

To create and apply a new Security Policy:

1. In the vSphere Web Client, click **Networking and Security > Service Composer > Security Policies**.
2. Select the **Create Security Policy** icon.
   The **New Security Policy** wizard opens.
3. Click **Next** until the **Network Introspection Services** page shows.
4. Click the **Add Network Introspection Service** icon (+).
5. Enter the `<from_rule_name>` and description.
6. Select your **Service Name** and **Profile** that was created during registration ("Registering a vSEC Gateway Service" on page 27).
7. Set **Destination** to Any.
8. Set **Source** to **Policy's Security Groups**.
9. Add a new rule: enter the `<to_rule_name>` and description.
10. In the **Network Introspection Services** page, change the **Source** parameter to Any.
    The Destination parameter changes to **Policy's Security Groups**.
11. Select the **Service Name** and **Profile** that was created during registration.
12. Click **OK**.
13. Click **Finish**.
14. Select the new Security Policy and click **Apply Policy**.
15. In the **Apply Policy** window, select the Security Group and click **OK**.

   **Note** - You must not apply the security policy to more than one group.
Adding an ESX Host to a vSEC Protected ESX Cluster

You can add a new host to an ESX cluster. The procedure includes steps in both the vSphere Web client and SmartDashboard.

To add a new host to a cluster:

1. In the vSphere Web Client, right-click the ESX cluster object and select Add Host. vSEC Gateway is automatically installed on the new host.
2. Configure the Agent VM setting ("Configuring Agent VM Host Settings" on page 24) for the new host.
3. If you do not use an IP address pool or Automatic Provisioning:
   a) Run these commands from a console:
      
      ```
      # set interface eth0 ipv4-address <ip> mask-length <length>
      # set static-route default nexthop gateway address <default_gw_ip>
      # save config
      ```
      This sets the new vSEC Gateway IP address.
   b) Run the First Time Wizard.
4. Make sure there is connectivity between the cluster members and the Security Management Server. Resolve connectivity issues before you continue.

Do these steps if you did not enable Automatic Provisioning:

1. In SmartDashboard, add the new vSEC Gateway as a new member of the Check Point cluster object.
2. Establish SIC trust.
3. Install a policy from SmartDashboard to the cluster.

Removing a Host from a Cluster

To remove a host from a cluster:

1. In the vSphere Web Client, go to Hosts and Clusters.
2. Select the host.
3. Click Actions > Enter Maintenance Mode.
4. Move the host from the cluster to a Data Center.
5. Select the host.
6. Click Actions > Exit Maintenance Mode.
7. Reboot the ESX server to make sure that the changes are in effect.
8. If you did not enable Automatic Provisioning, remove the cluster member in SmartDashboard.
vMotion

vMotion lets you migrate active VMs between ESX hosts. You must configure network interfaces on source and target hosts.

For minimum impact on connectivity, applications, and security:

- The VMware distributed firewall on the target ESX host handles existing connections until they are closed or reset.
- The vSEC service that runs on the target ESX host secures new connections to and from the migrated VM.

⚠️ Important ⚠️

To maintain security:

- Initialize the sessions of the connections that need a control channel and a data channel.
- Re-initialize HTTPS connections after vMotion.

Configuring Check Point Blades and Management High Availability Failover

Configuring Application Control Policy

To use the Application Control Software Blade in vSEC:

1. In SmartDashboard, open Application Control and URL Filtering.
2. In the Rule Base, change the destination from Internet to Any.

Configuring Threat Emulation

Threat Emulation is a cloud service that copies files on to a VM and reports the results to a POD. Threat Emulation requires more disk space on the vSEC Gateway. If you see alerts about disk space, see sk92907 http://supportcontent.checkpoint.com/solutions?id=sk92907. To add more space, see to sk94671 https://supportcontent.checkpoint.com/solutions?id=sk94671.

To run Threat Emulation:

1. Click on the Threat Prevention tab.
2. Click Profiles > Edit > Threat Emulation Settings.
3. Select Inspect incoming and outgoing files.
4. Click OK.

If you see a SIC error during activation, disregard it.
Configuring Identity Awareness in vSEC

Configure vSEC to use Identity Awareness to see Security Group details in the vSEC logs. If you do not have the Identity Awareness blade enabled, you must enable Terminal Servers.

**To enable Terminal Servers:**

1. In SmartDashboard, open the **Firewall** tab.
2. Open the **Identity Awareness** tab, at the bottom.
3. Choose a Gateways & Servers.
   - The **Identity Awareness** window opens.
4. Select **Terminal Servers**.
5. Click **Settings**.
   - The Terminal Servers window opens.
6. Click **Edit**.
   - The Accessibility window opens.
7. Configure the portal to be accessible **Through all interfaces**.
8. Click **OK**.

**Management High Availability Failover**

Failover from an Active Management Server to the Standby Management Server is a manual procedure. You must manually synchronize the management servers before and after failover.

**To manually fail over a Security Management Server:**

1. In SmartDashboard connected to the Primary or Secondary Management Server, select **File > Policy > Management High Availability**.
2. Click **Synchronize**.
3. Click **OK**.
   - To learn more, see the *Synchronization Procedures* section in the *R77 Security Management Server Administration Guide*.
4. Start a manual failover:
   a) Change the Active Management Server to Standby.
   b) Change the Standby Management Server to Active.
   - To learn more, see the *Changing a Server to Active or Standby* section in the *R77 Security Management Server Administration Guide*.
5. On the new Active Management Server, run:
   ```bash
   # cpved stop
   # vsec config > change global parameters > Service Manager IP Address
   ```
   Follow the instructions on the screen to enter the new Service Manager IP address. The Service Manager IP address is the IP Address of the Security Management Server which is routable from NSX.
6. If the vSEC Gateway OVF URL is on your new Active Management Server, run:

vsec config > change global parameters > <ve_ovf_url>

Enter the OVF URL in this format:

https://<ip_address>:<port>/ve/<ovf_name>.ovf

**Note** - This step is only relevant for the addition of OVF files to the new Active Management Server. If you already have this feature, it must be changed in NSX.

7. Do steps 1 and 2 again to synchronize the management servers.
Uninstalling the vSEC Gateway Service

⚠️ **Important** - Do not use this procedure for an upgrade.
You must uninstall the vSEC Gateway service before you uninstall vSEC from the vSEC Management Server.

To uninstall the vSEC Gateway Service:

1. In the vSphere Web Client, go to Networking and Security > Service Composer > Security Policies.
2. Select the applicable policy.
3. Click Actions > Delete.
4. Remove the service deployment
   a) In the vSphere Web Client, go to Home > Networking and Security > Installation > Service Deployments.
   b) Select the service and click Delete service deployment (x).
5. Connect to the vSEC Management Server with a console or SSH client.
6. Run: `vsec config`
7. From the menu, click Remove Service.
8. Select the NSX and the services to delete from the list.
9. If you did not enable Automatic Provisioning, in SmartDashboard, delete the applicable cluster object.