Check Point
SOFTWARE TECHNOLOGIES LTD.

5 July 2017

VSEC CONTROLLER

R80.10

Administration Guide

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

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 Version of this Document

Download the latest version of this document
http://supportcontent.checkpoint.com/documentation_download?ID=54943.

To learn more, visit the Check Point Support Center
http://supportcenter.checkpoint.com.

Check Point R80.10

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

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 R80.10 Administration Guide.

Revision History

Date	Description
5 July 2017	Updated CPUSE instructions. ("vSEC Controller Monitoring and Troubleshooting").
06 June 2017	First release of this document

Contents

Terms

ARM

Azure Resource Manager. Technology to administer assets using Resource Group.

AWS

Amazon Web Services. Public cloud platform that offers global compute, storage, database, application and other cloud services.

Cisco ACI

Cisco Application Centric Infrastructure. Comprehensive SDN architecture, policy-based automation solution for increased scalability through a distributed enforcement system with greater network visibility. Trademark of Cisco ®.

Cisco APIC

Cisco Application Policy Infrastructure Controller. Automation and management point for the Cisco ACI fabric. It centralizes access to fabric information, optimizes the application lifecycle for scale and performance, and supports flexible application provisioning across physical and virtual resources.

Contract

In SDN, a policy between EPGs, with one EPG providing and one EPG consuming, to virtualize a physical network cable connection.

Data Center

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

ESX

A VMware physical hypervisor server that hosts one or more Virtual Machines (VMs) and other virtual objects. All references to ESX are also relevant for ESXi unless specifically noted otherwise. Trademark of VMware, Inc.

Microsoft Azure

Collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of datacenters managed by Microsoft.

NSX Manager

Basic network and security functionality for virtual computer environments. A VMware product family for SDN of Virtual Machines on the cloud (previously known as vShield). Trademark of VMware, Inc.

OpenStack

An open source cloud computing infrastructure for service providers and enterprises. It includes modules for administration, storage, networking and VM deployment and control.

Private Network (L3)

Similar to VRF, separates routing instances, and can be used as an admin separation.

Region

In AWS, a geographic area to place resources. Each region has multiple, isolated locations known as Availability Zones.

Resource Group for Microsoft Azure

Object used in ARM to monitor, control access, provision and manage billing for collections of assets that are required to run an application, or used by a client or company department.

SDDC

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

SDN

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

Security Group for AWS

Acts as a virtual firewall that controls the traffic for one or more instances. Security groups are associated with network interfaces.

Security Group for NSX

A collection of virtual objects that defines the NSX Distributed Firewall protection policy.

Service Graph

Ordered set of function nodes between terminals, which identifies network service functions required by an application. Required for vSEC integration.

Service Manager

Component that manages the communication between Check Point products, the vSEC Controller and the NSX, through the VMware REST API.

Tenant for ACI

Group of users, to isolate access to resources. Also known as *project*.

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.

vNIC

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

VPC

Virtual Private Cloud. A private cloud that exists in the public cloud of Amazon. It is isolated from other virtual networks in the AWS cloud.

vSEC Controller

Provisions SDDC 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. Security Gateway VE 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.

VSX

Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These virtual devices provide the same functionality as their physical counterparts.

VSX VS

Virtual device with the functionality of a physical Security Gateway with all supported Software Blades.

Introduction to the vSEC Controller

The vSEC cloud security solution delivers advanced threat protection to private or public cloud infrastructures. It controls and manages the security in both the physical and virtual environments with one unified management solution. With trusted APIs, the vSEC Controller connects to the Software-Defined Data Center (SDDC) and integrates the virtual cloud environment with Check Point Security Gateways. The vSEC Controller automatically updates the security policy on security logs. It updates GUI, API, and security logs with new and changed appliances, computers, devices, and addresses.

Check Point Security Gateways run on virtual machines. Deploy the gateway in the public and private cloud for perimeter and lateral protection, and industry-leading advanced threat prevention security. The vSEC Gateway integrates seamlessly with SDN solutions, such as VMware vCenter, VMware NSX, and Cisco ACI.

The vSEC Controller integrates with these virtual cloud environments:

- VMware vCenter
- VMware NSX
- Cisco ACI
- Amazon Web Services (AWS)
- Microsoft Azure
- OpenStack

Upgrading from the R80 vSEC Controller

To upgrade the vSEC Controller v1 and v2 to R80.10, see sk111841 http://supportcontent.checkpoint.com/solutions?id=sk111841 for upgrade instructions.

Important Information

1. When you upgrade the vSEC Controller to R80.10 the following files are overwritten with default values:
   - vSEC Controller v1
     - `vsec.conf` (found in `$VSECDIR/conf`)
   - vSEC Controller v2
     - `vsec.conf` (found in `$VSECDIR/conf`)
     - `tagger_db.C` (found in `$MDS_FWDIR/conf`)

   Before you begin the upgrade, back up any files that you have changed.
2. A Multi-Domain Server that contains imported Data Center objects in the Global Domain is not supported in the upgrade to R80.10. You must remove objects from the Global Domain before you install the upgrade.
3. Before you perform the upgrade on the Management server, if you have a Cisco APIC server, keep only one URL. After the upgrade, add the other URLs.
4. For upgrades from the vSEC Controller v1, manually connect again to each Data Center Server. For those servers that communicate with HTTPS, in SmartConsole double-click the Data Center object and trust the certificate again.

Note - During the upgrade, the vSEC Controller does not communicate with the Data Center. Therefore, Data Center objects are not updated on the Security Management Server or the Security Gateways.

Installing the vSEC Controller Enforcer Hotfix on Security Gateways

In This Section:

Installing the vSEC Controller Enforcer Hotfix on R77.30

Install the vSEC Controller Enforcer Hotfix on R77.30 Security Gateways with CPUSE, online or offline.

To install the Hotfix on R77.30 gateways with CPUSE online:

1. Open the Gaia Portal > **Upgrades (CPUSE)**.
2. Click **Status and Actions**.
3. Select the R77.30 vSEC Controller Enforcer Hotfix package.
4. Click the **More** button on the toolbar.
5. Click **Verifier**.
6. Select the vSEC Controller Enforcer Hotfix package.
7. Click **Install Update**.

   The online installation starts immediately. The gateway reboots when installation is complete.

To install the Hotfix on R77.30 gateways with CPUSE offline:

1. Install the latest build of CPUSE Agent from sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

   See *Section 3* to find the latest CPUSE build, and *Section 4-A* to download and import a CPUSE package.
2. Open the Gaia Portal > **Upgrades (CPUSE)**.
3. Click **Status and Actions**.
4. Click the **Import Package** button on the toolbar.

   The **Import Package** window opens.
5. Click **Browse** and go to the CPUSE package (offline TGZ file or exported TAR file).
6. Click **Upload**.
7. Above the list of all software packages, click **Showing Recommended packages**, and select **All**.
8. Select the imported package.
9. Click **More** > **Verifier**.
10. Select this package and click **Install Update**.

    The offline installation starts immediately. The gateway reboots when installation is complete.

Installing the vSEC Controller Enforcer Hotfix on R77.20

Use the CLI (Legacy) installation to install the R77.20 vSEC Controller Enforcer Hotfix on R77.20 Security Gateways.

To install the R77.20 vSEC Controller Enforcer Hotfix with CLI:

1. Download the R77.20 vSEC Controller Enforcer Hotfix package.
2. Extract the package on the gateway.
3. From the extracted folder, run: `fw1_wrapper_<HOTFIX_NAME>`
4. Follow the prompts.
5. Reboot the gateway.

Uninstalling the R77.20 and R77.30 Hotfix

To uninstall the Hotfix from R77.30 gateways:

1. Open the Gaia portal > **CPUSE** > **Status and Actions**.
2. Select the **vSEC Controller Hotfix** package.
3. Click **Uninstall**.

To uninstall the Hotfix from R77.20 gateways:

Run:

```
cd /opt/CPSuite-R77
./uninstall_fw1_wrapper_<HOTFIX_NAME>
```

For the correct file name, see sk111963
http://supportcontent.checkpoint.com/solutions?id=sk111963.

Activating the Identity Awareness Blade

In This Section:

Activating Identity Awareness for R80.10

For a Security Gateway to work with Data Center objects, enable the IDA Blade and the IDA API, and add 127.0.0.1 to the trusted clients list.

To activate Identity Awareness:

1. In SmartConsole, double-click the gateway. The **General Properties** window shows.
2. In the **Network Security** tab, select the Identity Awareness Software Blade.
   The **Identity Awareness Configuration** > **Methods for Acquiring Identity** window opens.
   Remove the **AD Query** selection if it is not necessary.
3. Select **I do not wish to configure an Active Directory at this time**.
   The Identity Awareness blade is activated by default.
4. Click **Next** > **Finish**.
5. From the **General Properties** window, select **Identity Awareness**.
6. From the **Identity Awareness** window, select **Identity Web API**.
7. Click **Settings**. The **Identity Web API Settings** window shows.
8. From the **Authorized Clients** section, add the 127.0.0.1 host object.
9. Enter a secret word in **Selected Client Secret**. Press **Generate** to create the client secret. Click **OK**.
10. Install the policy.

Activating Identity Awareness for R77.30 and R77.20

To work with Data Center objects, the Identity Awareness Blade and Terminal Server have to be enabled.

To activate Identity Awareness:

1. In SmartConsole, double-click the gateway. The **General Properties** window shows.
2. In the **Network Security** tab, select the Identity Awareness Software Blade.
   The **Identity Awareness Configuration** > **Methods for Acquiring Identity** window opens.
   Remove the **AD Query** selection if it is not necessary.
3. Select **Terminal Servers** > **Next**.
   The **Identity Awareness Configuration** > **Integration with Active Directory** window opens.
4. Select **I do not wish to configure an Active Directory at this time**.
   The Identity Awareness Software Blade is activated by default.

5. Click **Next** > **Finish**.
6. Install the policy.

To enable Identity Awareness on R77.30 Security Gateways, there must be communication between the vSEC Controller and the Identity Awareness daemon on the gateway. Run `pdp api enable`. On VSX gateways, run this command on every Virtual System.

Integrating with Data Center Servers

In This Section:

Enabling the vSEC Controller

In the R80.10 Security Management Server, the vSEC Controller is off by default.

To enable the vSEC Controller, run: `vsec on`

`vSEC turned on successfully` shows in the window.

To enable the vSEC Controller on the Security Management Server High Availability and the Multi-Domain Server High Availability, run: `vsec on` on each server

To disable the vSEC Controller, run: `vsec off.` When you disable the vSEC Controller, the vSEC Controller functionality will not work.

Connecting to a Data Center Server

The Management Server connects to the SDDC through the Data Center server object on SmartConsole.

To create a connection to the Data Center:

1. In SmartConsole, select **Objects** > **Object Explorer**.
2. Click **New** > **Server** > **Data Center**.
   The **Data Center Server** window opens.
3. Enter credentials and connection properties.
4. Click **Test Connection** to establish a secure connection.
   If the certificate window opens, confirm the certificate and click **Trust**.
5. When the **Connection Status** changes to **Connected**, click **OK**.
   If the status is not **Connected**, troubleshoot the issues before you continue ("vSEC Controller Monitoring and Troubleshooting" on page 30).

Note - If the connection properties of any Data Center servers such as credentials or the URL change, make sure to install the policy again.

Creating Access Rules with Data Center Objects

Define security policies with rules that include the Data Center objects.

Important - If the Management Server is not connected to the Data Center server, the Data Center objects will not import. To make sure the servers are connected, open the **Data Center Server** object in SmartConsole and see that the **Status** is **Connected**.

You can add Data Center objects to the Source and Destination of rules in the Access Control Policy and in the Threat Prevention Policy.

To add Data Center objects to Access Control Policy:

1. In SmartConsole, open **Security Policies**.
2. In a rule, in the **Source** or **Destination** column, click **+** to add new items.
3. Click **Import**.
4. Select a Data Center object, or click **New Data Center Server**.
5. In the window that opens, select the objects to add.
6. Install policy.

Data Center objects that are imported to the security policy are designed for well-defined groups of machines (EPGs, VMs, and so on).

Check Point Management API

The Check Point Management API includes Data Center commands to show Data Center Servers and their contents, and to show, delete, and import Data Center objects. Use the API to automate Data Center security management and monitoring.

There are different interfaces for the management API:

- SmartConsole command window
- `mgmt_cli` executable for Windows, Linux, Gaia
- Gaia secure shell (clish)
- Web services over HTTPS

Work with API documentation specific to the Data Centers on your local server:

1. In SmartConsole, select **Manage & Settings** > **Blades.**
2. In **Management API**, click **Advanced Settings.**
3. Change **Access Settings** to **All IP Addresses**. Click **OK**.
4. Publish.
5. In an SSH session, run: `api reconf`

   Now you can access `https://<`*management_IP*`>/api_docs`

To change the API configuration and to learn more, see the R80.10 API documentation https://sc1.checkpoint.com/documents/latest/APIs/#introduction~v1.1.

vSEC Controller for VMware Servers

To connect the vSEC Controller to a VMware vCenter or VMware NSX Data Center Server:

1. In SmartConsole, click **New object** > **More objects types** > **Server**.
2. Click **Data Center** > **New vCenter/New NSX**.
3. In the window that opens, **Hostname** field, enter the IP address or DNS name of the vCenter or NSX Manager server.
4. In **Username**, enter your VMware administrator username.
5. In **Password**, enter the password for the VMware administrator username.
6. Click **OK**.

vSEC Controller for vCenter

The Check Point Data Center Server connects to the VMware vCenter and retrieves object data. The vSEC Controller updates IP addresses and other object properties in the **Data Center Objects**.

You must have a VMware vCenter username with at least Read-Only permissions.

VMware vCenter Objects

VMware vCenter objects appear in the **Hosts and Clusters** view in the vCenter vSphere Web Client.

- **Cluster** - A collection of ESXi hosts and associated virtual machines configured to work as a unit.
- **Datacenter** - An aggregation of many object types required to work in a virtual infrastructure. These include hosts, virtual machines, networks, and datastores.
- **Folder** - Enables you to group similar objects.
- **Host** - The physical computer where you install ESXi. All virtual machines run on a host.
- **Resource pool** - Compartmentalizes the host or cluster CPU and memory resources.
- **Virtual machine** - A virtual computer environment where a guest operating system and associated application software runs.
- **vSphere vApp** - A packaging and managing application format. A vSphere vApp can contain multiple virtual machines.

Imported Properties	Description
IP	vCenter server IP address or DNS name **Note** - You must install VMware tools on each virtual machine to retrieve the IP addresses for each computer
Note	VMware vCenter object notes
URI	Object path

vSEC Controller for VMware NSX Manager Server

The vSEC Controller integrates the VMware NSX Manager Server with Check Point security. The Check Point Data Center Server connects to the VMware NSX Manager Server and retrieves object data. The vSEC Controller updates IP addresses and other object properties in the **Data Center Objects** group.

You must have a VMware NSX username with permission of an auditor or greater to access the vSEC Controller.

Note - This role is sufficient for vSEC Controller functionality. More permissions might be required for service registration (vSEC Gateway for NSX).

VMware NSX Objects

The VMware NSX Controller object is the Security Group. It enables a static or dynamic grouping based on objects such as virtual machines, vNICs, vSphere clusters, logical switches, and so on.

Imported Properties	Description
IP	All the security group IP addresses
Note	Description value of a security group
URI	Object path

Threat Prevention Tagging for vSEC Gateway for NSX

Threat Prevention Tagging

Threat Prevention Tagging automatically assigns Security Tags to Data Center objects based on Threat Prevention analysis and group affiliation. This enables the usage of dynamic Security Groups in policy rules.

Enable Threat Prevention Tagging for Anti-Bot and Anti-Virus services to the vSEC for NSX Gateway. When a threat from an infected VM reaches the gateway and is denied entry, it is tagged as an infected VM in the NSX Manager.

To apply Threat Prevention Tagging:

1. Deploy the vSEC Gateway for NSX service. See *vSEC Gateway for NSX Managed by the vSEC Controller* home page http://supportcontent.checkpoint.com/solutions?id=sk114518.
2. To enable Threat Prevention on the vSEC for NSX Gateway, see the *R80.10 Administration Guide* http://supportcontent.checkpoint.com/solutions?id=sk111841.

To activate tagging:

1. Run the command: `tagger_cli`
2. Select **Activate Cluster**.
   vSEC for NSX Clusters with active Anti-Bot and/or Anti-Virus blades on them, show.
3. Select the Cluster.
   Make sure **Cluster activated successfully** shows.

When it is activated, the Cluster automatically tags infected VMs in the NSX Manager Server. The

Security Tags are:

- Default Anti-Bot Security Tag: `Check_Point.BotFound`
- Default Anti-Virus Security Tag: `Check_Point.VirusFound`

The Security Tags are created automatically in the NSX Manager Server when the Cluster is activated.

When Security Tags are configured, you can create policy rules based on the Security Groups that contain those tags ("Creating Access Rules with Data Center Objects" on page 17).

Advanced options:

Use advanced menu options to configure the tags.

Show Activated Gateways - Lists the activated Clusters and the status of each vSEC for NSX Gateway.

Modify Anti-Bot Security Tag - Enable or disable the tagging for the Anti-Bot blade and change the Security Tag.

Modify Anti-Virus Security Tag - Enable or disable the tagging for the Anti-Virus blade and change the Security Tag.

Modify White List - IP Addresses listed in the White List are not tagged. (Split by spaces. Ranges are not accepted.)

Create New Security Tag - Creates a new Security Tag in the NSX Manager Server.

Update Data - When you add a new ESX to a Cluster, vSEC for NSX Gateway automatically updates the Threat Prevention Tagging data within 15 minutes. Select this option to manually update the data on the new vSEC for NSX Gateway.

Threat Prevention Tagging Logs

In SmartConsole, in the **Logs & Monitor** tab, see **vSEC Tagging** in the **Blade** column.

VM Tagged Successfully

The message below shows when Threat Prevention tagging successfully tagged the Virtual Machine due to malicious traffic.

`The Virtual Machine <`*vm_id*`> was tagged successfully with Security Tag '<`*tag_name*`>' in NSX <`*nsx_ip*`>`

Two VM IP Addresses with the Same IP in One ESX

The message below shows when an IP address appears twice in the ESX. This avoids false positive tags of Virtual Machines with duplicated IP addresses in one ESX.

`The IP address <`*vm_ip*`> appears twice in the ESX <esx_ip>. The infected Virtual Machine was not tagged`

vSEC Tagging Failed to Get Objects from the Data Center Repository

Symptom

There was an error getting a Data Center object from the R80.10 Security Management Server API.

```
Failed to get data from the Data Center <data_center_ip>
```

Solution

From SmartConsole, confirm there is a trusted connection for the vSEC Controller.

VM on the White List

The message below shows when the IP address of a Virtual Machine is on the White List. It is being ignored.

```
Threat Prevention Tag is ignored because the VM IP '<vm_ip>' is on the White List
```

vSEC Controller for Cisco ACI

The vSEC Controller integrates the Cisco ACI fabric with Check Point security. The Check Point Data Center Server connects to the ACI fabric and retrieves object data. The vSEC Controller updates IP addresses and other object properties in the **Data Center Objects** group. It supports the connection to an APIC cluster for redundancy.

To learn more, see R77.30 vSEC Gateway for ACI managed by the R80 vSEC Controller.

Prerequisites:

- You must have a Cisco ACI user role with at least tenant-epg read permissions.

  Note - This role is sufficient for vSEC Controller functionality. More permissions may be required for device package installation (vSEC for ACI).
- Enable Bridge Domain unicast routing to enable IP address learning for EPGs on the Cisco APIC.
- Define a subnet on the Bridge Domain to help the fabric maintain IP address learning tables. This prevents time-outs on silent hosts that respond to periodic ARP requests.

Connecting to Cisco ACI APIC Data Center Server

To connect to a Cisco ACI APIC Data Center Server:

1. In SmartConsole, click **New object** > **More objects types** > **Server**.
2. Click **Data Center** > **New APIC**.
3. In the window that opens, **New APIC Server**, enter the addresses of APIC cluster members, delimited with a semicolon.

   Important: The addresses can be HTTP or HTTPS, but not mixed.
4. In **Username**, enter your APIC service username.

   If you use login domains for APIC authentication, the username format is:
   `apic:<domain>\<username>`
5. In **Password**, enter the password for the APIC username.
6. Click **OK**.

Cisco APIC Objects

- **Tenant** - A logical separator for customers, BU, groups, traffic, administrators, visibility, and more.
- **Application Profile** - A container of logically related EPGs, their connections, and the policies that define those connections.
- **End-Point Group (EPG)** - A container for objects that require the same policy treatment. Examples of these are app tiers or services (usually VLAN).
- **L2 Out** - A bridged external network.
- **L2 External EPG** - An EPG that represents external bridged network endpoints.

vSEC Controller for Microsoft Azure

The vSEC Controller integrates the Microsoft Azure cloud with Check Point security. The Check Point Data Center Server connects to the Microsoft Azure cloud and retrieves object data. The vSEC Controller updates IP addresses and other object properties in the **Data Center Objects** group.

Connecting to Microsoft Azure

You must authenticate and connect to your Microsoft Azure account to pull objects. You can use Service Principal Authentication or Microsoft Azure Active Directory User Authentication.

- Service Principal Authentication (default)
  a) **Application ID** - Enter your Service Principal application ID in the UUID format.
  b) **Application Key** - Enter the Service Principal secret.
  c) **Directory ID** - Enter the Tenant ID from the Service Principal in the UUID format.

  You can create the Service Principal with the Azure portal, Azure Powershell and the Azure CLI.
- Microsoft Azure Active Directory User Authentication
  a) **User name** - Enter as <*username*>@<*domain*>. The needed account type is a *work* or *school* account.
  b) **Password** - Enter the password for your Microsoft Azure account.

The minimum recommended permission is Reader. You can assign Reader permission to all Resource Groups that you want to pull an item from, or add the permission on a subscription level.

Note - If you have less permissions, some of the functionality might not work.

Microsoft Azure Objects

- **Subscription** - Helps you organize access to your cloud components.
- **Virtual Network** - Represents your Microsoft Azure Virtual Network (VNET) in the cloud.
- **Subnet** - A range of IP addresses in a VNET. A VNET can be divided into many subnets.
- **Virtual Machine (VM)** - Virtual computing environments.
- **Virtual Machine Scale Set (VMSS)** - Manages sets of VMs.
- **Resource Group** - Holds the components of your subscription as a group.
- **Network Security Group (NSG)** - NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to the VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet.

Importing Objects in Microsoft Azure

To connect to the Microsoft Azure Data Center Server:

1. In SmartConsole, select **Objects** > **More objects types** > **Server**.
2. Click **Data Center** > **Azure**.

3. Select one of the authentication modes, **Service Principal** or **Azure AD User**. Click **OK**.
4. Import objects from your Microsoft Azure server to your policy.
   - **Network by Subscriptions** - Import VNETS, subnets, VMs or VMSSs.
   - **Network Security Groups (NSG) -** Import all IP addresses that belong to a specific NSG. The NSG is used only as a container for the list of all IPs (NICs and subnets) that are attached to this group.
   - **Tags** - Imports all the IP addresses of VMs and VMSSs that have specific tags and values.

   Note - All changes in Microsoft Azure are updated automatically with the Check Point security policy. Users with permissions to change Resource Tags in Microsoft Azure may be able to change their access permissions.
5. Install the Policy.

Imported Properties	Description
Name	Name of the object and of the object Resource Group. Format is: obj_name (obj_resource_group_name) The user can edit the name after importing the object.
Name in Server	Name of the object and of the object Resource Group. Format is: obj_name (obj_resource_group_name)
Type in Server	Object type.
IP Address	VMs or VMSS IP addresses. In the case of subnets, NSGs or Tags, the field contains a list of all the IPs in the container.
Note	Contains the address prefixes for VNETs and subnets.
URI	Object path.
Tags	Keys and Values attached to the Object.
Location	Physical location in Microsoft Azure.

Auto Scaling in Microsoft Azure

The Microsoft Azure Auto Scaling service with the Check Point Auto Scaling group can increase or decrease the number of vSEC Gateways according to the current load.

The vSEC Controller for Microsoft Azure can work with the Check Point Auto Scaling Group. The Check Point Management Server can update Data Center objects automatically on the Check Point Auto Scaling group.

Enable the Identity Awareness Blade as explained in *Auto Scaling in Microsoft Azure*, sk115533 http://supportcontent.checkpoint.com/solutions?id=sk115533, Section *6-A - Enabling additional Software Blades.*

vSEC Controller for Amazon Web Services

The vSEC Controller integrates the Amazon Web Services (AWS) cloud with Check Point security. The Check Point Data Center Server connects to the AWS cloud and retrieves object data. The vSEC Controller updates IP addresses and other object properties in the **Data Center Objects** group.

Configuring Permissions for Amazon Web Services

AWS Authentication

User Authentication - Uses **Access Key ID** and **Secret Access Key** credentials.

Role Authentication - Uses the AWS IAM role. You can use this option only when Security Management is deployed in AWS.

Minimal permissions from the User or Role:

- Effect: Allow
- Actions:
  - ec2:DescribeInstances
  - ec2:DescribeNetworkInterfaces
  - ec2:DescribeSubnets
  - ec2:DescribeVpcs
  - ec2:DescribeSecurityGroups
- Resource: All ("*")

For more information about Roles and the IAM policy, see *Amazon Web Services documentation* http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html.

Connecting to the Amazon Web Services Data Center Server

To connect to an AWS Data Center server:

1. In SmartConsole, click **New object** > **More objects types** > **Server**.
2. Click **Data Center** > **New AWS**.
3. Select the authentication method, **User Authentication** or **Role Authentication**.
4. If you choose **User Authentication**, enter your **Access Key ID** and **Secret Access Key**.
5. Select the **AWS region** to which you want to connect.
6. Click **OK**.

Amazon Web Services Objects

- **VPC** - Amazon Virtual Private Cloud enables you to launch resources into your virtual network.
- **Availability Zone** - A separate geographic area of a region. There are multiple locations with regions and availability zones worldwide.
- **Subnet** - All the IP addresses from the Network Interfaces related to this subnet.
- **Instance** - Virtual computing environments.
- **Tags** - Groups all the instances that have the same Tag Key and Tag Value.
- **Security Group** - Groups all the IP addresses from all the Network Interfaces associated with this Security Group.

Use one of these options to import AWS objects to your policy:

- **Regions** - Import AWS VPCs, subnets or instances from a certain region, to your security policy.
- **Security Groups** - Import all IP addresses that belong to a specific security group. The Security Group is used only as a container for the list of all IP addresses that are attached to this group.
- **Tags** - Import all instances that have a specific Tag Key or Tag Value.

Notes:

- Tags with Key and no Value are in the vSEC Controller as: "**Tag key=**"
- Leading and trailing spaces in Tag Keys and Values will be truncated.
- All changes in AWS are updated automatically with the Check Point security policy. Users with permissions to change resource tags in AWS may be able to change their access permissions.

Object Names

Object names are the same as those in the AWS console. VPC, subnet, instance, and Security Group are named as follows:

- Tag Name exists: "Object ID (value of the Tag Name)"
- Tag Name does not exist or is empty: "ObjectID"

Imported Properties	Description
Name	Resource name as shown in the AWS console. User can edit the name after importing the object.
Name in Server	Resource name as shown in the AWS console.
Type in Server	Resource type.
IP	Associated private and public IP addresses.
Note	CIDR for subnets and VPC objects.
URI	Object path.
Tags	Tags (Keys and Values) that are attached to the object.

Auto Scaling in Amazon Web Services

The AWS Auto Scaling service with the Check Point Auto Scaling group can increase or decrease the number of vSEC Gateways according to the current load.

The vSEC Controller for AWS works with the Check Point Auto Scaling Group. The Check Point Security Management Server updates Data Center objects automatically on the Check Point Auto Scaling group.

Enable the Identity Awareness Blade as explained in *Auto Scaling in AWS (Amazon Web Services)*, sk112575 http://supportcontent.checkpoint.com/solutions?id=sk112575, Section *5-E - Enabling additional Software Blades.*

vSEC Controller for OpenStack

The vSEC Controller integrates the Check Point Security Management Server with OpenStack Keystone. The Check Point Data Center server connects to OpenStack and retrieves network object data from OpenStack Neutron.

Connecting to an OpenStack Server

To connect to the OpenStack server:

1. In SmartConsole, select **Object Explorer**.
2. Click **New** > **More** > **Server** > **Data Center** > **OpenStack**.
   The Data Center window opens.
3. Enter credentials and connection properties:
   a) **Hostname** - The URL of your OpenStack server in this format:
   `http(s)://1.2.3.4:5000/<keystone_version>`
   Example: `https://1.2.3.4:5000/v2.0`
   Note - If you do not know your keystone URL, use this command to find it:
   `openstack endpoint show keystone | grep publicurl`
   b) **Username** - Username for the OpenStack server.
   c) **Password** - Password for your Username.
4. Select **Test Connection** to establish a secure connection.
   If the certificate window opens, confirm the certificate and click **Trust**.
5. When the connection status changes to **Connected**, click **OK**.
   If the status is not **Connected**, troubleshoot the issue before you continue ("vSEC Controller Monitoring and Troubleshooting" on page 30).

OpenStack Objects

- **Instances** - VMs inside the cloud.
- **Security groups** - Sets of IP address filter rules for networking access. They are applied to all instances within a project.
- **Subnet** - A block of IP addresses and associated configuration states. Subnets are used to allocate IP addresses when new ports are created on a network.

Imported Property	Description
IP	VM - VM IP address Security Group - IP addresses of the VMs inside the group Subnets - IP addresses of the VMs inside the subnet
Note	Instances - Empty Security Group - Description of the group Subnet - IP address and mask of the subnet
URI	Object path

vSEC Controller Monitoring and Troubleshooting

In This Section:

Traffic Logs

You can see vSEC Controller logs as traffic logs in the SmartConsole **Logs & Monitor** tab.

Notes:

- When a Data Center object matches a rule, vSEC Controller puts the object **name**, the **Source** or **Destination** fields, (not the **IP address**), in the log details.
- If an object from a higher level in the hierarchy is in the rule base, vSEC uses the lowest possible object in the log that matches the IP address.

Security Logs and Troubleshooting

This section describes notifications and issues in the SmartConsole **Logs & Monitor**.

Start Data Center Server Mapping

This message shows when the Check Point vSEC Controller successfully connects to a Data Center and begins to map all the Data Center objects:

"`Mapping of Data Center server url` *<url>* `with user` *<user>* `started`"

End Data Center Server Mapping

This message shows when the Check Point vSEC Controller completes mapping all Data Center objects, and begins to monitor Data Center changes:

"`Mapping of Data Center server url` *<url>* `with user` *<user>* `finished.`"

Data Center Objects Updated on Gateway

This message shows every time a Data Center object is successfully updated on the Security Gateway:

"`Data center server objects were successfully updated on gateway` *<name>*"

Connection Lost to Data Center Server

Symptom

Lost Data Center Server connection, possibly due to connectivity issues.

"Connection lost to Data Center server url *<url>* with user *<user>*."

Solution

Click Data Center **Test Connection** and verify the connection.

"Connection lost to Data Center server url *<url>* with user *<user>*."

Install Policy Failure

Symptom

The install policy process completed correctly, but the log shows this message:

"Failed to update policy with data center objects. Install policy again to resolve the issue."

There is corrupt policy data with a Data Center object.

Solution

Install policy again.

No Data Center Connectivity

Symptom

Persistent connectivity issues between the Management Server and the vSEC Controller to the Data Center Server exist. This message shows:

"Connectivity to data center server *<ip>* lost. Objects imported from this data center server are no longer being updated."

Solution

Resolve connectivity issues.

Failed Gateway Update

Symptom

vSEC Controller fails to update a gateway. There is no connectivity with the gateway. This message shows:

"Failed to update data center server objects on gateway *<name>*"

Solution

- Make sure there is SIC between the Security Gateway and the vSEC Controller.
- Make sure that the Identity Awareness API is enabled on the Security Gateway.

Gateway Policy Failure

Symptom

When a vSEC Controller fails to transfer a policy to a gateway, this message shows:

"`Failed to generate data center server objects of new policy, Security gateways are no longer updated with the new data center objects`"

Solution

Install policy again.

High Availability Failover - Fails to Stop Secondary Management

Symptom

When the vSEC Controller stops data transmission to gateways from a secondary management server, this message shows:

"`Failed to stop updates of data center objects on the secondary management server`"

Solution

Install policy again.

High Availability Failover - Fails to Start Primary Management

Symptom

When the vSEC Controller fails to start updating policies to the gateways, this message shows:

"`Failed to start updates from previous standby domain`"

Solution

Install policy again.

Multi-Domain Security Management – Delete Domain Failure

Symptom

When the vSEC Controller fails to stop Domain enforcement when a Domain is deleted, this shows:

"`Failed to stop updates of data center objects for deleted domain. Contact Check Point Support`"

Solution

Install policy again. If the issue persists, contact your Check Point partner or technical support.

Reset Security Gateway vSEC Controller State Tool

Symptom

Security Gateway data is deleted unpredictably.

Solution

The Security Gateway is not synchronized with the vSEC Controller data.

Use the `vsec_controller_cli` utility to reset the vSEC Controller state on the Security Gateway.

To reset the state:

1. On the management server, run: `vsec_controller_cli`
2. Select: `Resend enforcement data to gateway`
3. Select the gateway to reset.

Note - If data is not synchronized after reset, contact your Check Point partner or Technical Support.