Setting Up a Virtual Secure Gateway Application Container

This chapter contains the following sections:

Virtual Secure Gateway Application Containers

Cisco Virtual Secure Gateway (VSG) container type is used to provide enhanced security in virtual environments. You can use Cisco UCS Director to configure a Prime Network Services Controller (PNSC) in addition to its internal firewall (Cisco Virtual Security Gateway), which is then integrated into an application container.

Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. Cisco VSG enables a broad set of multi-tenant workloads that have varied security profiles to share a common compute infrastructure in a virtual data center private cloud or in a public cloud. By associating one or more virtual machines (VMs) into distinct trust zones, Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

Cisco VSG provides the following benefits:

- Trusted Multi-tenant Access—Granular, zone-based control and monitoring with context-aware security policies applied in a multi-tenant (scale-out) environment to strengthen regulatory compliance and simplify audits. Security policies are organized into security profile templates to simplify their management and deployment across many Cisco VSGs.
- Dynamic operation—On-demand provisioning of security templates and trust zones during VM instantiation and mobility-transparent enforcement and monitoring as live migration of VMs occur across different physical servers.
- Non-disruptive administration—Administrative segregation across security and server teams while enhancing collaboration, eliminating administrative errors, and simplifying audits.

Cisco VSG does the following:

- Enhances compliance with industry regulations.
- Simplifies audit processes in virtualized environments.
- Reduces cost by securely deploying a broad set of virtualized workloads across multiple tenants on a shared compute infrastructure, whether in virtual data centers or private/public cloud computing environments.

Virtual Security Gateway Application Container Prerequisites

The following is the prerequisite for the VSG Container configuration:

- When executing the Allocate Container VM Resources task, the default virtual network type is Distributed Virtual Portgroup N1K for VSG container. Ensure that you modify the primary DVSwitch name for VSG container.

Virtual Security Gateway Application Container Limitations

VSG Application Container Creation Process

Adding a PNSC Account

PNSC is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco virtual services. Designed for multiple-tenant operation, the PNSC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. The PNSC essentially provides the security component (firewall) to your VSG and application container, and separates the VMs from each other. The PNSC enables the centralized management of Cisco virtual services to be performed by an administrator through Cisco UCS Director.

Note PNSCs are not tied to any specific pod.

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add (+)**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Account Type field	Choose PNSC as the account type and click **Submit**.
Account Name field	The multi-domain account name.

Name	Description
Description field	The description of the multi-domain account.
Server Management drop-down list	From the drop-down list, choose **All Servers** or **Selected Servers** to manage servers accordingly.
Server Address field	The IP address of the PNSC server.
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	This field appears only when the **Use Credential Policy** check box is unchecked. The user ID to access the account.
Password field	This field appears only when the **Use Credential Policy** check box is unchecked. The password associated with the username.
Shared Secret Password field	This field appears only when the **Use Credential Policy** check box is unchecked. The pre-shared secret key of the account.
Transport Type drop-down list	This field appears only when the **Use Credential Policy** check box is unchecked.Choose a transport type: • HTTP**—**A standard protocol. • HTTPS**—**A standard and secure protocol.
Port field	This field appears only when the **Use Credential Policy** check box is unchecked. The port number (based on the transport type).
Contact Email field	The email address of the administrator or person responsible for this account.
Location field	The location of the device associated with the account.

Step 5 Click **Submit**.

Viewing PNSC Reports

After creating a PNSC account, you can view related reports using Cisco UCS Director.

The following reports are available under the **Physical** > **Network** menu.

- Summary
- Tenants
- vDCs
- vApps
- PNSC Firewall Policies
- VM Manager
- Clients
- HA ID Usage Report

Step 1 Choose **Physical** > **Network**.

Step 2 Expand **Multi-domain Manager**.
You can view PNSC accounts that were added under the Multi-domain Manager accounts.

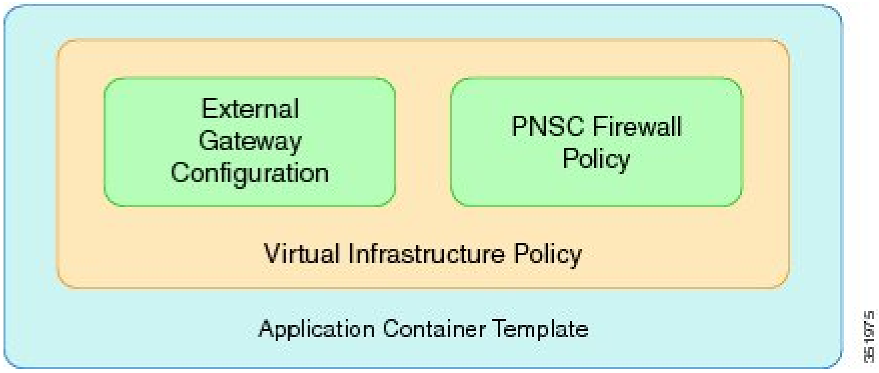
Step 3 Click a PNSC entry to view the available reports.

Integrating a VSG into an Application Container

You can use Cisco UCS Director to configure a PNSC in addition to its internal firewall (Cisco Virtual Security Gateway), which is then integrated into an application container.

The integration process consists of several stages:

- Upload an OVA file into Cisco UCS Director.
- Create a PNSC firewall policy (used to create a container with a PNSC).
- Create a virtual infrastructure policy. This policy defines which virtual account to use and what type of containers you want to provision.
- Create an application container template. This template uses the virtual infrastructure policy, computing policy, storage policy, and network policy as inputs into the template.


External Gateway Configuration
PNSC Firewall Policy
Virtual Infrastructure Policy
Application Container Template
351975

Uploading OVA Files

Cisco UCS Director allows an administrator, a group administrator, or an end user to upload OVA files to a predefined storage location.

Note Group administrators and end users are the only types with privileges to upload OVA files.

Before You Begin

Ensure that you have the proper access rights.

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **User OVF Management**.

Step 3 Click **Upload File**.

Step 4 On the **Upload File** screen, complete the following fields:

Name	Description
Folder Type drop-down list	The type of folder containing the OVA file. Choose one of the following: • Public—Choose this role to only reveal public files. • User—Choose this role if you are an end user. End users are not granted extensive privileges. The user role is well suited for first-level support, in which problem identification, remediation, and escalation are the primary goals. • Group—This role can deploy OVA files.
File Name field	The name of the OVA file to upload and display.
File field	Drop the OVA file or click **Select a File** to browse and choose the required file.
File Description field	The description of the file (if required).

Step 5 Click **Submit**.

Creating a PNSC Firewall Policy

You use a firewall policy to enforce network traffic on a Cisco VSG. The Cisco VSG is the internal firewall used as part of PNSC. A key component of the Cisco VSG is the policy engine. The policy engine uses the policy as a configuration that filters the network traffic that is received on the Cisco VSG.

Note The PNSC firewall policy supports both standalone and high availability (HA) modes.

Step 1 Choose **Physical** > **Network**.

Step 2 Expand **PNSC accounts** listed under **Multi-Domain Managers**.

Step 3 Click PNSC account for which you want to create a firewall policy.

Step 4 Click **PNSC Firewall Policies**.

Step 5 Click **Add**.

Step 6 On the **Create Firewall Policy** screen, complete the following fields:

Name	Description
Policy Name field	A unique name for the firewall policy.
Policy Description field	A description of the firewall policy.

Step 7 Click **Next**.

Step 8 Expand PNSC Zones and click **Add (+)** to create a zone.

Step 9 On the **Add Entry to PNSC Zones** screen, complete the following fields:

Name	Description
Zone Name field	A unique name for the zone.
Zone Description field	A description of the zone.
Zone Conditions	Expand **Zone Conditions** and click **Add** to add the zone condition.
Attribute Type drop-down list	Choose Network or VM as the type of attribute.
Attribute Name drop-down list	Choose the attribute from the list which varies according to the attribute type.
Operator drop-down list	Choose a type of operator.

Name	Description
Attribute Value field	Enter the attribute value based on the chosen attribute type.

Step 10 Click **Submit**.

Step 11 Click **Next**.

Step 12 Expand **PNSC ACL Rules** and click **Add (+)** to create a PNSC ACL rule entry.

Step 13 On the **Add Entry to PNSC ACL Rules** screen, complete the following fields:

Name	Description
Name field	The name of the ACL rule. The name must be unique to the container.
Description field	The description of the ACL rule.
Action drop-down list	The type of action allowed for the rule. Choose one of the following: • **Permit—**Permits use on the matching traffic. • **Drop—**Drops use of the rule on the matching traffic. • **Reset—**Resets the rule on the matching traffic.
Condition Match Criteria drop-down list	Choose a condition that need to be met.
Protocol/Service drop-down list	Choose protocol or service from the list.
Any Protocol check box	If checked, the rule applies to all protocols. If unchecked, you must specify the operator ('equals', 'notequals') and protocol (for example, IP or EGP).
Source Conditions	
Attribute Type drop-down list	Choose the type of attribute.
Attribute Name drop-down list	Choose the name of the attribute from the drop-down list that vaies as per the attribute type.
Operator drop-down list	Choose the type of operator.
Attribute Value field	The attribute value.
Destination Conditions	
Attribute Type drop-down list	Choose the type of attribute.

Name	Description
Attribute Name drop-down list	Choose the name of the attribute from the drop-down list that vaies as per the attribute type.
Operator drop-down list	Choose the type of operator.
Attribute Value field	The attribute value.

Step 14 Click **Submit**.

Step 15 Click **Next**.

Step 16 On the **PNSC-VSG Configuration** screen, complete the following fields:

Name	Description
Use Unified Fabric check box	Check the check box to use unified fabric.
VSG OVF URL drop-down list	Choose an OVA file from the list of OVA files that are uploaded to Cisco UCS Director.
Admin Password for the VSG field	The administrator password for the VSG.
Policy agent shared secret Password field	The policy agent shared password.
Deployment mode drop-down list	The type of deployment. Choose one of the following: • **Standalone—**Standalone mode. • **HA—**High availability mode.
VSG HA Id field	The VSG HA ID. The available range is 1-4095.
Network Type drop-down list	Choose the network type from the list.
VLAN ID Range field	The VLAN ID range (for example, 100-199).
Use same vlan/vxlan check box	If checked, uses the same VLAN ID or VXLAN ID for both VSG HA and Data port groups.
Name field	The name of the VSG.
Primary VSG Section (HA mode only)	
Name field	The name of the primary VSG.

Name	Description
Deployment Configuration drop-down list	The deployment configuration. Choose one of the following: • **Deploy Small VSG** • **Deploy Medium VSG** • **Deploy Large VSG**
Disk Format drop-down list	The format to store the virtual disk. Choose one of the following: • **Thick Provision Lazy Zeroed** • **Thick Provision Easy Zeroed** • **Thin Provision**
Secondary VSG (HA mode only)	
Name field	The name of the primary VSG.
Deployment Configuration drop-down list	The deployment configuration. Choose one of the following: • **Deploy Small VSG** • **Deploy Medium VSG** • **Deploy Large VSG**
Disk Format drop-down list	The format to store the virtual disk. Choose one of the following: • **Thick Provision Lazy Zeroed** • **Thick Provision Easy Zeroed** • **Thin Provision**

Step 17 Click **Submit**.

Step 18 Click **OK**.

Creating a Virtual Infrastructure Policy

The virtual infrastructure policy defines which VM to use and what type of container you want to provision. This policy also defines which PNSC account you want to tie to this particular account.

Note Any gateway-related Linux based VM image parameters can be added to this policy.

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Virtual Infrastructure Policies**.

Step 3 Click **Add Policy (+)**.

Step 4 On the **Create a virtual infrastructure policy** screen, complete the following fields:

Name	Description
Policy Name field	The unique name for the virtual infrastructure policy.
Policy Description field	The description of the virtual infrastructure policy.
Container Type drop-down list	Choose the VSG container type.
Select Virtual Account drop-down list	Choose a virtual account (cloud).

Step 5 Click **Next**.

Step 6 On the **Virtual Infrastructure Policy - PNSC Information** screen, complete the following fields:

Name	Description
PNSC Account field	Expand the PNSC accounts and choose a PNSC account.
VSG Template Configuration section	
PNSC Firewall Policy drop-down list	Choose a firewall policy.

Step 7 Click **Next**.

Step 8 On the **Virtual Infrastructure Policy - Fencing Gateway** screen, complete the following fields:

Name	Description
Gateway Required check box	Check this box if gateway is required.
Select Gateway Policy drop-down list	This field appears only when the **Gateway Required** check box is chosen. Choose a gateway policy.
Gateway Summary	Displays a summary of the gateway set for the virtual infrastructure policy.

Step 9 Click **Next**. The **Virtual Infrastructure Policy - Summary** screen appears, displaying your current settings.

Step 10 Click **Submit**.

Creating an Application Template for a VSG

Step 1 Choose **Policies** > **Application Containers**.

Step 2 On the **Application Containers** page, click **Application Container Templates**.

Step 3 Click **Add Template**. The **Add Application Container Template** page appears. Complete the following fields:

Name	Description
Template Name field	The name of the new template.
Template Description field	The description of the template.

Step 4 Click **Next**. The **Application Container Template - Select a Virtual Infrastructure policy** screen appears. In this screen, you choose the cloud on which the application container is deployed. Complete the following field:

Name	Description
Select Virtual Infrastructure Policy drop-down list	Choose a virtual infrastructure policy to deploy to the container.

Step 5 Click **Next**. The **Application Container: Template - Internal Networks** screen appears.

Note Only one network is allowed per VSG container.

Step 6 Click **Add (+)** icon to add a network. The **Add Entry to Networks** screen appears. Complete the following fields:

Name	Description
Network Name field	The network name. The name should be unique within the container. You can use a maximum of 128 characters.
Network Type drop-down list	Choose the network type.
Information Source drop-down list	Choose the information source from the list.
VLAN ID Range field	The VLAN ID range. This value controls the number of containers that can be cloned or created.
Network IP Address field	The network IP address for the container.

Name	Description
Network Mask field	The network mask.
Gateway IP Address field	The IP address of the default gateway for the network. A NIC with this IP address is created on the GW VM. **Note** The IP address is configured on the inside interface of the gateway.

Step 7 Click **Submit**.
Next, you can add and configure the gateway VM that will be provisioned in the application container.

Step 8 Click **OK**.

Step 9 Click **Next**.
The **Application Conatiner Template - VMs** screen appears.

Step 10 Click **Add (+)** to add a VM. Complete the following fields:

Name	Description
VM field	The name of the VM. The full name contains the container name as well as this name.
Description field	The description of the VM.
Provision VM using Content Library Template check box	Check to view and choose a VM template from the content library VM templates. If unchecked, you have to choose VM template from VM image templates.
Content Library VM Template field	This field appears only when the **Provision VM using Content Library VM Template** check box is checked. Expand the list and choose a VM template from the content library.
VM Image drop-down list	This field appears only when the **Provision VM using Content Library Template** check box is unchecked. Choose an image to be deployed.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs to be allocated to the VM.
Memory drop-down list	Choose the amount of memory (in MB) to be allocated to the VM.
CPU Reservation (MHz) field	The CPU reservation for the VM in Mhz.
Memory Reservation (MB) field	The memory reservation for the VM.
Disk Size (GB) field	The custom disk size for the VM. To use the template disk size specify the value of zero. The specified disk size overrides the disk size of the selected image. **Note** If this value is less than template size, this value is ignored.

Name	Description
VM Password Sharing Option drop-down list	Choose an option on how to share the VM's username and password with the end users. If **Share after password reset** or **Share template credentials** is chosen, the end user needs to specify a username and password for the chosen templates.
Use Network Configuration from Image check box	If checked, the network configuration from the image is applied to the provisioned VM.
VM Network Interfaces field	Expand VM Network Interafces and choose the VM network interface information. If you are adding another network interface, go to Step 11.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quantity field	The number of VM instances to provision when the container is created. **Note** Each VM will have a unique name and IP address.

Step 11 (Optional) Click **Add (+)** to add a new (multiple) VM network interface. Complete the following fields:

Name	Description
VM Network Interface Name field	The name of the VM network interface.
Select the Network drop-down list	Choose a network.
IP Address field	The IP address of the network.

Step 12 Click **Next**.

Step 13 Click **Ok**.
The **Application Container Template - External Gateway Security Configuration** screen appears. You can specify the security configuration components, such as port mapping and outbound access control lists (ACLs).

Step 14 Click **Add (+)** to add a port mapping. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol for the port mapping.
Mapped Port drop-down list	Choose the mapped port for the selected protocol.
Remote IP Address field	The IP address of the remote machine.
Remote Port field	The remote machine port number.

Step 15 Click **Submit**.

Step 16 Click **OK**.

Step 17 Click **Add (+)** icon to add an Outbound ACL, in the **Application Container Template - External Gateway Security Configuration** screen. Complete the following fields:

Name	Description
Protocol drop-down list	Choose a protocol.
Select Network drop-down list	The network to which the rules need to apply.
Source Address field	The source classless inter domain routing (CIDR) IP address.
Destination Address field	The destination CIDR IP address.
Action field	The action that is applied on the matching network traffic.

Step 18 Click **Submit**.

Step 19 Click **OK**.

Step 20 Click **Next**.

Step 21 On the **Application Container Template - Deployment Policies** screen, complete the following fields:

Name	Description
Compute Policy drop-down list	Choose a policy to deploy all of the compute components of the virtual container.
Storage Policy drop-down list	Choose a policy to deploy all of the storage components of the virtual container.
Network Policy field	Choose a policy to deploy to the container gateway. Hosts considered to be part of the computing policy should be associated with the Cisco Nexus 1000 (used to deploy Cisco VSG). **Note** This field is only used for the outside interface of the container gateway. Also, resource allocation should be associated with a Cisco Nexus 1000 Series switch.
Systems Policy field	The value used for DNS and other OS license configurations.
Cost Model field	Choose a cost model.
Use common network policy check box	Check the check box to use the common network policy defined above for the VSG management network.
Management Network Policy drop-down list	If the **Use common network policy** is unchecked, choose a network policy for the VSG management network.

Step 22 Click **Next**.

Step 23 On the **Application Container Template - Options** screen, complete the following fields:

Name	Description
End User Self-Service Policy drop-down list	Choose an end user self-service policy applicable for the application container template.
Enable Self-Service Deletion of Containers check box	If checked, enables self-service deletion of containers.
Enable VNC Based Console Access check box	If checked, enables VNC-based console access to VM.
Technical Support Email Addresses field	Enter the comma-separated list of email addresses of individuals who should receive emails regarding the container provisioning.

Step 24 Click **Next**.

Step 25 Choose a workflow to setup the container.

Step 26 Expand the workflow list and select a workflow (for example, Workflow Id 431 Fenced Container Setup - VSG).

Note A workflow should contain allocated resources. For example, if it is a VSG workflow it should contain a Cisco Nexus 1000 Series resource.

Step 27 Click **Select**.

Step 28 Click **Submit**.