Securing Containers Using a PNSC and a Cisco VSG

This chapter contains the following sections:

About Prime Network Service Controllers

Prime Network Services Controller (PNSC) is a virtual appliance, based on Red Hat Enterprise Linus (RHEL), that provides centralized device and security policy management of the Cisco Virtual Security (VSG) and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall.

Note The Cisco Virtual Security Gateway works within the PNSC.

Designed for multi-tenant operation, PNSC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. Multi-tenancy refers to the architectural principle that calls for a single instance of the software to run on a Software-as-a-Service (SaaS) server, serving multiple client organizations or tenants. Multi-tenancy is contrasted with a multi-instance architecture, where separate instances are set up for different client organizations. With a multi-tenant architecture, a software application is designed to virtually partition data and configurations, so that each tenant works with a customized virtual application instance.

The components of a PNSC are listed below:

- Creating a Prime Network Service Controller (PNSC) account within Cisco UCS Director.
- Collecting PNSC objects in the inventory.
- Providing PNSC object inventory reports.
- Supporting PNSC object actions.
- Supporting PNSC object workflow tasks.

You can also use Cisco UCS Director to manage your VSGs.

Note In order to see your PNSC configuration, you should download the vCenter extension file from the PNSC and import that into your vSphere client application. After completing that download, execute a PNSC inventory from within Cisco UCS Director. The VM Manager report (under PNSC) will display the corresponding vCenter information.

Adding a PNSC Account

Cisco Prime Network Services Controller (Cisco Prime NSC) 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, Cisco Prime NSC 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 Cisco Prime Network Services Controller 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 On the menu bar, choose **Administration** > **Physical Account**.

Step 2 Click the **Multi-Domain Manager Account** tab.

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

Step 4 In the **Multi-Domain Manager Account** dialog box, complete the following fields:

Name	Description
Account Name field	The multi-domain account name.
Description field	Description of the multi-domain.
Account Type field	Description of the account. Choose PNSC.
Server Address field	The IP address of the PNSC server.
User ID field	The administrator's user ID.
Password field	The administrator's user password.
Transport Type drop-down list	Choose a transport type: • HTTP: standard protocol. • HTTPS: standard and secure protocol.
Port field	The port number (based on the transport type).

Name	Description
Description field	A description of the account.
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 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 On the menu bar, choose **Physical > Network** .
The **All Pods** screen appears.

Step 2 In the left-hand pane, click the **Multi-domain Manager**.
The PNSC account entry appears.

Step 3 Click the **Network Accounts** tab.
You can view PNSC accounts that were added under either the Default datacenter or the Multi-domain Manager accounts.

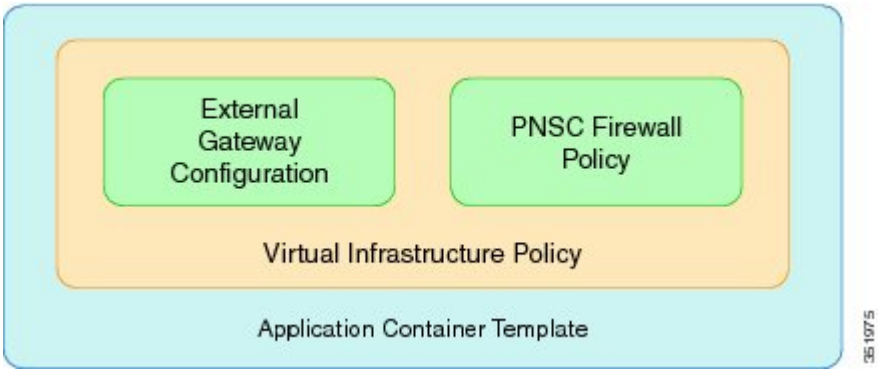
Step 4 Click on a PNSC entry to view the available reports.

Integrating a VSG into an Application Container

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.

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 (as shown below).



The Cisco Virtual Security Gateway (VSG) is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments. The Cisco VSG enables a broad set of multi-tenant workloads that have varied security profiles, so that they can 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, the Cisco VSG ensures that access to trust zones is controlled and monitored through established security policies.

The Cisco VSG provides the following benefits:

- Trusted multi-tenant access—Zone-based control and monitoring with context-aware security policies in a multi-tenant (scale-out) environment to strengthen regulatory compliance and simplify audits. Security policies are organized into security profiles 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—Administration segregation across security and server teams that provides collaboration, eliminates administrative errors, and simplifies audits.

The Cisco VSG does the following:

- Provides compliance with industry regulations.
- Simplifies audit processes in a virtualized environment.

- Reduces cost by securely deploying virtualized workloads across multiple tenants on a shared compute infrastructure, whether in virtual data centers or private/public cloud computing.

Uploading OVA Files

Cisco UCS Director allows an administrator, group administrator, or 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 On the menu bar, choose the **Administration** tab.

Step 2 Click the **Upload Files** tab.

Step 3 Click **Upload File**.

Step 4 In the **Upload File** dialog box, 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.
Select a file for upload field	Browse to choose the required file. Click **OK** when the **File Upload** confirmation dialog box appears.
File Description field	The description of the file (if required).

Step 5 Click **Submit**.

Step 6 When the **Once Submit Result - Upload Successfully** dialog box appears, click **OK**. Uploaded files are accessible under the **Upload Files** tab.

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 On the menu bar, choose **Physical > Network**.

Step 2 Click the **Network Accounts** tab.

Step 3 Click on the PNSC account.

Step 4 Click on the **PNSC Firewall Policies** tab.

Step 5 Click **Add**.

Step 6 In the **Create a firewall policy** dialog box, 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 Click **Add (+)** to create a zone.

Step 9 In the **Add Entry to PNSC Zones** dialog box, complete the following fields:

Name	Description
Zone Name field	A unique name for the zone.
Zone Description field	A description of the zone.
Rules Section	
Attribute Type field	The type of attribute.
Attribute Name field	The name of the attribute.
Operator field	The type of operator.
Attribute Value field	The attribute value.

Step 10 Click **Submit**.

Step 11 Click **OK**.

Step 12 Click **Next**.

Step 13 Click **Add (+)** to create a PNSC ACL rule entry.

Step 14 In the **Add Entry to PNSC ACL Rules** dialog box, 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.
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 field	The type of attribute.
Attribute Name field	The name of the attribute.
Operator field	The type of operator.
Attribute Value field	The attribute value.
Destination Conditions	
Attribute Type field	The type of attribute.
Attribute Namefield	The name of the attribute.
Operator field	The type of operator.

Step 15 Click **Submit**.

Step 16 Click **Next**.

Step 17 In the **PNSC-VSG Configuration** pane, complete the following fields:

Name	Description
Configuration Section	
VSG OVF URL drop-down list	The URL of the OVF file.
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.
VLAN ID Range field	The VLAN ID range (for example, 100-199).
Use same vlan check box	If checked, uses the same VLAN 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.
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.

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**

Step 18 Click **Submit**.

Step 19 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 On the menu bar, choose **Policies** > **Application Containers**.

Step 2 Click the **Virtual Infrastructure Policies** tab.

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

Step 4 In the **Create a virtual infrastructure 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.
Container Type drop-down list	Choose a container type. For virtual infrastructure policies, choose VSG.

Name	Description
Select Virtual Account drop-down list	Choose a virtual account (cloud).

Step 5 Click **Next**.

Step 6 In the **Modify Virtual Infrastructure policy** screen, complete the following fields:

Name	Description
PNSC Account drop-down list	Choose a PNSC account.
VSG Template Configuration section	
PNSC Firewall Policy drop-down list	Choose a policy.

Step 7 Click **Next**.

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

Name	Description
Gateway Type drop-down list	Choose a PNSC account.
VM Image for the Gateway drop-down list	Choose a VM.
Number of Virtual CPUs drop-down list	Choose the number of virtual CPUs.
Memory drop-down list	Choose the amount of memory to allocate to the VM.
CPU Reservation in MHz field	The CPU reservation for the VM.
Memory Reservation in MB field	The memory reservation for the VM.
Root Login for the Template field	The root login for the template.
Root Password for the Template field	The root password for the template.
Gateway Password Sharing Option drop-down list	Choose a sharing option for the gateway.

Step 9 Click **Submit**.

Creating an Application Template for a VSG

Step 1 On the menu bar, choose **Policies** > **Application Containers**.

Step 2 Click the **Application Container Templates** tab.

Step 3 Click **Add Template**. The **Create a Application Container Template** screen 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 section 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 the **(+) Add** icon to add a network. The **Add Entry to Networks** dialog box 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.
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.
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 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 **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.
VM Image drop-down list	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 0. 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.
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 Interface field	Choose the VM network interface information. If you are adding another network interface, go to Step 9.
Maximum Quantity field	The maximum number of instances that can be added in this container after it is created.
Initial Quality 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 - Security Configuration** screen appears. You can specify the security configuration components, such as port mapping and outbound access control lists (ACLs).

Step 14 Click the **Add (+)** icon 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 internal system.
Remote Port field	The remote machine's port number.

Step 15 Click **Submit**.

Step 16 Click **OK**.

Step 17 Click the **Add (+)** icon to add an Outbound ACL. The **Application Container: Template - Security Configuration** dialog box appears. 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 In the **Application Container Template - Deployment Policies** page, 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** was unchecked, choose a network policy for the VSG management network.

Step 22 Click **Next**.

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

Name	Description
Enable Self-Service Power Management of VMs check box	If checked, enables self-service power management of VMs.
Enable Self-Service Power Resizing of VMs check box	If checked, enables self-service resizing of VMs.
Enable Self-Service VM Snapshot Management check box	If checked, enables self-service snapshot management of VMs.
Enable Self-Service Deletion of VMs check box	If checked, enables self-service power deletion of VMs.
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.

Name	Description
Technical Support Email Addresses field	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 In the **Select** table choose 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**.