Overview

This chapter contains the following sections:

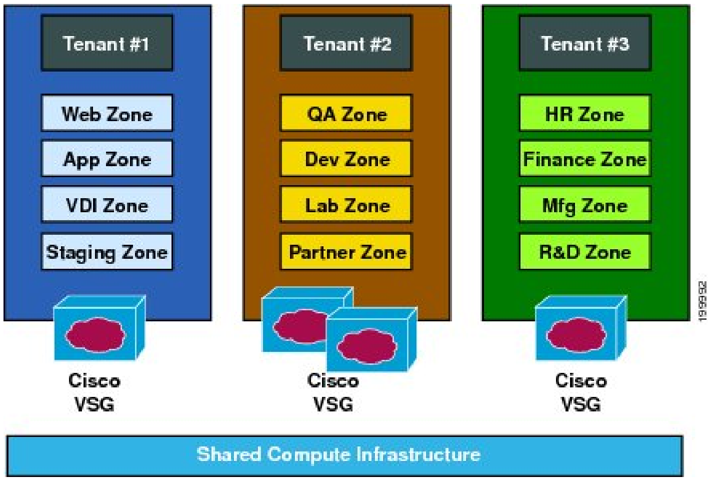
Information About Installing Cisco PNSC and Cisco VSG

You must install Cisco Prime Network Services Controller (PNSC) and Cisco VSG in a particular sequence on the Cisco Nexus 1000V switch to have a functioning virtual system.

Information About Cisco VSG

Cisco VSG is a virtual firewall appliance that provides trusted access to virtual data center and cloud environments with dynamic policy-driven operation, mobility-transparent enforcement, and scale-out deployment for dense multi-tenancy. 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. The following figure shows the trusted zone-based access control that is used in per-tenant enforcement with Cisco VSG.

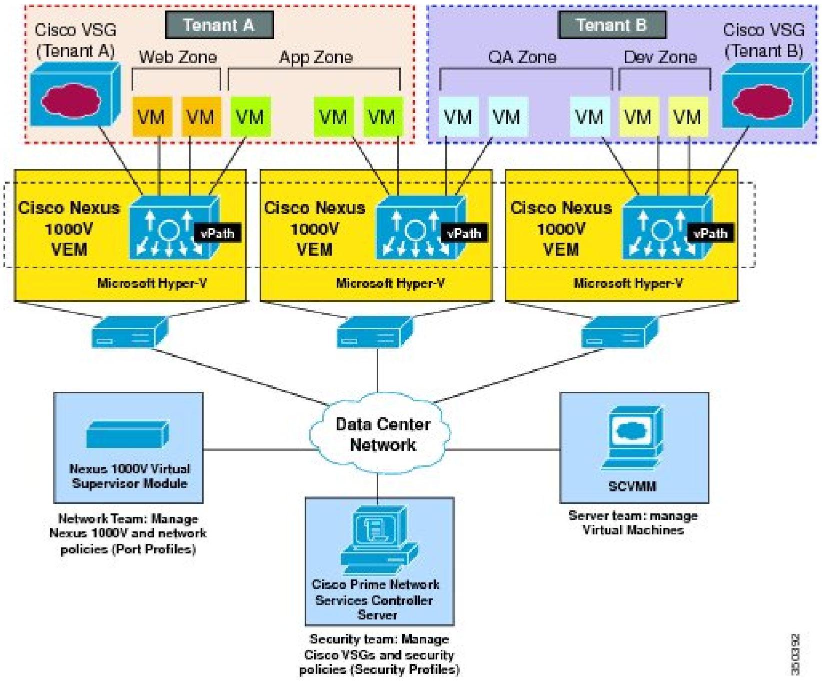
Figure 1: Trusted Zone-Based Access Control Using Per-Tenant Enforcement with Cisco VSG



Cisco Prime NSC and VSG Architecture

Cisco VSG operates with Cisco Nexus 1000V Series switch on KVM on Red Hat Enterprise Linux OpenStack Platform and leverages the virtual network service data path (Cisco vPath). Cisco vPath steers traffic, whether external-to-VM or VM-to-VM, to Cisco VSG of a tenant. Initial packet processing occurs in Cisco VSG for policy evaluation and enforcement. After the policy decision is made, Cisco VSG offloads policy enforcement of the remaining packets to Cisco vPath.

Figure 2: Cisco Virtual Security Gateway Deployment Topology



Cisco vPath supports the following features:

- Tenant-aware flow classification and subsequent redirection to a designated Cisco VSG tenant
- Per-tenant policy enforcement of flows offloaded by the Cisco VSG to Cisco vPath

Cisco VSG and the VEM provide the following benefits:

- Each Cisco VSG can provide protection across multiple physical servers, which eliminates the need for you to deploy a virtual appliance per physical server.
- By offloading the fast-path to one or more Cisco vPath Virtual Ethernet Modules (VEMs), Cisco VSG enhances security performance through distributed Cisco vPath-based enforcement.
- You can use Cisco VSG without creating multiple switches or temporarily migrating VMs to different switches or servers. Zone scaling, which is based on security profiles, simplifies physical server upgrades without compromising security or incurring application outages.
- For each tenant, you can deploy Cisco VSG in an active-standby mode to ensure that Cisco vPath redirects packets to the standby Cisco VSG when the primary Cisco VSG is unavailable.
- You can place Cisco VSG on a dedicated server so that you can allocate the maximum compute capacity to application workloads. This feature enables capacity planning to occur independently and allows for operational segregation across security, network, and server groups.

Trusted Multitenant Access

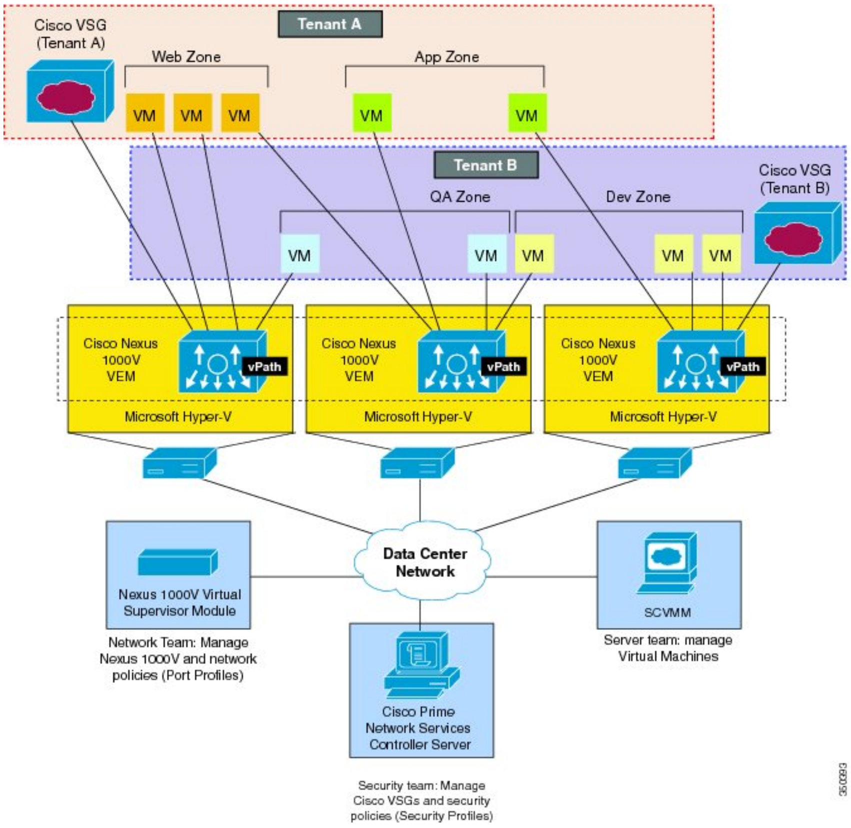
You can transparently insert a Cisco VSG into the Microsoft Hyper-V environment where Cisco Nexus 1000V is deployed. One or more instances of Cisco VSG is deployed on a per-tenant basis, which allows a highly scale-out deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. You can deploy Cisco VSG at the tenant level in Hyper-V and manage each tenant instance using Microsoft System Center Virtual Machine Manager (SCVMM).

As you instantiate VMs for a given tenant, their association to security profiles (or zone membership) occurs immediately through binding with the Cisco Nexus 1000V port profile. Each VM is placed upon instantiation into a logical trust zone. Security profiles contain context-aware rule sets that specify access policies for traffic that enters and exits each zone. You can apply controls to zone-to-zone traffic and to external-to-zone (and zone-to-external) traffic. Zone-based enforcement occurs within a VLAN because a VLAN often identifies a tenant boundary. The Cisco VSG evaluates access control rules and then offloads enforcement to the Cisco Nexus 1000V VEM vPath module. Upon enforcement, Cisco VSG can permit or deny access and can generate optional access logs. Cisco VSG also provides policy-based traffic monitoring capability with access logs.

Dynamic Virtualization-Aware Operation

A virtualization environment is dynamic, where frequent additions, deletions, and changes occur across tenants and across VMs. The following figure shows how the structured environment can change over time due to dynamic VMs.

Figure 3: Cisco VSG Security in a Dynamic VM Environment, Including VM Live Migration



Cisco VSG operating with Cisco Nexus 1000V (and Cisco vPath) supports a dynamic VM environment. When you create a tenant with Cisco VSG (standalone or active-standby pair) on Cisco Prime NSC, associated security profiles are defined that include trust zone definitions and access control rules. Each security profile is bound to a Cisco Nexus 1000V port profile (authored on the Cisco Nexus 1000V Virtual Supervisor Module (VSM) and published to Microsoft SCVMM.

When a new VM is instantiated, the server administrator assigns appropriate port profiles to the virtual Ethernet port of the VM. Because the port profile uniquely refers to a security profile and VM zone membership, Cisco VSG immediately applies the security controls. You can repurpose a VM by assigning it to a different port profile or security profile.

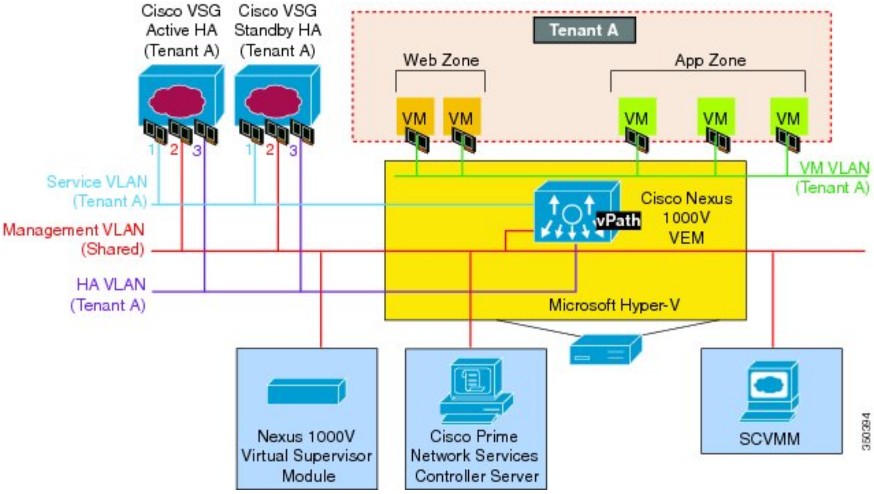
As VM migration events are triggered, VMs move across physical servers. Because Cisco Nexus 1000V ensures that port profile policies follow the VMs, associated security profiles also follow these moving VMs, and security enforcement and monitoring remain transparent to the migration events.

Setting Up Cisco VSG and VLAN

You can set up Cisco VSG in an overlay fashion so that VMs can reach Cisco VSG irrespective of its location. The Cisco vPath component in Cisco Nexus 1000V VEM intercepts the packets from the VM and sends them to Cisco VSG for further processing.

Figure 4: Cisco Virtual Security Gateway VLAN Usages

In the following figure, Cisco VSG connects to three different VLANs (service VLAN, management VLAN, and HA VLAN). Cisco VSG is configured with three vNICS—data vNIC (1), management vNIC (2), and HA vNIC (3)—with each of the vNICs connected to one of the VLANs through a port profile.



The VLAN functions are as follows:

- The service VLAN provides communications between Cisco Nexus 1000V VEM and Cisco VSG through a physical router. Cisco VSG data interface and VEM interface are configured on different subnets. All the Cisco VSG data interfaces are part of the service VLAN and the VEM interacts with Cisco VSG using the router.

- The management VLAN connects the management platforms such as ????Microsoft SCVMM????, Cisco PNSC, Cisco Nexus 1000V VSM, and managed Cisco VSGs. The Cisco VSG management vNIC is part of the management VLAN.

- The HA VLAN provides the heartbeat mechanism and identifies the active and standby relationship between the Cisco VSGs. The Cisco VSG vNICs are part of the HA VLAN.

You can allocate one or more VM data VLANs for VM-to-VM communications. In a typical multi-tenant environment, the management VLAN is shared among all the tenants and the service VLAN, HA VLAN, and the VM data. VLANs are allocated on a per-tenant basis. However, when VLAN resources become scarce, you might decide to use a single VLAN for service and HA functions.

Information About Cisco Prime NSC

Cisco PNSC virtual appliance is based on Red Hat Enterprise Linux (RHEL), which provides centralized device and security policy management of Cisco VSG for Cisco Nexus 1000V Series switch. Designed for multi-tenant operation, Cisco PNSC provides seamless, scalable, and automation-centric management for virtual data center and ???cloud environments???. With a web-based GUI, CLI, and XML APIs, Cisco PNSC enables you to manage Cisco VSGs that are deployed throughout the data center from a centralized location.

Note Multi-tenancy is when a single instance of the software runs on a Software-as-a-Service (SaaS) server, serving multiple client organizations or tenants. In contrast, multi-instance architecture has separate software instances set up for different client organizations. With a multi-tenant architecture, a software application can virtually partition data and configurations so that each tenant works with a customized virtual application instance.

Cisco PNSC is built on an information model-driven architecture, where each managed device is represented by its sub-components.

Cisco Prime NSC Key Benefits

Cisco PNSC provides the following key benefits:

- Rapid and scalable deployment with dynamic, template-driven policy management based on security profiles.
- Seamless operational management through XML APIs that enable integration with third-party management tools.
- Greater collaboration across security and server administrators, while maintaining administrative separation and reducing administrative errors.

Cisco Prime NSC Components

Cisco PNSC architecture includes the following components:

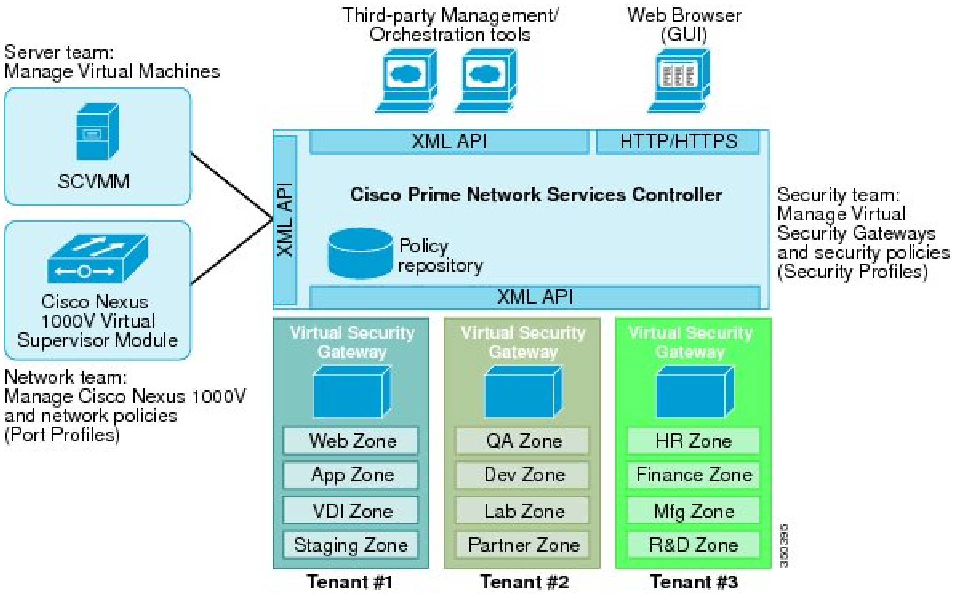
- A centralized repository for managing security policies (security templates) and object configurations that allow managed devices to be stateless.
- A centralized resource management function that manages pools of devices that are commissioned and pools of devices that are available for commissioning. This function simplifies large scale deployments as follows:
    - Devices can be pre-instantiated and then configured on demand
    - Devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools

- A distributed management-plane function that uses an embedded management agent on each device that allows for a scalable management framework.

Cisco Prime NSC Architecture

The Cisco PNSC architecture includes the components in the following figure:

Figure 5: Cisco Prime NSC Components


Third-party Management/ Orchestration tools
Web Browser (GUI)
Server team: Manage Virtual Machines
SCVMM
XML API
HTTP/HTTPS
XML API
Cisco Prime Network Services Controller
Policy repository
XML API
Security team: Manage Virtual Security Gateways and security policies (Security Profiles)
Cisco Nexus 1000V Virtual Supervisor Module
Network team: Manage Cisco Nexus 1000V and network policies (Port Profiles)
Virtual Security Gateway
Web Zone
App Zone
VDI Zone
Staging Zone
Tenant #1
Virtual Security Gateway
QA Zone
Dev Zone
Lab Zone
Partner Zone
Tenant #2
Virtual Security Gateway
HR Zone
Finance Zone
Mfg Zone
R&D Zone
Tenant #3
350395

Cisco Prime NSC Security

Cisco PNSC uses security profiles for tenant-centric template-based configuration of security policies. A security profile is a collection of security policies that are predefined and applied on an on-demand basis at the time of Virtual Machine (VM) instantiation. These profiles simplify authoring, deployment, and management of security policies in a dense multi-tenant environment, reduce administrative errors, and simplify audits.

Cisco Prime NSC API

The Cisco PNSC API allows you to coordinate with third-party provisioning tools for programmatic provisioning and management of Cisco VSGs. This feature allows you to simplify data center operational processes and reduce the cost of infrastructure management.

Cisco Prime NSC and VSG

Cisco PNSC operates with the Cisco Nexus 1000V Series VSM to achieve the following scenarios:

- Security administrators who author and manage security profiles as well as manage Cisco VSG instances. Security profiles are referenced in Cisco Nexus 1000V Series port profiles through Cisco PNSC interface.
- Network administrators who author and manage port profiles as well as manage Cisco Nexus 1000V Series switches. Port profiles are referenced in ?????Microsoft SCVMM???? through the Cisco Nexus 1000V Series VSM interface.

- Server administrators who select the appropriate port profiles in ?????Microsoft SCVMM???? when instantiating a virtual machine.

System Requirements

System requirements for Cisco Prime NSC are as follows:

- Microsoft Windows Server with SCVMM 2012 SP1, SCVMM 2012 R2, or SCVMM 2016.
- Intel VT that is enabled in the BIOS.
- 4 GB RAM for Prime NSC ISO installation.
- One of the following, depending on InterCloud functionality:
    - With InterCloud functionality, 220 GB on shared network file storage (NFS) or storage area network (SAN), and configured on two disks as follows:
        - Disk 1: 20 GB
        - Disk 2: 200 GB
    - Without InterCloud functionality, 40 GB on shared NFS or SAN, and configured on two disks as follows:
        - Disk 1: 20 GB
        - Disk 2: 20 GB
- Adobe Flash Player plugin 11.2 or higher.
- Any of the following browsers:
    - Internet Explorer 9.0 or higher
    - Mozilla Firefox 23.0 or higher
    - Google Chrome 29.0 or higher

  Access to Cisco Prime NSC application using a Web browser and the following ports (if the deployment uses a firewall, make sure to permit the following ports):

    - 443 (HTTPs)
    - 80 (HTTP/TCP)
    - 843 (Adobe Flash)

Note If you are running Firefox or IE and do not have Flash, or you have a version of Flash that is older than 11.2, a message displays asking you to install Flash and provides a link to the Adobe website.