Overview

This chapter includes the following sections:

Cisco Virtual Network Management Center Overview

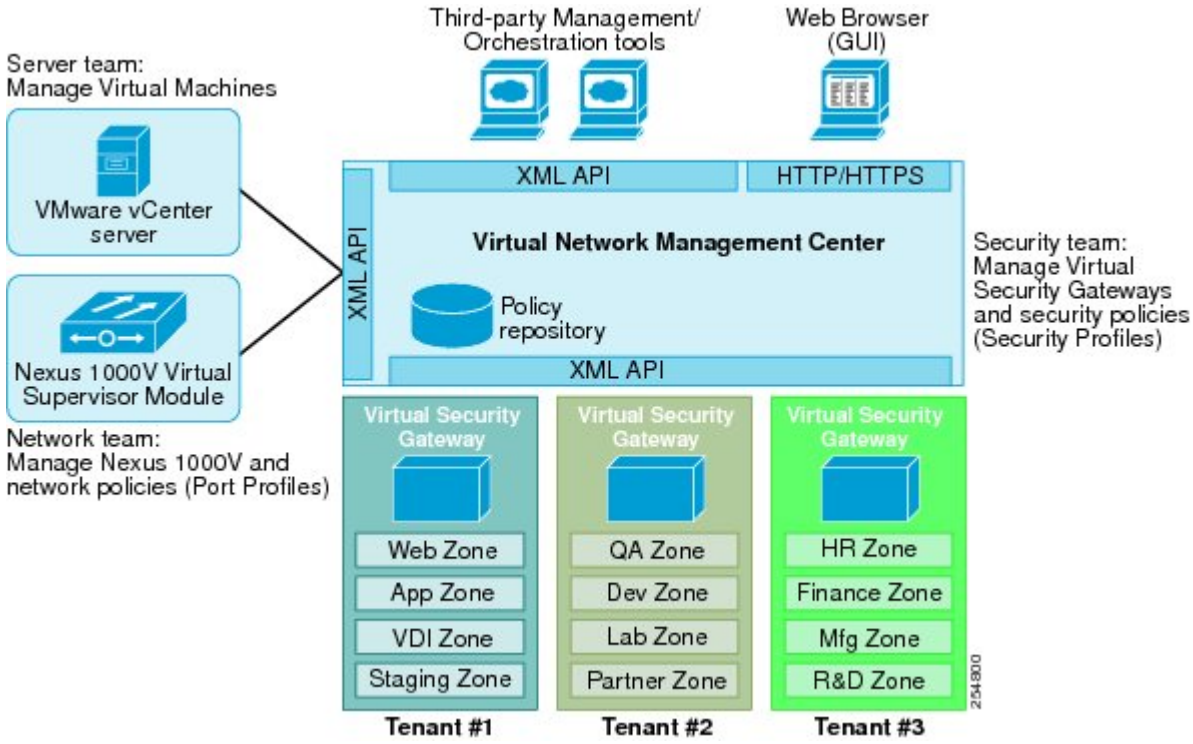
Cisco Virtual Network Management Center (Cisco VNMC) is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco Virtual Security Gateways (Cisco VSGs) for the Cisco Nexus 1000V Series switch. Designed for multi-tenant operation, the Cisco VNMC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. With built-in GUI, CLI, and XML APIs, the Cisco VNMC allows you to manage Cisco VSGs that are deployed throughout the data center from a centralized location. The Cisco VNMC is built on the information model-driven architecture where each managed device is represented by its sub-components (or objects) that are parametrically defined. This model-centric approach enables the Cisco VNMC to provide secure multi-tenant virtualized infrastructure with Cisco VSGs.

The Cisco VNMC provides the following key benefits:

- Rapid and scalable deployment through policy management based on security profiles
- Seamless operational management through XML APIs that enable programmatic integration with third-party management and orchestration tools

- Non-disruptive administration model enabling greater collaboration across security and server teams while maintaining administrative separation and reducing administrative errors

Figure 1: Cisco VNMC in a Multi-Tenant Environment



Cisco VNMC provides centralized device and policy management of Cisco VSGs in a multi-tenant virtual data center and/or private/public cloud.

The Cisco VNMC uses security profiles for tenant-centric configuration of security policies. A security profile is a collection of security policies that can be pre-defined and applied on an on-demand basis at the time of VM instantiation. This profile-driven approach significantly simplifies authoring, deployment, and management of security policies in a dense multi-tenant environment while also enhancing deployment agility and scale. Security profiles also help reduce administrative errors as well as simplify audits.

An important characteristic of Cisco VNMC is its north-bound XML API support, which facilitates coordination with third-party provisioning tools for programmatic provisioning and management of Cisco VSGs.

By providing visual and programmatic controls, the Cisco VNMC enables the security operations team to author and manage security policies for virtualized infrastructure, while enhancing collaboration with server and network operations teams. This non-disruptive administration model ensures that administrative segregation of duties remain in place to minimize administrative errors as well as to simplify compliance and audit requirements. The Cisco VNMC operates with the Nexus 1000V Virtual Supervisor Module (VSM) to achieve the following workflow:

- The network administrator can author and manage port profiles through Cisco Nexus 1000V distribute virtual switches. Port profiles on the Cisco Nexus 1000V Series switch can be propagated to the VMware Virtual Center as port groups and referenced by Virtual Machines.

- Security profiles are created in the Cisco VNMC and referenced in Cisco Nexus 1000V Series switch port profiles. Port profiles are created on the Nexus 1000V VSM.
- The server administrator can select the appropriate port profile in the VMware Virtual Center when instantiating a virtual machine.

The Cisco VNMC implements an information-model driven architecture in which each managed device, such as the Cisco VSG, is represented by the object information model of the device. Specifically, this model-driven architecture includes:

- A centralized repository for managing security policies and object configurations, thus allowing the managed devices to be stateless
- A centralized resource management function that distinctly manages pool of devices that are commissioned in service and pool of devices that are available for commissioning. This simplifies large-scale deployments because managed devices can be pre-instantiated and then configured on demand and devices can be allocated and de-allocated dynamically across commissioned and non-commissioned pools
- A distributed management-plane function implemented using an embedded management agent on each managed device, thus enabling a scalable management framework

Cisco VNMC System Requirements

Cisco VNMC has the following system requirements:

- Cisco VNMC Virtual Appliance—1 virtual CPU at 1.5-GHz, 2-GB RAM, 25-Gb hard disk (vDisk), 1 management network interface

Note 3-GB RAM is required for a Cisco VNMC ISO installation.

- Hypervisor and Hypervisor Manager—
  - VMware vSphere 4.1.0 and 5.0 releases with VMware ESX or ESXi
  - VMware vCenter 4.1.0 and 5.0 releases
- Interfaces and Protocols—HTTP/HTTPS, Lightweight Directory Access Protocol (LDAP)
- Web-based GUI client—
  - Flash 10.1
  - Operating system—Support details are as follows:

Table 1: Operating System Support Matrix

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Windows	Supported	Supported
Apple MAC OS	X	X

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Linux	X	X

Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php

Cisco VNMC Features

The Cisco VNMC includes the following features:

Multi-device Management

All Cisco Virtual Security Gateway for Nexus 1000V Series Switch devices are centrally managed which simplifies provisioning and troubleshooting in a scaled-out data center. In addition, the device profile object specifies device configuration policies that you can apply to one or more firewall profile managed resources.

Security Profile

A security profile enables you to represent the Cisco VSG security policy configuration in a profile, which simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and enables a highly scaled out data center environment.

Stateless Device Provisioning

The stateless configuration model is enabled with a management agent that is embedded with Cisco VSGs, that allows the Cisco VNMC to be a highly scalable device provisioning model.

Security Policy Management

Security policies are authored, edited, and provisioned for all Cisco VSGs in a data center, which simplifies the operation and management of security policies as well as ensures that the required security is accurately represented in the associated security policies.

Context Aware Security Policies

The Cisco VNMC interacts with VMware vCenter to obtain VM contexts that you can leverage to institute granular policy controls across their virtual infrastructure.

Dynamic Security Policy and Zone Provisioning

The Cisco VNMC interacts with the Nexus 1000V VSM to bind the security profile with the corresponding Cisco Nexus 1000V Series switch port profile. When VMs are dynamically instantiated and applied to appropriate port profiles, their association to trust zones is also established.

Multi-tenant Management

The Cisco VNMC can manage Cisco VSGs and security policies in a dense multi-tenant environment, so that you can rapidly add or delete tenants and update tenant-specific configurations and security policies. This feature significantly reduces administrative errors, ensures segregation of duties within the administrative team, and simplifies audit procedures.

Role-Based Access Control

Role-Based Access Control (RBAC) simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures. With RBAC, organizations are able to reduce administrative errors and simultaneously simplify auditing requirements. The Cisco VNMC supports local and remote authentication with RBAC.

XML-Based API

The Cisco VNMC full-featured XML APIs allow external system management and orchestration tools to programmatically provision Cisco VSGs and provide seamless and scalable operational management.