Installation Overview

This section contains the following topics:

Prime Network Services Controller Overview

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services. For the latest release updates and overview, see the corresponding data sheet.

Cisco Prime Network Services Controller is the primary management element for Cisco Nexus 1000VE Switches and Services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000VE switches and services deliver a highly secure multitenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

Cisco Prime Network Services Controller enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. is built on an information-model architecture in which each managed device is represented by its subcomponents (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG security services.

Note Starting with Cisco PNSC Release 3.4.2a, Cisco Adaptive Security Appliance (ASA 1000V), Cisco Cloud Services Router (CSR), Citrix NetScaler VPX, Citrix NetScaler, and KVM Hypervisor, and Microsoft HyperV platforms are not supported.

Hypervisor Support

The Prime Network Services Controller platform supports multiple VM Managers through their APIs and through tight integration with Nexus 1000VE Virtual Supervisor Modules (VSMs) and Virtual Ethernet Modules (VEMs).

Cisco Dynamic Fabric Automation Integration Support

Cisco Dynamic Fabric Automation (DFA) delivers fabric optimization, management, and automation capabilities under Cisco Unified Fabric. Prime Network Services Controller plays a critical role in the Cisco DFA solution with L4-7 services integration. Prime Network Services Controller integrates with Cisco Data Center Network Manager (DCNM) to support the managed resources and services in a VMware vSphere environment.

Consistent and Efficient Security Policies

Prime Network Services Controller uses security profiles for template-based configuration of security policies. A security profile is a collection of security policy sets and integrated policies and rules that can be predefined and applied on demand at the time of virtual machine instantiation. This profile-based approach significantly simplifies authoring, deployment, and management of security policies, including dense multi-tenant environments, while enhancing deployment agility and scaling. Security profiles also help reduce administrative errors and simplify audits.

The XML API for Prime Network Services Controller facilitates integration with northbound network provisioning tools for programmatic network and security provisioning and management of Cisco VSG (VSG) and ASA 1000V. The option of programmatic control of those virtual appliances can greatly simplify operational processes and reduce infrastructure management costs.

Nondisruptive Administration Model

By providing visual and programmatic controls, Prime Network Services Controller can enable the security operations team to author and manage security policies for virtualized infrastructure and enhance collaboration with the server and network operations teams. This nondisruptive administration model helps ensure administrative segregation of duties to reduce errors and simplify regulatory compliance and auditing:

- Security administrators can author and manage security profiles and manage VSG instances. Security profiles are referenced in Nexus 1000VE port profiles.
- Network administrators can author and manage port profiles, and manage Nexus 1000VE switches. Port profiles with referenced security profiles are available in VMware vCenter through the Nexus 1000VE VSM programmatic interface with VMware vCenter.
- Server administrators can select an appropriate port profile in VMware vCenter when instantiating a virtual machine.

Efficient Management for Easier Scalability

Prime Network Services Controller implements an information-model architecture in which each managed device, such as VSG or Cisco ASA 1000V, is represented by the device's object-information model. This model-based architecture helps enable the use of:

- Stateless managed devices—Security policies (security templates) and object configurations are abstracted into a centralized repository and used as templates against any virtual device type.
- Dynamic device allocation—A centralized resource management function manages pools of devices that are commissioned (deployed) in service and a pool of devices that are available for commissioning. This approach simplifies large-scale deployments because managed devices can be preinstantiated and then configured on demand, and devices can be allocated and deallocated dynamically across commissioned and noncommissioned pools.
- Scalable management—A distributed management-plane function is implemented using an embedded agent on each managed device that helps enable greater scalability.

Features and Benefits

The following table lists the features and benefits of using .

Features	Description	Benefits
Multiple-Device Management	Prime Network Services Controller provides central management of installed VMs (edge routers, edge firewalls, compute firewalls, and load balancers) and Nexus 1000V. **Note** Citrix NetScaler VPX, CSR 1000V and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Starting with Cisco PNSC release 3.4.2a, only Cisco VSG is supported.	Simplifies provisioning and troubleshooting in a scaled-out data center.
Security Profiles	A security profile represents the VSG security policy configuration in a profile (template).	Simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and helps enable a highly scaled-out data center environment.
Stateless Device Provisioning	The management agents in VSG are stateless, receiving information from .	• Enhances scalability. • Provides robust endpoint failure recovery without loss of configuration state.
Security Policy Management	Security policies are authored, edited, and provisioned centrally.	• Simplifies operation and management of security policies. • Helps ensure that security intent is accurately represented in the associated security policies.
Context-Aware Security Policies	obtains virtual machine contexts from VMware vCenter.	Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure.

Features	Description	Benefits
Support virtual services for DFA environments	Cisco Prime NSC obtains tenant information and allows virtual services to be added to DFA virtual overlay networks.	—
Dynamic Security Policy and Zone Provisioning	interacts with the Nexus 1000V VSM to bind the security profile to the corresponding Nexus 1000V port profile. When virtual machines are dynamically instantiated by server administrators and appropriate port profiles applied, their association with trust zones is also established.	Helps enable security profiles to stay aligned with rapid changes in the virtual data center.
Multi-Tenant (Scale-Out) Management	is designed to manage VSG security policies in a dense multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies.	Reduces administrative errors, helps ensure segregation of duties in administrative teams, and simplifies audit procedures.
Role-Based Access Control (RBAC)	RBAC simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures.	• Reduces administrative errors. • Enables detailed control of user privileges. • Simplifies auditing requirements.
XML-Based API	XML API allows external system management and orchestration tools to programmatically provision VSG .	• Allows the use of the best-in-class management software. • Offers transparent and scalable operation management.

Note Citrix NetScaler VPX, CSR 1000V, and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Hypervisors Openstack KVM and Microsoft HyperV are supported in PNSC releases up to 3.4.1d.