Enabling Service Chaining on Cisco Nexus 1000V Series

Introduction

Cisco Nexus® 1000V Series Switches offer Cisco® Virtual Services Data Path (vPath) architecture to support virtualized network services with intelligent traffic steering and performance acceleration.

Cisco vPath Service Chaining is a new model of delivering virtual services for the dynamic virtualized or cloud-based data center. Cisco vPath provides embedded intelligence within Cisco Nexus 1000V Series Virtual Ethernet Modules (VEMs) to dynamically apply multiple services to virtual machine (VM) traffic. vPath communicates with service nodes over tunnels, decoupling service nodes from network topology. The Cisco vPath architecture provides a forwarding-plane abstraction and a programmable framework for inserting or removing network services such as firewalls, load balancers, and WAN optimization at the hypervisor layer. Before vPath Service Chaining, vPath supported only one virtual network service instance per port-profile.

This guide explains Cisco vPath Service Chaining architecture, provides deployment guidelines, and explains on how to enable vPath Service Chaining with the Cisco Virtual Security Gateway (VSG) and the Cisco ASA 1000V Cloud Firewall.

Intended Audience

This document is intended for security architects, network architects, network engineers, virtualization administrators, and server administrators interested in understanding and deploying vPath Service Chaining with Cisco VSG and Cisco ASA 1000V in virtual VMware environment using Cisco Nexus 1000V Series Switch.

Cisco vPath Benefits

Cisco vPath for Cisco Nexus 1000V Series Switches provides the following benefits:

- Enables granular enforcement of network policies
- Eliminates the need for placing network services inline - using the overlay model, Cisco vPath can tunnel traffic to network services placed anywhere in the network
- Provides virtual machine mobility awareness
- Provides multitenancy awareness
- Enables data-path acceleration by offloading policy from network services to Cisco vPath
- Provides a scale-out model for horizontal scaling of network infrastructure
- Enables chaining of multiple network services

Network Service Delivery Challenges

Traditional network services cannot provide dynamic, high-mobility, and scalable infrastructure for virtualized environments. Factors contributing to these limitations are:

- The need to reconfigure all network elements for any network service changes
- Inefficient new services insertion and upgrades
- No support for dynamic scaling of resources
- Lack of single management control for different services, such as VM security, firewall, Network Address Translation (NAT), and VPN

In the absence of efficient service chaining architecture, physical network elements or service appliances are manually configured, leading to complex topologies that do not scale well.

Solution: Cisco vPath Service Chaining on the Cisco Nexus 1000V Series

Networks have long needed the ability to deliver multiple services on a given flow. Cisco vPath significantly simplifies the deployment model by acting as the orchestrator of the service chain to deliver multiple services while the control and management plane enables seamless provisioning of these services.

vPath Service Chaining offers the virtualized or cloud-based data center the following benefits:

- Ability to span virtualized computing resources in public, private, or hybrid cloud environments, with zone and edge security
- Ability to enforce policies based on full contextual understanding of security and VM contexts
- A robust platform that provides seamless integration with different virtual services and supports data acceleration by offloading policy from service nodes
- Single management interface for intra-tenant and tenant-edge security services

Cisco vPath is an intelligent traffic interception and granular policy enforcement engine for different network services. vPath has ability to accelerate the data path by offloading policy from network services to Cisco.

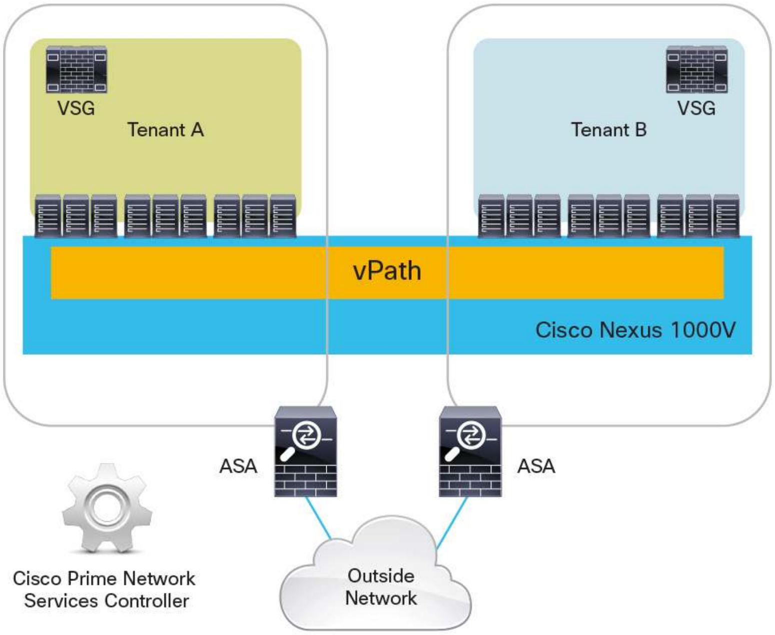
Cisco Nexus 1000V vPath currently supports the following Cisco network services:

- Cisco Virtual Security Gateway (VSG): Transparent, zone-based intra-tenant compute firewall
- Cisco ASA 1000V Cloud Firewall: Tenant-edge firewall

Cisco VSG provides security firewall for east-west (intra-VLAN) traffic, and Cisco ASA 1000V provides security for north-south (inter-VLAN) traffic.

Figure 1. Multi-Tenant Environment with Cisco VSG and Cisco ASA 1000V

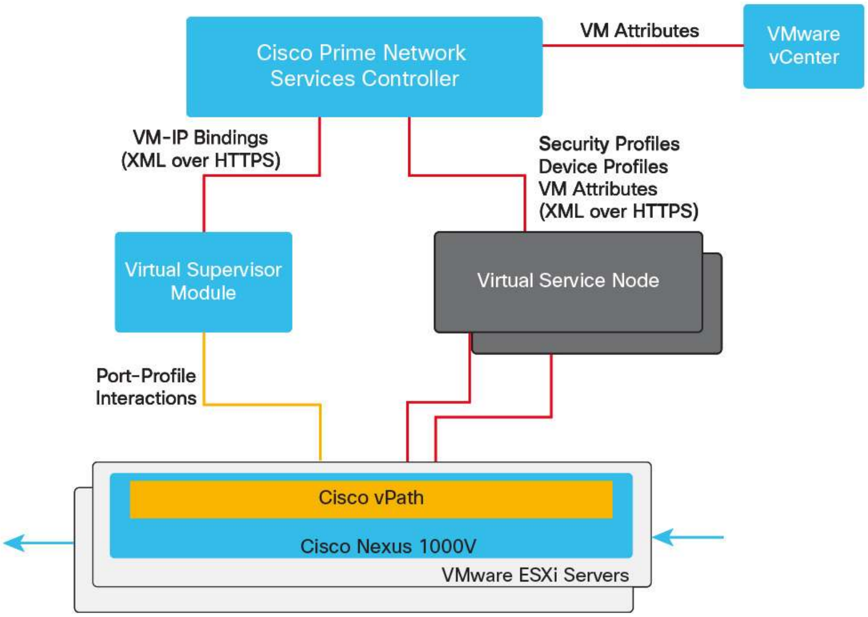
This is logical/conceptual diagram of positioning VSG and ASA 1000V in a Multi-Tenant Architecture.



Cisco vPath Service Chaining is available with Cisco Nexus 1000V Series Switches Release 1.5(2), Cisco VSG Release 1.4 and Cisco Prime Network Services Controller Release 2.0 and later.

Cisco vPath Service Chaining Architecture

Figure 2. vPath Architecture Components, and Their Interactions



vPath Service Chaining Architecture Components

vPath Service Chain architecture has four main components: the management plane, the control plane, the virtual service nodes, and the service data plane.

Management Plane

The Cisco Prime Network Services Controller is the management plane responsible for the entire orchestration, management, and control of virtual network services. It provides unified management for multiple service types. Cisco Prime Network Services Controller is a multidevice, multitenant-aware policy manager.

Cisco Prime Network Services Controller also provides northbound XML APIs to be programmed via different orchestration tools. Cisco Prime Network Services Controller interacts with Cisco Nexus 1000V Virtual Supervisor Module control plane and server management entities like vCenter to fetch virtual machine-specific attributes and states.

Control Plane

Cisco Virtual Network Service Agent (VNSA) running in Cisco Nexus 1000V Virtual Supervisor Module is the control plane bridge between Cisco Prime Network Services Controller and vPath. Virtual Supervisor Module in its primary function is the distributed virtual switch (DVS), that manages all the Virtual Ethernet Modules (VEM) that are part of DVS. In virtual services architecture, virtual service agents on the Virtual Supervisor Module propagate VM notification to Cisco Prime Network Services Controller, in order to fetch additional information from host management entities, like vCenter.

Virtual Network Service Agent is primarily responsible for all interactions with vPath, which includes programming of service tables, service path tables, flow tables, and vPath statistics.

Virtual Service Nodes (VSN)

Each service instance (for example, Cisco Virtual Security Gateway or Cisco ASA Cloud Firewall) is defined as a Virtual Service Node. Virtual Service Nodes typically belong to a single tenant. Each service node can be either Layer 2 or Layer 3 adjacent to vPath. VSG service-specific traffic transport between vPath and VSN is encapsulated using a Layer 2 (MAC-in-MAC) or Layer 4 (User Datagram Protocol [UDP]) tunnel, based on the VSN adjacency.

Service Data Plane

The service data plane includes vPath, which is embedded in the Virtual Ethernet Module on the Cisco Nexus 1000V Series. vPath is a distributed service data path, a service traffic classifier, and service enforcement point. vPath intercepts traffic in the switch data plane in both directions (that is, both ingress and egress flows).

vPath maintains four types of tables, which are crucial for its operations to classify and redirect traffic flows to enforce service policies.

- Service table: Determines services to be delivered for the type of traffic
- Service node table: Defines all service nodes activated in service path
- Path table: Orchestrates multiple service delivery in particular order for the same flow
- Flow table: Tracks the state of each flow

vPath is flow aware. vPath programs flow entries in its flow table for all the intercepted flows, and redirects flows to service nodes defined in service path.

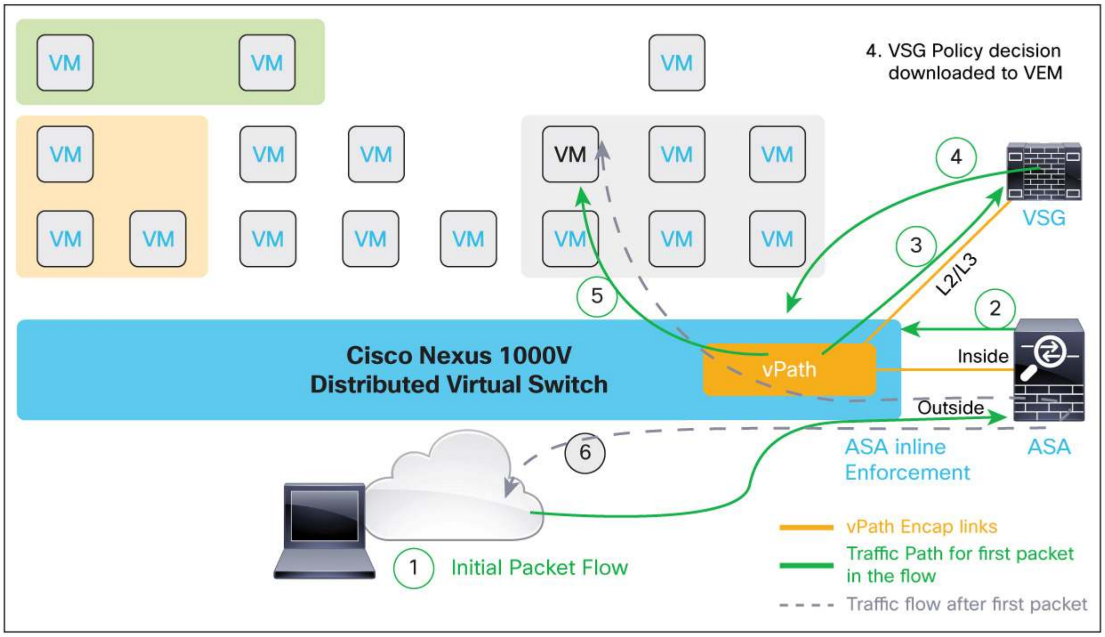
vPath Service Chaining Packet Flow

Following examples show packet flow in detail with Cisco VSG and Cisco ASA 1000V virtual services enabled with vPath:

vPath Service Chaining Example 1 with VSG and ASA

In the following example, an outside client is trying to access a VM protected by both Cisco VSG and Cisco ASA (Figure 3).

Figure 3. vPath Service Chaining Example 1


VM
4. VSG Policy decision downloaded to VEM
4
VSG
3
L2/L3
2
5
Cisco Nexus 1000V Distributed Virtual Switch
vPath
Inside
Outside
6
ASA inline Enforcement
ASA
1
Initial Packet Flow
vPath Encap links
Traffic Path for first packet in the flow
Traffic flow after first packet

The flow shown in Figure 3 includes the following events:

1. Initial packet sourced from outside client will be send to ASA, where inbound policies are evaluated. ASA is inline for the flow originating from outside (Internet), and this packet does not go through vPath, but directly to ASA. From ASA after policy evaluation, packets are sent to vPath.
2. After the ASA service node evaluates policies for this flow, the packet is returned to vPath. Based on the service chain configuration, vPath forwards packets to the appropriate network services (firewall, load balancer, etc) by encapsulating the original packet using Cisco vPath encapsulation. Cisco vPath encapsulation also includes the policy information that network services need to apply to the traffic flow.
3. ASA evaluates the policy for this flow and takes action based on the set policy. vPath then looks up the flow table, identifies whether the flow is a new flow, looks up the service path table, and encapsulates and forwards the packet to VSG service node.
4. VSG analyzes the policies for this flow and sends a decision back to the VEM. The VEM enforces the decision on this packet and caches this decision in the flow table for further packets in the flow.
5. Based on the decision received from the VSG, in this example vPath enforces the policy decision to permit traffic and forwards the packet to the VM.
6. Subsequent flows from the outside client come to ASA and after ASA policies are applied, vPath forwards these flows directly to the VM, based on cached VSG policy decision.

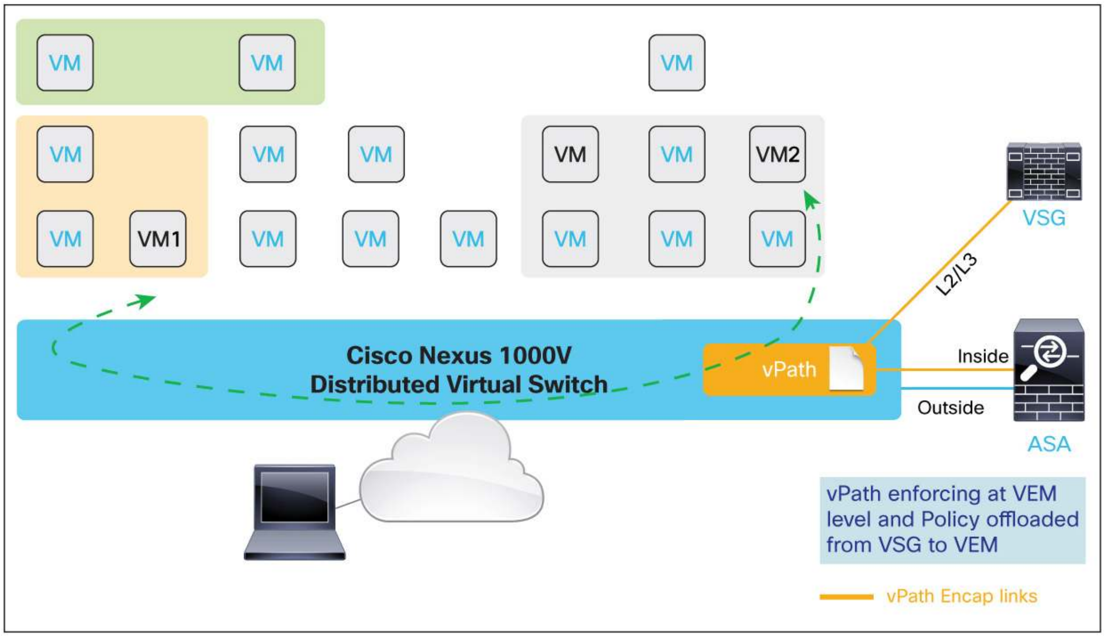
Network services optionally instruct Cisco vPath to offload further processing of the flow to vPath, providing performance acceleration for the network services. On the basis of the policy result, Cisco vPath will add the flow to its flow table and forward the original packet to the eventual destination or to any additional network services.

Multiple network services can be chained using Cisco vPath with centralized configuration.

Service Chaining Example 2 with VSG and ASA

The example shown in Figures 4 illustrates VM to VM communication in a same subnet.

Figure 4. vPath Service Chaining Example 2


VM
VM1
VM2
VSG
L2/L3
Cisco Nexus 1000V
Distributed Virtual Switch
vPath
Inside
Outside
ASA
vPath enforcing at VEM level and Policy offloaded from VSG to VEM
vPath Encap links

As Figure 4 shows, for subsequent flows following the first packet flow, policy enforcement is offloaded to VEM, and VM-to-VM traffic in same subnet is not redirected to a service node. The policy is enforced by vPath component integrated in VEM in the Cisco Nexus 1000V data plane.

Network services evaluate the policy and send policy action back to Cisco vPath. In addition, network services can optionally instruct Cisco vPath to offload further processing of the flow to vPath, providing performance acceleration for the network services.

On the basis of the policy result, Cisco vPath will add the flow to its flow table and forward the original packet to the eventual destination or to any additional network services.

Multiple network services can be chained using Cisco vPath with centralized configuration.

vPath to Service Node Communications

VSG can be Layer 2 or Layer 3 adjacent to VEM and vPath. ASA can only be Layer 2 adjacent to vPath.

There are two ways in which service nodes and vPath communicate:

- **Over Layer 2:** If the VEM and service node are in the same Layer 2 domain, the best way to connect them is to use the Layer 2 connectivity mode. Cisco vPath encapsulation provides MAC-in-MAC Layer 2 encapsulation.

- **Over Layer 3:** If the VEM and service node are in different Layer 2 domains, the Layer 3 connectivity mode should be used. The Layer 3 mode will encapsulate the packet using MAC-in-UDP tunnels. The service node implementation is independent of Cisco Nexus 1000V Series Virtual Supervisor Module-to-VEM communication (whether in Layer 2 or Layer 3 mode). Only VSG supports Layer 3 adjacency with VEM.

Cisco vPath Service Chaining Features

Service chaining architecture supports and enhances all dynamic provisioning, multitenancy, and mobility features, and does not impact any functionality with respect to these features, and preserves administrative boundaries.

Dynamic Service Provisioning

Dynamic service provisioning helps to ensure that services are associated to the VMs and not tied to router or switch ports. So the policies stay with the VM when the VM moves with VMware vMotion, and dynamically gets applied to a new VM on boot up.

vPath steers traffic to service nodes over tunnels, decoupling service nodes from network topology. This frees the service node from rigid requirements of being inline of the data path or being compatible with the underlying transport technology, such as VLAN or Virtual Extensible LAN (VXLAN).

In Cisco Nexus 1000V Series, the network parameters for each VM are dynamically provisioned by using port-profile mechanism. This same mechanism is extended to apply service policies along with network policies for the VM traffic. Policies are applied to the VM using port-profiles and not to physical switch or router interfaces. Policies move and stay with VM.

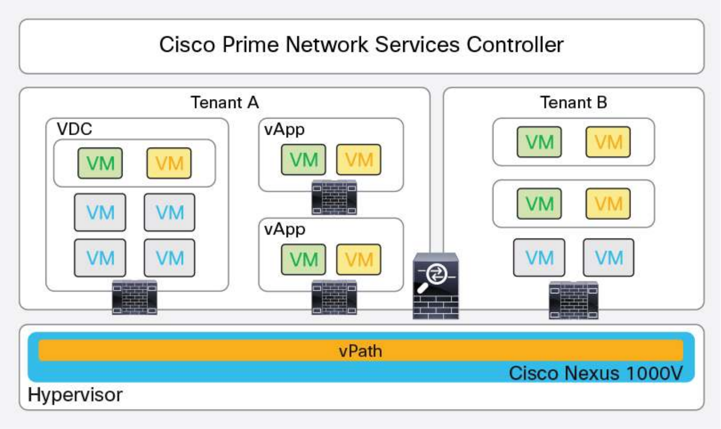
Multitenancy

vPath tables are multitenant-aware, so each vPath can serve service nodes that belong to different tenants. vPath redirects VM traffic to service node belonging to the same tenant as the VM. This enables clear tenant separation while providing the benefits of virtualization, including tenant scalability.

Cisco Prime Network Services Controller is designed to manage Cisco VSG, ASA, and security policies in a dense, multitenant environment, so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies.

Figure 5 vPath Service Chaining in Multitenant Environment, depicts the multitenant deployment of VSG. In architecture shown in the figure, Tenant A has its own VSG that provides security policies for its VMs. Tenant B has its own, separate VSG to manage its security policies for its VMs.

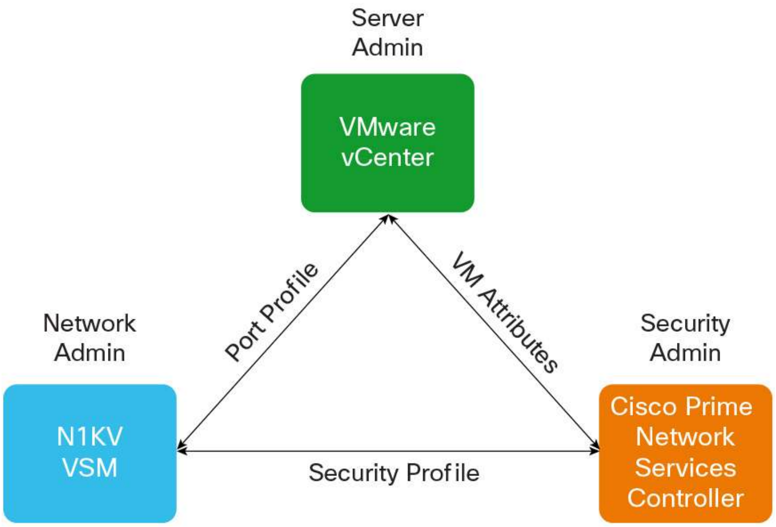
Figure 5. Multitenant Environment



Administrative Boundaries

vPath virtual services architecture (Figure 6) facilitates a collaborative management model, where roles and responsibilities are clearly defined. The security administrator owns security policy; the network administrator owns network policy; and the server administrator associates network policy to VMs. Once all the policies with port-profiles are associated, policies get dynamically provisioned when a new VM comes up or the VM moves from one server to another.

Figure 6. Preserve Administrative Boundaries



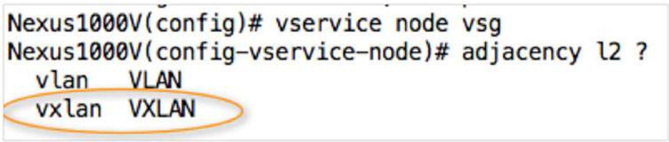
Mobility

The Cisco vPath solution handles both the virtual machine and the service node mobility in a highly efficient and dynamic way. When VM moves from one host to another, vPath on the destination host continues to steer traffic to the same service node as the source host. vPath on the destination host rebuilds flow table entries for that VM on first seeing traffic to and from that VM. With Cisco vPath solution service profiles remain unchanged for the VM and service policies stay with VM.

VXLAN

Service nodes can be deployed on Virtual Extensible LAN (VXLAN) instead of VLANs while using the Layer 2 deployment mode. VXLANs are terminated at the switches and hence service nodes do not see VXLAN tagged packets, although VXLAN tags may be made available via the service contexts in the service encapsulation. The packet flows are the same for both VLAN and VXLAN.

The following snippet shows example of a VXLAN supported configuration, highlighting VXLAN



```
Nexus1000V(config)# vservice node vsg
Nexus1000V(config-vservice-node)# adjacency l2 ?
  vlan   VLAN
  vxlan  VXLAN
```

vPath is VXLAN-aware, where Layer 2 flow interception and adjacency are supported to intercept Layer 2 frames on VXLAN interface or the VM. vPath has the ability to support a mixed mode of interception and adjacency, where the intercepted traffic is on VXLAN, the service node is on VXLAN, or both entities are VXLAN.

Enabling vPath Service Chaining in the Virtual Data Center

In this section, we explain step-by-step how to deploy virtual services (Cisco Virtual Security Gateway [VSG] and Cisco ASA 1000V Cloud Firewall) in a virtual data center.

The configurations discussed in this document use the following versions of the software components:

- Cisco Nexus 1000V Release 1.5(2)
- Cisco VSG Release VSG 1.4
- Cisco Prime Network Services Controller Release 2.0
- Cisco ASA 1000V 8.7.1
- VMware vSphere Release 5.0

Cisco vPath Deployment Prerequisites

This section covers various aspects of deploying Cisco vPath Service Chaining architecture with VSG and ASA services in your network.

Cisco Nexus 1000V Series Infrastructure

Before installing Cisco vPath Service Chaining, you must install Cisco Nexus 1000V Series Software Version 4.2(1) SV1.5.2 in your environment and perform the basic configuration of the Cisco Nexus 1000V Series Switch. This will include the following:

- Installing and configuring the Virtual Supervisor Module
- Providing access to shared storage
- Creating the necessary port-profiles, including
    - Uplink port profiles
    - VMkernel port profiles
    - VM-data port profiles
- Registering the Virtual Supervisor Module to vCenter
- Installing two or more Virtual Ethernet Modules (VEMs)
- Adding the VEMs to the Virtual Supervisor Module

This paper will not go into the details of how to install and deploy the Cisco Nexus 1000V Series. Please refer to the Cisco Nexus 1000V Deployment Guide:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html

Service Chaining Components

Cisco VSG

Cisco VSG uses three network interfaces in the following order:

1. VSG data interface
2. VSG management interface
3. VSG high-availability (HA) interface

Create additional VLANs for VSG data and HA on Virtual Supervisor Module and allow the VLANs to forward on the system uplink(s). Create these VLANs on the upstream switch. You can have the same VLAN for both the HA and data interfaces or different VLAN's based on your network topology.

The existing management VLAN in your setup can be used to manage VSG.

We recommend that you use the Open Virtual Appliance (OVA) for the VSG installation, which simplifies the installation process. Since Cisco Prime Network Services Controller is the centralized management center for VSG, it will be located in your management VLAN. There are no specific network requirements for setting up Cisco Prime Network Services Controller.

Cisco ASA

Cisco ASA uses four network interfaces in the following order:

1. ASA management interface
2. ASA inside data interface
3. ASA outside data interface
4. HA [high availability] interface

The existing management VLAN in your setup can be used to manage ASA.

We recommend that you use the OVA for the ASA installation, which simplifies the installation process. Since Cisco Prime Network Services Controller is the centralized management center for ASA, it will be located in your management VLAN. There are no specific network requirements for setting up Cisco Prime Network Services Controller.

Services Installation and Initial Setup

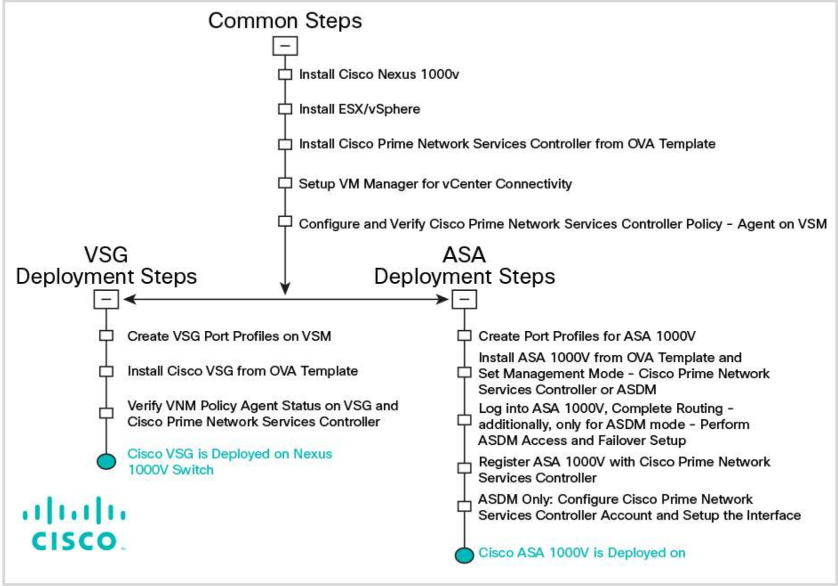
The server administrator must install the Cisco Prime Network Services Controller, VSG, and ASA in following order:

1. Install the Cisco Prime Network Services Controller as a virtual appliance.
2. Install the VSG as a virtual appliance.
3. Install the ASA as a virtual appliance
4. Register VSG to Cisco Prime Network Services Controller.
5. Register ASA to Cisco Prime Network Services Controller.
6. Register Virtual Supervisor Module to Cisco Prime Network Services Controller.

7. Register Cisco Prime Network Services Controller to vCenter.

For details about initial deployment steps, please refer installation guides for Cisco VSG, Cisco Prime Network Services Controller, and Cisco ASA 1000V Cloud Firewall. Figure 7 summarizes the deployment workflow.

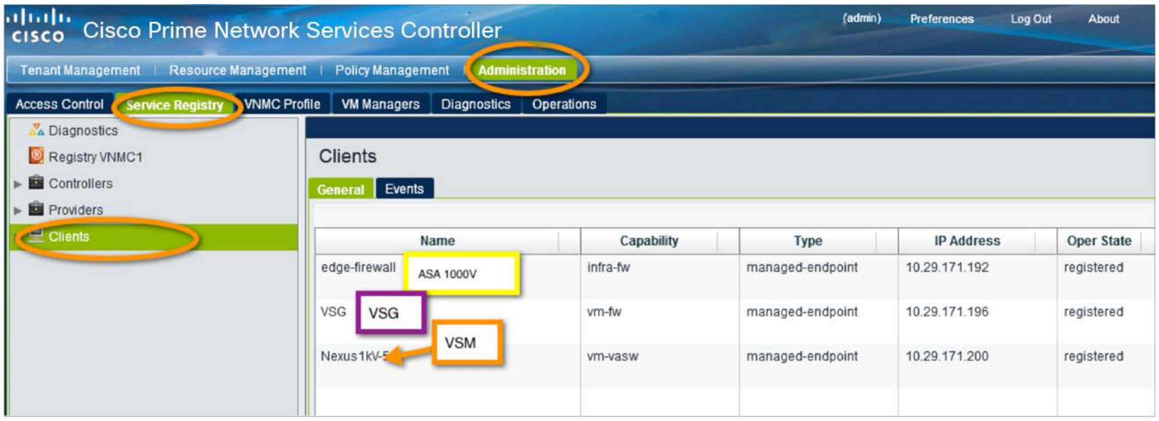
Figure 7. Deployment Workflow for VSG, ASA 1000V, Cisco Prime Network Services Controller and Cisco Nexus 1000V


Common Steps
Install Cisco Nexus 1000v
Install ESX/vSphere
Install Cisco Prime Network Services Controller from OVA Template
Setup VM Manager for vCenter Connectivity
Configure and Verify Cisco Prime Network Services Controller Policy - Agent on VSM
VSG Deployment Steps
ASA Deployment Steps
Create VSG Port Profiles on VSM
Install Cisco VSG from OVA Template
Verify VNM Policy Agent Status on VSG and Cisco Prime Network Services Controller
Cisco VSG is Deployed on Nexus 1000V Switch
Create Port Profiles for ASA 1000V
Install ASA 1000V from OVA Template and Set Management Mode - Cisco Prime Network Services Controller or ASDM
Log into ASA 1000V, Complete Routing - additionally, only for ASDM mode - Perform ASDM Access and Failover Setup
Register ASA 1000V with Cisco Prime Network Services Controller
ASDM Only: Configure Cisco Prime Network Services Controller Account and Setup the Interface
Cisco ASA 1000V is Deployed on
cisco

Verify Services Registered with Cisco Prime Network Services Controller

To verify the VSG and ASA 1000V services registered with Cisco Prime Network Services Controller, access the Cisco Prime Network Services Controller GUI interface using Cisco Prime Network Services Controller management IP address in web browser (Figure 8).

Figure 8. Verifying Clients Registered with Cisco Prime Network Services Controller in Service Registry Page



Clients

Name	Capability	Type	IP Address	Oper State
edge-firewall	infra-fw	managed-endpoint	10.29.171.192	registered
VSG	vm-fw	managed-endpoint	10.29.171.196	registered
Nexus1kV-5	vm-vasw	managed-endpoint	10.29.171.200	registered

After completing these tasks, you should be ready to start defining and implementing the security policies for VSG and ASA.

Configuring VSG and ASA Security Profiles and enabling security firewall for Virtual Machines

Tasks:

Configure and Manage Security Device and Profiles

Overview of Steps for the Security Administrator

In Cisco Prime Network Services Controller, the security administrator must perform the following steps:

1. Understand logical network topology [Figure 8] considered in this example.
2. Create a Tenant - TenantA.
3. Add zones for Tenant.
4. Assign VSG and ASA to a Tenant, This example shows services enabled for single Tenant.
5. Define the security profile for compute firewall.
6. Create policy set and add rules to the policy.
7. Bind the policy set to the security profile.
8. Define the edge device profile for edge firewall.
9. Define edge security profile for the edge firewall.
10. Add the policy set and create rules for the edge security policy.
11. Attach inbound security profile to outside interface on ASA.

After the above 11 steps are completed, Network Administrator needs to bind security profile to port-profiles.

Overview of Steps for the Network Administrator

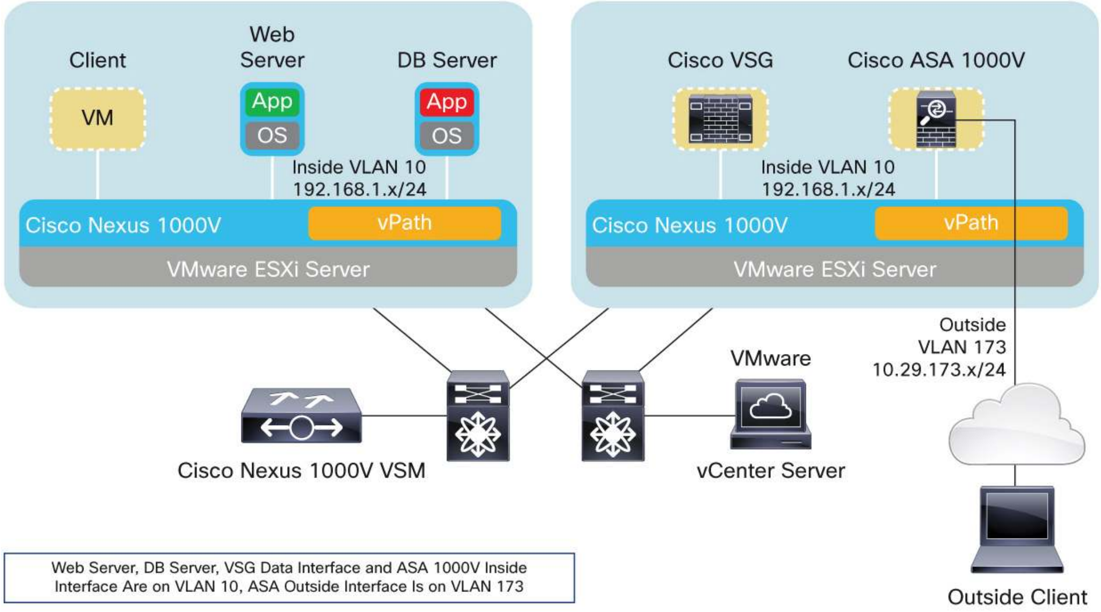
In the Virtual Supervisor Module, the network administrator must perform the following steps:

12. Define service nodes (Cisco VSG and ASA 1000V on Cisco Nexus 1000V Series).
13. Define vPath Services Chaining and add multiple service nodes to service chain.
14. Enable service chain per port-profile.
15. Verify service chain and nodes status.
16. Verify policies applied to traffic flow.

Security Administrator Step 1: Understanding Network Topology

Figure 9 shows conceptual view of typical network topology with all the necessary components in place for the vPath Service Chaining solution.

Figure 9. Network Topology for vPath Service Chaining



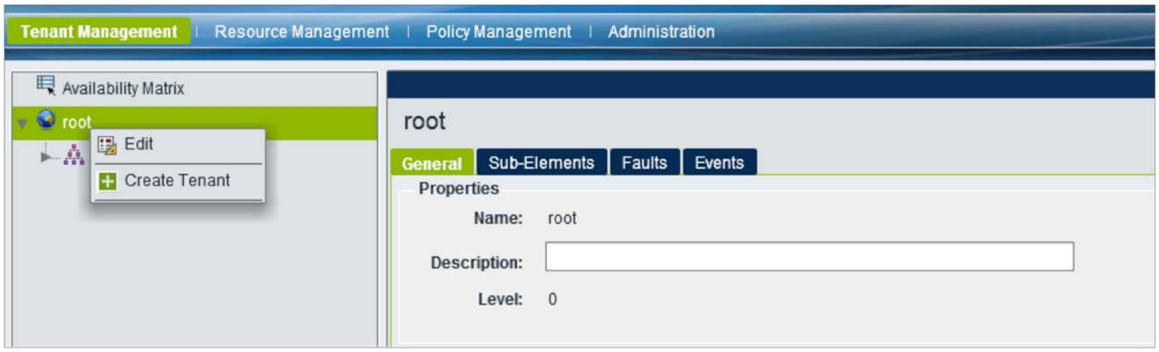
Security Administrator Step 2: Creating a Tenant

Multi-tenancy is a core concept of cloud computing, and the tenant concept can be applied in many ways. Tenants could represent different companies sharing a public cloud service, or different departments using a private enterprise cloud. A tenant is simply a logical container for virtual machines, networking, security services, etc.

Cisco Prime Network Services Controller and vPath is multitenant aware. Each tenant administrator will get respective tenant view in Cisco Prime Network Services Controller. Cisco VSG and ASA services are deployed per Tenant. Cisco VSG provides the compute firewall for inter-tenant communication or East-West communication, and ASA provides the tenant-edge firewall or North-bound access protection.

Log into the Cisco Prime Network Services Controller web interface using the management IP address and choose the Tenant Management section. Right-click the root and create a tenant (Figure 10).

Figure 10. Creating a Tenant



Name: root

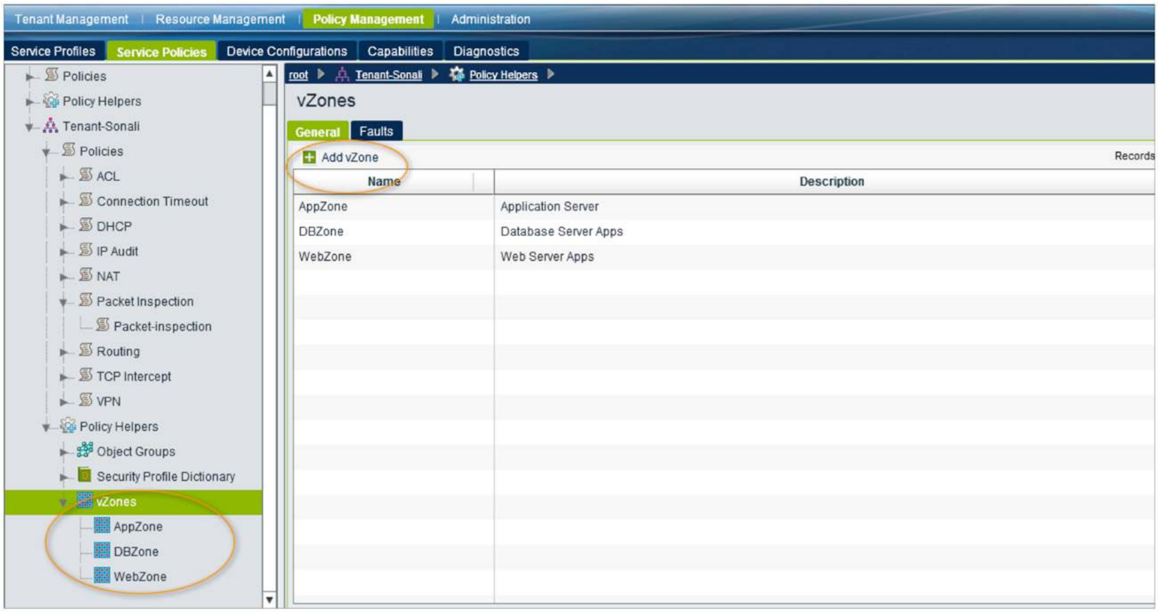
Description:

Level: 0

Security Administrator Step 3: Adding Zones to a Tenant

Logical zones can be created using network or VM attributes or a combination of both. Zones for policy rules can be defined using VM-context or network context, and policies can be applied to VM traffic based on logical user-defined zones (Figure 11).

Figure 11. Adding Zones for a Tenant



Name	Description
AppZone	Application Server
DBZone	Database Server Apps
WebZone	Web Server Apps

Security Administrator Step 4. Assigning VSG and ASA Services to a Tenant

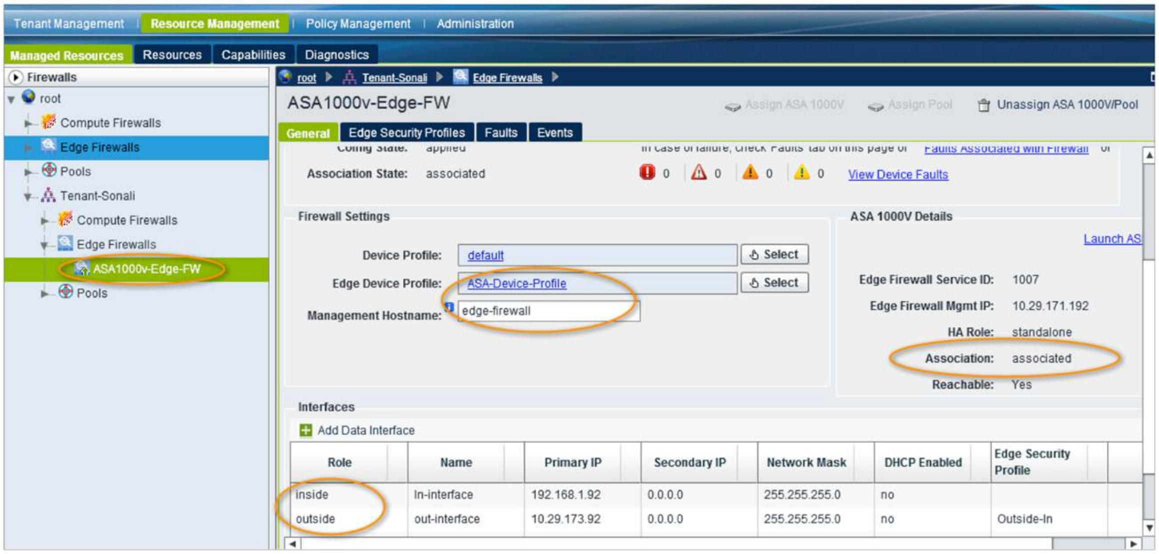
At this point, VSG and ASA is deployed and visible to Cisco Prime Network Services Controller, but it is not associated with any tenant or policies.

Create Compute Firewall for TenantA, and associate with VSG instance you've deployed.

Create an Edge Firewall object in TenantA. Create two data interfaces called **inside** and **outside**. After creating the Edge Firewall, associate it with the ASA1000V virtual machine. Click the new Edge Firewall and then click the **Assign ASA 1000V** button.

Figure 12 shows an example of assigning ASA services to the tenant edge firewall.

Figure 12. Assigning ASA Services to the Tenant Edge



ASA1000v-Edge-FW

Config State: applied

In case of failure, check Faults tab on this page or Faults Associated with Firewall

Association State: associated

0 0 0 0

Firewall Settings

Device Profile: default

Edge Device Profile: ASA-Device-Profile

Management Hostname: edge-firewall

ASA 1000V Details

Edge Firewall Service ID: 1007

Edge Firewall Mgmt IP: 10.29.171.192

HA Role: standalone

Association: associated

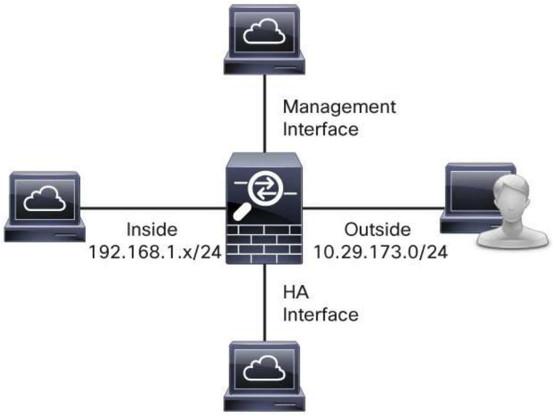
Reachable: Yes

Interfaces

Role	Name	Primary IP	Secondary IP	Network Mask	DHCP Enabled	Edge Security Profile
inside	In-interface	192.168.1.92	0.0.0.0	255.255.255.0	no	
outside	out-interface	10.29.173.92	0.0.0.0	255.255.255.0	no	Outside-In

Figure 13 shows ASA 1000V Interface Information

Figure 13. ASA 1000V Interfaces

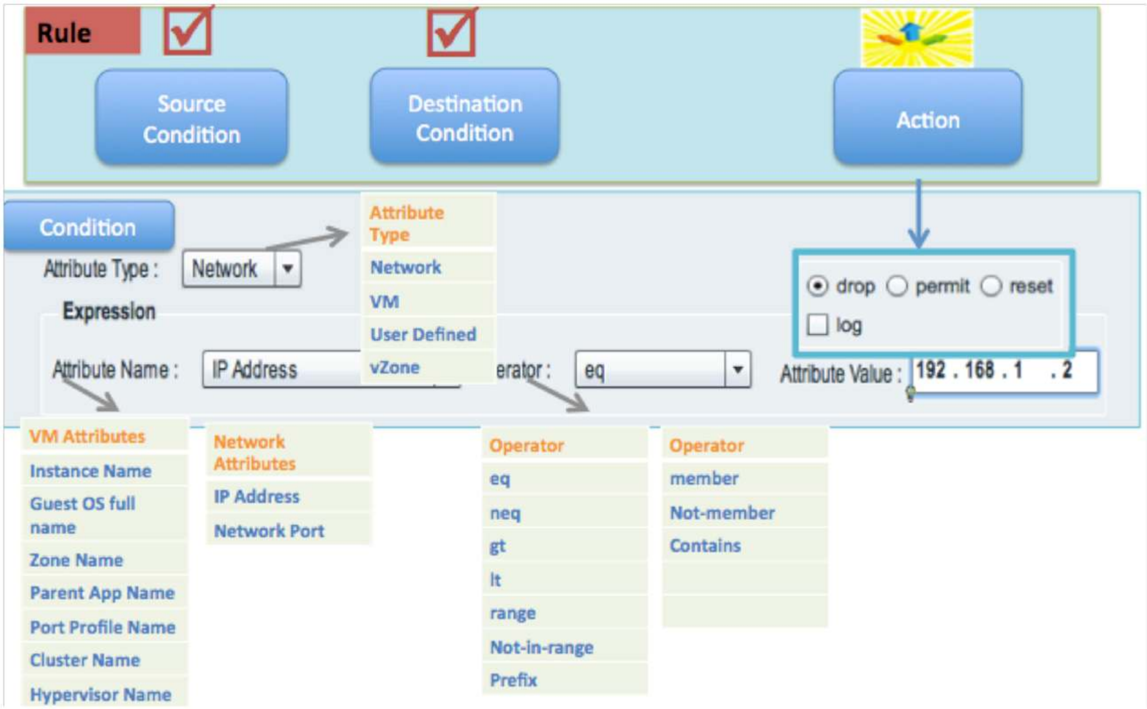


Security Administrator Step 5. Defining the Firewall Security Profile and Policy Set

East-west VM access policy rules are controlled by VSG, and northbound and southbound access rules are controlled by ASA security service.

The security policy in Cisco Prime Network Services Controller uses network attributes, VMware VM attributes, and VM custom attributes (see the access control list rule construct in Figure 14). You can define multiple policies for a tenant. All the policies are published to the VSG through a security profile. These policies can be applied at any organizational level within a tenant. Policies can be assigned using VM attributes, network attributes, or logical user-defined zones using these attributes.

Figure 14. ACL Rule Construct Options with VSG



Attribute Type : Network

Expression

Attribute Name : IP Address

Operator : eq

Attribute Value : 192 . 168 . 1 . 2

● drop ○ permit ○ reset

□ log

Attribute Type
Network
VM
User Defined
vZone

VM Attributes
Instance Name
Guest OS full name
Zone Name
Parent App Name
Port Profile Name
Cluster Name
Hypervisor Name

Network Attributes
IP Address
Network Port

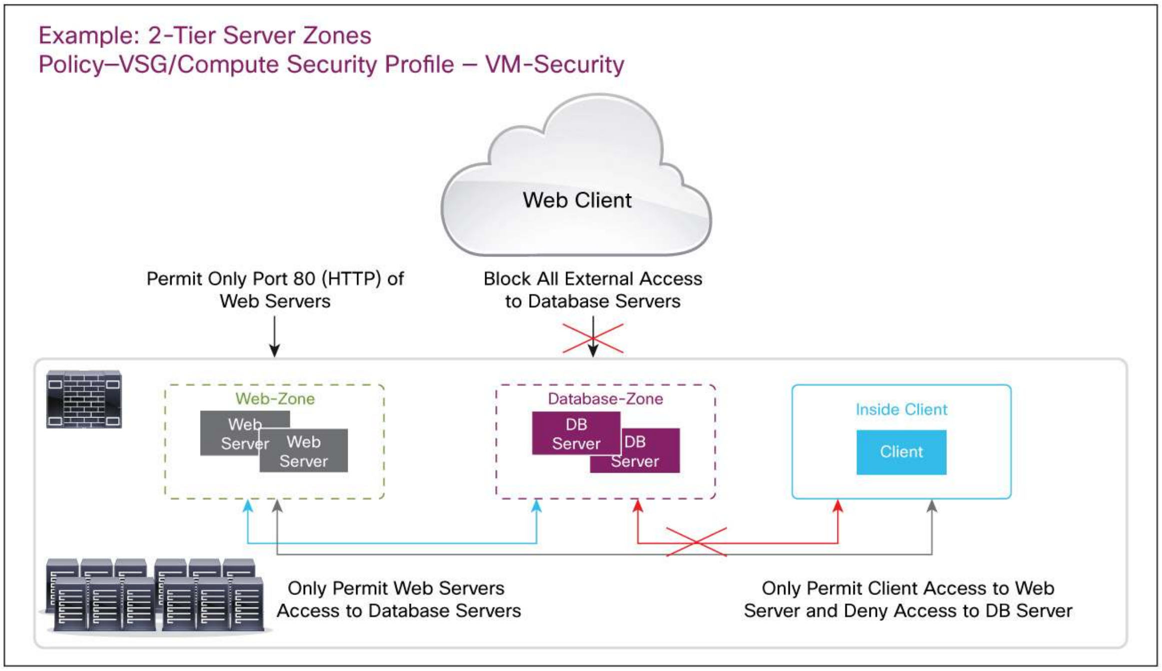
Operator
eq
neq
gt
lt
range
Not-in-range
Prefix

Operator
member
Not-member
Contains

Security Administrator Step 6. Defining the Security Profile and Policy Set for Compute Firewall

Security profiles are configured in Cisco Prime Network Services Controller Policy Management interface. The predefined zones can be used to define the security policy for each tenant.

Figure 15. Example of VSG Security Policy Rules for Tenant A, 2-Tier Server Zone


Example: 2-Tier Server Zones
Policy–VSG/Compute Security Profile – VM-Security
Web Client
Permit Only Port 80 (HTTP) of Web Servers
Block All External Access to Database Servers
Web-Zone
Web Server
Web Server
Database-Zone
DB Server
DB Server
Inside Client
Client
Only Permit Web Servers Access to Database Servers
Only Permit Client Access to Web Server and Deny Access to DB Server

Example of security policy rules for Tenant A, which will be applied to this use case:

- Permit only port 80 (HTTP) for virtual machines in the web zone
- Permit port 22 (SSH) for virtual machines that belong to the database zone
- Allow communications only between web servers and database servers
- Allow communications only between client and web servers
- Explicitly deny all traffic to all zones

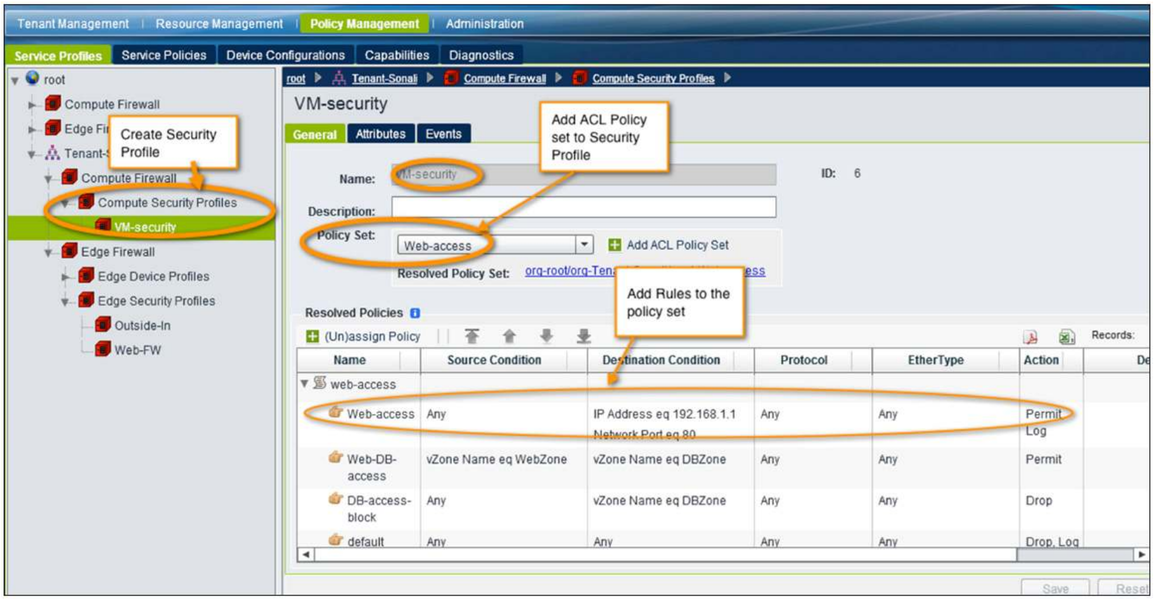
Security Administrator Step 7. Attach Policy Set to Security Profile - Compute Firewall

Policy sets are attached to security profile. When enabling VM policies, security profiles are used to attach security policies to VM's.

Select Compute firewall and create new Security Profile for Tenant A: example - VM-Security.

Within Security Profile, Create Policy Set (for policies described in Figure x in this example) and create rules for the policy set.

Figure 16. Example for step 6 and 7



Create Security Profile

Add ACL Policy set to Security Profile

Add Rules to the policy set

VM-security

Name: VM-security

ID: 6

Description:

Policy Set: Web-access

Resolved Policy Set: org-root/org-Tena ... ess

Name	Source Condition	Destination Condition	Protocol	EtherType	Action	De
web-access						
Web-access	Any	IP Address eq 192.168.1.1 Network Port eq 80	Any	Any	Permit Log	
Web-DB-access	vZone Name eq WebZone	vZone Name eq DBZone	Any	Any	Permit	
DB-access-block	Any	vZone Name eq DBZone	Any	Any	Drop	
default	Any	Any	Any	Any	Drop, Log	

Security Administrator Step 8. Defining the Edge Device Profile for Edge Firewall

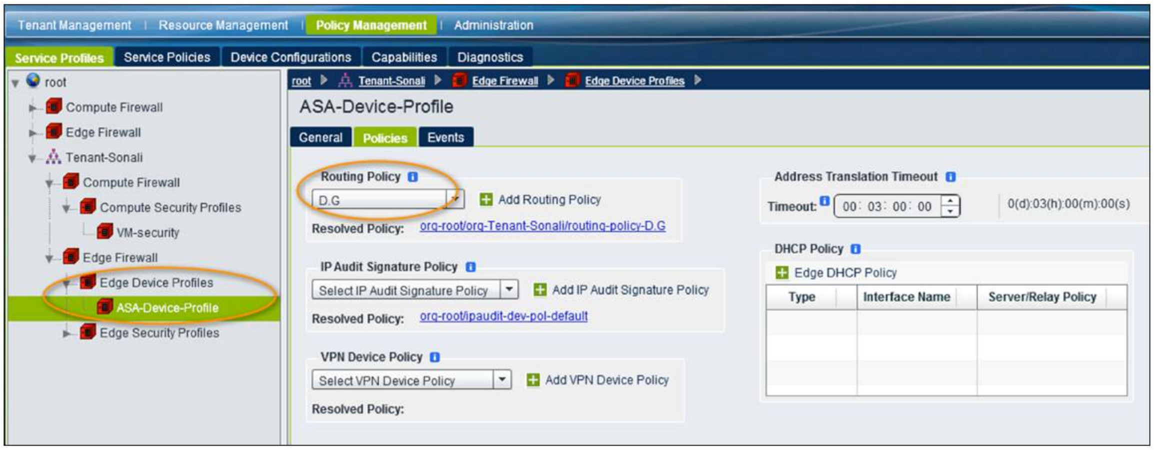
Cisco Prime Network Services Controller allows configuration of security devices (ASA1000V and VSG) using a set of configuration profiles. There are three profile types used to create these configurations. Each profile type contains different types of policies. The three profile types are:

- **Device Profile** - Contains policies that apply to both ASA1000V and VSG (Syslog, SNMP)
- **Compute Security Profiles** - Contains policies that apply to VSG only (VM based ACLs)
- **Edge Device Profiles** - Contains policies that apply to ASA1000V only (Routing, DHCP)
- **Edge Security Profiles** - Contains policies that apply to an interface of an ASA1000V (ACLs, NAT)

Profiles and policies are created in the Policy Management tab, and are applied to an ASA1000V or VSG in the Resource Management tab.

Navigate to **Cisco Prime Network Services Controller → Policy management → Service Profiles**. Select Edge Device Profiles and create new Device Profile (Figure 16). In this example, the **Routing Policy (D.G)** is configured with the default gateway for the outside interface. Other device policies like Dynamic Host Configuration Protocol (DHCP) and VPN can also be configured for the device.

Figure 17. Define Edge Device Profile for the Edge Firewall Cisco ASA 1000V



ASA-Device-Profile

Routing Policy: D.G
Resolved Policy: org-root/org-Tenant-Sonali/routing-policy-D.G

IP Audit Signature Policy: Select IP Audit Signature Policy
Resolved Policy: org-root/ipaudit-dev-pol-default

VPN Device Policy: Select VPN Device Policy
Resolved Policy:

Address Translation Timeout
Timeout: 00: 03: 00: 00 0(d):03(h):00(m):00(s)

DHCP Policy

Type	Interface Name	Server/Relay Policy

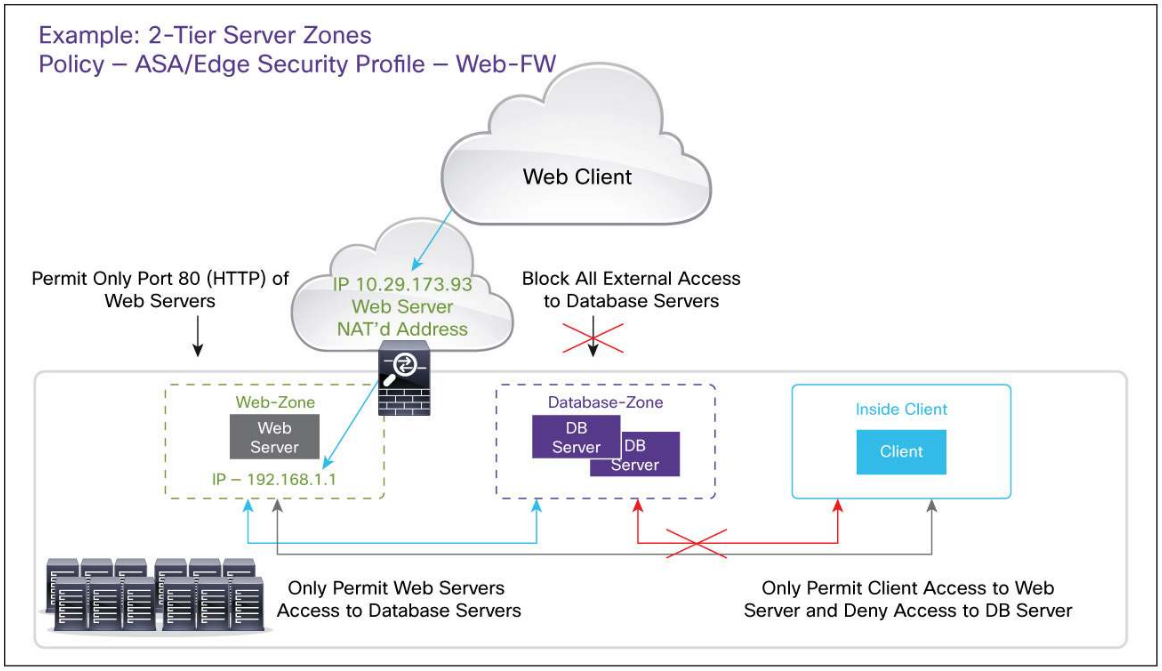
Security Administrator Step 9. Adding the Policy Set and Creating Rules for the Policy Set of Edge Firewall

Edge Security Profiles apply to an interface of an ASA1000V. They contain policies such as ACLs, NAT, TCP intercept, and some VPN configuration.

Edge Security Profiles are applied differently than Device Profiles or Edge Device Profiles. Because they do not apply to the device as a whole, but only to a specific interface, they cannot be applied to the Edge Firewall in Cisco Prime Network Services Controller. An Edge Security Profile is instead applied to the port-profiles in the Nexus1000V virtual switch.

After the device policy is created for edge firewall, you need to define edge security profile and add policies for NAT, ACL, and Packet Inspection etc. to this profile to be applied to inbound traffic.

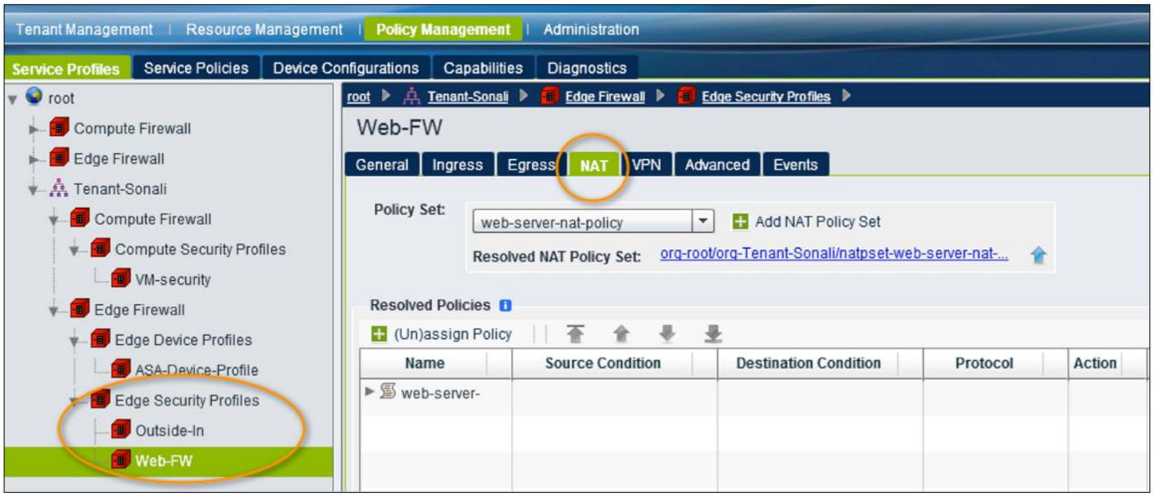
Figure 18. Example of Rules Configured for Edge Firewall


Example: 2-Tier Server Zones
Policy – ASA/Edge Security Profile – Web-FW
Web Client
Permit Only Port 80 (HTTP) of Web Servers
IP 10.29.173.93
Web Server
NAT'd Address
Block All External Access to Database Servers
Web-Zone
Web Server
IP – 192.168.1.1
Database-Zone
DB Server
DB Server
Inside Client
Client
Only Permit Web Servers Access to Database Servers
Only Permit Client Access to Web Server and Deny Access to DB Server

Next, create a new profile under Edge Security Profiles. For outbound traffic only one Profile is needed, but for inbound traffic an outside Profile is required in addition to the inside profile you just configured.

The outside interface Profile must be applied from Cisco Prime Network Services Controller, not Nexus 1000V, example shown with Outside-In Profile applied to Outside interface for Ingress Traffic.

Outside-In security policies are used for inbound traffic (Figure 19).



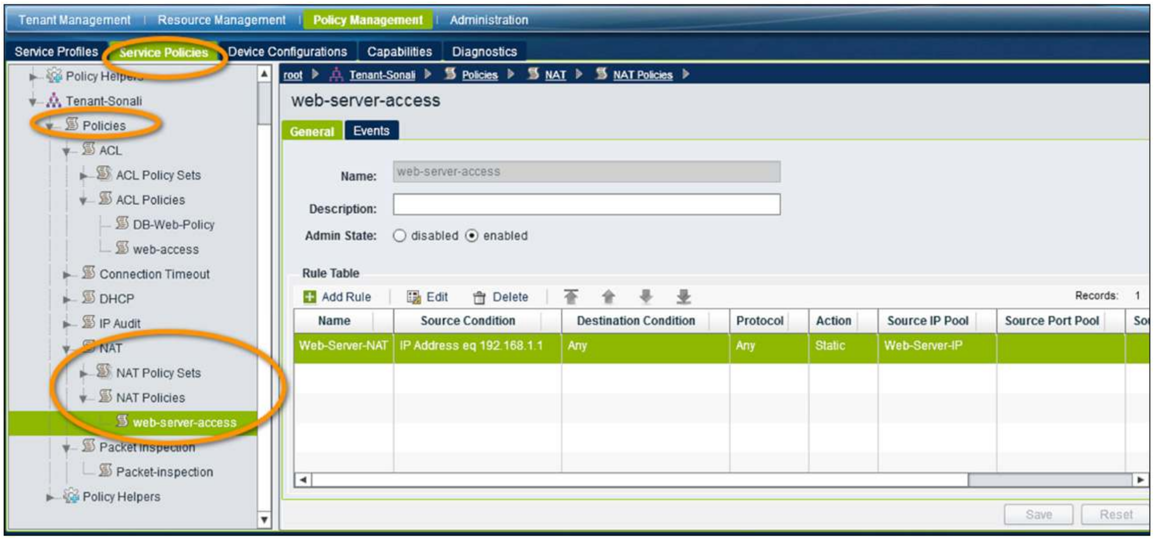
Policy Set: web-server-nat-policy

Resolved NAT Policy Set: org-root/org-Tenant-Sonali/natpset-web-server-nat-...

Name	Source Condition	Destination Condition	Protocol	Action
web-server-				

Figure 19 shows a comprehensive list of policies that can be added to edge security profile.

Figure 19. Policy Options for Edge Security Profile Options



web-server-access

Name: web-server-access

Description:

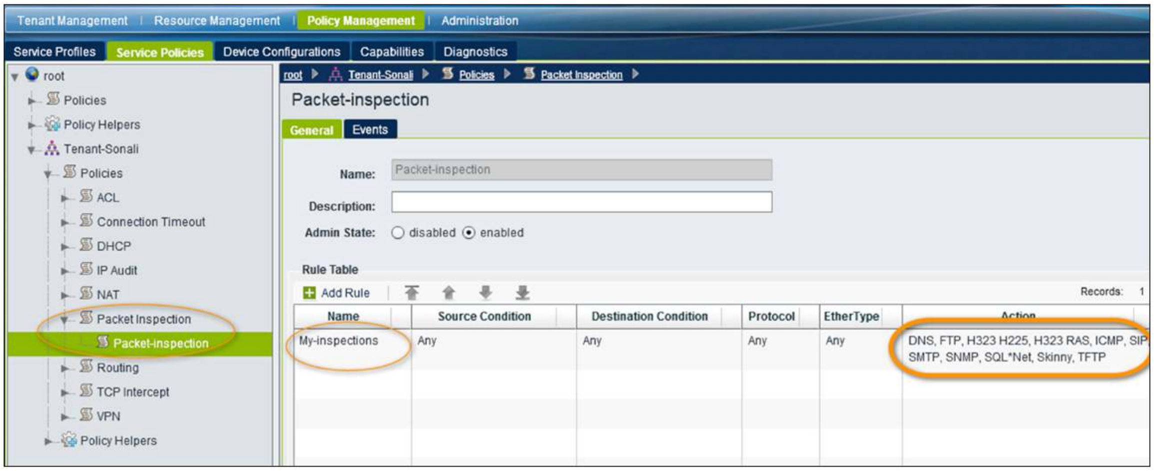
Admin State: ○ disabled ● enabled

Rule Table

Records: 1

Name	Source Condition	Destination Condition	Protocol	Action	Source IP Pool	Source Port Pool	So
Web-Server-NAT	IP Address eq 192.168.1.1	Any	Any	Static	Web-Server-IP		

Figure 20. Example of Packet Inspection Policy Added to the Web-FW Security Profile



Packet-inspection

Name: Packet-inspection

Description:

Admin State: ○ disabled ● enabled

Rule Table

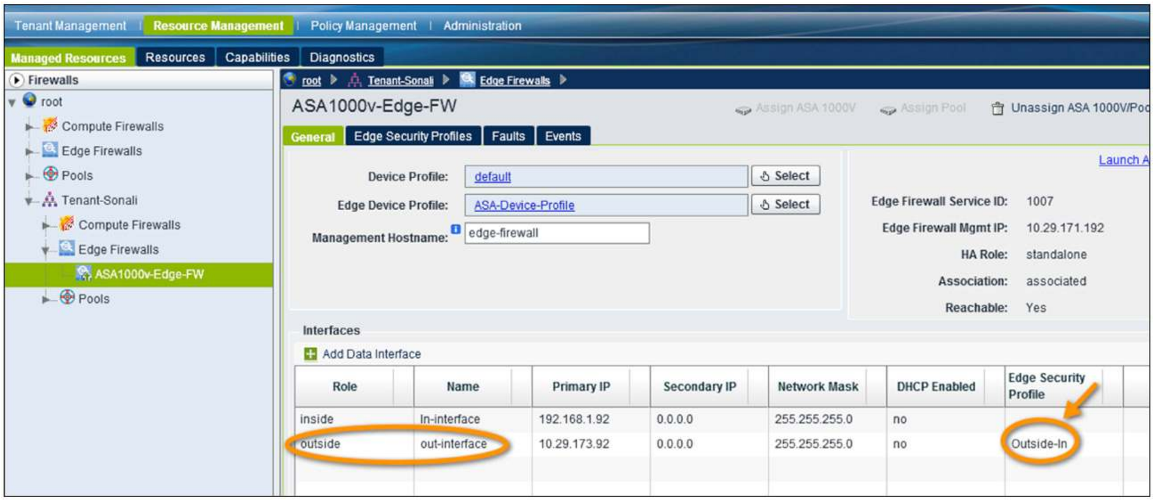
Records: 1

Name	Source Condition	Destination Condition	Protocol	EtherType	Action
My-inspections	Any	Any	Any	Any	DNS, FTP, H323 H225, H323 RAS, ICMP, SIP SMTP, SNMP, SQL*Net, Skinny, TFTP

8. Attach inbound security profile to outside interface on Cisco ASA

To enable policies for Inbound traffic, you need to attach Security profile to Outside interface of Edge Security Device (ASA).

Figure 21. Example to Bind Inbound Profile to ASA Outside Interface (Edge Firewall)



ASA1000v-Edge-FW

Device Profile: default

Edge Device Profile: ASA-Device-Profile

Management Hostname: edge-firewall

Edge Firewall Service ID: 1007

Edge Firewall Mgmt IP: 10.29.171.192

HA Role: standalone

Association: associated

Reachable: Yes

Role	Name	Primary IP	Secondary IP	Network Mask	DHCP Enabled	Edge Security Profile
inside	In-interface	192.168.1.92	0.0.0.0	255.255.255.0	no	
outside	out-interface	10.29.173.92	0.0.0.0	255.255.255.0	no	Outside-In

Enabling vPath Service Chaining on the Cisco Nexus 1000V Series

All the steps in this section will be executed in Nexus 1000V Virtual Supervisor Module console.

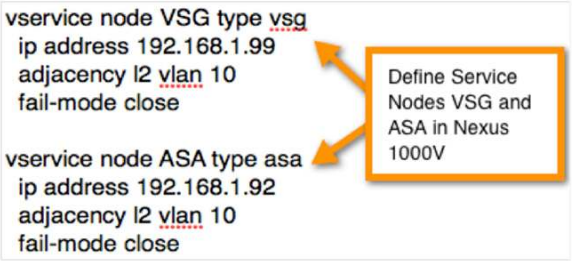
To enable firewall service policies for VM workload in the network, you need to attach security profile to port-profile on Cisco Nexus 1000V Series. All the traffic traversing the virtual ports associated with that port profile is subjected to policy evaluation.

Network Administrator Step 12: Defining Service Nodes

The next step is to define the service nodes for both VSG and ASA service instances on Nexus 1000V.

To define VSG service node, use VSG data interface IP address and data VLAN ID. VSG can be Layer 2 or Layer 3 adjacent to Cisco Nexus 1000V Series (vPath), regardless of Virtual Supervisor Module to VEM adjacency mode.

To define ASA service node, you need to use ASA inside interface IP address and corresponding VLAN. ASA can be Layer 2 adjacent to Nexus 1000V (vPath), regardless of Virtual Supervisor Module to VEM adjacency mode. The following code shows configuration example of 2 nodes added each of type vsg and type asa:

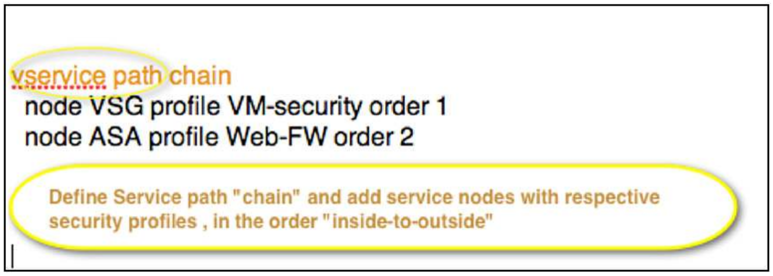


```
vservice node VSG type vsg
  ip address 192.168.1.99
  adjacency l2 vlan 10
  fail-mode close

vservice node ASA type asa
  ip address 192.168.1.92
  adjacency l2 vlan 10
  fail-mode close
```

Define Service Nodes VSG and ASA in Nexus 1000V

Network Administrator Step 13: Chaining VSG and ASA Services in Service Path

Use the service path to define service chaining with multiple service nodes, in a specific order. The order for service nodes chaining should be applied **Inside-to-Outside**. This is where you apply security profiles created for VSG and ASA to the service path, as follows:



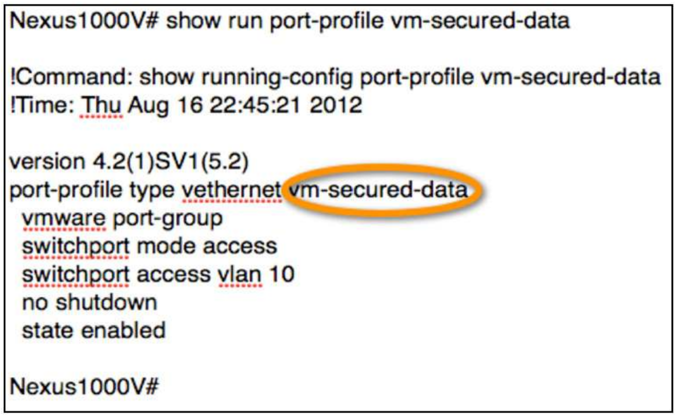
```
vservice path chain
  node VSG profile VM-security order 1
  node ASA profile Web-FW order 2
```

Define Service path "chain" and add service nodes with respective security profiles , in the order "inside-to-outside"

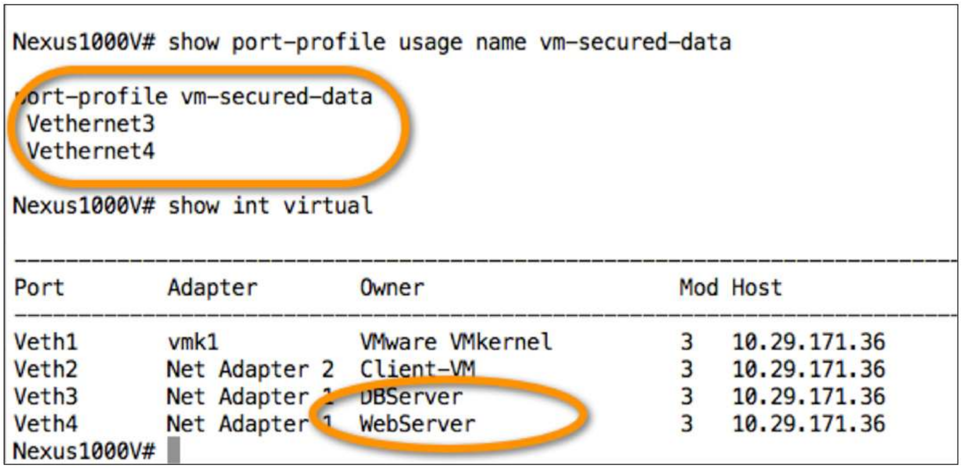
Network Administrator Step 14: Enabling Service Chain Per Port-Profile

Port-profiles provide flexibility to add individual service nodes or multiple services chained together using the virtual service path.

In the example shown in the following code, vm-secured-data port-profile is attached to WebServer and DBServer, and will be used to enable Zone based Firewall (VSG) and Edge Firewall (ASA) Security.

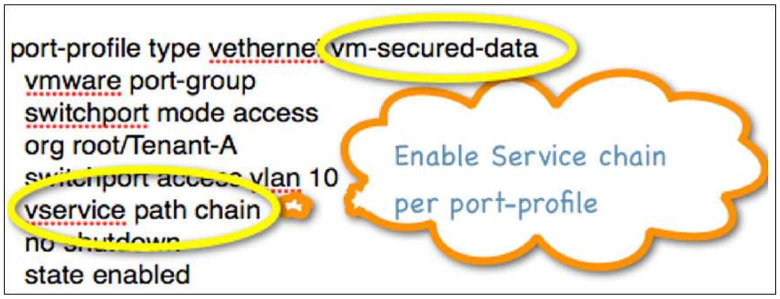


```
Nexus1000V# show run port-profile vm-secured-data

!Command: show running-config port-profile vm-secured-data
!Time: Thu Aug 16 22:45:21 2012

version 4.2(1)SV1(5.2)
port-profile type vethernet vm-secured-data
  vmware port-group
  switchport mode access
  switchport access vlan 10
  no shutdown
  state enabled

Nexus1000V#
```



```
Nexus1000V# show port-profile usage name vm-secured-data

port-profile vm-secured-data
 Vethernet3
 Vethernet4

Nexus1000V# show int virtual

-------------------------------------------------------------------------------
Port        Adapter        Owner                   Mod Host
-------------------------------------------------------------------------------
Veth1       vmk1           VMware VMkernel         3   10.29.171.36
Veth2       Net Adapter 2  Client-VM               3   10.29.171.36
Veth3       Net Adapter 1  DBServer                3   10.29.171.36
Veth4       Net Adapter 1  WebServer               3   10.29.171.36
Nexus1000V#
```

Identify port-profiles to enable firewall security. In the following example, the workload uses the port-profile **vm-secured-data** to enable service chain. Along with **vservice path** command, you need to also define **Tenant Org** for this port-profile. This will be same tenant where the VSG and ASA services are assigned and security profiles are created in Cisco Prime Network Services Controller.

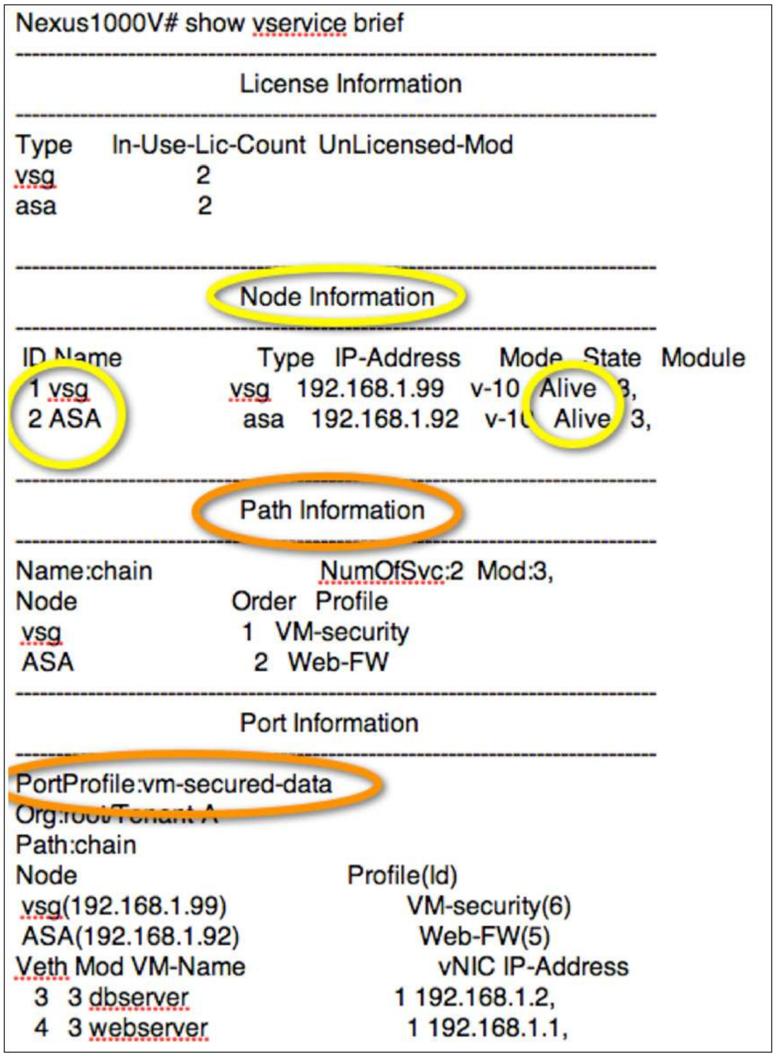


```
port-profile type vethernet vm-secured-data
  vmware port-group
  switchport mode access
  org root/Tenant-A
  switchport access vlan 10
  vservice path chain
  no shutdown
  state enabled
```

Enable Service chain per port-profile

Network Administrator Step 15: Verifying the Path, Node, and Profile Configurations and Service Node Status

With commands **show vservice brief/detail**, verify service node status is alive and service chain is attached to desired VMs, as follows:

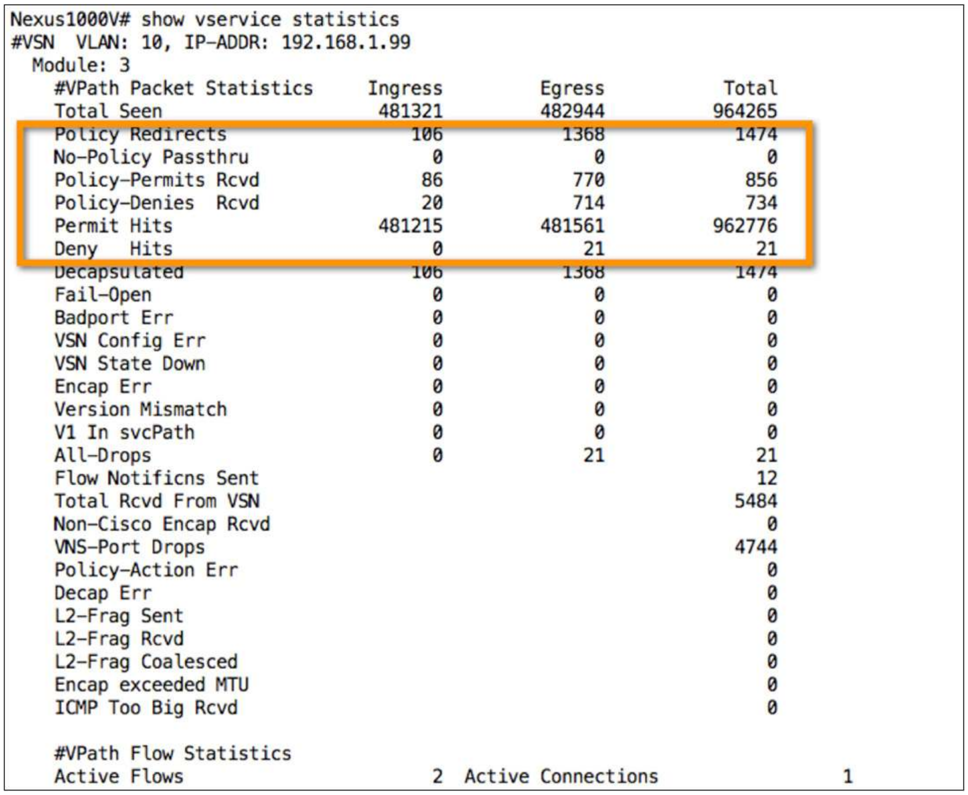


```
Nexus1000V# show vservice brief
--------------------------------------------------------------------------------
                              License Information
--------------------------------------------------------------------------------
Type     In-Use-Lic-Count  UnLicensed-Mod
vsg             2
asa             2

--------------------------------------------------------------------------------
                              Node Information
--------------------------------------------------------------------------------
ID Name                  Type   IP-Address     Mode   State   Module
 1 vsg                  vsg    192.168.1.99   v-10   Alive   3,
 2 ASA                   asa    192.168.1.92   v-10   Alive   3,

--------------------------------------------------------------------------------
                              Path Information
--------------------------------------------------------------------------------
Name:chain                        NumOfSvc:2  Mod:3,
Node                     Order  Profile
 vsg                       1   VM-security
 ASA                        2   Web-FW
--------------------------------------------------------------------------------
                              Port Information
--------------------------------------------------------------------------------
PortProfile:vm-secured-data
Org:root/Tenant-A
Path:chain
Node                                 Profile(Id)
 vsg(192.168.1.99)                        VM-security(6)
 ASA(192.168.1.92)                         Web-FW(5)
Veth Mod VM-Name                             vNIC IP-Address
  3   3 dbserver                          1 192.168.1.2,
  4   3 webserver                          1 192.168.1.1,
```

Network Administrator Step 16: Verifying Service Chain Insertion

The final step is to verify the services inserted in the traffic flow by accessing Web Server at port 80 from both inside and outside client. The outside client will use web server's IP address.

Verify Statistics on Virtual Supervisor Module or on VSG and ASA Console, to get information on number of packet flows, flow policy hits, or policy miss and actions implemented for the flow. vPath statistics display data stats for combined flows, as follows:



```
Nexus1000V# show vservice statistics
#VSN  VLAN: 10, IP-ADDR: 192.168.1.99
  Module: 3
    #VPath Packet Statistics      Ingress         Egress          Total
    Total Seen                     481321         482944         964265
    Policy Redirects                  106           1368           1474
    No-Policy Passthru                  0              0              0
    Policy-Permits Rcvd                86            770            856
    Policy-Denies  Rcvd                20            714            734
    Permit Hits                    481215         481561         962776
    Deny   Hits                         0             21             21
    Decapsulated                      106           1368           1474
    Fail-Open                           0              0              0
    Badport Err                         0              0              0
    VSN Config Err                      0              0              0
    VSN State Down                      0              0              0
    Encap Err                           0              0              0
    Version Mismatch                    0              0              0
    V1 In svcPath                       0              0              0
    All-Drops                           0             21             21
    Flow Notificns Sent                                              12
    Total Rcvd From VSN                                            5484
    Non-Cisco Encap Rcvd                                              0
    VNS-Port Drops                                                 4744
    Policy-Action Err                                                 0
    Decap Err                                                         0
    L2-Frag Sent                                                      0
    L2-Frag Rcvd                                                      0
    L2-Frag Coalesced                                                 0
    Encap exceeded MTU                                                0
    ICMP Too Big Rcvd                                                 0

    #VPath Flow Statistics
    Active Flows                        2  Active Connections               1
```

Summary

Network intelligence (vPath) for virtual services is critical for:

- Non-disruptive operation
- Simplified deployment
- Optimized performance
- Dynamic scalability
- Separation of duties

Cisco Nexus 1000V Series vPath functionality provides an innovative architecture for deploying network services in today's virtual multitenant data centers. It provides a programmable architecture for insertion and removal of network services, providing the business agility needed in cloud-based data centers. In addition, the Cisco vPath Service Chaining provides a single control point for multiple network services, making network services deployments simpler, faster. and less error prone.

For More Information

Cisco Nexus 1000V Series Switches: http://www.cisco.com/en/US/partner/products/ps9902/index.html.

Cisco VSG: http://www.cisco.com/en/US/partner/products/ps11208/index.html.

Cisco ASA 1000V Cloud Firewall: http://www.cisco.com/en/US/partner/products/ps12233/index.html.

Cisco Virtualized Multitenant Data Center Validated Design:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C11-716028-01 06/13