CHAPTER 1

Cisco vPath and vServices Overview

This chapter provides an overview of the Cisco vPath and vServices and includes the following sections:

Information About the Cisco vPath and vServices

This section provides an overview of the Cisco vPath and vServices and includes the following topics:

Overview of vPath

Cisco Virtual Service Data Path (vPath) is the service intelligence embedded in the Cisco Nexus 1000V Series switch.

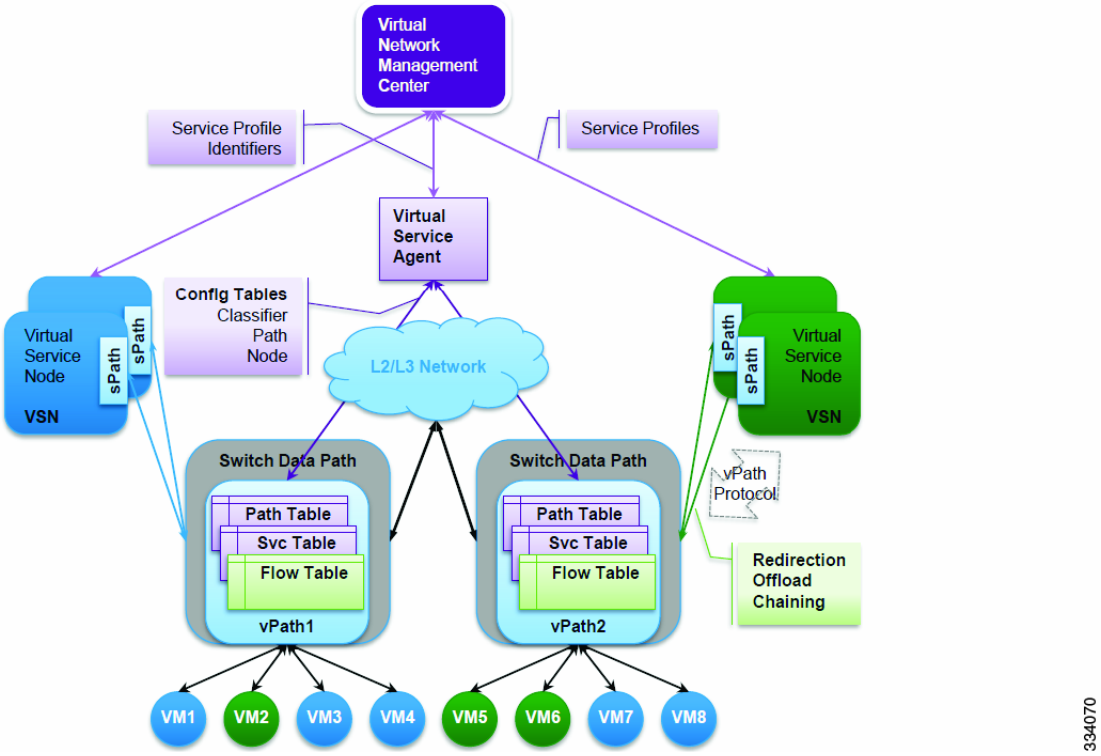
vPath provides the forwarding plane abstraction and programmability required to implement the Layer 2 to Layer 7 network services such as segmentation firewalls, edge firewalls, load balancers, WAN optimization, and others. It is embedded in the Cisco Nexus 1000V Series switch Virtual Ethernet Module (VEM). It intercepts the traffic whether external to the virtual machine or traffic from virtual machine to virtual machine and then redirects the traffic to the appropriate virtual service node (VSN) such as Cisco Virtual Security Gateway (VSG), Cisco ASA 1000V, Cisco Virtual Wide Area Application Services (vWAAS) for processing. vPath uses overlay tunnels to steer the traffic to the virtual service node and the virtual service node can be either Layer 2 or Layer 3 adjacent.

The Cisco network virtual service (vService) is supported by the Cisco Nexus 1000V using the vPath. It provides trusted multitenant access and supports the VM mobility across physical servers for workload balancing, availability, or scale.

The basic functions of vPath includes traffic redirection to a virtual service node (VSN) and service chaining. Apart from the basic functions, vPath also includes advanced functions such as traffic off load, accleration and others.

vPath steers traffic, whether external to the virtual machine or from a virtual machine to a virtual machine, to the virtual service node. Initial packet processing occurs in the VSN for policy evaluation and enforcement. Once the policy decision is made, the virtual service node may off-load the policy enforcement of remaining packets to vPath.

Figure 1-1 Virtual Service Datapath (vPath)



Overview of Virtual Services (vServices)

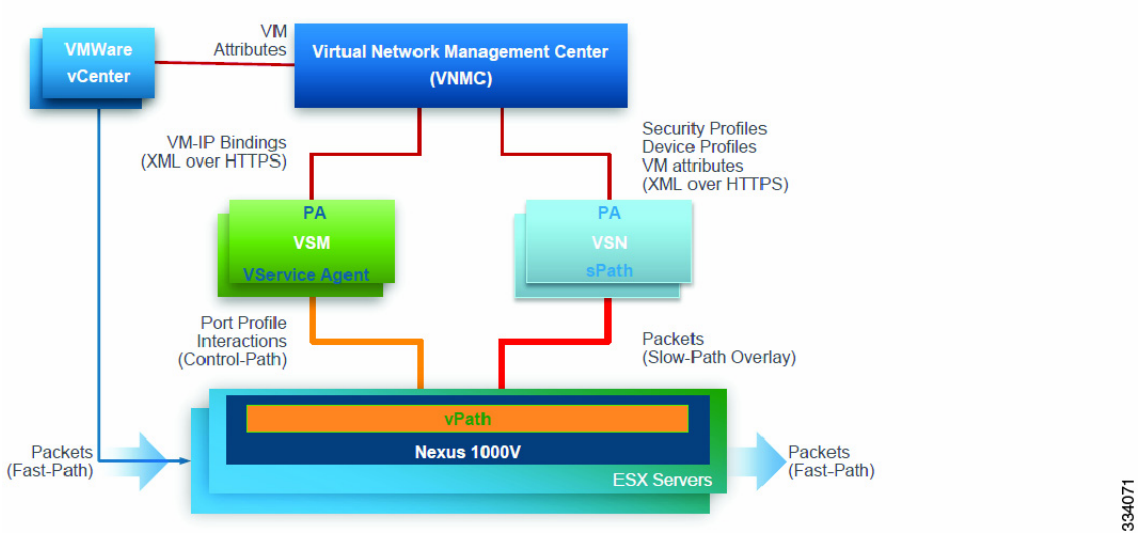
Virtual Services include the various Layer 4 through Layer 7 network services such as firewalls, edge firewalls, load balancers, WAAN optimization and others which are virtualized and delivered as virtual machines.

The following virtual services are supported by Cisco Nexus 1000V Series switch using the vPath:

- **Cisco Virtual Security Gateway (VSG):** Provides trusted multitenant access with granular zone-based security policies for VMs. Cisco VSG delivers security policies across multiple servers. It supports VM mobility across physical servers for workload balancing, availability, or scale.
- **Cisco Virtual Wide Area Network Application Services (vWAAS):** A WAN optimization solution, helps deliver assured application performance acceleration to IT users connected to enterprise data centers and enterprise private clouds.
- **Cisco ASA for 1000V:** Provides trusted security to multi-tenant virtual and cloud infrastructures at the edge. When implemented with the Cisco Nexus 1000V Switch, it provides consistent security across physical, virtual, and cloud infrastructures.

Virtual Services Architecture

Figure 1-2 Virtual Services Architecture



The Virtual Services Architecture provides a framework for delivering virtual services. vPath is the main component of the architecture and it is embedded in the Cisco Nexus 1000V Series switchVEM. It acts as a service traffic classifier and as a service dispatcher. It selects the traffic requiring service and steers it to the appropriate virtual service node for service delivery. vPath performs all its functions on tenant boundaries in order to provide tenant isolation.

The other components of the virtual service architecture includes:

- The Virtual Network Management Center (VNMC), a multi tenant policy manager responsible for device and policy management and integration with VMware vCenter. VNMC is the overall management and orchestration component of the virtual service architecture.
- The Cisco Nexus 1000V Series switchVSM, responsible for all the interactions with vPath and with VNMC.The Virtual Service Agent on theCisco Nexus 1000V Series switch is responsible for all the control aspects of vPath such as traffic classification, traffic redirection, service chaining, traffic off loading and accleration.
- Virtual Service Node (VSN), responsible for the service processing. The various virtual services supported include VSG, vWAAS, ASA for 1000V and others. The VSNs can include many instances of the same virtual service or different virtual service types.

Benefits of vPath and Virtual Services Architecture

vPath and virtual services architecture include the following benefits:

- Dynamic Service Provisioning, page 1-4
- Service Binding, page 1-4
- Service Overlay, page 1-5
- Mobility, page 1-5
- Multi-Tenancy, page 1-6

- Service Accleration and Programmability, page 1-6
- Service Chaining, page 1-7

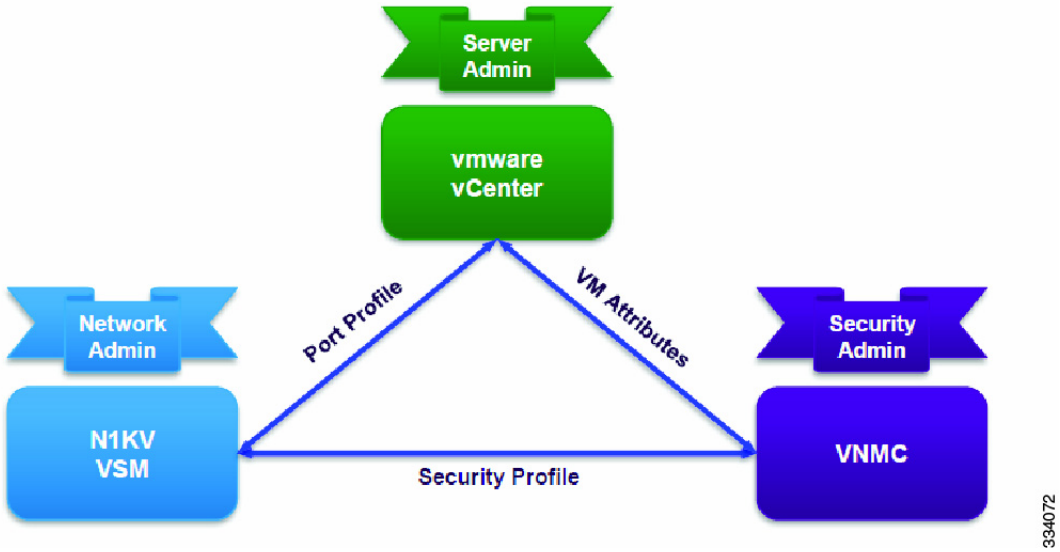
Dynamic Service Provisioning

vPath supports dynamic provisioning of virtual machines via service profiles and ensures that the service profiles follow vMotion events. In a service profile you can configure the service parameters. In VSG and ASA 1000V the service profiles map to a policy. In VSG, the service profile is referred to as a security profile. In ASA 1000V, the service profile is called edge profile.

The service parameters are configured in a service profile and then attached to a port profile. When the virtual machines get instantiated and attached to a port profile, the service profile also gets dynamically attached to the virtual machine.Once associated all the policies are dynamically provisioned to a virtual machine as the virtual machine comes up or moves from one server to another.

The virtual services architecture supports a collaborative management model where the roles and responsibilities of network administrator, server administrator and service administrator are clearly defined.

Figure 1-3 Dynamic Service Provisioning



Service Binding

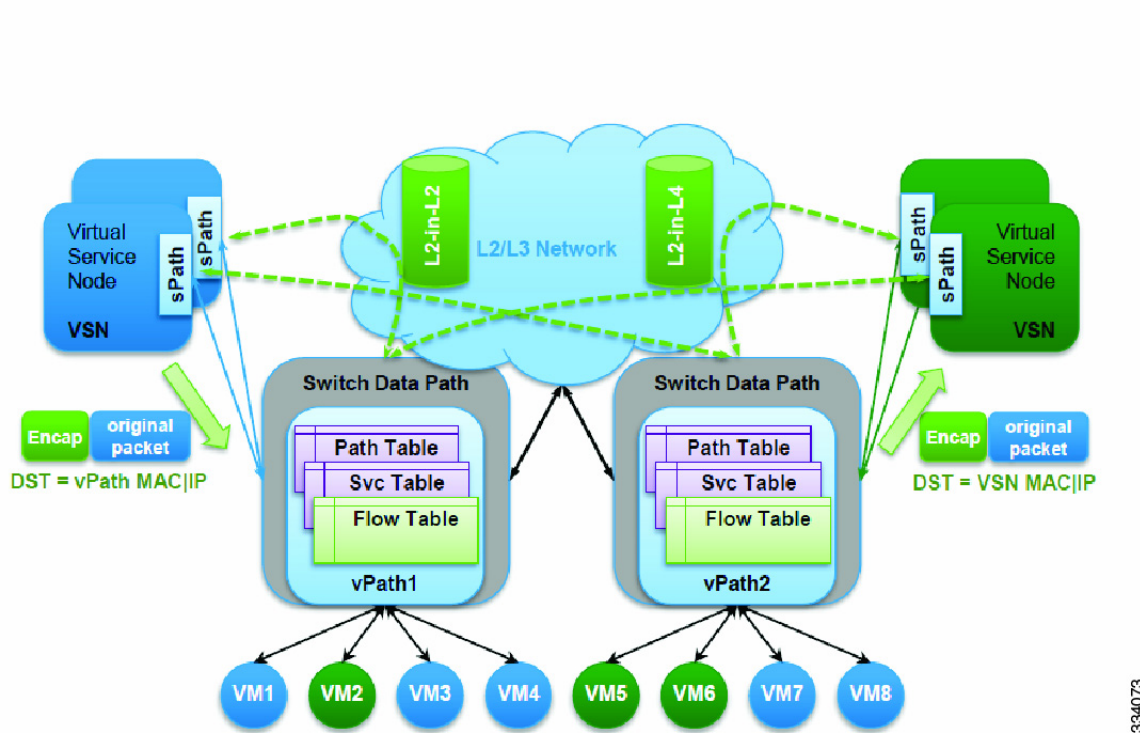
Due to dynamic service provisioning, a service profile is associated with the virtual machines as they are instantiated. vPath then assigns a service profile identifier to the service profile. vPath thus enables different service profile bindings on traffic associated with the different virtual machines. Virtual service nodes then use the service profile identifier to choose the appropriate policy to apply to the traffic or deliver the service.

Service Overlay

vPath uses overlay tunnels to steer the traffic to the virtual service node and the virtual service node can be either Layer 2 or Layer 3 adjacent. The overlay tunnel model enables the mobility of the virtual service nodes and is independent of the transport technologies such as VLAN or VXLAN used in Layer 2 deployments. As shown in the following figure, the tunnels can be L2 or L4. MAC-in-MAC encapsulation is used in the L2 tunnel and MAC in UDP encapsulation is used in the L4 tunnel.

In L4 tunnel, UDP encapsulation enables load balancing of the packets onto the links at the network elements and enables NICs to support Receive Side Scaling (RSS).

Figure 1-4 Service Overlay



Mobility

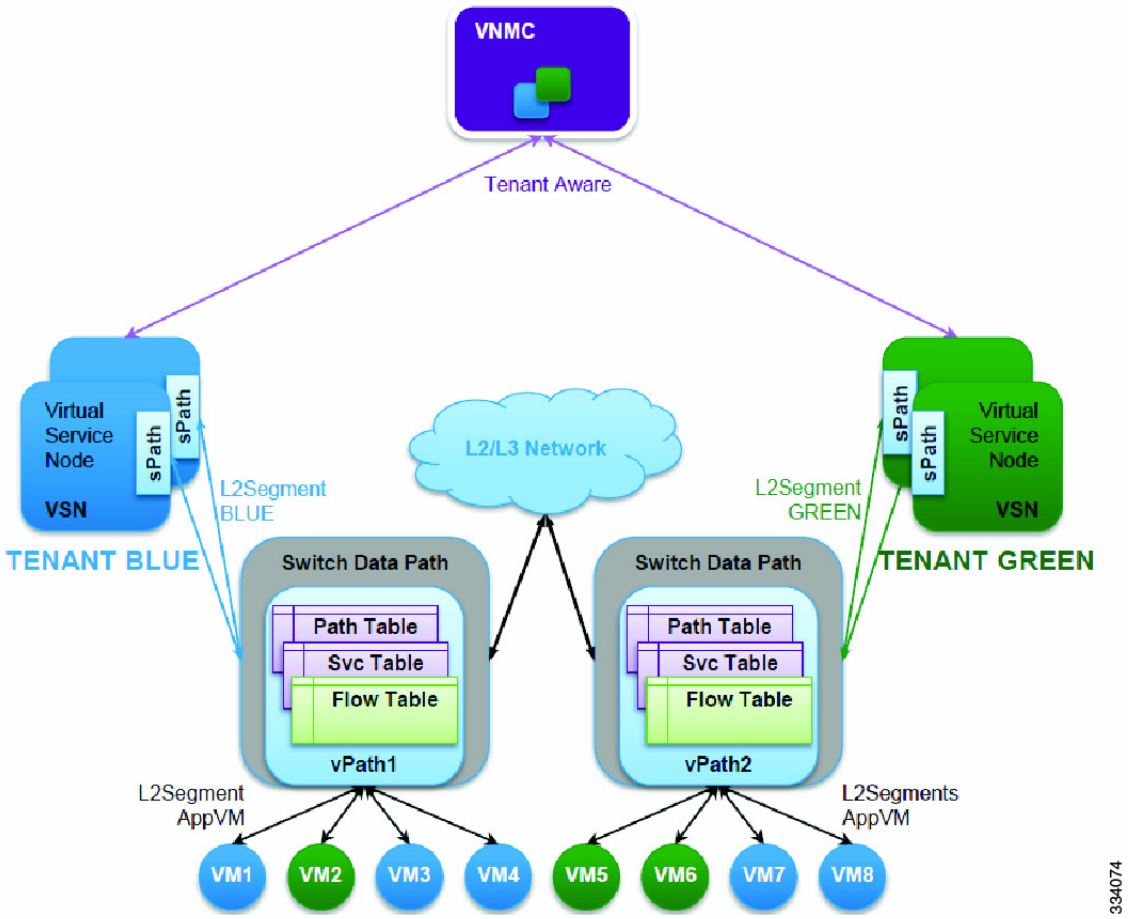
The virtual services architecture enables the mobility of the virtual machine as well as the virtual service node. Dynamic service provisioning ensures that the virtual machine traffic flow continues to be handled by the appropriate virtual service node. This is possible since the service profile remains the same in the port profile and the port profile moves along with the virtual machine. As a result the virtual machine in the new host will continue to use the same virtual service node for service processing.

Service overlay ensures that the virtual service node is reachable on the new host and the virtual machines continue to forward traffic to the same virtual service node.

Multi-Tenancy

vPath is tenant aware and it can serve virtual service nodes belonging to different tenants. The virtual services architecture enables vPath to support overlapping IP addresses among different tenants. vPath steers traffic from the virtual machines to the virtual service nodes in the same tenant thus enabling tenant separation.

Figure 1-5 Multi-tenancy

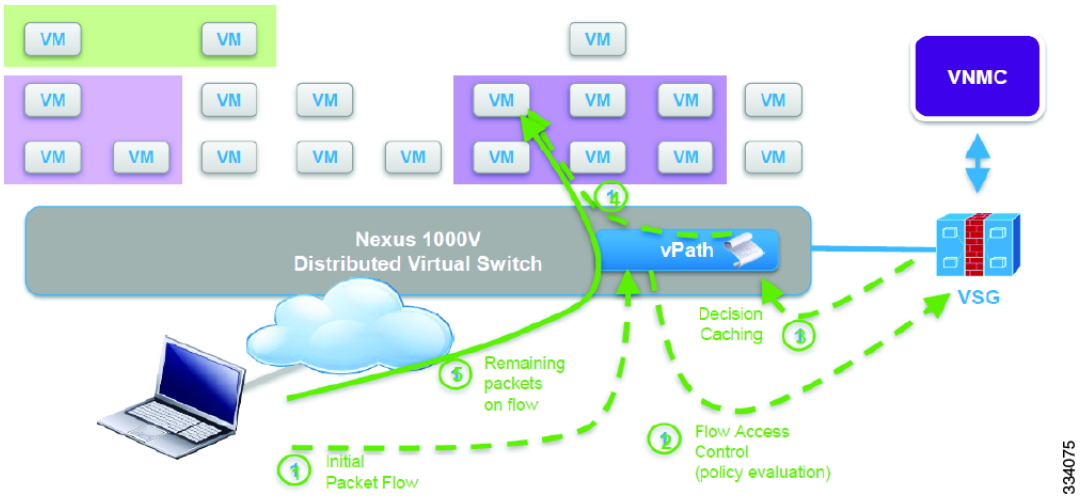


Service Accleration and Programmability

vPath steers traffic, whether external to the virtual machine or from a virtual machine to a virtual machine, to the virtual service node. The virtual service node can either continue to process the redirected traffic or off load the traffic to vPath. The off loaded traffic is processed by vPath leading to increased performance in service delivery of the Cisco Nexus 1000V Series switch.

vPath also has the ability to enforce the actions on the traffic as specified by the virtual service node. Virtual service nodes can then choose to intercept reverse traffic without any static configurations on the switch or choose to off load some traffic.

Figure 1-6 Service Accleration



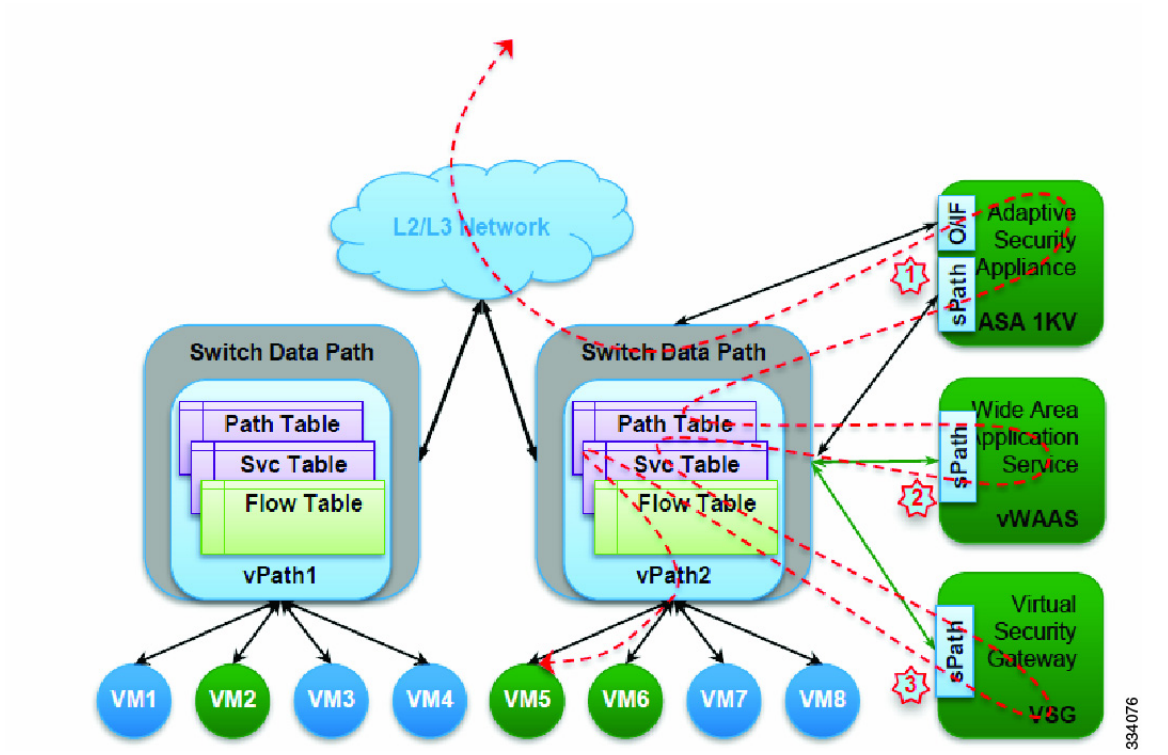
Service Chaining

Service chaining allows multiple service nodes to be included in a service path so that the packets that belong to a particular flow can travel through all the virtual service nodes in the sevice chain. Each service node in a chain uses the security profile specified in the **vservice** command for that VSN.

A service path consists of an ordered list of services to be applied to a packet flow and it is used to define the service chain. When a packet reaches a virtual machine with vPath service chaining enabled, vPath intercepts the packet and redirects the packet to multiple VSNs in a specified order.

vPath thus acts as an orchestrator of the chain to deliver multiple services and VNMC enables the provisioning of service chains.

Figure 1-7 Service Chaining



Currently vPath service chaining supports the following virtual service nodes:

- Cisco VSG
- ASA 1000V

The following order for vPath service chaining is supported:

- VSG -> ASA

You can configure service chaining by using the **vservice** command. When a vservice node is directly bound to a port profile, the Cisco Nexus 1000V considers this binding as a service path with a single service. Cisco Nexus 1000V supports two service options:

- Single service that is bound to a port profile
- Multiple services that are bound to a port profile

A virtual service node can be shared by different service chains and it can be applied at different positions in different chains. The vPath chained services are applied both at ingress and at egress, relative to cisco Nexus 1000V switch. The virtual service node sequence defined in the service path is the order of services that are applied to an ingress packet. For an egress packet, the order is reversed.

For example, if you have a virtual machine that has the following service path:

```
vservice path sp1
    node vsg1 profile vsg-profile1
    node asa1 profile asa-profile1
```

When the traffic is sent by the VM and it arrives at the switch (at ingress), the services get applied in this order:

```
VSG -> ASA
```

When traffic is destined to the VM and leaves the switch (at egress), the services are applied in this order:

```
ASA -> VSG
```

Note Because the Cisco ASA 1000V must be the last node in the chain, Cisco supports this order only for the current release.

Version Compatibility

The following table lists the version compatibility of the virtual service nodes with Cisco Nexus 1000V Series switch.

Table 1-1 Virtual Service Node and Nexus 1000V Release Compatibility

Virtual Service Node	Minimum Required Version of Cisco Nexus 1000V
Cisco Virtual Service Gateway (VSG)	4.2(1)SV1(4)
Cisco Virtual Wide Area Network Application Services (vWAAS)	4.2(1)SV1(4)
Cisco ASA for 1000V	4.2(1)SV1(5.2)

The following table lists the version compatibility of the vPath features with Cisco Nexus 1000V Series switch.

Table 1-2 vPath Features Compatibility with Nexus 1000V Release

vPath Features	Minimum Required Version of Cisco Nexus 1000V
Traffic redirection	4.2(1)SV1(4)
Off load	4.2(1)SV1(4)
Accleration	4.2(1)SV1(4)
Multi-tenancy	4.2(1)SV1(4)
TCP state full checks	4.2(1)SV1(4a)
VSN ping	4.2(1)SV1(4a)
L3 adjacency	4.2(1)SV1(5.1)
VMs on VXLAN	4.2(1)SV1(5.1)
VSN on VXLAN	4.2(1)SV1(5.2)
Service chaining	4.2(1)SV1(5.2)

Licensing

Since Cisco Virtual Service Data Path (vPath) is the service intelligence embedded in the Cisco Nexus 1000V Series switch, one Cisco Nexus 1000V Series switch license is needed for each installed server CPU on every VEM in the distributed architecture.There is no limit to the number of cores per CPU. See *Cisco Nexus 1000V License Configuration Guide, Release 4.2(1)SV1(5.1)* for more information on Cisco Nexus 1000V Series switch license.

In addition to the Cisco Nexus 1000V Series switch license, you also require license for some of the virtual services such as VSG and ASA1000V.

See the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(4.1)* for more information on VSG license.

See the *Cisco ASA 1000V* documentation for more information on ASA1000V license.

Cisco Nexus 1000V Series switch does not require any licenses for vWAAS, but vWAAS may have its own licensing requirements.

See the Cisco vWAAS documentation for more information on vWAAS license.