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, page 1-1
- Version Compatibility, page 1-10
- Licensing, page 1-11

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, page 1-1
- Overview of Virtual Services (vServices), page 1-2
- Virtual Services Architecture, page 1-3
- Benefits of vPath and Virtual Services Architecture, page 1-3

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 between virtual machines and then redirects the traffic to the appropriate virtual service (vservice) 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 basic functions of vPath includes traffic redirection to a vservice and service chaining. Apart from the basic functions, vPath also includes advanced functions such as traffic off load, acceleration 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 vservice 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.

**Note**

The maximum vPath connection limit is 64,000. For more information, see *Cisco Virtual Security Gateway for VMware vSphere Release Notes*.

**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.

Citrix NetScaler 1000v: provides service delivery platform with the most comprehensive set of application security, acceleration and load balancing capabilities across the platforms.

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 Cisco Prime Network Services Controller (PNSC), a multi-tenant policy manager responsible for device and policy management and integration with VMware vCenter. PNSC 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 PNSC. The Virtual Service Agent on the Cisco Nexus 1000V Series switch is responsible for all the control aspects of vPath such as traffic classification, traffic redirection, service chaining, traffic offloading and acceleration.

- Virtual Service (vservice), responsible for the service processing. The various virtual services supported include VSG, vWAAS, ASA for 1000V, Citrix NetScaler 1000V, and others. The vservices 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

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.
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).
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.
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.
Service Chaining

A service chain is an ordered list of services applied to a packet flow or traffic. A service path identifies a forwarding path used to implement a service chain.

The vPath intercepts traffic (packets/frames) originating from a virtual machine or destined to a virtual machine and directs the traffic through the service path delivering the traffic to each service along the path. vPath thus acts as an orchestrator of the chain to deliver multiple services and PNSC enables the provisioning of service chains.
Currently vPath service chaining supports the following virtual service nodes:

- Cisco VSG
- ASA 1000V
- vWAAS
- Citrix NetScaler 1000V

The service chain can have the following path configuration:

- vWAAS -> ASA 1000V -> Citrix NetScaler 1000V -> VSG
- ASA 1000V -> VSG
- ASA 1000V -> Citrix NetScaler 1000V
- ASA 1000V -> Citrix NetScaler 1000V -> VSG
- Citrix NetScaler 1000V on N1110 -> VSG

For example, in case of VSG -> ASA 1000V vPath service chaining, you can configure service chaining by using the vservice command. When a service 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:

```bash
vservice path sp1
node vsg1 profile vsg-profile1
node asal 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

Example of vService path with VSG and Citrix NetScaler 1000V node.

```
vservice path path1
node vsg1 profile sp2 order 1
node Citrix NetScaler 1000V order 2
```

## Version Compatibility

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

<table>
<thead>
<tr>
<th>Virtual Service Node</th>
<th>Minimum Required Version of Cisco Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Virtual Service Gateway (VSG)</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>Cisco Virtual Wide Area Network Application Services (vWAAS)</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>Cisco ASA for 1000V</td>
<td>4.2(1)SV1(5.2)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>vPath Features</th>
<th>Minimum Required Version of Cisco Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic redirection</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>Off load</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>Acceleration</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>4.2(1)SV1(4)</td>
</tr>
<tr>
<td>TCP state full checks</td>
<td>4.2(1)SV1(4a)</td>
</tr>
<tr>
<td>vservice ping</td>
<td>4.2(1)SV1(4a)</td>
</tr>
<tr>
<td>L3 adjacency</td>
<td>4.2(1)SV1(5.1)</td>
</tr>
<tr>
<td>VMs on VXLAN</td>
<td>4.2(1)SV1(5.1)</td>
</tr>
<tr>
<td>vservice on VXLAN</td>
<td>4.2(1)SV1(5.2)</td>
</tr>
<tr>
<td>Service chaining</td>
<td>4.2(1)SV1(5.2)</td>
</tr>
</tbody>
</table>
Licensing

Starting with Release 4.2(1)VSG2(1.1), Cisco VSG license is integrated with the Cisco Nexus 1000V Multi-Hypervisor License. You need to install the Nexus1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere. The Cisco Nexus 1000V VSM is available in two modes: essential and advanced. VSG functionality is available only in the advanced mode. You need to install the Nexus 1000V Multi-Hypervisor License and change the VSM mode to advanced mode. When the Nexus1000V Multi-Hypervisor License is installed, the license for Cisco VSG is automatically included.

For more information about Nexus1000V Multi-Hypervisor License for Cisco VSG for VMware vSphere, see the *Cisco Nexus 1000V for Microsoft Hyper-V License Configuration Guide*.

**Note**

On Cisco Nexus 1000V VEM, the VSG license checkout happens as soon as the VEM comes online even if there is no port with VSG protected VM. If you try to bring up a protected port on an offline VEM, the protected port (configured with VSG or ASA vservice) cannot be brought up in headless mode because the License checkout on VEM does not happen when VSM-VEM connectivity is down.