White Paper

Cisco Nexus 1000V Series Switches: Deploy Cisco vPath Service-Chaining Architecture

What You Will Learn

Network services such as firewalls, load balancers, and WAN optimization are critical for providing the security, scalability, resiliency and enhanced user experiences that today's business applications demand. Deployment of multiple network services in the traffic path is a complex process and often requires the use of multiple VLANs, resulting in reconfiguration of switches and routers. In addition, there is no central place at which network administrators can configure all the services they want in a specific order. The Cisco® Virtual Services Data Path (vPath) service-chaining capability of the Cisco Nexus® 1000V Series Switches simplifies the deployment of network services, providing operational simplicity and business agility in multitenant private and public cloud deployments.

Cisco vPath Architecture

Cisco vPath provides embedded intelligence within Cisco Nexus 1000V Series virtual Ethernet modules (VEMs). The Cisco vPath architecture provides a forwarding-plane abstraction and a programmable framework for inserting network services such as firewalls, load balancers, and WAN optimization at the virtual access layer. Cisco vPath is implemented in the switch data path with a set of configuration tables, flow tables, and well-defined interfaces for adding and removing flow entries. Each entry in the flow table associates a data path action (for example, a redirect, permit, or drop action). Cisco vPath enables separation of the control plane and data plane with well-defined APIs.

Because Cisco vPath resides in the switch data path, if configured, it can intercept the incoming traffic and the virtual machine-to-virtual machine traffic and redirect it to appropriate network services for processing. The network service nodes can be deployed as either Layer 2 or Layer 3 adjacent to Cisco vPath. Cisco vPath uses overlay tunnels for redirecting packets to network service nodes. Network services can optionally offload packet processing from network service nodes by programming appropriate flow entries in the Cisco vPath flow table, and also can insert flow entries to intercept traffic on demand. Cisco vPath also provides data-path orchestration to chain multiple services as well as service clustering to scale services.

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 multi-tenancy awareness
- Enables data-path accelaration 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

Cisco vPath Service-Chaining Architecture

The Cisco Nexus 1000V vPath service-chaining feature provides the capability to define multiple network services in a specific order that network traffic flow must follow to reach the end application. Network administrators can define the network services in the Cisco Nexus 1000V Series port profile, and they can also define the specific order that they want the traffic flow to follow for the defined network services. This Cisco Nexus 1000V vPath capability significantly simplifies the deployment of virtual network services. Because network services can be defined in a centralized place, it also makes insertion and removal of network services much simpler.

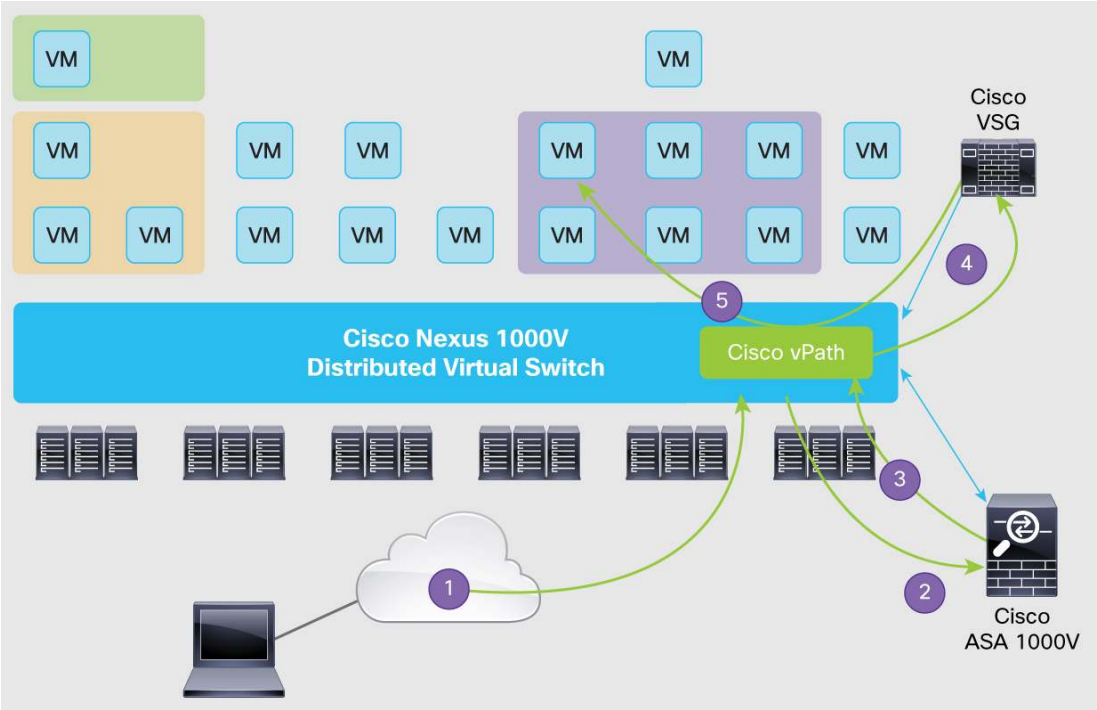
Cisco Nexus 1000V vPath currently supports the following Cisco network services:

- Cisco Virtual Security Gateway (VSG): Firewall within the tenant
- Cisco ASA 1000V Cloud Firewall: Tenant-edge firewall
- Cisco Virtual Wide Area Application Services (vWAAS): Virtual WAN optimization service

The Cisco vPath service-chaining capability is available with Cisco Nexus 1000V Series Switches Release 1.5(2) and later. The first release of Cisco vPath service-chaining supports two network services, Cisco ASA 1000V and Cisco VSG.

Figure 1 illustrates the virtual multitenant security use case using Cisco Nexus 1000V Series service-chaining capabilities with Cisco VSG and Cisco ASA 1000V. Securing a virtual multitenant data center requires tenant-edge firewalls that can protect northbound and southbound traffic and also firewalls within the tenant that can protect eastbound and westbound traffic. Cisco ASA 1000V and Cisco VSG provide a comprehensive security solution for both tenant-edge and intratenant security needs using the Cisco Nexus 1000V vPath service-chaining feature.

Figure 1. Cisco Nexus 1000V vPath Service Chaining Using Cisco ASA 1000V and Cisco VSG



Cisco Nexus 1000V vPath is flow aware. It maintains flow tables to track the state of each flow. For example, a given flow may include the following events:

1. Cisco vPath intercepts packets for a new flow destined for a virtual machine. It looks up the flow table and determines that the new flow does not exist.
2. On the basis of the user configuration, Cisco 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. Network services evaluate the policy and send the 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.
4. 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.

Conclusion

Cisco Nexus 1000V vPath 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 data centers. In addition, the Cisco vPath service-chaining capability 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 C11-713736-00 08/12