

Cisco Nexus 1000V Switch and Cisco vPath 2.5 Virtual Services Ecosystem

Introduction

The Cisco Nexus® 1000V Switch offers Cisco® Virtual Services Data Path (vPath) architecture to support virtualized network services with intelligent traffic steering, service chaining, and performance acceleration.

Cisco vPath Service Chaining is a new model for delivering virtual services for the dynamic virtualized or cloud-based data center. Cisco vPath provides embedded intelligence within Cisco Nexus 1000V virtual Ethernet modules (VEMs) to dynamically apply multiple services to virtual machine traffic. Cisco vPath communicates with service nodes over Cisco vPath overlay tunnels, decoupling service nodes from the underlying network topology. The Cisco vPath architecture provides a forwarding-plane abstraction and a programmable framework for inserting or removing network services such as distributed and edge firewalls, load balancers, and WAN optimization at the hypervisor layer.

Before Cisco vPath Service Chaining, Cisco vPath supported only Cisco virtual network services chained per port profile. With the Cisco vPath Release 2.5 ecosystem release, you can add both Cisco and third-party virtual services seamlessly in a service chain per port profile.

This guide explains the Cisco vPath Service Chaining architecture, provides deployment guidelines, and explains how to enable Cisco vPath Service Chaining addressing most common use cases.

Intended Audience

This document is intended for security architects, network architects, network engineers, virtualization administrators, cloud architects, and server administrators interested in understanding and deploying Cisco vPath Service Chaining with Cisco Virtual Security Gateway (VSG), Citrix NetScaler 1000V, Cisco Virtual Wide Area Applications Services (vWAAS), and Cisco Adaptive Security Appliances (ASA) for Nexus 1000V Series Switch in a virtual VMware environment using a Cisco Nexus 1000V distributed virtual switch.

Cisco vPath Benefits

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

- Enables transparent addition of Cisco and third-party services per virtual machine port
- Enables policy-based service insertion for virtual workloads
- Eliminates the need to place network services inline or tied to the application virtual machine's network topology; 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
- Lack of support for dynamic scaling of resources
- Lack of single-control management for different services, such as virtual machine security, firewall, Network Address Translation (NAT), VPN, and server load balancing

In the absence of an efficient service-chaining architecture, physical and virtual network elements and service appliances must be manually configured, leading to complex topologies that do not scale well.

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

Networks have long needed the capability 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 transparent provisioning of these services.

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

- Capability to span virtualized computing resources in public, private, or hybrid cloud environments, with zone and edge security
- Capability to enforce policies based on full contextual understanding of security and virtual machine contexts
- Robust platform that provides transparent integration with a variety of virtual services and supports data acceleration by offloading policy from service nodes
- Single management interface for intratenant and tenant-edge security services

Cisco vPath is an intelligent traffic interception and detailed policy-enforcement engine for a variety of network services. Cisco vPath can accelerate the data path by offloading policy from network services to Cisco.

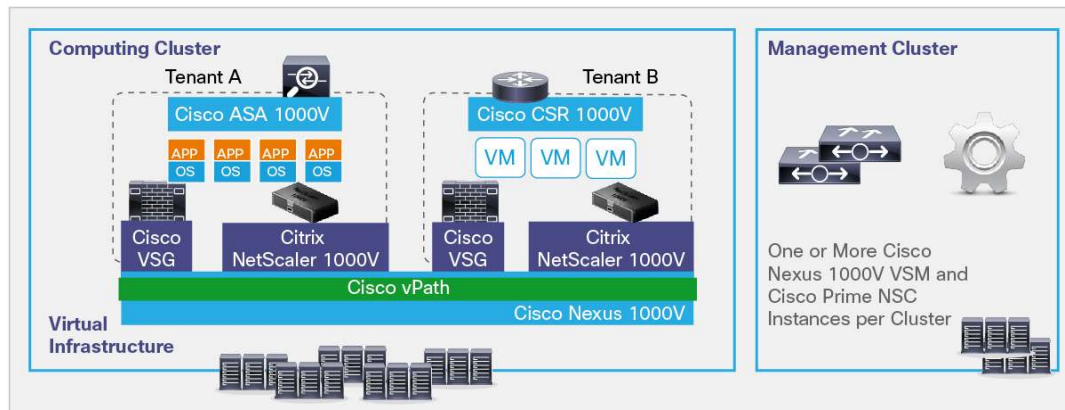
The Cisco Nexus 1000V with Cisco vPath currently supports the following Cisco network services:

- Cisco VSG: Transparent, zone-based intratenant computing firewall for east-west traffic
- Citrix NetScaler 1000V: Application delivery controller that provides Layer 4 through 7 server load balancing with additional features
- Cisco vWAAS: Virtual WAN optimization service for accelerating applications and reducing the network traffic footprint on WAN links
- Cisco ASA 1000V Cloud Firewall: Tenant-edge firewall that provides security for north-south traffic

Cisco vPath Service Chaining is available with Cisco Nexus 1000V Switch Release 2 (2.1a), Cisco VSG Release 2.1, Citrix NetScaler 1000V Release 10.1, Cisco ASA 1000V Release 8.7.1, and Cisco Prime™ Network Services Controller (NSC) Release 3.0.2 and later.

Figure 1 presents a logical diagram of a multitenant environment with Cisco vPath Service Chaining.

Figure 1. Logical Diagram of Multitenant Environment Positioning Cisco VSG, Cisco Cloud Services Router (CSR) 1000V, Citrix NetScaler 1000V, and Cisco ASA 1000V



Integrating Ecosystem Services with Cisco vPath

In the first ecosystem release of Cisco vPath 2.5, Citrix NetScaler 1000V is tightly integrated with Cisco vPath for intelligent interception and redirection.

Citrix NetScaler 1000V is a software-based virtual application delivery controller (ADC) appliance that provides the comprehensive Citrix NetScaler feature set. This easy-to-deploy application delivery solution can be integrated with the overall [Cisco Nexus 1000V cloud networking portfolio](#) and run on multiple hypervisor platforms. In this way, it can be deployed on demand anywhere in the data center using the [Cisco Nexus 1100 Cloud Services Platform](#) or as a virtual machine on the VMware vSphere hypervisor.

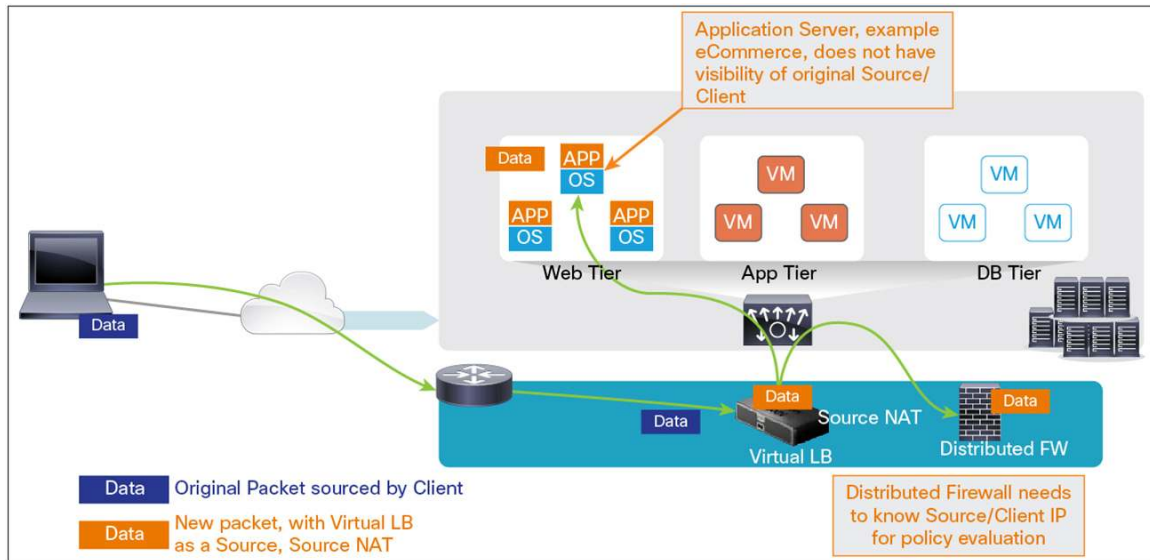
The simplicity and flexibility of Citrix NetScaler 1000V make it a cost-effective tool for fully optimizing every web application and more effectively integrating networking services with application delivery.

Virtual Server Load-Balancer Challenges without Cisco vPath

Typically, the server load balancer (SLB) needs to see traffic in both directions - from client to the server and from the server to the client - to apply stateful load-balancing policies. To help ensure that reverse packets - that is, packets that originated in the server-to-client direction - are received by the SLB, the SLB is deployed with one of following options (Figure 2):

- **Source NAT:** Source NAT is the preferred option and is easy to deploy. With this option, the source IP address for the packet is changed to that of the SLB. In this case, the original client or source information is hidden from the application server. If any other service, such as a distributed firewall, is enabled for the application virtual machine between the SLB and the application, this service will also not know who the original source is and will fail on policy evaluation.

Figure 2. Virtual Load Balancer without Cisco vPath

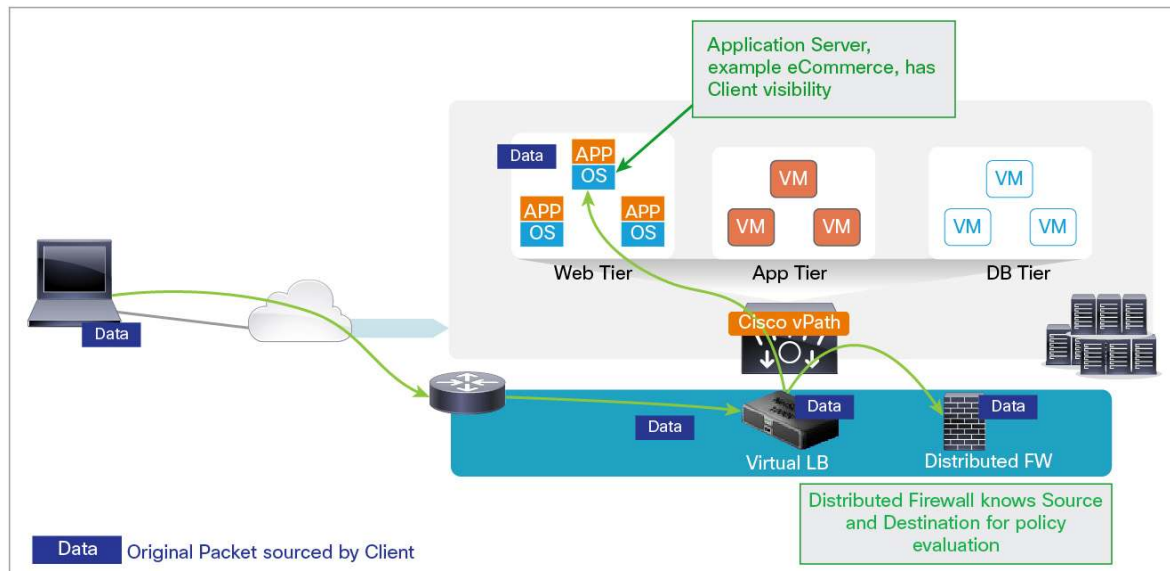


- Policy-Based Routing (PBR): This option routes server return packets to the virtual load balancer. It is a highly complex option and increases operation overhead.
- Inline mode: This option deploys the SLB as an inline device, making it the default gateway for workload servers. It can lead to performance bottlenecks and does not provide an optimal use of resources because it does not allow selective processing, to process only traffic of interest to the virtual load balancer.

The integration of Cisco Nexus 1000V, Cisco vPath, and Citrix NetScaler 1000V offers a number of benefits (Figure 3):

- Preserves source information without the need for Source NAT or PBR; Cisco vPath redirects server return traffic to Citrix NetScaler 1000V.
- Enables topology-agnostic service deployment, providing more agility and scalability and ease of deployment.
- Enables transparent service chaining with other network services such as distributed firewalls active between the load balancer and the back-end servers.
- Enables new east-west flow use cases for server load balancing.

Figure 3. Virtual Load Balancer with Cisco vPath



Cisco vPath Service Chaining Architecture Components

The Cisco vPath Service Chaining architecture has four main components: the management plane, control plane, virtual service nodes (VSNs), and service data plane.

Management Plane

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

Cisco Prime NSC also provides northbound XML APIs to be programmed using a variety of orchestration tools. Cisco Prime NSC interacts with Cisco Nexus 1000V virtual supervisor module (VSM) control-plane and server-management entities such as VMware vCenter to fetch virtual machine-specific attributes and states.

Citrix NetScaler 1000V can be managed using an embedded management web interface; alternatively, management is available through Cisco Prime NSC.

Control Plane

The Cisco virtual network service agent (VNSA) running in the Cisco Nexus 1000V VSM is the control-plane bridge between Cisco Prime NSC and Cisco vPath. The VSM in its primary function is the distributed virtual switch (DVS) that manages all the Cisco VEMs that are part of the DVS. In virtual services architecture, virtual service agents on the VSM propagate virtual machine notifications to Cisco Prime NSC to fetch additional information from host management entities such as VMware vCenter.

The VNSA is primarily responsible for all interactions with Cisco vPath, which includes programming of service tables, service path tables, flow tables, and Cisco vPath statistics.

Virtual Service Nodes

Each service instance (for example, Cisco VSG or Cisco ASA Cloud Firewall) is defined as a VSN. VSNs typically belong to a single tenant. Each service node can be either Layer 2 or Layer 3 adjacent to Cisco vPath. Cisco VSG service-specific traffic transport between Cisco vPath and the 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 Cisco vPath, which is embedded in the VEM on the Cisco Nexus 1000V. Cisco vPath is a distributed service data path, service traffic classifier, and service enforcement point. Cisco vPath intercepts traffic in the switch data plane in both directions (that is, both ingress and egress flows).

Cisco 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 the service path.
- Path table: Orchestrates delivery of multiple services in a particular order for the same flow.
- Flow table: Tracks the state of each flow.

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

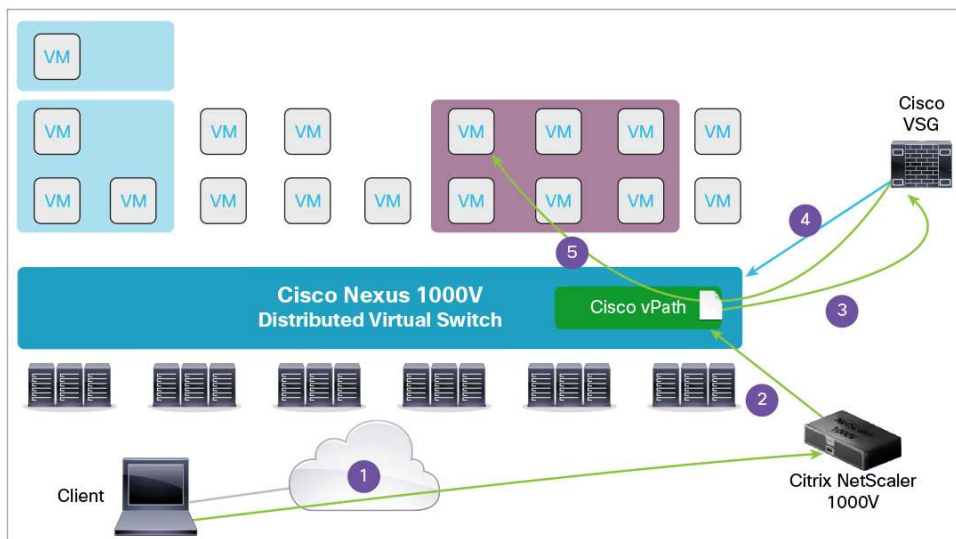
Cisco vPath Service Chaining Packet Flow

The examples that follow show packet flow in detail with Cisco VSG and Citrix NetScaler 1000V virtual services enabled with Cisco vPath.

Cisco vPath Service Chaining Example with Cisco VSG and Citrix NetScaler 1000V

In the example in Figure 4, the client is trying to access a web application server running in a virtual machine protected by Cisco VSG and load balanced with Citrix NetScaler 1000V.

Figure 4. Cisco vPath Service Chaining Client-to-Server Flow 1

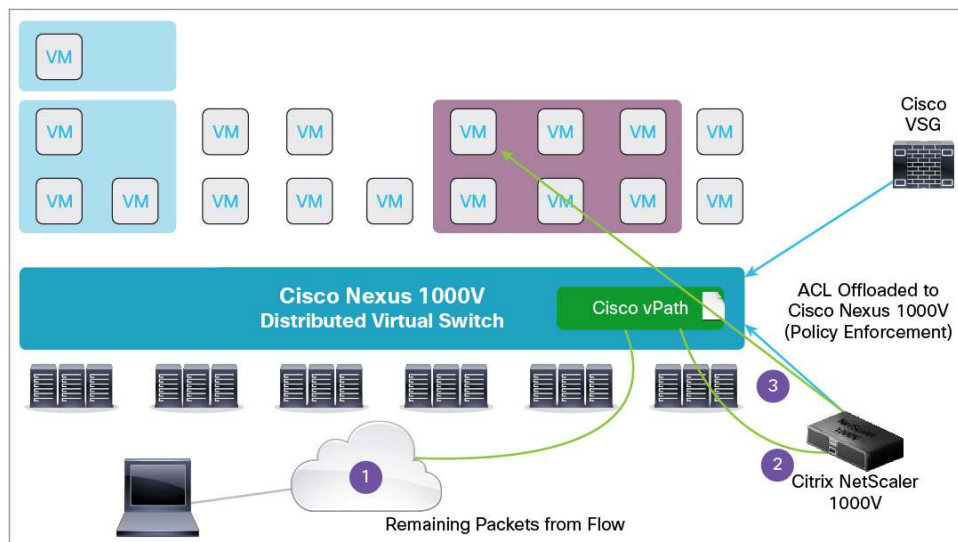


The flow shown in Figure 4 includes the following events:

1. The initial packet sourced from the client is destined for the Citrix NetScaler 1000V's virtual IP address. Citrix NetScaler 1000V selects the destination web server on the basis of the configured load-balancing algorithm. Citrix NetScaler 1000V is inline for the flow originating outside (on the Internet), and this packet does not go through Cisco vPath, but directly to Citrix NetScaler 1000V. After policy evaluation, Citrix NetScaler 1000V encapsulates the original packet with a Cisco vPath header and forwards it to the destination web server.
2. The packet arrives at the data plane of the Cisco Nexus 1000V (the VEM) to which the web server virtual machine is connected. Cisco vPath, watching this virtual machine, intercepts the packet, removes the Cisco vPath encapsulation, and creates an entry for this connection, for packets received from Citrix NetScaler 1000V.
3. Cisco vPath looks up the flow table, identifies whether the flow is a new flow, looks up the service-path table for the next service in the path, and encapsulates and forwards the packet to the Cisco VSG service node for new flows.
4. Cisco 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 other packets in the flow.
5. On the basis of the decision received from Cisco VSG, in this example Cisco vPath enforces the policy decision to permit traffic and forwards the packet to the virtual machine.
6. As shown in Figure 5, subsequent flows from the outside client come to Citrix NetScaler 1000V, and after load balancing, Cisco vPath forwards these flows directly to the virtual machine on the basis of the cached Cisco VSG policy decision.

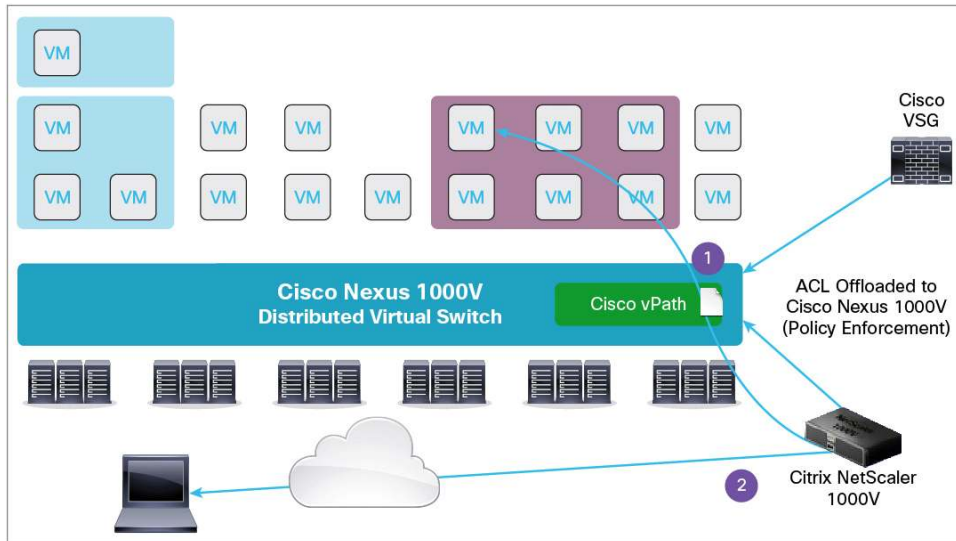
Figure 5. Service Chaining Client to Server Flow 2

Remaining Packets from Flow



7. As shown in Figure 6, for a response packet from the web server virtual machine to the client, Cisco vPath intercepts the packet, enforces cached distributed firewall Cisco VSG policies, and redirects the packet to Citrix NetScaler 1000V, which is the next service in the service chain for the web server virtual machine. Finally, Citrix NetScaler 1000V updates the source IP address to the virtual IP address and forwards the packet to the client.

Figure 6. Server to Client Flow with Cisco vPath



Network services optionally instruct Cisco vPath to offload additional processing of the flow to Cisco vPath, providing performance acceleration for 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 policy configuration.

Communication Between Cisco vPath and Service Nodes

Service nodes can be Layer 2 or Layer 3 adjacent to Cisco vPath and the VEM. In the Cisco vPath Release 2.5 ecosystem, all services except Cisco ASA 1000V in a service chain need to be configured as Layer 3 adjacent to Cisco vPath.

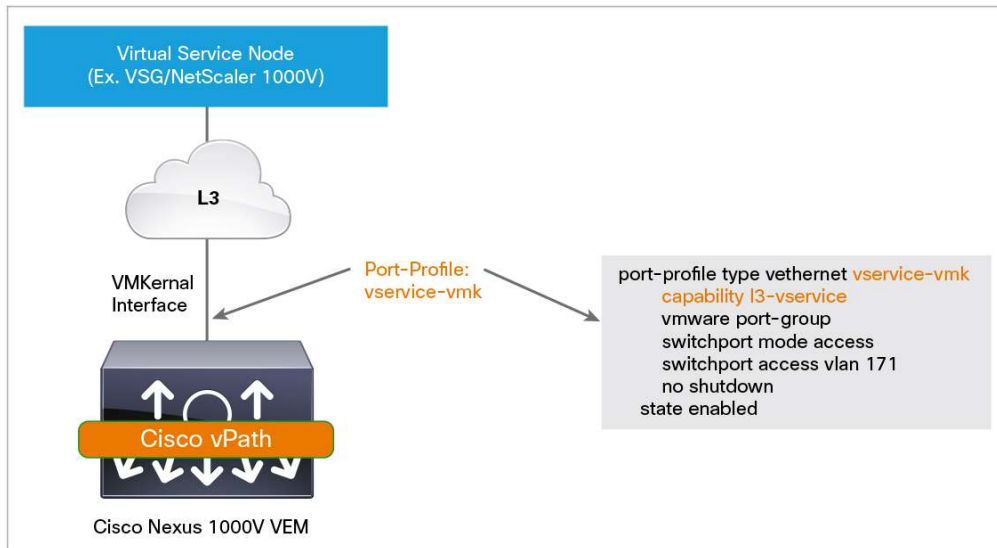
Service nodes and Cisco vPath communicate in two ways:

- Over Layer 2: If the VEM and the 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 the service node are in different Layer 2 domains, the Layer 3 connectivity mode should be used. The Layer 3 mode encapsulates the packet using MAC-in-UDP tunnels. The service node implementation is independent of Cisco Nexus 1000V VSM-to-VEM communication (whether in Layer 2 or Layer 3 mode).

In the case of Layer 3 adjacency, a VMware VMkernel interface is created on every host and hypervisor with a **capability-l3-vservice** port profile attached to it. VMkernel used for VSM-VEM control communication can be shared for **capability-l3-vservice**, or you can use a dedicated VMkernel to keep data separate from management traffic.

Figure 7 shows a sample configuration of a port profile attached to the VEM VMkernel interface.

Figure 7. Cisco vPath Layer 3 Adjacency: Add the **capability-l3-vservice** Port Profile to the VMkernel Interface



Cisco vPath Service Chaining Features

Cisco vPath Service Chaining architecture supports and enhances dynamic provisioning, multitenancy, and mobility features. It does not affect any functions of these features, and it preserves administrative boundaries.

Dynamic Service Provisioning

Dynamic service provisioning helps ensure that services are associated with the virtual machines and not tied to routers or switch ports. Therefore, policies stay with a virtual machine when the virtual machine is moved with VMware vMotion and are dynamically applied to a new virtual machine when the virtual machine is launched.

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

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

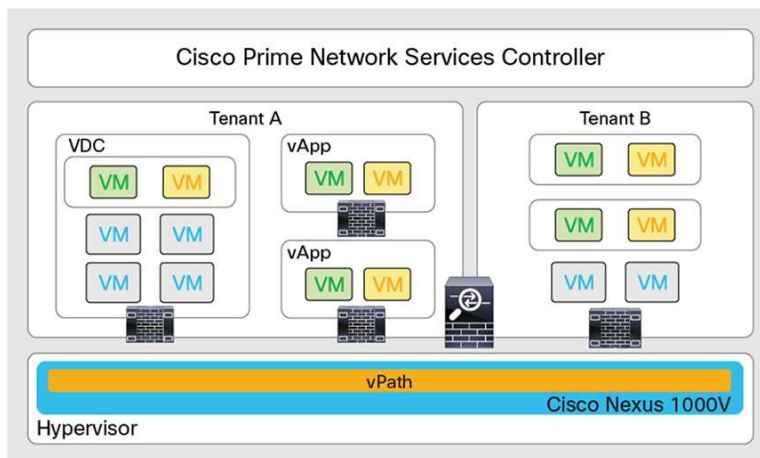
Multitenancy

Cisco vPath tables are multitenant aware, so each Cisco vPath instance can serve virtual machines and service nodes that belong to a variety of tenants. Cisco vPath redirects virtual machine traffic to the service node belonging to the same tenant as the virtual machine. This approach enables clear tenant separation while providing the benefits of virtualization, including tenant scalability.

Cisco Prime NSC is designed to manage Cisco VSG, Cisco 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. Cisco Prime NSC provides a single point for managing all Cisco vPath ecosystem virtual services.

Figure 8 shows Cisco vPath Service Chaining in a multitenant environment, with multitenant deployment of Cisco VSG. In the design shown in the figure, Tenant A has its own Cisco VSG, which provides security policies for its virtual machines. Tenant B has its own separate Cisco VSG to manage its security policies for its virtual machines.

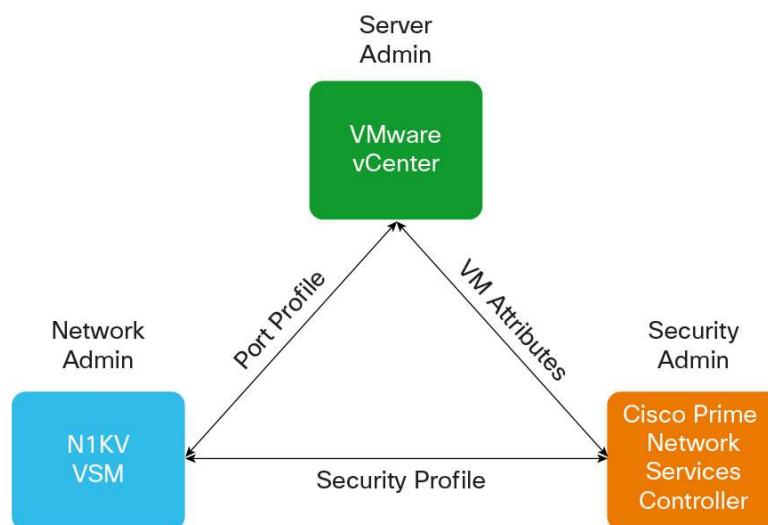
Figure 8. Multitenant Environment



Administrative Boundaries

Cisco vPath virtual services architecture facilitates a collaborative management model in which roles and responsibilities are clearly defined (Figure 9). The security administrator owns security policy, the network administrator owns network policy, and the server administrator associates network policy with virtual machines. After all the policies with port profiles are associated, policies are dynamically provisioned when a new virtual machine is activated or the virtual machine moves from one server to another.

Figure 9. Preserving Administrative Boundaries



Mobility

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

VXLAN

Service nodes can be deployed on VXLANs 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 through the service contexts in the service encapsulation. The packet flows are the same for both VLAN and VXLAN.

Cisco vPath is VXLAN aware, with Layer 2 flow interception and adjacency supported to intercept Layer 2 frames on the VXLAN interface or the virtual machine. Cisco vPath can support mixed-mode of interception and adjacency, with the intercepted traffic on VXLAN, the service node on VXLAN, or both entities are on VXLAN.

Note: New services added in Cisco vPath Release 2.5 for ecosystem deployment do not support virtual machines or service nodes on VXLAN segments.

Enabling Cisco vPath Service Chaining in the Virtual Data Center

The sections that follow explain step by step how to deploy virtual services using Cisco VSG and the Citrix NetScaler 1000V ADC in a virtual data center. Two use case are presented as examples.

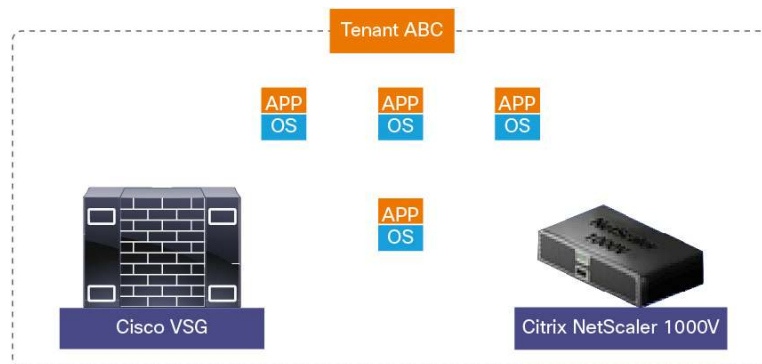
The configurations discussed in this document use the following versions of the software components:

- Cisco Nexus 1000V Release 2.2.1a
- Cisco VSG Release 2.1
- Cisco Prime NSC Release 3.0
- Cisco ASA 1000V Release 8.7.1
- Citrix NetScaler 1000V Release 10.1
- Cisco vWAAS
- VMware vSphere and vCenter Release 5.0 or 5.1

Cisco vPath 2.5 Ecosystem Use Case 1: Deploying Cisco VSG and Citrix NetScaler 1000V in a Service Chain for Virtual Machines per Tenant

In use case 1, **Cisco VSG and Citrix NetScaler 1000V** are deployed in a service chain for virtual machines per tenant. Cisco VSG provides virtual machine isolation with zone-based firewall policies, and Citrix NetScaler 1000V provides state-of-the-art load-balancing for tenant web servers. Figure 10 provides a conceptual view of use case 1.

Figure 10. Conceptual View of Cisco VSG and Citrix NetScaler 1000V Use Case 1



Cisco Nexus 1000V Infrastructure Prerequisites

Before installing Cisco vPath Service Chaining with Cisco VSG and Citrix NetScaler 1000V services on your network, you must install Cisco Nexus 1000V Software Release 4.2(1) SV2.2.1a in your environment and perform the basic configuration of the Cisco Nexus 1000V Switch:

- Install and configure the VSM
- Provide access to shared storage
- Create the necessary port profiles, including:
 - Uplink port profiles
 - Port profile with **capability-l3control**
 - Port profile with **capability-l3-vservice** attached to VMkernel
 - Virtual machine data port profiles
- Register the VSM with VMware vCenter
- Install two or more VEMs
- Add the VEMs to the VSM

This document does not discuss the details of Cisco Nexus 1000V installation and deployment. Please refer to the Cisco Nexus 1000V deployment and installation guides:

- http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html
- http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_sv2_2_1/install_upgrade/guide/b_Installation_and_Upgrade_Release_4_2_1SV2_2_1_series_release_chapter_010.html

Service Chaining Component Prerequisites

Cisco VSG and Citrix NetScaler 1000V must meet certain prerequisites.

Cisco VSG

Cisco VSG uses three network interfaces, in the following order:

1. Cisco VSG data interface (also called the service interface)
2. Cisco VSG management interface
3. Cisco VSG high-availability interface

Configure proxy Address Resolution Protocol (ARP) on the switch virtual interface (SVI) or upstream router for the Cisco VSG data interface:

- When encapsulated traffic that is destined for Cisco VSG is connected to a subnet other than the host service vmknic subnet, the VEM does not use the hypervisor host routing table. Instead, the vmknic initiates ARP for the remote Cisco VSG IP addresses. You must configure the upstream router to respond by using the proxy ARP feature.
- The VEM does not support a routing function, and it is assumed that the upstream switch or router is configured with proxy ARP.

Create additional VLANs for high availability on the VSM and allow the VLANs to forward on the system uplinks. Create these VLANs on the upstream switch. You can use the same VLAN for both the high-availability and data interfaces, or you can use different VLANs, depending on your network topology.

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

The Open Virtual Appliance (OVA) for the Cisco VSG installation is recommended, to simplify the installation process. Because Cisco Prime NSC is the centralized management center for Cisco VSG, it is located in your management VLAN. There are no specific network requirements for setting up Cisco Prime NSC.

Cisco NetScaler 1000V

Citrix NetScaler 1000V can be deployed in one-arm mode or two-arm mode. In this example, Citrix NetScaler 1000V is deployed in one-arm mode.

Citrix NetScaler 1000V uses two interfaces, in the following order:

1. Citrix NetScaler 1000V management interface (NetScaler IP [NSIP] addresses).
2. Citrix NetScaler 1000V service interface (used for virtual IP, subnet IP [SNIP], and Cisco vPath addresses).

Please refer to the Citrix NetScaler 1000V getting-started guide for more information about installation:

- http://www.cisco.com/en/US/products/ps13296/prod_installation_guides_list.html

Note: Citrix NetScaler 1000V can be deployed in one-arm mode with one virtual network interface card (vNIC) or in two-arm mode with two vNICs enabled on the virtual machine. These interfaces are separate from the management interface at which you configure NSIP.

The data (or service) interface on Citrix NetScaler 1000V can be an access port or a trunk port. A trunk port is required if you have multiple subnets for virtual IP, SNIP, and Cisco vPath interfaces, etc., and deploy in one-arm mode. In two-arm mode, a trunk port is required if you have multiple virtual IP and SNIP interfaces in multiple, different subnets.

The existing management VLAN in your setup can be used to manage Citrix NetScaler 1000V.

The OVA for the Citrix NetScaler 1000V installation is recommended, to simplify the installation process. You can access the embedded management GUI for Citrix NetScaler 1000V by accessing the NSIP (management IP) interface from the web browser.

Services Installation and Initial Setup

The server administrator must install Cisco Prime NSC, Cisco VSG, and Citrix NetScaler 1000V in the following order:

1. Install Cisco Prime NSC as a virtual appliance
2. Register Cisco Prime NSC with VMware vCenter
3. Install Cisco VSG as a virtual appliance
4. Install Citrix NetScaler 1000V as a virtual appliance
5. Register Cisco VSG with Cisco Prime NSC
6. Register the VSM with Cisco Prime NSC

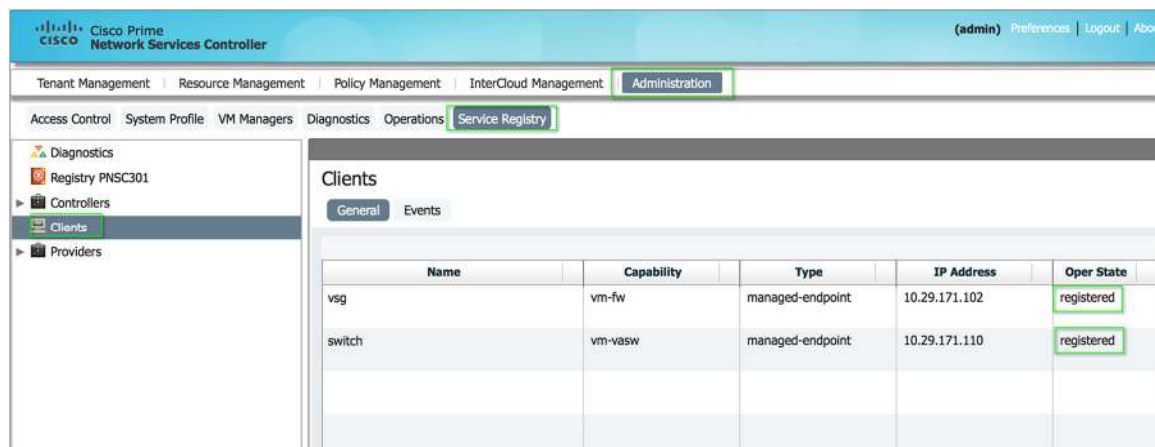
For more information about the initial deployment steps, please refer to the installation guides for Cisco VSG, Cisco Prime NSC, and Citrix NetScaler 1000V.

Verifying the Services Registered with Cisco Prime NSC

To verify that the Cisco VSG service is registered with Cisco Prime NSC, access the Cisco Prime NSC GUI using the Cisco Prime NSC management IP address in the web browser (Figure 11).

Verify clients (Cisco VSG and Cisco Nexus 1000V VSM) registered with Cisco Prime NSC in the service registry.

Figure 11. Cisco Prime NSC Services Registry



Name	Capability	Type	IP Address	Oper State
vsg	vm-fw	managed-endpoint	10.29.171.102	registered
switch	vm-vasw	managed-endpoint	10.29.171.110	registered

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

Configuring and Managing Settings for Security Devices and Profiles for Cisco VSG and Citrix NetScaler 1000V

For use case 1, you will configure the Cisco VSG security profile and enable the security firewall for virtual machines. You will also configure the Citrix NetScaler 1000V load-balancing profile and enable it for web server virtual machines.

Overview of Steps for the Security Administrator

In Cisco Prime NSC, the security administrator must perform the following steps:

1. Create a tenant: TenantABC.
2. Add zones for the tenant.
3. Assign Cisco VSG to a tenant. This example shows services enabled for a single tenant.
4. Define the security profile for the computing firewall.
5. Create a policy set and add rules in the policy.
6. Bind the policy set to the security profile.

After these steps are complete, the network administrator needs to bind the security profile to the port profiles.

Overview of Steps for the Network Administrator on Citrix NetScaler 1000V

On the VSM, the network administrator must perform the following steps to configure Citrix NetScaler 1000V as an SLB and to bind the security profile to the port profile:

1. Configure the SNIP and virtual IP addresses.
2. Configure the Cisco vPath parameter on Citrix NetScaler 1000V.
3. Define the server load-balancing properties, virtual server, and services on Citrix NetScaler 1000V.

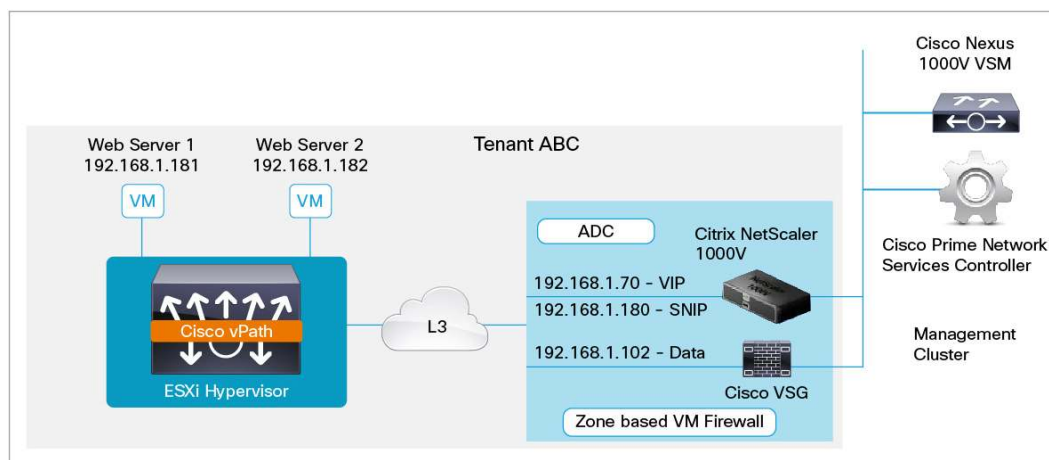
Overview of Steps for the Network Administrator to Use Cisco Nexus 1000V

1. Define the service nodes (Cisco VSG and Citrix NetScaler 1000V) on the Cisco Nexus 1000V.
2. Define Cisco vPath Services Chaining and add the service nodes you defined to the service chain.
3. Enable the service chain for each port profile.
4. Verify the status of the service chain and service nodes.
5. Verify the status of the virtual load-balancer server and services in Citrix NetScaler 1000V.
6. Verify that load balancing and security policies are applied to the flows.

Network Topology

Figure 12 presents a conceptual view of a typical network topology with all the necessary components in place for the Cisco vPath Service Chaining solution.

Figure 12. Tenant Network Topology View with Virtual Services



Step-by-Step Instructions

Follow the steps presented here to configure use case 1.

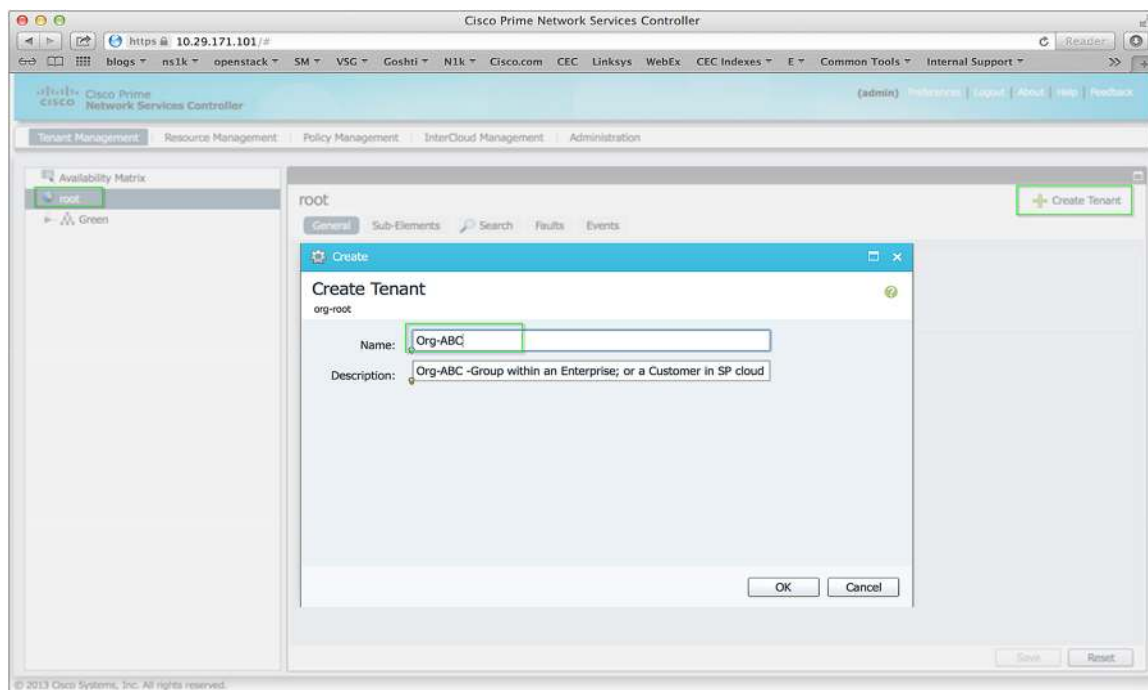
Security Administrator Step 1: Create a Tenant

Multitenancy is a core concept of cloud computing, and the tenant concept can be applied in many ways. Tenants can represent different companies sharing a public cloud service, or they can represent different departments or business groups in a private enterprise data center. A tenant is simply a logical container for virtual machines, networking, security services, etc.

Cisco Prime NSC and Cisco vPath is multitenant aware. Each tenant administrator has a view of his or her respective tenants in Cisco Prime NSC. Cisco VSG and ASA services are deployed per tenant. Cisco VSG provides the computing firewall for intertenant communication, or east-west communication, and Cisco ASA provides the tenant-edge firewall, or northbound access protection.

Log into the Cisco Prime NSC web interface using the management IP address and select the Tenant Management tab. Right-click the root and create a tenant (Figure 13).

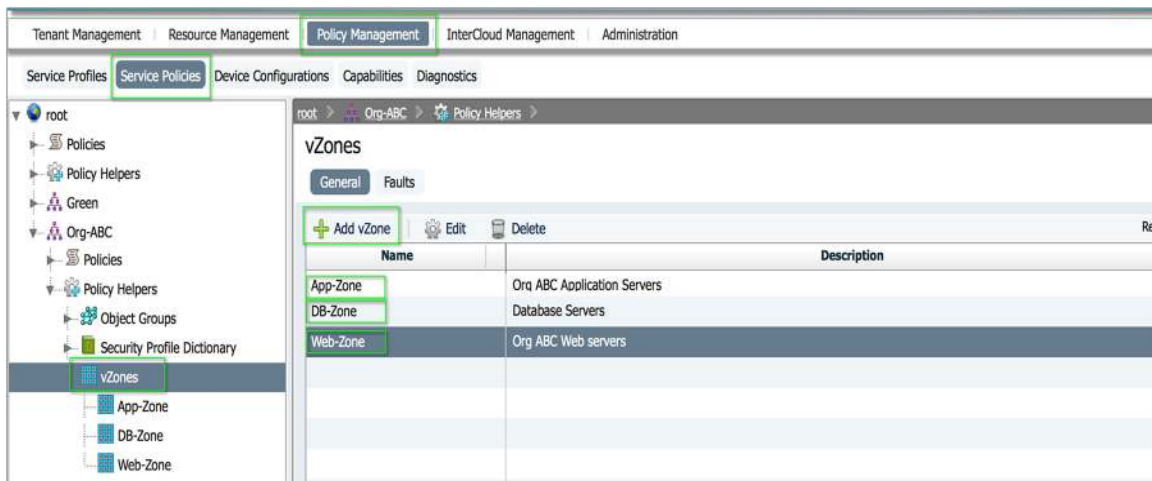
Figure 13. Create a Tenant



Security Administrator Step 2: Add Zones to a Tenant

Create logical zones using network or virtual machine attributes or a combination of both. Zones for policy rules can be defined using the virtual machine context or network context, and policies can be applied to virtual machine traffic based on logical user-defined zones (Figure 14).

Figure 14. Adding Zones for a Tenant



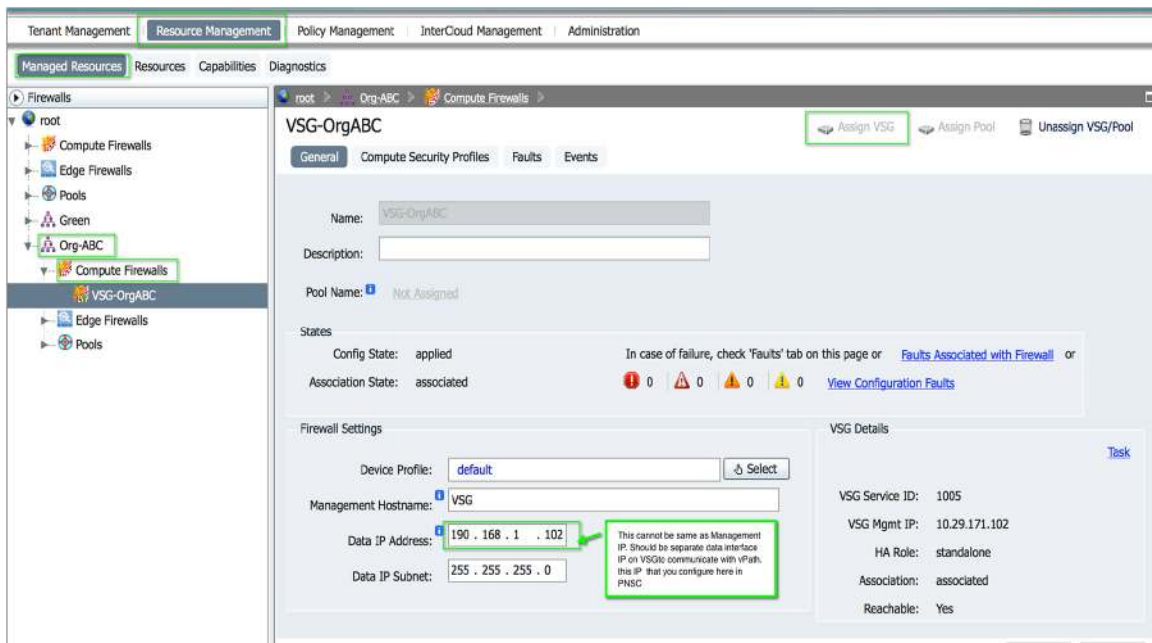
Security Administrator Step 3: Assign Cisco VSG Service to a Tenant

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

Create a computing firewall for TenantABC and associate it with the Cisco VSG instance that you have deployed.

In the example in Figure 15, Cisco VSG services are assigned to the tenant computing firewall.

Figure 15. Assigning Cisco VSG as a Tenant Computing Firewall



Security Administrator Step 4: Define the Firewall Security Profile and Policy Set

East-west virtual machine access policy rules are controlled by Cisco VSG, and northbound and southbound access rules are controlled by the Cisco ASA security service.

The security policy in Cisco Prime NSC uses network attributes, VMware virtual machine attributes, and virtual machine custom attributes (see the access control list [ACL] rule construct in Figure 16). You can define multiple policies for a tenant. All the policies are published to Cisco VSG through a security profile. These policies can be applied at any organizational level within a tenant. Policies can be assigned using virtual machine attributes, network attributes, or logical user-defined zones using these attributes.

Figure 16. ACL Rule Construct Options with Cisco VSG

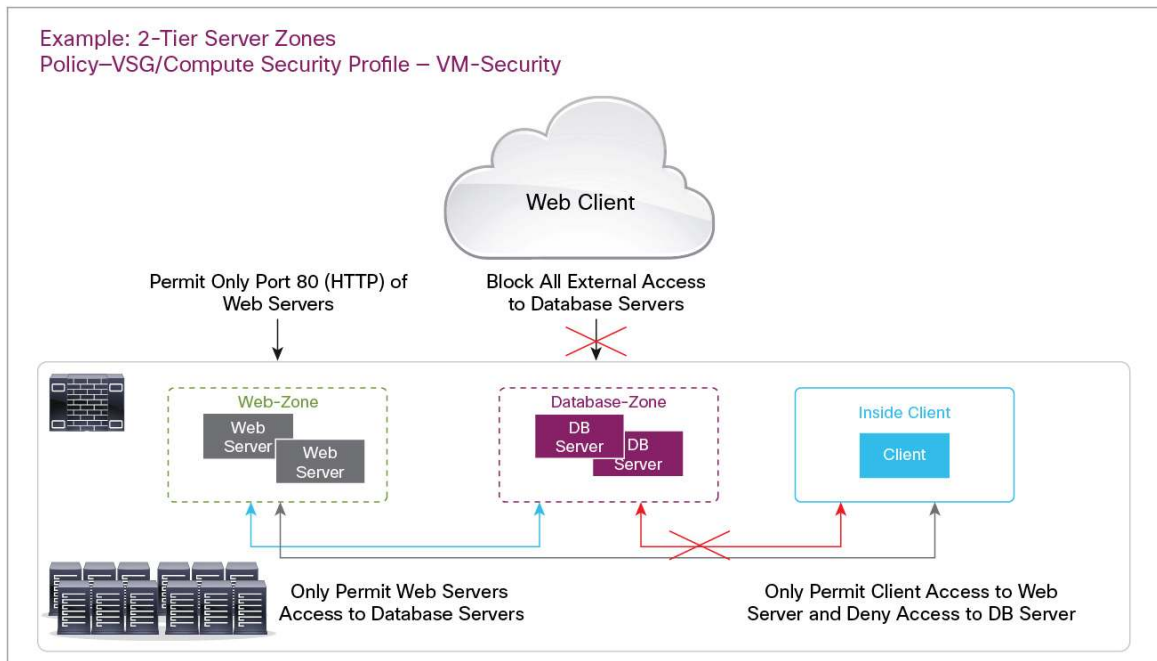
Attribute Type	VM Attributes	VM Attributes	Network Attributes
Network	Instance Name	Port Profile Name	IP Address
VM	Guest OS full name	Cluster Name	Network Port
vZone	Zone Name	Hypervisor Name	
User Defined	Parent App Name		

Operator	Action
eq	Not-in-range
neq	Prefix
gt	member
lt	Not-member
range	Contains

Security Administrator Step 5: Define the Security Profile and Policy Set for the Computing Firewall

Configure security profiles on the Cisco Prime NSC policy management interface. The predefined zones can be used to define the security policy for each tenant (Figure 17).

Figure 17. Example of Cisco VSG Security Policy Rules for Tenant A in a Two-Tier Server Zone



The following example of security policy rules for Tenant A is applied to use case 1:

- Permit only port 80 (HTTP) for virtual machines in the web zone
- Permit port 22 (Secure Shell [SSH]) for virtual machines that belong to the database zone
- Allow communication only between web servers and database servers
- Allow communication only between clients and web servers
- At the end of a security profile, an explicit deny rule is applied by default

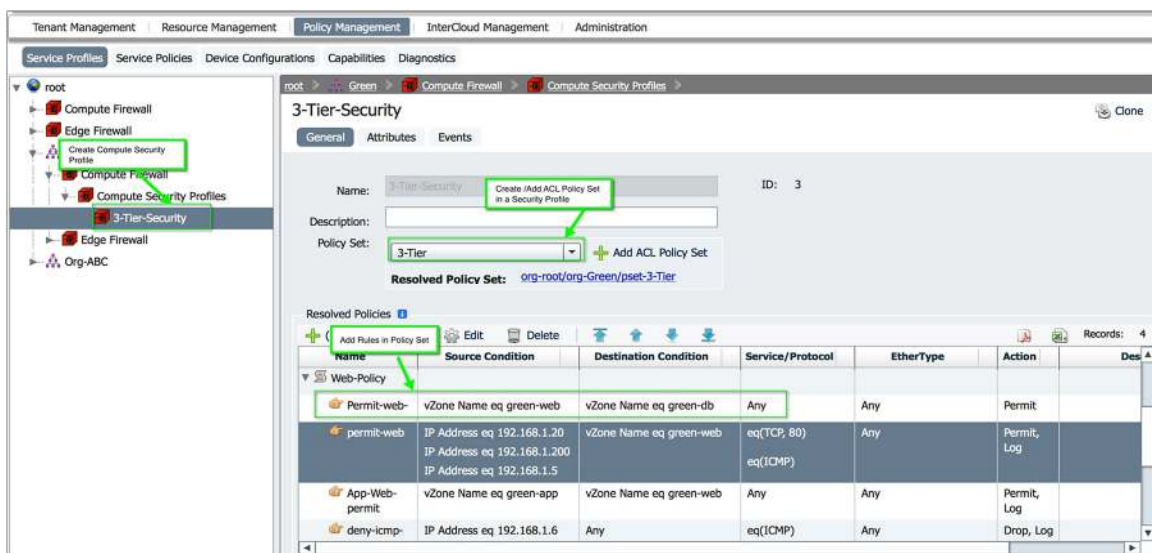
Security Administrator Step 6: Attach the Policy Set to the Security Profile for the Computing Firewall

Policy sets are attached to security profiles. When you enable virtual machine policies, security profiles are used to attach security policies to the virtual machines.

Select the computing firewall and create a new security profile for Tenant A: for example, VM-Security.

Within the security profile, create a policy set (for the policies shown in Figure 18 in this example) and create rules for the policy set.

Figure 18. Defining the Policy Example for Step 5 and 6



Network Administrator Step 7: Configure SNIP and Virtual IP Addresses on Citrix NetScaler 1000V

To configure Citrix NetScaler 1000V as a virtual load balancer with Cisco vPath, you need to specify the following settings at the Citrix NetScaler 1000V web Interface:

- Cisco vPath parameter
- Virtual load-balancing server and services

To specify these details, after the Citrix NetScaler 1000V virtual machine is instantiated and the management IP address is configured, open Microsoft Internet Explorer on your client PC and enter the NSIP address (Citrix NetScaler 1000V management interface IP address). Log in with the default user name **nsroot** and the default password **nsroot** (Figure 19).

Figure 19. Citrix NetScaler 1000V Web Login

Welcome! Skip

Before you can use your appliance, it must be assigned a NetScaler IP address, which is the management IP address. Also assign a subnet IP address to which your servers can connect, and allocate or upload your licenses.

System

NetScaler IP Address* 10 . 29 . 171 . 115

Netmask* 255 . 255 . 255 . 0

Hostname ns1000v

DNS (IP Address) +

Time Zone* Coordinated Universal Time

☐ Change Administrator Password

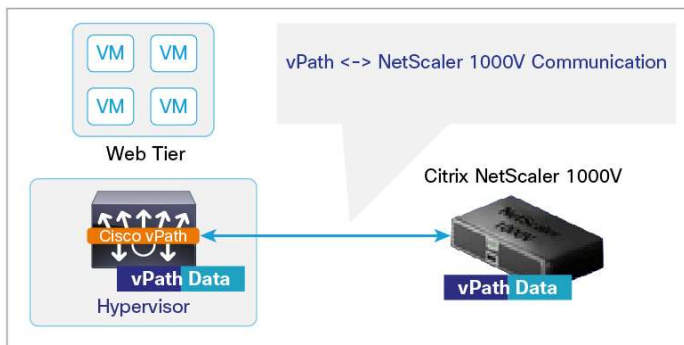
[Continue](#)

The Welcome screen appears. Fill in the subnet IP address (the SNIP address), which will be used to connect to the resource servers; the hostname; and the DNS server address (optional). Select the correct time zone and optionally change the administrator password. Click Continue.

Choose Configuration > System > Network and configure the SNIP and virtual IP IP addresses.

The SNIP address on Citrix NetScaler 1000V is used for back-end service monitoring, keepalive, and Cisco vPath communications. You can use an existing SNIP address to transport traffic between Cisco vPath (server virtual machine) and Citrix NetScaler 1000V (Figure 20), or you can choose a dedicated SNIP address.

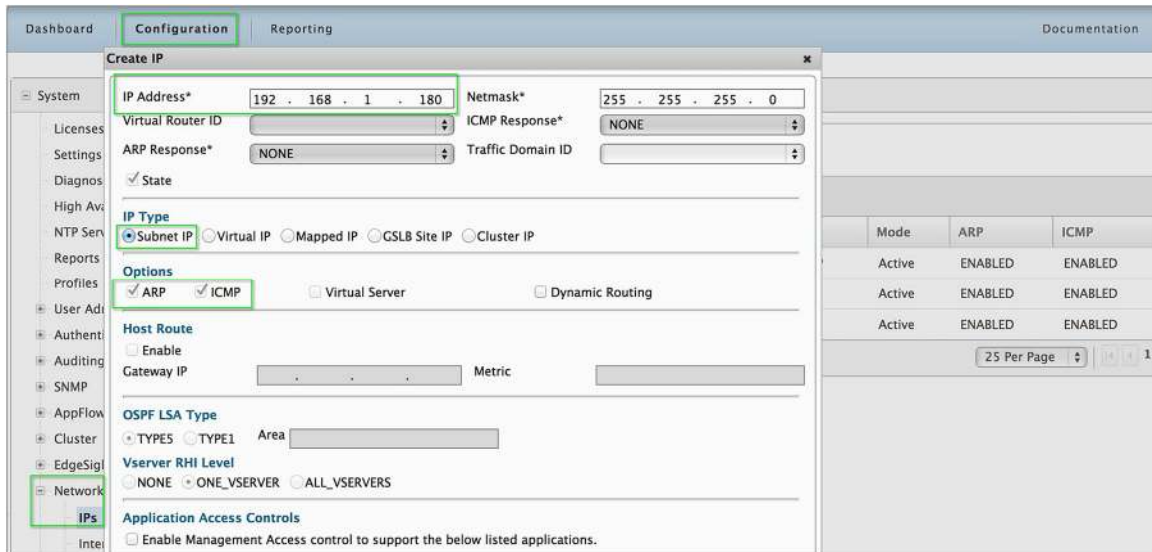
Figure 20. Communication Between Citrix NetScaler 1000V and Cisco vPath



The virtual IP address is used for load balancing the virtual server IP address, and it needs to be configured on the Load Balancing screen shown in subsequent steps.

Add the SNIP and virtual IP addresses by selecting the IP type for each (Figure 21).

Figure 21. Configuring SNIP and Virtual IP Addresses on Citrix NetScaler 1000V



After this step, you should have a minimum of three IP addresses configured on Citrix NetScaler 1000V (Figure 22):

- Citrix NetScaler IP address
- Subnet IP address
- Virtual IP address

Figure 22. Configured IP Address Types

Type
Netscaler IP
Subnet IP
Virtual IP

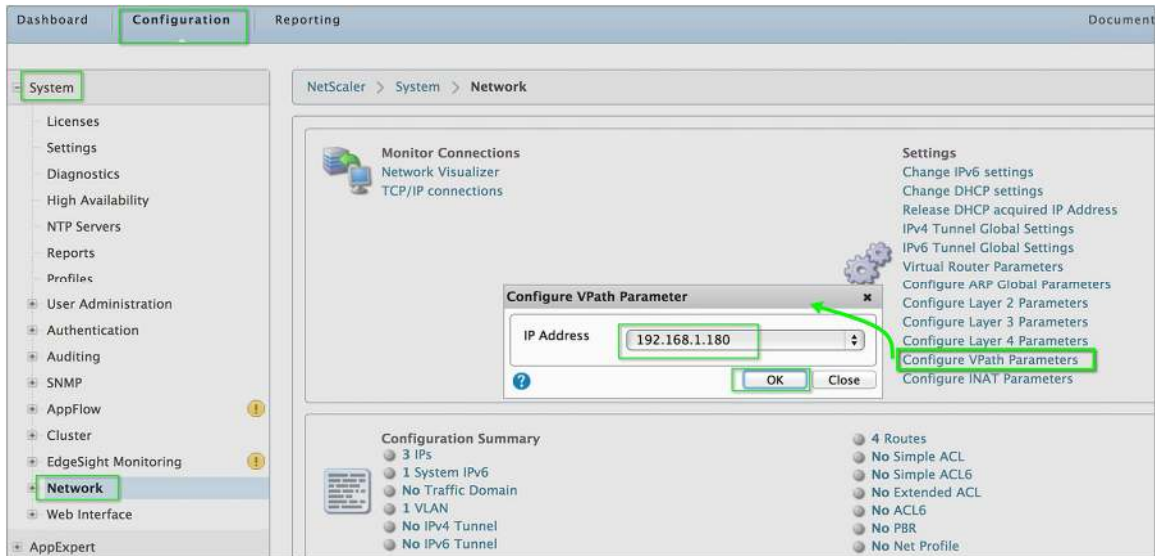
Network Administrator Step 8: Define the Cisco vPath Source Parameter on Citrix NetScaler 1000V

All the data to and from Citrix NetScaler 1000V to the back-end service virtual machine is Cisco vPath encapsulated.

To configure the Cisco vPath parameter (source IP address) in Citrix NetScaler 1000V, choose Configuration > Network > Settings > Configure vPath Parameters.

Note that Cisco vPath is enabled by default; you just need to tell Citrix NetScaler 1000V which interface and IP address to use for Cisco vPath communication (Figure 23).

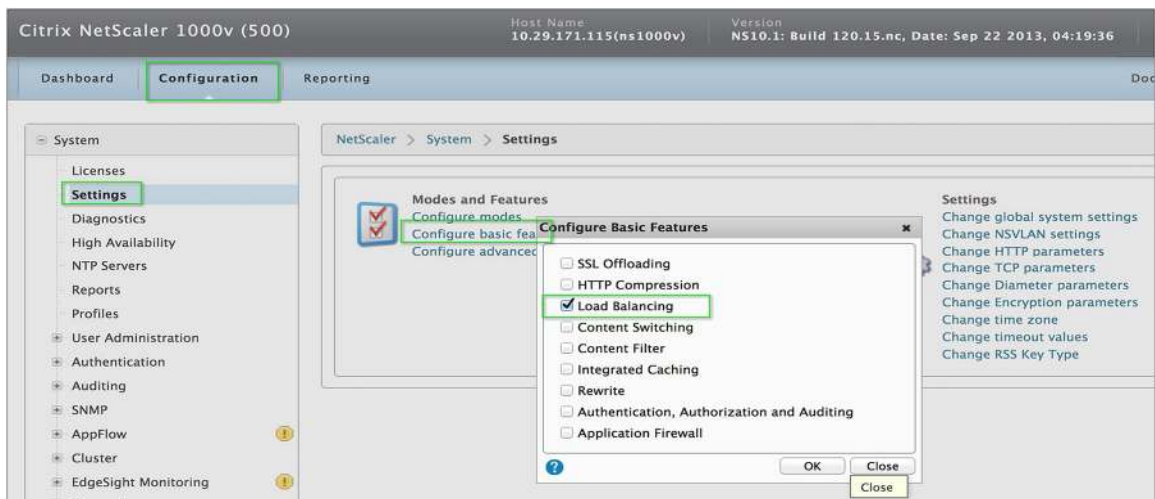
Figure 23. Configuring Cisco vPath IP on Citrix NetScaler 1000V



Network Administrator Step 9: Define the SLB Properties, Virtual Server, and Services on Citrix NetScaler 1000V

To verify that load balancing is enabled, choose Configuration > Settings > Configure Basic Features and select Load Balancing (Figure 24).

Figure 24. Enabling Load Balancing



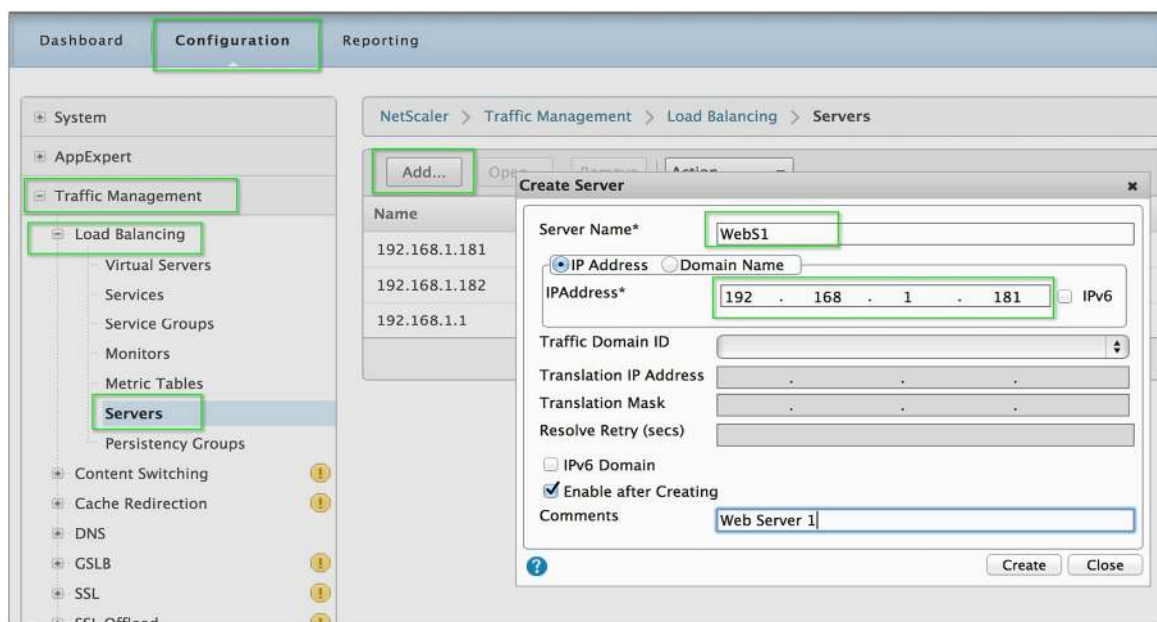
In the Load Balancing section in the navigation pane, specify, in this order:

- Servers
- Services
- Virtual server

To perform all load-balancing configuration, choose Configuration > Traffic Management > Load Balancing.

Select Servers and set up two servers. Click the Add option to add a server with a name for the web server and IP 192.168.1.181; then click Create. Similarly add a second server, using its own IP address (Figure 25).

Figure 25. Adding a Web Server for Load Balancing

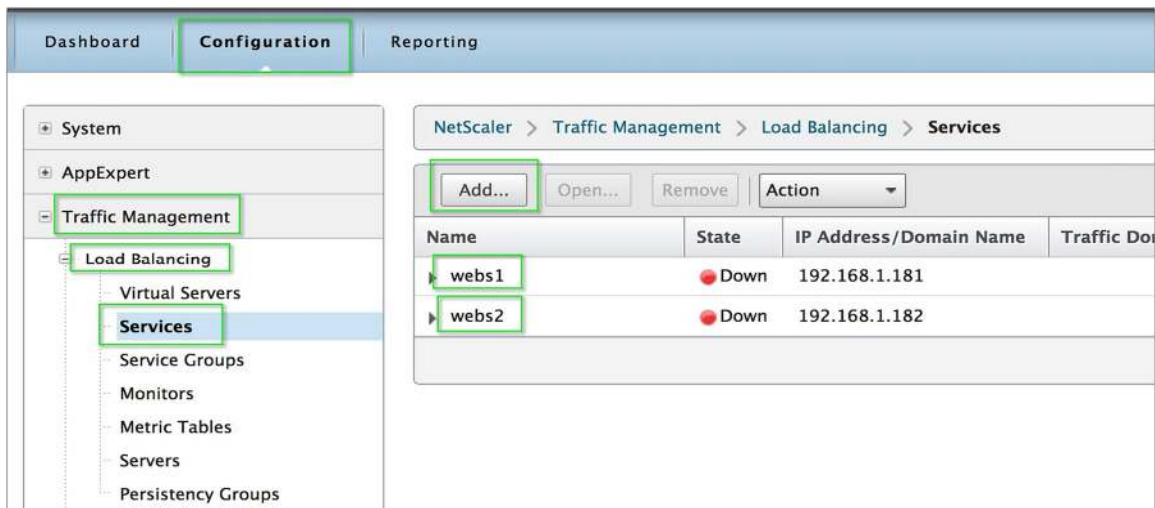


After the servers are set up, add them as a service. Select the Services tab and click Add to add a service.

Configure the name as **webs1** and select Web Server 1, which you just added. Change the protocol to HTTP and use port 80; then click Create. Repeat the same steps for Web Server 2 (Figure 26).

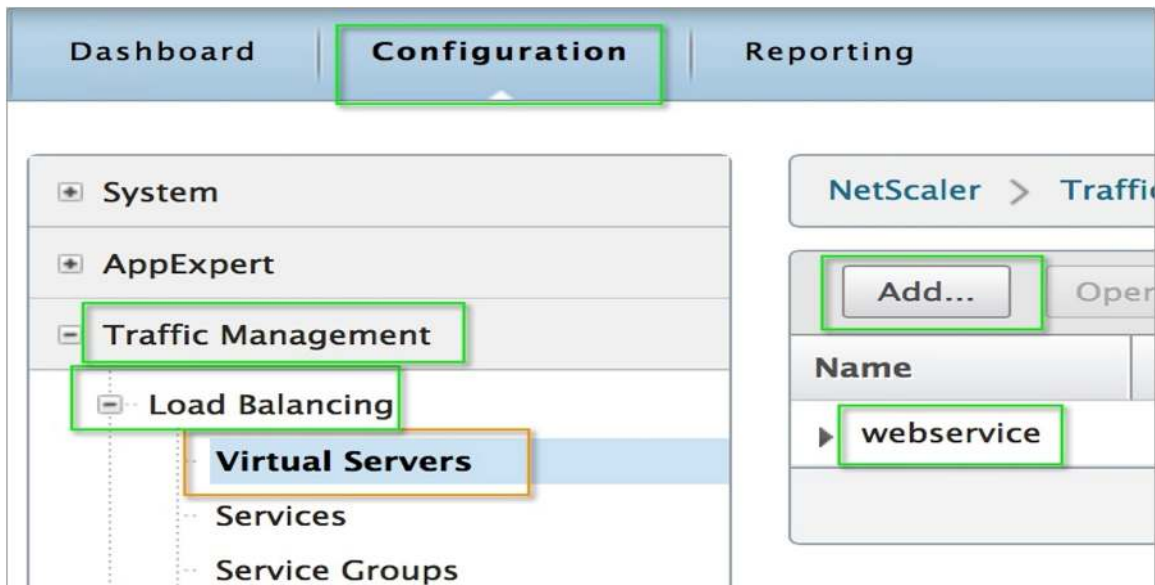
Note: The service state will be listed as Down. This status appears because you have not yet assigned the Citrix NetScaler 1000V ADC as a service on the Cisco Nexus 1000V with Cisco vPath in the port profile for Web Servers 1 and 2. You will complete this task in the next steps. Citrix NetScaler 1000V is tightly integrated with the Cisco Nexus 1000V and Cisco vPath architecture and does not work without a Cisco vPath port profile attached to back-end servers.

Figure 26. Configuring the Load-Balancing Service



Now create the load-balancing virtual server. Click Add and configure the name and virtual IP address along with the protocol, services, and load-balancing method (for example, round-robin) using the options available (Figure 27).

Figure 27. Binding the Service to the Virtual Server Virtual IP Address



After all set up is complete, save the running configuration by clicking Save in the upper-right corner of the Citrix NetScaler GUI.

Network Administrator Steps 10 to 14

10. Define Cisco vPath Services Chaining and add the service nodes you have defined to the service chain.
11. Enable the service chain for each port profile.
12. Verify the status of the service chain and service nodes.
13. Verify the status of the virtual load-balancing server and services on Citrix NetScaler 1000V.
14. Verify that the load-balancing and security policies are applied to the flows.

Enabling Cisco vPath Service Chaining on the Cisco Nexus 1000V

You perform all the steps in this section on the Cisco Nexus 1000V VSM console.

To enable the virtual machine firewall and load-balancing service policies for the virtual machine workload on the network, attach these services to the port profile on the Cisco Nexus 1000V. For Cisco VSG, also bind the tenant computing security profile defined in Cisco Prime NSC to the port profile. All the traffic traversing the virtual ports associated with that port profile is subject to policy evaluation.

Defining Service Nodes

Next define the service nodes for the Cisco VSG and Citrix NetScaler 1000V service instances on the Cisco Nexus 1000V.

Communication Between Virtual Service Nodes and the VEM (Cisco vPath)

A VSN (Cisco VSG, Citrix NetScaler 1000V, Cisco vWAAS, etc.) receives traffic from the VEM when service is enabled on a port profile. The redirection of the traffic is performed using Cisco vPath. Cisco vPath encapsulates the original packet and sends it to the VSN. The VSN has a service or data interface (for example, Data0 in Cisco VSG, or SNIP in Citrix NetScaler 1000V) with an IP address for Cisco vPath communication.

All service nodes in the Cisco vPath 2.5 ecosystem should be Layer 3 adjacent to Cisco vPath. A service node can be deployed in same Layer 2 domain, but the configuration in Cisco vPath needs to be Layer 3 adjacent with the service interface IP configuration instead of the VLAN.

In this configuration, Layer 3 communication is through the VSN's data or service interface and a VMkernel interface on each VEM. Each VEM hosting a virtual machine with Cisco vPath services active needs VMkernel to communicate with the service node's data interface. The VMkernel interface can be the same one used for VSM and VEM (Layer 3 control) communication. The VEM needs IP address reachability only to the tenant-specific Cisco VSG or Citrix NetScaler 1000V in this scenario, to redirect traffic from Cisco vPath to the service node for policy evaluation and enforcement.

The VSM configuration example that follows shows how Cisco VSG and Citrix NetScaler 1000V Layer 3 adjacency is configured on the VSM.

For Layer 3 adjacency, a new port profile is defined on the VSM with **capability I3-vservice**, and this port profile needs to be associated with a VMkernel interface on each VEM.

An alternative approach is to use the same VMkernel interface on a protected host that is used for VSM and VEM control traffic for communication between Cisco VSG and the VEM. You implement this approach by adding **capability I3-vservice** to the same port profile as the one used for VSM and VEM (Layer 3 control) communication.

In this case, all your data traffic will flow through this interface along with VMware ESXi management and Cisco Nexus 1000V control traffic.

Use the following configuration example for guidance:

```
port-profile type vethernet nlkv-l3
  capability l3control
  capability l3-vservice
  vmware port-group
  switchport mode access
  switchport access vlan 171
  no shutdown
  system vlan 171
  state enabled
```

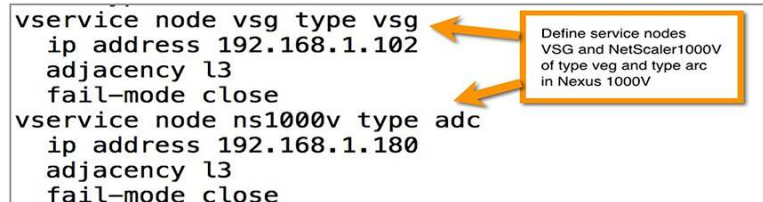
Network Administrator Step 10: Define Service Nodes for Cisco VSG and Citrix NetScaler 1000V

To define the Cisco VSG service node, use the Cisco VSG data interface IP address. Cisco VSG can be Layer 2 or Layer 3 adjacent to the Cisco Nexus 1000V (Cisco vPath), regardless of the VSM-to-VEM adjacency mode.

To define the Citrix NetScaler 1000V service node, use the Cisco vPath interface IP address for Citrix NetScaler (as configured earlier in step 8). The following code example shows the configuration of two nodes of type **vsg** and type **adc**:

Define Cisco VSG and Citrix NetScaler 1000V service nodes of type **veg** and type **arc** in Cisco Nexus 1000V

```
vservice node vsg type vsg
  ip address 192.168.1.102
  adjacency l3
  fail-mode close
vservice node ns1000v type adc
  ip address 192.168.1.180
  adjacency l3
  fail-mode close
```

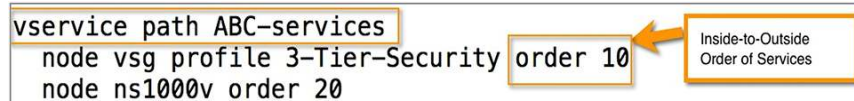


Define service nodes
VSG and NetScaler1000V
of type veg and type arc
in Nexus 1000V

Network Administrator Step 11: Chaining Cisco VSG and ASA Services in the Service Path

Use the service path to define service chaining with multiple service nodes in a specific order. Apply the order for service-node chaining inside to outside for traffic from the server to the client. Also apply the security profiles created for Cisco VSG (**3-Tier-Security** in this example) and the ADC or load-balancing policy for Citrix NetScaler 1000V to the service path (service chain) as follows:

```
vservice path ABC-services
  node vsg profile 3-Tier-Security order 10
  node ns1000v order 20
```



Inside-to-Outside
Order of Services

Network Administrator Step 12: Enable Service Chain per Port Profile

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

In the following example code snippet, the **service-ABC** port profile is attached to the ABC tenant web server and will be used to enable zone-based firewall (Cisco VSG) and load-balancing policy:

```
switch# show run port-profile service-ABC

!Command: show running-config port-profile service-ABC
!Time: Fri Nov 8 14:57:30 2013

*version 4.2(1)SV2(2.1a)
port-profile type vethernet service-ABC
  vmware port-group
  switchport mode access
  switchport access vlan 270
  no shutdown
  state enabled
```

```
switch# show port-profile usage name service-ABC

port-profile service-ABC
Vethernet4
Vethernet10
Vethernet11

switch# show int virtual
```

Port	Adapter	Owner
Veth1	vmk1	VMware VMkernel
Veth4	Net Adapter 1	web1-green
Veth6	vmk2	VMware VMkernel
Veth7	Net Adapter 1	NS1000V
Veth9	Net Adapter 2	NS1000V
Veth11	Net Adapter 1	web2-green
Veth13	Net Adapter 1	App-server2

Identify port profiles to enable load-balancer and firewall security. In the following example, the workload uses the port profile **service-ABC** to enable the service chain. Along with the **vservice path** command, you need to define **Tenant Org** for this port profile. This tenant is the same one for which the Cisco VSG services are assigned and security profiles are created in Cisco Prime NSC.

```
switch# show run port-profile service-ABC

!Command: show running-config port-profile service-ABC
!Time: Thu Nov 7 20:23:19 2013

version 4.2(1)SV2(2.1a)
port-profile type vethernet service-ABC
  vmware port-group
  switchport mode access
  switchport access vlan 270
  org root/Org-ABC
  vservice path ABC-services
  no shutdown
  state enabled
```

Enable Service Chain per Port Profile

Network Administrator Step 13: Verify the Cisco vPath, Node, and Profile Configurations and Service Node Status

Use the commands **show vservice brief** and **show vservice detail** to verify that the service node is alive and that the service chain is attached to the desired virtual machines:

```
switch# show vservice brief
-----
                        License Information
-----
Type      In-Use-Lic-Count  UnLicensed-Mod
vsg              2
asa              0
-----

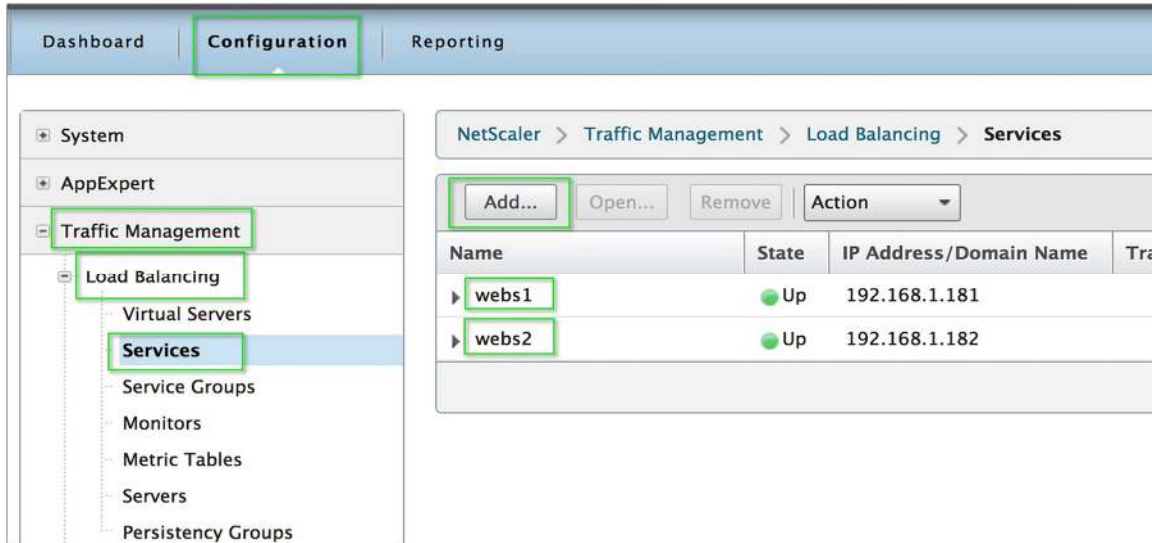
                        Node Information
-----
ID  Name      Type  IP-Address  Mode  State  Module
1  ns1000v    adc   192.168.1.180  l3    Alive  3,
2  vsg        vsg   192.168.1.102  v-270 Alive  3,
-----

                        Path Information
-----
Name:ABC-services      NumOfSvc:2  Mod:3,
Node                   Order      Profile
vsg                    10        3-Tier-Security
ns1000v                20        --
-----

                        Port Information
-----
PortProfile:service-ABC
vsg:1000/green
Path:ABC-services
Node
vsg(192.168.1.102)
ns1000v(192.168.1.180)
Veth Mod VM-Name
4 3 web1-green
11 3 web2-green
Profile(Id)
3-Tier-Security(3)
--
vNIC IP-Address
1 192.168.1.181
1 192.168.1.182
switch#
```


Using the Citrix NetScaler 1000V GUI, verify that the status is now Up for the load-balancing virtual server and services (Figure 28).

Figure 28. Verifying that the Load-Balancing Service State Is Up in the Citrix NetScaler 1000V GUI



Network Administrator Step 14: Verify Service Chain Insertion

The final step is to verify that the services are inserted in the traffic flow. To do this, access the web server at port 80 by viewing the virtual IP address in the client browser.

View the statistics and live connections on the VSM or on the Cisco VSG and Citrix NetScaler 1000V monitoring console to get information about the number of packet flows, flow policy hits and misses, and actions implemented for the flow. Enter the following commands on the Cisco Nexus 1000V to obtain statistics and connection details:

Show vservice statistics

Show vservice connection

```
switch# show vserv connection
Actions(Act):
d - drop
p - permit
r - redirect
n - not processed
Flags:
A - seen ack for syn/fin from src
E - tcp conn established (SasA done)
F - seen fin from src
R - seen rst from src
S - seen syn from src
T - tcp conn torn down (FafA done)
s - reset
t - passthrough
e - error
upper case - offloaded
a - seen ack for syn/fin from dst
f - seen fin from dst
r - seen rst from dst
s - seen syn from dst
x - IP-fragment connection

#Port-Profile:service-ABC
#Module 3
Proto SrcIP[:Port]      SAct DstIP[:Port]      DAct  Flags  Bytes
icmp 192.168.1.180      Pp    192.168.1.181      Pp      648
icmp 192.168.1.180      Pp    192.168.1.182      Pp      546
tcp 192.168.1.6:49196   Pp    192.168.1.182:80   Pp  f    11649
tcp 192.168.1.6:49197   Pp    192.168.1.182:80   Pp  E     8606

switch#
```


You have now successfully load balanced your web servers while enabling virtual machine security. You can test your configuration by opening a browser and going to <http://192.168.1.70> (the virtual IP address you created). Every time you refresh the screen, you should see a different webpage.

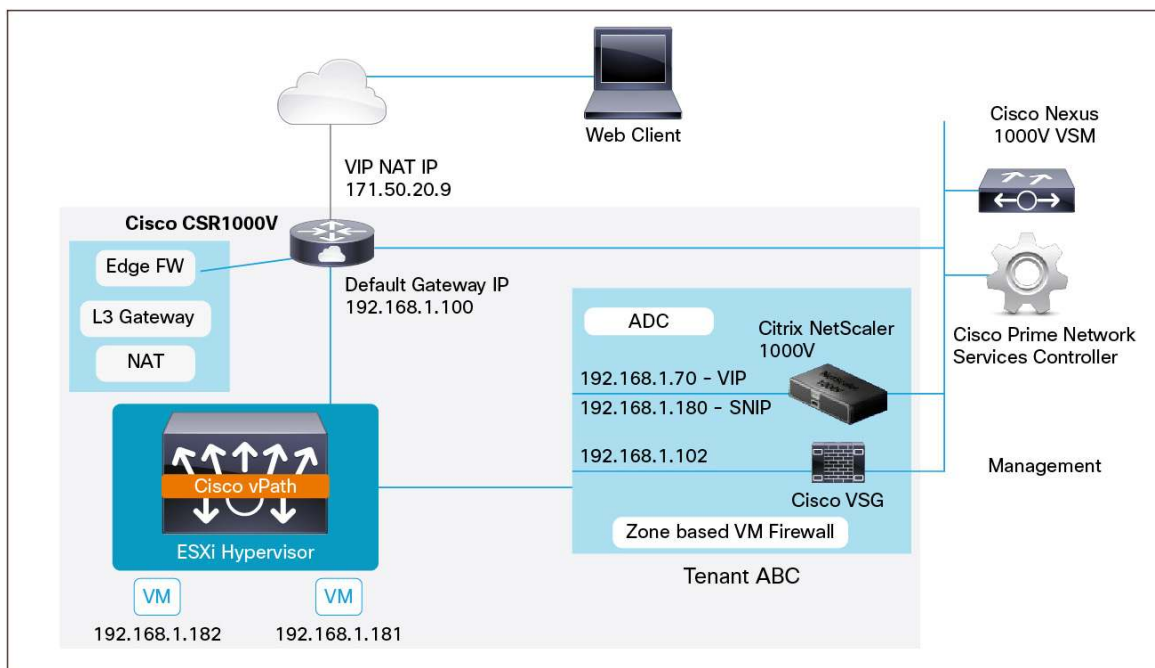
Cisco vPath 2.5 Ecosystem Use Case 2: Extending the Service Chain to Include Additional Services Using Cisco CSR 1000V

The Cisco CSR 1000V is a single-tenant router in a virtual form factor that delivers comprehensive WAN gateway functions to multitenant provider-hosted clouds. Using familiar, industry-leading Cisco IOS® Software networking capabilities, the Cisco CSR 1000V enables enterprises to transparently extend their WANs to external provider-hosted clouds, and it enables cloud providers to offer enterprise-class networking services to their tenants.

The service chain configured in use case 1 can be extended to include a Layer 3 edge gateway and firewall using the Cisco CSR 1000V. Note that the Cisco CSR 1000V is a standalone service node and is not enabled through Cisco vPath. It is deployed inline for northbound traffic.

Figure 29. Tenant Network Topology with Cisco VSG, Citrix NetScaler 1000V, and Cisco CSR 1000V

The topology example in Figure 29 shows a tenant edge firewall, edge Layer 3 gateway, and NAT configured on the Cisco CSR 1000V. NAT is configured for the Citrix NetScaler 1000V virtual IP address, at which Internet clients can access web servers using the public IP address of the virtual IP interface. The Cisco CSR 1000V virtual appliance can be deployed on the Cisco Nexus 1000V VEM or on a native hypervisor switch.



Extending the Service Chain to Include Additional Services, Cisco CSR 1000V, and Cisco vWAAS

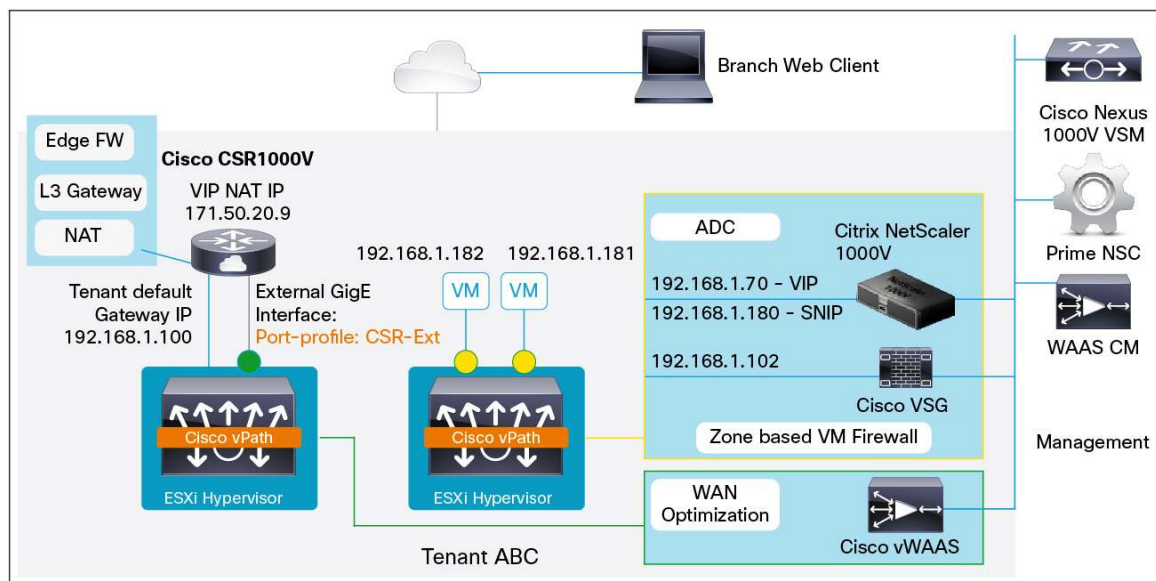
Cisco vWAAS is the only WAN optimization and application acceleration solution that is deployed in an application-specific, virtualization-aware, and on-demand manner. Using policy-based configuration on the Cisco Nexus 1000V Switch, Cisco vWAAS is associated with application server virtual machines as they are instantiated or moved. This approach helps enable cloud providers to offer rapid delivery of WAN optimization services with little network configuration or disruption in cloud-based environments.

Cisco vWAAS is designed for both enterprises and service providers that plan to offer private and virtual private cloud-based application delivery services over the WAN to their internal or external customers. Cisco vWAAS can be deployed in the physical data center and in private clouds and in virtual private clouds offered by service providers.

Cisco vWAAS is the first virtual service active for packets destined for the server virtual machine from the web client. Cisco vWAAS is enabled with Cisco vPath on the Cisco CSR 1000V external or outbound interface that connects your cloud to the external network. The Cisco CSR 1000V needs to be deployed behind the Cisco Nexus 1000V VEM so you can enable Cisco vWAAS as a service with Cisco vPath on the Cisco CSR interface.

In the topology in Figure 30, Cisco vPath service is active in two places: the Cisco vWAAS service on the Cisco CSR 1000V virtual machine port, and the Cisco VSG and Citrix NetScaler 1000V service chain on an application server virtual machine port.

Figure 30. Tenant Network Topology with Cisco VSG, Citrix NetScaler 1000V, Cisco CSR 1000V, and Cisco vWAAS



Sample configurations for enabling these services (Cisco vWAAS, Cisco VSG, and Citrix NetScaler 1000V) on the Cisco Nexus 1000V VSM are shown here:

```
switch# show run port-p CSR-Ext

!Command: show running-config port-profile CSR-Ext
!Time: Fri Nov  8 17:21:05 2013

version 4.2(1)SV2(2.1a)
port-profile type vethernet CSR-Ext
  vmware port-group
  switchport mode access
  switchport access vlan 2001
  vservice node vWAAS
  no shutdown
  state enabled

switch# show run port-p CSR-Int

!Command: show running-config port-profile CSR-Int
!Time: Fri Nov  8 17:21:07 2013

version 4.2(1)SV2(2.1a)
port-profile type vethernet CSR-Int
  vmware port-group
  switchport mode access
  switchport trunk allowed vlan 270
  switchport access vlan 270
  no shutdown
  state enabled
```

```
vservice path ABC-services
  node vsg profile 3-Tier-Security order 10
  node ns1000v order 20
```

Inside-to-Outside
Order of Services

```
switch# show run port-profile service-ABC

!Command: show running-config port-profile service-ABC
!Time: Fri Nov  8 17:18:17 2013

version 4.2(1)SV2(2.1a)
port-profile type vethernet service-ABC
  vmware port-group
  switchport mode access
  switchport access vlan 270
  org root/Green
  vservice path ABC-services
  no shutdown
  state enabled
```

Conclusion

Network intelligence for virtual services such as that provided by Cisco vPath is critical for:

- Topology-agnostic service insertion
- Nondisruptive operation
- Simplified deployment
- Optimized performance
- Dynamic scalability
- Separation of duties

Cisco vPath for the Cisco Nexus 1000V provides an innovative architecture for transparent deployment of Cisco and third-party virtual 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, Cisco vPath Service Chaining provides a single control point for multiple network services, making network services deployment simpler, faster, and less error prone.

For More Information

Citrix NetScaler 1000V Getting started guide:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/solutions/citrix-ns/10_1/citrix_gsg.pdf.

Cisco vPath 2.5 ecosystem reference portal:

http://www.cisco.com/cisco/web/docs/solutions/n1kv/vpath-ecosys/2_5/index.html.

Cisco Nexus 1000V deployment guide:

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html.

Cisco Prime Network Services Controller getting started guide:

http://www.cisco.com/en/US/docs/net_mgmt/virtual_network_mgmt_center/3.0/quick-start-guide/b_30_Quick_Start_Guide.pdf.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)