

Enable Cisco Virtual Security Gateway Service on a Virtual Extensible LAN Network in VMware vCloud Director



What You Will Learn

Many organizations are building or considering public and private clouds to support multitenant environments. The tenants in this environment need segmentation at the network level, but traditional network segmentation mechanisms such as IEEE 802.1Q VLAN tagging may not be sufficient for large-scale cloud deployments because the number of LAN segments is limited to 4096. Virtual Extensible LAN (VXLAN) defines a 24-bit LAN segment identifier to provide segmentation at cloud scale. The Cisco Nexus® 1000V Switch can be configured to use VXLAN to provide segmentation in a VMware vCloud Director environment. In addition, the Cisco Nexus 1000V with Cisco® Virtual Services Data Path (vPath) makes it possible to configure network services for an organization network that is backed by a VXLAN pool in VMware vCloud Director. Cisco Virtual Security Gateway (VSG) is a virtual firewall for Cisco Nexus 1000V Series Switches that delivers security and compliance for virtual computing environments. In a VMware vCloud Director environment, Cisco VSG can be inserted to provide tenant-level security when the organization network is backed by a VXLAN pool provided by a Cisco Nexus 1000V Switch. This document will show the reader how to enable the Cisco VSG service for all virtual applications (vApps) on an organization network created in VMware vCloud Director using a VXLAN-backed pool.

Note: This document does not discuss the details or best practices for deploying the Cisco 1000V Series Switches. For more information, see the links in the “For More Information” section of this document.

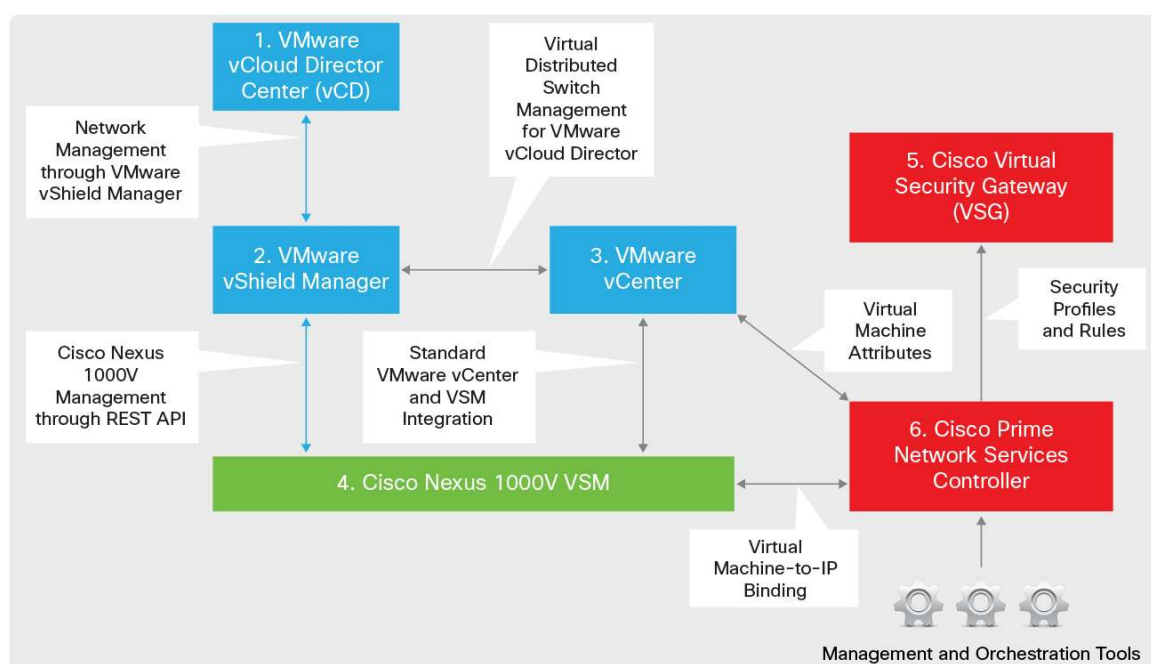
Intended Audience

This document is intended for security architects, network architects, network engineers, virtualization administrators, and server administrators interested in understanding and deploying Cisco VSG in an environment using Cisco Nexus 1000V Series VXLAN technology with VMware vCloud Director.

Solution Architecture

Figure 1 shows the solution architecture for deploying Cisco VSG with Cisco Nexus 1000V with VMware vCloud Director to support VXLAN.

Figure 1. Solution Architecture



The main components of the solution are:

- VMware vCloud Director and VMware vShield Manager communication: VMware vCloud Director provides network services to the cloud through VMware vShield Manager. VMware vShield Manager interacts with the Cisco Nexus 1000V Virtual Supervisor Module (VSM) to make the Cisco Nexus 1000V available to VMware vCloud Director to build any type of network when you are building a tenant cloud. Each VMware vCloud Director cell requires access to a VMware vShield Manager host, which provides network services to the cloud. You must have a unique instance of VMware vShield Manager for each VMware vCenter server you add to VMware vCloud Director.
- Cisco Nexus 1000V and VMware vShield Manager communication: VMware vCloud Director interacts with the Cisco Nexus 1000V using VMware vShield Manager. The VSM implements a representational state transfer (REST) API that allows the user to create all types of networks supported by VMware vCloud Director. This API allows the user to design and implement networks in VMware vCloud Director that then are created on the Cisco Nexus 1000V Switch.

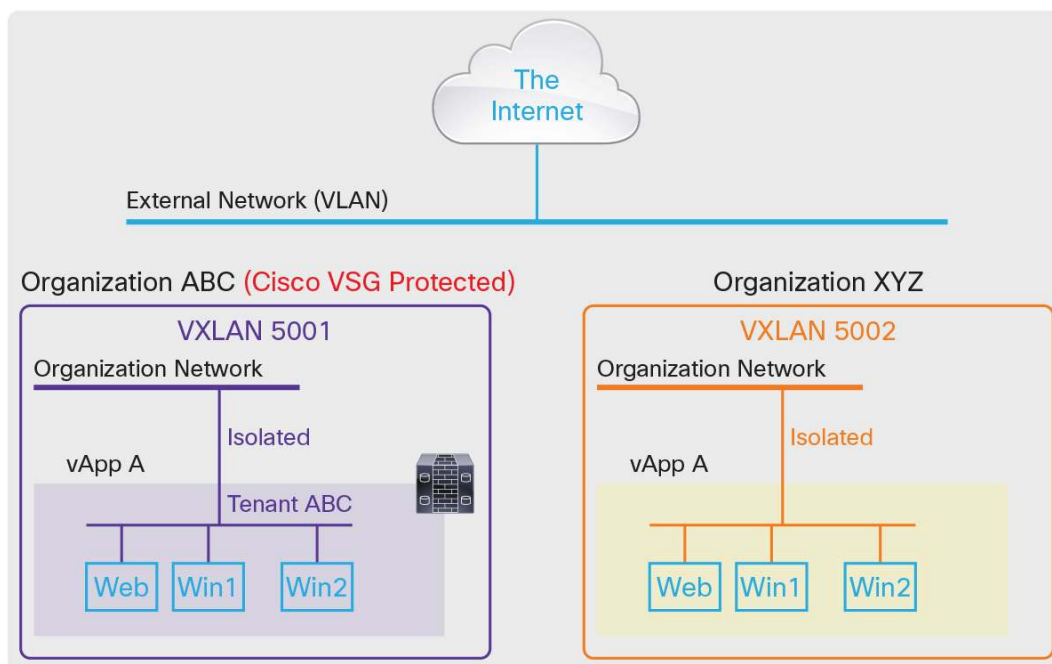
VMware vShield Manager needs the following information to manage the VSM:

- VSM connectivity details
- Number of multicast addresses available for the VMware vCloud Director
- Number of VXLANs that can be consumed by VMware vCloud Director
- VMware vShield Manager and vCenter communication: This communication occurs when an organization requires a routed network. VMware vShield Manager instantiates a VMware vShield edge appliance dynamically to provide Network Address Translation (NAT) and IP gateway service for the organization network.
- VMware vCenter and Cisco Nexus 1000V VSM communication: VMware vCenter provides centralized control and visibility to VMware vSphere virtual infrastructure. The Cisco Nexus 1000V is tightly integrated with VMware vCenter. This integration enables the network administrator and the server administrator to collaborate efficiently. The networking policies can be enforced in the virtual access layer just as in the physical network, but the Cisco Nexus 1000V helps maintain separation of duties for the network and server teams. There is no change in this integration for a VXLAN deployment.
- Cisco Prime Network Services Controller and Cisco VSG communication: Cisco VSG registers with Cisco Prime Network Services Controller through the policy agent configuration performed on Cisco VSG. Cisco Prime Network Services Controller then pushes the security and device policies to Cisco VSG. No policy configuration is performed through the Cisco VSG command-line interface (CLI) after Cisco VSG is registered with Cisco Prime Network Services Controller. The CLI is available to the administrator for monitoring and troubleshooting purposes.
- Cisco Nexus 1000V VSM and Cisco Prime Network Services Controller communication: VSM registers with Cisco Prime Network Services Controller through the policy agent configuration performed on the VSM. The steps for registration are similar to those for registering Cisco VSG with Cisco Prime Network Services Controller. After registration, the VSM can send the IP-to-virtual machine binding to Cisco Prime Network Services Controller. IP-to-virtual machine mapping is required by Cisco VSG to evaluate policies that are based on virtual machine attributes. The VSM also resolves the security profile ID using Cisco Prime Network Services Controller. This security profile ID is sent in every vPath packet to Cisco VSG and is used to identify the policy for evaluation.
- Cisco Prime Network Services Controller-to-VMware vCenter communication: Cisco Prime Network Services Controller registers with VMware vCenter for visibility into the VMware environment. This visibility allows the security administrator to define policies based on the VMware virtual machine attributes. Cisco Prime Network Services Controller integrates through an XML plug-in. The process is similar to the process for integration of the Cisco Nexus 1000V VSM with VMware vCenter.
- Management and orchestration tools: Cisco Prime Network Services Controller can also be programmed by third-party management and orchestration tools through XML APIs.

Sample Two-Tier Web Application on VXLAN with Cisco VSG

This document describes the configuration of two organizations: ABC and XYZ. Each organization is running a two-tier web application with a web server and client. In this scenario, the Cisco VSG service will be inserted for organization ABC, and this configuration will be compared with that of organization XYZ, which does not use the Cisco VSG service (Figure 2).

Figure 2. Sample Two-Tier Web Application



Solution Component Versions

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

- Cisco Nexus 1000V Release 4.2(1)SV1(5a)
- Cisco VSG Release 4.2(1)VSG1(3.1a)
- Cisco Prime Network Services Controller Release 1.3(1a)
- VMware vSphere Release 5.0
- VMware vCloud Director Release 5.0
- VMware vShield Manager Release 5.0

Solution Prerequisites

- All VMware vSphere components are deployed. These include:
 - VMware vCenter Server 5.0
 - Two or more hosts running VMware ESXi 5.0 or later
- The Cisco Nexus 1000V VSM is installed and functioning.
- The Cisco Nexus 1000V Virtual Ethernet Module (VEM) is installed on the VMware ESX and ESXi hosts that are part of VMware vCloud Director.
- The VMware vCloud Director cells and database are completely installed.
- The VMware vCloud Director provider virtual data center (vDC) and organizations are defined.
- The Cisco Nexus 1000V VSM is successfully registered with VMware vShield Manager, the VXLAN feature is enabled, and the VXLAN pool is created in VMware vShield Manager.

- Cisco Prime Network Services Controller is installed, and VMware vCenter, the Cisco Nexus 1000V VSM, and Cisco VSG are registered successfully with Cisco Prime Network Services Controller.
- Cisco VSG is installed and registered with Cisco Prime Network Services Controller.

Steps to Enable Cisco VSG for an Organization Network on VXLAN in VMware vCloud Director

The following sections present the steps required to enable Cisco VSG for an organization network on a VXLAN in VMware vCloud Director:

- Create the network segment policy and port profile for the organization using the Cisco Nexus 1000V CLI
- Create and verify the internal organization network on a VXLAN in VMware vCloud Director
- Enable Cisco VSG service for organization ABC:
 - Create a tenant for organization ABC
 - Create zone definitions for use in tenant ABC policies
 - Create a security profile for tenant ABC
 - Configure the policy sets that are part of the security profile
 - Configure the security policy for the policy set
 - Assign Cisco VSG to tenant ABC
 - Bind the security profile to the port profile associated with the network segment policy using the Cisco Nexus 1000V CLI

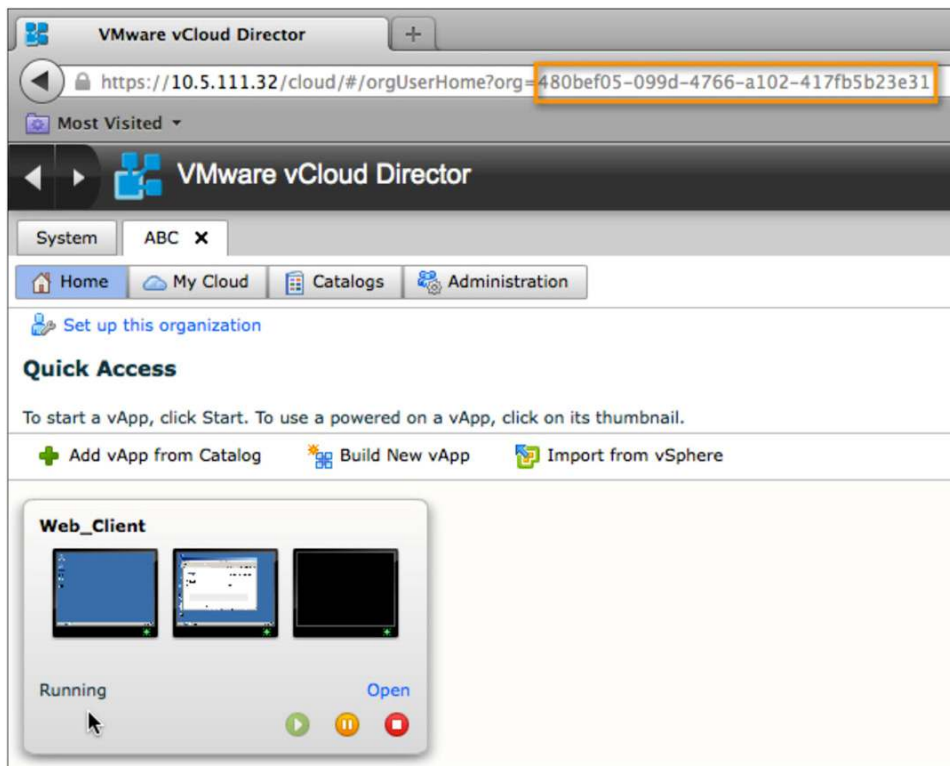
Create the Network Segment Policy and Port Profile for the Organization

Organization networks created in VMware vCloud Director can inherit a port profile defined in the Cisco Nexus 1000V if you import the port profile in a network segment policy associated with the organization.

A network segment policy is tied to an organization through the organization's universal user ID (UUID). This UUID is found in the URL created in VMware vCloud Director for the organization. This example uses the UUID for organization ABC (Figure 3). The following VMware knowledgebase article discusses how to obtain the UUID for an organization defined in VMware vCloud Director:


http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2012943.

Figure 3. Organization UUID in VMware vCloud Director



The UUID is then used in the following configuration at the Cisco Nexus 1000V CLI to create a network segment policy and associate it with organization ABC:

```
config t
  network-segment policy org-abc-policy
  id 480bef05-099d-4766-a102-417fb5b23e31
  type segmentation
  import port-profile tenant-abc-profile
end
```



The port profile **tenant-abc-profile** is initially created with no configuration. After you have defined the Cisco VSG policy in Cisco Prime Network Services Controller, you can configure the port profile to apply the security policy:

```
config t
  port-profile type vethernet tenant-abc-profile
  no shutdown
  state enabled
end
```

Organization XYZ will inherit the default network segment policy for its organization networks. This policy and the port profile imported by it are predefined and have the following configuration:

```
network-segment policy default_segmentation_template
  description Default template used for isolation backed pool
  type segmentation
  import port-profile NSM_template_segmentation

port-profile type vethernet NSM_template_segmentation
  no shutdown
  description NSM default port-profile for VXLAN networks. Do not delete.
  state enabled
```

Create and Verify the Internal Organization Network on VXLAN

The next step is to verify the port profiles generated for the organization networks for the ABC and XYZ organizations. The creation of the organization networks and vApps running on the networks is beyond the scope of this document, Figures 4 and 5 show the screens assuming that you have created the organization networks and deployed the web vApps on them.

Figure 4. Organization ABC vApp Deployed on ABC_Internal_Net_01

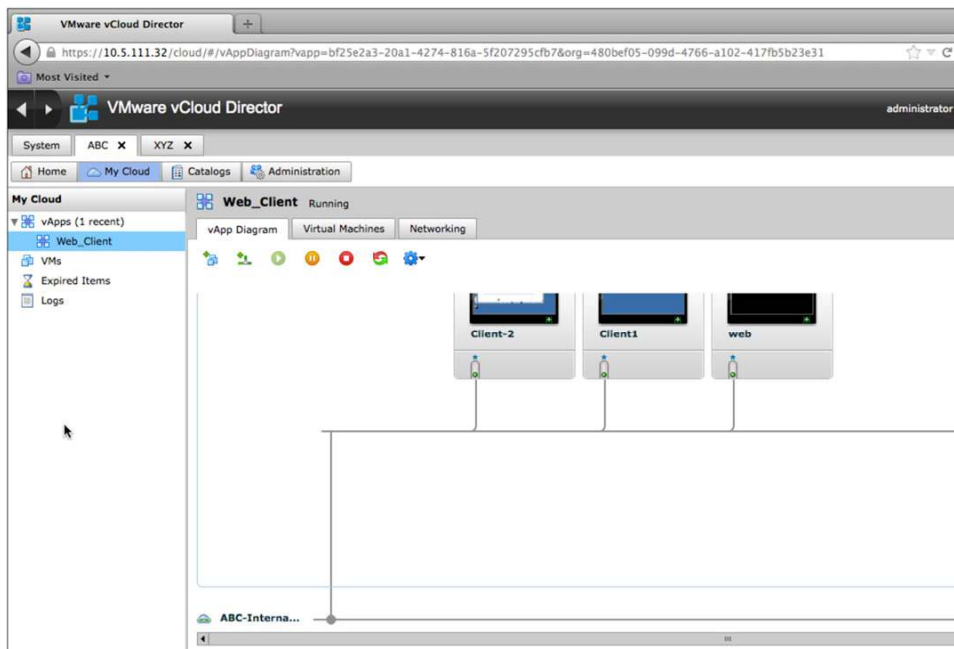
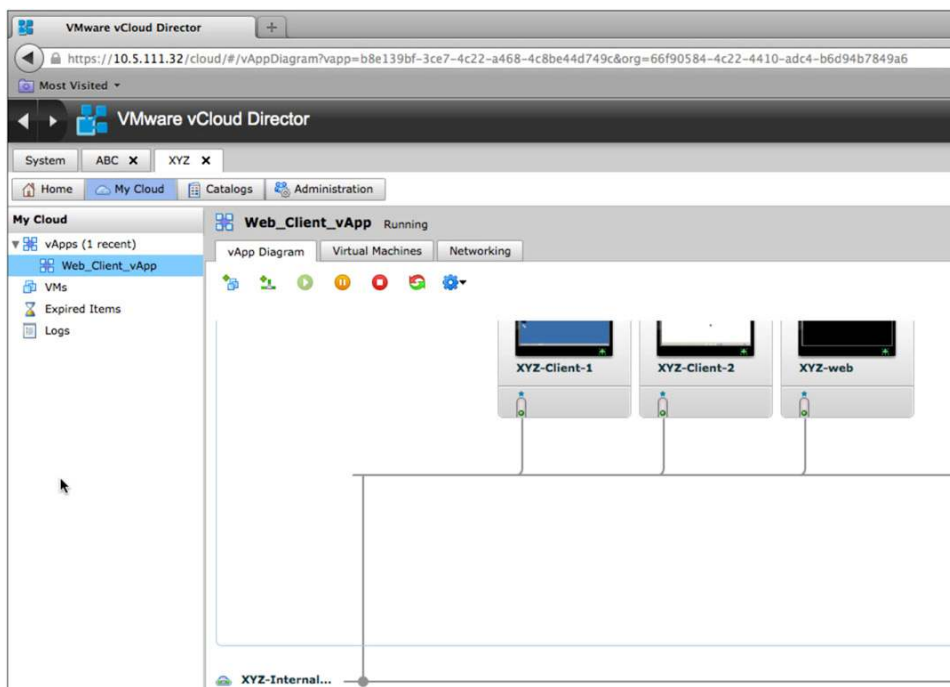


Figure 5. Organization XYZ vApp Deployed on XYZ_Internal_Net_01



The creation of the organization network in VMware vCloud Director triggers the creation of a port profile on the Cisco Nexus 1000V. The port profile created for organization ABC will inherit the **tenant-abc-profile**, and the profile for organization XYZ will inherit a default template. Here is the configuration to verify the port profile for each organization.

Organization ABC:

```
Nexus1000V-15a# show run port-profile dvs.VCDVSABC-Internal-Net-01-efa882ae-cb66-4774-98de-4422f030aad0

!Command: show running-config port-profile dvs.VCDVSABC-Internal-Net-01-efa882ae-cb66-4774-98de-4422f030aad0
!Time: Tue Aug 14 09:13:13 2012


version 4.2(1)SV1(5.1a)
port-profile type vethernet dvs.VCDVSABC-Internal-Net-01-efa882ae-cb66-4774-98de-4422f030aad0
  vmware port-group
  port-binding static auto expand
  inherit port-profile tenant-abc-profile
  switchport access bridge-domain "dvs.VCDVSABC-Internal-Net-01-efa882ae-cb66-4774-98de-4422f030aad0"
  description NSM created profile. Do not delete.
  state enabled
```


Organization XYZ:

```
Nexus1000V-15a# show run port-profile dvs.VCDVSXYZ-Internal-Net01-40a6d867-dc2d-4f7a-875b-0ae040796648

!Command: show running-config port-profile dvs.VCDVSXYZ-Internal-Net01-40a6d867-dc2d-4f7a-875b-0ae040796648
!Time: Tue Aug 14 09:40:50 2012

version 4.2(1)SV1(5.1a)
port-profile type vethernet dvs.VCDVSXYZ-Internal-Net01-40a6d867-dc2d-4f7a-875b-0ae040796648
    vmware port-group
    port-binding static auto expand
    inherit port-profile NSM_template_segmentation
    switchport access bridge-domain "dvs.VCDVSXYZ-Internal-Net01-40a6d867-dc2d-4f7a-875b-0ae040796648"
    description NSM created profile. Do not delete.
    state enabled
```



Enable Cisco VSG Service for the Organization

One or more instances of Cisco VSG can be deployed on a per-tenant basis, which allows a highly scalable deployment across many tenants. Tenants are isolated from each other, so no traffic can cross tenant boundaries. A tenant can be further divided into the following levels:

- Virtual data center
- Virtual application
- Virtual tier

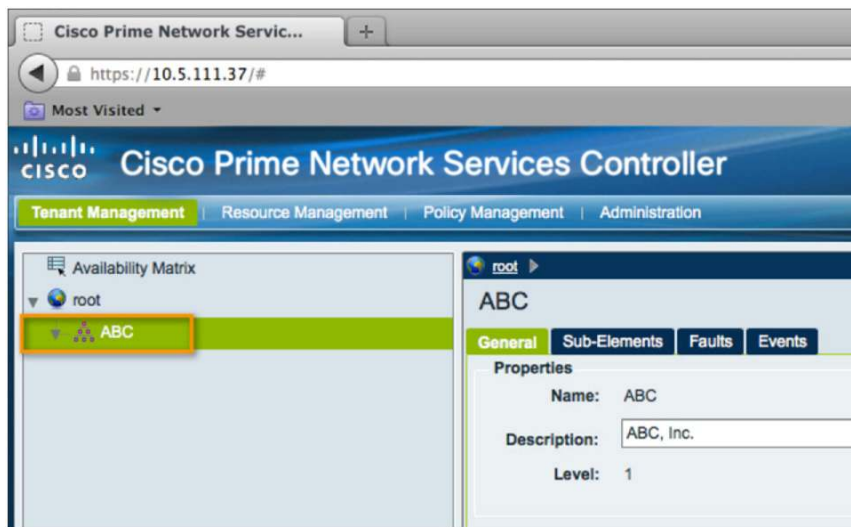
Each instance in a tenant tree is classified as an organization level. Depending on the use case, you can deploy Cisco VSG at the tenant level, at the vDC level, or at the vApp level.

This configuration example creates a tenant to represent organization ABC. The Cisco Prime Network Services Controller GUI is the configuration tool for Cisco VSG, and the following steps show the configuration in Cisco Prime Network Services Controller of a simple security policy for tenant ABC.

Create a Tenant for the Organization

The Tenant Management tab in the Cisco Prime Network Services Controller web interface provides information about the tenants (Figure 6).

Figure 6. Tenant ABC in Cisco Prime Network Services Controller Representing Organization ABC

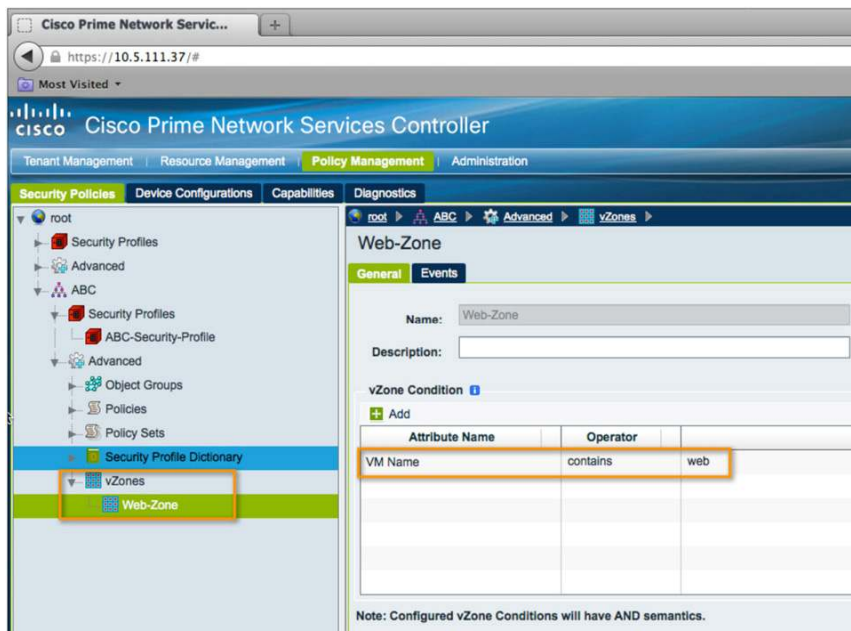


After the tenant has been created, you use the Policy Management tab to define zones, policies, policy sets, and security profiles.

Create Zone Definitions for Use in Tenant Policies

To secure the two-tier application for organization ABC, in this example a single zone called Web-Zone is defined based on the virtual machine attributes (Figure 7).

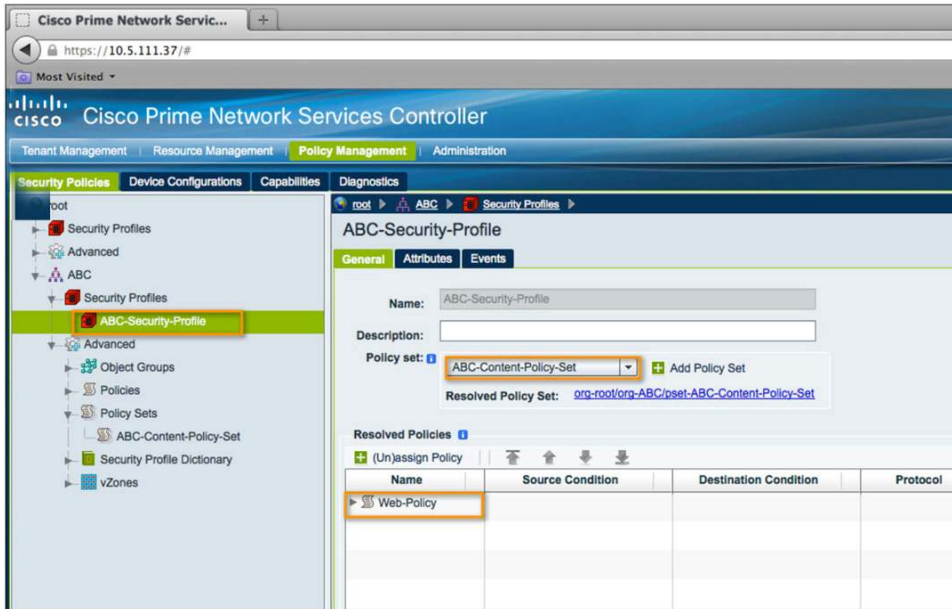
Figure 7. Zones Defined for Tenant ABC



Create a Security Profile for the Tenant

Figure 8 shows the security profile that will be applied in the Cisco Nexus 1000V VSM. The security profile in Cisco Prime Network Services Controller can contain one or more policy sets. The security profile in this example is ABC-Security-Profile, and it contains one policy set, called ABC-Content-Policy-Set.

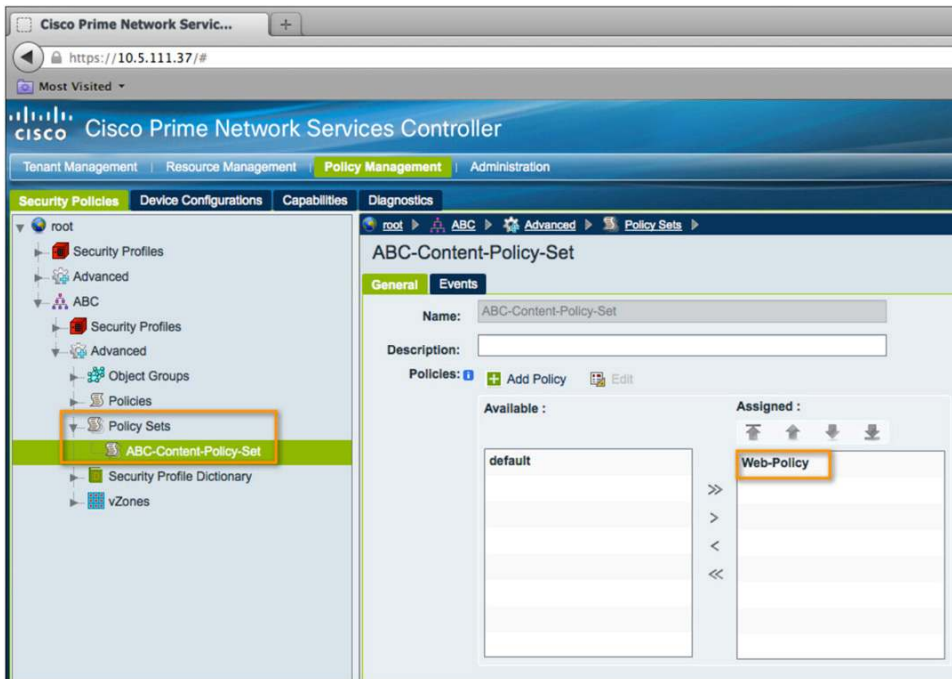
Figure 8. Security Profile ABC-Security-Profile



Configure the Policy Sets That Are Part of the Security Profile

The security profile consists of a policy set called ABC-Content-Policy-Set. A policy set provides the user with the flexibility to add and remove policies in the set as requirements change without affecting existing policies. In this case, the policy set includes only one policy (Figure 9).

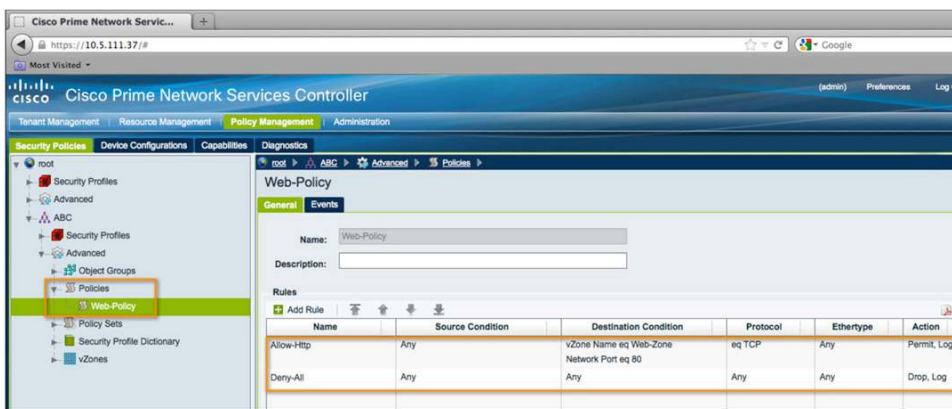
Figure 9. Policy Set Using Web Policy Security Policy



Configure the Security Policy for the Policy Set

The zone Web-Zone is used in the definition of the security policy Web-Policy. The rules for the security policy allow only HTTP traffic on port 80 to the web server and deny all other traffic (Figure 10).

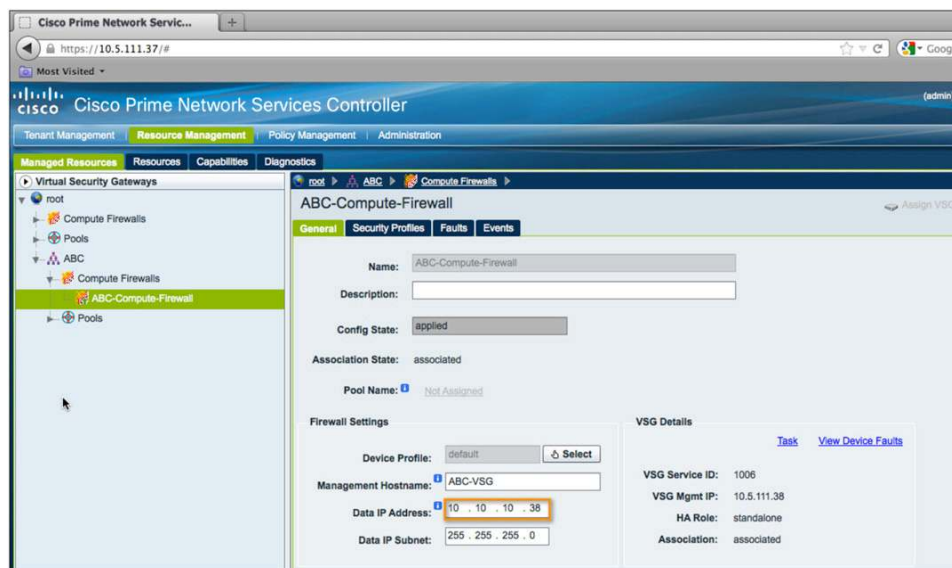
Figure 10. Web-Policy Security Policy for Tenant ABC



Assign Cisco VSG to the Tenant

The Cisco VSG instance assigned to the tenant for organization ABC is shown on the Cisco Prime Network Services Controller Resource Management tab (Figure 11). The IP address for the Cisco VSG data interface is defined here as 10.10.10.38 and will be used in the Cisco Nexus 1000V configuration to enable the service on the port profile.

Figure 11. Cisco VSG Assigned to a Tenant



Bind the Security Profile to the Port Profile

The final step in the addition of the Cisco VSG service is the configuration on the Cisco Nexus 1000V to enable the service for organization ABC. In this example, you first associate the port profile **tenant-abc-profile** with the tenant **ABC** defined in Cisco Prime Network Services Controller; then you configure the **vn-service** command to apply **ABC-Security-Profile** through the Cisco VSG data interface. You apply the following configuration commands to the port profile to accomplish this:

```
port-profile type vethernet tenant-abc-profile
org root/ABC
vn-service ip-address 10.10.10.38 vlan 21 security-profile ABC-Security-Profile
```

The final configuration for the port profile is as follows:

```
port-profile type vethernet tenant-abc-profile
org root/ABC
no shutdown
vn-service ip-address 10.10.10.38 vlan 21 security-profile ABC-Security-Profile
state enabled
```

The Cisco VSG service is now configured to work with the Cisco Nexus 1000V Switch deployed with VMware vCloud Director using VXLAN.

Conclusion

The Cisco Nexus 1000V Switch with VXLAN support and integration with VMware vCloud Director provides numerous advantages for customers, enabling customers to use LAN segments in a robust and customizable way without disrupting existing operations. Furthermore, network services such as Cisco VSG can be easily inserted to enforce security policies in this environment. As demonstrated in this document, Cisco Prime Network Services Controller and VSG can be integrated transparently into a VXLAN network using Cisco Nexus 1000V with VMware vCloud Director.

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>
- VMware vCloud Director: <http://www.vmware.com/products/vcloud-director>
- VMware vSphere: <http://www.vmware.com/go/vsphere>
- Deployment guide for Cisco Nexus 1000V Series Switches:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html
- Deployment guide for Cisco Nexus 1000V with VMware vCloud Director using VXLAN:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/deployment_guide_c07-703595.html
- Deployment guide for Cisco VSG:
http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps11208/deployment_guide_c07-647435.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.

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)