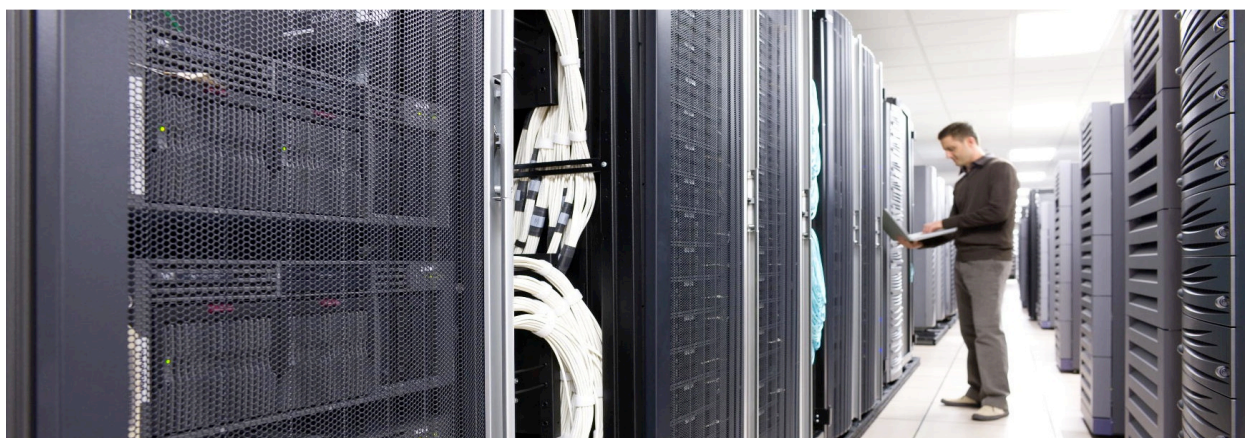


Enable Cisco VSG service on an organization VXLAN network in VMware vCloud Director



Many organizations are moving towards building public and private clouds to support a multi-tenant environment. The tenants in this environment need to have segmentation at the network level, traditional network segmentation mechanisms like 802.1Q VLAN tagging may not be sufficient for large scale cloud deployments as the number of LAN segments is limited to 4096. Virtual Extensible LAN (or 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 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 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 vCloud Director environment, VSG can be inserted to provide tenant-level security when the organization network is backed by a VXLAN pool provided by the Cisco Nexus 1000V switch.

Intended Audience

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

What You Will Learn

This document will guide the reader on how the VSG service can be enabled for all vApps on an organization network created in VMware vCloud Director using a VXLAN backed pool.

This white paper will not go into the details or best practices for deploying the 1000V series switches. For information regarding Cisco Nexus 1000V Series Switches Deployment Guide refer to:

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

For information on deploying Cisco Nexus 1000V with VMware vCloud Director using VXLAN please refer to:

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/deployment_guide_c07-703595.html

The VSG deployment guide can be found here:

http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps11208/deployment_guide_c07-647435.html

Solution Architecture

The solution architecture for deploying Cisco Virtual Security Gateway with Cisco Nexus 1000V with vCloud Director to support VXLAN includes the following components. These components and their interactions are discussed below.

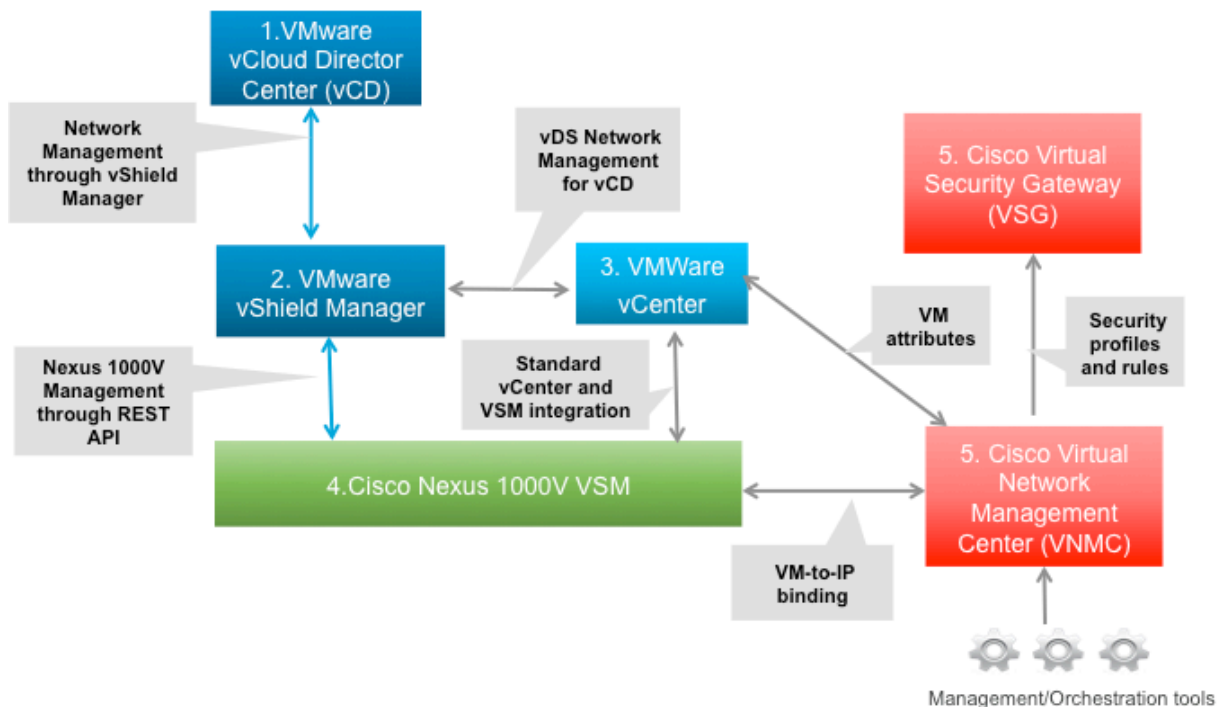


Figure 1. Solution Architecture

The main components of the solution are:

- **VMware vCloud Director and VMware vShield Manager communication** - vCloud Director provides network services to the cloud via VMware vShield Manager. vShield Manager interacts with Cisco Nexus 1000V VSM to make the 1000V available to vCloud Director to build any type of network when building a tenant cloud. Each vCloud Director cell requires access to a vShield Manager host, which in turn provides network services to the cloud. You must have a unique instance of vShield Manager for each vCenter server you add to vCloud Director.

-
- **Cisco Nexus 1000V and VMware vShield Manager communication** - vCloud Director interacts with the Cisco Nexus 1000V using vShield Manager. The VSM implements a representational state transfer (REST) API that allows the user to create all types of networks supported by vCloud Director. This allows the user to design and implement networks in vCloud Director which that then get created on the Cisco Nexus 1000V Series Switch.

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

- a) VSM connectivity details
 - b) Number of multicast addresses available for the vCloud Director
 - c) Number of VXLANs that can be consumed by vCloud Director
- **VMware vShield Manager and vCenter communication** - This communication will occur when an organization routed network is required for an organization. vShield Manager will instantiate a vShield Edge appliance dynamically to provide Network Address Translation (NAT), and IP gateway service for an organization network.
 - **vCenter and Cisco Nexus 1000V VSM communication** - 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. While the networking policies can be enforced in the virtual access layer just like as in the physical network, Cisco Nexus 1000V helps maintain separation of duties for the network and server teams. There is no change in this integration with regards to VXLAN deployment.
 - **Cisco VNMC and Cisco VSG communication** - VSG registers to VNMC via the policy agent configuration done on VSG. Once registered, VNMC pushes the security and device policies to VSG. No policy configuration is done via the VSG command-line interface (CLI) once it is registered to VNMC. The CLI is available to the administrator for monitoring and troubleshooting purposes.
 - **Cisco Nexus 1000V VSM and Cisco VNMC communication** - VSM registers to VNMC via the policy agent configuration done on VSM. The steps to register are similar to those for VSG to VNMC registration. Once registered, VSM can send IP-to-VM binding to VNMC. IP-to-VM mapping is required by the VSG for evaluating policies that are based on VM attributes. VSM also resolves the security-profile ID using VNMC. This security-profile ID is sent in every vPath packet to VSG and is used to identify the policy for evaluation.
 - **Cisco VNMC to vCenter communication** - Cisco VNMC registers to vCenter for visibility into the VMware environment. This allows the security administrator to define the policies based on the VMware VM attributes. VNMC integrates via an XML plug-in. The process is similar to the way the Cisco Nexus 1000V VSM integrates with vCenter.
 - **Management and Orchestration tools** – Cisco VNMC can also be programmed by third-party management and orchestration tools through XML APIs.

Sample 2-tier Web application on VXLAN with VSG

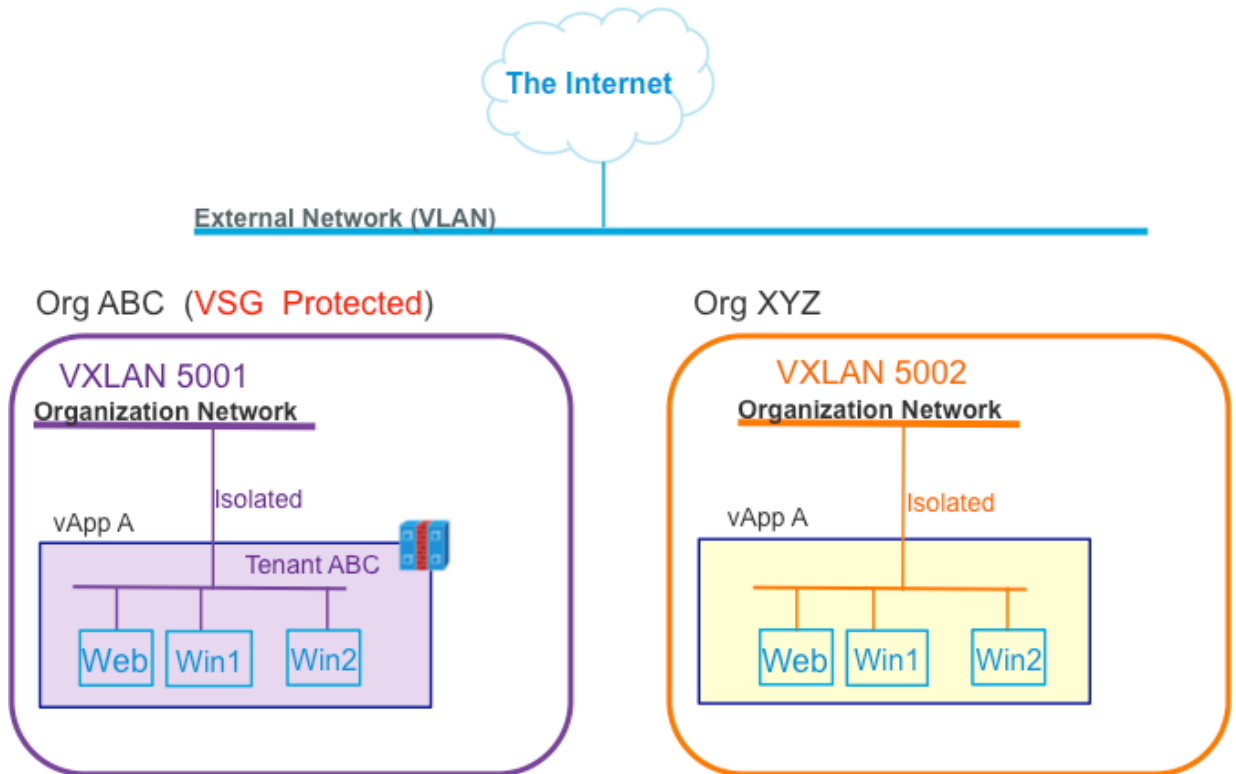


Figure 2. Sample 2-tier web application

In this white paper we will be configuring two organizations – ABC and XYZ. Each organization is running a 2-tier web application with a web server and client. In this scenario we will insert the Cisco VSG service for organization ABC and contrast the configuration with that of organization XYZ for which the VSG service is not inserted.

Solution Components – Versions

This white paper is written using the following versions for the different software components -

- Cisco Nexus 1000V version 4.2(1)SV1(5a)
- Cisco VSG version 4.2(1)VSG1(3.1a)
- Cisco VNMC version 1.3(1a)
- VMware vSphere version 5.0
- VMware vCloud Director version 5.0
- VMware vShield Manager version 5.0

Pre-requisites

- All vSphere components have been deployed. These include:

-
- vCenter Server 5.0
 - Two or more hosts running ESXi 5.0 or later
 - The Cisco Nexus 1000V Virtual Supervisor Module (VSM) is installed and functioning.
 - The Cisco Nexus 1000V Virtual Ethernet Module (VEM) is installed on the ESX/ESXi hosts that are part of vCloud Director.
 - The vCloud Director cell(s) and database have been completely installed.
 - The vCloud Director provider vDC and organizations have been defined
 - The Cisco Nexus 1000V VSM is successfully registered with vShield Manager, the VXLAN feature has been enabled and the VXLAN pool created in vShield Manager.
 - The Cisco VNMC is installed and vCenter, Cisco Nexus 1000V VSM and Cisco VSG have registered successfully with VNMC.
 - The Cisco VSG is installed and registered with Cisco VNMC.

Steps to enable VSG for an organization network on VXLAN in vCloud Director

The following sections will detail the steps that are required to enable VSG for an organization network on VXLAN and vCloud Director. In a nutshell the steps are as follows –

- Create the network-segment policy and port-profile for the organization on the Nexus 1000V CLI
- Create and verify internal organization network on VXLAN in vCloud Director
- Enable VSG service for organization ABC. This step involves the performing the following –
 - Create a tenant for organization ABC
 - Create a security-profile for the tenant ABC
 - Create zone definitions for use in policies
 - Configure the policy-sets that are part of the security-profile
 - Configure the policies that are in the policy-set
 - Assign a VSG to tenant ABC
 - Bind the security-profile to the port-profile tied to the network-segment policy on the Nexus 1000V CLI
- Bind the security-profile to the port-profile created in the first step on the Nexus 1000V CLI

Create the network-segment policy and port-profile for the organization

Organization networks created in vCloud Director can inherit a port-profile defined in the Cisco Nexus 1000V by importing the port-profile in a network-segment policy associated with the organization.

A network-segment policy is tied to an organization through the organization UUID. This UUID is found in the URL created in vCloud Director for the organization. In this example, we are interested in the UUID for organization ABC, Inc. The following VMware KB article details how to obtain the UUID for an organization defined in vCloud Director -

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

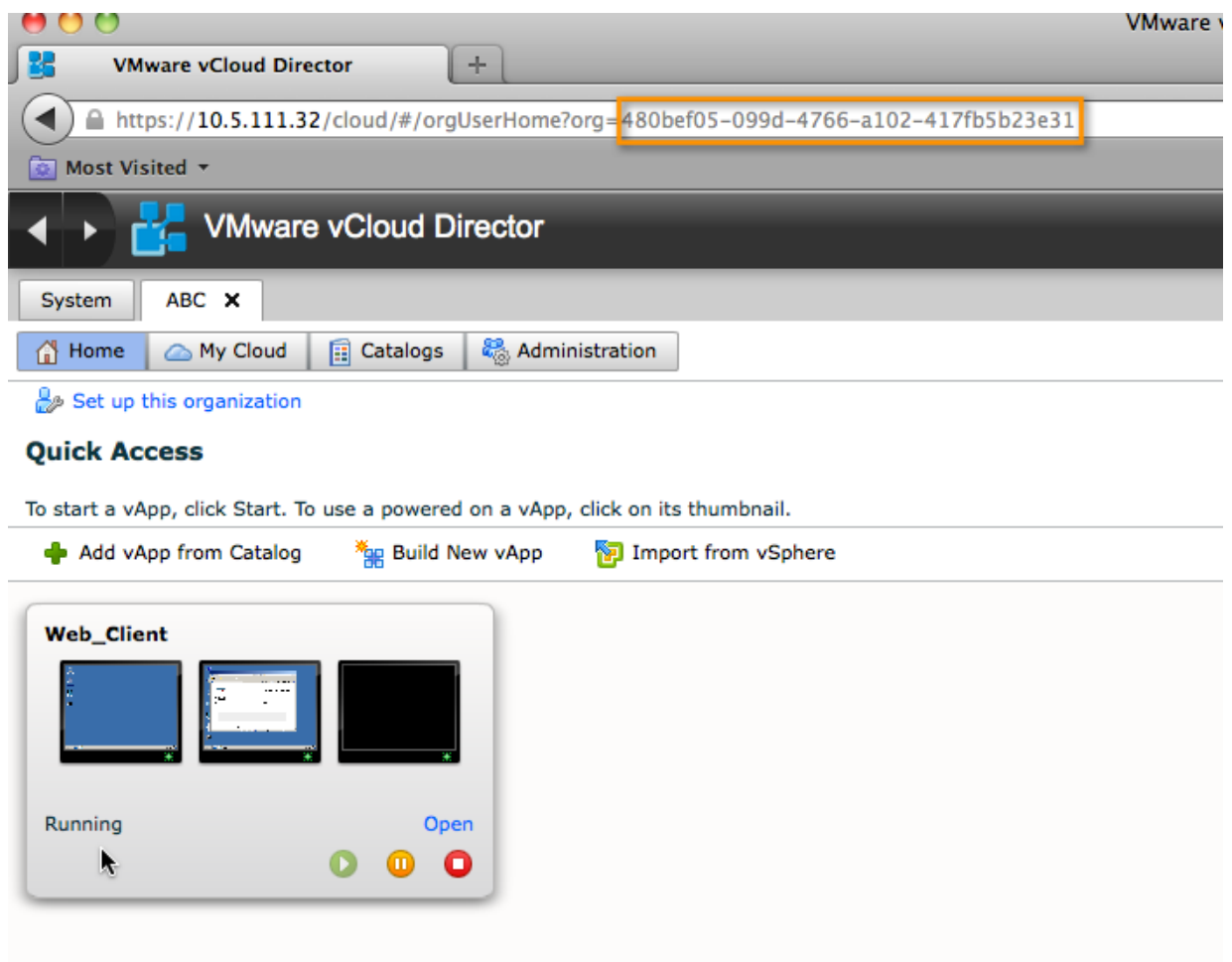



Figure 3. Organization UUID in vCloud Director

The UUID obtained above is then used in the following configuration on the Cisco Nexus 1000V CLI to create a network-segment policy and tie it to 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. Once we have defined the VSG policy in VNMC, we can configure the port-profile to apply the security policy.

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

The organization XYZ will inherit the default network-segment policy for its organization networks. This and the port-profile imported by it are pre-defined 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 internal organization network on VXLAN

The next step is verifying the port-profiles that are generated for the organization networks for the ABC and XYZ organizations. The creation of the organization network and vApps running on the network is beyond the scope of this paper, assuming the user has created the organizations network and deployed the web vApp on it, the network diagram for each organization is as follows:

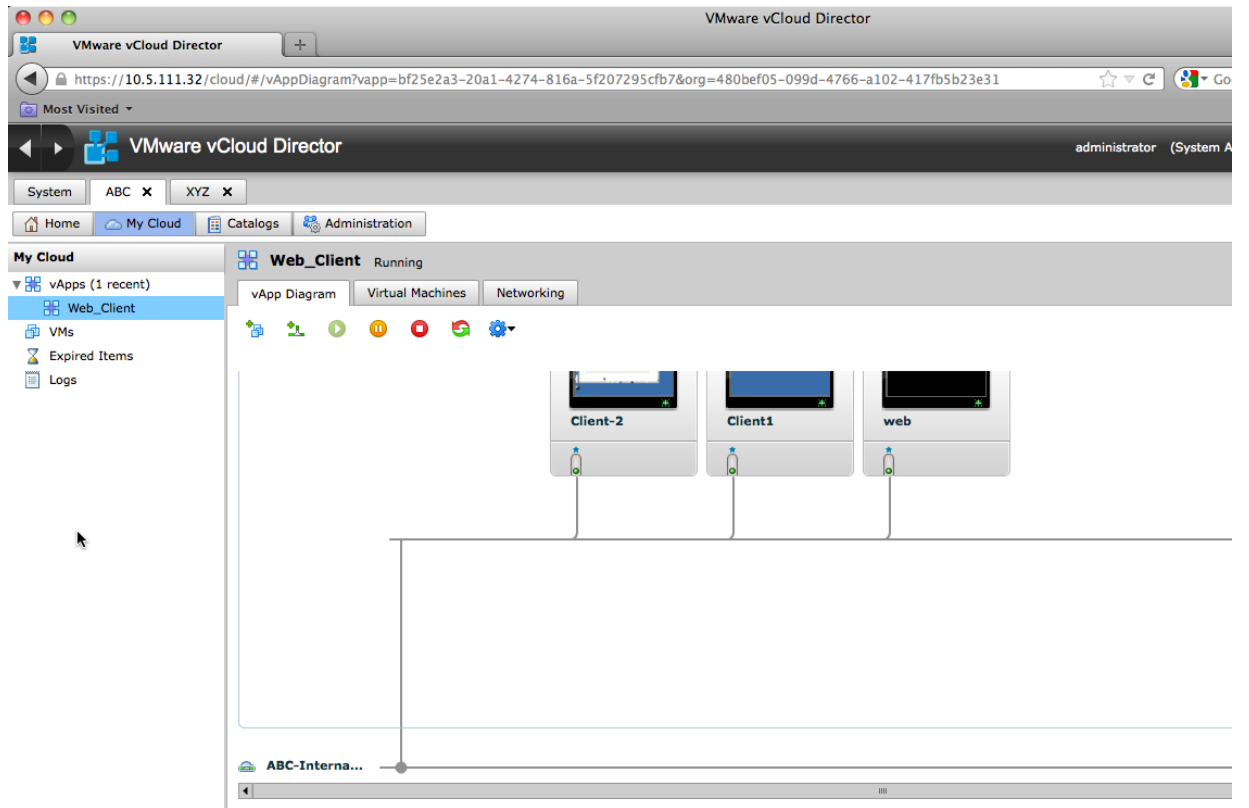


Figure 4. Organization ABC vApp deployed on ABC_Internal_Net_01

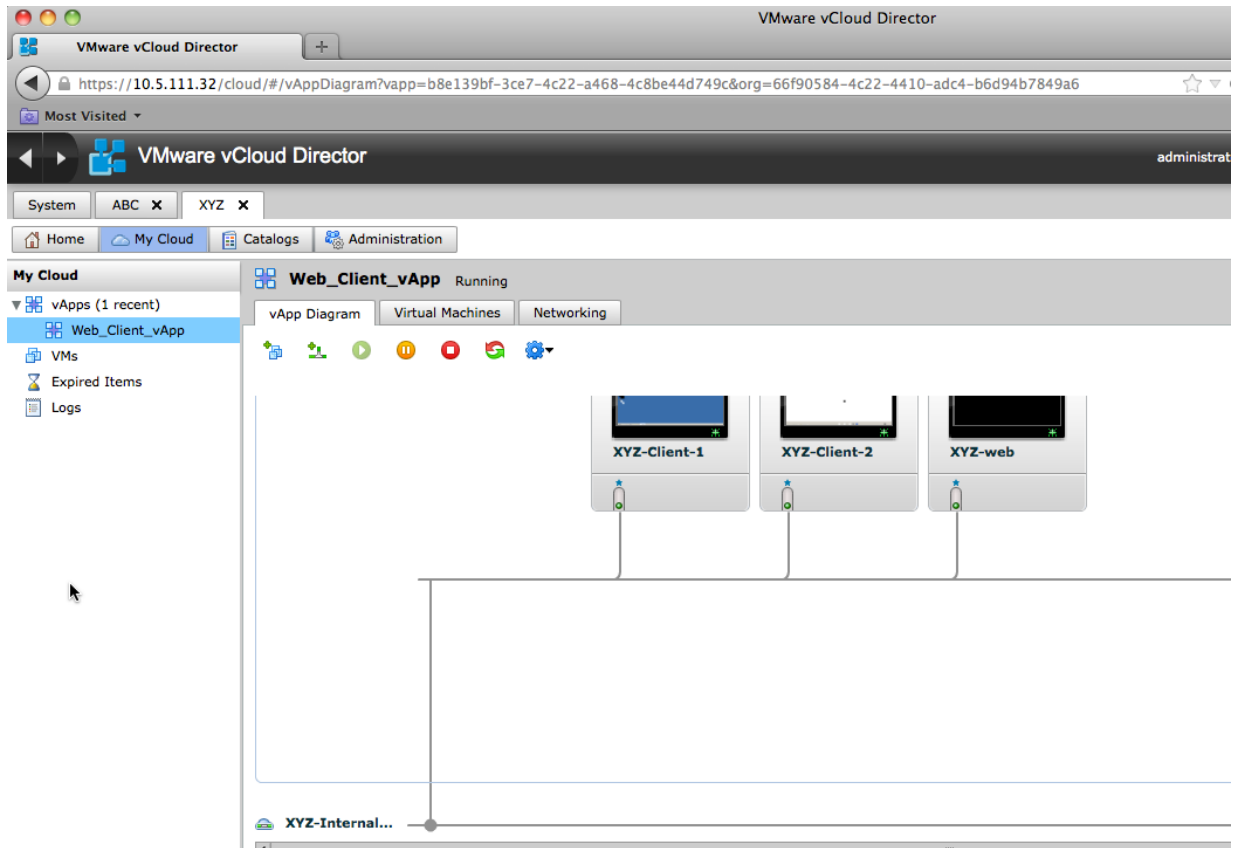


Figure 5. Organization XYZ vApp deployed on XYZ_Internal_Net_01

The creation of the organization network in vCloud Director triggers the creation of a port-profile on the Nexus 1000V. The port-profile created for organization ABC will inherit the **tenant-abc-profile**, while the organization XYZ will inherit a default template. Here we will 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 VSG service for organization ABC

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 to the following levels:

- Virtual data center
- Virtual application
- Virtual tier

Each instance in a tenant tree is classified as an org level. Depending on the use case, you can deploy a Cisco VSG at the tenant level, at the virtual data center (vDC) level, or at the vApp level.

In this configuration example we will be creating a tenant to represent organization ABC. The VNMC GUI is the configuration tool for VSG, and in the following steps we will look at the configuration in VNMC for a simple security policy for the tenant ABC.

Create a tenant for organization ABC

The Tenant Management tab in the Cisco VNMC web interface provides information about the tenants.

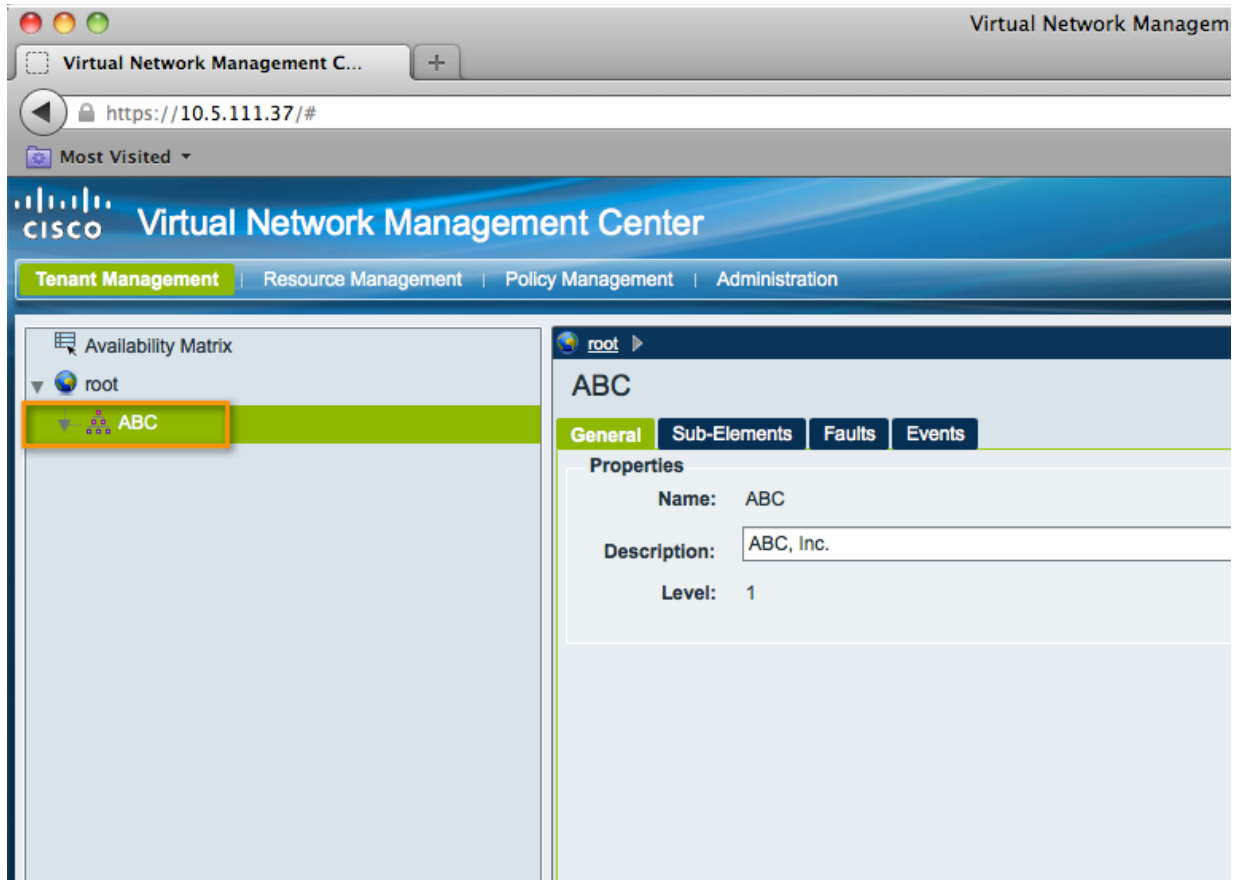


Figure 6. Tenant ABC in Cisco VNMC representing organization ABC, Inc

Once the tenant has been created the Policy Management tab is used to define zones, policies, policy sets and security profiles.

Zone definition for tenant ABC

In order to secure the two-tier application for organization ABC, a single zone called **Web-Zone** has been defined based on VM attributes.

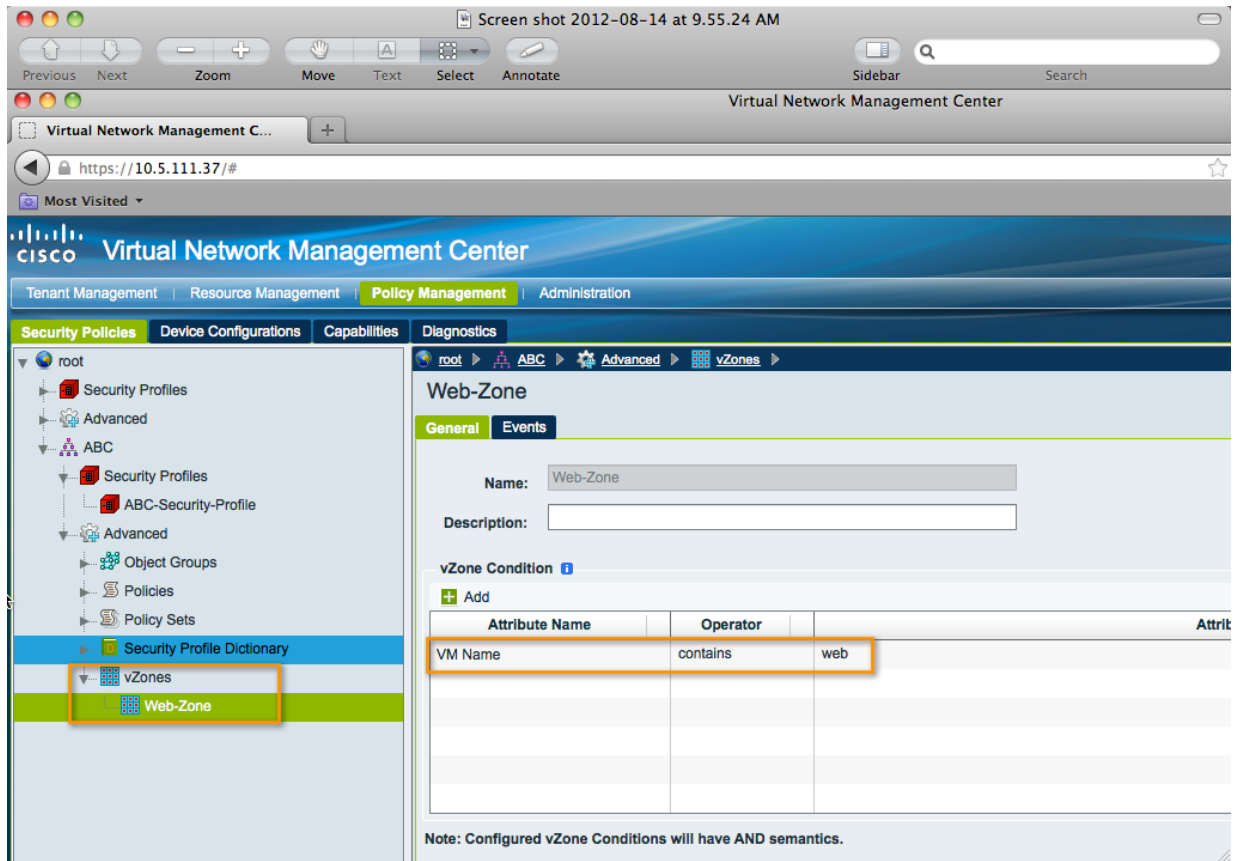


Figure 7. Zones defined for tenant ABC

Security profile for tenant ABC

We are now ready to view the security profile that will be applied in the Nexus 1000V VSM. The security-profile in VNMC can contain one or more policy-sets. The security profile in this example is the **ABC-Security-Profile** and contains one policy-set which is the **ABC-Content-Policy-Set**.

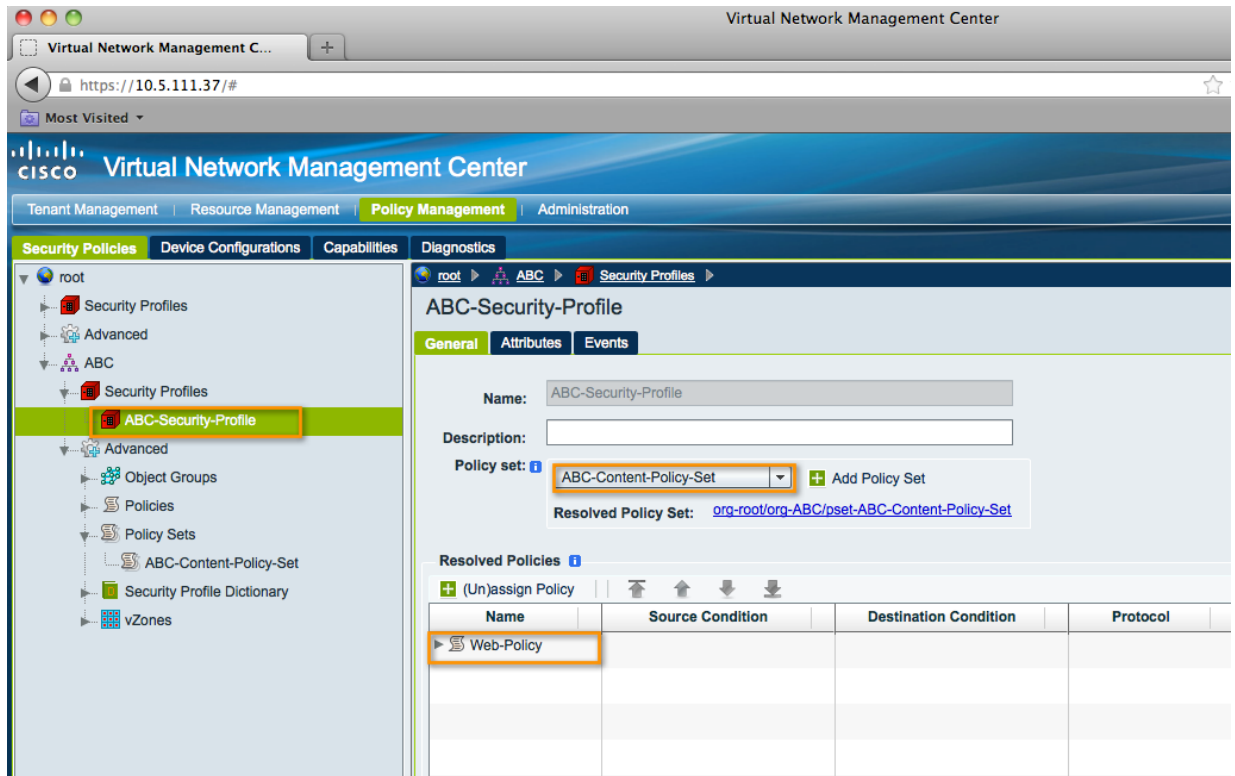


Figure 8. Security Profile ABC-Security-Profile

Policy Set definition

The security profile consists of a policy-set **ABC-Content-Policy-Set**. A policy set provides the user with the flexibility of adding and removing policies to a set as their requirements change without affecting existing policies. In this case the policy-set has only one policy included in it.

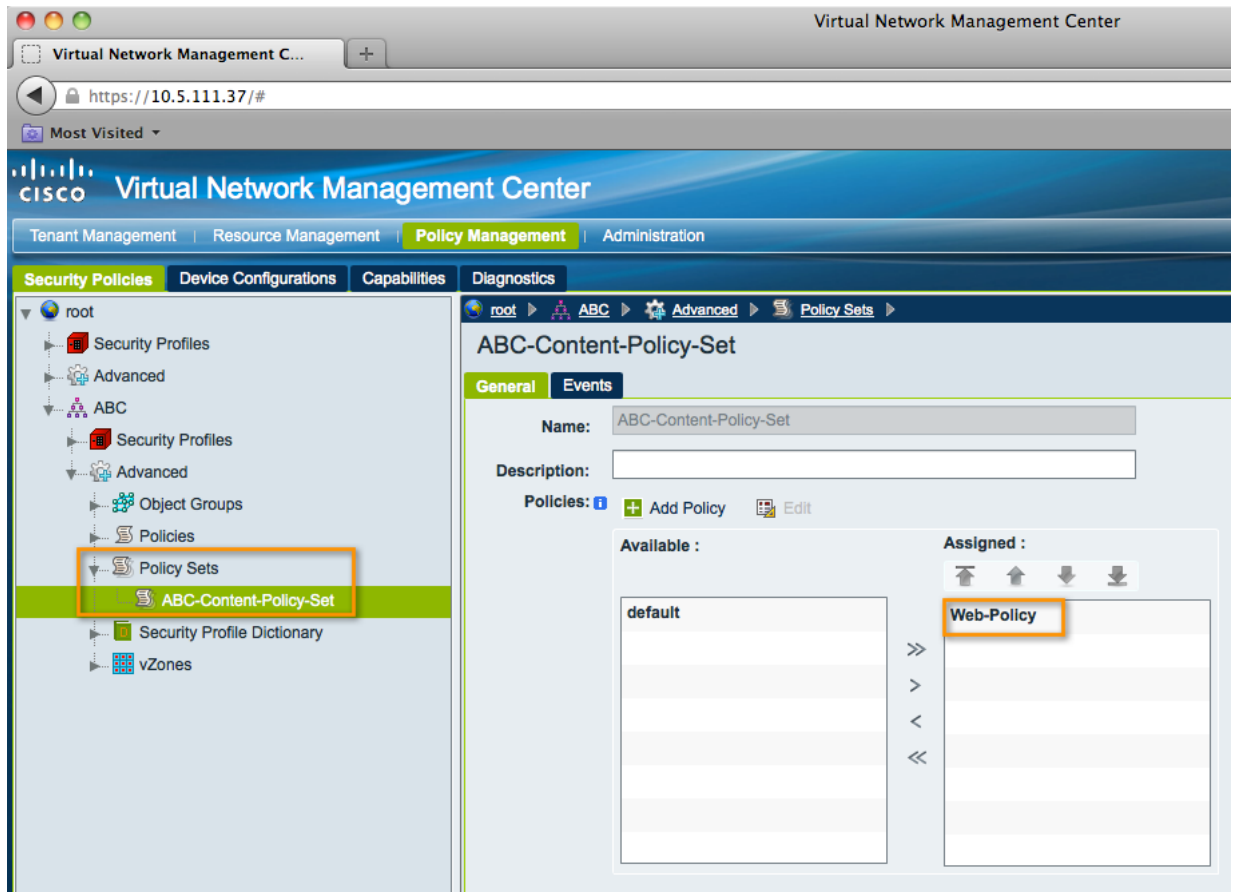


Figure 9. Policy Set using Web-Policy security policy

Security Policy definition

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

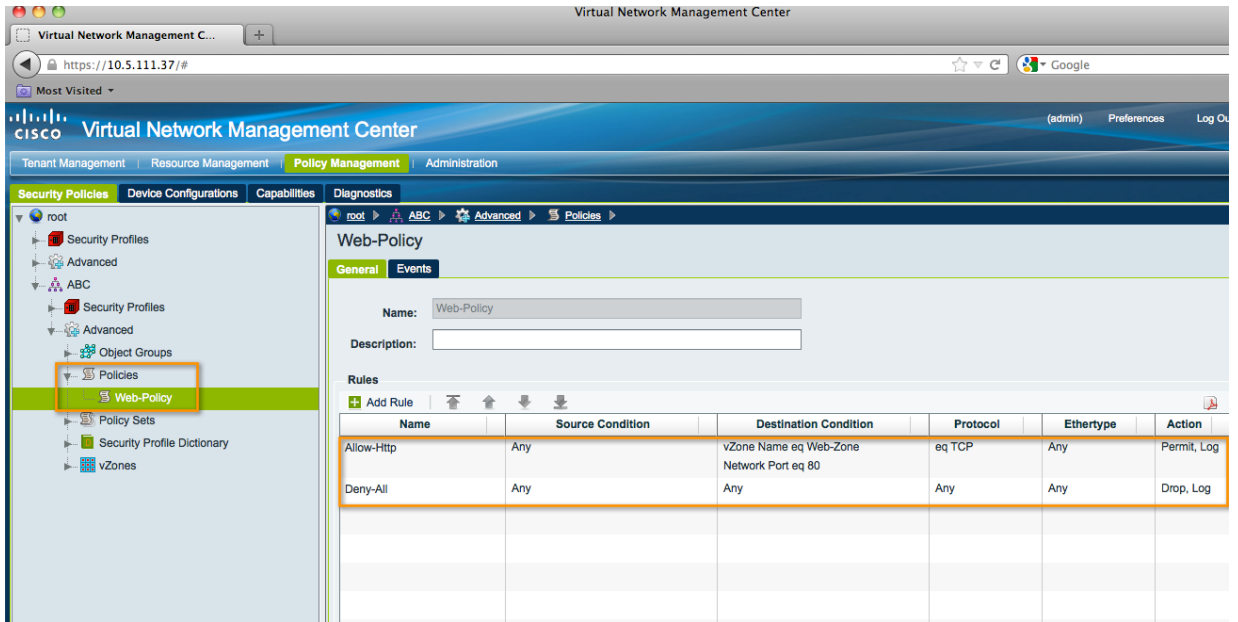


Figure 10. Web-Policy security policy for tenant ABC

Assigning a VSG to a tenant

The VSG assigned to the tenant for organization ABC can be seen in the Resource Management tab of VNMC. The IP address for the VSG data interface is defined here to be 10.10.10.38 and will be used in the Nexus 1000V configuration to enable the service on the port-profile.

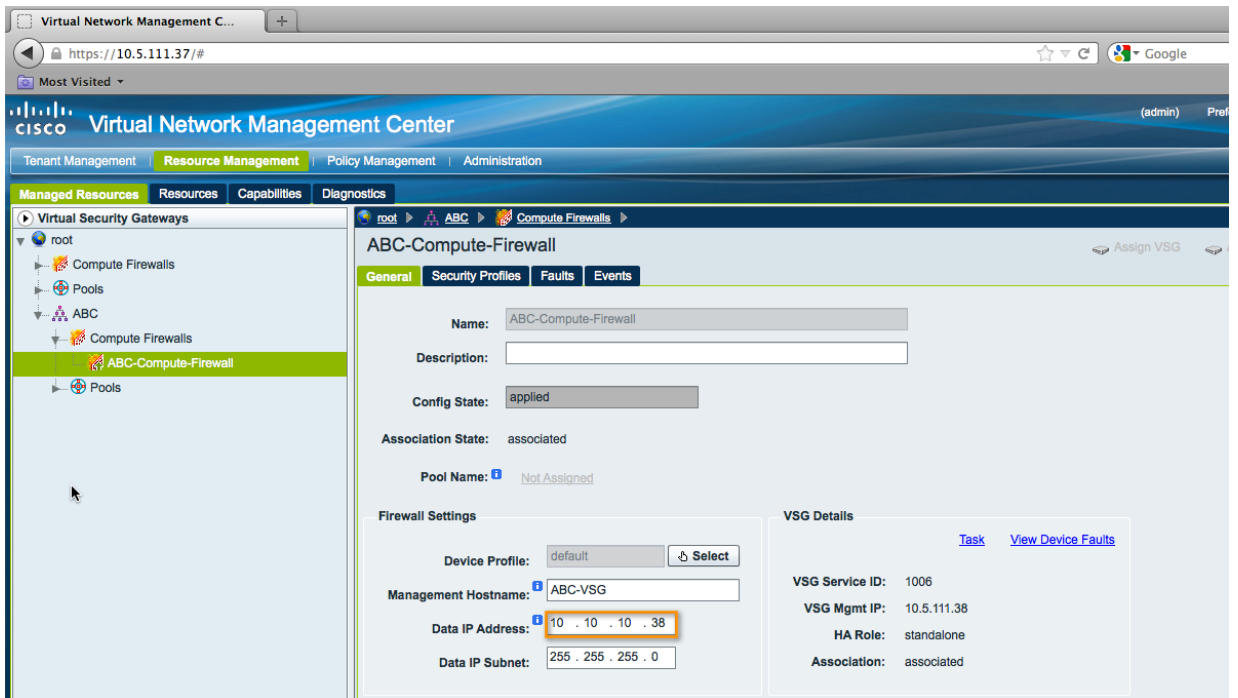


Figure 11. VSG assigned to a tenant

Bind the security-profile to the port-profile

The final step in the addition of the VSG service is the configuration on the Nexus 1000V to enable the service for organization ABC. We first associate the port-profile **tenant-abc-profile** with the tenant **ABC** defined in VNMC, and then configure the vn-service command to apply the **ABC-Security-Profile** through the VSG data interface. The following configuration commands are applied 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 on 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
```

We have now successfully configured the VSG service to work with the Nexus 1000V deployed with VMware vCloud Director using VXLAN.

Conclusion

The Cisco Nexus 1000V Series Switch with VXLAN support and integration with vCloud Director provide numerous advantages for customers, enabling customers to use LAN segments in a robust and customizable way without disrupting existing operational modes. Furthermore, network services such as VSG can be easily inserted to enforce security policies in this environment. As demonstrated in this paper, Cisco VNMC and Cisco VSG can be integrated in a seamless manner into a VXLAN network when 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>



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)

Printed in USA

CXX-XXXXXX-XX 10/11