



fineDoc Number: EDCS-<XXXXXX>
Last Revision Date: February 3, 2011
Created by: Steve Winters
Template Ver. Number: EDCS-XXXX Rev X

Virtual Security Gateway Infrastructure Configuration White Paper



TABLE OF CONTENTS

1	INTRODUCTION	3
2	REQUIREMENTS	3
3	COMMUNICATION PATHS	3
4	INSTALL AND CONFIGURE VSG	4
4.1	VSM Prep-work	4
4.2	Install VSG VM	5
5	CONFIGURE VNMC	5
5.1	Install VNMC VM	5
5.2	Register VSG and VSM with VNMC	6
5.2.1	Register VSG to VNMC	6
5.2.2	Register VSM to VNMC	6
5.2.3	Confirm registration on the VNMC	6
5.3	Register VNMC with vCenter	7
5.4	Assign VSG to a Tenant	9
5.4.1	Create Tenant	10
5.4.2	Define the Tenant's VSG system parameters	10
5.5	Create a compute firewall	15
6	SUMMARY	20

1 Introduction

The Cisco Nexus 1000V Virtual Service Gateway is a Cisco developed server virtualization firewall architecture for VMware ESX 4.0u1 and higher environments. The VSG applies policy, or zone based rule sets to virtual machines (VM's) in a vSphere datacenter.

The purpose of this document is to walk the reader through the infrastructure requirements and configurations for a successful Virtual Security gateway (VSG) deployment.

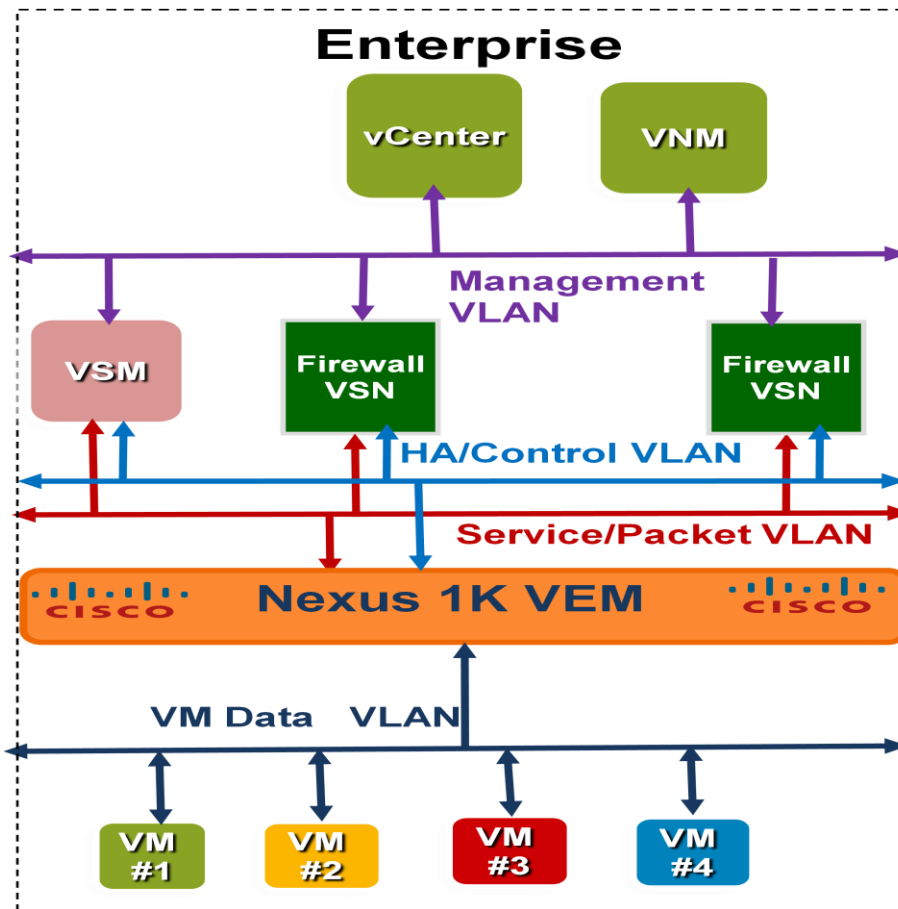
2 Requirements

We assume that the reader has:

- Installed VMware vCenter/vSphere 4.0U1/U2 or 4.1
- Installed Cisco Nexus 1000V release 1.4
- Created a Nexus 1000V Distributed Virtual Switch (DVS) under VC
- At least 2 ESX 4.0U1/U1 or 4.1 servers with VEM installed
- Added the ESX hosts to the Nexus 1000V

3 Communication paths

The following diagram demonstrates the required connectivity between the major components of the firewalled environment:



VSG VM requires three vNICs:

- Management
 - VNM talks to vCenter, VSM, and Firewall VSN
- HA
 - Firewall VSN HA-pair exchanges HA messages over the HA VLAN.
 - It can be shared with VSM Control VLAN.
 - It can also be shared with the Service VLAN
 - *** In this document however, the HA-VSN is its own VLAN ***
- Service VLAN (this is referred to as the “data” VLAN on the VSG)
 - N1K vPath and VSG communicate over Service VLAN. It can be shared with VSM Packet VLAN

4 Install and Configure VSG

4.1 VSM Prep-work

VSG requires service, management, and HA vlan's. (This is conceptually akin to the VSM network requirements (control, management, packet VLAN's).)

Create a Service VLAN and HA Vlan on the VSM to support the VSG VM:

```
n1kv# conf t
```

```
n1kv(config)# port-profile type vethernet service-vsn
n1kv(config-port-prof)# vmware port-group
n1kv(config-port-prof)# switchport mode access
n1kv(config-port-prof)# switchport access vlan 100
n1kv(config-port-prof)# no shutdown
n1kv(config-port-prof)# state enabled
n1kv(config-port-prof)# exit
```

```
n1kv(config)# port-profile type vethernet ha-vsn
n1kv(config-port-prof)# vmware port-group
n1kv(config-port-prof)# switchport mode access
n1kv(config-port-prof)# switchport access vlan 10
n1kv(config-port-prof)# no shutdown
n1kv(config-port-prof)# state enabled
n1kv(config-port-prof)# exit
```

4.2 Install VSG VM

Install VSG VM from OVA file, or from ISO image. If installing from ISO, use the following as a guideline for the VM:

- Custom Configuration
- Linux, (Other 2.6 Linux (32 bit))
- 2 GB HD
- 2 GB Memory
- 3 NIC's in this order:
 - Service-vsn (VMXNET3)
 - Management (E1000)
 - Ha-vsn (E1000)

then:

- Power on the VM
- attach the VSG iso image
- select install

provide a secure password and answer the ensuing prompts

5 Configure VNMC

The Cisco Virtual Network Management Controller (VNMC) virtual machine is a powerful and extensible XML based GUI front-end used for creating policies that then are assigned to a VSG (or VSG's) in a single tenant or multi-tenant environment.

5.1 Install VNMC VM

Installation of the VNMC from the ova file is trivial: simply answer when prompted and complete the fields appropriately. The "shared secret" password is the authentication password that the VNMC will expect from the VSG and VSM as part of their registration process with the VNMC.

5.2 Register VSG and VSM with VNMC

A policy agent runs on the VSG and VSM and is used to communicate with the VNMC. The policy agent resides in bootflash:

5.2.1 Register VSG to VNMC

```
cae-vsg1# dir bootflash:
...
  21072111      Feb 02 09:36:34 2011  vnmc-vsgpa.1.0.1j.bin
...
cae-vsg1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cae-vsg1(config)# vnm-policy-agent
cae-vsg1(config-vnm-policy-agent)# registration-ip 172.18.217.209
cae-vsg1(config-vnm-policy-agent)# shared-secret *****
cae-vsg1(config-vnm-policy-agent)# policy-agent-image vnmc-vsgpa.1.0.1f.bin
```

Verify the connectivity from the VSG CLI:

***** Note, it may take up to a minute for the policy agent to authenticate and register to the VNMC *****

```
cae-vsg1# sh vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(0.414)-vsn
```

5.2.2 Register VSM to VNMC

```
cae-bl-vsm1# dir bootflash:
...
  20827098      Feb 02 08:28:24 2011  vnmc-vsmpa.1.0.1j.bin
...
cae-bl-vsm1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cae-bl-vsm1(config)# vnm-policy-agent
cae-bl-vsm1(config-vnm-policy-agent)# registration-ip 172.18.217.209
cae-bl-vsm1(config-vnm-policy-agent)# shared-secret *****
cae-bl-vsm1(config-vnm-policy-agent)# policy-agent-image vnmc-vsmpa.1.0.1j.bin
```

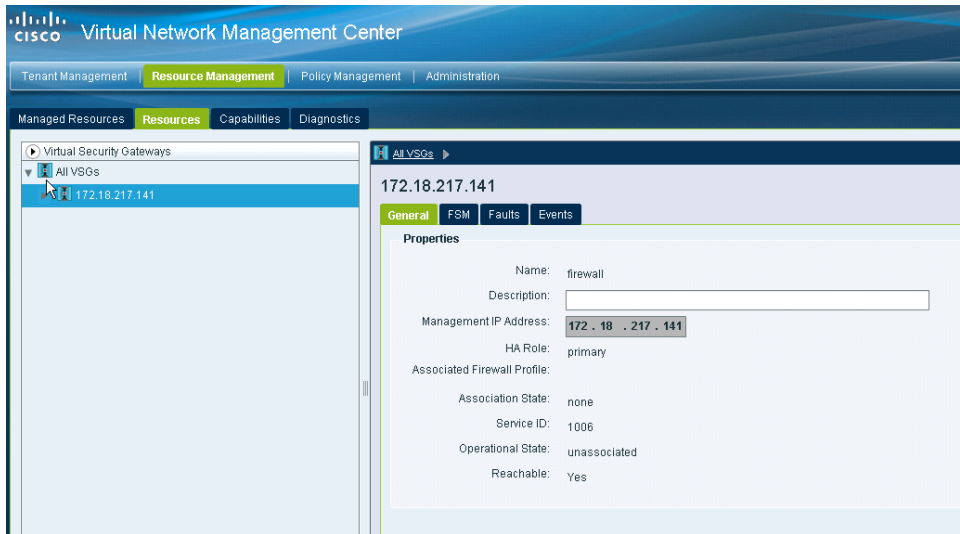
Verify the connectivity from the VSM CLI:

***** Note, it may take up to a minute for the policy agent to authenticate and register to the VNMC *****

```
cae-bl-vsm1# sh vnm-pa status
VNM Policy-Agent status is - Installed Successfully. Version 1.0(0.414)-vsm
```

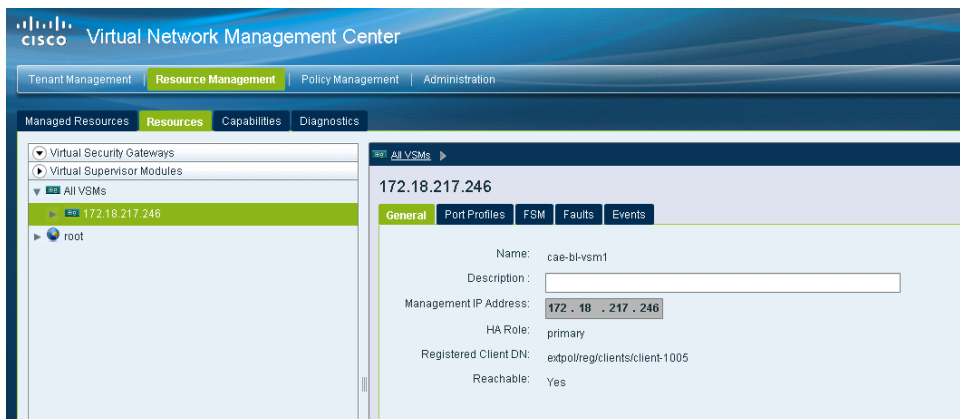
5.2.3 Confirm registration on the VNMC

To confirm from the VNMC GUI that VSG and VSM have successfully registered, log into VNMC as admin, and go to the Resource Management->Resources tab, select Virtual Services Gateways and verify that the VNMC sees VSG:



The “Operational State” of “Unassociated” is normal at this stage of the setup; this simply means that the VSG hasn’t been pressed into service in a Tenant’s compute firewall.

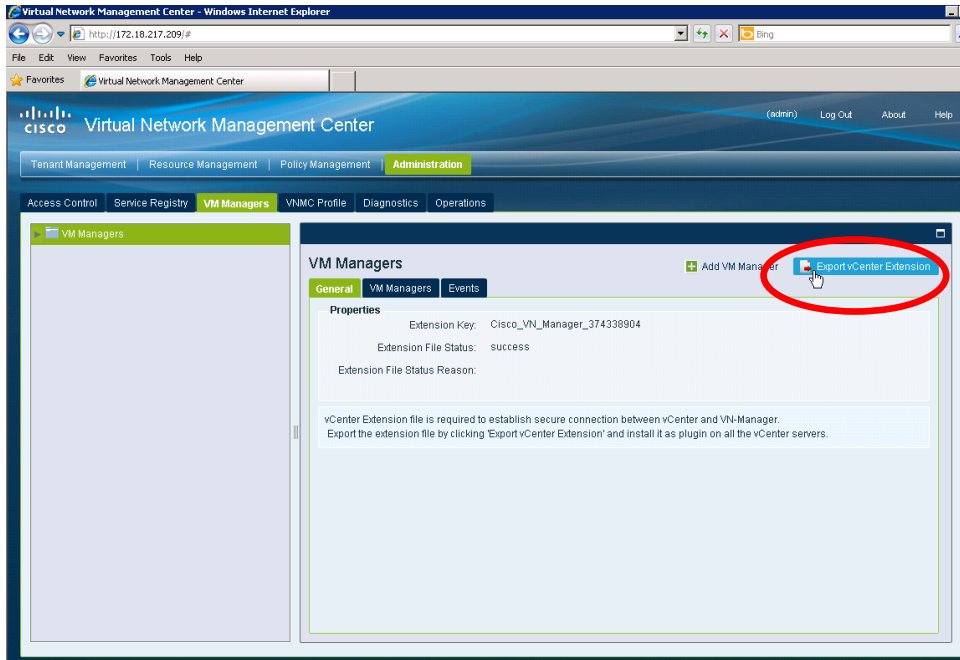
Similarly, Resource Management->Resources tab, select Virtual Supervisor Modules verifies that the VNMC sees VSM:



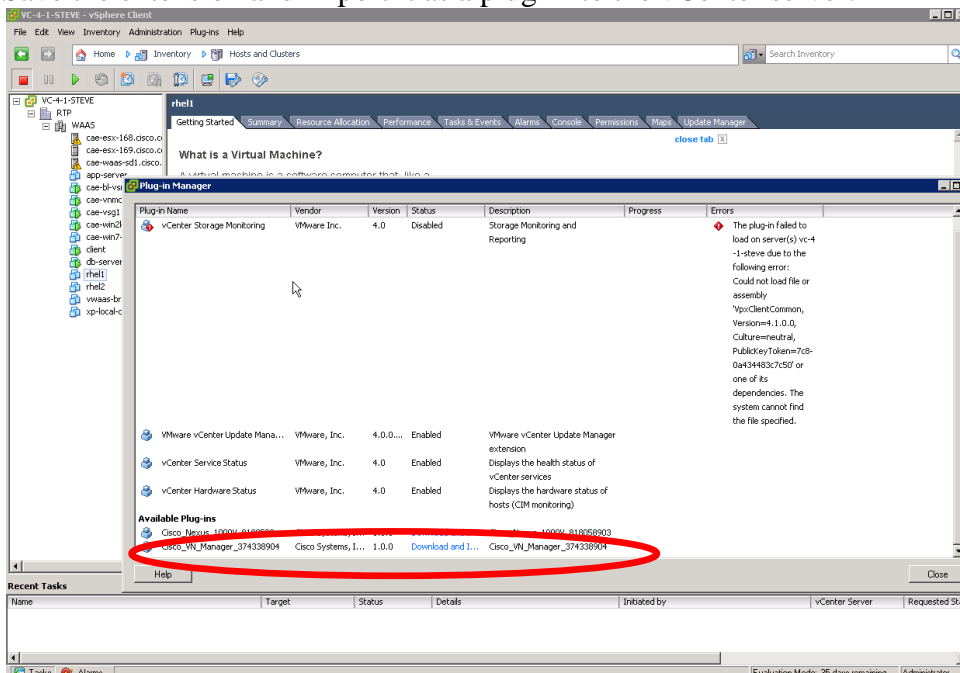
5.3 Register VNMC with vCenter

Certain vCenter information (such as VM profile properties) can be used as discriminators in VSG policies. VNMC needs to register with vCenter to retrieve this info.

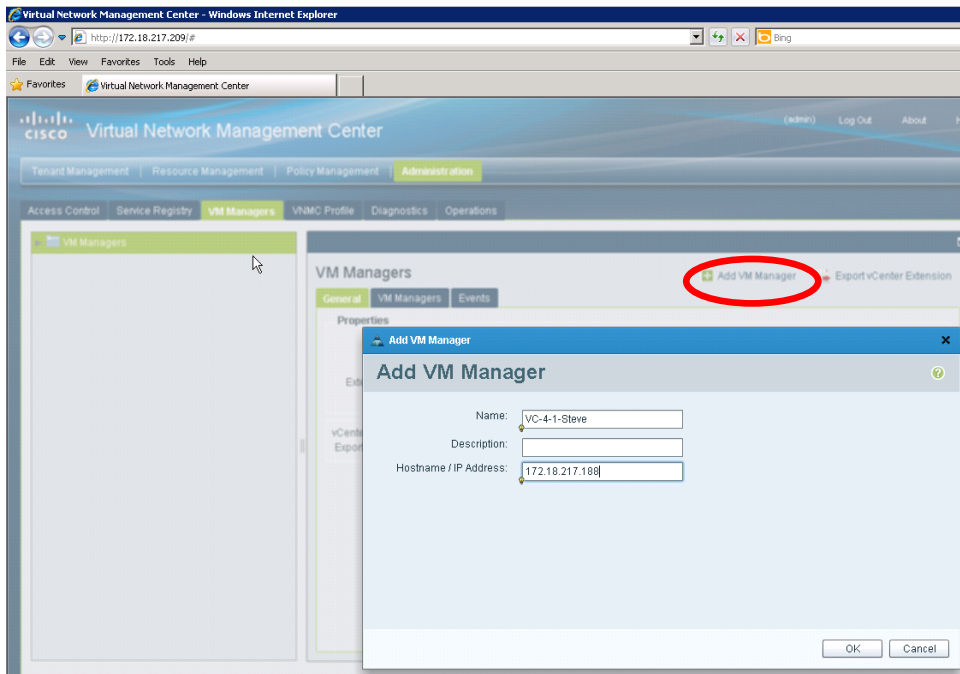
Select Administration->VM Managers tab and “Export vCenter Extension”:



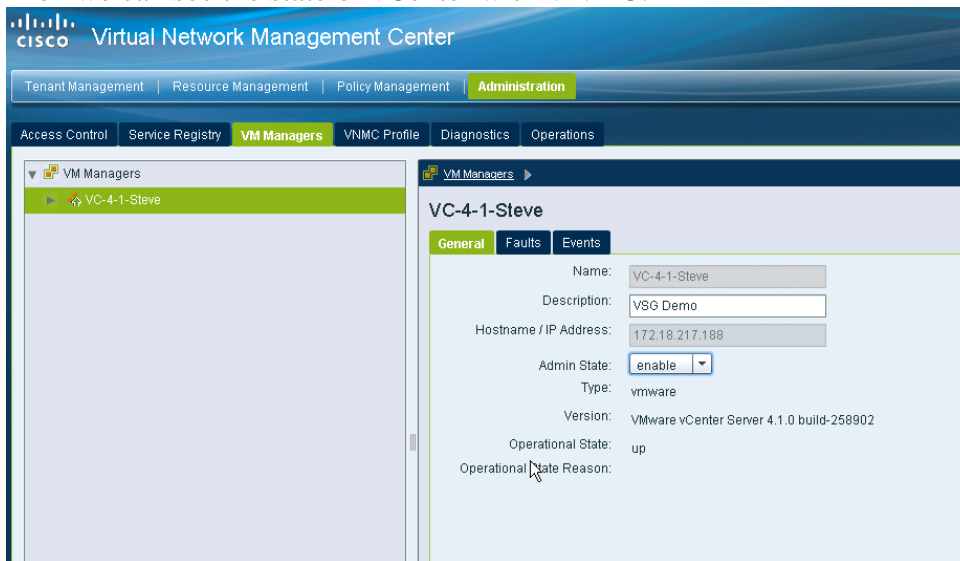
Save the extension and import it as a plug-in to the vCenter server:



Next, let the VNMC know about vCenter. Select VM Managers and “+ Add VM Manager” button:



Then we can see the state of vCenter with VNMC:

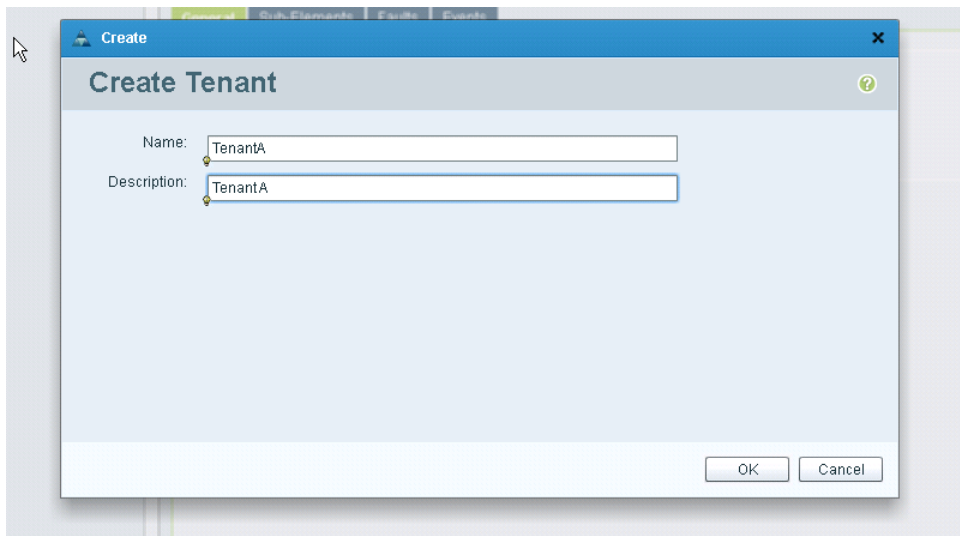


5.4 Assign VSG to a Tenant

VNMC Firewall provides for firewall policy applications based on a tenant concept. There may be multiple tenants (companies, business units, etc.); each requiring their own unique traffic blocking. (For example, TenantA would require a separate firewall from TenantB.)

5.4.1 Create Tenant

Select “Tenant Management” tab and add tenant (this organizational unit will be used to as a hierarchy discriminator for applied policy searches)



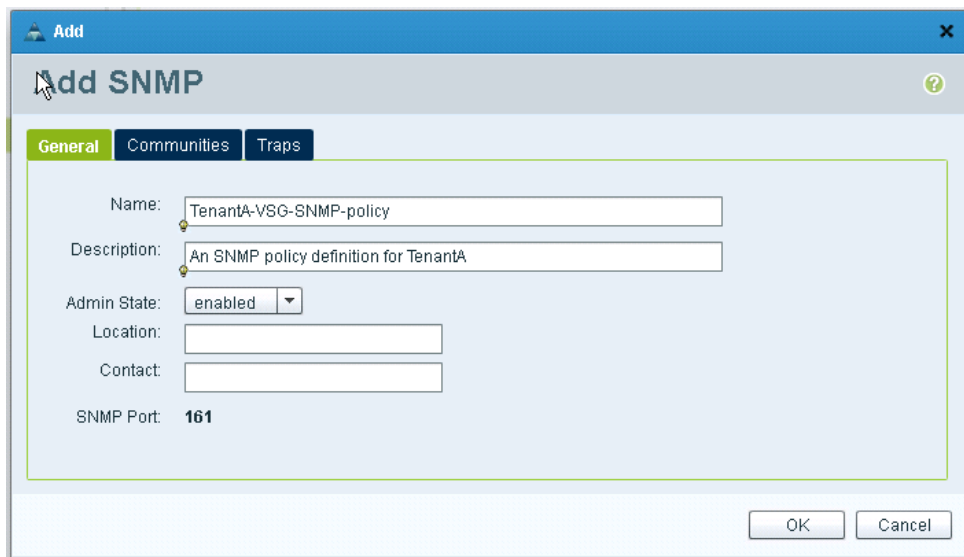
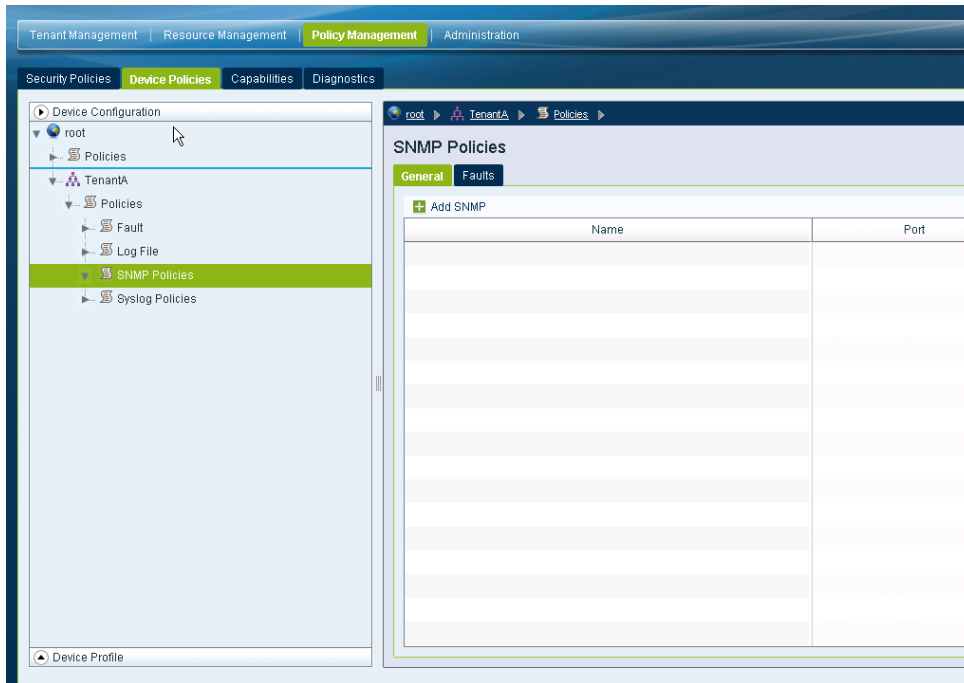
The screenshot shows a 'Create Tenant' dialog box. The title bar includes a user icon, the word 'Create', and a close button (X). The dialog title is 'Create Tenant'. There are two input fields: 'Name:' containing 'TenantA' and 'Description:' containing 'TenantA'. At the bottom right, there are 'OK' and 'Cancel' buttons. A mouse cursor is visible on the left side of the dialog.

5.4.2 Define the Tenant’s VSG system parameters

5.4.2.1 Define VSG device policies

Select “Policy Management -> Device Policies” tab

Select the “Device Configuration” pull down and select the Syslog and SNMP VSG device policies that we want to assign to “TenantA”:



Add a community string

Perform similar sequence for TenantA's Syslog policy:

Tenant Management | Resource Management | **Policy Management** | Administration

Security Policies | **Device Policies** | Capabilities | Diagnostics

Device Configuration

- root
 - Policies
 - TenantA
 - Policies
 - Fault
 - Log File
 - SNMP Policies
 - TenantA-VSG-SNMP-policy
 - Syslog Policies**

root > TenantA > Policies > Syslog Policies

Syslog Policies

General | Faults

+ Add Syslog

Name	Port

Security Policies | **Device Policies** | Capabilities | Diagnostics

Device Configuration

- root
 - Policies
 - TenantA
 - Policies
 - Fault
 - Log File
 - SNMP Policies
 - TenantA-VSG-SNMP-policy
 - Syslog Policies**

root > TenantA > Policies > Syslog Policies

Syslog Policies

General | Faults

Add Syslog

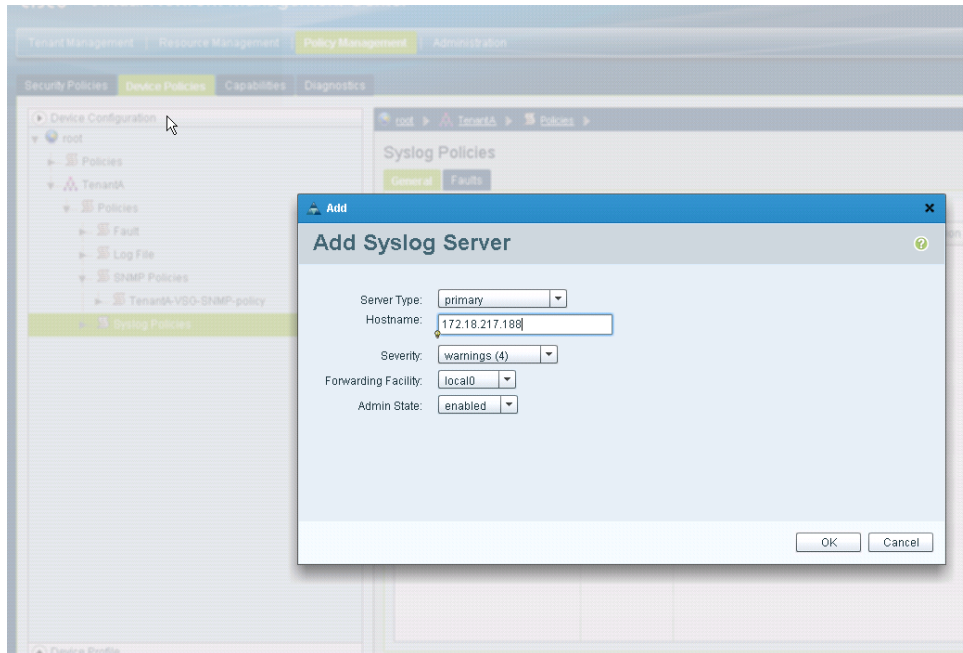
General | Servers | Local Destinations

Name: TenantA-Syslog_policy

Description: Syslog policy for TenantA

Port: 514

OK Cancel

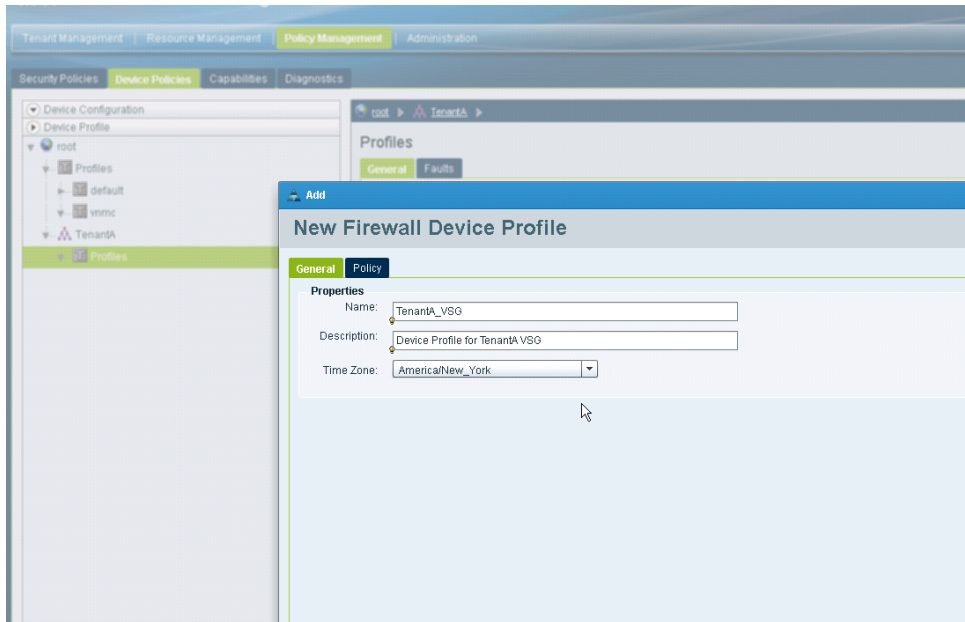
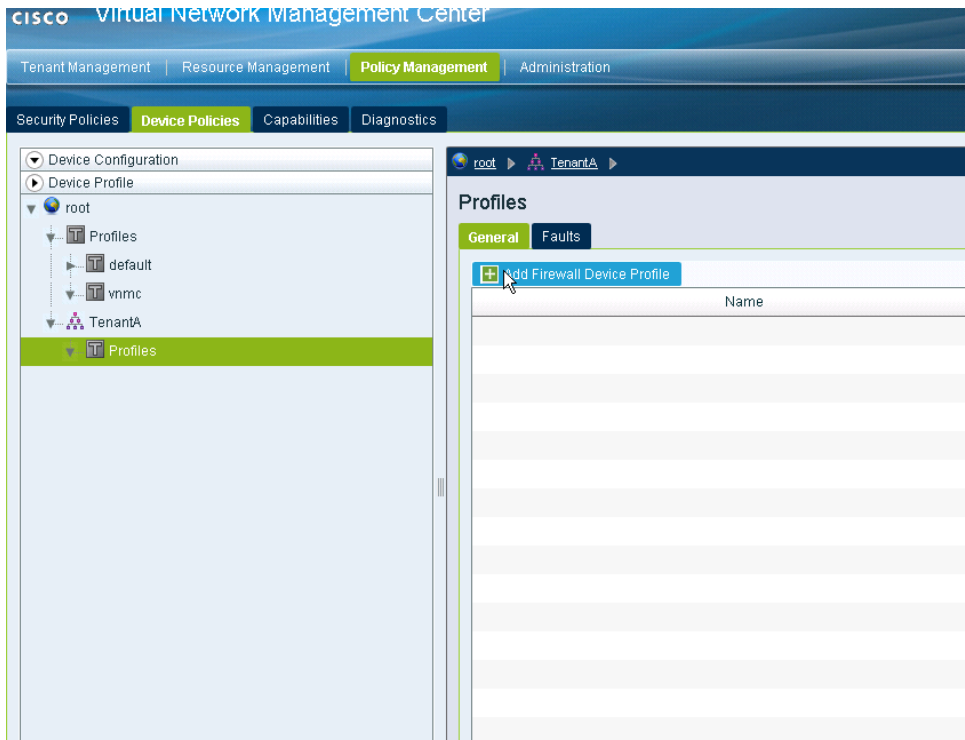


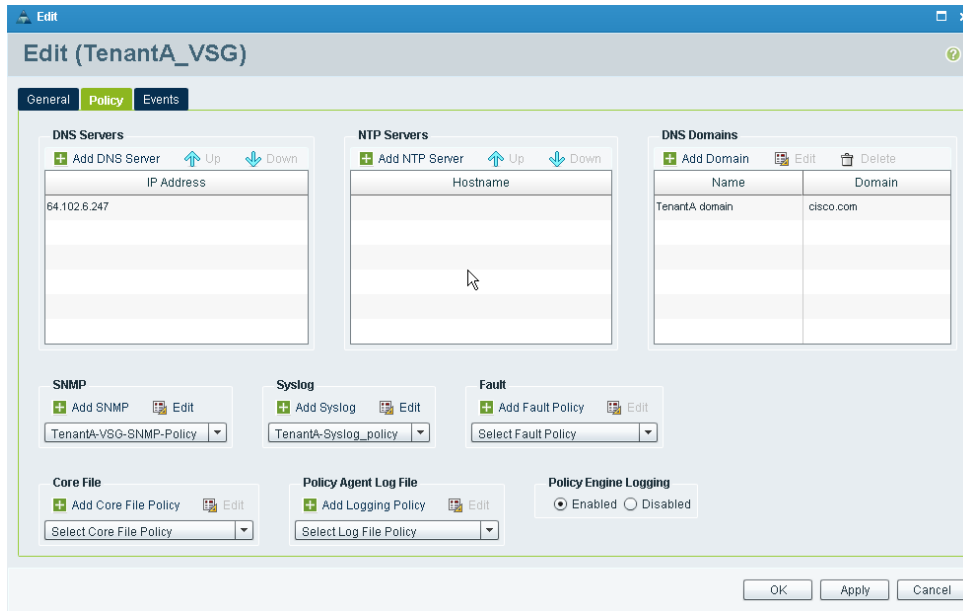
Note that we created one policy each for SNMP and syslog, respectively...multiple policies could have been defined for this tenant for later assignment to the VSG device profile (for example, a lab SNMP policy for testing purposes, then a production policy for final rollout)

5.4.2.2 Create a device profile to assign to the tenant's VSG

Select "Policy Management -> Device Policies" tab

Select the "Device Profile" pull down and select the tenant that we want to Add a profile for:





Note, as indicated in the previous test case, we could have created multiple profiles for this tenant (profile for lab, profile for production, etc.)

5.5 Create a compute firewall

The “compute firewall” is, for all intents and purposes, the VSG. When the “compute firewall” is assigned a VSG (either a single VSG, as in this case, or from a pool of VSG’s), that VSG inherits the configuration that is defined for the “compute firewall”.

Select “Resource Management -> Managed Resources” tab
Select the “Virtual Service Gateways” pull down and select the tenant that we want to Add a firewall for (in this case, we currently only have the one tenant, TenantA):

CISCO Virtual Network Management Center

Tenant Management | **Resource Management** | Policy Management | Administration

Managed Resources | Resources | Capabilities | Diagnostics

Virtual Security Gateways

- root
 - Firewall Profiles
 - Pools
 - TenantA
 - Firewall Profiles**
 - Pools

root > TenantA > Firewall Profiles

Firewall Profiles

General | Faults

+ Add Compute Firewall

Name	Description

Create Add Compute Firewall

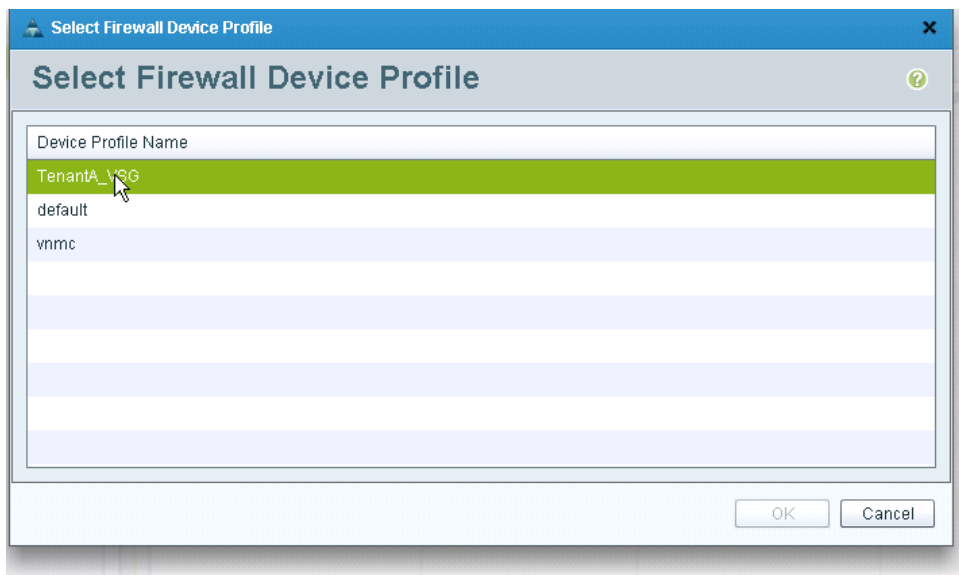
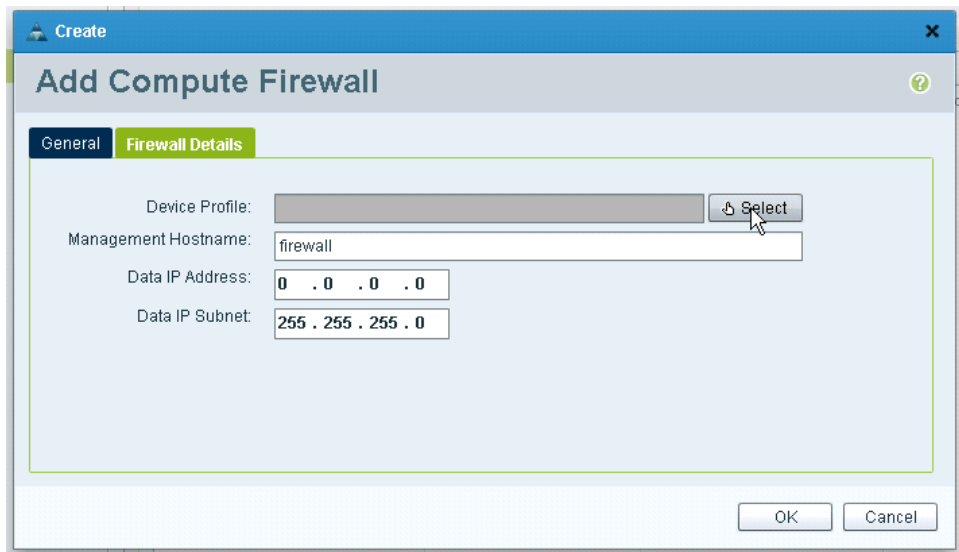
General | Firewall Details

Name:

Description:

Config State: not-applied

OK Cancel



Note that the device profile that was created previously was selected.

The "Data IP" address does not have to be a routable address. "Data0 IP" is needed so that the VEM can arp on its L2 interface and learn the MAC address of the VSG. (In future VSG releases, should L3 connectivity to the VEM be supported, the Data IP address may need to be a routable IP; until then, the data IP can be an arbitrary, non-conflicting address on the VSG's service-vlan.)

Create Add Compute Firewall

General **Firewall Details**

Device Profile: TenantA_VSG

Management Hostname: firewall

Data IP Address: 10 . 10 . 10 . 10

Data IP Subnet: 255 . 255 . 255 . 0

Now, assign a VSG to this tenant's firewall profile:

Tenant Management | **Resource Management** | Policy Management | Administration

Managed Resources | Resources | Capabilities | Diagnostics

Virtual Security Gateways

- root
 - Firewall Profiles
 - Pools
 - TenantA
 - Firewall Profiles
 - TenantA-firewall**
 - Pools

root > TenantA > Firewall Profiles > **TenantA-firewall**

General | Firewall Details | Faults | Events

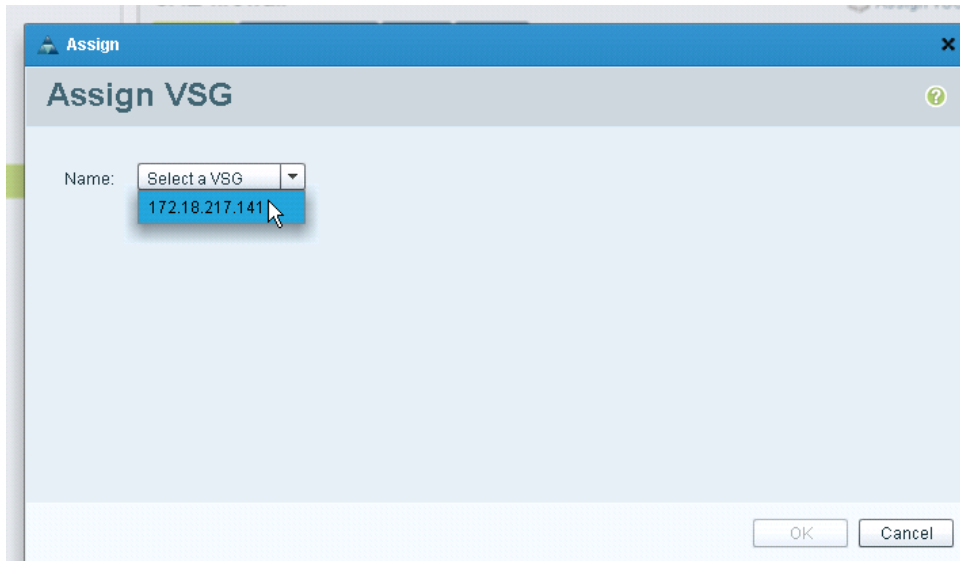
Name: TenantA-firewall

Description: Firewall for TenantA

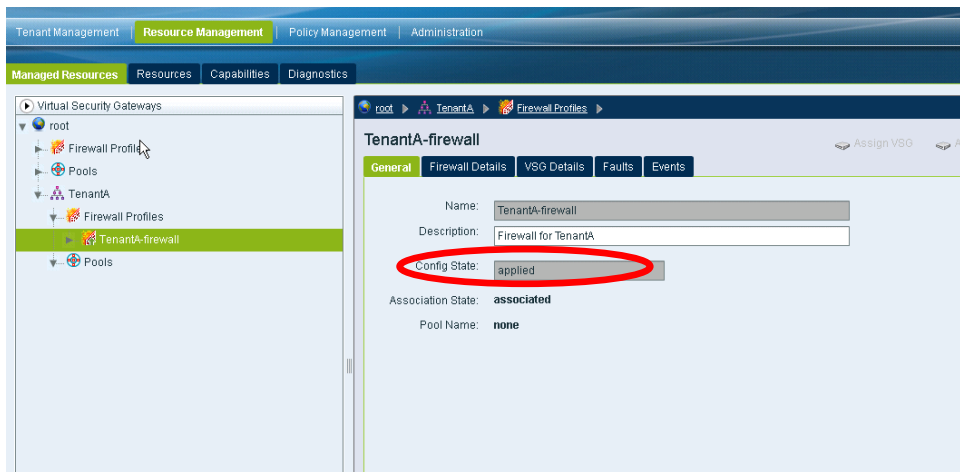
Binding State: **not-applied**

Association State: **unassociated**

Pool Name: **none**



Note that the config state will move from “applying” to “applied” once the configuration has been downloaded to the VSG.



Also note that the device profile policy information that was entered in the test cases above, shows up in the “sh run” output on the VSG (**highlighted** below...items in **bold red** are discussed in related white papers; however, note that the default top-level root level policy is to drop all packets; this means that any applied security profile with no policy set applied will default to deny all):

```
cae-vsg1# sh run

!Command: show running-config
!Time: Sat Nov 6 12:34:00 2010
```

```

version 4.2(1)VSG1(1)

vrf context management
  ip domain-name cisco.com
  ip name-server 172.18.217.235
  ip route 0.0.0.0/0 172.18.217.1
vlan 1

interface data0
  ip address 10.10.10.10/24

security-profile default@root
  policy default@root
  custom-attribute vnsporg "root"
rule default/default-rule@root
  action 10 drop
policy default@root
  rule default/default-rule@root order 2
service firewall logging enable
vnm-policy-agent
  policy-agent-image //bootflash/nexus-1000v-pa-mzg.VSG1.0.439.bin
  registration-ip 172.18.217.209
  shared-secret *****
  log-level info
logging server 172.18.217.188 6 facility local0

```

6 Summary

- Some VSM prep work is required (create 2 port-profiles: one VLAN to support VSG L2 control information to the VEM, and one VLAN to support VSG HA traffic)
- VSG VM is installed using either OVA or ISO
- VNMC OVA is installed
- VSG and VSM register to VNMC
- VNMC registers with VMware to receive vCenter VM property information
- VSG parameters get defined (syslog server, DNS, SNMP, etc.)
- Tenant Compute Firewall is created
- VSG gets assigned to the Tenant's compute firewall