CHAPTER 5

FAQs About the ASA 1000V

This document provides answers to the most frequently asked questions (FAQs) related to the ASA 1000V solution and deployment.

- Can two ASA 1000Vs have the same IP addresses if they belong to the same tenant hierarchy?
- What is the expected behavior if multiple VMs in the same tenant/datacenter/vApp/tier have the same IP address?
- In the Cisco Nexus 1000V, do you configure vservice node, security profile, or org configuration for the inside interface of the ASA 1000V?
- When I configure Cisco VNMC policy agent parameters on the ASA 1000V, what CLI output can I expect to see?
- Can I connect the ASA 1000V to the Cisco VNMC with the management interface only, or can I use the inside interface or outside interface as well?
- Should Cisco VNMC be directly connected to the ASA 1000V management interface?
- Can you use the ASA 1000V CLI to change the ASA 1000V management mode from ASDM to VNMC or from VNMC to ASDM after deploying the ASA 1000V?
- Do I need to install a license file on ASA 1000V for it to work?
- I have an ASA 1000V deployed in VNMC mode and have policies created in the VNMC Security Profiles section, but I do not see the policies getting applied on the ASA 1000V.
- Can I have some VM hosts on the inside network that are assigned dynamic IP addresses via DHCP and some that are assigned static IP addresses?

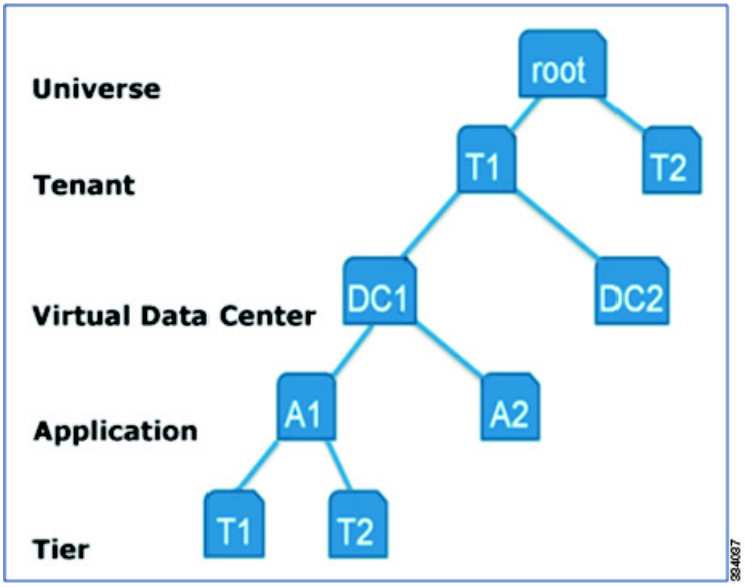
- Why does packet tracer/capture show security profile information for packets coming from VM hosts on the inside network?
- When I ping from an inside VM host to the ASA 1000V inside IP address and capture packets, I see only ICMP echo request packets.
- The VM hosts on my inside network have two interfaces (virtual NICs). Can each of these interfaces belong to a different tenant?
- Because the ASA 1000V has inside and outside interfaces (except management and failover), can the inside interface serve as trunk interfaces to serve multiple VLANs in the tenant?
- In Cisco VNMC, when I delete the edge security profile associated with my VM hosts, can I recreate it using the same name?
- After entering the no vnmc org org_name command in ASDM mode, can I recreate the same organization structure using the same security profile names for all security profile interfaces?
- My ASA 1000V is deployed in VNMC Mode. I mistakenly deleted the ASA 1000V edge firewall in Cisco VNMC. What do I do?
- My ASA 1000V is deployed in ASDM Mode. I mistakenly deleted the ASA 1000V edge firewall in Cisco VNMC. What do I do?
- In Cisco VNMC, do I have to configure both an edge security profile and an edge device profile to configure VPN on ASA 1000V?

For information about troubleshooting your ASA 1000V deployment, see the *Cisco ASA 1000V Troubleshooting Guide* at ASA 1000 Documentation.

Questions

Q. Can two ASA 1000Vs have the same IP addresses if they belong to the same tenant hierarchy?

A. No. Any ASA 1000Vs deployed in the same hierarchy cannot have the same IP address. The following diagram shows a hierarchy that consists of the levels root – T1 – DC1 – A1 – T1. An ASA 1000V in tenant T1 and an ASA 1000V in vApp A1 cannot have the same IP addresses. However, an ASA 1000V deployed in Tenant T1 and an ASA 1000V deployed in Tenant T2 can have the same IP addresses.



Q. What is the expected behavior if multiple VMs in the same tenant/datacenter/vApp/tier have the same IP address?

A. Currently, if multiple VMs in the same tenant/datacenter/vApp/tier have the same IP address, traffic will not pass through the ASA 1000V. Avoid configuring the ASA 1000V in this way, because changing the IP address will not fix the issue.

Q. In the Cisco Nexus 1000V, do you configure vservice node, security profile, or org configuration for the inside interface of the ASA 1000V?

A. No. For the ASA 1000V port profile, you do not need to configure a vservice node, security profile, or an org configuration for the ASA 1000V inside interface.

Q. When I configure Cisco VNMC policy agent parameters on the ASA 1000V, what CLI output can I expect to see?

A. With the current ASA 1000V image, you will see the following type of output on the console when you configure VNMC policy-agent parameters:

```
ciscoasa# config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
ciscoasa(config)# vnmc policy-agent
ciscoasa(config-vnmc-policy-agent)# registration host 172.23.195.171
ciscoasa(config-vnmc-policy-agent)# shared-secret Vnmcpass1

Trustpoint CA certificate accepted.
ciscoasa(config-vnmc-policy-agent)#
```

Q. Can I connect the ASA 1000V to the Cisco VNMC with the management interface only, or can I use the inside interface or outside interface as well?

A. No. You can only connect the ASA 1000V to the Cisco VNMC using the management interface.

Q. Should Cisco VNMC be directly connected to the ASA 1000V management interface?

A. No. You are not required to directly connect the Cisco VNMC to the ASA 1000V management interface. Typically, a host-specific route should be added on the ASA 1000V to reach the Cisco VNMC through the management interface because the ASA 1000V default gateway is reached through the ASA 1000V outside interface.

Q. Can you use the ASA 1000V CLI to change the ASA 1000V management mode from ASDM to VNMC or from VNMC to ASDM after deploying the ASA 1000V?

A. No. You cannot change the management mode after deploying the ASA 1000V. To change the management mode, you must redeploy the ASA 1000V. When you redeploy the ASA 1000V, you must reconfigure all policies that you previously configured for the ASA 1000V.

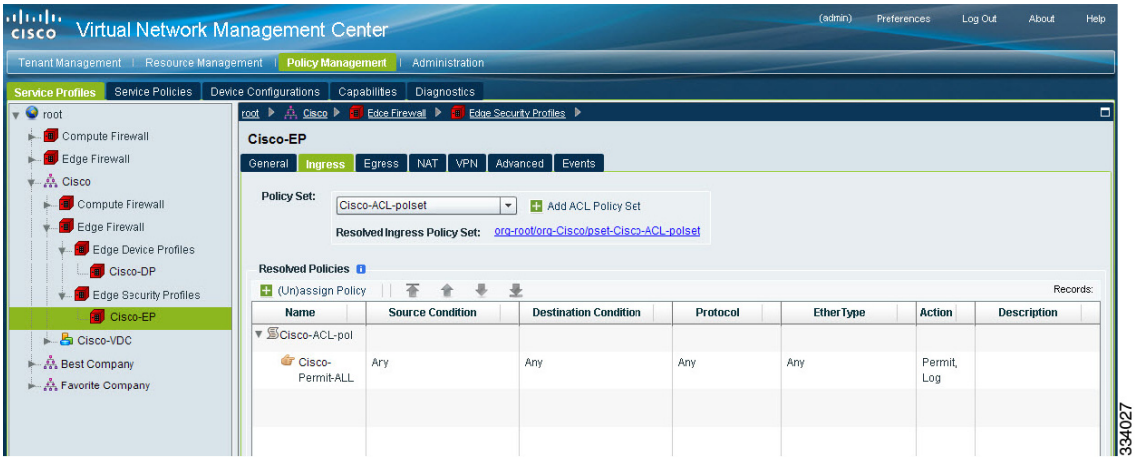
Q. Do I need to install a license file on ASA 1000V for it to work?

A. No. Unlike traditional ASAs, you do not need to install a license file on the ASA 1000V. However, you need to install a license file on the Cisco Nexus 1000V for the ASA 1000V. Cisco will provide you with the appropriate license file to install on the Cisco Nexus 1000V.

Q. I have an ASA 1000V deployed in VNMC mode and have policies created in the VNMC Security Profiles section, but I do not see the policies getting applied on the ASA 1000V.

A. When the ASA 1000V is configured to use VNMC mode, each policy that is applied on the ASA 1000V needs to be a part of a policy set and the policy set must be assigned to an edge security profile for the policies to be applied on the Cisco Nexus 1000V.

The following screen shows how to define policies and policy sets in Cisco VNMC.



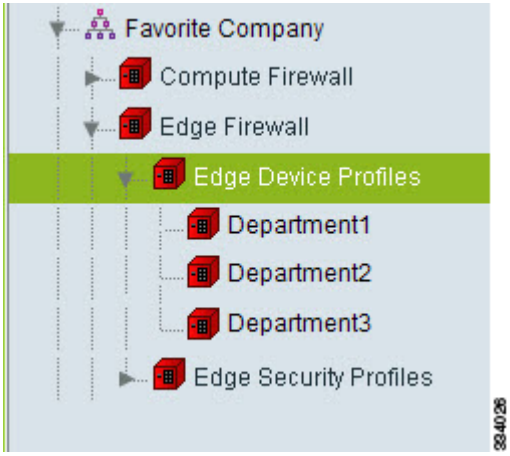
Q. Can I have some VM hosts on the inside network that are assigned dynamic IP addresses via DHCP and some that are assigned static IP addresses?

A. The VM hosts that have static IP addresses are not reachable by outside hosts. Any VM host that is assigned a dynamic IP address via DHCP will always be reachable from outside hosts.

However, an outside host will be able to reach an inside host that has a static IP address when the inside host has communicated with the outside host (for example, using ping or ARP).

Q. Why does packet tracer/capture show security profile information for packets coming from VM hosts on the inside network?

A. As shown in the following screen, all the VM hosts that are on the inside network belong to an edge security profile and each edge security profile has specific policies defined.



The Cisco organization has three edge security profiles for Department1, Department2, and Department3. The VM hosts belonging to each department have separate policies defined for them.

To ensure that the correct policies are applied to the traffic from VM hosts in Department1, Department2 and Department3, the ASA 1000V needs to identify the edge security profile to which the VM host belongs.

Tagging packets with security profile information allows the ASA 1000V to identify the edge security profile that a VM host belongs to and apply the policies associated with that edge security profile.

Q. When I ping from an inside VM host to the ASA 1000V inside IP address and capture packets, I see only ICMP echo request packets.

A. With the current ASA 1000V version, only ICMP echo request packets are displayed in capture outputs for traffic from inside VM hosts to the ASA 1000V inside interface IP address. This is a display issue, and the inside VM host should receive the ICMP echo reply packets from the ASA 1000V inside interface.

When an inside host is pinged from the ASA 1000V interface and packets captured, both ICMP echo request and reply packets are displayed correctly. This issue does not affect the traffic sent from inside VM hosts to outside hosts.

Q. The VM hosts on my inside network have two interfaces (virtual NICs). Can each of these interfaces belong to a different tenant?

A. No. All the interfaces of a VM host should belong to the same tenant.

Q. Because the ASA 1000V has inside and outside interfaces (except management and failover), can the inside interface serve as trunk interfaces to serve multiple VLANs in the tenant?

A. No. The ASA 1000V only supports one inside subnet. It does not support VLAN trunk ports.

Q. In Cisco VNMC, when I delete the edge security profile associated with my VM hosts, can I recreate it using the same name?

A. No. Deleting and recreating the edge security profile using the same name causes your inside VM hosts to be unreachable. When you delete the edge security profile and recreate it with same name in the same tenant/datacenter/app/tier, the ASA 1000V will drop all packets from that edge security profile after it is recreated.

To resolve this issue, perform one of the following workarounds:

Workaround 1

1. From VMWare vCenter, determine the port profile to which the VM hosts belong. (In the following example, the VM hosts belong to the port profile inside-hosts-1.)
2. On the Cisco Nexus 1000V console, enter the following commands:

```
Nexus1000v# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Nexus1000v(config)# port-profile type vethernet inside-hosts-1
Nexus1000v(config-port-prof)# no vservice node name profile profile_name
Nexus1000v(config-port-prof)# vservice node name profile profile_name
```

Workaround 2

1. Save the running-config to the startup-config using the **copy running-config startup-config** command.
2. Reload the Nexus 1000V switch using the **reload** command.

Q. After entering the **no vnmc org** *org_name* command in ASDM mode, can I recreate the same organization structure using the same security profile names for all security profile interfaces?

A. No. If you configured the security profiles and VNMC organization structure, then entered the **no vnmc org** *org_name* command, you cannot recreate the same organization structure using the same security profile names for all security profile interfaces.

The ASA 1000V will drop packets from inside hosts belonging to all edge security profiles in the organization structure, even if you recreate the organization correctly.

To resolve this issue, perform one of the following workarounds:

Workaround 1

1. Save the running-config to the startup-config using the **copy running-config startup-config** command.
2. Reload the Nexus 1000V switch using the **reload** command.

Workaround 2

1. From VMWare vCenter, determine the port profile for all affected VM hosts.
2. For each port profile, enter the following commands on the Cisco Nexus 1000V VSM console:

```
Nexus1000v# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Nexus1000v(config)# port-profile type vethernet port-profile_name
Nexus1000v(config-port-prof)# no vservice node name profile profile_name
Nexus1000v(config-port-prof)# vservice node name profile profile_name
```

Enter these commands for the port profile for all the inside VM hosts.

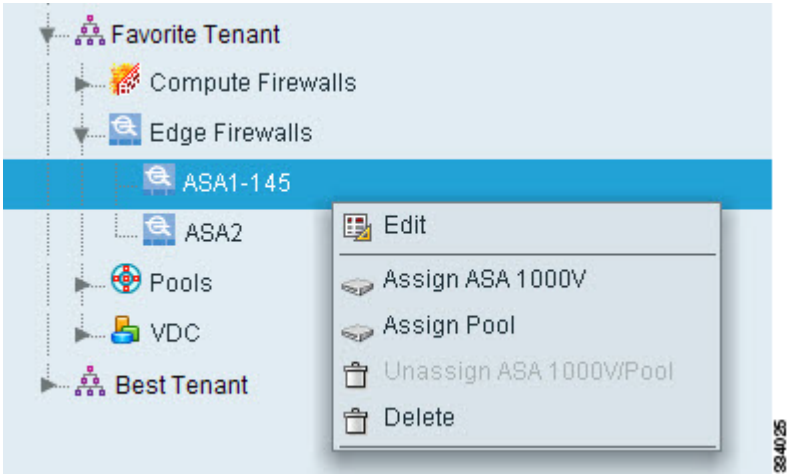
Q. My ASA 1000V is deployed in VNMC Mode. I mistakenly deleted the ASA 1000V edge firewall in Cisco VNMC. What do I do?

A. When you mistakenly delete the edge firewall for the ASA 1000V, perform the following steps in Cisco VNMC:

1. From the Edge Firewalls section, create a new edge firewall with the same parameters as the one you deleted. See the Cisco VNMC Help for more information.

Note You do not need to recreate the edge security profiles in Cisco VNMC.

2. Select the edge firewall that you recreated and choose **Assign Virtual-ASA**.



3. Verify that the configuration state shows applied:

Q. My ASA 1000V is deployed in ASDM Mode. I mistakenly deleted the ASA 1000V edge firewall in Cisco VNMC. What do I do?

A. If you mistakenly deleted the edge firewall for the ASA 1000V, perform the following steps:

1. If you have enabled SSH/Telnet on the ASA 1000V, connect to the CLI using SSH or Telnet.

   or

   Log into VMware vCenter Client and navigate to the console for the ASA 1000V VM.

2. Enter the **vnmc org** command; for example:

   vnmc org root/Tenant2

   Entering this command recreates the edge firewall in Cisco VNMC.

Q. In Cisco VNMC, do I have to configure both an edge security profile and an edge device profile to configure VPN on ASA 1000V?

A. Yes. In Cisco VNMC, the VPN configuration is divided into two sections:

- Global or device configuration (IKE configuration and tunnel group peer configuration are considered global). Global or device configuration must be configured under Edge Device Profile.
- Interface configuration (crypto map configuration is considered an interface configuration). Interface configuration must be configured under Edge Security Profile.