Cisco ASA 1000V Troubleshooting Guide, Release 8.7(1)

August 31, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: N/A, Online only

Cisco ASA 1000V Troubleshooting Guide, Release 8.7(1)

CONTENTS

Preface

The *Cisco ASA 1000V Troubleshooting Guide* provides information about how to recognize a problem, determine its cause, and find possible solutions.

This preface includes the following sections:

Audience

This publication is for experienced network and security administrators who configure and maintain a Cisco ASA 1000V.

Document Organization

This document is organized into the following chapters:

Title	Description
Chapter 1, "Overview of Troubleshooting"	Describes basic troubleshooting information, the available troubleshooting tools, and the steps to take before requesting technical support.
Chapter 2, "Validating the ASA 1000V Configuration"	Describes how to validate your system configuration.
Chapter 3, "Case Studies in Traffic Failure"	Describes case studies in troubleshooting traffic failures.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use these conventions:

`courier` font	Terminal sessions and information that the switch displays are in `courier` font.
`boldface courier` font	Information that you must enter is in **`boldface courier`** font.
`italic courier` font	Arguments for which you supply values are in *`italic courier`* font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Related Documentation

For more information about the individual components that comprise the ASA 1000V, see the following documentation:

- VMware
  http://www.vmware.com/support/pubs/
- Cisco Nexus 1000V
  http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
- Cisco Virtual Network Management Center (VNMC)
  http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html
- ASA 1000V
  http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

- ASDM
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- (Optional) Cisco Virtual Security Gateway (VSG), Version 1.4

  http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Overview of Troubleshooting

This chapter introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when configuring and using the ASA 1000V.

This chapter includes the following sections:

Overview of the Troubleshooting Process

To troubleshoot your configuration, perform the following steps:

Step 1 Collect information that defines the specific symptoms.

Step 2 Identify all potential problems that could be causing the symptoms.

Step 3 Eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Overview of Best Practices

Best practices are the recommended steps that you should take to ensure the correct operation of your configuration. We recommend the following general best practices:

- See the ASA 1000V release notes, VNMC 2.0 release notes, and Nexus 1000V release notes for the latest features, guidelines, limitations, and caveats.
- Enable system message logging. See the "Overview of Symptoms" section on page 1-3.
- Verify and troubleshoot any new configuration changes after implementing them.

Troubleshooting Basics

This section introduces questions to ask when troubleshooting a problem with ASA 1000V or associated components. Use the answers to these questions to identify the scope of the problem and to plan a course of action.

This section includes the following topics:

Troubleshooting Guidelines

By answering the questions in the following subsections, you can determine the paths you need to follow and the components that you should investigate further.

Answer the following questions to determine the status of your installation:

- Is this a newly installed system or an existing installation? (It could be a new host, switch, or VLAN).
- Has the host ever been able to see the network?
- Are you trying to solve an existing application problem (too slow, too high latency, excessively long response time) or did the problem show up recently?
- What changed in the configuration or in the overall infrastructure immediately before the applications started to have problems?

To discover a network problem, use the following general network troubleshooting steps:

Step 1 Collect information about problems in your system. See the "Collecting Information" section on page 1-3.

Step 2 Verify the configuration for your storage subsystems and servers.

Collecting Information

This section highlights the tools that are commonly used to troubleshoot problems within your network. These tools are a subset of what you may use to troubleshoot your specific problem.

You should also have an accurate topology of your network to help isolate problem areas.

Enter the following commands and examine the outputs:

- **show vsn**
- **show version**
- **show running-config**
- **show logging**
- **show interfaces brief**
- **show vlan**
- **show tech support vsn**

Overview of Symptoms

The symptom-based troubleshooting approach provides multiple ways to diagnose and resolve problems. By using multiple entry points with links to solutions, this guide best serves users who may have identical problems that are perceived by different indicators. Search this guide in PDF form, use the index, or rely on the symptoms and diagnostics listed in each chapter as entry points to access necessary information in an efficient manner.

Using a given a set of observable symptoms on a network, it is important to be able to diagnose and correct software configuration issues and inoperable hardware components so that the problems are resolved with minimal disruption to the network. Those problems and corrective actions include the following:

- Identify key ASA 1000V troubleshooting tools.
- Obtain packet captures, core dumps, and other diagnostic data for use by the TAC.

System Messages

The system software sends the syslog (system) messages to the console (and, optionally, to a logging server on another system) during operation. Not all messages indicate a problem with your system. Some messages are only informational, while others might help diagnose problems with links, internal hardware, or the system software.

Troubleshooting with Logs

The ASA 1000V generates many types of system messages and sends them to a syslog server. You can view these messages on the console or through the Adaptive Security Device Manager (ASDM) to determine what events may have led up to the current problem condition.

Use the following commands to access and view logs in the ASA 1000V:

- **show logging asdm**—Displays ASDM syslog buffer content.

- **show logging message**—Displays enabled and disabled syslog messages at the non-default level.
- **show logging queue**—Displays the syslog message queue.
- **show logging setting**—Displays the syslog message settings.

Copying Files

You may be required to move files to or from the ASA 1000V. These files may include log, configuration, traceroute, or packet capture files.

The ASA 1000V always acts as a client, so that an FTP/HTTP/TFTP session always originates from the ASA 1000V and either pushes files to an external system or pulls files from an external system.

The **copy** command allows you to copy files between local and remote locations.

The following example shows the options available for the **copy** command:

```
hostname# copy ?

/noconfirm      Copies the file without a confirmation prompt.
/pcap           Copies packets in libpcap format, which can be opened using a standard
                packet analyzer tool such as Wireshark.
running-config  Specifies the running configuration stored in memory.
startup-config  Specifies the startup configuration stored in flash memory.
url             Specifies the source or destination file to be copied.

hostname# copy /pcap ?
/add-spid       Specifies vPath headers included from packets to the exported pcap file.
```

Cisco Support Communities

For additional information, visit one of the following support communities:

- Cisco Support Community for Server Networking
- Cisco Communities: Nexus 1000V
- Cisco Communities: Network Management
- Cisco Communities: Security

Contacting Cisco TAC or VMware Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in this guide, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service provider assist you as quickly as possible:

- Version of the Cisco Nexus 1000V and Cisco VNMC software that you are running
- Version of the ESX or ESXi and vCenter Server software that you are running
- Version of the ASA 1000V software that you are running
- Contact phone number
- Brief description of the problem

- Brief explanation of the steps that you have already taken to isolate and resolve the problem

If you purchased the ASA 1000V and support contract from Cisco, contact the Technical Assistance Center (TAC). Cisco provides L1, L2, and L3 support.

If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco, contact Cisco Technical Support at the following URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtm

If you purchased the ASA 1000V from Cisco and an SNS through VMware, contact VMware for Cisco Nexus 1000V support. VMware provides L1 and L2 support. Cisco provides L3 support.

After you have collected this information, see the "Obtaining Documentation and Submitting a Service Request" section on page -vii.

For more information about the steps to take before calling Technical Support, see the "Collecting Information" section on page 1-3.

Additional References

For more information about the individual components that comprise the ASA 1000V, see the following documentation:

- VMware
  http://www.vmware.com/support/pubs/
- Cisco Nexus 1000V

  http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
- Cisco Virtual Network Management Center (VNMC)

  http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html
- ASA 1000V
  http://www.cisco.com/en/US/products/ps12233/index.html
- ASDM
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- (Optional) Cisco Virtual Security Gateway (VSG), Version 1.4

  http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 2

Validating the ASA 1000V Configuration

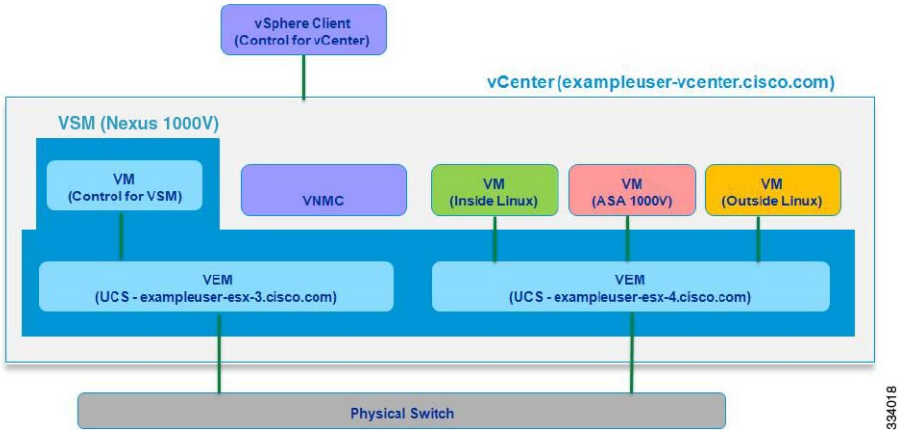
This chapter describes how to validate the ASA 1000V configuration. To make sure that the configuration works correctly, follow the validation procedures listed in the sequence as shown in this chapter. The sample output from certain commands helps indicate whether or not an issue exists.

The chapter includes the following sections:

Topology Used for Troubleshooting

To help isolate problem areas, you should also have an accurate topology of your system configuration. Figure 2-1 shows the topology that provides the basis for the examples and case studies in this guide.

Figure 2-1 Topology Used for Troubleshooting



This system configuration includes the following components:

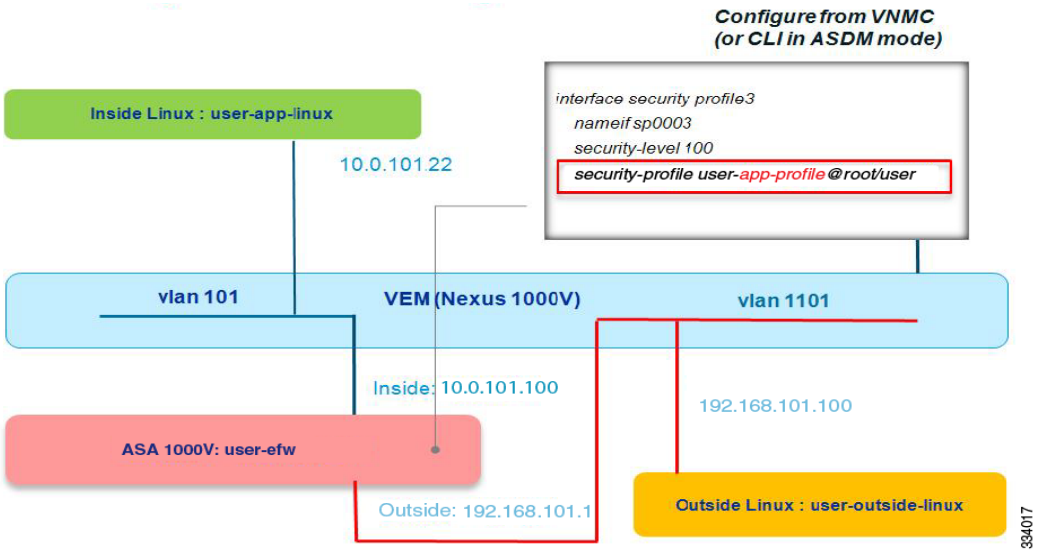
- The Cisco Nexus 1000V switch, the software platform on which the ASA 1000V runs
- The Virtual Services Module (VSM), the control software for the Cisco Nexus 1000V switch
- The Virtual Ethernet Module (VEM), a component of the Cisco Nexus 1000V switch
- The Virtual Network Management Center (VNMC), one of the two available GUI managers
- An inside Linux Virtual Machine (VM)
- The ASA 1000V VM
- The outside Linux VM
- vCenter, the VM manager
- The vSphere client, the vCenter manager
- Two server hosts (for example, UCS) that are connected to a physical switch

Security Profile Configuration in the Cisco VNMC

You need to verify the entire system configuration to make sure that traffic can pass between the inside and outside Linux machines (VMs).

The first step is to validate that a security profile has been created in the Cisco VNMC and was pushed to the ASA 1000V. Figure 2-2 shows the topology for a security profile configuration in the Cisco VNMC.

Figure 2-2 Security Profile Configuration in the Cisco VNMC



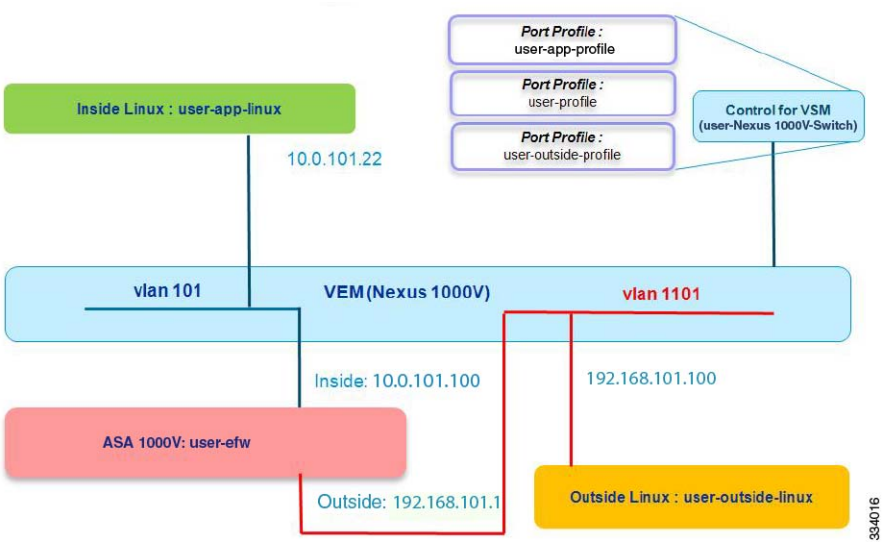
Make sure that you have configured a security profile from the Cisco VNMC or from the ASA 1000V CLI if you are using the ASDM mode. This configuration shows the following:

- The inside VM and the inside ASA 1000V connect to the same VLAN (101).
- The outside VM and the outside ASA 1000V connect to the same VLAN (1101).

Port Profile Configuration in the VSM

The next step is to validate that the port profile has been correctly configured in the VSM. Figure 2-3 shows the topology for a valid port profile configuration in the VSM.

Figure 2-3 Port Profile Configuration in the VSM

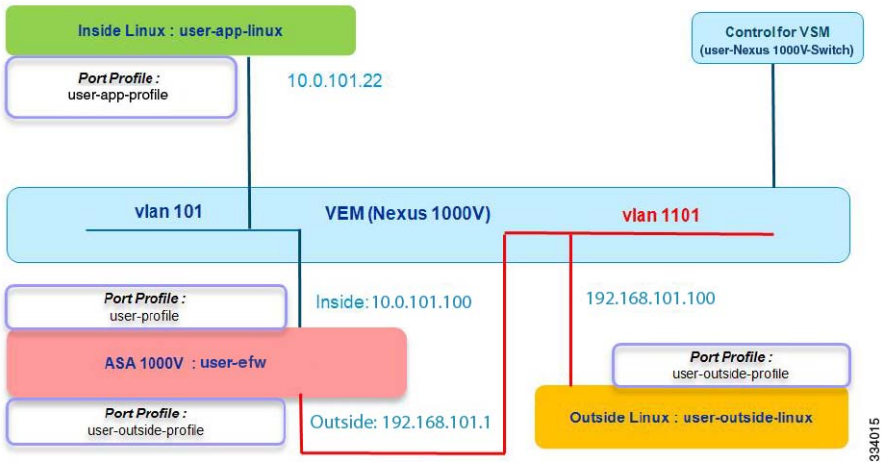


Make sure that you have configured three port profiles through the VSM console: one for the inside Linux VM (user-app-profile), one for the inside ASA 1000V interface and VMs (user-profile), and one for the outside ASA 1000V interface (user-outside-profile).

Port Profile Assignment from vCenter to the VMs

The next step is to validate that port profiles were correctly assigned from vCenter to the VMs. Figure 2-4 shows the topology for a valid port profile assignment from vCenter to the VMs.

Figure 2-4 Port Profile Assignment from vCenter to the VMs



Make sure that you have completed the following tasks in this step:

- Assigned the first port profile (user-app-profile) to the inside Linux VM and specified that this port profile (user-app-profile) has the vservice configuration.
- Assigned the second port profile (user-profile) to the inside ASA 1000V interface and specified that this port profile (user-profile) does *not* have the vservice configuration.
- Assigned the third port profile (user-outside-profile) to the outside ASA 1000V interface and outside Linux VM, and specified that this port profile (user-outside-profile) does *not* have the vservice configuration.

Binding of the Organization Path, ASA 1000V, and Security Profile to the Port Profile in the VSM

The next step is to validate that the binding of the organization (org) path (root/user), ASA 1000V (vservice node vASA-user), and security profile (user-app-profile) to the port profile in the VSM was completed correctly. Figure 2-5 shows the topology for correctly binding the organization path, ASA 1000V, and security profile to the port profile in the VSM.

Figure 2-5 Binding of the Org Path, ASA 1000V, and Security Profile to the Port Profile in the VSM

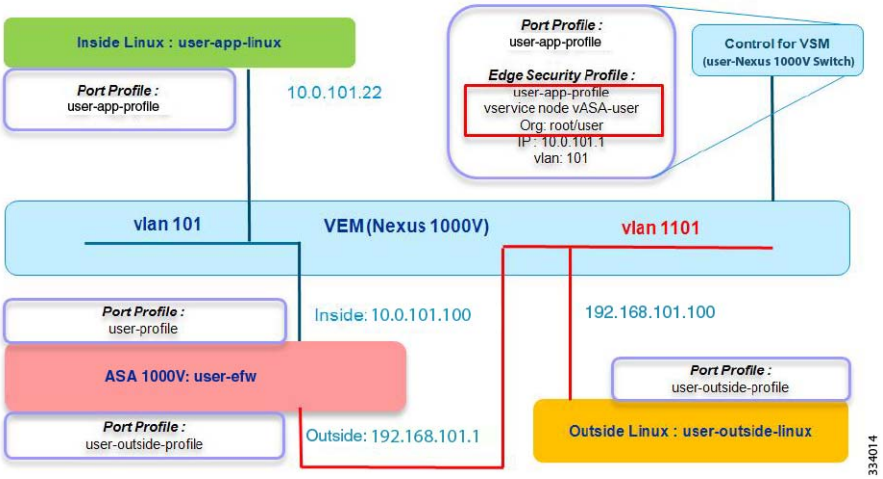
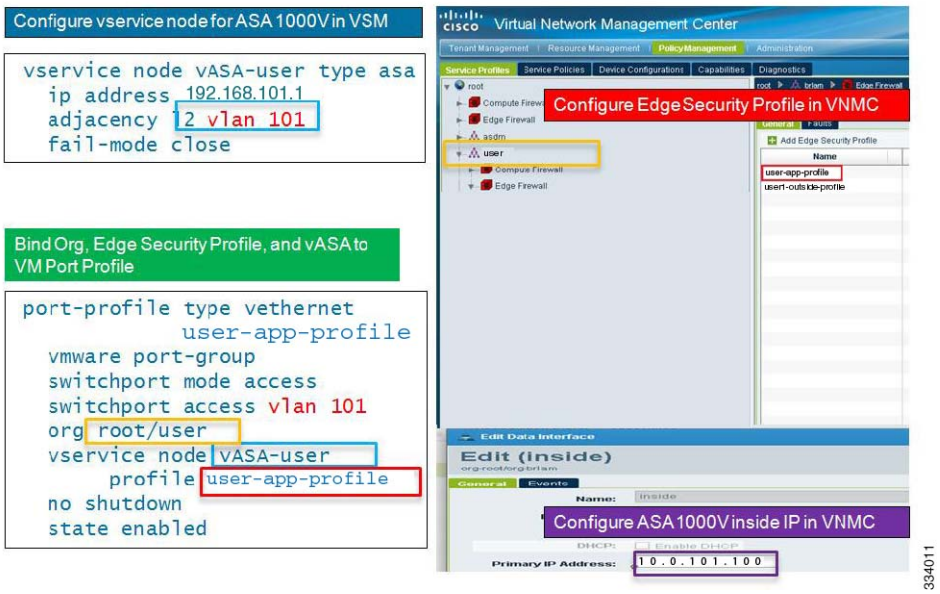


Figure 2-6 shows a visual representation of the steps that you should have performed for binding of the organization path, ASA 1000V, and security profile to the port profile in the VSM. Colored boxes on the right and left sides of the illustration indicate matching values.

Figure 2-6 Binding of the Org Path, ASA 1000V, and Security Profile to the Port Profile in the VSM



To bind the organization path, ASA 1000V, and security profile to the port profile in the VSM, make sure that you have performed the following steps:

1. Configured the edge security profile in the Cisco VNMC.
2. Completed binding of the organization, edge security profile, and vASA to the VM port profile.
3. Configured the vservice node for the ASA 1000V in the VSM.
4. Created an edge firewall under root/user and configured the ASA 1000V inside IP address in the Cisco VNMC.
5. Assigned the ASA 1000V instance to the edge firewall in the Cisco VNMC.

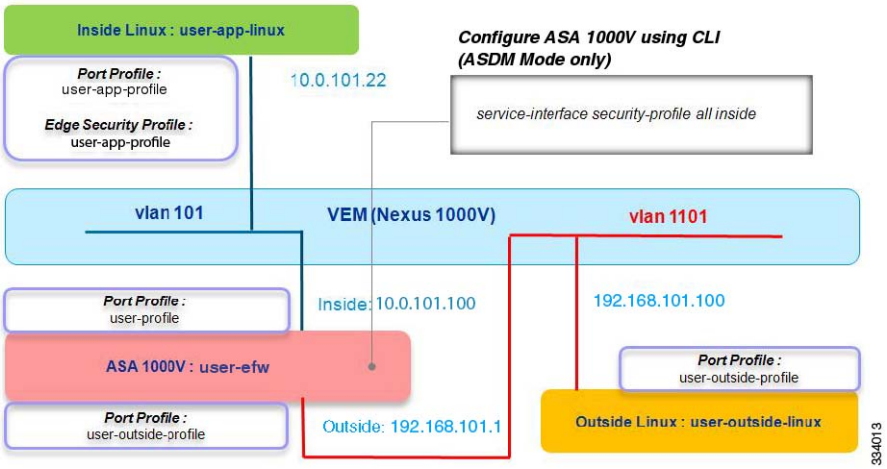
Note Make sure that the IP address for the inside interface of the ASA 1000V in the VSM matches the IP address for the inside interface of the ASA 1000V in the Cisco VNMC.

There is no need for the name of the port profile to be the same as the name of the edge security profile that is used in the **vservice** command in the port profile. In this example, user-app-profile is used in both for convenience.

Security Profile-to-Interface Mapping in the ASA 1000V

The next step applies only if you are using the ASDM mode. This mapping is automatically configured if you are using the VNMC mode. Make sure that you have completed this step by entering the **service-interface security-profile all inside** command at the ASA 1000V CLI or through the ASDM GUI. This configuration shows that all security profile traffic uses the inside interface for traffic to the ASA 1000V and to servers for the inside VMs. Figure 2-7 shows the topology of a correct configuration for security profile-to-interface mapping in the ASA 1000V.

Figure 2-7 Security Profile-to-Interface Mapping in the ASA 1000V

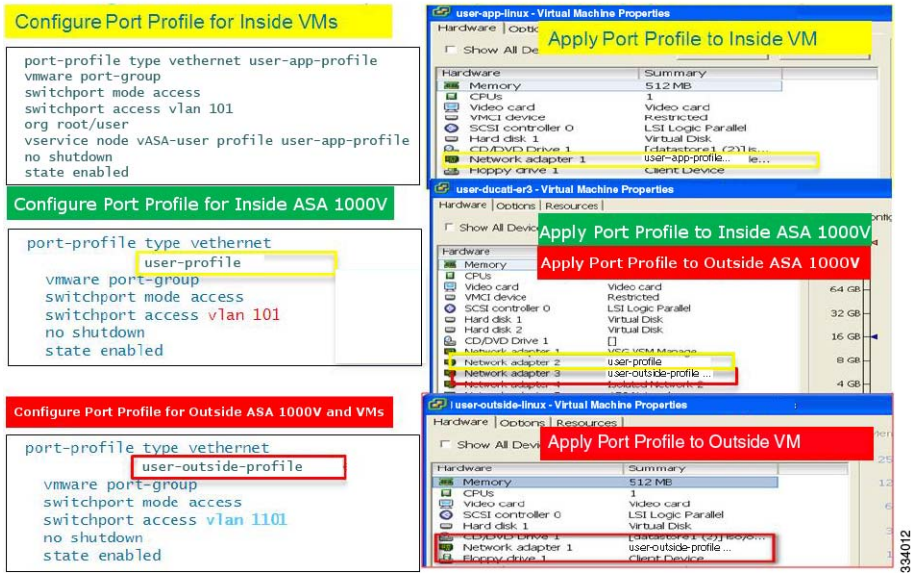


The configuration that enables traffic to flow between the inside VMs and the outside VMs is complete.

Port Profile Configuration in the VSM and Application in vCenter

Figure 2-8 shows a visual representation of the steps that you should have performed to configure the port profile for inside VMs in the VSM and apply this configuration in vCenter. Colored boxes on the right and left sides of the illustration indicate matching values.

Figure 2-8 Port Profile Configuration in the VSM and Application in vCenter



To configure the port profile for inside VMs in the VSM and apply this configuration in vCenter, make sure that you have performed the following steps:

1. Configured the port profiles for the inside VMs.
2. Applied the port profiles to the inside VMs.
3. Configured the port profiles for the inside ASA 1000V.
4. Applied the port profiles to the inside ASA 1000V and then to the outside ASA 1000V.
5. Configured the port profiles for the outside ASA 1000V and the VMs.
6. Applied the port profiles to the outside VMs.
7. Assigned network adapters 1 and 2 for the ASA 1000V in the same sequence as shown in Figure 2-8.
8. Validated that the inside VLAN of the inside VM is on the same inside interface as the ASA 1000V.
9. Validated that the vservice node IP address for the ASA 1000V matches the inside IP address of the Cisco VNMC.

VSM Module Configuration

To make sure that the VSM module has been correctly configured, use the **show module** command on the Cisco Nexus 1000V switch to display the current statistics and configuration settings.

The following is sample output from the **show module** command:

```
Switch# show module
Mod  Ports  Module-Type                      Model               Status
---  -----  -------------------------------  ------------------  ------------
1    0      Virtual Supervisor Module        Nexus1000V          active
3    248    Virtual Ethernet Module          NA                  ok
4    248    Virtual Ethernet Module          NA                  ok

Mod  Sw                Hw
---  ----------------  ------------------------------------------------
1    4.2(1)SV1(5.2)    0.0
3    4.2(1)SV1(5.2)    VMware ESXi 4.1.0 Releasebuild-260247 (2.0)
4    4.2(1)SV1(5.2)    VMware ESXi 4.1.0 Releasebuild-260247 (2.0)

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA

Mod  Server-IP        Server-UUID                          Server-Name
---  ---------------  -----------------------------------  --------------------
1    10.0.10.10       NA                                   NA
3    172.23.34.129    849aa5f8-a4ce-11df-be27-f866f223184e  exampleuser-esx-3.cisco.com
4    172.23.34.134    ab420101-aefe-11df-a902-1cdf0f1d532c  exampleuser-esx-4.cisco.com
```

In this example, the following applies:

- The active status for Module 1 is for the current terminal session only.
- The Server UUID is the UCS host on the Cisco Nexus 1000V switch.
- Two servers are connected to the Cisco Nexus 1000V switch.
- The output shows the statistics for all the components bound together.

VSM vCenter Configuration

To make sure that the VSM vCenter configuration is correct, use the **show svs connection** command on the Cisco Nexus 1000V switch. The following is sample output from the **show svs connections** command:

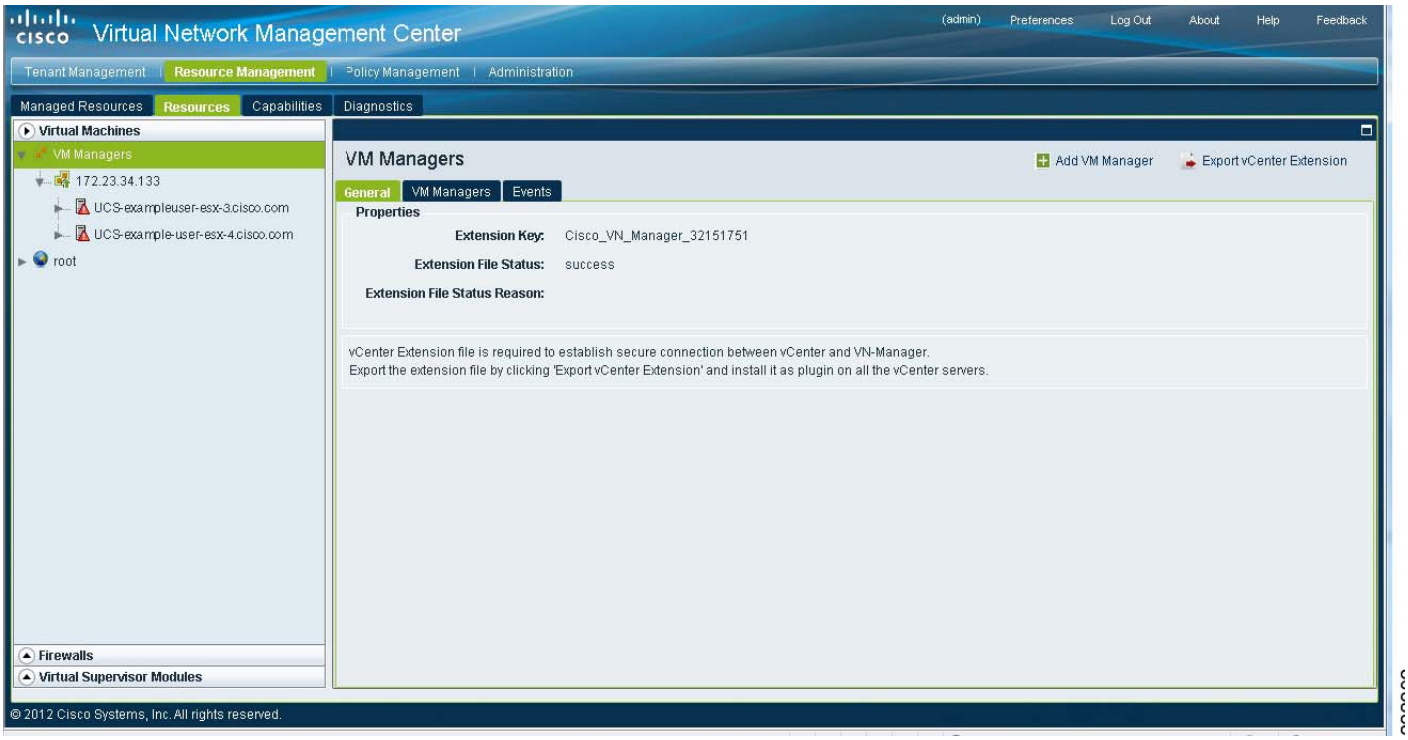
```
Switch# show svs connections

connection vCenter:
    ip address: 10.1.1.3
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: Org/user-DC
    admin:
    max-ports: 8192
    DVS uuid: b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27
    config status: Enabled
    operational status: Connected
    sync status: Complete
    version: VMware vCenter Server 4.1.0 build-345043
    vc-uuid: 32D940A7-CB4E-467A-AD42-923A8AF53192
```

The output shows the IP address for the main data center that contains the servers and the data center name.

Cisco VNMC VM Manager

To make sure that the Cisco VNMC VM Manager has been correctly configured to manage the VMs, in the Cisco VNMC, choose **Resource Management > Resources > Virtual Machines > VM Managers**. Figure 2-9 shows the UCS host that is being managed by the Cisco VNMC.

Figure 2-9 Cisco VNMC VM Manager



Dynamic VSM Interface Configuration

Make sure that the dynamic VSM interface has been correctly configured. The dynamic VSM interface configuration shows multiple vEthernet interfaces, including the outside, inside, and inside VM interfaces, and the virtual network interface cards (vNICs) for the VMs. To validate that the dynamic VSM interfaces have been correctly configured, use the **show running-config interface** command on the Cisco Nexus 1000V switch. The following is sample output from the **show running-config interface** command:

```
Switch# show running-config interface

interface Vethernet5
  inherit port-profile user-outside-profile
  description user-outside-linux, Network Adapter 1
  vmware dvport 4579 dvswitch uuid "b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27"
  vmware vm mac 0050.568E.00A1
interface Vethernet40
  inherit port-profile user-outside-profile
  description user-ASA-1000V-efw, Network Adapter 3
  vmware dvport 4581 dvswitch uuid "b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27"
  vmware vm mac 0050.568E.011F
```

```
interface Vethernet43
  inherit port-profile user-profile
  description user-ASA-1000V-efw, Network Adapter 2
  vmware dvport 4548 dvswitch uuid "b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27"
  vmware vm mac 0050.568E.011B
interface Vethernet55
  inherit port-profile user-app-profile
  description user-app-linux, Network Adapter 1
  vmware dvport 4866 dvswitch uuid "b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27"
  vmware vm mac 0050.568E.00A0
```

The output shows the following:

- user-ASA-1000V-efw is the ASA 1000V machine with the outside interface associated with vEthernet 40 and the inside interface associated with vEthernet 43.
- user-app-linux is the inside Linux machine and is associated with vEthernet 55.
- user-outside-linux is the outside Linux machine and is associated with vEthernet 5.

To view the interface status for the VSM, use the **show interface status** command on the Cisco Nexus 1000V switch. The following is sample output from the **show interface status** command:

```
Switch# show interface status
--------------------------------------------------------------------------------
Port           Name               Status   Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
mgmt0          --                 up       routed    full    1000    --
Eth3/6         --                 up       trunk     full    1000    --
Eth4/6         --                 up       trunk     full    1000    --
Veth1          VSM-Nexus1000V-4.2 up       2         auto    auto    --
Veth2          VSM-Nexus1000V-4.2 up       3         auto    auto    --
..
Veth5          user-outside-linux up       1101      auto    auto    --
Veth40         user-ASA1000V-efw, up       1101      auto    auto    --
Veth43         user-ASA1000V-efw, up       101       auto    auto    --
Veth55         user-app-linux, N  up       101       auto    auto    --
..
..
```

The output shows the following:

- vEthernets and their associated VLANs and VMs.
- vEthernet 5 and vEthernet 40 are on the same VLAN.
- vEthernet 43 and vEthernet 55 are on the same VLAN.

VEM Port Configuration

To validate that the VEM port has been correctly configured, use the **show port** command on the ESX or ESXi server on which the VEM is installed. The following is sample output from the **show port** command on the VEM:

```
~ # vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
  58     Veth40         UP      UP    FWD       0                 user-ASA1000V-efw.eth2
  59     Veth43         UP      UP    FWD       0                 user-ASA1000V-efw.eth1
  64     Veth5          UP      UP    FWD       0                 user-outside-linux.eth0
  65     Veth55         UP      UP    FWD       0                 user-app-linux.eth0
```

The output shows the following:

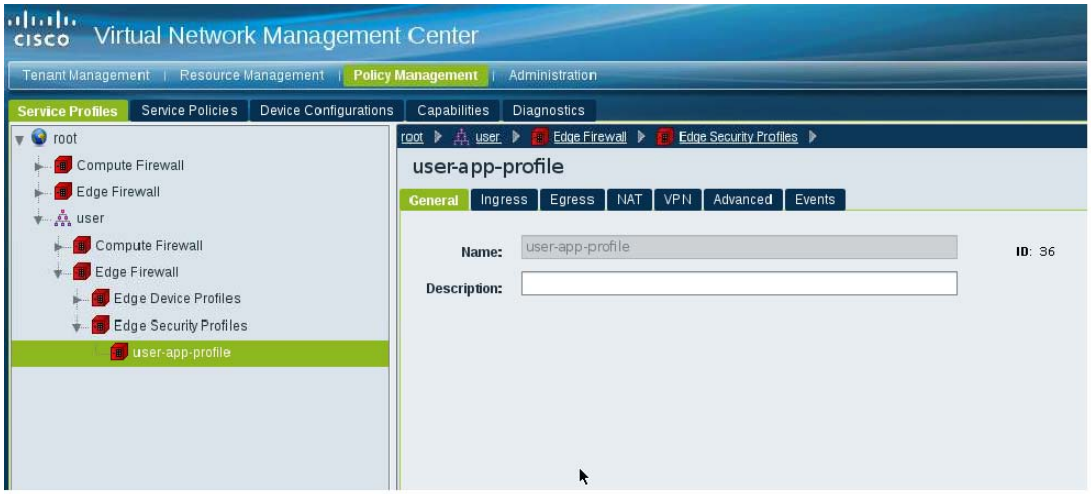
- The LTL column shows the VEM port IDs, which are internally generated by the VEM.
- The VSM Port column shows the associated vEthernets.
- The vEthernet-VM associations shown must be the same as those that appear in the VSM.

Note You can enter commands on the VEM from the VEM shell (SSH access is required) or from the VSM CLI using the **module vem # execute** command. An example from the VSM is the **module vem 3 execute vemcmd show port** command.

Cisco VNMC Security Profile ID

The security profile ID (SPID) is mapped to an edge security profile and is generated by the Cisco VNMC. The SPID is encapsulated in the traffic packet. To validate that the Cisco VNMC SPID has been correctly configured, in the Cisco VNMC, choose **Policy Management > Service Profiles > root > User > user-app-profile**. Figure 2-10 shows an example of a correctly configured Cisco VNMC SPID.

Figure 2-10 Cisco VNMC SPID



VSM vService Configuration

To validate that the VSM vservice has been correctly configured, use the **show vservice detail** command on the Cisco Nexus 1000V switch. The following is sample output from the **show vservice detail** command:

```
Switch# show vservice detail
#License Information
Mod    VSG    ASA
  3      0      2
  4      0      2

#Node Information
#Node ID:13      Name:vASA-user
```

```
 Type:asa       IPAddr:10.0.101.1       Fail:close  Vlan:101
 Mod  State     MAC-Addr                VVer
   4  Alive     00:50:56:8e:01:1b          2

#PortProfile:user-app-profile               Org:root/user
Node:vASA-user                              Profile(Id):user-app-profile(36)
#Veth55
 VM-Name :user-app-linux
 NIC-Name:Network Adapter 1
 DV-Port :4866
 VM-UUID :42 0e 13 70 3c 73 06 3b-3e c2 3c 80 da df 63 87
 DVS-UUID:b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27
 IP-Addrs:10.0.101.22
```

The output shows the following:

- The name of the VSN, which is vASA-user. This VSN appears earlier in this guide in the port profile running configuration under the user-app-profile.
- The IP address, 10.0.101.1, specified in this example refers to the inside interface of the ASA 1000V, which is used for all vPath traffic.
- The port profile that was assigned.
- The inside VM, user-app-linux, and its IP address, 10.0.101.22.
- The VSM gets the security profile ID from the VNMC. For example, Profile(Id): user-app-profile (36).
- Each VM and its associated vEthernet.
- The edge security profile - SPID mapping. The user-app-profile edge security profile is associated with SPID 36.
- A correlation also exists between the IP address of the inside machine, user-app-linux, and SPID 36.
- All the items that appear in the output are bound together.
- The number of ASA 1000V and VSG licenses in use.

VSN Configuration in the VSM

To validate the VSN configuration in the VSM, use the **show vservice brief** command on the Cisco Nexus 1000V switch. The following is sample output from the **show vservice brief** command:

```
Switch# show vservice brief
--------------------------------------------------------------------------------
                                License Information
--------------------------------------------------------------------------------
Type      In-Use-Lic-Count  UnLicensed-Mod
vsg                     0
asa                     4

--------------------------------------------------------------------------------
                                Node Information
--------------------------------------------------------------------------------
 ID Name                    Type   IP-Address      Mode   State   Module
 ......
 ......
 13 vASA-user               asa    10.0.101.1      v-101  Alive   4,
 ......
 ......
```

```
--------------------------------------------------------------------------------
                                  Path Information
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:user-app-profile
Org:root/user
Node:vASA-user(10.0.101.1)                    Profile(Id):user-app-profile(36)
Veth Mod VM-Name                              vNIC IP-Address
  55   4 user-app-linux                         1 10.0.101.22,

--More--
```

Module 4 shows the inside interface configuration of the ASA 1000V, which displays information for all vPath traffic.

To see vEthernet information, use the **show vservice port brief | detail** command on the Cisco Nexus 1000V switch. The following is sample output from the **show vservice port brief** command:

```
Switch# show vservice port brief
--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:user-app-profile
Org:root/user
Node:vASA-user(10.0.101.1)                    Profile(Id):user-app-profile(36)
Veth Mod VM-Name                              vNIC IP-Address
  55   4 user-app-linux                         1 10.0.101.22,

--More--
```

The following is sample output from the **show vservice port detail** command:

```
Switch# show vservice port detail
--------------------------------------------------------------------------------
                                  Port Information
--------------------------------------------------------------------------------
PortProfile:user-app-profile
Org:root/user
Node:vASA-user(10.0.101.1)                   Profile(Id):user-app-profile(36)
Veth55
 Module  :4
 VM-Name :user-app-linux
 vNIC:Network Adapter 1
 DV-Port :4866
 VM-UUID :42 0e 13 70 3c 73 06 3b-3e c2 3c 80 da df 63 87
 DVS-UUID:b0 6a 0e 50 e2 e4 79 25-76 d8 24 d4 02 b0 32 27
 IP-Addrs:10.0.101.22,

--More--
```

The output shows the following:

- The VSN data IP address is for the edge security profile, which has the same IP address as the Cisco VNMC does.
- That 36 is the SPID that is mapped to the security profile and is embedded in the packet.

VSN Configuration in the VEM

To validate the VSN configuration in the VEM, use the **show vsn binding** command on the ESX or ESXi server on which the VEM is installed. The following is sample output from the **show vsn binding** command:

```
~ # vemcmd show vsn binding
  VSG Services Disabled | VSG Licenses Available   0
  ASA Services Enabled  | ASA Licenses Available   2
   LTL   PATH   VSN  SWBD              IP  P-TYPE  P-ID
    63     5     9    21        10.0.21.1       2     2
    65     6    13   101       10.0.101.1       2    36
```

LTL 65 is associated with user-app-linux, which is the inside VM. As a result, the VEM can correlate the inside VM with SPID 36. A profile type of 2 indicates the edge security profile.

To validate the IP address of the inside VM, use the **show learnt ip** command on the Cisco Nexus 1000V switch. The following is sample output from the **show learnt ip** command:

```
~ # vemcmd show learnt ip
      IP Address LTL   VLAN    BD
                      /SegID
      10.0.21.36  63     21    10
     10.0.101.22  65    101    18
```

The VEM learns the IP addresses of the VMs present on the network and knows the IP address of the inside VM, which is user-app-linux. The IP and SPID information is the same in the VEM and in the VSM.

ASA 1000V IP-SPID Mapping (Control Path)

To validate the ASA 1000V IP-SPID mapping from the control path, use the **show vsn** command on the ASA 1000V. The following is sample output from the **show vsn** command:

```
ASA1000V# show vsn
Configuration through VNMC: enabled

vsn security-profile info:
security-profile : user-outside-profile@root/user
SPID             : 35
Interface        : sp0001

security-profile : default@root
SPID             : 2
Interface        : sp0002

security-profile : user-app-profile@root/user
SPID             : 36
Interface        : sp0003

vsn ip-binding info:
IP               : 10.0.101.22
security-profile : user-app-profile@root/user
Interface        : sp0003
ASA1000V#
```

The output shows the binding (mapping) information in the Cisco VNMC, ASA 1000V, and Cisco Nexus 1000V switch, and the following:

- SPID bindings from the control path.
- IP-SPID bindings that are the same as the VSM and VEM output.
- The user-app-profile edge security profile has been mapped to the ASA 1000V.
- All vPath traffic passes through security profile 3 (sp003) on the ASA 1000V.

ASA 1000V IP-SPID Mapping (Data Path)

To validate the ASA 1000V IP-SPID binding from the data path, use the **show asp table vsn ip-binding** command on the ASA 1000V. You can use this command in ASDM or in VNMC mode. The following is sample output from the **show asp table vsn ip-binding** command:

```
ASA1000V(config)# show asp table vsn ip-binding
SPID          IP Address
11            10.0.0.26
11            10.0.0.20
11            10.0.0.25
```

This output may help determine if the control path or data path is the issue that requires resolution.

To validate the security profile-SPID binding from the data path, use the **show asp table vsn security-profile** command on the ASA 1000V. You can only use this command when you are in ASDM mode. The following is sample output from the **show asp table vsn security-profile** command on the ASA 1000V:

```
ASA1000V(config)# show asp table vsn security-profile
SPID          Security profile
11            sp1
```

ASA 1000V Services for Security Profile Interfaces

To validate the ASA 1000V services for security profiles, use the **show running-config service-interface** command on the ASA 1000V. The following is sample output from the **show running-config service-interface** command:

```
ASA1000V# show running-config service-interface
service-interface security-profile all inside
```

You only need to enter this command if you use the ASDM mode. The command runs automatically if you use the VNMC mode. The security profile interface is not a physical interface that can send or receive vPath tagged traffic from the Cisco Nexus 1000V switch. You can associate the physical interface to be used to send or receive vPath traffic using the **service-interface** command.

VSM Interface Counters

To see the vEthernet statistics, use the **show interface counters** command on the Cisco Nexus 1000V switch. The following is sample output from the **show interface counters** command:

```
Switch# show interface counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Veth55                 43639             25386               19              163
Veth40                 18772               198                0              532
Veth43                117240             28656                0              608

--------------------------------------------------------------------------------
Port               OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Veth55               1512452               327                0           149429
Veth40                 60508               613               18               51
Veth43                141150               340               18           134246
```

VEM Packet Statistics

To see the correlation between the VSM and VEM statistics, use the **show packets** command on the ESX or ESXi server on which the VEM installed. The following is sample output from the **show packets** command on the VEM:

```
~ # vemcmd show packets
LTL    RxUcast TxUcast    RxMcast TxMcast RxBcast TxBcast    Txflood Rxdrop Txdrop  Name
65     25386   327        19      0       163     149429     1593    0      0       user-app-linux.eth0
58     198     613        0       18      532     51         21      0      0       user-ASA1000V-efw.eth2
59     28656   340        0       18      608     134246     1926    0      0       user-ASA1000V-efw.eth1
```

The packet statistics on the VEM and on the VSM must match each other in a working configuration.

ASA 1000V vPath Counters

To see the packets sent or received on the service interface, use the **show counters** command on the ASA 1000V. The following is sample output from the **show counters** command:

```
ASA1000V# show counters
Protocol     Counter                        Value    Context
IP           IN_PKTS                        18342    Summary
IP           OUT_PKTS                         167    Summary
VPATH        IN_PKTS                          181    Summary
VPATH        OUT_PKTS                          29    Summary
VPATH        OUT_VSN_PKTS                     152    Summary
VPATH        HA_COMMON_OUT_PKTS                 1    Summary
VPATH        HA_COMMON_OUT_BYTES               56    Summary
IP           TO_ARP                         10105    Summary
IP           TO_UDP                           157    Summary
UDP          IN_PKTS                          157    Summary
UDP          OUT_PKTS                         157    Summary
SSLERR       BAD_PROTOCOL_VERSION_NUMBER        2    Summary
SSLERR       BAD_SIGNATURE                      2    Summary
SSLALERT     TX_CLOSE_NOTIFY                  101    Summary
```

```
SSLALERT      TX_WARNING_ALERT                101    Summary
SSLDEV        NEW_CTX                           1    Summary
SSLNP         OPEN_CONN                         1    Summary
SSLNP         HANDSHAKE_START                 101    Summary
<---More-->
```

In this output, the vPath counters specify the following:

- IN_PKTS—The number of packets received from the Cisco Nexus 1000V switch (for the service interface).
- OUT_PKTS—The number of packets sent to the Cisco Nexus 1000V switch (for the service interface).
- OUT_VSN_PKTS—Control–related packets.
- HA_COMMON_OUT_PKTS—The number of packets sent during failover replication.
- HA_COMMON_OUT_BYTES—The number of bytes sent during failover replication.

Example

An ICMP packet is sent from an inside VM to the outside, with five ping packets.

The **show counters** command output shows that the vPath counters on the ASA 1000V were the following:

```
ASA1000V# show counters
Protocol      Counter                       Value    Context
VPATH         IN_PKTS                          12    Summary
VPATH         OUT_PKTS                          5    Summary
VPATH         OUT_VSN_PKTS                      7    Summary
```

The result is the following:

- 5 vPath IN_PKTS—Five packets were received by the service interface from the Cisco Nexus 1000V switch.
- 5 vPath OUT_PKTS—Five packets were sent by the service interface to the Cisco Nexus 1000V switch.
- 7 vPath OUT_VSN_PKTS—Seven packets were control-related packets.

VSM vService Statistics

To see VSM vService statistics, use the **show vservice statistics vlan 101** command on the Cisco Nexus 1000V switch. The following is sample output from the **show vservice statistics vlan 101** command:

```
Switch(config)# show vservice statistics vlan 101
#VSN  VLAN: 101, IP-ADDR: 10.0.101.1
  Module: 4
    #VPath Packet Statistics     Ingress         Egress           Total
    Total Seen                         5              0               5
    Policy Redirects                   0              0               0
    No-Policy Passthru                 0              0               0
    Policy-Permits Rcvd                0              5               5
    Policy-Denies  Rcvd                0              0               0
    Permit Hits                        0              0               0
    Deny   Hits                        0              0               0
    Decapsulated                       0              5               5
    Fail-Open                          0              0               0
    Badport Err                        0              0               0
    VSN Config Err                     0              0               0
```

```
    VSN State Down                  0              0              0
    Encap Err                       0              0              0
    All-Drops                       0              0              0
    Flow Notificns Sent                                            0
    Total Rcvd From VSN                                            7
    Non-Cisco Encap Rcvd                                           0
    VNS-Port Drops                                                 1
```

The output shows the following:

- The counters on the ASA 1000V and the VSM are the same.
- The VSM saw five packets and decapsulated them.
- The VSM received seven control-related packets from the service node.

ASA 1000V Interface Statistics

To see interface statistics for the ASA 1000V, use the **show interface** command on the ASA 1000V. The following is sample output from the **show interface** command:

```
ASA1000V(config)# show interface
Interface GigabitEthernet0/0 "inside", is up, line protocol is up
Interface security profile “sp0003”, is up, line protocol is up
security-profile user-app-profile@root/user, spid 36
service-interface is inside
  Hardware is 1825445EM rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex (Full-duplex), Auto-Speed (1000Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 0050.568e.011b, MTU 1500
        IP address 10.0.101.1, subnet mask 255.255.255.0
        98 packets input, 6272 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 8 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        51 packets output, 3600 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        48 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (255/205)
        output queue (blocks free curr/low): hardware (204/204)
   Traffic statistics for "inside":
        44 packets input, 2024 bytes
        45 output, 1260 bytes
        0 packets dropped
<---More--->
```

The output shows the following:

- The service interface is the inside interface.
- All vPath traffic traverses this interface.
- Any issues that occur with vPath encapsulation should appear in the L2 decode drop values.
- A non-zero value indicates the number of dropped packets for the vPath header. In this example, no packets have been dropped.
- The security profile interface sp0003 is up, and no packets have been dropped.
- The service interface is configured as the inside interface.

To see interface statistics for security profiles, use the **show interface** command on the ASA 1000V. The following is sample output from the **show interface** command for security profiles:

```
ASA1000V(config)# show interface
Interface security-profile "sp0003", is up, line protocol is up
        security-profile user-app-profile@root/user, spid 36
   Traffic statistics for "sp0003":
         29 packets input, 2436 bytes
         29 packets output, 2436 bytes
         0 packets dropped
       1 minute input rate 0 pkts/sec, 0 bytes/sec
       1 minute output rate 0 pkts/sec, 0 bytes/sec
       1 minute drop rate, 0 pkts/sec
       5 minute input rate 0 pkts/sec, 0 bytes/sec
       5 minute output rate 0 pkts/sec, 0 bytes/sec
       5 minute drop rate, 0 pkts/sec
    Traffic statistics for "sp0003":
          29 packets input, 2436 bytes
          29 packets output, 2436 bytes
          0 packets dropped
       1 minute input rate 0 pkts/sec, 0 bytes/sec
       1 minute output rate 0 pkts/sec, 0 bytes/sec
       1 minute drop rate, 0 pkts/sec
       5 minute input rate 0 pkts/sec, 0 bytes/sec
       5 minute output rate 0 pkts/sec, 0 bytes/sec
       5 minute drop rate, 0 pkts/sec
ASA1000V(config)#
```

The output indicates that security profile interface sp0003 is up, and no packets have been dropped.

CHAPTER 3

Case Studies in Traffic Failure

When the ASA 1000V cannot pass traffic from the inside to the outside interface or vice-versa, you can take a number of steps to troubleshoot this issue.

This chapter describes the following three case studies used for troubleshooting:

Case Study 1

Five packets from the Linux machine are sent outside.

Testing Traffic

To test whether or not traffic can pass through from the inside to the outside interface, perform one of the following steps:

- Ping the inside to outside interface from the Linux machine by entering the following command:

```
user-app-linux# ping user-outside-linux.cisco.com -c 5
5 packets transmitted, 0 received, 100% packet loss, time 3999 ms
```

- Enter the following command on the ASA 1000V:

```
user-ASA1000V-efw(config)# show asp drop

Frame drop:
   No route to host (no-route)                                  21
   Flow is denied by configured rule (acl-drop)                  1
   FP L2 rule drop (l2 acl)                                      3
   Security-profile not matched (security-profile-not-matched)5

Last clearing: 14:43:34 UTC Jun 20 2012 by enable_15

Flow drop:

Last clearing: 14:43:34 UTC Jun 20 2012 by enable_15
```

The output indicates that an issue with the security profile exists.

Debugging the Issue

To debug the issue, perform the following steps:

1. Check the IP address-to-security profile binding on the ASA 1000V by entering the following command:

```
user-ASA1000V-efw(config)# show vsn
Configuration through VNMC: enabled

vsn security-profile:
security-profile: user-outside-profile@root/user
SPID            : 35
Interface       : sp0001

security profile: default@root
SPID            : 2
Interface       : sp0002

security-profile: user-app-profile@root/user
SPID            : 36
Interface       : sp0003
```

The IP binding is missing, which indicates that it was not pushed to the VNMC.

2. In the Cisco VNMC, check the port profile-to-edge security profile binding by doing the following:
   a. Choose **Resource Management > Managed Resources > Firewalls**.
   b. In the Firewalls list, choose **root > (selected org) > Edge Firewalls > (selected edge firewall)**.

      If the port profile-to-edge security profile binding is missing in the Edge Security Profiles tab on the right, then it indicates that the binding was not pushed from the VSM to the Cisco VNMC.

3. In the VSM, check the port profile for the inside VMs by entering the following command on the Cisco Nexus 1000V switch:

```
user-N1K-Switch# show running-config port-profile user-app-profile
version 4.2(1)SV1(5.2)
port-profile type vethernet user-app-profile
  vmware port-group
  switchport mode access
  switchport access vlan 101
no shutdown
  state enabled
```

The security profile, org, and ASA 1000V-to-port-profile binding are missing. The missing binding is the primary cause of the configuration issue.

Resolving the Issue

To resolve the configuration issue, perform the following steps:

1. Add the org in which the security profile resides.
2. Add the binding of the ASA 1000V vservice node and security profile to the port profile.

The following example shows the results of performing these two steps:

```
user-N1K-Switch# show running-config port-profile user-app-profile
version 4.2(1)SV1(5.2)
port-profile type vethernet user-app-profile
```

```
vmware port-group
switchport mode access
switchport access vlan 101
org root/user
vservice node vASA-user profile user-app-profile
no shutdown
state enabled
```

The org root/user has been added. The ASA 1000V vservice node and security profile have been bound to the port profile.

Case Study 2

A traffic failure has occurred on the ASA 1000V.

Determining the Cause of Failure

To determine the cause of the traffic failure in this case, enter the following command on the ASA 1000V:

```
user-ASA1000V-efw(config)# show interface

Interface security-profile "user-app-profile", is down, line protocol is down
security-profile user-app-profile@root/user, spid 36
service-interface is unassigned
Traffic statistics for "sp0003":
29 packets input, 2436 bytes
29 packets output, 2436 bytes
0 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
```

The output indicates that the security profile is down and the service interface for the security profile has not been assigned.

Debugging the Issue

To debug this issue, enter the following command on the ASA 1000V:

```
user-ASA1000V-efw(config)# show running-config service-interface
```

A blank output confirms that the service interface has not been configured. This issue occurs in the ASDM mode only; the service interface is automatically configured in the VNMC mode.

Resolving the Issue

The resolution is to configure the service interface on the ASA 1000V by entering the following command in ASDM mode:

```
user-ASA1000V-efw(config)# service-interface security-profile all inside
```

Case Study 3

A traffic failure has occurred on the ASA 1000V.

Determining the Cause of Failure

To determine the cause of the traffic failure in this case, perform the following steps:

1. Enter the **show asp drop** command on the ASA 1000V.

```
user-ASA1000V-efw(config)# show asp drop

Frame drop:
  No route to host (no-route)                                  494
  Flow is denied by configured rule (acl-drop)                   5
  Slowpath security checks failed (sp-security-checks)           1
  FP L2 rule drop (l2_acl)                                     550

Last clearing: 15:35:06 UTC Jun 20 2012 by enable_15

Flow drop:

Last clearing: 15:35:06 UTC Jun 20 2012 by enable_15
```

No vPath-related packets have been dropped.

2. Check whether or not the ACL configuration has been pushed from the Cisco VNMC to the ASA 1000V by entering the **show running-config access-list** and **show running-config access-group** commands on the ASA 1000V.

The output of these two commands indicates that the ACL policy was not configured correctly in the Cisco VNMC.

Resolving the Issue

To resolve the issue, reconfigure the ACL policy correctly in the Cisco VNMC.