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, page 3-1
- Case Study 2, page 3-3
- Case Study 3, page 3-4

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.