CHAPTER 9

ACLs

This chapter describes how to identify and resolve problems that relate to Access Control Lists (ACLs).

This chapter includes the following sections:

About Access Control Lists (ACLs)

An ACL is an ordered set of rules for filtering traffic. When the device determines that an ACL applies to a packet, it tests the packet against the rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies a default rule. The device processes packets that are permitted and drops packets that are denied.

ACLs protect networks and specific hosts from unnecessary or unwanted traffic. For example, ACLs are used to disallow HTTP traffic from a high-security network to the Internet. ACLs also allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

The following types of ACLs are supported for filtering traffic:

- IP ACLs—The device applies IP ACLs only to IP traffic.
- MAC ACLs—The device applies MAC ACLs only to non-IP traffic.

For detailed information about how rules are used to configure how an ACL configures network traffic, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(1).*

ACL Configuration Limits

The following configuration limits apply to ACLs:

- You cannot have more that 128 rules in an ACL.
- You cannot have more than 10,000 ACLs (spread across all the ACLs) in one VEM.

ACL Restrictions

The following restrictions apply to ACLs:

- You cannot apply more than one IP ACL and one MAC ACL in each direction on an interface.
- A MAC ACL applies only to Layer 2 packets.
- VLAN ACLs are not supported.
- IP fragments are not supported n ACL rules.
- Non initial fragments are not subject to ACL lookup.
- The established option to specify TCP flags is not supported.
- You cannot have two not-equal-to (neq) operators in the same rule.

Troubleshooting ACLs

The commands listed in this section can be used on the VSM to see the policies that are configured and applied on the interfaces.

Use the following command to display configured ACLs:

- **show access-list summary**

Use following commands on the VSM to see run-time information of the ACLMGR and ACLCOMP during configuration errors, and to collect ACLMGR process run-time information configuration errors:

- **show system internal aclmgr event-history errors**
- **show system internal aclmgr event-history msgs**
- **show system internal aclmgr ppf**
- **show system internal aclmgr mem-stats (to debug memory usage and leaks)**
- **show system internal aclmgr status**
- **show system internal aclmgr dictionary**

Use the following commands to collect ACLCOMP process run-time information configuration errors:

- **show system internal aclcomp event-history errors**
- **show system internal aclcomp event-history msgs**
- **show system internal aclcomp pdl detailed**
- **show system internal aclcomp mem-stats** (to debug memory usage and leaks)

Displaying ACL Policies on the VEM

The commands listed in this section can be used to display configured ACL policies on the VEM.

Use the following command to list the ACLs installed on that server

```
~ # module vem 3 execute vemcmd show acl
Acl-id Ref-cnt  Type Numrules  Stats
    1      1    IPv4      1    disabled
```

The Acl-id is the local ACLID for this VEM. Ref-cnt refers to the number of instances of this ACL in this VEM.

Use the following command to list the interfaces on which ACLs have been installed

```
~ # module vem 3 execute vemcmd show acl pinst
LTL   Acl-id    Dir
 16       1    ingress
```

Debugging Policy Verification Issues

To debug a policy verification failure, follow these steps:

Step 1 On the VSM, enter the **debug logfile** *filename* command to redirect the output to a file in bootflash.

Step 2 Enter the **debug aclmgr al**l command.

Step 3 Enter the **debug aclcomp all** command.

For the VEMs where the policy exists, or is being applied, enter the following these steps from the VSM. The output goes to the console.

Step 4 Enter the **module vem** *module-number* **execute vemdpalog debug sfaclagent all** command.

Step 5 Enter the **module vem** *module-number* **execute vemdpalog debug sfpdlagent all** command.

Step 6 Enter the **module vem** *module-number* **execute vemlog debug sfacl all** command.

Step 7 Enter the **module vem** *module-number* **execute vemlog start** command.

Step 8 Enter the **module vem** *module-number* **execute vemlog start** command.

Step 9 Configure the policy that was causing the verify error.

Step 10 Enter the **module vem** *module-number* **execute vemdpalog show all** command.

Step 11 Enter **module vem** *module-number* **execute vemlog show all** command.

Save the Telnet or SSH session buffer to a file. Copy the logfile created in bootflash.