Access Control Lists

This chapter describes how to identify and resolve problems that relate to access control lists (ACLs).

Information About 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 ACL rules are used to configure network traffic, see the *Cisco Nexus 1000V for Microsoft Hyper-V Security Configuration Guide.*

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 Virtual Ethernet Module (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 on ACL rules.
- Non-initial fragments are not subject to an 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.
- ACLs are not supported in port channels.

ACL Troubleshooting Commands

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

Display the configured ACLs by entering this command:

- **show access-list summary**

Display the run-time information of the ACLMGR and ACLCOMP during configuration errors and to collect ACLMGR process run-time information configuration errors by entering these commands on the VSM:

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

Collect ACLCOMP process run-time information configuration errors by entering these commands:

- **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)
- **show system internal aclcomp ppf control**

Displaying ACL Policies on the VEM

You can use the commands in this section to display configured ACL policies on the VEM.

To list the ACLs installed on that server, enter this command:

- **module vem** *module-number* **execute vemcmd show acl**

```
n1000v # module vem 3 execute vemcmd show acl
Acl-id Ref-cnt  Type  Numrules  Stats    Stat-id
    1     33    IPv4    127     enabled      9
    2     81    IPv4    127     enabled     10
    3     33    IPv4    127     enabled     11
```

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

To list the interfaces on which ACLs have been installed, enter this command:

- **module vem** *module-number* **execute vemcmd show acl pinst**

```
n1000v# module vem 3 execute vemcmd show acl pinst
LTL   Acl-id    Dir
 16       1    ingress
```

Debugging Policy Verification Issues

Step 1 Redirect the output to a file in bootflash by entering the **debug logfile** *filename* command on the VSM.

Step 2 Configure all debug flags of aclmgr by entering the **debug aclmgr all** command.

Step 3 Configure all debug flags of aclcomp by entering the **debug aclcomp all** command.

Step 4 From the VSM enter the following steps:

Note The output goes to the console.

a. Enable ACL logging on the DPA by entering these commands:
   - **module vem** *module-number* **execute vemcmd dpa debug sfaclagent all**
   - **module vem** *module-number* **execute vemcmd dpa debug sfpdlagent all**

b. Enable logging on the VEM by enter the **module vem** *module-number* **execute vemlog debug sfacl all** command.

c. Enable DPA logging for viewing by entering the **module vem** *module-number* **execute vemlog start** command.

d. Enable DPA logging for viewing by entering the **module vem** *module-number* **execute vemlog start** command.

Step 5 Configure the policy that was causing the verification error.

Step 6 Display DPA logs by entering the **module vem** *module-number* **execute vemlog show all** command.

Step 7 Save the Telnet or SSH session buffer to a file.

Step 8 Copy the logfile created in bootflash.