CHAPTER 15

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 ACL rules are used to configure network traffic, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV2(1.1)).*

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.
- ACL is not supported in port channels.

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.

Troubleshooting ACL Logging

This section includes the following topics:

Using the CLI to Troubleshoot ACL Logging on a VEM

The commands in this section will help you troubleshoot ACL logging by examining ACL flows.

Viewing Current Flows

You can troubleshoot ACL logging by viewing the current flows on a VEM. Enter the following command:

vemcmd show aclflows stats

EXAMPLE

The following shows an example of the output when you enter this command:

```
[root@esx /]# vemcmd show aclflows stats
Current Flow stats:
    Permit Flows:        1647
    Deny Flows:             0
    Current New Flows:    419        --- current new flows yet to be reported.
```

Viewing Active Flows

You can display all the active flows on a VEM by entering the following command:

vemcmd show aclflows [permit | deny]

If you do not specify **permit** or **deny**, the command displays both.

EXAMPLE

The following shows an example of the output when you enter this command:

```
[root@esx /]# vemcmd show aclflows [permit | deny]
If       SrcIP           DstIP           SrcPort DstPort Proto Direction Action   Stats
Veth4    192.168.1.20    192.168.1.10       5345    8080     6 Ingress   permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5769     6 Egress    permit   1
Veth4    192.168.1.20    192.168.1.10       6256    8080     6 Ingress   permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5801     6 Egress    permit   1
Veth4    192.168.1.20    192.168.1.10       5217    8080     6 Ingress   permit   1
Veth4    192.168.1.10    192.168.1.20       8080   57211     6 Egress    permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5865     6 Egress    permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5833     6 Egress    permit   1
Veth4    192.168.1.20    192.168.1.10       5601    8080     6 Ingress   permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5705     6 Egress    permit   1
Veth4    192.168.1.10    192.168.1.20       8080    5737     6 Egress    permit   1
Veth4    192.168.1.20    192.168.1.10       5473    8080     6 Ingress   permit   1
Veth4    192.168.1.20    192.168.1.10      57211    8080     6 Ingress   permit   1
```

Flushing All ACL Flows

You can use this command to detect any new flows affecting the VEM. Clear all the existing flows, then you can detect new flows that match any expected traffic. Syslog messages are not sent when you do this. Enter the following command:

vemcmd flush aclflows

Showing Flow Debug Statistics

You can show ACL debug statistics.

To display internal ACL flow statistics, enter the following command:

vemcmd show aclflows dbgstats

To clear all internal ACL flow debug statistics, enter the following command:

vemcmd clear aclflows dbgstats

ACL Logging Troubleshooting Scenarios

This section describes situations that you might encounter when you are using ACL logging.

Troubleshooting a Syslog Server Configuration

If syslog messages are not being sent from the VEM, you can check the syslog server configuration and check if ACL logging is configured by entering the commands shown in the following procedure.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the VSM and VEM CLI.

SUMMARY STEPS

1. **show logging ip access-list status**
2. **vemcmd show acllog config**
3. **vemcmd show aclflows dbgstats**

PROCEDURE

	Command	Description

Step 1	**show logging ip access-list status**
	Example
	`n1000v # show logging ip access-list status`
	`n1000v #`
		Verifies that the remote syslog server is configured properly.

Step 2	**vemcmd show acllog config**
	Example:
	`n1000v# vemcmd show acllog config`
	`n1000v #`
		Verifies ACL logging on the VEM.

Step 3	**vemcmd show aclflows dbgstats**
	Example:
	`n1000v# vemcmd show aclflows dbgstats`
	`n1000v #`
		Checks to see if any errors occurred.

Troubleshooting an ACL Rule That Does Not Have a Log Keyword

If the ACL rule does not have a log keyword, any flow matching the ACL is not reported although the ACL statistics continue to advance. You can verify a log keyword by entering the commands shown in the following procedure.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the VSM and VEM CLI.

SUMMARY STEPS

1. **show running-config aclmgr**
2. **show logging ip access-list status**
3. **vemcmd show acllog config**

PROCEDURE

	Command	Description

Step 1	**show running-config aclmg**
	Example
	`n1000v # show running-config aclmg`
	`n1000v #`
		Verify that the log keyword is enabled

Step 2	**show logging ip access-list status**
	Example:
	`n1000v # show logging ip access-list status`
	`n1000v #`
		Verify that ACL logging is configured properly

Step 3	**vemcmd show acllog config**
	Example:
	`n1000v # vemcmd show acllog config`
	`n1000v #`
		Verifies ACL logging on the VEM.

Troubleshooting a Maximum Flow Limit Value That is Too Low

If the number of flows does not reach 5000 for either permit of deny flows, you can increase the maximum flows by entering the commands shown in the following procedure.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the VSM and VEM CLI.

SUMMARY STEPS

1. **show logging ip access-list status**

2. **vemcmd show acllog config**
3. **logging ip access-list cache max-deny- flows <*num*>**

PROCEDURE

	Command	Description

Step 1	**`show logging ip access-list status`**
	Example:
	`n1000v # show logging ip access-list status`
	`n1000v #`
		Verifies that ACL logging is configured properly.

Step 2	**`vemcmd show acllog config`**
	Example:
	`n1000v # vemcmd show acllog config`
	`n1000v #`
		Verifies ACL logging on the VEM.

Step 3	**`logging ip access-list cache max-deny-flows`** *<num>*
	Example:
	`n1000v # logging ip access-list cache max-deny- flows <num>`
	`n1000v #`
		Increases maximum flows to the desired value.

Troubleshooting a Mismatched Configuration between a VSM and a VEM

If syslog messages are not being sent and the flow information counters are invalid, the configuration between a VSM and a VEM might be mismatched. Enter the commands shown in this procedure.

Modify any mismatched configurations using the appropriate configuration command. If the problem persists, enable acllog debugging on both VSM and the VEM and retry the commands.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show logging ip access-list status**
2. **vemcmd show acllog config**

PROCEDURE

	Command	Description

Step 1	**show logging ip access-list status**
	Example:
	`n1000v # show logging ip access-list status`
	`n1000v #`
		Verifies that ACL logging is configured properly.

Step 2	**vemcmd show acllog config**
	Example:
	`n1000v # vemcmd show acllog config`
	`n1000v #`
		Verifies ACL logging on the VEM.