



ACLs

This chapter describes how to identify and resolve problems that relate to Access Control Lists (ACLs) and includes the following sections:

- [Information About Access Control Lists, page 16-1](#)
- [ACL Configuration Limits, page 16-1](#)
- [ACL Restrictions, page 16-2](#)
- [ACL Troubleshooting Commands, page 16-2](#)
- [Displaying ACL Policies on the VEM, page 16-2](#)
- [Debugging Policy Verification Issues, page 16-3](#)
- [Troubleshooting ACL Logging, page 16-3](#)

Information About Access Control Lists

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.
- IPv6—The device applies IPv6 ACLs only to IPv6 traffic

For detailed information about how ACL rules are used to configure network traffic, see the *Cisco Nexus 1000V Security Configuration Guide*.

ACL Configuration Limits

The following configuration limits apply to ACLs:

- You cannot have more than 128 rules in an ACL.

- The maximum number of ACLs is 128 (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 on ACL rules.
- Noninitial fragments are not subject to ACL lookup.
- You cannot have two not-equal-to (neq) operators in the same rule.
- ACL is not supported in port channels.

ACL Troubleshooting Commands

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 Virtual Ethernet Module (VEM).

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

```
switch(config-if)# module vem 3 execute vemcmd show acl
```

```

AclId RefCnt Type Rules StatId AclName (Stats: Permit/Deny/NoMatch)
-----
1 0 IPv4 1 1 v4 (Enb: 0/0/0)
2 0 IPv6 0 2 v6 (Dis: 0/0/0)

```

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

You can debug a policy verification failure.



Note

This section is applicable only to VEMs that are available in older releases. The VEMs in the latest release do not have any policy verification failure issue.

-
- Step 1** On the VSM, redirect the output to a file in bootflash.
- debug logfile filename**
- Step 2** Enter the **debug acmgr all** 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 sfpdagent 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, page 16-4](#)

- [ACL Logging Troubleshooting Scenarios, page 16-5](#)

Using the CLI to Troubleshoot ACL Logging on a VEM

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

Viewing Current Flows

You can troubleshoot ACL logging by viewing the current flows on a VEM.

vemcmd show aclflows stats

EXAMPLE

The following example shows how to troubleshoot ACL logging:

```
[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.

vemcmd show aclflows [permit | deny]

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

EXAMPLE

The following example shows how to display all the active flows on a VEM:

```
[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 the **vemcmd flush aclflows** command to detect any new flows that affect the VEM. Clear all the existing flows, and then you can detect new flows that match any expected traffic. Syslog messages are not sent when you do this action.

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

- Log in to the VSM and VEM CLI.

PROCEDURE

	Command	Description
Step 1	<pre>show logging ip access-list status</pre> <p>Example:</p> <pre>switch# show logging ip access-list status switch #</pre>	Verifies that the remote syslog server is configured properly.
Step 2	<pre>vemcmd show acllog config</pre> <p>Example:</p> <pre>switch# vemcmd show acllog config switch #</pre>	Verifies ACL logging on the VEM.
Step 3	<pre>vemcmd show aclflows dbgstats</pre> <p>Example:</p> <pre>switch# vemcmd show aclflows dbgstats switch #</pre>	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 that matches the ACL is not reported although the ACL statistics continue to advance. You can verify a **log** keyword.

BEFORE YOU BEGIN

- Log in to the VSM and VEM CLI.

PROCEDURE

	Command	Description
Step 1	show running-config aclmg Example switch# show running-config aclmg switch #	Verifies that the log keyword is enabled.
Step 2	show logging ip access-list status Example: switch# show logging ip access-list status switch #	Verifies that ACL logging is configured properly.
Step 3	vemcmd show acllog config Example: switch# vemcmd show acllog config switch #	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 or deny flows, you can increase the maximum flows.

BEFORE YOU BEGIN

- Log in to the VSM and VEM CLI.

PROCEDURE

	Command	Description
Step 1	show logging ip access-list status Example: switch# show logging ip access-list status switch #	Verifies that ACL logging is configured properly.

	Command	Description
Step 2	vemcmd show acllog config Example: switch# vemcmd show acllog config switch #	Verifies ACL logging on the VEM.
Step 3	logging ip access-list cache max-deny-flows <num> Example: switch# logging ip access-list cache max-deny- flows <num> switch #	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.

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

BEFORE YOU BEGIN

- Log in to the CLI in EXEC mode.

PROCEDURE

	Command	Description
Step 1	show logging ip access-list status Example: switch# show logging ip access-list status switch #	Verifies that ACL logging is configured properly.
Step 2	vemcmd show acllog config Example: switch# vemcmd show acllog config switch #	Verifies ACL logging on the VEM.

