ACLs

This chapter describes how to identify and resolve problems related to Access Control Lists (ACLs). This chapter contains the following sections:

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 that 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:

- More than one IP ACL and one MAC ACL in each direction cannot be applied 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 the ACL lookup.
- In the same rule, you cannot have two not-equal-to (neq) operators.
- ACL is not supported in port channels.

Displaying ACL Policies on the VEM

Use the following commands to display configured ACL policies on the Virtual Ethernet Module (VEM):

- Command to list the ACLs installed on a 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)
```

  AclId is the local ACL ID for this VEM. RefCnt refers to the number of instances of this ACL in this VEM.

- 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, do the following:

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.

Procedure

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 all** command.

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

For the VEMs where the policy exists, or is being applied, enter the commands in the following 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 Configure the policy that was causing the verification error.

Step 9 Enter the **module vem** *module-number* **execute vemdpalog show all** command.

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

Step 11 Save the Telnet or SSH session buffer to a file. Copy the logfile created in bootflash.

Troubleshooting ACL Logging

Using the CLI to Troubleshoot ACL Logging on a VEM

Viewing Current Flows

You can view the current flows on a VEM by using the **vemcmd show aclflows stats** 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 view the active flows on a VEM by using the **vemcmd show aclflows** [**permit** | **deny**] command. If you do not specify permit or deny, the command displays both.

```
[root@esx /]# vemcmd show aclflows permit
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

To display internal ACL flow statistics, enter the **vemcmd show aclflows dbgstats** command. To clear all internal ACL flow debug statistics, enter the **vemcmd clear aclflows dbgstats** command.

ACL Logging Troubleshooting Scenarios

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 or Action	Purpose
Step 1	**show logging ip access-list status**	Verifies that the remote syslog server is configured properly.
Step 2	**vemcmd show acllog config**	Verifies ACL logging on the VEM.
Step 3	**vemcmd show aclflows dbgstats**	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 or Action	Purpose
Step 1	**show running-config aclmg**	Verifies that the **log** keyword is enabled.
Step 2	**show logging ip access-list status**	Verifies that ACL logging is configured properly.
Step 3	**vemcmd show acllog config**	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 or Action	Purpose
Step 1	**show logging ip access-list status**	Verifies that ACL logging is configured properly.
Step 2	**vemcmd show acllog config**	Verifies ACL logging on the VEM.
Step 3	**logging ip access-list cache max-deny-flows** *num*	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 or Action	Purpose
Step 1	**show logging ip access-list status**	Verifies that ACL logging is configured properly.
Step 2	**vemcmd show acllog config**	Verifies ACL logging on the VEM.

ACL Troubleshooting Commands

You can use the following commands on the VSM to see the policies that are configured and applied on the interfaces:

- Command to display configured ACLs: **show access-list summary**
- Commands to collect the run-time information of the ACLMGR during 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**
- **show system internal aclmgr status**
- **show system internal aclmgr dictionary**

- Commands to collect the run-time information of the ACLCOMP during 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**