Nexus 7000 and 7700 Series Switches Optimized ACL Logging Configuration Example

Document ID: 118907

Contributed by Richard Michael, Cisco TAC Engineer.
Apr 15, 2015

Contents

Introduction

This document describes how to configure Optimized Access Control List (ACL) Logging (OAL) on the Cisco Nexus 7000 and 7700 Series switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Nexus configurations with basic ACLs before you attempt the configuration that is described in this document.

Components Used

The information in this document is based on these hardware and software versions:

- Cisco Nexus 7000 Series switches
- Cisco Nexus 7700 Series switches

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Logging−enabled ACLs provide insight into traffic as it traverses the network or is dropped by network devices. Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions of the network device. In order to reduce CPU cycles, the Cisco Nexus 7000 Series switch uses OALs.

The use of OALs provides hardware support for ACL logging. The OAL permits or drops packets in the hardware and uses an optimized routine in order to send information to the Supervisor so that it can generate the logging messages. For example, when a packet hits an ACL with logging enabled while it is forwarded in the hardware, a copy of the packet is created in the hardware and the packet is punted to the Supervisor for logging in accordance with the time interval that is configured.

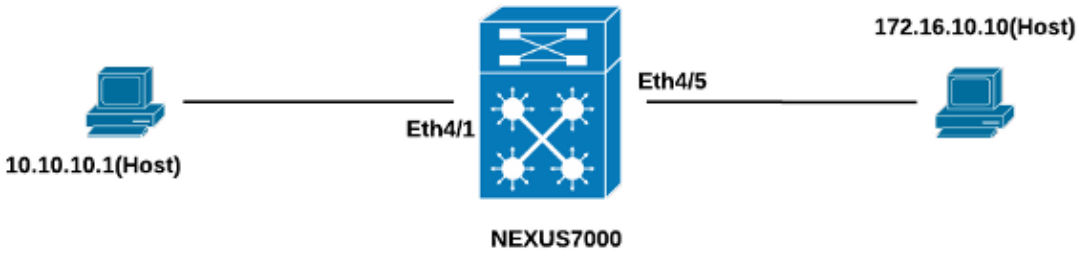
Configure

This section provides information that you can use in order to configure the Nexus switch for the use of OALs.

In the example that is described in this section, there is a host at IP address 10.10.10.1 that sends traffic to another host at IP address 172.16.10.10 through a Nexus 7000 Series interface, which has an ACL with logging configured.

Network Diagram

The connection between the hosts and the Nexus 7000 Series switch occurs as per this topology:



Configurations

Complete these steps in order to configure the switch for the use of OALs:

1. Configure these global commands in order to enable OAL:

```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
logging ip access-list cache threshold 0
```

Here is an example:

```
Nexus-7000# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. Apply this configuration for logging:

```
logging level acllog <number>
acllog match-log-level <number>
logging logfile [name] <number>
```

   Here is an example:

```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level  5
Nexus-7000(config)# logging logfile acllog 5
```

3. Configure the ACL in order to enable logging. The entries must be configured with the ***log*** keyword enabled, as shown in this example:

```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
Nexus-7000(config-acl)#
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
10 permit ip 10.10.10.1/32 172.16.10.10/32 log
20 deny ip any any log
Nexus-7000(config-acl)#
```

4. Apply the ACL that you configured in the previous step to the required interface:

```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
Nexus-7000(config-if)#
Nexus-7000(config-if)# show run int ethernet 4/1
!Command: show running-config interface Ethernet4/1
!Time: Mon Jun 30 16:30:38 2014
version 6.2(6)
interface Ethernet4/1
  ip access-group test1 in
  ip access-group test1 out
  ip address 10.10.10.2/24
  no shutdown
Nexus-7000(config-if)#
```

Verify

Use the information that is provided in this section in order to verify that your configuration works properly.

In the example that is used in this document, the ping is initiated from the host at IP address 10.10.10.1 to the host at IP address 172.16.10.1. Enter the ***show logging ip access-list cache*** command into the CLI in order to verify the traffic flow:

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

You can see the logging every 300 seconds, as this is the default time interval:

```
Nexus−7000# show logging logfile
2014 Jun 29 19:19:01 Nexus−7000 %SYSLOG−1−SYSTEM_MSG : Logging logfile (acllog)
 cleared by user
2014 Jun 29 19:20:57 Nexus−7000 %VSHD−5−VSHD_SYSLOG_CONFIG_I: Configured from vty by
 admin on console0
2014 Jun 29 19:21:18 Nexus−7000 %ACLLOG−5−ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
 Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
 "ICMP"(1), Hit−count = 2589
2014 Jun 29 19:26:18 Nexus−7000 %ACLLOG−5−ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
 Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
 "ICMP"(1), Hit−count = 4561
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Configuration Notes

This section provides additional information about the configuration that is described in this document.

Detailed ACL Logging

In Nexus Operating System (NX−OS) Releases 6.2(6) and later, *detailed* ACL logging is available. The feature logs this information:

- Source and destination IP addresses
- Source and destination ports
- Source interface
- Protocol
- ACL name
- ACL action (permit or deny)
- Applied interface
- Packet count

Enter the ***logging ip access−list detailed*** command into the CLI in order to enable detailed logging. Here is an example:

```
Nexus−7000(config)# logging ip access−list detailed
ACL Log detailed Logging feature is enabled. Hit−count of existing ACL Flow entry will
 be reset to zero and will contain Hit Count per ACL type Flow.
Nexus−7000(config)#
```

Here is an example logging output after detailed logging is enabled:

```
2014 Jul 18 02:20:38 Nexus7k−1−oal %ACLLOG−6−ACLLOG_FLOW_INTERVAL: Src IP: 10.10.10.1,
 Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/5, Protocol:
 "ICMP"(1), ACL Name: test1, ACE Action: Permit, Appl Intf: Ethernet4/5, Hit−count: 69
```

Global OAL Command Descriptions

This section describes the global OAL commands that are used in order to configure the Nexus 7000 Series switch for the use of OALs.

Command	*Description*
Switch(config)# logging ip access−list cache {{entries number_of_entries} | {interval seconds} | {rate−limit number_of_packets} | {threshold number_of_packets}}	This command sets the OAL global parameters.
Switch(config)# no logging ip access−list cache {entries | interval | rate−limit | threshold}	This command reverts the OAL global parameters to the default settings.
entries num_entries	These parameters specify the maximum number of log entries that are cached in the software. The range is 0 to 1,048,576. The default value is 8,000 entries.
interval seconds	These parameters specify the maximum time interval before an entry is sent to a syslog. The range is 5 to 86,400. The default value is 300 seconds.
threshold num_packets	These parameters specify the number of packet matches (hits) before an entry is sent to a syslog. The range is 0 to 1,000,000. The default value is 0 packets (rate limiting is off), which means that the system log is not triggered by the number of packet matches.

Note: The *no* form of these CLI commands only reverts the parameters to the default settings if they have been changed; it does not remove the configuration, as the Nexus 7000 Series switch only has the option of OAL.

Logging Command Descriptions

This section describes the logging commands that are used in order to configure the Nexus 7000 Series switch for the use of OALs.

Command	*Description*
switch(config)# acllog match−log− level number Example: switch(config)# acllog match−log− level 3	This command specifies the logging level that must be matched before entries are logged in the ACL log (acllog). The range is 0 to 7. The default is value is 6.
Switch(config)# no acllog match−log− level number Example: switch(config)# no acllog match−log− level 6	This command reverts the logging level to the default setting (6).
Switch(config)# logging level facility severity−level Example: switch(config)# logging level acllog 3	This command enables logging messages from the specified facility that have the specified severity level or higher. In the example that is used in this document, the *acllog* level is set to 3, whereas the default setting is 2.
Switch(config)# no logging level [facility severity−level] Example: switch(config)# no logging level acllog 3	This command resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the device resets all facilities to their default levels. In the example that is used in this document, the acllog is reverted to the default (2).
Switch(config)# logging logfile logfile−name severity−level [size bytes] Example: switch(config)# logging logfile acllog 3	This command configures the name of the log file that is used in order to store the system messages and the minimum severity level before logging occurs. You can optionally specify a maximum file size. The default severity level is 5, and the default file size is 10,485,760.
	This command disables logging to the log file.

Switch(config)# no logging
logfile [logfile−name
severity−level [size bytes]]
Example: switch(config)# no
logging logfile acllog 3

Note: In order for the log messages to be entered in the logs, the logging level for the ACL log facility (acllog) and the logging severity level for the logfile must be greater than or equal to the ACL log *match−log−leve*l setting.

Guidelines and Limitations

Here are some important guidelines and limitations that you should consider before you apply the configuration that is described in this document:

- The Nexus 7000 and 7700 Series switches support only OAL.
- ACL logging does not work with the ACL Capture feature.
- The *log* option in egress ACLs is not supported for multicast packets.
- Detailed logging support is not available for IPv6 packets.
- The logging level for the *acllog* facility and the *logging logfile* severity must be configured such that they are greater than or equal to the *acllog match−log−level* setting.
- Do not use the ***hardware access−list capture*** command while OAL is used. When this command is used alongside OAL, and you enable ACL capture, a warning message appears in order to inform you that ACL logging is being disabled for all Virtual Device Contexts (VDCs). When you disable ACL capture, ACL logging is enabled. In order for this process to work properly, disable with the use of the ***no hardware access−list capture*** command.

Updated: Apr 15, 2015 Document ID: 118907