Nexus 7000和7700系列交换机优化ACL日志记录配置示例

目录

简介

本文档介绍如何在Cisco Nexus 7000和7700系列交换机上配置优化访问控制列表(ACL)日志记录(OAL)。

先决条件

要求

思科建议您在尝试本文档中所述的配置之前，先了解使用基本ACL的Nexus配置。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- 思科 Nexus 7000 系列交换机
- 思科 Nexus 7700 系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

启用日志记录的ACL可在流量通过网络或被网络设备丢弃时提供对流量的洞察。遗憾的是，ACL日志记录可能会占用CPU的资源，并且会对网络设备的其他功能产生负面影响。为减少CPU周期，Cisco Nexus 7000系列交换机使用OAL。

使用OAL为ACL日志记录提供硬件支持。OAL允许或丢弃硬件中的数据包，并使用优化的例程将信息发送到Supervisor，以便其能够生成日志记录消息。例如，当数据包在硬件中转发时命中启用了日志记录的ACL时，会在硬件中创建数据包的副本，并且数据包会根据配置的时间间隔发送到管理引擎进行日志记录。

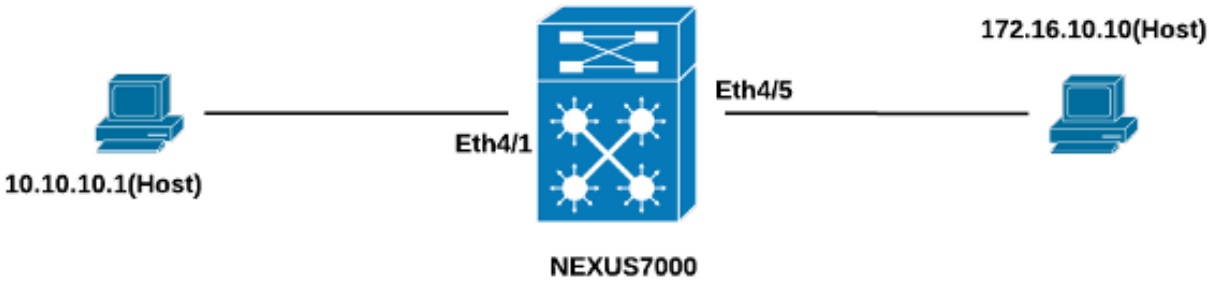
配置

本节提供可用于配置Nexus交换机以使用OAL的信息。

在本节介绍的示例中，有一台IP地址为10.10.10.1的主机通过Nexus 7000系列接口将流量发送到另一台IP地址为172.16.10.10的主机，该接口配置了ACL并配置了日志记录。

网络图

主机与Nexus 7000系列交换机之间的连接按照以下拓扑进行：



配置

要配置交换机以使用OAL，请完成以下步骤：

1. 配置以下全局命令以启用OAL:

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

示例如下：

```
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. 将此配置应用于日志记录：

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

示例如下：

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

3. 配置ACL以启用日志记录。必须在启用log关键字的情况下配置这些条目，如本例所示：

```
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. 将您在上一步中配置的ACL应用到所需接口：

```
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)#
```

验证

使用本节中提供的信息验证配置是否正常工作。

在本文档中使用的示例中，从IP地址为10.10.10.1的主机向IP地址为172.16.10.1的主机发起ping操作。在CLI中输入show logging ip access-list cache命令以验证流量：

```
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#
```

您可以每300秒查看一次日志记录，因为这是默认时间间隔：

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

配置注释

本节提供有关本文档中描述的配置的其他信息。

详细的ACL日志记录

在Nexus操作系统(NX-OS)版本6.2(6)及更高版本中，可*以使*用详细的ACL日志记录。功能记录以下信息：

- 源和目的 IP 地址
- 源端口和目的端口
- 来源接口
- 协议
- ACL 名称
- ACL操作（允许或拒绝）
- 应用的接口
- 数据包计数

在CLI中**输入logging ip access-list detailed命令以启**用详细日志记录。示例如下：

```
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)#
```

以下是启用详细日志记录后的日志记录输出示例：

```
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
```

全局OAL命令说明

本节介绍用于配置Nexus 7000系列交换机以使用OAL的全局OAL命令。

命令	
Switch(config)# logging ip access-list cache {{entries number_of_entries} | {间隔秒数} | {rate-limit number_of_packets} | {threshold number_of_packets}}	此命令设置OAL全局参数。
Switch(config)# no logging ip access-list cache {entries |间隔 |速率限制 |阈值	此命令将OAL全局参数恢复为默认设置。
条目 num_entries	这些参数指定在软件中缓存的最大日志条目数。范围为0到1,048,576。默认值为8,00
间隔 秒	这些参数指定将条目发送到系统日志之前的最大时间间隔。范围为5至86,400。默认
阈值 num_packets	这些参数指定在条目发送到系统日志之前数据包匹配（命中）的数量。范围为0到1,0

注意：这些CLI命令的*no*形式仅在参数已更改时将其恢复为默认设置；它不会删除配置，因为Nexus 7000系列交换机只有OAL选项。

日志记录命令说明

本节介绍配置Nexus 7000系列交换机以使用OAL时使用的日志记录命令。

命令	
switch(config)# acllog match-log-level number 示例：switch(config)# acllog match-log-level 3	此命令指定在条目记录到ACL日志(acllog)之前必须匹配的日志记录级别。 范围为0至
Switch(config)# no acllog match-log-level number 示例：switch(config)# no acllog match-log-level 6	此命令将日志记录级别恢复为默认设置(6)。
Switch(config)#	此命令启用来自指定严重性级别或更高级别的设施的日志记录消息。在本文档中使用

logging level facility severity-level 示例：switch(config)# logging level acllog 3	
Switch(config)# no logging level [facility severity-level] 示例：switch(config)# no logging level acllog 3	此命令将指定设施的日志记录严重性级别重置为其默认级别。如果未指定设施和严重 级别，设备将所有设施重置为其默认级别。在本文档中使用的示例中，acllog恢复为
Switch(config)# logging logfile logfile-name severity-level [size bytes] 示例：switch(config)# logging logfile acllog 3	此命令配置用于存储系统消息的日志文件的名称以及发生日志记录之前的最低严重级
Switch(config)# no logging logfile [logfile-name severity-level [size bytes]] 示例：switch(config)# no logging logfile acllog 3	此命令禁用日志记录到日志文件。

> **注意：**为了在日志中输入日志消息，ACL日志工具(acllog)的日志记录级别和日志文件的日志记录严重性级别必须大于或等于ACL日志*match-log-level*设置。

准则和限制

在应用本文档中描述的配置之前，您应考虑以下一些重要准则和限制：

- Nexus 7000和7700系列交换机仅支持OAL。
- ACL日志记录与ACL捕获功能不兼容。
- 对于组播数据包，*出口ACL*中的log选项不受支持。
- IPv6数据包不提供详细的日志记录支持。
- 必须配置*acllog*工具的日志记录级别和*日志记录日志文件*严重性，使其大于或等于*acllog match-log-level设置*。
- 在使用OAL时，请勿使用**hardware access-list capture**命令。当此命令与OAL一起使用，并且您启用ACL捕获时，将显示一条警告消息，以通知您所有虚拟设备环境(VDC)的ACL日志记录已禁用。 禁用ACL捕获时，ACL日志记录将启用。要使此过程正常工作，请使用no hardware access-list capture**命令禁用该**过程。