连结7000和7700系列交换机优化ACL记录配置示例

目录

简介

本文描述如何配置记录(OAL)在Cisco连结7000和7700系列交换机的优化访问控制表(ACL)。

先决条件

要求

思科建议您有连结配置知识与基本ACL的，在您尝试在本文描述的配置前。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- Cisco Nexus 7000系列交换机
- Cisco连结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

当穿程网络或由网络设备，丢弃记录日志启用的ACL提供见解到流量。不幸地， ACL记录强化中央处理，并且能负影响网络设备的其他功能。为了减少CPU周期， Cisco连结7000系列交换机使用OALs。

使用OALs为ACL记录提供硬件支持。OAL在硬件里允许或丢弃数据包并且使用一优化惯例为了发送信息到Supervisor，以便能生成日志消息。例如，当数据包押与启用时的记录日志的ACL，当在硬件里时转发，数据包的复制在硬件里创建，并且数据包被踢到登陆的符合Supervisor与配置的时间间隔。

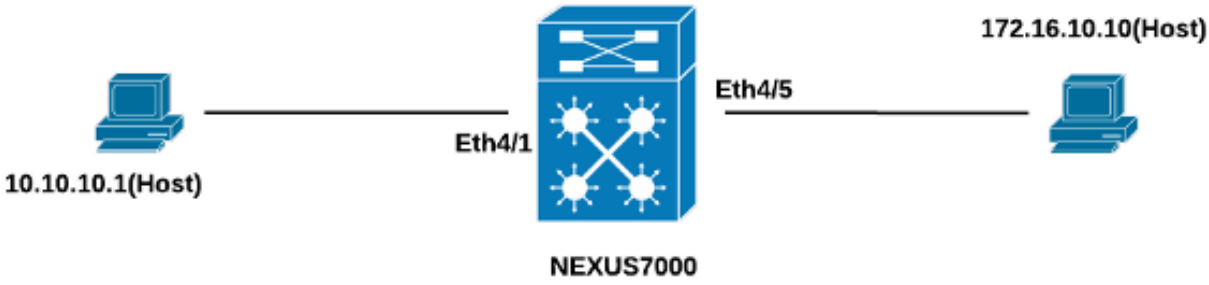
配置

此部分提供您能使用为了配置连结交换机为使用OALs的信息。

在此部分描述，有主机在IP地址10.10.10.1发送流量到另一台主机在IP地址172.16.10.10通过连结7000系列接口，有与配置的记录日志的ACL的示例中。

网络图

主机和连结7000系列交换机之间的连接根据此拓扑发生：



配置

完成这些步骤为了配置交换机为使用OALs ：

1. 配置这些global命令为了启用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. 申请此配置记录：

```
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
```

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为了启用日志。必须配置条目与**日志关键字**启用，如此示例所显示：

```
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. 应用该的ACL您配置在上一步对必需的接口：

```
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

请使用在此部分被提供为了验证的信息您的配置适当地工作。

在本文使用的示例中， ping从在IP地址10.10.10.1的主机启动对在IP地址172.16.10.1的主机。进入**cache命令show logging的IP访问控制列表**到CLI为了验证通信流：

```
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#
```

您能看到记录日志每300秒，和这默认时间时间间隔：

```
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

此部分提供关于在本文描述的配置的其他信息。

详细的ACL记录

在连结操作系统的(NX-OS)版本6.2(6)及以后，*详细的*ACL记录是可用的。功能记录此信息：

- 源和目的 IP 地址
- 源端口和目的端口
- 源接口
- 协议
- ACL名称
- ACL操作(permit或拒绝)
- 已应用接口
- 数据包计数

进入**detailed命令记录日志的IP访问控制列表**到CLI为了启用详细日志。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)#
```

这是示例操作日志输出，在详细日志启用后：

```
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)#
```

全局OAL命令描述

此部分描述使用为了配置连结7000系列交换机为使用OALs的全局OAL命令。

命令	
记录IP访问控制列表缓存的Switch(config)- {{条目number_of_entries}|{间隔秒钟}|{速率限制number_of_packets}|{阈值number_of_packets}}	此命令设置

Switch(config)- no logging IP访问控制列表缓存{条目|间隔|速率限制|阈值} 条目 num_entries 间隔 秒钟 阈值 num_packets	此命令恢复 这些参数指 在条目发送 这些参数指

注意：如果他们更改，这些CLI命令*no表示*只恢复参数对默认设置;因为连结7000系列交换机只有OAL的选项，它不删除配置。

logging命令说明

此部分描述使用为了配置连结7000系列交换机为使用OALs的记录日志命令。

命令	
switch(config)- acllog匹配LOG级别数 **示例**：switch(config)- acllog匹配LOG 3级	此命令指定必须匹配的日志级别，在条目登陆ACL日志前(acllo
Switch(config)-没有acllog匹配LOG级别数 **示例**：switch(config)-没有acllog匹配LOG级别6	此命令恢复日志级别对默认设置(6)。
Switch(config)-日志级别设备严重级别 **示例**：switch(config)-日志级别acllog 3	此命令启用有指定的严重级别或更加高从指定的设备的日志消
Switch(config)- no logging级别[facility severity-level] **示例**：switch(config)- no logging级别acllog 3	此命令重置指定的设备的记录日志严重级别对其默认级别。如果成水平，设备重置所有设施对他们的默认级别。在本文使用的
记录日志文件日志文件NAME严重级别[size bytes]的Switch(config)- **示例**：记录日志文件acllog 3的switch(config)-	此命令配置使用为了存储系统消息和最低的严重级别日志文件的
Switch(config)- no logging日志文件[logfile-name severity-level [size bytes]] **示例**：switch(config)- no logging日志文件acllog 3	此命令禁用记录日志到日志文件。

注意：为了在日志能将输入的日志消息， ACL日志设备的(acllog)日志级别和日志文件的记录日志严重级别必须是大于或等于ACL日志匹配LOG*级别*设置。

指南和限制

这是您应该考虑的一些重要指南和限制，在您运用在本文描述的配置前：

- 连结7000和7700系列交换机支持仅OAL。
- ACL记录不与ACL捕获功能一起使用。
- 在出口ACL的*日志*选项不为组播信息包支持。

- 详细日志支持为IPv6数据包不是可用的。

- *必须*配置*acllog*设备和*记录日志日志文件*严重性的日志级别这样他们是大于或等于*acllog匹配LOG级别*设置。

- 当使用时，请勿使用**access-list capture命令的硬件**OAL。 当此命令沿着OAL和您使用enable (event) ACL捕获时，警告消息出现为了通知您ACL记录为所有虚拟设备上下文(VDCs)禁用。当您禁用ACL捕获时， ACL记录启用。为了此进程能适当地工作，与**access-list capture命令**使用的禁用**没有的硬件**。