Nexus 7000和7700系列交換機最佳化ACL日誌記錄配置示例

目錄

簡介

本檔案介紹如何在Cisco Nexus 7000和7700系列交換器上設定最佳化存取控制清單(ACL)記錄(OAL)。

必要條件

需求

思科建議您在嘗試本文檔中所述的配置之前，先瞭解具有基本ACL的Nexus配置。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Cisco Nexus 7000 系列交換器
- Cisco Nexus 7700 系列交換器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

啟用日誌記錄的ACL可深入瞭解流量穿越網路或被網路裝置丟棄的情況。遺憾的是，ACL日誌記錄會佔用大量的CPU資源，而且可能對網路裝置的其他功能產生負面影響。為了減少CPU週期，Cisco Nexus 7000系列交換機使用OAL。

OAL的使用為ACL記錄提供硬體支援。OAL允許或丟棄硬體中的資料包，並使用最佳化的常式向Supervisor傳送資訊，以便其生成日誌記錄消息。例如，當資料包在硬體中轉發時到達啟用了日誌記錄的ACL時，會在硬體中建立資料包的副本，並將資料包轉發到Supervisor以根據配置的時間間隔進行記錄。

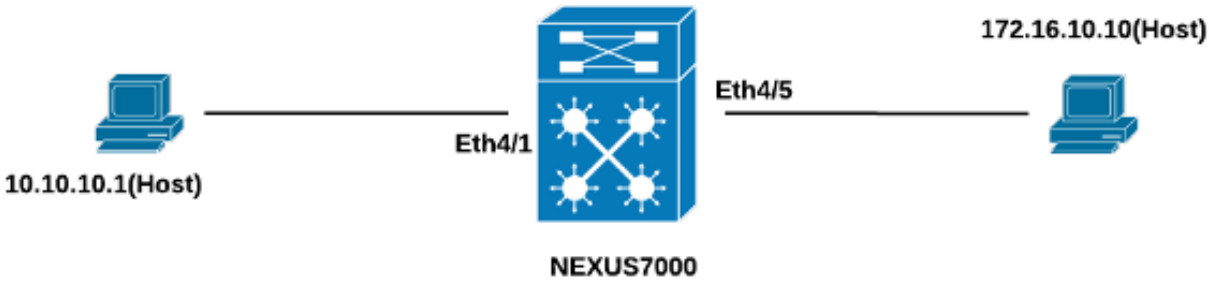
設定

本節提供的資訊可用於配置Nexus交換機以使用OAL。

在本節介紹的示例中，IP地址為10.10.10.1的主機通過Nexus 7000系列介面將流量傳送到IP地址為172.16.10.10的另一台主機，該介面具有配置有日誌記錄的ACL。

網路圖表

主機和Nexus 7000系列交換機之間的連線按照以下拓撲進行：



組態

完成以下步驟，設定交換器以使用OAL:

1. 設定以下全域命令以啟用OAL:

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

以下是範例：

```
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. 將此配置應用於日誌記錄：

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

以下是範例：

```
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以啟用日誌記錄。必須在啟用了log關鍵字的情況下配置條目，如以下示例所示：

```
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. 將您在上一步中配置的ACL應用到所需的介面：

```
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)#
```

驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

在本文檔中使用的示例中，從IP地址為10.10.10.1的主機向IP地址為172.16.10.1的主機啟動ping。在CLI中輸入show logging ip access-list cache命令以驗證流量：

```
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#
```

您可以看到每300秒的日誌記錄，因為這是預設的時間間隔：

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

疑難排解技術筆記

本節提供有關本檔案中所述配置的其他資訊。

詳細的ACL記錄

在Nexus作業系統(NX-OS)版本6.2(6)及更高版本中，詳細的*ACL*日誌記錄可用。該功能記錄以下資訊：

- 源和目標IP地址
- 來源和目的地連線埠
- 源介面
- 通訊協定
- ACL名稱
- ACL操作（允許或拒絕）
- 應用的介面
- 資料包計數

在CLI中輸入**logging ip access-list detailed**命令以啟用詳細日誌記錄。以下是範例：

```
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)#
```

以下是啟用詳細記錄後記錄輸出的範例：

```
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
```

全域性OAL命令說明

本節介紹用於配置Nexus 7000系列交換機以使用OAL的全域性OAL命令。

指令	
Switch(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packets} | {threshold number_of_packets}	此命令設定OAL全域性引數。
Switch(config)# no logging ip access-list cache {entries |間隔 | rate-limit |閾值}	此命令將OAL全域性引數還原為預設設定。
條目 num_entries	這些引數指定在軟體中快取的最大日誌條目數。範圍為0至1,048,576。預設值為8,000
間隔 秒	這些引數指定將條目傳送到系統日誌之前的最大時間間隔。範圍為5到86,400。預設值
閾值 num_packets	這些引數指定在將條目傳送到系統日誌之前資料包匹配（命中）的數量。範圍為0到1

附註：這些CLI命令的*no*形式僅在引數已更改時將其還原為預設設定；它不會刪除配置，因為Nexus 7000系列交換機只具有OAL選項。

Logging命令說明

本節介紹用於配置Nexus 7000系列交換機以使用OAL的logging命令。

指令	說
switch(config)# acllog match-log-level number 範例：switch(config)# acllog match-log-level 3	此命令指定在ACL日誌(acllog)中記錄條目之前必須匹配的日誌記錄級別。 範圍為0至
Switch(config)# no acllog match-log-level number 範例：switch(config)# no acllog match-log-level 6	此命令將日誌記錄級別還原為預設設定(6)。

Switch(config)# logging level facility severity-level 範例：switch(config)# logging level acllog 3	此命令啟用指定設施中具有指定嚴重性級別或更高級別的日誌記錄消息。在本文檔中
Switch(config)# no logging level [facility severity-level] 範例：switch(config)# no logging level acllog 3	此命令將指定設施的日誌記錄嚴重性級別重置為其預設級別。如果不指定設施和嚴重級別，裝置會將所有合作室重置為其預設級別。在本文檔中使用的示例中，acl日誌
Switch(config)# logging logfile logfile-name severity-level [size bytes] 範例：switch(config)# logging logfile acllog 3	此命令配置用於儲存系統消息的日誌檔案的名稱，以及日誌記錄之前的最低嚴重性級
Switch(config)# no logging logfile [logfile-name severity-level [size bytes]] 範例：switch(config)# no logging logfile acllog 3	此命令禁用日誌記錄到日誌檔案。

> **附註**：要在日誌中輸入日誌消息，ACL日誌設施(acllog)的日誌級別和日誌檔案的日誌嚴重性級別必須大於或等於ACL日誌*match-log-level*設置。

准則和限制

以下是應用本檔案所述的設定之前，您應該考慮的一些重要原則與限制：

- Nexus 7000和7700系列交換機僅支援OAL。
- ACL日誌記錄不能與ACL捕獲功能配合使用。
- 組播資料包不支援輸出ACL中的*log*選項。
- 詳細日誌記錄支援不可用於IPv6資料包。
- 必須配置*acllog*設施的日誌記錄級別和*logging logfile*嚴重性，以使其大於或等於*acllog match-log-level* 設定。
- 在使用OAL時，請勿使用**hardware access-list capture**命令。當此命令與OAL一起使用時，當您啟用ACL捕獲時，將顯示一條警告消息，通知您正在禁用所有虛擬裝置上下文(VDC)的ACL日誌記錄。 禁用ACL捕獲時，將啟用ACL日誌記錄。為了使該過程正常工作，請使用**no hardware access-list capture**命令禁用。