Nexus 7000系列交換機ACL捕獲示例

目錄

簡介

訪問控制清單(ACL)捕獲允許您選擇性地捕獲介面或虛擬區域網(VLAN)上的流量。當您為ACL規則啟用捕獲選項時，將根據指定的允許或拒絕操作轉發或丟棄與此規則匹配的資料包，還可以將其複製到備用目標埠以進行進一步分析。可以應用帶捕獲選項的ACL規則：

1. 在VLAN中，
2. 在所有介面的輸入方向上，
3. 在所有第3層介面上處於輸出方向。

Nexus 7000 NX-OS版本5.2及更高版本支援此功能。本文檔提供了一個示例，作為如何配置此功能的快速參考指南。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Nexus 7000（5.2.x及更高版本）。
- M1系列線卡。

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。

慣例

如需檔案慣例的相關資訊，請參閱思科技術提示慣例。

ACL配置示例

以下是應用於VLAN的ACL擷取組態範例，也稱為虛擬LAN存取控制清單(VACL)擷取。指定的十千兆位嗅探器可能並非對所有場景都可行。在此類場景中，選擇性流量捕獲非常有用，尤其是在流量量大的故障排除過程中。

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

您還可以檢查訪問清單的三重內容可定址儲存器(TCAM)程式設計。此輸出適用於模組1的VLAN 500。

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------

Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
```

```
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

注意事項

1. 在系統中的任何指定時間，只能跨虛擬裝置環境(VDC)啟用一個ACL捕獲會話。
2. Nexus 7000 F1系列模組不支援ACL擷取。
3. Nexus 7000 F2系列模組當前不支援ACL捕獲，但可能會在規劃圖中進行此操作。
4. Cisco NX-OS版本6.1(1)及更高版本支援Nexus 7000 M2系列模組上的ACL捕獲。
5. Cisco NX-OS版本5.2(1)及更高版本支援Nexus 7000 M1系列模組上的ACL捕獲。
6. ACL捕獲與ACL日誌記錄不相容。 因此，如果您的ACL中有一個**log**關鍵字，則這些關鍵字在您全域性輸入**hardware access-list capture**後不起作用。
7. 由於CSCug20139錯誤，本文檔中的示例使用**capture session**記錄了每個ACE而不是每個ACL，直到錯誤被解決。

相關資訊

- Cisco Nexus 7000系列NX-OS安全配置指南6.x版IP ACL配置示例
- 技術支援與文件 - Cisco Systems