Nexus 7000系列交换机ACL捕获示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[ACL配置示例](#)
[注意事项](#)
[相关信息](#)

简介

访问控制列表(ACL)捕获提供选择性捕获接口或虚拟局域网(VLAN)上的流量的能力。为ACL规则启用捕获选项时，会根据指定的允许或拒绝操作转发或丢弃与此规则匹配的数据包，并且还可以复制到备用目标端口进行进一步分析。可应用带捕获选项的ACL规则：

1. 在VLAN中，
2. 在所有接口的入口方向上，
3. 在所有第3层接口的出口方向。

Nexus 7000 NX-OS版本5.2及更高版本支持此功能。本文档提供了一个示例，作为有关如何配置此功能的快速参考指南。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带5.2.x及更高版本的Nexus 7000。
- M1系列线卡。

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。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

ACL配置示例

以下是应用于VLAN的ACL捕获的示例配置，也称为虚拟LAN访问控制列表(VACL)捕获。指定的10千兆位剪刀可能不适用于所有场景。选择性流量捕获在这种场景中非常有用，特别是在流量较大时进行故障排除时。

```
!! 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
```

您还可以检查访问列表的三重内容可寻址存储器(TCAM)编程。此输出适用于模块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]
```

注意事项

1. 在系统中的任意给定时间，在虚拟设备环境(VDC)中，只能有一个ACL捕获会话处于活动状态。
2. Nexus 7000 F1系列模块不支持ACL捕获。
3. Nexus 7000 F2系列模块目前不支持ACL捕获，但这可能已在规划图中。
4. Cisco NX-OS 6.1(1)版及更高版本支持Nexus 7000 M2系列模块上的ACL捕获。
5. Cisco NX-OS版本5.2(1)及更高版本支持Nexus 7000 M1系列模块上的ACL捕获。
6. ACL捕获与ACL日志记录不兼容。 因此，如果您有带有log关键字的ACL，则在您全局输入硬件访问列表捕获后，**这些ACL将无法运行**。
7. 由于Bug CSCug20139，本文档中的示例在解决Bug之前，记录为每个ACE（而不是每个ACL）**捕获**会话。

相关信息

- **Cisco Nexus 7000系列NX-OS安全配置指南，版本6.x，IP ACL配置示例**
- **技术支持和文档 - Cisco Systems**