使用运行 CatOS 软件的 Cisco Catalyst 6000/6500 执行 VACL 捕获以进行细致的流量分析

目录

简介

本文档提供了使用VLAN访问控制列表(ACL)(VACL)捕获端口功能以更精细的方式进行网络流量分析的示例配置。本文档还说明了VACL捕获端口使用与基于VLAN的交换端口分析器(SPAN)(VSPAN)使用相比的优势。

要在运行Cisco IOS®软件的Cisco Catalyst 6000/6500上配置VACL捕获端口功能，请参阅VACL捕获以使用运行Cisco IOS软件的Cisco Catalyst 6000/6500进行精细流量分析。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 虚拟LAN — 有关详细信息，请参阅虚拟LAN/VLAN中继协议(VLAN/VTP) — 简介。
- 访问列表 — 有关详细信息，请参阅配置访问控制。

使用的组件

本文档中的信息基于运行Catalyst OS版本8.1(2)的Cisco Catalyst 6506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。

相关产品

此配置也可用于运行Catalyst OS版本6.3及更高版本的Cisco Catalyst 6000/6500系列交换机。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

基于VLAN的SPAN

SPAN将流量从任何VLAN中的一个或多个源端口或从一个或多个VLAN复制到目的端口以进行分析。本地 SPAN 支持源端口、源 VLAN 和目标端口位于同一台 Catalyst 6500 系列交换机上。

源端口是为进行网络流量分析而进行监控的端口。源 VLAN 是为进行网络流量分析而进行监控的 VLAN。基于VLAN的SPAN(VSPAN)是对一个或多个VLAN中的网络流量进行分析。您可以将VSPAN配置为入口SPAN、出口SPAN或两者。源VLAN中的所有端口都成为VSPAN会话的可操作源端口。目标端口（如果它们属于任何管理源VLAN）从运行源排除。如果从管理源VLAN添加或删除端口，则操作源会相应修改。

VSPAN会话准则：

- 中继端口作为VSPAN会话的源端口，但如果这些VLAN对于中继处于活动状态，则仅监控Admin源列表中的VLAN。
- 对于配置了入口和出口SPAN的VSPAN会话，系统根据您拥有的管理引擎类型运行：WS-X6K-SUP1A-PFC、WS-X6K-SUP1A-MSFC、WS-X6K-S1A-MSFC2、WS-X6K-S2-PFC2、WS-X6K-S1S1S1S1AAS1AAMSFC2、WS-SUP720、WS-SUP32-GE-3B — 如果数据包在同一VLAN上交换，则SPAN目标端口会转发两个数据包。WS-X6K-SUP1-2GE、WS-X6K-SUP1A-2GE - SPAN目标端口仅转发一个数据包。
- 带内端口不作为VSPAN会话的运行源。
- 清除VLAN后，会从VSPAN会话的源列表中删除该VLAN。
- 如果管理员源VLAN列表为空，则VSPAN会话被禁用。
- VSPAN配置不允许非活动VLAN。
- 如果任何源VLAN成为RSPAN VLAN，则VSPAN会话将变为非活动状态。

有关源VLAN的详细信息，请参阅源VLAN的特征。

VLAN ACL

VACL可以访问控制所有流量。您可以配置交换机上的VACL，以应用于路由到VLAN或从VLAN路由或在VLAN内桥接的所有数据包。VACL严格用于安全数据包过滤和将流量重定向到特定物理交换机

端口。与Cisco IOS ACL不同，VACL不是按方向（输入或输出）定义的。

您可以在第3层地址上为IP和IPX配置VACL。所有其它协议都通过MAC地址和使用MAC VACL的EtherType进行访问控制。IP流量和IPX流量不受MAC VACL控制。所有其他流量类型（AppleTalk、DECnet等）均归类为MAC流量。MAC VACL用于访问控制此流量。

VACL中支持的ACE

VACL包含访问控制条目(ACE)的有序列表。 每个VACL只能包含一种类型的ACE。每个ACE都包含与数据包内容匹配的多个字段。每个字段都可以有一个相关的位掩码，以指示哪些位相关。操作与每个ACE关联，该操作描述在发生匹配时系统应如何处理数据包。操作取决于功能。Catalyst 6500系列交换机在硬件中支持三种类型的ACE:

- IP ACE
- IPX ACE
- 以太网ACE

下表列出了与每个ACE类型关联的参数：

ACE类型	TCP或UDP	ICMP	其他IP	IPX	以太网
第4层参数	源端口	-	-	-	-
	源端口操作员	-	-	-	-
	目标端口	-	-	-	-
	目标端口运营商	ICMP代码	-	-	-
	不适用	ICMP类型	不适用	-	-
第3层参数	IP ToS字节	IP ToS字节	IP ToS字节	-	-
	IP 源地址	IP 源地址	IP 源地址	IPX源网络	-
	IP 目的地址	IP 目的地址	IP 目的地址	IP目的网络	-
	-	-	-	IP目标节点	-
	TCP或UDP	ICMP	其他协议	IPX数据包类型	-
第2层参数	-	-	-	-	EtherType
	-	-	-	-	以太网源地址
	-	-	-	-	以太网目的地址

使用 VACL 相对于使用 VSPAN 的优势

使用 VSPAN 进行流量分析有多种限制：

- 所有流入 VLAN 的第 2 层流量都将被捕获。这会增加要分析的数据量。
- 可以在 Catalyst 6500 系列交换机上配置的 SPAN 会话数是有限的。有关详细信息，请参阅功能摘要和限制。
- 目标端口将接收所有受控源端口发送和接收的流量的副本。如果目标端口使用过度，则可能发生拥塞。这种拥塞会影响一个或多个源端口上转发的流量。

VACL 捕获端口功能可帮助克服其中一些限制。VACL主要不用于监控流量。但是，由于具备广泛的流量分类功能，因此引入了捕获端口功能，因此网络流量分析可以变得简单得多。下面是使用 VACL 捕获端口相对于使用 VSPAN 的优势：

- 细致的流量分析VACL 可以根据源 IP 地址、目标 IP 地址、第 4 层协议类型、源和目标第 4 层端口以及其他信息进行匹配。此功能使 VACL 非常适用于进行细致的流量标识和过滤。
- 会话数VACL在硬件中实施。可创建的ACE数量取决于交换机中可用的TCAM。
- 目标端口超额订阅细致的流量标识可减少转发到目标端口的帧数，因而可以最大限度地降低其超额订阅的可能性。
- 性能VACL在硬件中实施。在 Cisco Catalyst 6500 系列交换机上对 VLAN 应用 VACL 不会产生性能影响.

配置

本部分提供有关如何配置本文档所述功能的信息。

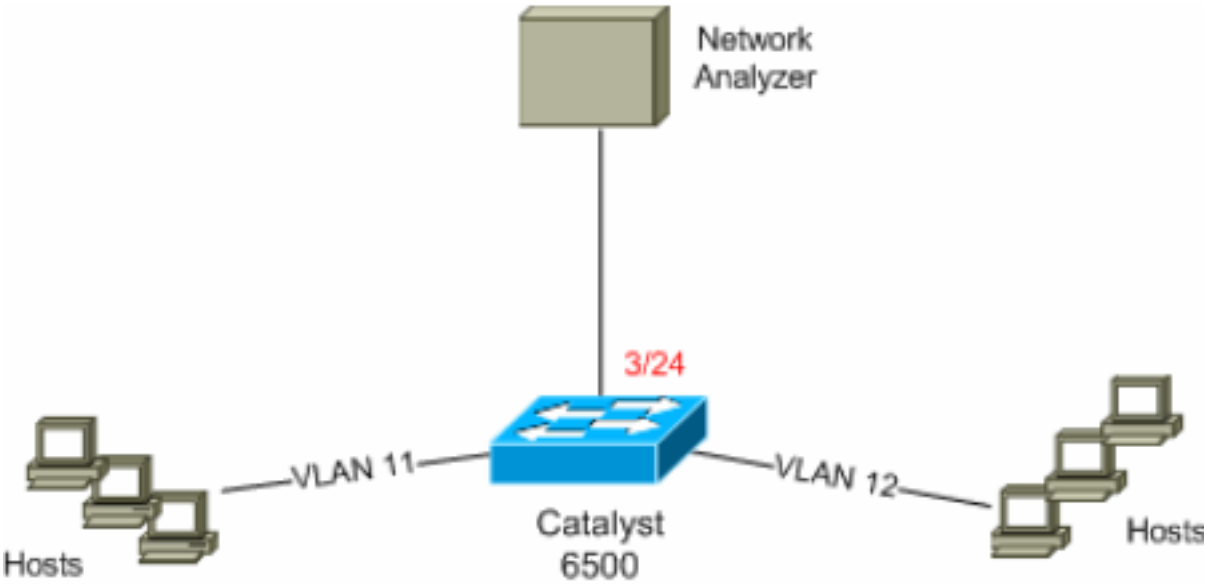
本文档使用以下配置：

- 基于 VLAN 的 SPAN 配置
- VACL 配置

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



基于 VLAN 的 SPAN 配置

此配置示例列出捕获VLAN 11和VLAN 12中流动的所有第2层流量并将其发送到网络分析器设备所需的步骤。

1. 指定关注的流量。在本例中，流入VLAN 100和VLAN 200的流量。

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

因此，所有属于VLAN 11和VLAN 12的第2层流量都会被复制并发送到端口3/24。

2. 使用show span all命令检验SPAN配置。

```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

VACL 配置

在本配置示例中，网络管理员有多个需求：

- 需要捕获从VLAN 12中的主机范围(10.12.12.128/25)到VLAN 11中特定服务器(10.11.11.100)的HTTP流量。
- 发往组地址239.0.0.100的传输方向的组播用户数据报协议(UDP)流量需要从VLAN 11捕获。

1. 使用安全ACL定义相关流量。请记住，要为定义的所有ACE提供关键字capture。

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
```

```
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. 验证ACE配置是否正确以及顺序是否正确。

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. 将ACL提交到硬件。

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. 检验ACL的状态。

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. 将 VLAN 访问映射应用于相应的 VLAN。

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. 检验ACL到VLAN的映射。

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. 配置捕获端口。

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

注意：如果ACL映射到多个VLAN，则必须将捕获端口配置到所有这些VLAN。要使捕获端口允许多个VLAN，请将端口配置为中继，并仅允许映射到ACL的VLAN。例如，如果ACL映射到VLAN 11和12，则完成配置。

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. 检验捕获端口配置。

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show security acl info** — 显示当前配置或最后提交到NVRAM和硬件的VACL内容。

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```

- **show security acl map** — 显示特定ACL、端口或VLAN的ACL到VLAN或ACL到端口的映射。

```
6K-CatOS> (enable) show security acl map all
ACL Name                         Type Vlans
-------------------------------- ---- -----
HttpUdp_Acl                         IP   11
6K-CatOS> (enable)
```

- **show security acl capture-ports** — 显示捕获端口列表。

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 使用运行 Cisco IOS 软件的 Cisco Catalyst 6000/6500 执行 VACL 捕获已进行粒度流量分析
- 配置访问控制 — Catalyst 6500系列软件配置指南，8.6
- LAN 产品支持页
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems