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

目录

简介

本文提供一个示例配置，用以说明如何使用 VLAN ACL (VACL) 捕获端口功能进行更为细致的网络流量分析。本文还介绍了使用 VACL 捕获端口相对于使用基于 VLAN 的 SPAN (VSPAN) 的优势。

要在运行 Catalyst OS 软件的 Cisco Catalyst 6000/6500 上配置 VACL 捕获端口功能，请参阅 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。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- IP 访问列表：有关更多信息，请参阅配置 IP 访问列表。
- 虚拟局域网：有关更多信息，请参阅VLAN 中继协议 (VLANs/VTP) - 简介。

使用的组件

本文档中的信息基于以下软件和硬件版本：运行Cisco IOS®软件版本12.2(18)SXF8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

此配置也可以用于运行 Cisco IOS 软件版本 12.1(13)E 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 （交换端口分析程序）将来自任意 VLAN 中一个或多个源端口或来自一个或多个 VLAN 的数据流复制到目标端口进行分析。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 VLAN 是为进行网络流量分析而进行监控的 VLAN。基于 VLAN 的 SPAN (VSPAN) 使用 VLAN 作为 SPAN 的源。源 VLAN 中的所有端口将成为源端口。源端口是为进行网络流量分析而进行监控的端口。中继端口可以配置为源端口并与非中继源端口混合，但 SPAN 不会从源中继端口复制封装。

对于配置了入口和出口的 VSPAN 会话，如果数据包已在同一个 VLAN 上进行交换，则会从目标端口转发两个数据包（一个作为来自输入端口的入口数据流，一个作为来自输出端口的出口数据流）。

VSPAN 只监控离开或进入 VLAN 中第 2 层端口的流量。

- 如果您将某个 VLAN 配置为输入源并将数据流路由到所监控的 VLAN 中，则不会监控路由的数据流，因为该数据流永远也不会成为进入 VLAN 中第 2 层端口的入口流量。
- 如果您将某个 VLAN 配置为输出源并将数据流路由出所监控的 VLAN，则不会监控路由的数据流，因为该数据流永远也不会成为离开 VLAN 中第 2 层端口的出口流量。

有关源 VLAN 的更多信息，请参阅源 VLAN 的特性。

VLAN ACL

VACL 可以为在 VLAN 内桥接的所有数据包或路由到或路由出 VLAN 或广域网接口的所有数据包提供访问控制以进行 VACL 捕获。与仅在路由器接口上进行配置并仅在所路由的数据包上应用的常规 Cisco IOS 标准或扩展 ACL 不同，VACL 应用于所有数据包，并且可以应用于任何 VLAN 或广域网接口。VACL 在硬件中处理。VACL 使用 Cisco IOS ACL。VACL 忽略硬件中不支持的所有 Cisco IOS ACL 字段。

您可以为 IP、IPX 和 MAC 层流量配置 VACL。应用于广域网接口的 VACL 仅支持 IP 流量进行

VACL 捕获。

当您配置 VACL 并将其应用于 VLAN 时，将根据此 VACL 检查进入 VLAN 的所有数据包。如果您将 VACL 应用于 VLAN，将 ACL 应用于 VLAN 中的路由接口，则先根据 VACL 检查进入 VLAN 的数据包，然后在允许的情况下，在由路由接口处理之前，根据输入的 ACL 检查数据包。在将数据包路由到其他 VLAN 时，先根据应用于路由接口的输出 ACL 检查数据包，然后在允许的情况下，应用为目标 VLAN 配置的 VACL。如果为某一数据包类型配置了 VACL 并且有一个属于该类型的数据包与 VACL 不匹配，则默认操作是拒绝。下面是在 VACL 中使用捕获选项的指导原则。

- 捕获端口不能是 ATM 端口。
- 对于 VLAN，捕获端口需要处于生成树转发状态。
- 交换机对捕获端口的数量没有限制。
- 捕获端口仅获取已配置的 ACL 允许的数据包。
- 捕获端口只传输属于捕获端口 VLAN 的流量。请将捕获端口配置为传送所需 VLAN 的中继，以便捕获进入很多 VLAN 的流量。

注意：ACL组合不正确可能会中断流量。在设备中配置 ACL 时要十分小心。

注意：Catalyst 6000系列交换机上的IPv6不支持VACL。换句话说，VLAN ACL 重定向和 IPv6 不兼容，因此 ACL 不能用于匹配 IPv6 流量。

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。有关更多信息，请参阅本地 SPAN 和 RSPAN 会话限制。
- 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 的主要设计用途并不是监控流量，但因为具有可对流量进行分类的多种功能，因而引入了捕获端口功能以使网络流量分析变得更加简单。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 在硬件中有强制要求；可创建的访问控制条目(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 在硬件中有强制要求；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

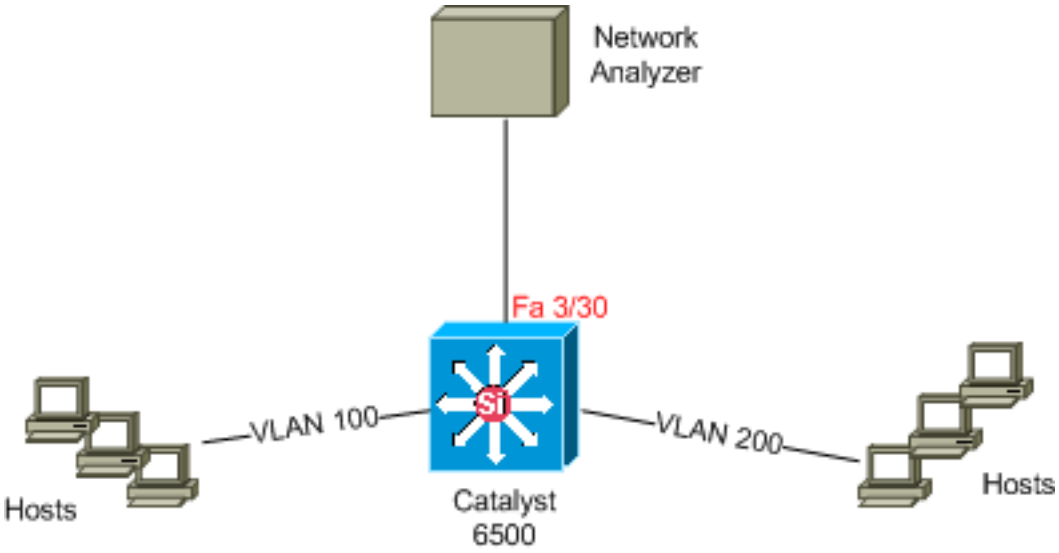
本部分提供有关如何配置本文档所述功能的信息。

- 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)可查找有关本文档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

本配置示例列出了捕获所有流入 VLAN 100 和 VLAN 200 的所有第 2 层流量并将这些流量发送到网络分析器设备所需的步骤。

1. 指定关注的流量。在本示例中，它是流入 VLAN 100 和 VLAN 200 的流量。

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. 为捕获的流量指定目标端口。

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

这样，属于VLAN 100和VLAN 200的所有第2层流量都会被复制并发送到端口Fa3/30。如果目标端口是受监控流量的同一VLAN的一部分，则不捕获从目标端口流出的流量。

用 **show monitor 命令验证您的 SPAN 配置。**

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
```

```
    RX Only       : None
    TX Only       : None
    Both          : 100,200
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs      : None
Dest RSPAN VLAN   : None
```

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 200 中一定范围内的主机 (10.20.20.128 /25) 到 VLAN 100 中特定服务器 (10.10.10.101) 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 100捕获。

1. 定义要捕获并发送进行分析的关注流量。
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. 定义一个大型 ACL 以映射所有其他流量。
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```
3. 定义 VLAN 访问映射。
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. 将 VLAN 访问映射应用于相应的 VLAN。
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. 配置捕获端口。
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

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 vlan access-map - 显示 VLAN 访问映射的内容。**

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter - 显示关于 VLAN 过滤器的信息。**

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

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 CatOS 软件的 Cisco Catalyst 6000/6500 执行 VACL 捕获以进行细致的流量分析
- Cisco Catalyst 6500 系列交换机支持
- LAN 产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems