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

本文提供一配置示例为使用VLAN访问控制列表(ACL) (VACL)网络流量分析的捕获端口功能以更加粒状的方式。本文也陈述VACL捕获端口使用情况优点与基于vlan的交换端口分析器(SPAN) (VSPAN)使用情况相对。

为了配置VACL请捕获运行Cisco IOS软件在思科Catalyst 6000/6500的端口功能，粒状数据流分析的参考的VACL捕获用运行Cisco IOS软件的思科Catalyst 6000/6500。

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 —参考的VLAN中继协议(VLAN/VTP) -介绍欲知更多信息。
- 访问列表—参考配置访问控制欲知更多信息。

使用的组件

本文档中的信息根据运行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

此配置可能也与运行Catalyst OS版本6.3及以后的Cisco Catalyst 6000/6500系列交换机一起使用。

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复制流量从所有VLAN的一个或更多源端口或从一个或更多VLAN到分析的一个目的地端口。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)是网络流量的分析在一个或更多VLAN的。您能配置VSPAN作为入口Span端口，出口Span或者两个。源VLAN的所有端口变为VSPAN会话的操作源端口。目的地端口，如果他们属于任何管理源VLAN，从可操作的来源被排除。如果从管理源VLAN添加或取消端口，相应地修改可操作的来源。

VSPAN会话的指南：

- 中继端口包括作为VSPAN会话的源端口，但是在管理源来源列表仅的VLAN监控，如果这些VLAN为中继是活跃的。
- 对于VSPAN会话用配置的入口和出口Span，系统运行基于您有Supervisor引擎的种类：WS-X6K-SUP1A-PFC， WS-X6K-SUP1A-MSFC， WS-X6K-S1A-MSFC2， WS-X6K-S2-PFC2， WS-X6K-S1A-MSFC2， WS-SUP720， WS-SUP32-GE-3B —两数据包由SPAN目的地端口转发，如果数据包在同样VLAN得到交换。WS-X6K-SUP1-2GE， WS-X6K-SUP1A-2GE —仅一数据包由SPAN目的地端口转发。
- 一个带内端口没有包括作为VSPAN会话的可操作的来源。
- 当清除时VLAN，从VSPAN会话的源列表删除。
- 如果管理源VLAN列表是空的， VSPAN会话禁用。
- 非激活VLAN没有为VSPAN配置允许。
- 如果其中任一个源VLAN变为RSPAN VLAN， VSPAN会话使不激活。

源VLAN参考的特性关于源VLAN的更多信息。

VLAN ACL

VACL能访问控制所有流量。您能配置在交换机的VACL适用于路由或在VLAN外面或在VLAN内桥接的所有信息包。VACL严格是为安全信息包过滤和重定向流量对特定物理交换机端口。不同于Cisco

IOS ACL， VACL没有由方向定义(输入或输出)。

您能配置在第3层地址的VACL IP和IPX的。其他协议是通过MAC地址被控制的访问和以太网类型使用MAC VACL。IP数据流和IPX数据流不是MAC VACL控制的访问。其他流量类型(AppleTalk，DECNet，等等)分类作为MAC流量。MAC VACL用于访问控制此流量。

支持VACL ACE

VACL包含排好序的列表访问控制条目(ACE)。每个VACL只能包含一个类型ACE。每个ACE包含匹配数据包的内容的一定数量的字段。每个字段能有指示相关的位掩码哪些位是相关的。描述的操作关联与每个ACE什么系统应该用数据包执行，当匹配发生时。操作是从属的功能。Catalyst 6500系列交换机在硬件里支持ACE的三种类型：

- IP ACE
- IPX ACE
- 以太网ACE

此表列出关联与每个ACE类型的参数：

ACE类型	TCP或UDP	ICMP	其他IP	IPX	以太网
Layer4参数	源端口	--	--	--	--
	源端口操作员	--	--	--	--
	目的端口	--	--	--	--
	目的地端口操作员	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目的地网络	--
	--	--	--	IP目的地节点	--
	TCP或UDP	ICMP	其他协议	IPX数据包类型	--
Layer2参数	--	--	--	--	以太网类型
	--	--	--	--	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。参考的功能汇总和限制欲知更多信息。
- 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不主要设计监控流量。然而，以各种各样的功能分类流量，捕获端口功能介绍，以便网络流量分析能变得更加简单。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在硬件方面被强制执行。可以创建ACE的数量取决于在交换机的TCAM联机。
- 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在硬件方面被强制执行。没有VACL的应用程序的影响性能对在Cisco Catalyst 6500系列交换机的VLAN。

配置

本部分提供有关如何配置本文档所述功能的信息。

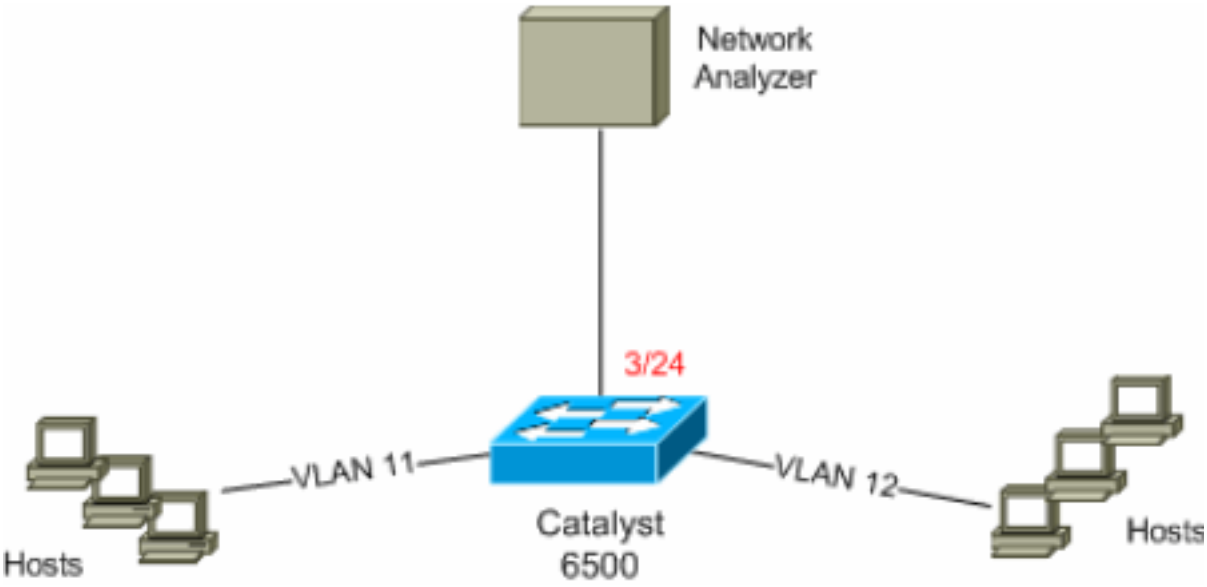
本文档使用以下配置：

- 基于 VLAN 的 SPAN 配置
- VACL 配置

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



基于 VLAN 的 SPAN 配置

此配置示例列出要求的步骤捕获在VLAN11和VLAN 12的流和发送他们到网络分析器设备的所有Layer2流量。

1. 指定关注的流量。在本例中，它是在VLAN 100和VLAN 200流的流量。`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` 使用此，属于VLAN11和VLAN 12的所有Layer2流量复制并且发送到端口3/24。
2. 验证您的与**all命令的show span的**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：

- 从范围的HTTP数据流主机(10.12.12.128/25)在对一个特定服务器(10.11.11.100)的VLAN 12在VLAN11需要捕获。
- 组播在为组地址的239.0.0.100注定的传送方向的用户数据报协议(UDP)流量需要从VLAN11捕获。

1. 使用安全ACL，定义关注数据流。切记提及定义的所有ACE的关键字**捕获**。`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. 如果ACE配置正确和按适当的顺序，请验证。`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. 做ACL到硬件。`6K-CatOS> (enable) **commit security acl** *HttpUdp_Acl* ACL commit in progress. ACL 'HttpUdp_Acl' successfully committed. 6K-CatOS> (enable)`
4. 验证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. 验证ACL对VLAN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被映射对多个VLAN，则必须配置捕获端口到所有那些VLAN。为了做捕获端口允许多个VLAN，配置端口作为中继和允许仅VLAN被映射对ACL。例如，如果ACL被映射对VLAN 11和12，然后请完

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. 验证捕获端口配置。`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信息**—显示配置或最后当前做到NVRAM和硬件VACL的内容。`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地图**—显示特定ACL、端口或者VLAN的ACL到VLAN或端口映射。`6K-CatOS> (enable) **show security acl map all** ACL Name Type Vlans ---------- ---- ----- HttpUdp_Acl IP 11 6K-CatOS> (enable)`
- **show security ACL捕获端口**—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