Captura de VACL para análise de tráfego granular com Cisco Catalyst 6000/6500 executando CatOS Software

Contents

Introduction

Este documento oferece uma configuração de exemplo do uso da característica de porta de captura VLAN Access Control List (ACL) (VACL) para análise de tráfego de rede de forma mais granulada. Este documento também indica a vantagem do uso da porta de captura VACL em oposição ao uso do Switched Port Analyzer (SPAN) (VSPAN) baseado em VLAN.

Para configurar o recurso de Porta de Captura de VACL no Cisco Catalyst 6000/6500 que executa o software Cisco IOS®, consulte Captura de VACL para Análise de Tráfego Granular com o Cisco Catalyst 6000/6500 executando o Cisco IOS Software.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- LAN virtual—Consulte Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) - Introdução para obter mais informações.
- Listas de acesso—Refira a configurar o controle de acesso para mais informações.

Componentes Utilizados

As informações neste documento são baseadas no Switch Cisco Catalyst 6506 Series que executa o Catalyst OS versão 8.1(2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

Essa configuração também pode ser usada com os switches Cisco Catalyst 6000 / 6500 Series que executam o Catalyst OS versão 6.3 e posterior.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

SPAN baseado em VLAN

O SPAN copia o tráfego de uma ou mais portas de origem em qualquer VLAN ou de uma ou mais VLANs para uma porta de destino para análise. O SPAN local suporta portas de origem, VLANs de origem e portas de destino no mesmo Switch Catalyst 6500 Series.

Uma porta de origem é uma porta monitorada para análise de tráfego de rede. Uma VLAN de origem é uma VLAN monitorada para análise de tráfego de rede. O SPAN baseado em VLAN (VSPAN) é a análise do tráfego de rede em uma ou mais VLANs. Você pode configurar VSPAN como SPAN de entrada, SPAN de saída ou ambos. Todas as portas nas VLANs de origem se tornam as portas de origem operacional para a sessão de VSPAN. As portas de destino, se pertencerem a qualquer das VLANs de origem administrativa, serão excluídas da origem operacional. Se você adicionar ou remover as portas das VLANs de origem administrativa, as fontes operacionais serão modificadas de acordo.

Diretrizes para sessões de VSPAN:

- As portas de tronco são incluídas como portas de origem para as sessões de VSPAN, mas somente as VLANs que estão na lista de origem do administrador são monitoradas se essas VLANs estiverem ativas para o tronco.
- Para sessões de VSPAN com SPAN de entrada e saída configurado, o sistema opera com base no tipo de mecanismo de supervisor que você tem: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—Dois pacotes são encaminhados por a porta de destino de

SPAN se os pacotes forem comutados na mesma VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE—Somente um pacote é encaminhado pela porta de destino de SPAN.

- Uma porta inband não está incluída como origem operacional para as sessões de VSPAN.
- Quando uma VLAN é removida, ela é removida da lista de origem das sessões de VSPAN.
- Uma sessão de VSPAN é desabilitada se a lista de VLANs de origem do administrador estiver vazia.
- As VLANs inativas não são permitidas para a configuração de VSPAN.
- Uma sessão de VSPAN ficará inativa se qualquer uma das VLANs de origem se tornar as VLANs de RSPAN.

Consulte Características da VLAN de Origem para obter mais informações sobre VLANs de origem.

VLAN ACL

As VACLs podem controlar todo o tráfego. Você pode configurar as VACLs no switch para aplicar a todos os pacotes que são roteados para dentro ou para fora de uma VLAN ou que estão ligados em uma VLAN. As VACLs são estritamente para filtragem de pacotes de segurança e redirecionamento de tráfego para portas de switch físicas específicas. Diferentemente das ACLs do Cisco IOS, as VACLs não são definidas por direção (entrada ou saída).

Você pode configurar as VACLs nos endereços da Camada 3 para IP e IPX. Todos os outros protocolos são controlados por meio dos endereços MAC e EtherType usando as VACLs MAC. O tráfego IP e o tráfego IPX não são controlados pelas VACLs MAC. Todos os outros tipos de tráfego (AppleTalk, DECnet, etc.) são classificados como tráfego MAC. As VACLs MAC são usadas para controlar esse tráfego.

ACEs suportadas em VACLs

A VACL contém uma lista ordenada de entradas de controle de acesso (ACEs). Cada VACL pode conter ACEs de apenas um tipo. Cada ACE contém um número de campos correspondentes ao conteúdo de um pacote. Cada campo pode ter uma máscara de bit associada para indicar quais bits são relevantes. Uma ação é associada a cada ACE que descreve o que o sistema deve fazer com o pacote quando ocorre uma correspondência. A ação depende do recurso. Os switches Catalyst 6500 Series suportam três tipos de ACEs no hardware:

- ACEs IP
- ACEs IPX
- ACEs Ethernet

Esta tabela lista os parâmetros associados a cada tipo de ACE:

Tipo de ACE	TCP ou UDP	ICMP	Outro IP	IPX	Ethernet
Parâmetros da Camada 4	Porta de origem	-	-	-	-
	Operador de porta de origem	-	-	-	-
	Porta de Destino	-	-	-	-
	Operador	Código	-	-	-

	da porta de destino	ICMP			
	N/A	Tipo de ICMP	N/A	-	-
Parâmetros da Camada 3	Byte IP ToS	Byte IP ToS	Byte IP ToS	-	-
	Endereço IP de origem	Endereço IP de origem	Endereço IP de origem	Rede de origem IPX	-
	Endereço IP de destino	Endereço IP de destino	Endereço IP de destino	Rede de destino IP	-
	-	-	-	Nó de destino IP	-
	TCP ou UDP	ICMP	Outro protocolo	Tipo de pacote IPX	-
Parâmetros da Camada 2	-	-	-	-	EtherType
	-	-	-	-	Endereço de origem Ethernet
	-	-	-	-	Endereço de destino Ethernet

Vantagens do uso de VACL sobre o uso de VSPAN

Há várias limitações do uso de VSPAN para análise de tráfego:

- Todo o tráfego da camada 2 transmitido em uma VLAN é capturado. Isso aumenta a quantidade de dados a serem analisados.
- O número de sessões de SPAN que podem ser configuradas nos Catalyst 6500 Series Switches é limitado. Consulte Resumo e Limitações de Recursos para obter mais informações.
- Uma porta de destino recebe cópias do tráfego enviado e recebido para todas as portas de origem monitoradas. Se uma porta de destino receber um excesso de assinaturas, ela poderá ficar congestionada. Esse congestionamento poderá afetar o encaminhamento de tráfego em uma ou mais portas de origem.

O recurso Porta de Captura de VACL pode ajudar a superar algumas dessas limitações. As VACLs não são projetadas principalmente para monitorar o tráfego. No entanto, com uma grande variedade de recursos para classificar o tráfego, o recurso Capture Port foi introduzido para que a análise de tráfego de rede se tornasse muito mais simples. Estas são as vantagens do uso da

Porta de Captura de VACL sobre VSPAN:

- Análise de tráfego granularAs VACLs podem corresponder com base no endereço IP origem, endereço IP destino, tipo de protocolo da Camada 4, portas da Camada 4 origem e destino e outras informações. Esse recurso torna as VACLs muito úteis para a identificação e filtragem de tráfego granular.
- Número de sessõesAs VACLs são aplicadas no hardware. O número de ACEs que podem ser criadas depende do TCAM disponível nos switches.
- Excesso de assinatura da porta de destinoA identificação de tráfego granular reduz o número de quadros a serem encaminhados para a porta de destino e, assim, minimiza a probabilidade de sua sobreassinatura.
- DesempenhoAs VACLs são aplicadas no hardware. Não há penalidade de desempenho para a aplicação de VACLs a uma VLAN nos switches Cisco Catalyst 6500 Series.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

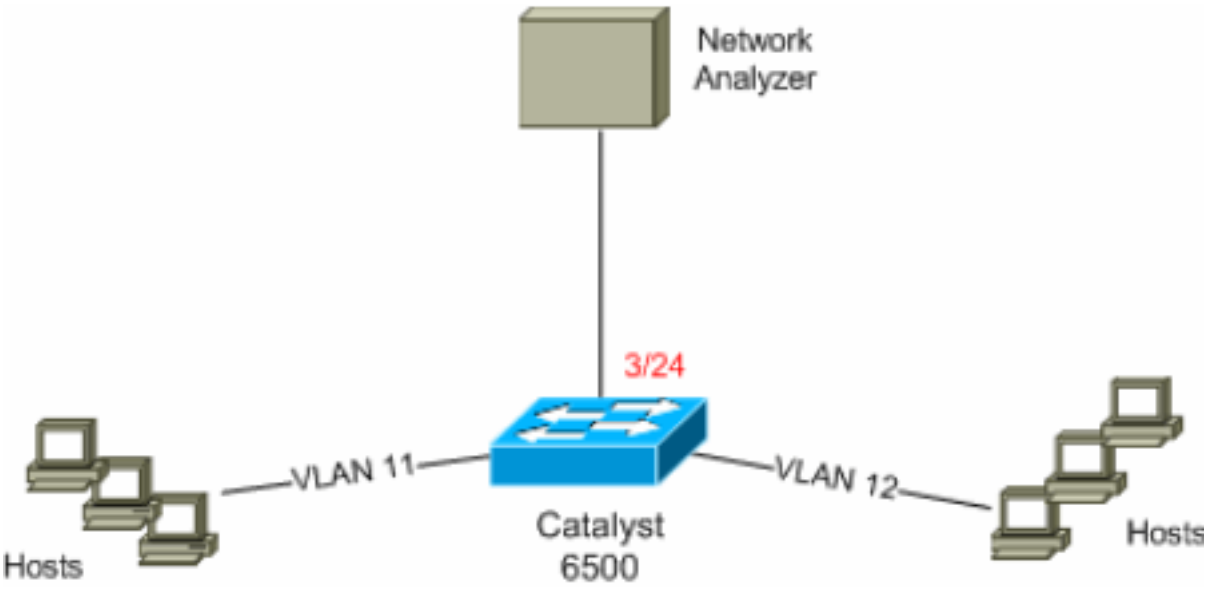
Este documento utiliza as seguintes configurações:

- Configuração com SPAN baseado em VLAN
- Configuração com VACL

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração com SPAN baseado em VLAN

Este exemplo de configuração relaciona as etapas obrigatórias para capturar todo o tráfego da

camada 2 transmitido em VLAN 11 e VLAN 12 e enviá-lo para o dispositivo analisador de redes.

1. Especifique o tráfego interessante.Neste exemplo, é o tráfego que flui na VLAN 100 e na VLAN 200.
```
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
```
   Com isso, todo o tráfego da Camada 2 que pertence à VLAN 11 e à VLAN 12 é copiado e enviado à porta 3/24.
2. Verifique sua configuração de SPAN com o comando **show span all**.
```
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)
```

Configuração com VACL

Neste exemplo de configuração, há vários requisitos do administrador de rede:

- O tráfego HTTP de uma faixa de hosts (10.12.12.128/25) na VLAN 12 para um servidor específico (10.11.11.100) na VLAN 11 precisa ser capturado.
- O tráfego de Multicast User Datagram Protocol (UDP) na direção de transmissão destinado ao endereço de grupo 239.0.0.100 precisa ser capturado da VLAN 11.

1. Defina o tráfego interessante usando as ACLs de segurança. Lembre-se de mencionar a **captura** da palavra-chave para todas as ACEs definidas.
```
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. Verifique se a configuração da ACE está correta e na ordem correta.

```
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. Confirme a ACL com o hardware.

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

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

4. Verifique o status da ACL.

```
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. Aplique o mapa de acesso à VLAN às VLANs apropriadas.

```
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. Verifique o mapeamento da ACL para a VLAN.

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

7. Configure a porta de captura.

```
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)
```

Observação: se uma ACL é mapeada para várias VLANs, a porta de captura deve ser configurada para todas essas VLANs. Para fazer com que a porta de captura permita várias VLANs, configure a porta como tronco e permita somente as VLANs mapeadas para a ACL. Por exemplo, se a ACL estiver mapeada para as VLANs 11 e 12, conclua a configuração.

```
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. Verifique a configuração da porta de captura.

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show security acl info** — Exibe o conteúdo da VACL que está configurada no momento ou firmada pela última vez na NVRAM e no hardware.

```
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** —Exibe o mapeamento de ACL para VLAN ou ACL para porta para uma ACL, porta ou VLAN específica.

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

- **show security acl capture-ports** — Exibe a lista de portas de captura.

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

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Captura de VACL para análise de tráfego granular com Cisco Catalyst 6000/6500 executando Cisco IOS Software
- Configurando o controle de acesso - Guia de configuração de software do Catalyst 6500 Series, 8.6
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems