Captação VACL para a análise de tráfego granulada com Cactos Software running do Cisco catalyst 6000/6500

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Produtos Relacionados
Convenções
Informações de Apoio
PERÍODO com base em VLAN
VLAN ACL
Vantagens do uso VACL sobre o uso VSPAN
Configurar
Diagrama de Rede
Configuração com PERÍODO com base em VLAN
Configuração com VACL
Verificar
Troubleshooting
Informações Relacionadas

Introdução

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.

A fim configurar o VACL capture a característica da porta no Cisco catalyst 6000/6500 que isso executa o software de Cisco IOS®, referem a captação VACL para a análise de tráfego granulada com Cisco IOS Software running do Cisco catalyst 6000/6500.

Pré-requisitos

Requisitos

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

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

Componentes Utilizados

A informação neste documento é baseada no Cisco Catalyst 6506 Series Switch que executa o Catalyst OS Release 8.1(2).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com Cisco catalyst 6000/6500 Series Switch que executa o Catalyst OS Release 6.3 e mais atrasado.

Convenções

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

Informações de Apoio

PERÍODO com base em VLAN

MEÇA cópias traficam de umas ou várias portas de origem em todo o VLAN ou de uns ou vários VLAN a uma porta do destino para a análise. O SPAN local apoia portas de origem, fonte VLAN, e portas do destino no mesmo Catalyst 6500 Series Switch.

Uma porta de origem é uma porta monitorada para a análise de tráfego de rede. Uma fonte VLAN é um VLAN monitorado para a análise de tráfego de rede. O PERÍODO com base em VLAN (VSPAN) é análise do tráfego de rede em uns ou vários VLAN. Você pode configurar o VSPAN como o span de ingresso, o span de saída, ou ambos. Todas as portas na fonte VLAN se transformam as portas de origem operacionais para a sessão VSPAN. As portas do destino, se pertencem a algum do origem administrativa VLAN, são excluídas da fonte operacional. Se você adiciona ou remove as portas do origem administrativa VLAN, as fontes operacionais estão alteradas em conformidade.

Diretrizes para sessões VSPAN:

- As portas de tronco são incluídas como as portas de origem para as sessões VSPAN, mas somente os VLAN que estão na lista de código de origem de administrador são monitorados se estes VLAN são ativos para o tronco.
- Para as sessões VSPAN com o ingresso e o span de saída configurados, o sistema opera-se baseado no tipo de Supervisor Engine 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 estão enviados pela porta do destino do PERÍODO se os pacotes obtêm ligados o mesmo VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE — Somente um pacote é enviado pela porta do destino do PERÍODO.

- Uma porta inband não é incluída como o Origem Operacional para as sessões VSPAN.
- Quando um VLAN é cancelado, está removido da lista de origem para as sessões VSPAN.
- Uma sessão VSPAN é desabilitada se a lista do código de origem de administrador VLAN está vazia.
- Os VLAN inativos não são permitidos a configuração VSPAN.
- Uma sessão VSPAN está feita inativa se alguma da fonte VLAN se transforma o RSPAN VLAN.

Refira características da fonte VLAN para obter mais informações sobre da fonte VLAN.

VLAN ACL

Os VACL enlatam o controle de acesso todo o tráfego. Você pode configurar os VACL no interruptor para aplicar-se a todos os pacotes em que são distribuídos ou fora de um VLAN ou construídos uma ponte sobre dentro de um VLAN. Os VACL são restritamente para o filtragem de pacote de informação da Segurança e tráfego da reorientação às portas de switch físicas específicas. Ao contrário do Cisco IOS ACL, os VACL não são definidos pelo sentido (entrada ou saída).

Você pode configurar os VACL nos endereços da camada 3 para o IP e o IPX. Todos protocolos restantes são acesso controlado através dos endereços MAC e Ethertype usando o MAC VACL. O tráfego IP e o tráfego IPX não são acesso controlado pelo MAC VACL. Todos tipos de tráfego restantes (APPLETALK, DECNet, e assim por diante) são classificados como o tráfego MAC. O MAC VACL é usado ao controle de acesso este tráfego.

ACE apoiados nos VACL

O VACL contém uma lista requisitada das entradas de controle de acesso (ACE). Cada VACL pode conter ACE de somente um tipo. Cada ACE contém um número de campos que são combinados contra os índices de um pacote. Cada campo pode ter uma máscara de bit associada para indicar que bit são relevantes. Uma ação é associada com cada ACE que descreve o que o sistema deve fazer com o pacote quando um fósforo ocorre. A ação é dependente da característica. Os Catalyst 6500 Series Switch apoiam três tipos de ACE no hardware:

- IP ACE
- IPX ACE
- Ethernet ACE

Esta tabela alista os parâmetros que são associados com cada tipo ACE:

Tipo ACE	TCP ou UDP	ICMP	O outro IP	IPX	Ethernet
Parâmetros da camada 4	Porta de origem	-	-	-	-
	Operador da porta de origem	-	-	-	-
	Porta de	-	-	-	-

	Destino				
	Operador da porta do destino	Código ICMP	-	-	-
	N/A	Tipo de ICMP	N/A	-	-
Parâmetros da camada 3	Byte ToS IP	Byte ToS IP	Byte ToS IP	-	-
	Endereço IP de origem	Endereço IP de origem	Endereço IP de origem	Rede da fonte IPX	-
	Endereço de destino IP	Endereço de destino IP	Endereço de destino IP	Rede do destino IP	-
	-	-	-	Nó do destino IP	-
	TCP ou UDP	ICMP	O outro protocolo	Tipo do pacote IPX	-
Parâmetros da camada 2	-	-	-	-	Ethertype
	-	-	-	-	Endereço de origem dos Ethernet
	-	-	-	-	Endereço de destino dos Ethernet

Vantagens do uso VACL sobre o uso VSPAN

Há diversas limitações do uso VSPAN para a análise de tráfego:

- Todo o tráfego da camada 2 transmitido em uma VLAN é capturado. Isto aumenta a quantidade de dados a ser analisados.
- O número da sessão de alcance que pode ser configurado nos Catalyst 6500 Series Switch é limitado. Refira o resumo e limitação de recursos para mais informação.
- 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.

A característica da porta da captação VACL pode ajudar a superar algumas destas limitações. Os VACL não são projetados primeiramente monitorar o tráfego. Contudo, com um amplo intervalo da capacidade de classificar o tráfego, a característica da porta da captação foi introduzida de

modo que a análise de tráfego de rede pudesse se tornar muito mais simples. Estas são as vantagens do uso da porta da captação VACL sobre o VSPAN:

- Análise de tráfego granuladaOs VACL podem combinar baseado no endereço IP de origem, endereço IP de destino, mergulham 4 tipo de protocolo, portas da fonte e da camada de destino 4, e a outra informação. Esta capacidade faz VACL muito úteis para a identificação e a filtração granuladas do tráfego.
- Número de sessõesOs VACL são reforçados no hardware. O número de ACE que podem ser criados depende em cima do TCAM disponível no Switches.
- Sobreassinatura da porta do destinoA identificação granulada do tráfego reduz o número de quadros a ser enviados à porta do destino e minimiza desse modo a probabilidade de sua sobreassinatura.
- DesempenhoOs VACL são reforçados no hardware. Não há nenhuma penalidade de desempenho para o aplicativo dos VACL a um VLAN nos Cisco Catalyst 6500 Series Switch.

Configurar

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

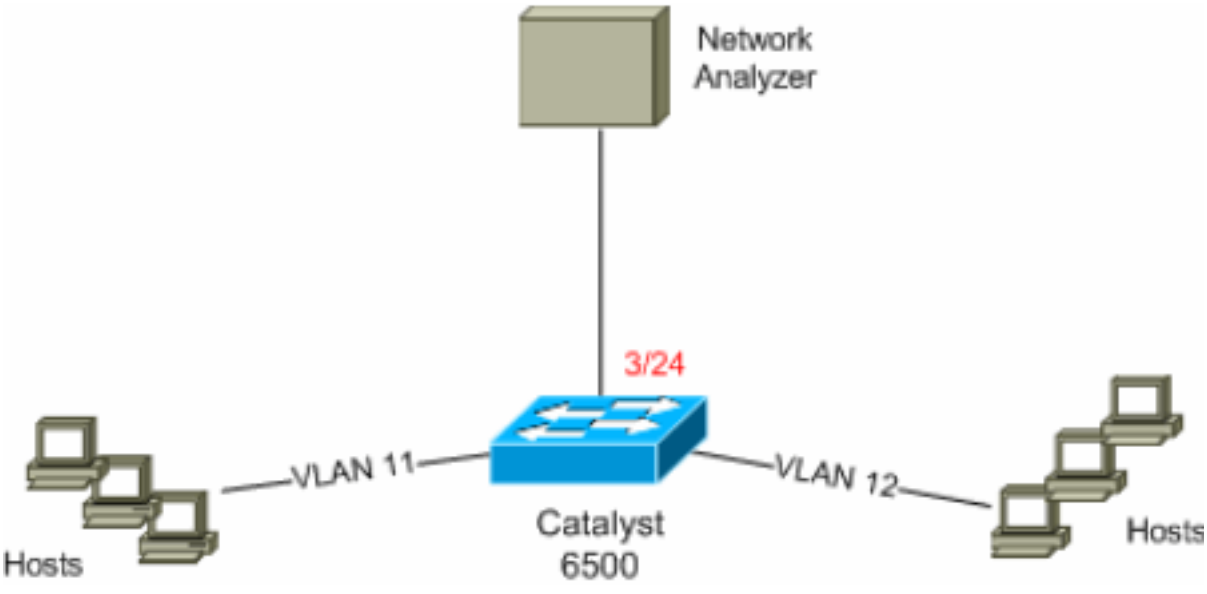
Este documento utiliza as seguintes configurações:

- Configuração com PERÍODO com base 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 PERÍODO com base em VLAN

Este exemplo de configuração alista as etapas exigidas para capturar todo o tráfego da camada 2 que os fluxos no VLAN 11 e no VLAN 12 e lhes enviam ao dispositivo do analisador de rede.

1. Especifique o tráfego interessante.Neste exemplo, é o tráfego que flui no VLAN 100 e no 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 isto, todo o tráfego da camada 2 que pertence ao VLAN 11 e ao VLAN 12 é copiado e enviado à porta 3/24.
2. Verifique sua configuração de span com o **comando all do período da mostra**.`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 umas exigências múltiplas do administrador de rede:

- O tráfego de HTTP de uma escala dos anfitriões (10.12.12.128/25) no VLAN 12 a um server específico (10.11.11.100) no VLAN 11 precisa de ser capturado.
- O tráfego do User Datagram Protocol (UDP) do Multicast no transmitir direção destinado para o endereço de grupo 239.0.0.100 precisa de ser capturado do VLAN 11.

1. Defina o tráfego interessante usando as seguranças ACL. Recorde mencionar a **captação da** palavra-chave para todos os ACE definida.`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 ACE está correta e na ordem apropriada.`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. Comprometa o ACL ao hardware.`6K-CatOS> (enable) **commit security acl** *HttpUdp_Acl* ACL commit in progress. ACL 'HttpUdp_Acl' successfully committed. 6K-CatOS> (enable)`
4. Verifique o estado do 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 do acesso de vlan aos VLAN apropriados.`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 ACL ao mapeamento VLAN.`6K-CatOS> (enable) **show security acl map** *HttpUdp_Acl* ACL HttpUdp_Acl is mapped to VLANs: 11 6K-CatOS> (enable)`
7. Configurar a porta da captação.`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)`
   Nota: Se um ACL é traçado aos vlan múltiplos, a seguir a porta da captação deve ser configurada a todos aqueles VLAN. A fim fazer a porta da captação permitir vlan múltiplos,

configurar a porta como o tronco e permitir somente os VLAN traçados ao ACL. Por exemplo, se o ACL é traçado a VLAN 11 e 12, termine então 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 de porta da captação.`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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre a informação acl da Segurança** — Indica os índices do VACL que são configurados atualmente ou comprometidos por último ao NVRAM e ao 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)`
- **mostre o mapa acl da Segurança** — Indica o ACL-à-VLAN ou o mapeamento da ACL-à-porta para um ACL, uma porta, ou um VLAN específico.`6K-CatOS> (enable) show security acl map all ACL Name Type Vlans ---------- ---- ----- HttpUdp_Acl IP 11 6K-CatOS> (enable)`
- **mostre captação-portas acl da Segurança** — Indica a lista de portas da captação.`6K-CatOS> (enable) show security acl capture-ports ACL Capture Ports: 3/24 6K-CatOS> (enable)`

Troubleshooting

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

Informações Relacionadas

- Captação VACL para a análise de tráfego granulada com Cisco IOS Software running do Cisco catalyst 6000/6500
- Configurando o controle de acesso - Manual de configuração do 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