Prevenção de exaustão de TCAM de ACL e QoS em Switches Catalyst 4500

Contents

Introduction

Os switches das séries Cisco Catalyst 4500 e Catalyst 4948 são compatíveis com Access Control List (ACL) de taxa de fios e o recurso QoS com o uso de Ternary Content Addressable Memory (TCAM). A habilitação dos ACL e das políticas não diminui o switching ou o desempenho do roteamento do switch quando os ACL são completamente carregados na TCAM. Se a TCAM é esgotada, os pacotes podem ser enviados através do caminho da CPU, que pode diminuir o desempenho desses pacotes. Este documento fornece detalhes sobre:

- Os diferentes tipos de TCAM que o Catalyst 4500 e o Catalyst 4948 usam
- Como o Catalyst 4500 programa os TCAMs
- Como configurar de forma otimizada as ACLs e TCAM no switch para evitar a exaustão do TCAM

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 4500 Series Switches
- Catalyst 4948 Series Switches

Observação: este documento se aplica somente aos switches baseados no software Cisco IOS® e não se aplica aos switches baseados em Catalyst OS (CatOS).

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.

Conventions

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

Informações de Apoio

Para implementar os vários tipos de ACLs e políticas de QoS no hardware, as tabelas de pesquisa de hardware (TCAM) dos programas Catalyst 4500 e vários registros de hardware no Supervisor Engine. Quando um pacote chega, o switch executa uma pesquisa na tabela de hardware (pesquisa de TCAM) e decide permitir ou negar o pacote.

O Catalyst 4500 suporta diferentes tipos de ACLs. A Tabela 1 descreve esses tipos de ACLs.

Tabela 1 - Tipos de ACLs suportadas nos switches Catalyst 4500

Tipo de ACL	Onde é aplicado	Tráfego controlado	Direção
RACL[1]	L3[2] porta, canal L3 ou SVI[3] (VLAN)	Tráfego IP roteado	Entrada ou saída
VACL[4]	VLAN (através do comando **vlan filter**)	Todos os pacotes que são roteados para dentro ou para fora de uma VLAN ou que são ligados em uma VLAN	Sem direção
PACL[5]	Porta L2[6] ou canal L2	Todo o tráfego IP e o tráfego não IPv4[7] (via MAC ACL)	Entrada ou saída

[1] RACL = ACL do roteador

2 L3 = Camada 3

[3] SVI = interface virtual comutada

[4] VACL = VLAN ACL

[5] PACL = porta ACL

[6] L2 = Camada 2

[7] IPv4 = IP versão 4

Arquitetura de programação de hardware de QoS e ACL do Catalyst 4500

O TCAM do Catalyst 4500 tem o seguinte número de entradas:

- 32.000 entradas para ACL de segurança, também conhecida como ACL de recurso
- 32.000 entradas para ACL de QoS

Para ACL de segurança e ACL de QoS, as entradas são dedicadas da seguinte maneira:

- 16.000 entradas para a direção de entrada
- 16.000 entradas para a direção de saída

A Figura 3 mostra a dedicação de entrada TCAM. Consulte a seção Tipos de TCAM para obter mais informações sobre TCAMs.

A Tabela 2 mostra os recursos da ACL disponíveis para vários Catalyst 4500 Supervisor Engines e switches.

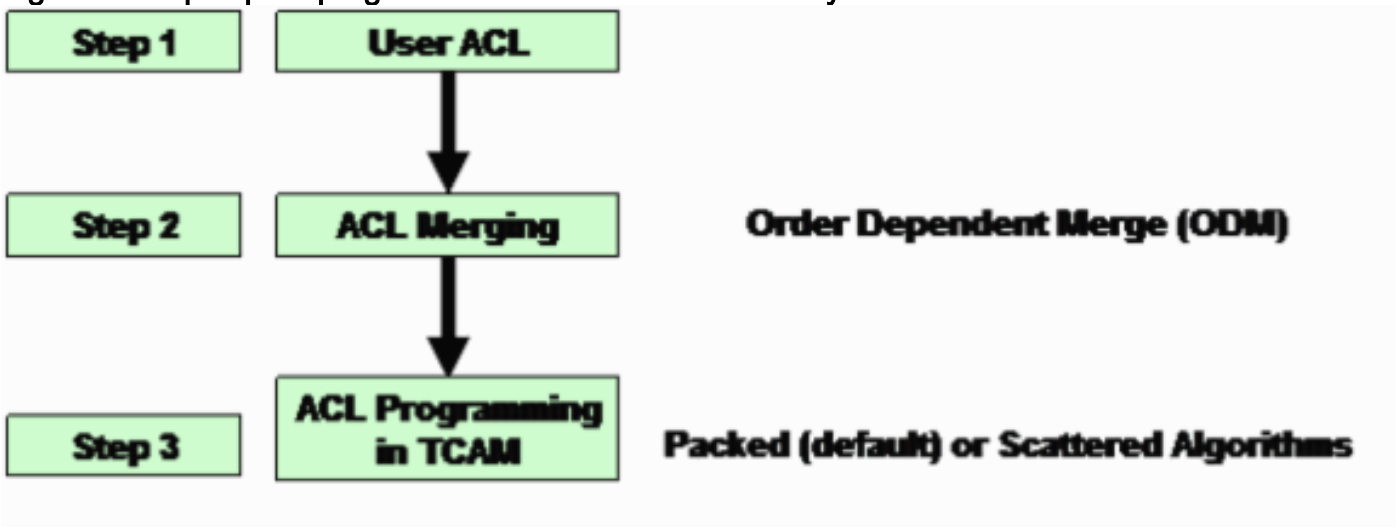
Tabela 2 - Recursos da ACL do Catalyst 4500 em vários Supervisor Engines e Switches

Produto	Versão TCAM	Recurso TCAM (por direção)	TCAM de QoS (por direção)
Supervisor Engine II+	2	8.000 entradas, 1.000 máscaras	8.000 entradas, 1.000 máscaras
Supervisor Engine II+TS/III/IV/V e WS-C4948	2	16.000 entradas, 2.000 máscaras	16.000 entradas, 2.000 máscaras
Supervisor Engine V-10GE e WS-C4948-10GE	3	16.000 entradas, 16.000 máscaras	16.000 entradas, 16.000 máscaras

O Catalyst 4500 usa TCAMs separados e dedicados para roteamento unicast e multicast IP. O Catalyst 4500 pode ter até 128.000 entradas de rota que as rotas unicast e multicast compartilham. No entanto, esses detalhes estão fora do escopo deste documento. Este documento discute apenas problemas de segurança e esgotamento de QoS TCAM.

A Figura 1 mostra as etapas para programar as ACLs em tabelas de hardware no Catalyst 4500.

Figura 1: Etapas para programar ACLs em Switches Catalyst 4500



Passo 1

Esta etapa envolve uma destas ações:

- Configuração e aplicação de uma ACL ou política de QoS a uma interface ou VLANA criação da ACL pode ocorrer dinamicamente. Um exemplo é o caso do recurso IP Source Guard (IPSG). Com esse recurso, o switch cria automaticamente um PACL para endereços IP associados à porta.
- Modificação de uma ACL que já existe

Observação: a configuração de uma ACL sozinha não resulta em programação de TCAM. A ACL (política de QoS) deve ser aplicada a uma interface para programar a ACL na TCAM.

Passo 2

A ACL deve ser mesclada antes de poder ser programada nas tabelas de hardware (TCAM). A mesclagem programa várias ACLs (PACL, VACL ou RACL) no hardware de forma combinada. Dessa forma, somente uma única pesquisa de hardware é necessária para verificar todas as ACLs aplicáveis no caminho de encaminhamento lógico do pacote.

Por exemplo, na Figura 2, um pacote que é roteado do PC-A para o PC-C pode ter essas ACLs:

- Um PACL de entrada na porta PC-A
- Uma VACL na VLAN 1
- Uma RACL de entrada na interface VLAN 1 na direção de entrada

Essas três ACLs são mescladas de modo que uma única pesquisa na TCAM de entrada seja suficiente para tomar a decisão de encaminhamento de permitir ou negar. Da mesma forma, somente uma única pesquisa de saída é necessária porque o TCAM é programado com o resultado mesclado dessas três ACLs:

- O RACL de saída na interface VLAN 2
- A VLAN 2 VACL
- O PACL de saída na porta PC-C

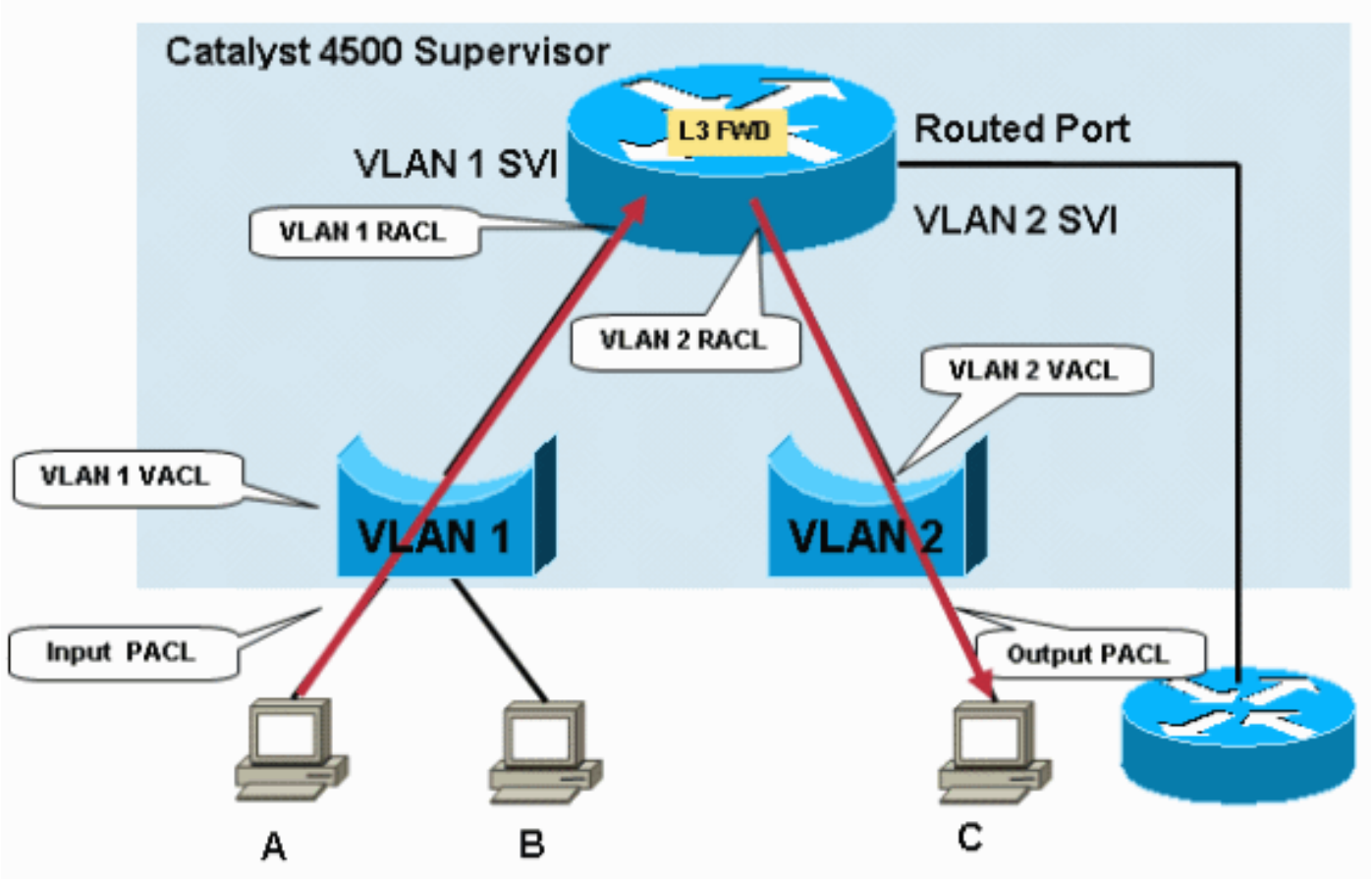
Com uma única pesquisa de entrada e uma de saída, não há nenhum encaminhamento de hardware de penalidade dos pacotes quando qualquer ou todas essas ACLs estão no caminho de encaminhamento de pacotes.

Observação: as pesquisas de TCAM de entrada e saída ocorrem ao mesmo tempo no hardware. Uma concepção equivocada comum é que a pesquisa de TCAM de saída ocorre após a pesquisa de TCAM de entrada, como sugere o fluxo do pacote lógico. Essa informação é importante de entender porque a política de saída do Catalyst 4500 não pode corresponder aos parâmetros de QoS modificados pela política de entrada. No caso da ACL de segurança, a ação mais grave ocorre. O pacote é descartado em uma destas situações:

- Se o resultado da pesquisa de entrada for descartado e o resultado da pesquisa de saída for permit
- Se o resultado da pesquisa de entrada for permit e o resultado da pesquisa de saída for drop

Observação: o pacote é permitido se os resultados de pesquisa de entrada e saída forem permitidos.

Figura 2: Filtragem via ACLs de segurança nos switches Catalyst 4500



A combinação de ACL no Catalyst 4500 depende do pedido. O processo também é conhecido como mesclagem dependente de pedido (ODM). Com ODM, as entradas da ACL são programadas na ordem em que aparecem na ACL. Por exemplo, se uma ACL contiver duas entradas de controle de acesso (ACEs), o switch programará a ACE 1 primeiro e, em seguida, programará a ACE 2. No entanto, a dependência do pedido é somente entre as ACEs dentro de uma ACL específica. Por exemplo, as ACEs na ACL 120 podem iniciar antes das ACEs na ACL 100 na TCAM.

Etapa 3

A ACL mesclada é programada no TCAM. O TCAM de entrada ou saída para ACL ou QoS é dividido em duas regiões: PortAndVlan e PortOrVlan. A ACL mesclada é programada na região PortAndVlan do TCAM se uma configuração tiver *ambas* as ACLs no mesmo caminho de pacote:

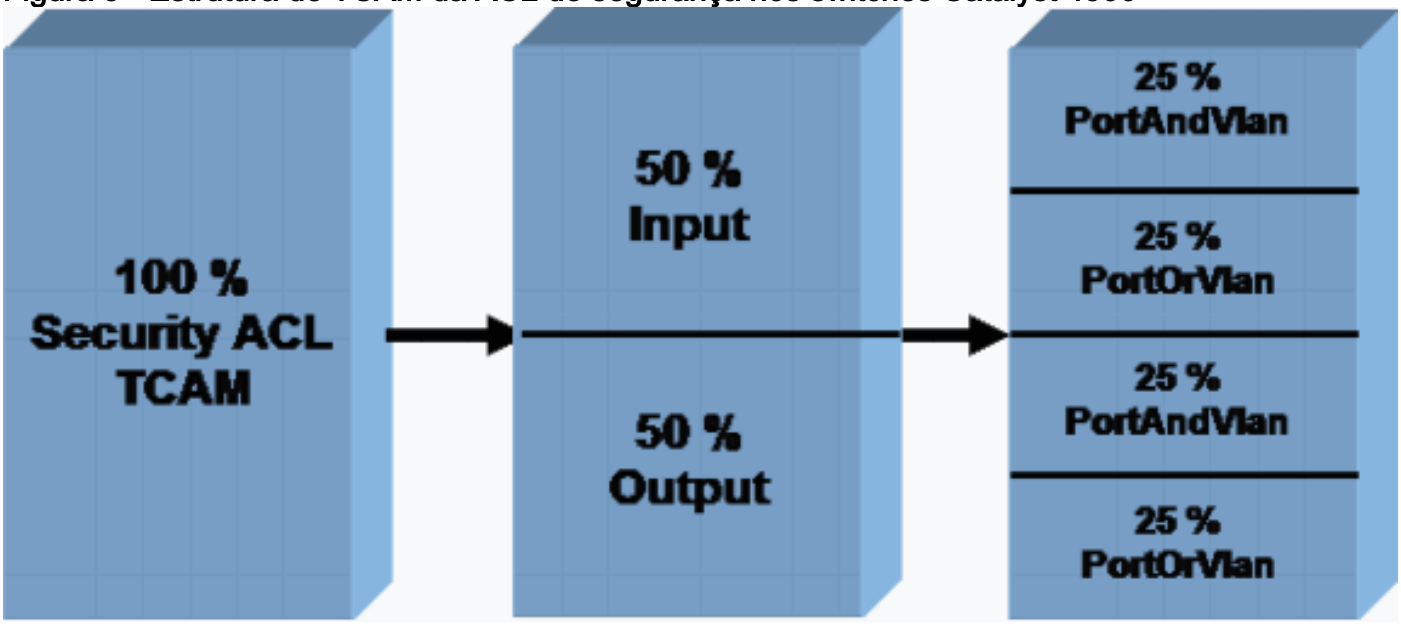
- A PACL**Observação:** o PACL é uma ACL de filtragem normal ou uma ACL dinâmica criada pelo IPSG.
- Uma VACL ou RACL

Uma ACL é programada na região PortOrVlan do TCAM se um caminho específico do pacote tiver apenas uma PACL ou uma VACL ou uma RACL. A Figura 3 mostra a gravação TCAM da ACL de segurança para vários tipos de ACLs. A QoS tem um TCAM dedicado, separado e gravado de forma semelhante.

No momento, não é possível modificar a alocação padrão do TCAM. No entanto, há planos para fornecer a capacidade de alterar a alocação de TCAM que está disponível para as regiões PortAndVlan e PortOrVlan em versões futuras do software. Essa alteração permitirá aumentar ou diminuir o espaço para PortAndVlan e PortOrVlan nos TCAMs de entrada ou saída.

Observação: qualquer aumento na alocação para a região PortAndVlan resultará em uma diminuição equivalente para a região PortOrVlan no TCAM de entrada ou saída.

Figura 3 - Estrutura de TCAM da ACL de segurança nos switches Catalyst 4500



O comando **show platform hardware ACL statistics usage brief** exibe essa utilização de TCAM por região para TCAMs de ACL e QoS. A saída do comando mostra as máscaras e entradas disponíveis e as divide por região, como na Figura 3. Este exemplo de saída é de um Catalyst 4500 Supervisor Engine II+:

Observação: consulte a seção Tipos de TCAM deste documento para obter mais informações sobre máscaras e entradas.

```
Switch#show platform hardware acl statistics utilization brief
                                      Entries/Total(%)  Masks/Total(%)
                                     ----------------  --------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
```

```
Output Acl(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Output Acl(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
Output Qos(PortAndVlan)      0 / 4096 (  0)      0 /  512 (  0)
Output Qos(PortOrVlan)       0 / 4096 (  0)      0 /  512 (  0)
L4Ops: used 2 out of 64
```

Tipos de TCAM

O Catalyst 4500 usa dois tipos de TCAM, como a Tabela 2 mostra. Esta seção apresenta a diferença entre as duas versões do TCAM para que você possa selecionar o produto apropriado para sua rede e configuração.

O TCAM 2 usa uma estrutura na qual oito entradas compartilham uma máscara. Um exemplo são oito endereços IP em ACEs. As entradas devem ter a mesma máscara que a máscara compartilhada. Se as ACEs tiverem máscaras diferentes, as entradas devem usar máscaras separadas conforme necessário. Esse uso de máscaras separadas pode levar à exaustão da máscara. A exaustão das máscaras na TCAM é uma das razões comuns para a exaustão da TCAM.

A TCAM 3 não tem tal restrição. Cada entrada pode ter sua própria máscara exclusiva no TCAM. A utilização total de todas as entradas disponíveis no hardware é possível, independentemente da máscara dessas entradas.

Para demonstrar essa arquitetura de hardware, o exemplo nesta seção mostra como um TCAM 2 e um programa TCAM 3 ACLs no hardware.

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

Este exemplo de ACL tem duas entradas que têm duas máscaras diferentes. A ACE 1 é uma entrada de host e, portanto, tem uma máscara /32. A ACE 2 é uma entrada de sub-rede com uma máscara /24. Como a segunda entrada tem uma máscara diferente, entradas vazias na Máscara 1 não podem ser usadas e uma máscara separada é usada no caso de TCAM 2.

Esta tabela mostra como essa ACL é programada no TCAM 2:

Máscaras	Entradas
Máscara 1 Corresponde: todos os 32 bits do endereço IP de origem "Não se importe": todos os bits restantes	IP de origem = 8.1.1.1
	Entrada vazia 2
	Entrada vazia 3
	Entrada vazia 4
	Entrada vazia 5
	Entrada vazia 6

	Entrada vazia 7
	Entrada vazia 8
Máscara 2 correspondente: 24 bits mais significativos do endereço IP de origem "Não se importe": todos os bits restantes	IP de origem = 8.1.1.0
	Entrada vazia 2
	Entrada vazia 3
	Entrada vazia 4
	Entrada vazia 5
	Entrada vazia 6
	Entrada vazia 7
	Entrada vazia 8

Embora haja entradas gratuitas disponíveis como parte da Máscara 1, a estrutura da TCAM 2 impede a população da ACE 2 na entrada vazia 2 para a Máscara 1. O uso dessa máscara não é permitido porque a máscara de ACE 2 não corresponde à máscara /32 de ACE 1. O TCAM 2 deve programar a ACE 2 com o uso de uma máscara separada, uma máscara /24.

Esse uso de uma máscara separada pode resultar em uma exaustão mais rápida dos recursos disponíveis, como a Tabela 2 mostra. Outras ACLs ainda podem usar as entradas restantes na Máscara 1. No entanto, na maioria dos casos, a eficiência do TCAM 2 é alta, mas não é 100%. A eficiência varia com cada cenário de configuração.

Esta tabela mostra a mesma ACL programada na TCAM 3. A TCAM 3 aloca uma máscara para cada entrada:

Máscaras	**Entradas**
Máscara 32 bits para o endereço IP 1	IP de origem = 8.1.1.1
Máscara 24 bits para o endereço IP 2	IP de origem = 8.1.1.0
Máscara vazia 3	Entrada vazia 3
Máscara vazia 4	Entrada vazia 4
Máscara vazia 5	Entrada vazia 5
Máscara vazia 6	Entrada vazia 6
Máscara vazia 7	Entrada vazia 7
Máscara vazia 8	Entrada vazia 8
Máscara vazia 9	Entrada vazia 9

Máscara vazia 10	Entrada vazia 10
Máscara vazia 11	Entrada vazia 11
Máscara vazia 12	Entrada vazia 12
Máscara vazia 13	Entrada vazia 13
Máscara vazia 14	Entrada vazia 14
Máscara vazia 15	Entrada vazia 15
Máscara vazia 16	Entrada vazia 16

Neste exemplo, as 14 entradas restantes podem ter entradas com máscaras diferentes, sem restrições. Portanto, o TCAM 3 é muito mais eficiente do que o TCAM 2. Este exemplo é muito simplificado para ilustrar a diferença entre as versões do TCAM. O software Catalyst 4500 tem várias otimizações para aumentar a eficiência da programação em TCAM 2 para um cenário de configuração prática. A seção Subotimizado TCAM Programming Algorithm para TCAM 2 deste documento discute estas otimizações.

Para TCAM 2 e TCAM 3 no Catalyst 4500, as entradas TCAM são compartilhadas se a mesma ACL for aplicada em interfaces diferentes. Essa otimização economiza espaço TCAM.

Solucionar problemas de esgotamento de TCAM

Quando a exaustão do TCAM ocorre nos switches Catalyst 4500 durante a programação de uma ACL de segurança, uma aplicação parcial da ACL ocorre através do caminho do software. Os pacotes que correspondem às ACEs que não são aplicadas na TCAM são processados no software. Esse processamento no software causa alta utilização da CPU. Como a programação da ACL do Catalyst 4500 depende do pedido, a ACL é sempre programada de cima para baixo. Se uma ACL específica não se encaixa totalmente na TCAM, as ACEs na parte inferior da ACL provavelmente não são programadas na TCAM.

Uma mensagem de aviso é exibida quando ocorre um estouro de TCAM. Aqui está um exemplo:

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Você também pode ver essa mensagem de erro na saída do comando **show logging** se tiver habilitado o syslog. A presença dessa mensagem indica conclusivamente que algum processamento de software ocorrerá. Consequentemente, pode haver alta utilização da CPU. A ACL que já foi programada na TCAM permanece programada na TCAM se a exaustão da capacidade da TCAM ocorrer durante a aplicação da nova ACL. Os pacotes que correspondem às ACLs que já foram programadas continuam a ser processados e encaminhados no hardware.

Observação: se você fizer alterações em uma ACL grande, a mensagem TCAM excedido poderá ser exibida. O switch tenta reprogramar a ACL no TCAM. Na maioria dos casos, a nova ACL modificada pode ser totalmente reprogramada no hardware. Se o switch puder reprogramar a ACL totalmente no TCAM com êxito, esta mensagem será exibida:

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

Use o comando **show platform software acl input summary interface** *interface-id* para verificar se a

ACL está totalmente programada no hardware.

Esta saída mostra a configuração da ACL 101 para a VLAN 1 e a verificação de que a ACL está totalmente programada no hardware:

Observação: se a ACL não estiver totalmente programada, uma mensagem de erro de esgotamento de TCAM poderá ser exibida.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip access-group 101 in
Switch(config-if)#end
Switch#
Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
    Current TagPair(port, vlan) : (null, 0/Normal)
    Current Signature          : {FeatureCam:(Security: 101)}
  Type                         : Current
    Direction                  : In
    TagPair(port, vlan)        : (null, 0/Normal)
    FeatureFlatAclId(state)    : 0(FullyLoadedWithToCpuAces)
    QosFlatAclId(state)        : (null)
    Flags                      : L3DenyToCpu
```

O campo `Sinalizadores` (`L3DenyToCpu`) indica que, se um pacote for negado por causa da ACL, o pacote é direcionado para a CPU. Em seguida, o switch envia uma mensagem de Internet Control Message Protocol (ICMP) inalcançável. Esse comportamento é o padrão. Quando os pacotes são direcionados para a CPU, pode ocorrer alta utilização da CPU no switch. No entanto, no Cisco IOS Software Release 12.1(13)EW e posterior, esses pacotes são limitados à taxa da CPU. Na maioria dos casos, a Cisco recomenda que você desative o recurso que envia mensagens ICMP inalcançáveis.

Esta saída mostra a configuração do switch para não enviar mensagens ICMP inalcançáveis e a verificação da programação TCAM após a alteração. O estado da ACL 101 agora é `FullyLoaded`, como mostra a saída do comando. O tráfego negado não vai para a CPU.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no ip unreachables
Switch(config-if)#end

Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
    Current TagPair(port, vlan) : (null, 1/Normal)
    Current Signature          : {FeatureCam:(Security: 101)}
  Type                         : Current
    Direction                  : In
    TagPair(port, vlan)        : (null, 1/Normal)
    FeatureFlatAclId(state)    : 0(FullyLoaded)
    QosFlatAclId(state)        : (null)
    Flags                      : None
```

Observação: se o TCAM de QoS for excedido durante a aplicação de uma determinada política

de QoS, essa política específica *não* será aplicada à interface ou VLAN. O Catalyst 4500 não implementa a política de QoS no caminho do software. Portanto, a utilização da CPU não aumenta quando o TCAM de QoS é excedido.

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

Emita o comando **show platform cpu packet statistics**. Determine se a fila de `processamento de sw da ACL` recebe um alto número de pacotes. Um número alto de pacotes indica a exaustão do TCAM de segurança. Essa exaustão de TCAM faz com que os pacotes sejam enviados à CPU para encaminhamento de software.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue  Queue                   Total
5 sec avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- ------
--- --------- ---------- Control                        57902635        22        16
12          3 Host Learning                    464678         0         0         0          0 L3
Fwd Low                      623229         0         0         0          0 L2 Fwd
Low                     11267182         7         4         6          1 L3 Rx
High                          508         0         0         0          0 L3 Rx
Low                       1275695        10         1         0          0 ACL
fwd(snooping)               2645752         0         0         0          0 ACL log,
unreach               51443268         9         4         5          5 ACL sw
processing             842889240      1453      1532      1267       1179

Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
----------------------- --------------- --------- --------- --------- ----------
L2 Fwd Low                          3270         0         0         0          0
ACL sw processing                  12636         0         0         0          0
```

Se você descobrir que a fila de `processamento de sw da ACL` não recebe uma quantidade excessiva de tráfego, consulte Alta Utilização da CPU em Switches Catalyst 4500 baseados no software Cisco IOS para outras causas possíveis. O documento fornece informações sobre como solucionar problemas de outros cenários de alta utilização da CPU.

O TCAM do Catalyst 4500 pode estourar por estes motivos:

- Um algoritmo de programação TCAM não ideal para TCAM 2
- O uso excessivo de operações da camada 4 (L4Ops) em uma ACL
- ACLs excessivas para o mecanismo supervisor ou tipo de switch

Algoritmo de programação TCAM não ideal para TCAM 2

Como a seção Tipos de TCAM discute, a eficiência de TCAM 2 é menor devido ao fato de oito entradas compartilharem uma máscara. O software Catalyst 4500 permite dois tipos de algoritmos de programação TCAM para TCAM 2 que melhoram a eficiência do TCAM 2:

- Embalado — adequado para a maioria dos cenários de ACL de segurança**Observação:** este é o padrão.
- Distribuído—Usado no cenário IPSG

Você pode alterar o algoritmo para um algoritmo distribuído, mas isso normalmente não ajuda se você tiver configurado apenas ACLs de segurança, como RACLs. O algoritmo disperso só é eficaz em cenários em que a mesma ACL pequena ou semelhante é repetida em várias portas. Esse cenário é o caso de um IPSG habilitado em várias interfaces. No cenário IPSG, cada ACL dinâmica:

- Tem um pequeno número de entradasIsso inclui permissões para endereços IP permitidos e uma negação no final para impedir o acesso da porta por endereços IP não autorizados.
- Érepetido para todas as portas de acesso configuradasA ACL é repetida para até 240 portas em um Catalyst 4507R.

Observação: o TCAM 3 usa o algoritmo compactado padrão. Como a estrutura TCAM é uma máscara por entrada, o algoritmo compactado é o melhor algoritmo possível. Portanto, a opção de algoritmo distribuído não está habilitada nesses switches.

Este exemplo está em um Supervisor Engine II+ configurado para o recurso IPSG. A saída mostra que, embora apenas 49% das entradas sejam usadas, 89% das máscaras são consumidas:

```
Switch#show platform hardware acl statistics utilization brief

                                  Entries/Total(%)  Masks/Total(%)
                                 -----------------  ---------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     4 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          L4Ops: used 2 out of 64
```

Nesse caso, uma alteração no algoritmo de programação do algoritmo compactado padrão para o algoritmo distribuído ajuda. O algoritmo disperso reduz o uso total da máscara de 89% para 49%.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scattered
Switch(config)#end
Switch#show platform hardware acl statistics utilization brief
                                  Entries/Total(%)  Masks/Total(%)
                                 -----------------  ---------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
          L4Ops: used 2 out of 64
```

Para obter informações sobre as práticas recomendadas para recursos de segurança em switches Catalyst 4500, consulte Práticas recomendadas para recursos de segurança do Catalyst 4500 para supervisores.

Uso excessivo de L4Ops em uma ACL

O termo L4Ops refere-se ao uso das palavras-chave **gt**, **lt**, **neq** e **range** na configuração da ACL. O Catalyst 4500 tem limites no número dessas palavras-chave que você pode usar em uma única ACL. A limitação, que varia de acordo com o Supervisor Engine e o switch, é de seis ou oito L4Ops por ACL. A Tabela 3 mostra o limite por Supervisor Engine e por ACL.

Tabela 3 - Limite L4Op por ACL em diferentes mecanismos e switches de supervisor Catalyst 4500

Produto	L4Op
Supervisor Engine II+/ II+TS	32 (6 por ACL)
Supervisor Engine III/IV/V e WS-C4948	32 (6 por ACL)
Supervisor Engine V-10GE e WS-C4948-10GE	64 (8 por ACL)

Se o limite L4Op por ACL for excedido, uma mensagem de aviso será exibida no console. A mensagem é semelhante a esta:

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

Além disso, se o limite L4Op for excedido, a ACE específica será expandida na TCAM. Resultados adicionais de utilização de TCAM. Este ACE serve como exemplo:

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

Com essa ACE em uma ACL, o switch usa apenas uma entrada e uma L4Op. No entanto, se seis L4Ops já forem usados nesta ACL, essa ACE será expandida para 10 entradas no hardware. Essa expansão pode potencialmente usar várias entradas na TCAM. O uso cuidadoso desses L4Ops evita o estouro de TCAM.

Observação: se esse caso envolve o Supervisor Engine V-10GE e o WS-C4948-10GE, oito L4Ops usados anteriormente na ACL resultam na expansão da ACE.

Lembre-se destes itens ao usar L4Op nos switches Catalyst 4500:

- As operações L4 são consideradas diferentes se o operador ou o operando forem diferentes.Por exemplo, esta ACL contém três operações L4 diferentes porque **gt 10** e **gt 11** são consideradas duas operações L4 diferentes:
  ```
  access-list 101 permit tcp host 8.1.1.1 any gt 10
  access-list 101 deny tcp host 8.1.1.2 any lt 9
  access-list 101 deny tcp host 8.1.1.3 any gt 11
  ```
- As operações L4 são consideradas diferentes se o mesmo operador/par de operandos se aplicar uma vez a uma porta de origem e uma vez a uma porta de destino.Aqui está um exemplo:
  ```
  access-list 101 permit tcp host 8.1.1.1 gt 10 any
  access-list 101 permit tcp host 8.1.1.2 any gt 10
  ```
- Os switches Catalyst 4500 compartilham L4Ops quando possível.Neste exemplo, as linhas

em ***itálico em negrito*** demonstram este cenário:Uso de L4Op para ACL 101 = 5Uso de L4Op para ACL 102 = 4 **Observação:** a palavra-chave **eq** não consome nenhum recurso de hardware L4Op.Uso total de L4Op = 8**Observação:** a ACL 101 e 102 compartilham um L4Op.**Observação:** L4Op é compartilhado mesmo se o protocolo, como TCP ou User Datagram Protocol (UDP), não corresponder ou a ação permit/deny não corresponder.

ACLs excessivas para o mecanismo supervisor ou tipo de switch

Como a Tabela 2 mostra, o TCAM é um recurso limitado. Você pode exceder o recurso TCAM de qualquer Supervisor Engine se configurar ACLs ou recursos excessivos, como o IPSG, com um alto número de entradas IPSG.

Se você exceder o espaço TCAM do Supervisor Engine, faça o seguinte:

- Se você tiver um Supervisor Engine II+ e executar uma versão do Cisco IOS Software *anterior* à versão 12.2(18)EW do Cisco IOS Software, faça o upgrade para a versão de manutenção mais recente do Cisco IOS Software Release 12.2(25)EWA.A capacidade de TCAM foi aumentada nas versões posteriores.
- Se você usar o rastreamento de DHCP e o IPSG e começar a ficar sem TCAM, use a versão de manutenção mais recente do Cisco IOS Software Release 12.2(25)EWA e use o algoritmo dividido no caso de produtos TCAM 2.**Observação:** o algoritmo distribuído está disponível no Cisco IOS Software Release 12.2(20)EW e posterior.A versão mais recente também tem aprimoramentos para melhor utilização do TCAM com rastreamento de DCHP e recursos de inspeção de protocolo de resolução de endereço dinâmico (ARP - Dynamic Address Resolution Protocol) (DAI).
- Se você começar a ficar sem TCAM porque o limite L4Op foi excedido, tente reduzir o uso de L4Op na ACL para evitar o estouro de TCAM.
- Se você usar muitas ACLs ou políticas semelhantes em várias portas na mesma VLAN, agregue-as em uma única ACL ou política na interface VLAN.Essa agregação economiza algum espaço TCAM. Por exemplo, quando você aplica políticas baseadas em voz, a QoS baseada em porta padrão é usada para classificação. Essa QoS padrão pode fazer com que a capacidade de TCAM seja excedida. Se você trocar a QoS para baseada em VLAN, reduzirá o uso de TCAM.
- Se você ainda tiver problemas com o espaço TCAM, considere um mecanismo supervisor avançado, como o Supervisor Engine V-10GE ou Catalyst 4948-10GE.Esses produtos usam o hardware TCAM 3 mais eficiente.

Summary

O Catalyst 4500 programa as ACLs configuradas com o uso da TCAM. O TCAM permite a aplicação das ACLs no caminho de encaminhamento de hardware sem impacto no desempenho do switch. O desempenho é constante apesar do tamanho da ACL, pois o desempenho das pesquisas da ACL está na taxa de linha. No entanto, o TCAM é um recurso finito. Portanto, se você configurar um número excessivo de entradas de ACL, você excederá a capacidade de TCAM. O Catalyst 4500 implementou várias otimizações e forneceu comandos para variar o algoritmo de programação do TCAM a fim de alcançar a máxima eficiência. Os produtos TCAM 3, como o Supervisor Engine V-10GE e o Catalyst 4948-10GE, oferecem a maioria dos recursos TCAM para políticas de segurança de ACL e QoS.

Informações Relacionadas

- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems