ACL e fuga de exaustão de TCAM de QoS em Catalyst 4500 Switch

Índice

Introdução

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 tipos diferentes de TCAM que o uso do Catalyst 4500 e do catalizador 4948
- Como o Catalyst 4500 programa os TCAM
- Como configurar otimamente os ACL e o TCAM no interruptor a fim evitar a exaustão de TCAM

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Catalyst 4500 Series Switch
- Catalyst 4948 Series Switch

Nota: Este documento aplica-se somente ao Switches com base no software de Cisco IOS® e não se aplica ao OS do catalizador (Cactos) - Switches baseado.

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.

Convenções

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

Informações de Apoio

A fim executar os vários tipos de ACL e políticas de QoS no hardware, nas tabelas de consulta de hardware dos programas do Catalyst 4500 (TCAM) e em vários registradores de hardware no Supervisor Engine. Quando um pacote chega, o interruptor executa uma consulta da tabela do hardware (consulta TCAM) e decide a um ou outro permit or deny o pacote.

Os tipos diferentes dos apoios do Catalyst 4500 de ACL. A tabela 1 esboça estes tipos de ACL.

Tabela 1 – Tipos de ACL que são apoiados em Catalyst 4500 Switch

Tipo ACL	**Onde é aplicado**	**Tráfego controlado**	**Direção**
RACL[1]	Porta L3[2], canal L3, ou SVI[3] (VLAN)	Tráfego do IP roteado	De entrada ou de partida
VACL[4]	VLAN (através do **comando vlan filter**)	Todos os pacotes em que são distribuídos ou fora de um VLAN ou em que são construídos uma ponte sobre dentro de um VLAN	Directionless
PACL[5]	Porta L2[6] ou canal L2	Todo o tráfego IP e tráfego non-IPv4[7] (através de MAC ACL)	De entrada ou de partida

[1] RACL = roteador ACL

2 L3 = Camada 3

[3] SVI = Switched Virtual Interface

[4] VACL = VLAN ACL

[5] PACL = porta ACL

[6] L2 = camada 2

IPv4 [7] = versão IP 4

Catalyst 4500 ACL e arquitetura de programação do QoS Hardware

O Catalyst 4500 TCAM tem o seguinte número de entradas:

- 32,000 entradas para a segurança ACL, que é sabida igualmente como a característica ACL
- 32,000 entradas para QoS ACL

Para a segurança ACL e o QoS ACL, as entradas são dedicadas da seguinte forma:

- 16,000 entradas para o sentido da entrada
- 16,000 entradas para o sentido da saída

Figura 3 mostra a dedicação da entrada de TCAM. Veja os tipos de seção TCAM para obter mais informações sobre dos TCAM.

A tabela 2 mostra os recursos ACL que estão disponíveis para os vários motores e Switches do supervisor do Catalyst 4500.

Tabela 2 – Recursos ACL do Catalyst 4500 nos vários motores e Switches do supervisor

Produto	Versão TCAM	Característica TCAM (pelo sentido)	QoS TCAM (pelo sentido)
Supervisor Engine II+	2	8000 entradas, 1000 máscaras	8000 entradas, 1000 máscaras
Supervisor Engine II+TS/III/IV/V e WS-C4948	2	16,000 entradas, 2000 máscaras	16,000 entradas, 2000 máscaras
V-10GE do Supervisor Engine e WS-C4948-10GE	3	16,000 entradas, 16,000 máscaras	16,000 entradas, 16,000 máscaras

Os usos do Catalyst 4500 separam, dedicaram TCAM para o unicast IP e o roteamento de transmissão múltipla. O Catalyst 4500 pode ter até 128,000 entradas da rota de que o unicast e

as rotas de transmissão múltiplas compartilham. Contudo, estes detalhes são fora do âmbito deste documento. Este documento discute somente a Segurança e as edições da exaustão de TCAM de QoS.

Figura 1 mostra as etapas para programar os ACL em tabelas do hardware no Catalyst 4500.

Figura 1 - Etapas para programar ACL em Catalyst 4500 Switch

Passo 1

Esta etapa envolve uma destas ações:

- Configuração e aplicativo de um ACL ou de uma política de QoS a uma relação ou a um VLANA criação de ACL pode ocorrer dinamicamente. Um exemplo é o exemplo da característica da proteção de origem de IP (IPSG). Com esta característica, o interruptor cria automaticamente um PACL para os endereços IP de Um ou Mais Servidores Cisco ICM NT que são associados com a porta.
- Alteração de um ACL que já exista

Nota: A configuração apenas de um ACL não conduz à programação TCAM. O ACL (política de QoS) deve aplicado a uma relação a fim programar o ACL no TCAM.

Passo 2

O ACL deve ser fundido antes que possa ser programado nas tabelas do hardware (TCAM). Os programas de fusão ACL múltiplos (PACL, VACL, ou RACL) no hardware em uma forma combinada. Desta maneira, somente uma única consulta de hardware é necessária para verificar contra todos os ACL aplicáveis no trajeto de encaminhamento lógico do pacote.

Por exemplo, em figura 2, um pacote que seja distribuído do PC-A ao PC-C potencialmente pode ter estes ACL:

- Uma entrada PACL na porta PC-A
- Um VACL no VLAN1
- Uma entrada RACL na relação VLAN1 no sentido da entrada

Estes três ACL são fundidos de modo que uma única consulta na entrada TCAM seja bastante para fazer a decisão de encaminhamento ao permit or deny. Similarmente, somente uma única consulta da saída é necessária porque o TCAM é programado com o resultado fundido destes três ACL:

- A saída RACL na relação VLAN2
- O VLAN2 VACL
- A saída PACL na porta do PC-C

Com uma única consulta para a entrada e uma para a saída, não há nenhum encaminhamento de hardware da pena dos pacotes quando alguns ou todos estes ACL estão no trajeto do encaminhamento de pacote.

Nota: As consultas TCAM da entrada e saída ocorrem ao mesmo tempo no hardware. Uma concepção errada comum é que a consulta TCAM da saída ocorre após a consulta TCAM da entrada, porque o fluxo de pacote de informação lógico sugere. Esta informação é importante de compreender porque a política emissora do Catalyst 4500 não pode combinar em parâmetros de QoS alterados política de entrada. No caso da segurança ACL, a maioria de ação séria ocorre. O

pacote é deixado cair em qualquer uma destas situações:

- Se o resultado de consulta da entrada é a gota e o resultado de consulta da saída são licença
- Se o resultado de consulta da entrada é a licença e o resultado de consulta da saída são gota

Nota: O pacote é permitido se ambos os resultados de consulta da entrada e saída são licença.

Figura 2 – Filtração através das seguranças ACL em Catalyst 4500 Switch

A fusão ACL no Catalyst 4500 é dependentes do ordem. O processo é sabido igualmente como o Order Dependent Merge (ODM). Com ODM, as entradas ACL são programadas na ordem em que aparecem no ACL. Por exemplo, se um ACL contém duas entradas de controle de acesso (ACE), o interruptor programa ACE 1 primeiramente e programa então ACE 2. Contudo, a dependência da ordem está somente entre os ACE dentro de um ACL específico. Por exemplo, os ACE em ACL 120 podem começar antes dos ACE no ACL 100 no TCAM.

Etapa 3

O ACL fundido é programado no TCAM. A entrada ou a saída TCAM para o ACL ou o QoS são uma separação mais adicional em dois regiões, PortAndVlan e PortOrVlan. O ACL fundido está programado na região de Porta E Vlan do TCAM se uma configuração tem *both of these* ACL no mesmo caminho de pacote de informação:

- UM PACL**Nota:** O PACL é um ACL de filtração normal ou ACL dinâmico IPSG-criado.
- Um VACL ou um RACL

Um ACL está programado na região de Porta Ou Vlan do TCAM se um caminho particular do pacote tem somente um PACL ou um VACL ou um RACL. Figura 3 mostra a segurança ACL TCAM que cinzela para vários tipos de ACL. QoS tem um TCAM similarmente cinzelado, separado, dedicado.

Atualmente, você não pode alterar a alocação padrão de TCAM. Contudo, há uns planos para fornecer a capacidade para mudar a alocação de TCAM que está disponível para o PortAndVlan e as regiões de Porta Ou Vlan em liberações de software futuro. Esta mudança permitirá que você aumente ou diminua o espaço para o PortAndVlan e o PortOrVlan na entrada ou na saída TCAM.

Nota: Todo o aumento na atribuição para a região de Porta E Vlan conduzirá a uma diminuição equivalente para a região de Porta Ou Vlan na entrada ou na saída TCAM.

Figura 3 – Estrutura da segurança ACL TCAM nos Catalyst 4500 Switch

O comando show platform hardware ACL statistics utilization brief indica esta utilização de TCAM por região para ACL e QoS TCAM. A saída do comando mostra as máscaras e as entradas disponíveis e divide-os pela região, como em figura 3. Este exemplo de saída é de um Supervisor Engine II+ do Catalyst 4500:

Nota: Veja os tipos de seção TCAM deste documento para obter mais informações sobre das máscaras e das 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 mostras da tabela 2. Esta seção apresenta a diferença entre as duas versões TCAM de modo que você possa selecionar o produto apropriado para suas rede e configuração.

O TCAM2 usa uma estrutura em que oito entradas compartilham de uma máscara. Um exemplo é oito endereços IP de Um ou Mais Servidores Cisco ICM NT nos ACE. As entradas devem ter a mesma máscara que a máscara de que compartilham. Se os ACE têm máscaras diferentes, as entradas devem usar máscaras separadas como necessário. Este uso de máscaras separadas pode conduzir para mascarar a exaustão. A exaustão da máscara no TCAM é um dos motivos comuns para a exaustão de TCAM.

O TCAM 3 não tem uma limitação. Cada entrada pode ter sua própria máscara original no TCAM. A utilização completa de todas as entradas que estão disponíveis no hardware é possível, apesar da máscara daquelas entradas.

A fim demonstrar esta arquitetura de hardware, o exemplo nesta seção mostra como um TCAM2 e um TCAM 3 programam ACL 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
```

Esta amostra ACL tem duas entradas que têm duas máscaras diferentes. O ACE 1 é uma entrada de host e assim que tem uma máscara de /32. O ACE 2 é uma entrada de sub-rede com uma máscara de /24. Porque a segunda entrada tem uma máscara diferente, as entradas vazias na máscara 1 não podem ser usadas e uma máscara separada é usada no caso do TCAM2.

Esta tabela mostra como este ACL é programado no TCAM2:

Máscaras	**Entradas**
Fósforo da **máscara 1**: todos os 32 bit do endereço IP de origem "não importa": todos os bit restante	Fonte IP= 8.1.1.1
	Entry2 vazio
	Entry3 vazio
	Entrada vazia 4
	Entrada vazia 5
	Entrada vazia 6

	Entrada vazia 7
	Entrada vazia 8
Fósforo da **máscara 2**: a maioria 24 de bit significativos do endereço IP de origem "não importa": todos os bit restante	Fonte IP= 8.1.1.0
	Entry2 vazio
	Entry3 vazio
	Entrada vazia 4
	Entrada vazia 5
	Entrada vazia 6
	Entrada vazia 7
	Entrada vazia 8

Mesmo que haja umas entradas livres disponíveis como parte da máscara 1, a estrutura TCAM2 impede a população de ACE 2 no entry2 vazio para a máscara 1. O uso desta máscara não é permissível porque a máscara de ACE 2 não combina a máscara de /32 de ACE 1. TCAM2 deve programar o ACE 2 com o uso de uma máscara separada, uma máscara de /24.

Este uso de uma máscara separada pode conduzir a uma exaustão mais rápida dos recursos disponíveis, como mostras da tabela 2. Outros ACL podem ainda usar as entradas restantes na máscara 1. Contudo, na maioria dos casos, a eficiência do TCAM2 é alta mas não é 100 por cento. A eficiência varia com cada cenário de configuração.

Esta tabela mostra que o mesmo ACL programado no TCAM 3. TCAM 3 atribui uma máscara para cada entrada:

Máscaras	Entradas
Bit da máscara 32 para o endereço IP de Um ou Mais Servidores Cisco ICM NT 1	Fonte IP= 8.1.1.1
Bit da máscara 24 para o endereço IP de Um ou Mais Servidores Cisco ICM NT 2	Fonte IP= 8.1.1.0
Máscara vazia 3	Entry3 vazio
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 enlatam cada um têm entradas com máscaras diferentes, sem limitações. Consequentemente, o TCAM 3 é muitos mais eficiente do que o TCAM2. Este exemplo é simplificado excedentemente a fim ilustrar a diferença entre as versões TCAM. O software do Catalyst 4500 tem as otimizações numerosas para aumentar a eficiência da programação no TCAM2 para um cenário de configuração prático. O algoritmo de programação TCAM subótimo para a seção TCAM2 deste documento discute estas otimizações.

Para TCAM2 e TCAM 3 no Catalyst 4500, as entradas de TCAM são compartilhadas se o mesmo ACL é aplicado em relações diferentes. Esta otimização salvar o espaço TCAM.

Pesquise defeitos a exaustão de TCAM

Quando a exaustão de TCAM ocorre em Catalyst 4500 Switch durante a programação de uma segurança ACL, um aplicativo parcial do ACL ocorre através do caminho de software. Os pacotes que combinam os ACE que não são aplicados no TCAM são processados no software. Isto que processa no software causa a utilização elevada da CPU. Porque a programação do Catalyst 4500 ACL é dependentes do ordem, o ACL é programado sempre de cima para baixo. Se um ACL específico não cabe inteiramente no TCAM, os ACE na parcela inferior do ACL não estão programados muito provavelmente no TCAM.

Um mensagem de advertência aparece quando um excesso TCAM acontece. 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 pode igualmente ver este Mensagem de Erro no **comando show logging** output se você permitiu o Syslog. A presença desta mensagem indica conclusivamente que algum processamento do software ocorrerá. Consequentemente, pode haver utilização elevada da CPU. O ACL que tem sido programado já nas sobras TCAM programou no TCAM se a exaustão da potencialidade de TCAM ocorre durante o aplicativo do ACL novo. Os pacotes que combinam os ACL que têm sido programados já continuam a ser processados e encaminhado no hardware.

Nota: Se você faz mudanças a um grande ACL, a mensagem TCAM-excedida pode ser indicada. O interruptor tenta reprogram o ACL no TCAM. Na maioria dos casos, o ACL novo, alterado pode ser reprogrammed inteiramente no hardware. Se o interruptor pode com sucesso reprogram o ACL na totalidade no TCAM, esta mensagem aparece:

```
*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** a fim verificar que o ACL está programado inteiramente no hardware.

Esta saída mostra a configuração do ACL 101 ao VLAN1 e à verificação que o ACL está programado inteiramente no hardware:

Nota: Se o ACL não é programado inteiramente, um Mensagem de Erro da exaustão de TCAM pode indicar.

```
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 das `bandeiras` (`L3DenyToCpu`) indica que, se um pacote é negado devido ao ACL, o pacote punted ao CPU. O interruptor manda então um mensagem inatingível de protocolo de mensagem de controle de Internet (ICMP). Este comportamento é o padrão. Quando os pacotes punted ao CPU, a utilização elevada da CPU pode ocorrer no interruptor. Contudo, no Cisco IOS Software Release 12.1(13)EW e Mais Recente, estes pacotes são limite de taxa ao CPU. Na maioria dos casos, Cisco recomenda que você desliga a característica que envia mensagens que não chega a seu destino do ICMP.

Esta saída mostra a configuração do interruptor para não enviar mensagens que não chega a seu destino do ICMP e a verificação do TCAM que programa após a mudança. O estado de ACL 101 é agora `FullyLoaded`, porque a saída do comando mostra. O tráfego negado não vai ao 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
```

Nota: Se o QoS TCAM é excedido durante o aplicativo de alguma política de QoS, essa política específica não está aplicada à relação ou ao VLAN. O Catalyst 4500 não executa a política de QoS no caminho de software. Consequentemente, a utilização CPU não crava quando QoS TCAM 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 o `interruptor ACL que processa a` fila recebe um alto número de pacotes. Um alto número de pacotes indica a exaustão da Segurança TCAM. Esta exaustão de TCAM faz com que os pacotes sejam enviados ao CPU para a transmissão do 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 encontra que o `interruptor ACL que processa a` fila não recebe uma quantidade excessiva de tráfego, refira a utilização elevada da CPU em Catalyst 4500 Switch com base no software do Cisco IOS para outras causas possíveis. O documento fornece a informação em como pesquisar defeitos outras encenações da utilização elevada da CPU.

O Catalyst 4500 TCAM pode transbordar por estas razões:

- Um algoritmo de programação TCAM subótimo para o TCAM2
- O uso excessivo de operações da camada 4 (L4Ops) em um ACL
- ACL excessivos para o Supervisor Engine ou o tipo de switch

Algoritmo de programação TCAM subótimo para o TCAM2

Porque os tipos da seção de TCAM discutem, a eficiência TCAM2 é mais baixo devido ao fato de

que oito entradas compartilham de uma máscara. O software do Catalyst 4500 permite dois tipos de algoritmos de programação TCAM para o TCAM2 que melhoram a eficiência do TCAM2:

- Embalado — Apropriado para a maioria de encenações da segurança ACL**Nota:** Esse é o padrão.
- Dispersado — Usado no cenário IPSG

Você pode mudar o algoritmo a um algoritmo dispersado, mas este não ajuda tipicamente se você configurou somente seguranças ACL, tais como o rACLs. O algoritmo dispersado é somente eficaz nas encenações onde o mesmo ou um ACL similar, pequeno são repetidos em portas numerosas. Esta encenação é o caso com um IPSG que seja permitido em interfaces múltiplas. No cenário IPSG, cada ACL dinâmico:

- Tem um pequeno número de entradasIsto inclui licenças para endereços IP de Um ou Mais Servidores Cisco ICM NT permitidos e uma negação na extremidade a fim impedir o acesso da porta por endereços IP de Um ou Mais Servidores Cisco ICM NT desautorizados.
- Érepetido para todas as portas do acesso configuradoO ACL é repetido para até 240 portas em um Catalyst 4507R.

Nota: O TCAM 3 usa o algoritmo embalado padrão. Porque a estrutura TCAM é uma máscara pela entrada, o algoritmo embalado é o algoritmo melhor possível. Consequentemente, a opção dispersada do algoritmo não é permitida neste Switches.

Este exemplo está em um Supervisor Engine II+ que é configurado para a característica IPSG. A saída mostra que, embora somente 49 por cento das entradas sejam usados, 89 por cento das máscaras estão consumidos:

```
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
```

Neste caso, uma mudança no algoritmo de programação do padrão embalou o algoritmo às ajudas dispersadas do algoritmo. O algoritmo dispersado reduz o uso total da máscara de 89 por cento a 49 por cento.

```
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 dos melhores prática para recursos de segurança em Catalyst 4500 Switch, refira melhores prática dos recursos de segurança do Catalyst 4500 para supervisores.

Uso excessivo do L4Ops em um ACL

O L4Ops do termo refere o uso da **GT**, do **lt**, do **neq**, e das palavras-chaves da **escala na** configuração ACL. O Catalyst 4500 tem limites no número destas palavras-chaves que você pode

usar em um único ACL. A limitação, que varia pelo Supervisor Engine e pelo interruptor, é seis ou oito L4Ops pelo ACL. A tabela 3 mostra o limite pelo Supervisor Engine e pelo ACL.

Tabela 3 – Limite do L4Op pelo ACL nos motores e no Switches diferentes do supervisor do Catalyst 4500

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

Se o limite do L4Op pelo ACL é excedido, um mensagem de advertência está indicado no console. A mensagem é similar 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.
```

Também, se o limite do L4Op é excedido, o ACE específico é expandido no TCAM. Resultados adicionais da utilização de TCAM. Este ACE serve como um exemplo:

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

Com este ACE em um ACL, o interruptor usa somente uma entrada e um L4Op. Contudo, se seis L4Ops são usados já neste ACL, este ACE é expandido às entradas 10 no hardware. Tal expansão pode potencialmente usar-se acima de muitas entradas no TCAM. O uso cuidadoso deste L4Ops impede o excesso TCAM.

Nota: Se este caso envolve o V-10GE do Supervisor Engine e o WS-C4948-10GE, oito L4Ops previamente usados no ACL conduzem à expansão ACE.

Mantenha estes artigos na mente quando você usa o L4Op em Catalyst 4500 Switch:

- As operações L4 estão consideradas diferentes se o operador ou o operando diferem.Por exemplo, este ACL contém três operações L4 diferentes porque a **GT 10** e a **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 estão consideradas diferentes se o mesmo par do operador/operando se aplica uma vez a uma porta de origem e uma vez a uma porta do 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 Catalyst 4500 Switch compartilham do L4Ops quando possíveis.Neste exemplo, as linhas em ***itálicos em caracteres gordos*** demonstram esta encenação:Uso do L4Op para o ACL 101 = o 5Uso do L4Op para o ACL 102 = 4 **Nota:** A palavra-chave do **eq** não consome alguns dos recursos do hardware do L4Op.Uso total do L4Op = **8Nota:** ACL 101 e 102 L4Ops da parte uma.**Nota:** O L4Op é compartilhado mesmo se o protocolo, tal como o TCP ou o User Datagram Protocol (UDP), não combina ou a licença/nega a ação não combina.

ACL excessivos para o Supervisor Engine ou o tipo de switch

Como a tabela 2 mostram, TCAM são uns recursos limitados. Você pode exceder os recursos TCAM de todo o Supervisor Engine se você configura ACL excessivos ou características como o IPSG com um alto número de entradas IPSG.

Se você excede o espaço TCAM para seu Supervisor Engine, tome estas etapas:

- Se você tem um Supervisor Engine II+ e você executa um Cisco IOS Software Release que esteja *mais adiantado* do que o Cisco IOS Software Release 12.2(18)EW, promova à versão de manutenção a mais atrasada do Cisco IOS Software Release 12.2(25)EWA.A potencialidade de TCAM foi aumentada nas liberações mais atrasadas.
- Se você usa a espião DHCP e o IPSG e você começa a ser executado fora do TCAM, a usar a versão de manutenção a mais atrasada do Cisco IOS Software Release 12.2(25)EWA e a usar o algoritmo dispersado no caso do Produtos TCAM2.**Nota:** O algoritmo dispersado está disponível no Cisco IOS Software Release 12.2(20)EW e Mais Recente.A liberação a mais atrasada igualmente tem realces para a melhor utilização de TCAM com espião DCHP e características dinâmicas da inspeção do Address Resolution Protocol (ARP) (DAI).
- Se você começa a ser executado fora do TCAM porque o limite do L4Op está excedido, tente reduzir o uso do L4Op no ACL a fim impedir o excesso TCAM.
- Se você usa muitas ACL ou políticas similares em várias portas no mesmo VLAN, agregue as em um único ACL ou a política na interface de VLAN.Esta agregação salvar algum espaço TCAM. Por exemplo, quando você aplica políticas Voz-baseadas, o padrão QoS com base na porta é usado para a classificação. Este padrão QoS pode causar a potencialidade de TCAM ser excedido. Se você comuta o QoS a com base em VLAN, você reduz o uso TCAM.
- Se você ainda tem os problemas com TCAM espaçam, consideram um Supervisor Engine da extremidade alta, tal como o V-10GE do Supervisor Engine ou o catalizador 4948-10GE.Este Produtos usa o hardware o mais eficiente TCAM 3.

Resumo

O Catalyst 4500 programa os ACL configurados com uso do TCAM. O TCAM permite o aplicativo dos ACL no trajeto do encaminhamento de hardware sem o impacto no desempenho do interruptor. O desempenho é constante apesar do tamanho do ACL porque o desempenho das consultas de ACL está na linha taxa. Contudo, o TCAM é uns recursos finitos. Consequentemente, se você configura um número excessivo de entradas ACL, você excede a potencialidade de TCAM. O Catalyst 4500 executou otimizações numerosas e desde que comandos variar o algoritmo de programação do TCAM a fim conseguir a eficiência máxima. O Produtos TCAM 3 tal como o V-10GE do Supervisor Engine e o catalizador 4948-10GE oferecem a maioria de recursos TCAM para a segurança ACL e as políticas de QoS.

Informações Relacionadas

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