Implemente listas de acesso em roteadores da Internet 12000 Series

Contents

Introduction

Este documento descreve o suporte para listas de controle de acesso (ACLs) nos Cisco 12000 Series Internet Routers.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos fundamentos de como uma ACL funciona em um roteador Cisco.

Consulte estes documentos para obter informações gerais sobre ACLs e seus aplicativos:

- Listas de controle de acesso: Visão geral e diretrizes
- Configuração de serviços IP: Filtrar pacotes IP

Componentes Utilizados

As informações neste documento são baseadas nos Cisco 12000 Series Internet Routers.

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.

Visão Geral do Suporte ACL no Cisco 12000 Series Internet Router

No Cisco 12000 Series Internet Router, as ACLs podem ser processadas em hardware (Application-Specific Integrated Circuit - ASIC), software (a CPU de uma placa de linha) ou como um recurso híbrido - processadas em software com assistência de hardware. Se uma ACL é processada em hardware ou software depende do aplicativo da ACL, do tipo de mecanismo da placa de linha e da interação das ACLs em outras placas de linha.

Os mecanismos de placa de linha do Cisco 12000 Series fornecem diferentes recursos de ACL. Para obter informações de suporte da ACL para um mecanismo de placa de linha específico, vá para a seção correspondente neste documento.

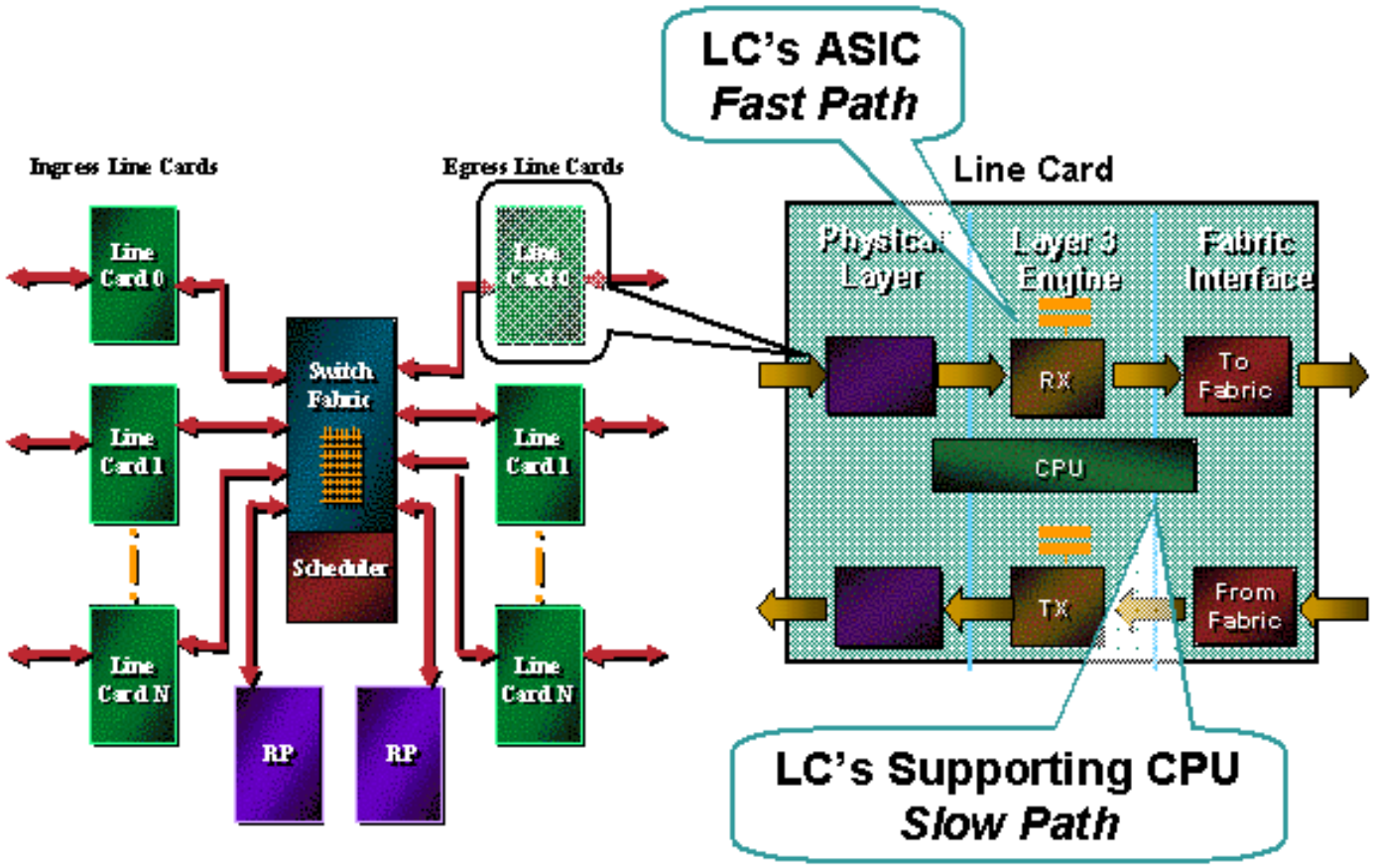
Observação: as ACLs multicast IP não são suportadas no Cisco IOS® Software Release 12.0S. O recurso de limite Multicast IP pode ser usado onde a filtragem multicast é necessária. Consulte Fast-Path Multicast Forwarding em Cisco 12000 Series Engine 2 e ISE Line Cards para obter mais informações.

ACLs com base em ASIC versus ACLs com base em CPU

O Cisco 12000 suporta todas as gerações de processamento de ACL. Uma compreensão operacional de como cada um desses modos de processamento funciona, interage e suporta um ao outro é essencial para o uso efetivo da ACL no Cisco 12000.

As primeiras gerações de processamento de ACL usaram uma CPU programável para processar a ACL. Com o tempo, os requisitos de processamento do pacote por segundo (PPS) excederam a capacidade das novas CPUs de se manterem atualizadas. Os ASICs foram criados para alcançar taxas de PPS mais altas para encaminhamento de roteadores e recursos. As ACLs carregadas na CPU da placa de linha (LC) foram carregadas no ASIC da LC. As ASICs continuaram a ser improvisadas para lidar com taxas de PPS mais elevadas. Esses ASICs de segunda geração foram desenvolvidos com base no trabalho pioneiro da geração anterior e oferecem mais recursos de ASIC. Como o Cisco 12000 é uma plataforma de roteamento distribuído, a interação

entre as várias gerações de processamento de ACL pode criar alguma confusão operacional.



Termos como ACL baseada em ASIC, ACL baseada em CPU, Fast Path, Slow Path e ASIC Punts são usados em todo este documento para ajudar a explicar o que ocorre com o processamento da ACL. Aqui estão explicações sobre estes termos:

- ACLs baseadas em ASIC (Fast Path)—as ACLs são carregadas e processadas no hardware ASIC. O envelope de desempenho do ASIC determina a profundidade, o desempenho e as capacidades do ACL. O Fast Path foi usado no caminho para ilustrar a diferença entre o processamento baseado em ASIC e o processamento feito na CPU que suporta LC. O termo mais genérico, baseado em ASIC, é usado neste documento.
- ACLs baseadas em CPU (Slow Path)—as ACLs são processadas no software na CPU da placa de linha. Para as placas de geração anterior (Engine 0 e, em alguns casos, Engine 1), todo o processamento é feito na CPU do LC. Os LCs baseados em ASIC executam o processamento de ACL em pacotes que são pontuados do ASIC. O caminho lento foi usado no passado para ilustrar como os pontos na CPU do LC eram mais lentos que o ASIC. O termo mais genérico, baseado em CPU, é usado neste documento.
- ASIC Punts — ASICs têm envelopes de design rigorosos. Quando um pacote excede o envelope projetado, ele é pontuado do ASIC para ser processado na CPU de suporte do LC ou enviado para o RP (Route Processor). As ACLs baseadas em ASIC cravam pacotes que estão fora do projeto do ASIC. Um exemplo é uma ACL que tem uma ACE com uma palavra-chave log ou log-input. As informações necessárias para registrar o pacote precisam ser processadas fora da ASIC e, por isso, o pacote é automaticamente apontado para fora da ASIC para a CPU LC e processado como uma ACL com base em CPU normal.

Observação: quando você configura o roteamento baseado em políticas (PBR) com instruções de correspondência para corresponder ACLs, as ACLs não devem corresponder à porta de origem. O roteador de switch gigabit (GSR) não suporta switching de hardware para o PBR com ACLs

que correspondem à porta de origem. Ele aciona a comutação de processos e o desempenho de GSR diminui.

Controle e gerenciamento da filtragem de plano

O Router Processor fornece serviços de plano de controle e gerenciamento na arquitetura distribuída do Cisco 12000 Series. As ACLs de caminho de recepção (rACLs) fornecem um recurso de filtragem distribuída simples para o tráfego de controle e gerenciamento destinado ao RP. Ele pode ser logicamente visto como uma camada adicional de segurança que tira proveito dos pontos fortes de uma arquitetura distribuída.

Configurando ACLs de caminho de recebimento de IP

O rACL foi introduzido através de uma isenção especial no controle de manutenção do Cisco IOS® Software Release 12.0(21)S2. É oficialmente suportado no Cisco IOS Software Release 12.0(22)S. Consulte IP Receive ACL para obter mais informações.

O Processador do Roteador fornece serviços de controle de tráfego aéreo na arquitetura distribuída da série Cisco 12000. As ACLs de recebimento fornecem recursos de filtragem para controlar o tráfego destinado ao RP, como atualizações de roteamento e consultas SNMP (Simple Network Management Protocol).

O rACL é considerado a Fase 1 de um esforço multifase para adicionar novas proteções ao controle e gerenciamento do tráfego plano. Novos aprimoramentos de limitação de taxa estão sendo adicionados por meio de atualizações de software.

Suporte IPv4 ACL por tipo de placa de linha

As placas de linha do 12000 Series fornecem diferentes capacidades de ACL por tipo de mecanismo. Esta seção descreve os recursos da ACL dos diferentes mecanismos de placa de linha. Para obter informações de suporte de ACL para um mecanismo de placa de linha específico, consulte a seção correspondente deste documento.

Há algumas características gerais para todas as ACLs (baseadas em ASIC e CPU):

- Somente uma ACL pode ser aplicada a uma interface para cada direção. Por exemplo, a interface POS 0/0 pode ter apenas uma ACL de entrada e uma ACL de saída.
- Os testes do pacote em relação a uma ACL param quando uma correspondência é localizada. Se uma ACL com 300 entradas corresponder ao pacote na entrada da lista de acesso (ACE) nº 45, o pacote será processado e o processamento da ACL será interrompido.
- Há uma entrada **deny all** implícita no final de cada ACL. Como resultado, se não houver correspondência na ACL, o pacote será descartado. As ACLs da Cisco são criadas com arquitetura de ACL *de permissão explícita*. Isso significa que deve haver uma ACE que corresponda ao pacote para que ele seja processado e encaminhado.
- As ACEs recém-adicionadas são sempre anexadas ao final da ACL. Sempre que a ACL exige atualizações, é uma boa prática remover a ACL (use o comando **no access-list**) e readicionar a nova ACL.
- Como os fragmentos de IP não iniciais não contêm informações de protocolo de Camada 4 no cabeçalho IP, somente os critérios de correspondência padrão são suportados para

fragmentos não iniciais. Detalhes completos sobre como as ACLs da Cisco estão em conformidade com a filtragem de fragmentos IP podem ser encontrados em Access Control Lists e em Fragmentos IP.

- As ACLs numeradas são processadas e aplicadas assim que são inseridas através da interface de linha de comando (CLI). Com ACLs grandes, isso às vezes resulta em um pico de CPU no RP ou na CPU do LC.

Mecanismo 0 – Processamento de ACL

O Engine 0 é a primeira placa de linha fornecida para o Cisco 12000. É todo o processamento e encaminhamento baseado em CPU. Portanto, as placas de linha Engine 0 processam ACLs na CPU do LC.

Essas placas de linha são baseadas no Engine 0:

Tipo de placa de linha	Tipo de interface	Conectividade
12 x DS3	Coaxial	SMB
12 x DS3	Coaxial	SMB
12 x E3	Coaxial	SMB
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR
1xOC12c/STM4c	POS	MM
6xCT3->DS1		SMB
2xCHOC3/STM1- >DS1/E1		IR
4xOC3c/STM1c	ATM	IR
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

Critérios de correspondência suportados

Todas as ACLs padrão, estendidas e turbo do software Cisco IOS versão 12.0S são suportadas no Engine 0.

Número de ACEs suportadas

O tamanho da ACL é limitado somente por requisitos de desempenho e recursos de memória disponíveis.

Processamento de saída ACL

ACLs de saída são processadas no caminho do recurso de ingresso das outras placas de linha do sistema. Um empurrão da ACL de saída para o lado de entrada dos outros LCs protege o backplane de encaminhar pacotes que serão descartados. Esta é uma função herdada da arquitetura distribuída no Cisco 7500. Uma explicação detalhada, os motivos e as diretrizes operacionais são fornecidos na Matriz de Interoperação de Placa de Linha ACL de Saída IPv4.

Comandos específicos da placa de linha

Nenhum.

Diretrizes operacionais e interações de placa de linha

- Se o NetFlow for configurado em uma placa de linha Engine 0 e uma ACL de saída for configurada em uma placa de linha do mecanismo de saída 3 ou 4+, a ACL de saída será processada pelas placas de linha de entrada e de saída para permitir que o NetFlow contabilize os pacotes negados pelas ACLs e os pacotes encaminhados.

Recomendações

A Cisco recomenda o uso de ACLs Turbo no Engine 0 para ACLs grandes. ACLs lineares pequenos são mais eficazes para ACLs menores porque os ACLs turbo precisam de memória extra.

Engine 1 – Processamento de ACL

Overview

A placa de linha Engine 1 é uma ponte entre o processamento baseado em CPU no Engine 0 e o ASIC de encaminhamento/recurso de primeira geração no Engine 2. Por padrão, as placas de linha do Engine 1 processam ACLs no software. Com o Cisco IOS Software Release 12.0(10)S e posterior, o Engine 1 fornece ACLs de hardware para placas equipadas com as versões 4 ou 5 do ASIC Salsa (consulte a Referência de Comando da Placa de Linha abaixo para determinar com qual versão do Salsa uma placa específica está equipada).

Essas placas de linha são baseadas no Engine 1:

Tipo de placa de linha	Tipo de interface	Conectividade
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100BaseF
1xGE	SX,	GBIC:
1xGE	SX,	GBIC:
2xOC12c/STM4c	DPT	IR

2xOC12c/STM4c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	MM
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	MM

Critérios de correspondência suportados

Todas as ACLs padrão, estendidas e turbo do software Cisco IOS versão 12.0S são suportadas na CPU LC (Slow Path). Além disso, o Engine 1 pode processar ACLs de entrada no ASIC de Salsa. O Salsa ASIC lida com o processamento da ACL de entrada junto com a pesquisa de rota, resultando em maior desempenho quando comparado ao processamento da ACL linear tradicional e ao processamento da ACL turbo. O SALSA ASIC não pode processar ACLs de saída ou ACLs de subinterface.

Número de ACEs suportadas

O tamanho da ACL é limitado somente por requisitos de desempenho e recursos de memória disponíveis.

Processamento de saída ACL

ACLs de saída são processadas no caminho do recurso de ingresso das outras placas de linha do sistema. Consulte a seção IPv4 Output ACL - Line Card Interoperation Matrix para obter mais informações.

Comandos específicos da placa de linha

- **access-list hardware salsa**
- **show controller l3 | incluir ASIC**

Diretrizes operacionais e interações de placa de linha

- O Salsa ASIC e PSA ASIC não podem ser operados simultaneamente. O comando access-list hardware aceita apenas PSA (Engine 2) ou Salsa (Engine 1), mas não ambos.
- Se o NetFlow for configurado em uma placa de linha Engine 1 e uma ACL de saída for configurada em uma placa de linha do mecanismo de saída 3 ou 4+, a ACL de saída será processada pelas placas de linha de entrada e de saída para permitir que o NetFlow contabilize os pacotes negados pelas ACLs e os pacotes encaminhados.

Recomendações

Para versões de placas de linha Engine 1 que não suportam ACLs de hardware, a Cisco recomenda o uso de ACLs Turbo para ACLs grandes. ACLs pequenas (com menos de 20 linhas) podem ser implementadas com ACLs lineares para conservar memória.

Mecanismo 2 - Processamento de ACL

Overview

O Engine 2 foi a primeira placa com um ASIC de encaminhamento/recurso. Com o Cisco IOS Software Release 12.0(10)S ou posterior, as placas de linha Engine 2 fornecem recursos de ACL de hardware no Packet Switching ASIC (PSA) de alto desempenho. Como em todos os ASICs de encaminhamento/recurso, envelopes de desempenho rigorosos colocam limites na capacidade do ASIC. O principal envelope de desempenho nas ACLs do Engine 2 é devido às limitações de memória no ASIC PSA.

O encaminhamento de pacotes no Engine 2 é feito pelo PSA ASIC. O PSA tem três memórias externas principais:

- PLU (Path-lookup)—Usado para armazenar nós de trie
- TLU (Table Lookup)—Usado para armazenar folhas FIB e possivelmente estruturas de balanceamento de carga. Também usado para conter muitas das estruturas de dados da ACL PSA
- SRAM—O local principal para estruturas de compartilhamento de carga

O recurso PSA ACL é uma implementação baseada em microcódigo da verificação de ACL. Um conjunto especial de instruções é carregado no chip PSA que permite a verificação básica da ACL. Há várias limitações para esse recurso que devem ser cuidadosamente compreendidas antes da implantação. Uma desvantagem importante para as ACLs PSA é a grande quantidade de memória de encaminhamento de hardware necessária.

O recurso PSA ACL exige que um grande bloco de memória PLU/TLU seja pré-alocado independentemente do número de prefixos, etc. Como essa alocação vem principalmente da área TLU, ela tem um impacto significativo no número de rotas que podem ser mantidas nessas placas quando as ACLs PSA são configuradas.

Além do descarte inicial da memória PLU/TLU, cada prefixo armazenado na memória TLU requer significativamente mais memória. A quantidade de memória necessária para cada prefixo varia, com base na direção da ACL aplicada (entrada vs saída) e no tipo de placa de linha. Em geral, as ACLs de saída exigem mais memória que ingresso e as placas de linha com mais portas físicas exigem mais memória do que aquelas com menos portas.

Caso a placa de linha Engine 2 não use ACLs, as estruturas de dados para ACL são criadas independentemente das ACLs reais configuradas. Para alterar para estruturas não-ACL menores, você deve configurar **nenhum psa de hardware de lista de acesso** no roteador. Esse comando desabilita todo o processamento da ACL em todas as placas de linha Engine2 em todas as direções. A Cisco recomenda usá-los com extremo cuidado.

Overview

Para fornecer desempenho de processamento de ACL independente da profundidade de correspondência, as ACLs do Engine 2 são integradas na tabela de encaminhamento de hardware. Veja abaixo explicações sobre como isso pode afetar a escalabilidade do prefixo.

Essas placas de linha são baseadas no Engine 2:

Tipo de placa de	Tipo de interface	Conectividade

linha		
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	Ativador	SR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	ATM	IR
4xOC12c/STM4c	ATM	MM
8xOC3cSTM1c	ATM/TS	IR
8xOC3c/STM1c	ATM/TS	MM
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

Critérios de correspondência suportados

Todos os critérios de compatibilidade de ACLs padrão e estendida suportados pelo Cisco IOS Software Release 12.0S, exceto as portas de origem da Camada 4. Máscaras descontínuas, campos de precedência de IP e portas de origem da Camada 4 são pontuadas do ASIC de PSA e processadas na CPU do LC.

Número de ACEs suportadas

Até cinco ACLs de entrada de 448 linhas no PSA. Uma ACL pode ser configurada por porta. As ACLs adicionais são administradas pela CPU da placa de linha. Veja a seção "Restrições" abaixo para restrições nas ACLs de saída.

Processamento de saída ACL

Uma ACL de saída configurada nesta placa de linha será executada no caminho do recurso de entrada das outras placas de linha no sistema. Consulte a ACL de saída IPv4 - Line Card Interoperation Matrix para obter detalhes.

Comandos específicos da placa de linha

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

Diretrizes operacionais e interações de placa de linha

- O processamento de ACL de caminho rápido exige que essas condições sejam atendidas:O ACL aplicado está dentro do limite de 128 ou 448.O comprimento deve ser inferior a 128 ACEs se o comando **access-list hardware psa limit 128** estiver configurado.Quando o pacote de microcódigo de ACL de 448 linhas for necessário, o comprimento deve ser menor que 448 ACEs.As ACLs de entrada e saída não são configuradas juntas por placa.Até cinco ACLs de saída podem ser configuradas no roteador.
- Somente ACLs de 128 linhas são suportadas em placas de linha POS OC-3/STM-1 de 8 e 16 portas. 448 ACLs de linha são suportados no POS OC-12/STM-4 de 4 portas, no POS OC-48/STM-16 de 1 porta e em placas de linha de Gigabit Ethernet de 3 portas.
- As ACLs de entrada têm prioridade no caminho rápido sobre as ACLs de saída quando ambas são configuradas simultaneamente na mesma placa (a ACL de saída é processada no caminho lento).
- Se uma ACL de saída for configurada em uma placa Engine 2 e a placa de linha de entrada for Engine 0/1/2/4, uma ACL de saída será processada na placa de entrada. Para outros tipos de mecanismo, a ACL de saída será processada no caminho lento de saída do Engine 2.
- As ACLs de saída não são suportadas para o tráfego IP para MPLS (o primeiro rótulo MPLS é "enviado" para um pacote IP).
- As informações de processamento da ACL são integradas ao FIB do hardware e podem afetar a escalabilidade do prefixo. A exaustão da memória do prefixo é relatada por falhas de alocação de memória com a assinatura "exmem=1" na mensagem de log que acompanha.

Recomendações

- As informações de processamento da ACL são integradas na tabela de encaminhamento CEF, o que reduz a escalabilidade do prefixo. Os aplicativos que não usam ACLs podem desabilitar o suporte ACL na tabela CEF e, portanto, aumentar a memória de prefixo disponível emitindo o comando **no access-list hardware psa**.
- A configuração do comando **no access-list hardware psa** desabilita todo o processamento da ACL por placas Engine 2, além de desabilitar o suporte PSA para ACLs. Ele não força a execução de software de ACLs. Essa condição também se aplica caso a placa de ingresso de saída tenha um ACL de saída configurado.
- A configuração do comando **access-list collection** após o comando **access-list hardware psa**

converte ACEs que excedem a capacidade do PSA em um Turbo ACL. Isto dá um desempenho de ACL ótimo para ACLs acima de 448 ACEs de comprimento.O microcódigo ACL padrão é 128 (a partir da versão 12.0(14)S/ST do Software Cisco IOS). Se ACLs menores estiverem em uso e a capacidade de 448 linhas não for necessária, a configuração do **comando access-list hardware psa limit 128** conserva a memória de encaminhamento (TLU), que melhora a escalabilidade do prefixo).O processamento da ACL turbo deve ser ativado com o comando **access-list collection** para ACLs maiores que 129 linhas, juntamente com o comando **access-list hardware psa limit 128**. Essa combinação processa as primeiras 128 linhas no ASIC PSA e as linhas restantes com ACLs Turbo, o que otimiza o desempenho enquanto conserva a memória de encaminhamento.

- A placa de linha ATM OC12 de 4 portas não suporta ACLs de entrada, mas fornece detecção de ACL de saída em microcódigo, o que permite o processo de ACL de saída no caminho lento.
- A placa de linha ATM 8xOC3 suporta ACLs de linha por vc 128 com Cisco IOS Software Release 12.0(23)S e posteriores. Um máximo de 16 ACLs de entrada distintas podem ser configuradas em caminho rápido. A ACL de 448 entradas é suportada por VC somente em caminho lento. As ACLs de saída não são suportadas.

Mecanismo 3 do ISE (IP Services Engine) - Processamento de ACL

Overview

O Engine 3 é a primeira placa de linha de encaminhamento de estágio duplo. O Engine 3 possui ASICs de encaminhamento/recursos no caminho de ingresso e saída. Isso permite que as ACLs sejam colocas no ASIC nos caminhos de entrada e de saída. Além disso, a estrutura ASIC do Engine 3 é um pipeline híbrido/array paralelo. A estrutura do ASIC implementa o processamento de ACL em TCAM (High-Speed Content Addresses Memory, memória endereçável de conteúdo ternário de alta velocidade) paralela, que fornece processamento de taxa de linha de até 20 K ACEs por entrada e 20 K ACEs por saída.

Essas placas de linha são baseadas no Engine 3:

Tipo de placa de linha	Tipo de interface	Conectividade
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xCHOC12/STM4 ->OC3/STM1- >DS3/E3	POS	IR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
8xOC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	IR
4xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	LR
1xOC48c/STM16	POS	SR

c		
1xOC48c/STM16c	POS	LR
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4xGE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

Critérios de correspondência suportados

Todos os critérios de correspondência padrão e estendida do software Cisco IOS versão 12.0S são suportados no caminho rápido, exceto para ACEs de log que são processados pela CPU da placa de linha.

Número de ACEs suportadas

- Processamento de taxa de linha na direção de entrada e saída por porta, por VLAN, por subinterface de Frame Relay e por subinterface ATM. Até 20.000 ACEs estendidos por direção e por placa são suportados.
- Os critérios de correspondência para a porta origem/destino TCP/UDP "range", "lt" e "gt" são todos tratados no hardware usando recursos "operador L4".
- O número de operandos L4 distintos é limitado a 32 para toda a placa de linha. Os operadores de porta de origem estão limitados a um máximo de seis.

Processamento de saída ACL

Suporte nativo a caminho rápido para processamento de ACL de saída de taxa de linha no ASIC de processamento de pacote de caminho de transmissão. Consulte a ACL de saída IPv4 - Line Card Interoperation Matrix para obter detalhes.

Comandos específicos da placa de linha

- **hw-module <*slot #*> tcam compilação no-merge***!—12.0(21)S3*
- **show-access-list hardware interface <*nome da interface*>**
- **show cef int pos[*x/y*] | inc if_number**

Diretrizes operacionais e interações de placa de linha

- Os pacotes correspondentes às ACEs de registro são processados no caminho lento.
- Pacotes que correspondem aos ACEs negados (acelerados para evitar a interrupção do sistema) são processados no caminho lento.
- Quando uma ACL inclui um intervalo de endereços, o hardware usa ACEs especiais

chamadas "ACEs de intervalo" que exigem até três ACEs.

- A união de ACL pode conservar os recursos de TCAM compartilhando ACEs comuns entre ACLs individuais. Para determinar se um ACL está oculto, use o comando de interface de hardware show-access-list.
- Os contadores de ACL não são suportados para ACLs mescladas. Com o Cisco IOS Software Release 12.0(21)S3 e posterior, a mesclagem de ACL pode ser desabilitada com o comando **hw-module <slot #> tcam collection no-merge**. Para determinar se uma ACL é mesclada, use o comando **show-access-list hardware interface**.
- Se o NetFlow for configurado em uma placa de linha Engine 0/1 e uma ACL de saída for configurada em uma placa de linha Engine 3 ou 4+ de saída, a ACL de saída será processada pelas placas de linha de entrada e de saída para permitir que o NetFlow contabilize os pacotes negados pelas ACLs, bem como os pacotes encaminhados.

Suporte ao contador de ACL

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

Definições:

- Por ACE—Suporte normal do software Cisco IOS, o **comando show access-list <*number*>** no RP/LC exibe a ACL e o contador associados a cada ACE. Ele está disponível somente quando a **mesclagem** está desativada antes de você configurar qualquer ACL. Isso pode ser feito usando este comando de configuração:
  `Router(config)#hw-module slot <number> tcam compile acl no-merge`

  Esta opção quando ativada desativa algumas otimizações de mesclagem de TCAM e afeta a escalabilidade. O efeito exato depende dos ACLs individuais.Observe também que os contadores não estarão corretos se o roteamento baseado em políticas for aplicado nessa interface. Nesse caso, deve ser usado o contador agregado.
- Por ACE (TCAM)—Contadores de hardware associados a cada entrada TCAM. Nenhuma configuração é necessária e não há impacto no desempenho/escalabilidade. Disponível somente na placa de linha usando esta CLI. Esses contadores não podem ser zerados pelo software.
  `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace`

  Uma nova CLI genérica para este comando estará disponível no Cisco IOS Software Release 22S:
  `LC-Slot4#show access-list hardware interface p0:1 in`

  Como no contador por ACE, os contadores TCAM são válidos somente quando PBR não é usado nessa interface com ACL.
- Agregado—Cada ACL mostra um contador de permissão/negação de resumo. É a soma de todos os contadores ACE individuais. Nenhuma configuração é necessária e não há impacto no desempenho ou na escalabilidade.

Recomendações

Nenhuma no momento.

Mecanismo 4 (POS) - Processamento de ACL

Overview

O mecanismo 4 fornece este suporte de ACL com o software Cisco IOS versão 12.0(18)S e posterior:

- As ACLs de saída são suportadas nas placas de linha E0/1/2 se a placa de linha Engine 4 for a placa de entrada. Nesta configuração, a ACL de saída é processada pela CPU da placa de linha de saída.

Essas placas de linha são baseadas no Engine 4:

Tipo de placa de linha	Tipo de interface	Tipo de mecanismo	Conectividade
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

Mecanismo 4+ (POS e DPT) – Processamento de ACL

Overview

O Engine 4+ introduz a funcionalidade da ACL ao portfólio de 10 Gigabits Cisco 12000 Series.

Até 1024 ACEs são suportados em cada caminho de entrada e saída. As ACLs de entrada e saída são processadas na taxa de linha para até 96 ACEs. O desempenho de compatibilidades maiores varia de acordo com a complexidade da compatibilidade.

Essas placas de linha POS são baseadas no Engine 4+:

Tipo de placa de linha	Tipo de interface	Conectividade
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM6	POS	IR

4c		
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

Critérios de correspondência suportados

Todos os critérios de ACL padrão e estendida suportados pelo Cisco IOS Software Release 12.0S são suportados no caminho rápido, exceto para ACEs de log ou fragmento.

Número de ACEs suportadas

Até 1024 ACEs são suportados por direção no caminho rápido.

Observação: 1021 das ACEs são configuráveis. Três entradas são reservadas para os ACEs implit **permit ip any any any**, **deny ip any any** e **send to CPU** commands.

Não há limite máximo para o número de ACEs suportados. Todas as ACEs além do limite de 1021 são executadas no caminho lento da placa de linha.

Processamento de saída ACL

Os ACLs de saída são processados no caminho rápido do lado de transmissão. Consulte a ACL de saída IPv4 - Line Card Interoperation Matrix para obter detalhes.

Comandos específicos da placa de linha

- **show tcam appl [*acl-in*] | *acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in*] | *acl-out*] memory <*port*> <*número de entradas*>**

Diretrizes operacionais e interações de placa de linha

- As ACLs de subinterface não são suportadas.
- O desempenho varia com a profundidade de correspondência.

- Entradas de intervalo usam duas regras de ACL (três se as duas entradas cruzarem um limite).
- Um ACL por interface física é suportado .
- Até 1024 ACEs (por direção) são suportadas no caminho rápido.
- Qualquer uma das 1024 ACEs de caminho rápido pode ser compartilhada entre portas.
- As ACEs que usam a palavra-chave fragment são filtradas no caminho lento.
- Os pacotes negados não são contados para ACEs sendo processados no caminho lento.
- Se o NetFlow for configurado em uma placa de linha Engine 0 e uma ACL de saída for configurada em uma placa de linha de mecanismo de saída 3 ou 4+, a ACL de saída será processada pelas placas de linha de entrada e de saída para permitir que o NetFlow contabilize os pacotes negados pelas ACLs, bem como os pacotes encaminhados.

Recomendações

Nenhuma no momento.

Mecanismo 4+ (Ethernet) - Processamento ACL

Overview

As placas de linha Engine 4+ Ethernet apresentam a funcionalidade de entrada ACL por vlan no hardware para o portfólio Cisco 12000 10-Gigabit Ethernet. Estas são algumas das características:

- As ACLs de entrada e saída podem ser aplicadas simultaneamente em uma única porta sem afetar o desempenho.
- As ACLs podem ser aplicadas por VLAN ou por porta.
- O desempenho da ACL de entrada de até 15K ACEs não diminui com a profundidade de correspondência.
- As ACLs de saída são processadas na taxa de linha para até 96 ACEs. O desempenho de compatibilidades maiores varia de acordo com a complexidade da compatibilidade.

Essas placas de linha Ethernet são baseadas no Engine 4+:

Tipo de placa de linha	Tipo de interface	Tipo de mecanismo
10xGE Rev B ("X-B")	SFP:	E4+
Modular	SFP:	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

Critérios de correspondência suportados

Todos os critérios de ACL padrão e estendida suportados pelo Cisco IOS Software Release 12.0S são suportados no caminho rápido, exceto para ACEs de log ou fragmento.

Número de ACEs suportadas

- Até 15.000 ACLs de entrada que podem ser configuradas por porta ou por VLAN.
- 1024 ACEs de saída por placa que podem ser aplicadas por porta.**Observação:** 1021 das ACEs são configuráveis. Três entradas são reservadas para os ACEs implit **permit ip any any any**, **deny ip any any** e **send to CPU** commands.

Processamento de saída ACL

As ACLs de saída são processadas originalmente no caminho rápido no lado de transmissão. Consulte a ACL de saída IPv4 - Line Card Interoperation Matrix para obter mais informações.

Comandos específicos da placa de linha

- **hw-module slot <*number*> ip acl merge**

Diretrizes operacionais e interações de placa de linha

- As ACEs que contêm a palavra-chave fragment são processadas no caminho lento.
- Os contadores de ACL não são suportados para ACLs combinadas com outros recursos.
- Os contadores de ACL não são suportados para ACLs mescladas. As ACLs mescladas são configuráveis com o comando **hw-module slot <*slot number*> ip acl merge**.
- Até 168 operações L4 são suportadas por placa de linha. Quando isso é excedido, a ACL é executada no caminho lento.
- Se uma placa de linha Engine 1 tiver o NetFlow de amostra ativado e uma ACL de saída estiver habilitada em uma placa de linha Engine 3 ou 4+ de saída, a ACL de saída será processada pelas placas de linha de entrada e de saída para permitir que o NetFlow contabilize os pacotes negados pelas ACLs e os pacotes encaminhados.

Recomendações

Nenhuma no momento.

Registro de ACL

Antes do Cisco IOS Software Release 12.0(21)S, as informações de registro da ACL foram enviadas ao RP exclusivamente através do MBUS (Maintenance Bus, barramento de manutenção). Durante altos níveis de atividade de registro da ACL, foi possível exceder a capacidade do MBUS. O Cisco IOS Software Release 12.0(21)S introduz várias otimizações que impedem esse cenário.

As situações de sobrecarga de MBUS são relatadas pelo software Cisco IOS com estas mensagens de erro:

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

Com o Cisco IOS Software Release 12.0(21)S e posterior, mensagens de registro de alta gravidade (gravidade 0-4) são entregues ao RP através do MBUS, enquanto mensagens de

registro de gravidade mais baixa (gravidade 5-7) são entregues ao RP através da matriz de comutação de maior capacidade. As mensagens de log da ACL são de alta gravidade, portanto agora são entregues ao RP através da matriz de comutação.

Essa funcionalidade de registro adicionada é configurável usando estes comandos:

- **logging method mbus [*Severity*]** — Determina quais mensagens, por gravidade, serão enviadas ao RP usando o MBUS. Mensagens de maior gravidade serão enviadas através da matriz de comutação.
- **show logging method** — Exibe o método de registro atual para todos os níveis de gravidade da mensagem.
- **logging sequence-nums** —Este comando permite que a placa de linha de envio sequencie mensagens de log numérico para que as mensagens possam ser reordenadas corretamente pelo RP. Sem esse comando, as mensagens de log podem ser entregues ao RP em ordem não sequencial.

IPv4 Saída ACL – Matriz de interoperação de placa de linha

Antes da introdução do processamento de ACL de saída com a versão do Engine 3 e do Engine 4+, as ACLs de saída eram processadas pela placa de linha de entrada. Os ACLs de saída foram atualizados para aproveitar os recursos de processamento de ACL de saída de alto desempenho do Engine 3 e do Engine 4+.

Este gráfico fornece um resumo de onde as ACLs de saída são processadas para diferentes combinações de placas de linha:

	Placa de Saída					
Placa de linha de entrada (ACL de saída aplicada à interface do membro)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E1	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E2	Ingresso	Ingresso	Ingresso	Saída	n/a	Saída
E3	Saída	Saída	Saída	Saída	n/a	Saída
E4	Saída	Saída	Saída	Saída	n/a	Saída
E4+	Saída	Saída	Saída	Saída	n/a	Saída

Suporte ACL de IPv6

As ACLs estendidas IPv6 são suportadas no caminho lento (entrada e saída) em E0, E1, E2, E3 e

E4+ no Cisco IOS Software Release 12.0(23)S.

No Engine 3, a funcionalidade da ACL IPv6 é suportada em hardware no Cisco IOS Software Release 12.0(25)S. As ACLs são aplicadas a uma interface específica, com uma instrução deny implícita no final de cada lista de acesso. As ACLs IPv6 são configuradas usando o comando **ipv6 access-list** com as palavras-chave deny e permit no modo de configuração global. As placas baseadas em Engine 3 suportam a filtragem de cabeçalhos de opções IPv6 baseados em tráfego, rótulos de fluxo e, opcionalmente, informações de tipo de protocolo de camada superior.

Referência a comandos de ACL do Cisco 12000

Comandos do Engine 1

- **access-list hardware salsa**
- **show controller l3 | incluir ASIC**

Comandos do Engine 2

- **access-list hardware psa limit 128**
- **no access-list hardware psa**
- **psa bypass**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

Comandos do Engine 3

- **hw-module <*slot #*> tcam compilação no-merge***!— a partir do software Cisco IOS versão 12.0(21)S3***
- **show-access-list hardware interface <*nome da interface*>**
- **show contr [*tofab|frfab*] alfa acl <*int*> vmr2ace**

Comandos Engine 4+

- **rótulo show access-list gen7**
- **show tcam appl [*acl-in] | acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in] | acl-out*] memory <*port*><*número de entradas*>**

Comandos Engine 4+ Ethernet

- **hw-module slot <*number*> ip acl merge**

Glossário

Esta seção fornece definições padrão de termos relevantes:

- **Planos de processamento**—Um dispositivo de rede pode ser logicamente dividido em três planos de processamento:Plano de dados—Processamento nos pacotes que fluem pelo dispositivo de rede.Plano de controle—Processamento nos pacotes usados para colar dispositivos de rede. Isso inclui protocolos de linha (como os Protocolos PPP e HDLC), protocolos de roteamento (Protocolo BGP, Protocolo RIPv2, Protocolo OSPF e assim por diante) e protocolos de cronometragem (como o Protocolo NTP).Plano de

gerenciamento—Processamento em pacotes usados para gerenciar os dispositivos de rede. Isso inclui telnet, Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), SNMP e outros protocolos de gerenciamento.
- **ACLs padrão**—As ACLs padrão filtram exclusivamente na Camada 3.
- **ACLs estendidas** —As listas de acesso IP estendidas usam endereços de origem e de destino para operações correspondentes, bem como informações opcionais de tipo de protocolo para melhor granularidade de controle.
- **ACLs processadas linearmente** —Processadas linearmente no software. O desempenho varia de acordo com a profundidade da correspondência (o número de entradas que precisam ser verificadas antes que uma correspondência seja determinada).
- **ACLs Turbo (Compiladas)** — As ACLs Turbo otimizam o processamento da ACL do software compilando uma ACL em uma série altamente otimizada de tabelas de pesquisa que aceleram o processamento do software. O desempenho das ACLs Turbo não varia com a complexidade de compatibilidade.
- **ACLs de entrada** —uma ACL aplicada ao tráfego que entra na porta à qual é aplicada.
- **ACLs de saída** — uma ACL aplicada ao tráfego que sai da porta em que é aplicada. Com algumas exceções, as ACLs de saída são processadas pela placa de linha de entrada.
- **ACLs de caminho de recepção** —As ACLs de caminho de recepção fornecem filtragem para o tráfego de controle destinado ao próprio roteador, como atualizações de roteamento e consultas SNMP.
- **Placa de linha de encaminhamento de estágio duplo** —Placas de linha que têm ASICs de encaminhamento/recurso no caminho de entrada e saída. Isso permite que a placa de linha execute recursos no fluxo de pacote de entrada e no fluxo de pacote de saída sem colocar pacotes na CPU do LC. Ele também permite que novas ondas de algoritmos de encaminhamento de estágios duplos sejam usadas no Cisco 12000. A placa de linha Engine 3 é um exemplo de uma placa de linha de encaminhamento de estágio duplo.
- **Placa de linha de encaminhamento de estágio único** —Placas de linha que têm ASICs de encaminhamento/recurso apenas no caminho de entrada. Essas placas de linha executam somente processamento baseado em ASIC nos pacotes que fluem no caminho de entrada. O tráfego de saída não é processado (apenas encaminhado), tratado pelos ASICs de entrada de outros LCs ou gerenciado pela CPU do LC. Engine 2, Engine 4 e Engine 4+ são exemplos de Placas de Linha de Encaminhamento de Estágio Único.

Informações Relacionadas

- Cisco 12000 Series Internet Routers
- Suporte Técnico e Documentação - Cisco Systems