Implementar listas de acceso en routers de Internet de la serie 12000

Contenido

Introducción

Este documento describe la compatibilidad con las listas de control de acceso (ACL) en los routers de Internet de la serie Cisco 12000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de los fundamentos de cómo funciona una ACL en un router Cisco.

Consulte estos documentos para obtener información general sobre las ACL y sus aplicaciones:

- Listas de control de acceso: Información General y Pautas
- Configuración de los Servicios IP: Filtrar paquetes IP

Componentes Utilizados

La información de este documento se basa en los routers de Internet de la serie Cisco 12000.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Información general sobre el soporte de ACL en el router de Internet de la serie Cisco 12000

En el router de Internet de la serie 12000 de Cisco, las ACL se pueden procesar en hardware (circuito integrado para aplicaciones específicas - ASIC), software (CPU de tarjeta de línea) o como función híbrida, y se procesan en software con asistencia de hardware. Si una ACL se procesa en hardware o software depende de la aplicación ACL, el tipo de motor de tarjeta de línea y la interacción de las ACL en otras tarjetas de línea.

Los motores de la tarjeta de línea de la serie 12000 de Cisco proporcionan capacidades ACL diferentes. Para obtener información de soporte de ACL para un motor de tarjeta de línea determinado, vaya a la sección correspondiente de este documento.

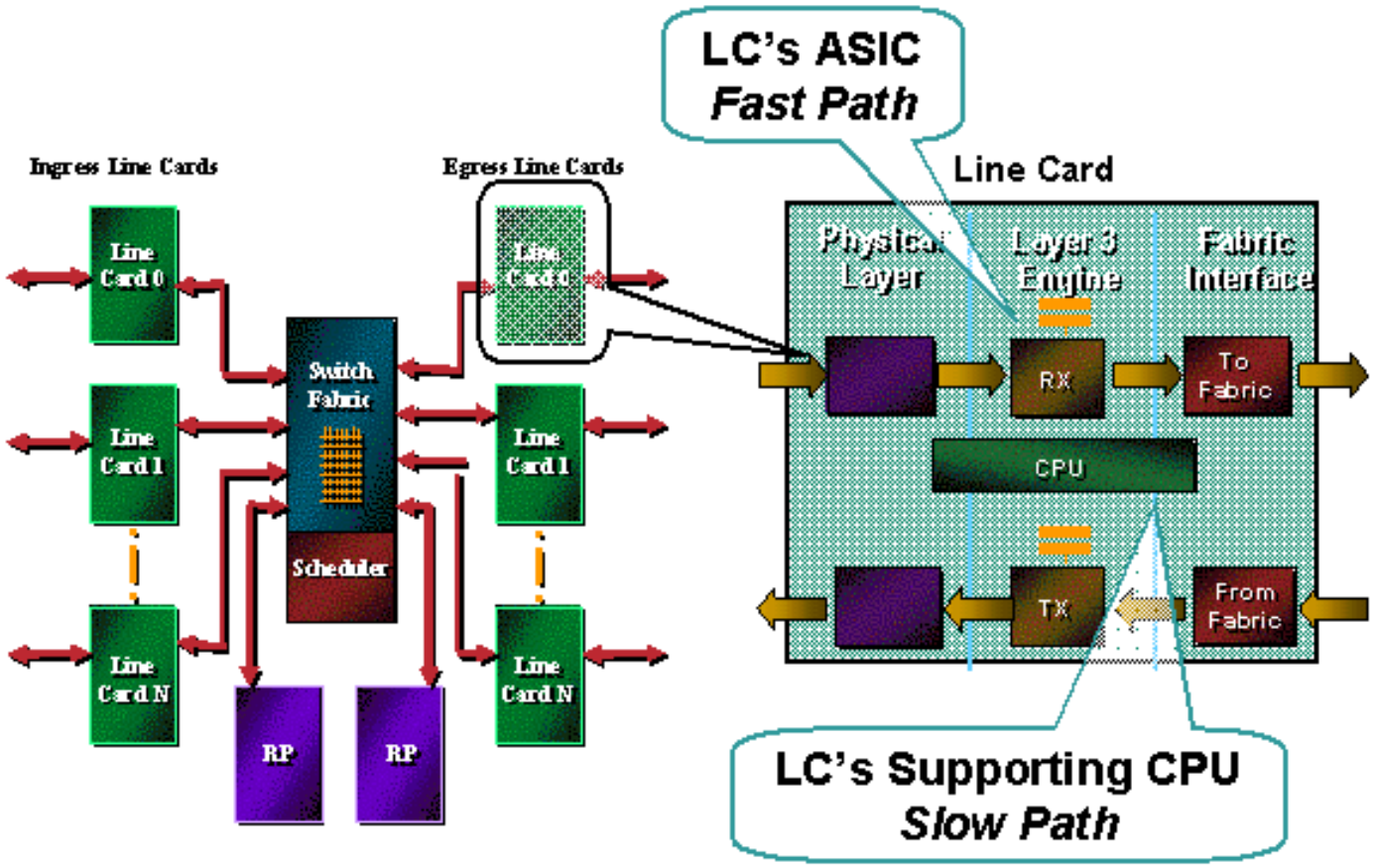
Nota: Las ACL de IP Multicast no se soportan en Cisco IOS® Software Release 12.0S. La función de límite de multidifusión IP se puede utilizar donde se requiere filtrado de multidifusión. Refiérase a Fast-Path Multicast Forwarding en Cisco 12000 Series Engine 2 y Tarjetas de Línea ISE para obtener más información.

ACL basadas en ASIC frente a ACL basadas en CPU

El Cisco 12000 admite todas las generaciones de procesamiento ACL. Una comprensión operativa de cómo funcionan, interactúan y se soportan entre sí cada uno de estos modos de procesamiento es esencial para el uso efectivo de ACL en el Cisco 12000.

Las primeras generaciones de procesamiento de ACL utilizaron una CPU programable para procesar la ACL. Con el tiempo, los requisitos de procesamiento de paquetes por segundo (PPS) excedieron la capacidad de las nuevas CPU para mantenerse al día. Los ASIC se diseñaron para lograr mayores tasas de PPS para el reenvío de routers y las capacidades de funciones. Las ACL cargadas en la CPU de la tarjeta de línea (LC) se cargaron luego en el ASIC LC. Se siguieron improvisando ASIC para gestionar tasas de PPS más elevadas. Estos ASIC de segunda generación se han basado en el trabajo pionero de la generación anterior y ofrecen más funciones ASIC. Dado que Cisco 12000 es una plataforma de routing distribuido, la interacción

entre las diversas generaciones de procesamiento de ACL puede crear cierta confusión operativa.



En este documento se utilizan términos como ACL basada en ASIC, ACL basada en CPU, trayecto rápido, trayecto lento y puntas ASIC para ayudar a explicar qué ocurre con el procesamiento de ACL. A continuación se explican estos términos:

- ACL basadas en ASIC (ruta rápida): las ACL se cargan y procesan en el hardware ASIC. El sobre de desempeño de ASIC determina la profundidad de la ALC, el desempeño y las capacidades. Fast Path se ha utilizado en la trayectoria para ilustrar la diferencia entre el procesamiento basado en ASIC y el procesamiento hecho en la CPU soportada por LC. El término más genérico, basado en ASIC, se utiliza en este documento.
- ACL basadas en CPU (trayecto lento): las ACL se procesan en software en la CPU de la tarjeta de línea. Para las tarjetas de primera generación (Motor 0 y en algunos casos Motor 1), todo el procesamiento se realiza en la CPU LC. Las LC basadas en ASIC realizan el procesamiento de ACL en los paquetes que son impulsados desde el ASIC. En el pasado se utilizó la ruta lenta para ilustrar cómo los punts a la CPU LC eran más lentos que el ASIC. El término más genérico, basado en CPU, se utiliza en este documento.
- Puntas ASIC: los ASIC tienen sobres de diseño estrictos. Cuando un paquete excede el sobre diseñado, se extrae del ASIC para que se procese en la LC que admite la CPU o se envíe al Procesador de ruta (RP). Las ACL basadas en ASIC puntean los paquetes que caen fuera del diseño del ASIC. Un ejemplo es una ACL que tiene una ACE con una palabra clave log o log-input. La información solicitada para registrar el paquete debe ser procesada fuera del ASIC, para que el paquete sea expulsado automáticamente fuera del ASIC, introducido en la CPU de LC y procesado como una ACL normal basada en CPU.

Nota: Cuando configura el routing basado en políticas (PBR) con sentencias coincidentes para que coincidan con las ACL, las ACL no deben coincidir con el puerto de origen. El router de switch gigabit (GSR) no admite switching de hardware para el PBR con ACL que coincidan con el puerto

de origen. Activa el switching de procesos y el rendimiento de GSR se degrada.

Filtrado de planos de administración y control

El procesador del router proporciona servicios de plano de control y gestión en la arquitectura distribuida de la serie Cisco 12000. Las ACL de ruta de recepción (rACL) proporcionan una sencilla capacidad de filtrado distribuido para el control y el tráfico de gestión destinado al RP. Lógicamente, se puede considerar como una capa adicional de seguridad que aprovecha los puntos fuertes de una arquitectura distribuida.

Configuración de los ACL de trayecto de recepción de IP

La rACL se introdujo a través de una exención especial en el acelerador de mantenimiento de Cisco IOS® Software Release 12.0(21)S2. Es oficialmente soportado en Cisco IOS Software Release 12.0(22)S. Consulte ACL de recepción de IP para obtener más información.

El Procesador del router brinda servicios del plano de control en la arquitectura distribuida de la serie Cisco 12000. Las ACL de recepción proporcionan funciones de filtrado para controlar el tráfico destinado al RP, como las actualizaciones de routing y las consultas SNMP (Simple Network Management Protocol).

La rACL se considera la Fase 1 de un esfuerzo de varias fases para agregar nuevas protecciones al control y la administración del tráfico del plano. Se están agregando nuevas mejoras de limitación de velocidad mediante actualizaciones de software.

Soporte de ACL de IPv4 por tipo de tarjeta de línea

Las tarjetas de línea de las series 12000 brindan diferentes capacidades de ACL para cada tipo de motor. Esta sección describe las capacidades ACL de los diferentes motores de tarjeta de línea. Para obtener información de soporte de ACL para un motor de tarjeta de línea determinado, consulte la sección correspondiente de este documento.

Existen algunas características generales para todas las ACL (basadas en ASIC y CPU):

- Sólo puede aplicarse una ACL a una interfaz para cada sentido. Por ejemplo, la interfaz POS 0/0 sólo puede tener una ACL de entrada y una ACL de salida.
- La prueba del paquete contra la ACL se detiene después de que se encontró una coincidencia. Si una ACL con 300 entradas de largo coincide con el paquete de la entrada de lista de acceso (ACE) n.º 45, el paquete se procesa y se detiene el procesamiento de ACL.
- Hay una entrada **deny all** implícita al final de cada ACL. Como resultado, si no hay coincidencia en la ACL, el paquete se pierde. Las ACL de Cisco se crean con la arquitectura ACL *de permiso explícito*. Esto significa que debe haber una ACE para que coincida con el paquete para que se procese y reenvíe.
- Las ACE recién agregadas siempre se agregan al final de la ACL. Siempre que la ACL requiere actualizaciones, es una buena práctica quitar la ACL (utilice el comando **no access-list**) y volver a agregar la nueva ACL.
- Debido a que los fragmentos IP no iniciales no contienen información de protocolo de Capa 4 en el encabezado IP, sólo se soportan los criterios de coincidencia estándar para los fragmentos no iniciales. Puede encontrar detalles completos sobre cómo las ACL de Cisco

cumplen con el filtrado de fragmentos IP en Listas de Control de Acceso y Fragmentos IP.
- Las ACL numeradas se procesan y aplican tan pronto como se ingresan a través de la interfaz de línea de comandos (CLI). Con las ACL grandes, esto a veces da como resultado un pico de CPU en el RP o en la CPU LC.

Motor 0 - Procesamiento de ACL

El motor 0 es la primera tarjeta de línea entregada para el Cisco 12000. Todo es procesamiento y reenvío basado en CPU. Por lo tanto, las tarjetas de línea de Motor 0 procesan las ACL en la CPU LC.

Estas tarjetas de línea se basan en el Motor 0:

Tipo de tarjeta de línea	Tipo de interfaz	Conectividad
12 x DS3	Coaxial	SMB
12 x DS3	Coaxial	SMB
12 x E3	Coaxial	SMB
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS (Packet over SONET)	IR
4x0C3c/STM1c	POS (Packet over SONET)	SR
4x0C3c/STM1c	POS (Packet over SONET)	LR
4x0C3c/STM1c	POS (Packet over SONET)	MM
1xOC12c/STM4c	POS (Packet over SONET)	IR
1xOC12c/STM4c	POS (Packet over SONET)	MM
6xCT3->DS1		SMB
2xCHOC3/STM1- >DS1/E1		IR
4x0C3c/STM1c	ATM	IR
4x0C3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

Criterios de concordancia admitidos

Todos los Cisco IOS Software Release 12.0S Standard, Extended ACL y Turbo ACL son soportados en el Motor 0.

Número de ACE admitidas

El tamaño de la ACL está limitado sólo por los requisitos de rendimiento y los recursos de

memoria disponibles.

Procesamiento de la ACL de salida

Los ACL de salida son procesados en el trayecto de característica de ingreso de las otras tarjetas de línea en el sistema. Una pulsación de la ACL de salida al lado de ingreso de las otras LC protege la placa de interconexiones de los paquetes que se van a descartar. Se trata de una función heredada de la arquitectura distribuida del Cisco 7500. En la Matriz de Interoperación de Tarjeta de Línea de ACL de Salida de IPv4 se proporciona una explicación detallada, los motivos y las pautas operativas.

Comandos específicos de la tarjeta de línea

Ninguno.

Pautas operacionales e interacciones de la tarjeta en línea

- Si NetFlow se configura en una tarjeta de línea de Motor 0 y una ACL de salida se configura en una tarjeta de línea de motor de egreso 3 o 4+, la ACL de salida se procesa tanto por las tarjetas de línea de ingreso como de egreso para permitir que NetFlow contemple los paquetes denegados por las ACL así como los paquetes reenviados.

Recomendaciones

Cisco recomienda el uso de Turbo ACL en el Motor 0 para ACL grandes. Las ACL lineales pequeñas son más eficaces para ACL más pequeñas ya que la ACL Turbo requiere más memoria.

Motor 1 - Procesamiento de ACL

Overview

La tarjeta de línea Engine 1 es un puente entre el procesamiento basado en CPU en el Motor 0 y el ASIC de reenvío/función de primera generación en el Motor 2. Las tarjetas de línea del motor 1 procesan las ACL en el software de forma predeterminada. Con Cisco IOS Software Release 12.0(10)S y versiones posteriores, el Motor 1 proporciona ACL de hardware para tarjetas equipadas con las versiones 4 o 5 de Salsa ASIC (consulte la Referencia de Comandos de Tarjetas de Línea a continuación para determinar con qué versión de Salsa está equipada una tarjeta en particular).

Estas tarjetas de línea se basan en el Motor 1:

Tipo de tarjeta de línea	Tipo de interfaz	Conectividad
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

Criterios de concordancia admitidos

Todas las ACL compatibles con Standard, Extended y Turbo de Cisco IOS Software Release 12.0S son compatibles con la CPU LC (trayecto lento). Además, el Motor 1 puede procesar las ACL de entrada en el ASIC Salsa. El ASIC Salsa gestiona el procesamiento de ACL de entrada junto con la búsqueda de rutas, lo que se traduce en un mayor rendimiento en comparación con el procesamiento de ACL lineal tradicional y el procesamiento Turbo ACL. El SALSA ASIC no puede procesar salidas ni subinterfaces ACL.

Número de ACE admitidas

El tamaño de la ACL está limitado sólo por los requisitos de rendimiento y los recursos de memoria disponibles.

Procesamiento de la ACL de salida

Los ACL de salida son procesados en el trayecto de característica de ingreso de las otras tarjetas de línea en el sistema. Consulte la sección Matriz de Interoperación de Tarjeta de Línea - ACL de Salida IPv4 para obtener más información.

Comandos específicos de la tarjeta de línea

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

Pautas operacionales e interacciones de la tarjeta en línea

- El ASIC Salsa y el ASIC PSA no pueden ser operados al mismo tiempo. El comando access-list hardware acepta sólo PSA (Motor 2) o Salsa (Motor 1) pero no ambos.
- Si NetFlow se configura en una tarjeta de línea de Motor 1 y una ACL de salida se configura en una tarjeta de línea de motor de egreso 3 o 4+, la ACL de salida se procesa tanto por las tarjetas de línea de ingreso como de egreso para permitir que NetFlow contemple los paquetes denegados por las ACL así como los paquetes reenviados.

Recomendaciones

Para las versiones de las tarjetas de línea del Motor 1 que no admiten ACL de hardware, Cisco recomienda el uso de Turbo ACL para ACL grandes. Las ACL pequeñas (menos de 20 líneas) pueden implementarse como ACL lineales para conservar la memoria.

Motor 2 - Procesamiento de ACL

Overview

Engine 2 fue la primera tarjeta de línea con una ASIC de reenvío/función. Con Cisco IOS Software Release 12.0(10)S y versiones posteriores, las tarjetas de línea Engine 2 proporcionan capacidades de ACL de hardware en el ASIC de conmutación de paquetes (PSA) de alto rendimiento. Al igual que con todos los ASIC de reenvío/función, los sobres de rendimiento estricto establecen límites en la capacidad del ASIC. El sobre de rendimiento clave en las ACL del Motor 2 se debe a las limitaciones de memoria en el ASIC PSA.

El reenvío de paquetes en el Motor 2 lo realiza el ASIC PSA. PSA tiene tres memorias externas principales:

- PLU (Path-lookup): se utiliza para almacenar nodos mtrie
- TLU (búsqueda de tabla): se utiliza para almacenar hojas FIB y posiblemente estructuras de balance de carga. También se utiliza para contener muchas de las estructuras de datos de ACL de PSA
- SRAM: la ubicación principal para las estructuras de carga compartida

La función PSA ACL es una implementación basada en microcódigo de la verificación ACL. Se carga un conjunto especial de instrucciones en el chip PSA que permite la verificación de ACL básica. Hay una serie de limitaciones a esta función que deben entenderse cuidadosamente antes de implementarla. Una desventaja importante para las ACL PSA es la gran cantidad de memoria de reenvío de hardware requerida.

La función PSA ACL requiere que se preasigne un bloque grande de memoria PLU/TLU independientemente del número de prefijos, etc. Debido a que esta asignación proviene principalmente del área TLU, tiene un impacto significativo en el número de rutas que se pueden mantener en estas tarjetas cuando se configuran ACL PSA.

Además del desembolso inicial de la memoria PLU/TLU, cada prefijo almacenado en la memoria TLU requiere significativamente más memoria. La cantidad de memoria requerida para cada prefijo varía según la dirección de la ACL aplicada (entrada vs salida) y el tipo de tarjeta de línea. En general, las ACL de salida requieren más memoria que el ingreso, y las tarjetas de línea con más puertos físicos requieren más memoria que las que tienen menos puertos.

En el caso de que la tarjeta de línea de Motor 2 no utilice ACL, las estructuras de datos para ACL se construyen independientemente de las ACL reales configuradas. Para cambiar a las estructuras no ACL más pequeñas, debe configurar **no access-list hardware psa** en el router. Este comando inhabilita todo el procesamiento ACL en todas las tarjetas de línea Engine2 en todas las direcciones. Cisco recomienda utilizarlos con extrema precaución.

Overview

Para proporcionar un rendimiento de procesamiento de ACL independiente de la profundidad de coincidencia, las ACL del Motor 2 se integran en la tabla de reenvío de hardware. Consulte a continuación las explicaciones sobre cómo esto puede afectar a la escalabilidad de prefijos.

Estas tarjetas de línea se basan en el Motor 2:

Tipo de tarjeta de línea	Tipo de interfaz	Conectividad
1xOC48c/STM16c	POS (Packet over SONET)	SR
1xOC48c/STM16c	POS (Packet over SONET)	LR
1xOC48c/STM16c	POS (Packet over SONET)	SR
1xOC48c/STM16c	POS (Packet over SONET)	LR
1xOC192c/STM64c	Habilitador	SR
16xOC3c/STM1c	POS (Packet over SONET)	IR
16xOC3c/STM1c	POS (Packet over SONET)	MM
4xOC12c/STM4c	POS (Packet over SONET)	IR
4xOC12c/STM4c	POS (Packet over SONET)	MM
4xOC12c/STM4c	POS (Packet over SONET)	IR
4xOC12c/STM4c	POS (Packet over SONET)	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

Criterios de concordancia admitidos

Todos los Cisco IOS Software Release 12.0S soportaban criterios de coincidencia de ACL estándar y ampliada, excepto los puertos de origen de capa 4. Las máscaras discontinuas, los campos de precedencia IP y los puertos de origen de Capa 4 se puntean desde el ASIC PSA y se procesan en la CPU LC.

Número de ACE admitidas

Hasta cinco ACL de entrada de 448 líneas en PSA. Se puede configurar una ACL por puerto. La CPU de la tarjeta de línea administra ACL adicionales. Consulte la sección "Restricciones" a continuación para ver las restricciones en las ACL de salida.

Procesamiento de la ACL de salida

Una ACL de salida configurada en esta tarjeta de línea se realizará en la trayectoria de la función de ingreso de las otras tarjetas de línea en el sistema. Consulte la Matriz de Interoperación de Tarjeta de Línea - ACL de Salida IPv4 para obtener más detalles.

Comandos específicos de la tarjeta de línea

- **límite de psa del hardware de lista de acceso 128**
- **no access-list hardware psa**
- **desviación psa**
- **show access-list psa detail**
- **show access-list psa summary**
- **show controller psa feature**

Pautas operacionales e interacciones de la tarjeta en línea

- El procesamiento de ACL de trayecto rápido requiere que se cumplan estas condiciones:La ACL aplicada se encuentra dentro del límite 128- o 448- ACE.La longitud debe ser menor que 128 ACE si el comando **access-list hardware psa limit 128** está configurado.La longitud debe ser menor a 448 ACE cuando se necesita el conjunto de microcódigos ACL de 448 líneas.Las ACL de entrada y salida no se configuran juntas por tarjeta.Se pueden configurar hasta 5 ACL de salida en el router.
- Solamente se soportan ACL de 128 líneas en tarjetas de línea POS OC-3/STM-1 de 8 y 16 puertos. Las ACL de 448 líneas son admitidas en los POS OC-12/STM-4 de 4 puertos, en los POS OC-48/STM-16 de 1 puerto y en las tarjetas de línea Gigabit Ethernet de 3 puertos.
- Las ACL de entrada tienen prioridad en el trayecto rápido sobre las ACL de salida cuando ambas se configuran simultáneamente en la misma tarjeta (la ACL de salida se procesa en el trayecto lento).
- Si se configura una ACL de salida en una tarjeta de Motor 2 y la tarjeta de línea de ingreso es Motor 0/1/2/4, una ACL de salida se procesará en la tarjeta de ingreso. Para otros tipos de motor, la ACL de salida se procesará en la trayectoria lenta de salida del Motor 2.
- Las ACL de salida no se soportan para el tráfico de IP a MPLS (la primera etiqueta MPLS que se "envía" a un paquete IP).
- La información de procesamiento de ACL se integra en la FIB de hardware y puede afectar a la escalabilidad del prefijo. Los errores de asignación de memoria informan del agotamiento de la memoria del prefijo con la firma "exmem=1" en el mensaje de registro adjunto.

Recomendaciones

- La información de procesamiento de ACL se integra en la tabla de reenvío de CEF, lo que

reduce la escalabilidad del prefijo. Las aplicaciones que no utilizan ACL pueden inhabilitar el soporte ACL en la tabla CEF y, por lo tanto, aumentar la memoria de prefijo disponible mediante la ejecución del comando **no access-list hardware psa**.

- La configuración del comando **no access-list hardware psa** inhabilita todo el procesamiento ACL por las tarjetas Engine 2 además de inhabilitar el soporte PSA para las ACL. No fuerza la ejecución de software de las ACL. Esta condición también se aplica si la tarjeta de línea de egreso tiene una ACL de salida configurada.
- La configuración del comando **access-list compilado** después del comando **access-list hardware psa** convierte las ACE que exceden la capacidad del PSA en un Turbo ACL. Esto ofrece un rendimiento óptimo de ACL para ACL de 448 ACE de longitud.El microcódigo predeterminado de ACL es 128 (a partir de la versión 12.0(14)S/ST del software del IOS de Cisco. Si se utilizan ACL más pequeñas y no se requiere la capacidad de 448 líneas, la configuración del comando **access-list hardware psa limit 128** conserva la memoria de reenvío (TLU), lo que mejora la escalabilidad del prefijo).El procesamiento Turbo ACL se debe habilitar con el comando **access-list compilado** para ACL de más de 129 líneas junto con el **comando access-list hardware psa limit 128**. Esta combinación procesa las primeras 128 líneas en el ASIC PSA y las líneas restantes con Turbo ACL, lo que optimiza el rendimiento al tiempo que conserva la memoria de reenvío.
- La tarjeta de línea ATM OC12 de 4 puertos no admite ACL de entrada, pero proporciona detección ACL de salida en microcódigo, lo que permite el proceso de ACL de salida en el trayecto lento.
- La tarjeta de línea ATM 8xOC3 soporta ACL de 128 líneas por VC con Cisco IOS Software Release 12.0(23)S y posteriores. Se puede configurar un máximo de 16 ACL de entrada diferentes en trayecto rápido. La ACL de entrada de 448 se soporta por VC solamente en trayecto lento. Los ACL de salida no son compatibles.

ISE (Motor de servicios IP) Motor 3 – Procesamiento de ACL

Overview

El Motor 3 es la primera tarjeta de línea de reenvío de dos etapas. El Motor 3 posee reenvío/función ASIC tanto en el trayecto de ingreso como en el de egreso. Esto permite colocar las ACL en el ASIC, tanto en el trayecto de entrada como en el de salida. Además, la estructura ASIC del Motor 3 es una matriz híbrida/paralela. La estructura ASIC implementa el procesamiento de ACL en la memoria direccionable ternaria de contenido (TCAM) paralela de alta velocidad, que proporciona un procesamiento de velocidad de línea de hasta 20 000 ACE por ingreso y 20 000 ACE por egreso.

Estas tarjetas de línea se basan en el Motor 3:

Tipo de tarjeta de línea	Tipo de interfaz	Conectividad
4xOC12c/STM4c	POS (Packet over SONET)	IR
4xOC12c/STM4c	POS (Packet over SONET)	MM
4xCHOC12/STM4 ->OC3/STM1-	POS (Packet over SONET)	IR

>DS3/E3		
16xOC3c/STM1c	POS (Packet over SONET)	IR
16xOC3c/STM1c	POS (Packet over SONET)	MM
8xOC3/STM1c	POS (Packet over SONET)	IR
8xOC3c/STM1c	POS (Packet over SONET)	MM
4x0C3c/STM1c	POS (Packet over SONET)	IR
4x0C3c/STM1c	POS (Packet over SONET)	MM
4x0C3c/STM1c	POS (Packet over SONET)	LR
1xOC48c/STM16c	POS (Packet over SONET)	SR
1xOC48c/STM16c	POS (Packet over SONET)	LR
1xCHOC48/STM16->STM4->OC3/STM1->DS3/E3	POS (Packet over SONET)	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4 x GE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

Criterios de concordancia admitidos

Todos los criterios de coincidencia estándar y ampliada de la versión 12.0S del software del IOS de Cisco se soportan en la trayectoria rápida excepto para las ACE de registro que son procesadas por la CPU de la tarjeta de línea.

Número de ACE admitidas

- Procesamiento de velocidad de línea tanto en dirección de ingreso como de egreso por puerto, por VLAN, por subinterfaz Frame Relay y por subinterfaz ATM. Se admiten hasta 20,000 ACE extendidas por dirección y por tarjeta.
- Todos los criterios de coincidencia para el "rango", "lt" y "gt" del puerto de origen/destino TCP/UDP se manejan en el hardware usando recursos de "operador L4".
- El número de operandos L4 diferentes está limitado a 32 para la tarjeta de línea completa. Los operadores de puerto de origen están limitados a un máximo de seis.

Procesamiento de la ACL de salida

Soporte de trayecto rápido nativo para procesamiento de ACL de salida de velocidad de línea en el ASIC de procesamiento de paquetes de trayecto de transmisión. Consulte la Matriz de Interoperación de Tarjeta de Línea - ACL de Salida IPv4 para obtener más detalles.

Comandos específicos de la tarjeta de línea

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

Pautas operacionales e interacciones de la tarjeta en línea

- Los paquetes que coinciden con las ACE de registro se procesan en la trayectoria lenta.
- Las ACE de denegación para la concordancia de paquetes (reguladas como protección ante interrupciones del sistema) se procesan en el trayecto lento.
- Cuando una ACL incluye un rango de direcciones, el hardware utiliza ACE especiales llamadas "ACE de rango" que requieren hasta tres ACE.
- La combinación de ACL puede conservar los recursos TCAM compartiendo ACE comunes entre ACL individuales. Para determinar si una ACL está fusionada, utilice el comando de interfaz de hardware show-access-list.
- Los contadores de ACL no se soportan para las ACL fusionadas. Con Cisco IOS Software Release 12.0(21)S3 y posteriores, la fusión de ACL se puede inhabilitar con el **comando hw-module <slot #> tcam compile no-merge**. Para determinar si una ACL se combina, utilice el comando **show-access-list hardware interface**.
- Si NetFlow se configura en una tarjeta de línea de Motor 0/1 y una ACL de salida se configura en una tarjeta de línea de Motor de egreso 3 o 4+, la ACL de salida será procesada tanto por las tarjetas de línea de ingreso como de egreso para permitir que NetFlow contabilice los paquetes denegados por las ACL así como los paquetes reenviados.

Soporte del contador ACL

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

Definiciones:

- Per-ACE: soporte normal del software Cisco IOS, el comando **show access-list <*number*>** en el RP/LC muestra la ACL y el contador asociados con cada ACE. Sólo está disponible cuando la **combinación** está inhabilitada antes de configurar alguna ACL. Esto se puede hacer usando este comando de configuración:
  `Router(config)#`**`hw-module slot <`***`number`***`> tcam compile acl no-merge`**

  Esta opción cuando está activada desactiva algunas optimizaciones de combinación TCAM y afecta a la escalabilidad. El efecto exacto depende de las ACL individuales.Tenga en cuenta también que los contadores no serán correctos si se aplica el ruteo basado en políticas en esa interfaz. En ese caso, se debe utilizar el contador agregado.

- Per-ACE (TCAM): contadores de hardware asociados a cada entrada TCAM. No es necesaria ninguna configuración y no hay impacto en el rendimiento/escalabilidad. Disponible sólo en la tarjeta de línea mediante esta CLI. Estos contadores no se pueden reiniciar por medio del software.
  `LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace`

  Una nueva CLI genérica para este comando estará disponible en Cisco IOS Software Release 22S:
  `LC-Slot4#show access-list hardware interface p0:1 in`

  Al igual que con el contador por ACE, los contadores TCAM son válidos solamente cuando PBR no se utiliza en esa interfaz con ACL.
- Agregado: cada ACL muestra un contador resumido de permiso/denegación. Esta es la suma de todos los contadores ACE individuales. No es necesaria ninguna configuración y no hay impacto en el rendimiento ni en la escalabilidad.

Recomendaciones

Ninguno en este momento.

Motor 4 (POS) – Procesamiento de ACL

Overview

El Motor 4 proporciona esta compatibilidad de ACL con la versión 12.0(18)S y posteriores del software del IOS de Cisco:

- Los ACL de salida son compatibles con las tarjetas de línea E0 si la tarjeta de ingreso es una tarjeta de línea de motor 4. En esta configuración, la ACL de salida es procesada por la CPU de la tarjeta de línea de egreso.

Estas tarjetas de línea se basan en el Motor 4:

Tipo de tarjeta de línea	Tipo de interfaz	Tipo de motor	Conectividad
4xOC48c/STM16c	POS (Packet over SONET)	E4	
4xOC48c/STM16c	POS (Packet over SONET)	E4	LR
1xOC192c/STM64c	POS (Packet over SONET)	E4	IR
1xOC192c/STM64c	POS (Packet over SONET)	E4	SR
1xOC192c/S	POS (Packet	E4	VSR-1

TM64c	over SONET)		
10xGE	SFP	E4	

Motor 4+ (POS y DPT) - Procesamiento de ACL

Overview

El motor 4+ introduce la funcionalidad de ACL en la cartera de productos de 10 gigabits de la serie 12000 de Cisco.

En cada uno de los trayectos de ingreso y de egreso, son soportadas hasta 1024 ACE. Las ACL de entrada y salida se procesan a velocidad de línea para hasta 96 ACE. El rendimiento para coincidencias más largas varía con el alcance de la coincidencia.

Estas tarjetas de línea POS se basan en el Motor 4+:

Tipo de tarjeta de línea	Tipo de interfaz	Conectividad
4xOC48c/STM16c	POS (Packet over SONET)	SR
4xOC48c/STM16c	POS (Packet over SONET)	LR
1xOC192c/STM64c	POS (Packet over SONET)	IR
1xOC192c/STM64c	POS (Packet over SONET)	SR
1xOC192c/STM64c	POS (Packet over SONET)	VSR-1
1xOC192/STM64c	POS (Packet over SONET)	LR
4xOC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	LR

Criterios de concordancia admitidos

Todos los criterios de ACL estándar y extendida admitidos de Cisco IOS Software Release 12.0S se soportan en la trayectoria rápida excepto para ACE de registro o fragmento.

Número de ACE admitidas

Se admiten hasta 1024 ACE por dirección en el trayecto rápido.

Nota: 1021 de las ACE son configurables. Se reservan tres entradas para los comandos ACE implícit **permit ip any any**, **deny ip any** y **send to CPU**.

No existe un límite máximo para el número de ACE admitidos. Cualquier ACE que exceda el límite 1021 se realiza en la trayectoria lenta de la tarjeta de línea.

Procesamiento de la ACL de salida

Las ACL de salida se procesan en el trayecto rápido de lado de transmisión. Consulte la Matriz de Interoperación de Tarjeta de Línea - ACL de Salida IPv4 para obtener más detalles.

Comandos específicos de la tarjeta de línea

- **show tcam appl [*acl-in* | *acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in* | *acl-out*] memory <*port*> <*number of entries*>**

Pautas operacionales e interacciones de la tarjeta en línea

- No se soportan las ACL de subinterfaz.
- El rendimiento varía según la profundidad de coincidencia.
- Las entradas de rango utilizan dos reglas ACL (tres si las dos entradas cruzan un límite).
- Se acepta una ACL por interfaz física.
- Se admiten hasta 1024 ACE (por dirección) en la ruta rápida.
- Cualquiera de las ACE de ruta rápida 1024 se puede compartir a través de los puertos.
- Las ACE que utilizan la palabra clave fragment se filtran en la ruta lenta.
- Los paquetes denegados no se cuentan para las ACE que se procesan en la trayectoria lenta.
- Si NetFlow se configura en una tarjeta de línea de Motor 0 y una ACL de salida se configura en una tarjeta de línea de motor de egreso 3 o 4+, la ACL de salida será procesada tanto por las tarjetas de línea de ingreso como de egreso para permitir que NetFlow contabilice los paquetes denegados por las ACL así como los paquetes reenviados.

Recomendaciones

Ninguno en este momento.

Motor 4 + (Ethernet) -Procesamiento de ACL

Overview

Las tarjetas de línea Ethernet de motor 4+ introducen la funcionalidad ACL de entrada por vlan en hardware en la cartera Cisco 12000 10-Gigabit Ethernet. Estas son algunas de las características:

- Las ACL de entrada y salida se pueden aplicar simultáneamente en un único puerto sin que ello afecte al rendimiento.
- Las ACL se pueden aplicar por VLAN o por puerto.

- El rendimiento de la ACL de entrada hasta 15 000 ACE no disminuye con la profundidad de coincidencia.
- Las ACL de salida se procesan a velocidad de línea para hasta 96 ACE. El rendimiento para coincidencias más largas varía con el alcance de la coincidencia.

Estas tarjetas de línea Ethernet se basan en el Motor 4+:

Tipo de tarjeta de línea	Tipo de interfaz	Tipo de motor
10xGE Rev B ("X-B")	SFP:	E4+
Modular	SFP:	E4+
1x10GE	10G	E4+
1x10GE	10G	E4+

Criterios de concordancia admitidos

Todos los criterios de ACL estándar y extendida admitidos de Cisco IOS Software Release 12.0S se soportan en la trayectoria rápida excepto para ACE de registro o fragmento.

Número de ACE admitidas

- Hasta 15 000 ACL de entrada que se pueden configurar por puerto o por VLAN.
- 1024 ACE de salida por tarjeta que se pueden aplicar por puerto.**Nota:** 1021 de las ACE son configurables. Se reservan tres entradas para los comandos ACE implícit **permit ip any any**, **deny ip any** y **send to CPU**.

Procesamiento de la ACL de salida

Las ACL de salida se procesan originariamente en la ruta rápida del lado de transmisión. Consulte la Matriz de Interoperación de Tarjeta de Línea - ACL de Salida IPv4 para obtener más información.

Comandos específicos de la tarjeta de línea

- **fusión de hw-module slot <*number*> ip acl**

Pautas operacionales e interacciones de la tarjeta en línea

- Las ACE que contienen la palabra clave fragment se procesan en la ruta lenta.
- Los contadores de ACL no son compatibles con las ACL combinadas con otras funciones.
- Los contadores de ACL no se soportan para las ACL fusionadas. Las ACL fusionadas se pueden configurar con el comando **hw-module slot <*slot number*> ip acl merge**.
- Se admiten hasta 168 operaciones L4 por tarjeta de línea. Una vez que se excede esto, la ACL se ejecuta en el trayecto lento.
- Si una tarjeta de línea de Motor 1 ha muestreado NetFlow habilitado y se habilita una ACL de salida en una tarjeta de línea de Motor de egreso 3 o 4+, la ACL de salida es procesada tanto por las tarjetas de línea de ingreso como de egreso para permitir que NetFlow contabilice los

paquetes denegados por las ACL así como los paquetes reenviados.

Recomendaciones

Ninguno en este momento.

Registro ACL

Antes de la versión 12.0(21)S del software Cisco IOS, la información de registro de ACL se enviaba al RP exclusivamente a través del bus de mantenimiento (MBUS). Durante los altos niveles de actividad de registro de ACL, fue posible exceder la capacidad del MBUS. La versión 12.0(21)S del software del IOS de Cisco introduce varias optimizaciones que evitan este escenario.

Las situaciones de sobrecarga MBUS son informadas por el software Cisco IOS con estos mensajes de error:

```
LCLOG-3-INVSTATE
```

```
MBUS_SYS-3-SEQUENCE
```

Con Cisco IOS Software Release 12.0(21)S y versiones posteriores, los mensajes de registro de gravedad alta (gravedad 0-4) se entregan al RP a través del MBUS, mientras que los mensajes de registro de gravedad inferior (gravedad 5-7) se entregan al RP a través del entramado de conmutación de mayor capacidad. Los mensajes de registro de ACL son de alta gravedad, por lo que ahora se entregan al RP a través del entramado de conmutación.

Esta funcionalidad de registro agregada se puede configurar mediante estos comandos:

- **logging method mbus [*severity*]**—Determina qué mensajes, por gravedad, se enviarán al RP usando el MBUS. Los mensajes de mayor gravedad se enviarán a través del entramado del switch.
- **show logging method**: muestra el método de registro actual para todos los niveles de gravedad del mensaje.
- **logging sequence-nums**: Este comando habilita la tarjeta de línea de envío para secuenciar los mensajes de registro de números de modo que el RP pueda reordenar los mensajes correctamente. Sin este comando, los mensajes de registro se pueden enviar al RP en orden no secuencial.

ACL de salida IPv4 - Matriz de interoperación de la tarjeta de línea

Antes de la introducción del procesamiento de ACL de salida con la versión de Motor 3 y Motor 4+, las ACL de salida fueron procesadas por la tarjeta de línea de ingreso. Las ACL de salida se han actualizado para tomar ventaja de las capacidades de procesamiento ACL de salida del motor 4+ del motor 3 de alto rendimiento.

Este gráfico proporciona un resumen de dónde se procesan las ACL de salida para diferentes combinaciones de tarjetas de línea:

	Tarjeta de línea de egreso					
Tarjeta de línea de entrada (ACL de salida aplicada a la interfaz de miembro)	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**
E0	Acceso	Acceso	Acceso	Egress	n/a	Egress
E1	Acceso	Acceso	Acceso	Egress	n/a	Egress
E2	Acceso	Acceso	Acceso	Egress	n/a	Egress
E3	Egress	Egress	Egress	Egress	n/a	Egress
E4	Egress	Egress	Egress	Egress	n/a	Egress
E4+	Egress	Egress	Egress	Egress	n/a	Egress

Soporte IPv6 ACL

Las ACL extendidas IPv6 se admiten en la ruta lenta (entrada y salida) en E0, E1, E2, E3 y E4+ en la versión 12.0(23)S del software del IOS de Cisco.

En el Motor 3, la funcionalidad de ACL IPv6 se soporta en el hardware en la versión 12.0(25)S del software del IOS de Cisco. Las ACL se aplican a una interfaz específica, con una sentencia deny implícita al final de cada lista de acceso. Las ACL IPv6 se configuran mediante el comando **ipv6 access-list** con las palabras clave deny y permit en el modo de configuración global. Las tarjetas basadas en el motor 3 admiten el filtrado de encabezados de opción IPv6 basados en tráfico, etiquetas de flujo y, opcionalmente, información de tipo de protocolo de capa superior.

Referencia de Comandos de Cisco 12000 ACL

Comandos del Motor 1

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

Comandos del motor 2

- **límite de psa del hardware de lista de acceso 128**
- **no access-list hardware psa**
- **desviación psa**
- **show access-list psa detail**
- **show access-list psa summary**

- **show controller psa feature**

Comandos del Motor 3

- **hw-module <*slot #*> tcam compile no-merge***!— desde la versión 12.0(21)S3 del software del IOS de Cisco*
- **show-access-list hardware interface <*nombre de interfaz*>**
- **show conf [*tofab|frfab*] alpha acl <*int*> vmr2ace**

Comandos Engine 4+

- **show access-list gen7 label**
- **show tcam appl [*acl-in | acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in | acl-out*] memory <*port*><*number of entries*>**

Comandos Ethernet Engine 4+

- **fusión de hw-module slot <*number*> ip acl**

Glosario

Esta sección proporciona definiciones estándar de los términos relevantes:

- **Planos de procesamiento**: un dispositivo de red se puede dividir lógicamente en tres planos de procesamiento:Plano de datos: procesamiento de los paquetes que fluyen a través del dispositivo de red.Plano de control: procesamiento de los paquetes utilizados para unir los dispositivos de red. Esto incluye protocolos de línea (por ejemplo, Point-to-Point Protocol – PPP y High-Level Data Link Control (HDLC), Routing Protocols (Border Gateway Protocol – BGP, Routing Information Protocol versión 2 – RIPv2, Open Shortest Path First – OSPF, etc.) y protocolos de temporización (como el Network Time Protocol – NTP).Plano de administración: procesamiento en paquetes que se utilizan para administrar los dispositivos de red. Esto incluye telnet, Secure Shell (SSH), protocolo de transferencia de archivos (FTP), protocolo de transferencia de archivos trivial (TFTP), SNMP y otros protocolos de gestión.
- **ACL estándar**: las ACL estándar filtran exclusivamente en la Capa 3.
- **ACL extendidas**: las listas de acceso IP extendidas utilizan direcciones de origen y destino para las operaciones coincidentes, así como información de tipo de protocolo opcional para obtener una granularidad de control más fina.
- **ACL procesadas lineales**: procesadas linealmente en el software. El rendimiento varía con el alcance de la coincidencia (la cantidad de entradas que deben verificarse antes de que se determine una coincidencia).
- **Turbo ACL (Compilado)**: las Turbo ACL optimizan el procesamiento de ACL de software mediante la compilación de una ACL en una serie de tablas de búsqueda altamente optimizadas que aceleran el procesamiento del software. El rendimiento de ACL turbo no varía con la profundidad de coincidencia.
- **ACL de entrada**: una ACL aplicada al tráfico que ingresa al puerto al que se aplica.
- **ACL de salida**: una ACL aplicada al tráfico que sale del puerto en el que se aplica. Con algunas excepciones, las ACL de salida son procesadas por la tarjeta de línea de entrada.
- **ACL de trayecto de recepción**: las ACL de trayecto de recepción proporcionan filtrado para el tráfico de control destinado al propio router, como actualizaciones de ruteo y consultas SNMP.

- **Tarjeta de línea de reenvío de dos etapas**: tarjetas de línea que tienen ASIC de reenvío/función tanto en la ruta de entrada como de salida. Esto permite que la tarjeta de línea realice funciones tanto en el flujo de paquetes de ingreso como en el flujo de paquetes de egreso sin enviar paquetes a la CPU LC. También permite el uso de nuevas oleadas de algoritmos de reenvío en dos etapas dentro del Cisco 12000. La tarjeta de línea del motor 3 es un ejemplo de una tarjeta de línea de reenvío de dos etapas.
- **Tarjeta de línea de reenvío de una sola etapa**: tarjetas de línea que tienen ASIC de reenvío/función sólo en la ruta de ingreso. Estas tarjetas de línea sólo realizan el procesamiento basado en ASIC en los paquetes que fluyen en el trayecto de ingreso. El tráfico de salida no se procesa (simplemente se reenvía), se gestiona mediante los ASIC de ingreso de otras LC o se administra mediante la CPU LC. El Motor 2, el Motor 4 y el Motor 4+ son ejemplos de tarjetas de línea de reenvío de una sola etapa.

Información Relacionada

- Cisco 12000 Series Internet Routers
- Soporte Técnico y Documentación - Cisco Systems