Directiva predeterminada del avión del control en el ejemplo de configuración del Catalyst 6500/Sup2T y del Catalyst 6880

Contenido

Introducción

Este documento describe detalladamente corresponden con a qué tipos de tráfico contra class-maps predeterminado, que son parte del Catalyst 6500 predeterminado Sup2T/la configuración de CoPP del Catalyst 6880 (Políticas del plano de control) que se configura automáticamente en el dispositivo. Esto se configura para proteger su CPU contra ser sobrecargado.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

CoPP se habilita por abandono en el Catalyst 6500/SUP2T y los Catalyst 6880 Switch y se basa en una plantilla preconfigurada. Algunos configuración class-map no tienen declaraciones de coincidencia correspondientes debido al hecho de que capturan el tráfico no en la lista de control de acceso (ACL) MAC/IP, pero bastante en las excepciones internas que son señaladas por el motor de reenvío cuando el tráfico es recibido por el Switch y una decisión de reenvío tomados.

Si un clase-mapa específico necesita ser agregado/ser modificado/ser quitado de la directiva actual de CoPP, después debe ser hecho del modo de configuración en el modo del directiva-mapa. Vea la guía de configuración de software de la versión 15.0SY del Catalyst 6500 - Políticas del plano de control (CoPP) para la sintaxis exacta.

Las clases de excepción del valor por defecto de CoPP tienen estas descripciones:

Caso	nombre del clase-mapa	Descripción
Error de la Unidad máxima de transmisión (MTU) (MTU)	clase-copp-MTU-fracaso	El tamaño de paquetes excede la talla del MTU de la interfaz saliente. Si el bit del Don't Fragment no se fija, se requiere la fragmentación. Si se fija el bit del Don't Fragment, el mensaje de destino inalcanzable del Internet Control Message Protocol (ICMP) indica que la “fragmentación necesitó y el DF fijar” esté supuesto para ser generado y para ser devuelto a la fuente. Referencia: RFC-791, RFC-1191
Error del Time to Live (TTL)	clase-copp-TTL-fracaso	Paquete TTL=1 (para el IPv4), límite del salto = 0 o 1 (para el IPv6) TTL = 0 (para el IPv4) se puede desechar en el hardware inmediatamente mientras que el salto anterior se supone destruir el paquete cuando TTL decremented a 0. El límite del salto = 0 (para el IPv6) es diferente de TTL = 0 porque se expone en el RFC-2460, la sección 8.2 que “a diferencia del IPv4, los Nodos del IPv6 no se requieren aplicar el curso de la vida del PAQUETE MÁXIMO. Ésa es la razón que el campo del Time to Live del IPv4 fue retitulado límite del salto en el IPv6". Esto significa que el paquete entrante del IPv6 con el límite del salto = 0 es todavía válido, y el mensaje ICMP se debe devolver. Referencia: RFC-791, RFC-2460
Opciones	clase-copp-opciones	Paquete con las opciones (para el IPv4), encabezado de extensión del salto por el salto (para el IPv6). Por ejemplo, RFC-2113 de la alerta del router, Source ruta estricta, y así sucesivamente.

		Los encabezados de extensión no son examinados ni son procesados por cualquier nodo a lo largo de la trayectoria de la salida de un paquete, hasta que el paquete alcance el nodo (o cada uno del conjunto de los Nodos en el ofmulticast del caso) identificado en el campo dirección de destino de la encabezado theIPv6. La única excepción es la encabezado de las opciones del salto por el salto, que lleva la información que se debe examinar y procesar por cada nodo a lo largo de la trayectoria de la salida de un paquete, que incluye los nodos de origen y de destino. El hardware que procesa en los campos de opción no se soporta, eso es proceso/transferencia del software es necesario. Referencia: RFC-791/RFC-2460
Error del reenvío de trayecto inverso (RPF) (unicast)	clase-copp-ucast-RPF-fracaso	El paquete que falla revisión de "RPF" se filtra. Sin embargo, debido a los recursos limitados en el hardware, revisión de "RPF" no puede ser hecho en hardware en ciertos casos (es decir, más de 16 interfaces RPF conectadas a un IP). Cuando sucede eso, el paquete se envía al software para un completo revisión de "RPF".
Falla de RPF (Multicast)	clase-copp-mcast-RPF-fracaso	El primer paquete de datos fallado RPF (dirigido a un grupo de multidifusión) se envía al software para que la multidifusión independiente de protocolo (PIM) - afirma el proceso para comenzar. Una vez que se hace el proceso, eligen a un router designado/a un promotor. Si el próximo paquete (el mismo flujo) no viene del router designado, acciona a una falla de RPF, y el hardware puede caerlo inmediatamente (para prevenir un ataque de Negación de servicio (DoS)). El primer paquete de datos fallado RPF (dirigido a un grupo de multidifusión) se envía al software para que el proceso de la PIM-afirmación comience. Una vez que se hace el proceso, eligen a un router designado/a un promotor. Si el próximo paquete (el mismo flujo) no viene del router designado, acciona a una falla de RPF, y el hardware puede caerlo inmediatamente (para prevenir un ataque DOS). Sin embargo, si la tabla de ruteo es

		actualizada, un nuevo router designado pudo necesitar ser elegido (vía PIM-afirme), que significa que el paquete fallado RPF necesita alcanzar el software (para que PIM-afirme comience otra vez). Para hacer eso, un escape periódico al mecanismo del software (por el flujo) para el paquete RPF-fallado está disponible en el hardware. Observe sin embargo, si hay una enorme cantidad de flujos entonces que un escape periódico puede ser demasiado para que el software dirija. El hardware CoPP todavía se requiere para el paquete fallado RPF del Multicast. Referencia: RFC-3704, RFC-2362
Reescritura de paquetes del hardware no soportada	clase-copp-unsupp-reescritura	Mientras que el hardware puede reescribir los paquetes en los diversos casos, algunos casos apenas no se pueden hacer en el diseño de hardware actual. Y para ésos, el hardware envía el paquete al software.
Ninguno-ruta ICMP ACL-descenso ICMP Redirección ICMP	clase-copp-ICMP-reorientar-inalcanzable	Los paquetes enviaron al software para la generación de mensajes ICMP. Por ejemplo la redirección ICMP, destino ICMP inalcanzable (por ejemplo. imposible acceder al host o administrativo prohibido). Referencia: RFC-792/RFC-2463
El Cisco Express Forwarding (CEF) recibe (el IP de destino es el IP del router)	clase-copp-reciba	Si el IP de destino del paquete es uno de los IP Addresses del router (golpeará el CEF reciben la adyacencia), después el software se supone para procesar el contenido.
El CEF espiga (el IP de destino pertenece a uno de la red del router)	clase-copp-espigue	Si el IP de destino del paquete pertenece a uno de la red del router, pero no se resuelve (es decir, ningún golpe en la tabla de la Base de información de reenvío (FIB)), golpeará la adyacencia de recolección CEF, siendo enviado al software adonde el procedimiento de resolución conseguirá comenzado. Para el IPv4, el mismo flujo continúa golpeando el CEF espiga hasta que se resuelva el direccionamiento. Para el IPv6, una entrada temporal de la BOLA que hace juego el IP de destino (y las puntas para caer la adyacencia en lugar de otro) consigue instaladas durante la resolución. Si no puede ser resuelto en la duración especificada, se quita la entrada de la BOLA (es decir, el mismo comienzo del

		flujo para golpear el CEF espiga otra vez).
Paquete destinado al IP de multidifusión 224.0.0.0/4	clase-copp-mcast-IP-control	El paquete de control necesita ser procesado por el software.
Paquete destinado al IP de multidifusión FF::/8	class-copp-mcast-ipv6-control	El paquete de control necesita ser procesado por el software.
Paquete de multidifusión que necesita ser copiado al software	clase-copp-mcast-copia	En algunos casos, el paquete de multidifusión necesita ser copiado al software para una actualización del estado (el paquete sigue siendo hardware interligado en el mismo VLA N). Por ejemplo, (*, G/m) golpeado para la entrada del modo denso, intercambio dual-RPF SPT.
Paquete de multidifusión que consigue una falta en la tabla de FIB	clase-copp-mcast-batea	El IP de destino (IP de multidifusión) es una falta en la tabla de FIB. El paquete se lleva en batea al software.
Fuente directamente conectada (IPv4)	clase-copp-IP-conectado	El tráfico Multicast de las fuentes directamente conectadas se envía al software donde un estado del Multicast puede ser creado (y instalado en el hardware).
Fuente directamente conectada (IPv6)	class-copp-ipv6-connected	El tráfico Multicast de las fuentes directamente conectadas se envía al software donde un estado del Multicast puede ser creado (y instalado en el hardware).
Paquete de difusión	clase-copp-transmitido	Los paquetes de broadcast (por ejemplo, IP/Non-IP con el broadcast DMAC y la unidifusión IP con el Multicast DMAC) se escapan al software.
Protocolo desconocido a (es decir, sin apoyo por) en términos de Hardware Switching	clase-copp-desconocido-protocolo	El protocolo del no IP, tal como Intercambio de paquetes entre redes (IPX) y así sucesivamente, no será hardware conmutado. Se envían al software y consiguen remitidos allí.
Tráfico de datos de multidifusión que viene adentro vía el puerto ruteado en donde se inhabilita el	class-copp-mcast-v4-data-on-routedPort	El tráfico de datos de multidifusión que viene adentro a través de un puerto ruteado (donde se inhabilita el PIM) se escapa al software. Sin embargo, no es necesario enviarlos al software así que se caen.

PIM Tráfico de datos de multidifusión que viene adentro vía el puerto ruteado en donde se inhabilita el PIM	class-copp-mcast-v6-data-on-routedPort	El tráfico de datos de multidifusión que viene adentro a través de un puerto ruteado (donde se inhabilita el PIM) se escapa al software. Sin embargo, no es necesario enviarlos al software así que se caen.
El ingreso ACL reorienta para interligar el paquete	clase-copp-ucast-ingreso-ACL-interligado	El hardware tiene 8 excepciones ACL-relacionadas fijadas por el software vía un ACL para reorientar. Éste se relaciona con los paquetes de unidifusión interligados el CPU por el ACL para el Ternary Content Addressable Memory (TCAM) relacionó las razones.
La salida ACL reorienta para interligar el paquete	clase-copp-ucast-salida-ACL-interligado	El hardware tiene 8 excepciones ACL-relacionadas fijadas por el software vía un ACL para reorientar. Éste se relaciona con los paquetes de unidifusión interligados el CPU por el ACL para el Ternary Content Addressable Memory (TCAM) relacionó las razones.
El mcast ACL reorienta a los Bridge Packet al CPU	clase-copp-mcast-ACL-interligado	El hardware tiene 8 excepciones ACL-relacionadas fijadas por el software vía un ACL para reorientar. Éste se relaciona con el proceso del Multicast.
Bridge ACL al CPU para el proceso del Server Load Balancing	clase-copp-SLB	El hardware tiene 8 excepciones ACL-relacionadas fijadas por el software vía un ACL para reorientar. Éste se relaciona con un hardware reorienta para una decisión del Equilibrio de carga de servidores (SLB).
El registro ACL VACL reorienta	clase-copp-VACL-registro	El hardware tiene 8 excepciones ACL-relacionadas fijadas por el software vía un ACL para reorientar. ¿Éste se relaciona con la redirección de paquete por el VLAN Access Control List (VACL) ACL con el CPU para el Cisco IOS? propósitos de registración.
Snooping del DHCP	clase-copp-DHCP-snooping	El DHCP snooped los paquetes se reorienta al CPU para el procesamiento DHCP
La directiva MAC basó la expedición	clase-copp-mac-pbf	La expedición basada directiva debe ser hecha en el CPU puesto que el hardware no es capaz remitir los paquetes en este caso.
control de admisión de red de la IP-admisión	clase-copp-IP-admisión	Para proporcionar el acceso a la red basado en las credenciales del antivirus del host, hay validación de la postura vía una de las estas opciones: (1) la interfaz L2 utilizará IP del puerto LAN (LPIP),

Inspección ARP dinámica	clase-copp-ARP-snooping	donde los paquetes del Address Resolution Protocol (ARP) se reorientan que al CPU, (2) la interfaz L3 utiliza el IP de gateway (GWIP). Después de la validación, hay la autenticación (*). Para una interfaz L2 es WebAuth, que realiza la interceptación del paquete HTTP y pudo también realizar el cambio de dirección URL (*). Para la interfaz L3, es AuthProxy. Para prevenir el ataque (hombre-en--medio) del envenenamiento ARP, inspección ARP dinámica (también conocida como inspección ARP dinámica (DAI)) valida los pedidos ARP/las respuestas por cuando las intercepta y después procesa en el CPU contra uno de éstos: (1) usuario configurado ARP ACL (para los host estáticamente configurados), (2) dirección MAC a los atascamientos de la dirección IP salvados en la base de datos de confianza (es decir, atascamientos del DHCP). Solamente los paquetes ARP válidos se utilizan para poner al día memoria caché ARP local o se remiten hacia fuera. El proceso de validación requiere la implicación de los paquetes ARP CPU, que significa que el hardware CoPP es necesario para prevenir un ataque DOS.
El ACL reorienta al CPU para el WCCP	clase-copp-wccp	Utilizado en caso de que el paquete/el flujo necesite ser reorientado al CPU para la decisión de reenvío del protocolo web cache communication (WCCP).
El ACL reorienta al CPU para la arquitectura de la inserción del servicio (el SIA)	clase-copp-servicio-inserción	Utilizado en caso de que el paquete/el flujo necesite ser reorientado al CPU para la decisión SIA.
Detección de red del IPv6	clase-copp-nd	Para reorientar el paquete de la detección de red del IPv6 al CPU para procesar más lejos. Referencia: RFC4861

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para marcar si había tráfico observado en CoPP configurado un de los class-maps, ingrese el comando de la **controle de plano del directiva-mapa de la demostración**.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco Catalyst 6500 Series Switch de protección usando las Políticas del plano de control, la tarifa del hardware que limita, y las listas de control de acceso
- Guía de configuración de software de la versión 15.0SY del Catalyst 6500 - Políticas del plano de control (CoPP)
- Soporte Técnico y Documentación - Cisco Systems