Ejemplo de Configuración de Política de Plano de Control Predeterminado en Catalyst 6500/Sup2T y Catalyst 6880

Contenido

Introducción

Este documento describe detalladamente qué tipos de tráfico coinciden con los class-maps predeterminados, que forman parte de la configuración predeterminada de Catalyst 6500 Sup2T / Catalyst 6880 CoPP (Control Plane Policing) configurada automáticamente en el dispositivo. Esto se configura para proteger su CPU de ser sobrecargada.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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.

Configurar

CoPP se habilita de forma predeterminada en los switches Catalyst 6500 / SUP2T y Catalyst 6880 y se basa en una plantilla preconfigurada. Algunas configuraciones de mapa de clase no tienen las sentencias de coincidencia correspondientes debido al hecho de que capturan el tráfico no en la lista de control de acceso (ACL) MAC/IP, sino en las excepciones internas que el motor de reenvío señala cuando el switch recibe el tráfico y se toma una decisión de reenvío.

Si se necesita agregar/modificar/eliminar un mapa de clase específico de la política CoPP actual, se debe hacer desde el modo de configuración en el modo de mapa de políticas. Consulte Guía de Configuración del Software Catalyst 6500 Release 15.0SY - Control Plane Policing (CoPP) para obtener la sintaxis exacta.

Las clases de excepción predeterminadas de CoPP tienen estas descripciones:

Caso	nombre de mapa de clase	Descripción
Falla de la unidad máxima de transmisión (MTU)	class-copp-mtu-fail	El tamaño del paquete excede el tamaño de la MTU de la interfaz saliente. Si el bit Don't Fragment no está configurado, se requiere fragmentación. Si el bit Don't Fragment está configurado, el mensaje Internet Control Message Protocol (ICMP) Destination Unreachable (Protocolo de mensajes de control de Internet [ICMP] Destination Unreachable [Destino inalcanzable] indica que se supone que se debe generar la "fragmentación necesaria y DF configurada" y enviarla de vuelta al origen. Referencia: RFC-791 y RFC-1191
Error de tiempo de vida (TTL)	class-copp-ttl-fail	Paquete TTL = 1 (para IPv4), Límite de saltos = 0 o 1 (para IPv6) TTL = 0 (para IPv4) se puede descartar en el hardware inmediatamente, ya que se supone que el salto anterior destruirá el paquete cuando TTL se reduzca a 0. Límite de saltos = 0 (para IPv6) es diferente de TTL = 0 porque se establece en RFC-2460, sección 8.2 que "A diferencia de IPv4, los nodos IPv6 no son necesarios para aplicar la duración máxima del paquete. Esta es la razón por la que el campo Tiempo de vida de IPv4 se cambió al nombre de Límite de saltos en IPv6". Esto significa que el paquete IPv6 entrante con límite de saltos = 0 sigue siendo válido y el mensaje ICMP debe ser enviado de vuelta. Referencia: RFC-791 y RFC-2460

Opciones	class-copp-options	Paquete con opciones (para IPv4), encabezado de extensión salto a salto (para IPv6). Por ejemplo, Router Alert RFC-2113, Strict Source Route, etc. Los encabezados de extensión no son examinados ni procesados por ningún nodo a lo largo de la trayectoria de entrega de un paquete, hasta que el paquete llegue al nodo (o a cada conjunto de nodos en el caso de multicast) identificado en el campo Destination Address del encabezado IPv6. La única excepción es el encabezado Opciones de Salto a Salto, que transporta información que debe ser examinada y procesada por cada nodo a lo largo de la trayectoria de entrega de un paquete, que incluye los nodos de origen y de destino. No se admite el procesamiento de hardware en los campos de opción, es decir, se necesita procesamiento/switching de software. Referencia: RFC-791/RFC-2460
Falla de Reenvío de Trayectoria Inversa (Unicast)	class-copp-ucast-rpf-fail	El paquete que falla la verificación RPF se filtra. Sin embargo, debido a los recursos limitados en el hardware, la verificación de RPF no puede realizarse en el hardware en ciertos casos (es decir, más de 16 interfaces RPF vinculadas a una IP). Cuando esto sucede, el paquete se envía al software para una verificación RPF completa.
Falla de RPF (Multicast)	class-copp-mcast-rpf-fail	El primer paquete de datos con error de RPF (dirigido a un grupo de multidifusión) se envía al software para que se inicie el proceso de afirmación de multidifusión independiente de protocolo (PIM). Una vez que se ha realizado el proceso, se elige un router/reenviador designado. Si el siguiente paquete (mismo flujo) no proviene del router designado, provoca una falla de RPF y el hardware puede descartarlo inmediatamente (para evitar un ataque de denegación de servicio (DoS)). El primer paquete de datos con error de RPF (dirigido a un grupo de multidifusión) se envía al software para que se inicie el proceso PIM-assert. Una

		vez que se ha realizado el proceso, se elige un router/reenviador designado. Si el siguiente paquete (el mismo flujo) no proviene del router designado, provoca una falla de RPF y el hardware puede descartarlo inmediatamente (para evitar un ataque de DoS). Sin embargo, si se actualiza la tabla de ruteo, es posible que deba elegirse un nuevo router designado (a través de PIM-assert), lo que significa que el paquete RPF fallido necesita alcanzar el software (para que PIM-assert se inicie de nuevo). Para ello, hay disponible una fuga periódica al mecanismo de software (por flujo) para el paquete con fallas de RPF en el hardware. Tenga en cuenta que, si hay una gran cantidad de flujos, una fuga periódica puede ser demasiado para que el software la gestione. El CoPP de hardware sigue siendo necesario para el paquete con error de RPF de multidifusión. Referencia: RFC-3704, RFC-2362
No se admite la reescritura de paquetes de hardware	class-copp-unsupp-rewrite	Aunque el hardware puede reescribir paquetes en varios casos, algunos casos simplemente no se pueden hacer en el diseño de hardware actual. Y para ellos, el hardware envía el paquete al software.
ICMP no-route ICMP acl-drop redireccionamiento ICMP	class-copp-icmp-redirect-unreachable	Paquetes enviados al software para la generación de mensajes ICMP. Por ejemplo, redirección ICMP, destino ICMP inalcanzable (por ejemplo, host inalcanzable o administrativamente prohibido). Referencia: RFC-792/RFC-2463
Cisco Express Forwarding (CEF) receive (la IP de destino es la IP del router)	class-copp-receive	Si la IP de destino del paquete es una de las direcciones IP del router (llegará a CEF receive adjacency), se supone que el software debe procesar el contenido.
Glean CEF (la IP de destino pertenece a una de las redes del router)	class-copp-glean	Si la IP de destino del paquete pertenece a una de las redes del router, pero no se resuelve (es decir, no se produce ningún impacto en la tabla de la Base de información de reenvío (FIB)), se producirá un impacto en la adyacencia de gateway CEF, que se enviará al software donde se iniciará el procedimiento de resolución. Para IPv4, el mismo flujo continúa llegando a la luz CEF hasta que se

		resuelve la dirección. Para IPv6, se instala durante la resolución una entrada FIB temporal que coincida con la IP de destino (y que, en su lugar, indique que se descarta adyacencia). Si no se puede resolver en la duración especificada, se quita la entrada FIB (es decir, el mismo flujo comienza a alcanzar nuevamente la luz CEF).
Paquete destinado a IP 224.0.0.0/4	class-copp-mcast-ip-control	El paquete de control debe ser procesado por el software.
Paquete destinado a IP FF de multidifusión::/8	class-copp-mcast-ipv6-control	El paquete de control debe ser procesado por el software.
Paquete de multidifusión que necesita copiarse en el software	class-copp-mcast-copy	En algunos casos, el paquete de multidifusión debe copiarse en el software para una actualización de estado (el paquete sigue siendo hardware puenteado en la misma VLAN). Por ejemplo, (*,G/m) pulsado para entrada en modo denso, switchover SPT de rpf dual.
Paquete de multidifusión que se pierde en la tabla FIB	class-copp-mcast-punt	La IP de destino (IP de multidifusión) es un error en la tabla FIB. El paquete se envía al software.
Fuente conectada directamente (IPv4)	class-copp-ip-connected	El tráfico de multidifusión de fuentes conectadas directamente se envía al software donde se puede crear un estado de multidifusión (e instalar en el hardware).
Fuente conectada directamente (IPv6)	class-copp-ipv6-connected	El tráfico de multidifusión de fuentes conectadas directamente se envía al software donde se puede crear un estado de multidifusión (e instalar en el hardware).
Paquete de difusión	class-copp-broadcast	Los paquetes de difusión (por ejemplo, IP/No IP con DMAC de difusión y unidifusión IP con DMAC de multidifusión) se filtran al software.
Protocolo desconocido para (es decir, no admitido por) en términos de switching de hardware	class-copp-unknown-protocol	El protocolo que no sea IP, como Intercambio de paquetes entre redes (IPX), etc., no se conmutará por hardware. Se envían al software y se reenvían allí.
Tráfico de datos de multidifusión entrante a través de puerto ruteado donde se inhabilita PIM	class-copp-mcast-v4-data-on-routedPort	El tráfico de datos de multidifusión que llega a través de un puerto ruteado (donde se inhabilita PIM) se filtra al software. Sin embargo, no es necesario enviarlos al software para que se descarten.

Tráfico de datos de multidifusión entrante a través de puerto ruteado donde se inhabilita PIM	class-copp-mcast-v6-data-on-routedPort	El tráfico de datos de multidifusión que llega a través de un puerto ruteado (donde se inhabilita PIM) se filtra al software. Sin embargo, no es necesario enviarlos al software para que se descarten.
Redirección ACL de ingreso para puentear el paquete	class-copp-ucast-ingress-acl-bridged	El hardware tiene 8 excepciones relacionadas con ACL establecidas por el software a través de una redirección ACL. Esta se relaciona con los paquetes de unidifusión puenteados a la CPU por la ACL por razones relacionadas con la Memoria direccionable de contenido ternario (TCAM).
Redirección ACL de salida para puentear el paquete	class-copp-ucast-egress-acl-bridged	El hardware tiene 8 excepciones relacionadas con ACL establecidas por el software a través de una redirección ACL. Esta se relaciona con los paquetes de unidifusión puenteados a la CPU por la ACL por razones relacionadas con la Memoria direccionable de contenido ternario (TCAM).
Redireccionamiento de ACL de difusión a paquetes de puente a la CPU	class-copp-mcast-acl-bridged	El hardware tiene 8 excepciones relacionadas con ACL establecidas por el software a través de una redirección ACL. Esta se relaciona con el procesamiento multidifusión.
Puente ACL a CPU para el procesamiento de Balanceo de Carga del Servidor	class-copp-slb	El hardware tiene 8 excepciones relacionadas con ACL establecidas por el software a través de una redirección ACL. Esta se relaciona con una redirección de hardware para una decisión de equilibrio de carga de servidor (SLB).
Redirección de registro ACL VACL	class-copp-vacl-log	El hardware tiene 8 excepciones relacionadas con ACL establecidas por el software a través de una redirección ACL. ¿Esta se relaciona con la redirección de paquetes mediante ACL de lista de control de acceso (VACL) de VLAN a la CPU para Cisco IOS? propósitos de registro.
snooping de DHCP	class-copp-dhcp-snooping	Los paquetes DHCP snooped se redirigen a la CPU para el procesamiento DHCP
Reenvío basado en política MAC	class-copp-mac-pbf	El reenvío basado en políticas se debe realizar en la CPU ya que el hardware no es capaz de reenviar paquetes en este caso.
Control de admisión de red IP	class-copp-ip-input	Para proporcionar acceso a la red basado en las credenciales antivirus del host, hay validación de estado a través de una de estas opciones: (1) La

		interfaz L2 utilizará IP de puerto LAN (LPIP), donde los paquetes de protocolo de resolución de direcciones (ARP) se redirigen a la CPU; (2) La interfaz L3 utiliza IP de gateway (GWIP). Después de la validación, existe la autenticación (*). Para una interfaz L2 es WebAuth, que realiza la intercepción de paquetes HTTP y también puede realizar la redirección URL (*). Para la interfaz L3, es AuthProxy.
Dynamic ARP Inspection	class-copp-arp-snooping	Para evitar el ataque de envenenamiento ARP (man-in-the-middle), la inspección ARP dinámica (también conocida como Dynamic ARP Inspection (DAI)) valida las solicitudes/respuestas ARP cuando las intercepta y luego las procesa en la CPU contra una de las siguientes: (1) ACL ARP configuradas por el usuario (para hosts configurados estáticamente), (2) vinculaciones de direcciones MAC a direcciones IP almacenadas en bases de datos de confianza (es decir, vinculaciones DHCP). Sólo se utilizan paquetes ARP válidos para actualizar la memoria caché ARP local o reenviarlos. El proceso de validación requiere la participación de la CPU de los paquetes ARP, lo que significa que se necesita CoPP de hardware para evitar un ataque de DoS.
Redirección de ACL a la CPU para WCCP	class-copp-wccp	Se utiliza en caso de que el paquete/flujo deba redirigirse a la CPU para la decisión de reenvío del protocolo de comunicación de caché web (WCCP).
Redirección de ACL a la CPU para la arquitectura de inserción de servicios (SIA)	class-copp-service-insert	Se utiliza en caso de que el paquete/flujo deba ser redirigido a la CPU para la decisión de SIA.
Detección de red IPv6	class-copp-nd	Para redirigir el paquete de Detección de Red IPv6 a la CPU para que continúe el proceso. Referencia: RFC4861

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar si se observó tráfico en cualquiera de los class-maps CoPP configurados, ingrese el **comando show policy-map control-plane**.

Troubleshoot

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

Información Relacionada

- Protección de los switches Catalyst de Cisco serie 6500 mediante políticas del plano de control, limitación de la velocidad de hardware y listas de control de acceso
- Guía de Configuración del Software Catalyst 6500 Release 15.0SY - Control Plane Policing (CoPP)
- Soporte Técnico y Documentación - Cisco Systems