Utilice la guía de refuerzo de Cisco IOS XE

Contenido

Introducción

Este documento describe información para proteger sus dispositivos del sistema Cisco IOS® XE, lo que aumenta la seguridad general de su documentación de red.

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.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estructurado en torno a los tres planos en los que se pueden categorizar las funciones de un dispositivo de red, este documento proporciona una descripción general de cada función incluida y referencias a elementos relacionados.

Los tres planos funcionales de una red, el plano de gestión, el plano de control y el plano de datos, proporcionan una funcionalidad diferente que debe protegerse.

1. Plano de administración: el plano de administración administra el tráfico que se envía al dispositivo Cisco IOS XE y está formado por aplicaciones y protocolos como Secure Shell (SSH) y el protocolo simple de administración de red (SNMP).
2. Plano de control: El plano de control de un dispositivo de red procesa el tráfico que es crucial para mantener en funcionamiento la infraestructura de la red. El plano de control consiste en aplicaciones y protocolos entre dispositivos de red, que incluyen el protocolo Border Gateway Protocol (BGP) y los protocolos Interior Gateway Protocols (IGP), como Enhanced Interior Gateway Routing Protocol (EIGRP) y Open Shortest Path First (OSPF).
3. Plano de datos: Reenvía datos mediante un dispositivo de red. El plano de datos no incluye el tráfico enviado al dispositivo Cisco IOS XE local.

   En este documento las funciones de seguridad se describen en profundidad para que usted pueda configurarlas. Sin embargo, cuando la descripción no es exhaustiva, la función se explica de una manera que le permita evaluar si necesita prestarle más atención a la función. Siempre que sea posible y adecuado, este documento contiene recomendaciones que, de ser implementadas, ayudan a asegurar una red.

Operaciones de Seguridad

Las operaciones de seguridad de la red constituyen un tema primordial. Aunque la mayor parte de este documento se dedica a la configuración segura de un dispositivo Cisco IOS XE, las configuraciones por sí solas no aseguran completamente una red. Los procedimientos operativos que se utilizan en la red contribuyen tanto a la seguridad como a la configuración de los dispositivos subyacentes.

Estos temas contienen las recomendaciones operativas que se le aconseja implementar. Estos temas resaltan áreas fundamentales específicas de las operaciones de la red y no son exhaustivos.

Monitoreo de Boletines y Respuestas de Seguridad de Cisco

El Equipo de Respuesta a Incidentes de Seguridad en Productos Cisco (PSIRT) crea y mantiene publicaciones, comúnmente conocidas como boletines de PSIRT, para los problemas relacionados con la seguridad en productos Cisco. El método usado para la comunicación de problemas de menor gravedad es Respuesta de Seguridad de Cisco. Las respuestas y los consejos de seguridad están disponibles en Respuestas y consejos de seguridad de Cisco

Puede encontrar información adicional sobre estos vehículos de comunicación en la política de vulnerabilidades de seguridad de Cisco

Para mantener una red segura, debe estar al tanto de los boletines y las respuestas de seguridad de Cisco que se han publicado. Debe tener conocimiento de una vulnerabilidad para que se pueda evaluar la amenaza que representa para una red. Consulte Clasificación de Riesgos para Anuncios de Vulnerabilidad de Seguridad para obtener ayuda en este proceso de evaluación.

Aprovechamiento de Autenticación, Autorización y Contabilización

El marco de trabajo de autenticación, autorización y auditoría (AAA) es vital para proteger los dispositivos de redes. El protocolo AAA proporciona autenticación de las sesiones de administración y puede también limitar a los usuarios a comandos específicos definidos por el administrador y registrar todos los comandos ingresados por cada usuario. En la sección Autenticación, autorización y auditoría de este documento, hallará más información sobre cómo aprovechar el AAA.

Centralización de Monitoreo y Colección de Registros

Para obtener información sobre los eventos actuales, emergentes e históricos relacionados con los incidentes de seguridad, su organización debe tener una estrategia unificada para el registro y la correlación de eventos. Esta estrategia debe aprovechar el registro de todos los dispositivos de red y utilizar capacidades de correlación personalizables y previamente diseñadas.

Después de que se implemente el registro centralizado, usted debe desarrollar un método estructurado para registrar el seguimiento de incidentes y análisis. De acuerdo con las necesidades de su organización, este método puede ser una simple revisión minuciosa de datos de registro e, incluso, un análisis avanzado basado en reglas.

Vea la sección Prácticas Recomendadas de Registro de este documento para obtener más información sobre cómo implementar el registro en los dispositivos de red Cisco IOS XE.

Uso de Protocolos de Seguridad Siempre Que Sea Posible

Muchos protocolos se utilizan para transportar datos de administración de red confidenciales Debe utilizar protocolos de seguridad siempre que sea posible. Una elección de protocolo de seguridad incluye el uso del SSH en vez de Telnet para cifrar los datos de autenticación y la información de administración. Además, debe utilizar protocolos de transferencia de archivos seguros al copiar datos de configuración. Un ejemplo es el uso del protocolo Secure Copy Protocol (SCP) en lugar de FTP o de TFTP.

Consulte la sección Sesiones de administración interactiva segura de este documento para obtener más información sobre la administración segura de los dispositivos Cisco IOS XE.

Netflow para Visibilidad del Tráfico

La herramienta Netflow le permite monitorear los flujos de tráfico en la red. Si bien en un principio su objetivo fue exportar la información del tráfico a las aplicaciones de administración de red, la herramienta Netflow también puede ser utilizada para mostrar la información de flujo en un router. Gracias a esta capacidad, usted puede ver el momento en que el tráfico cruza la red en tiempo real. Independientemente de si la información de flujo se exporta a un recolector remoto, se recomienda que configure los dispositivos de red para que admitan Netflow a fin de poder utilizar la herramienta como respuesta si es necesario.

Puede encontrar más información sobre esta función en la sección Identificación y Seguimiento del Tráfico de este documento y en Cisco IOS NetFlow (sólo usuarios registrados).

Administración de la Configuración

La administración de la configuración es un proceso mediante el cual se proponen, revisan, aprueban e implementan cambios de configuración. En el contexto de la configuración de un dispositivo Cisco IOS XE, dos aspectos adicionales de la administración de la configuración son fundamentales: el archivado de la configuración y la seguridad.

Usted puede utilizar archivos de configuración para restaurar los cambios que se realizan a los dispositivos de red. En un contexto de seguridad, los archivos de configuración también se pueden utilizar para determinar qué cambios se realizaron en la seguridad y cuándo ocurrieron estos cambios. Junto con los datos de registro del protocolo AAA, esta información puede contribuir con la auditoría de seguridad de los dispositivos de red.

La configuración de un dispositivo Cisco IOS XE contiene muchos detalles confidenciales. Los nombres de usuario, las contraseñas y el contenido de las listas de control de acceso son ejemplos de este tipo de información. El repositorio que utiliza para archivar las configuraciones de dispositivos de Cisco IOS XE debe estar protegido. El acceso inseguro a esta información puede disminuir la seguridad de toda la red.

Plano de Administración

El plano de administración consiste en funciones que permiten alcanzar las metas de administración de la red.

Esto incluye las sesiones de administración interactiva que emplean SSH y también recopilación de estadísticas con SNMP o NetFlow. Cuando usted considera la seguridad de un dispositivo de red, es crucial que el plano de administración esté protegido. Si un incidente de seguridad tiene la capacidad de disminuir las funciones del plano de administración, puede resultarle imposible recuperar o estabilizar la red.

En estas secciones se detallan las configuraciones y las funciones de seguridad disponibles en el software Cisco IOS XE, lo que ayuda a reforzar el plano de gestión.

Consolidación del Plano de Administración General

El plano de administración se utiliza para acceder, configurar y manejar un dispositivo, así como para monitorear sus operaciones y la red en las cual se ha implementado. El plano de administración es el que recibe y envía el tráfico para las operaciones de estas funciones. Usted debe proteger tanto el plano de administración como el de control de los dispositivos, porque las operaciones del plano de control afectan directamente las del plano de administración. El plano de administración utiliza esta lista de protocolos:

1. Simple Network Management Protocol
2. TELNET
3. Secure Shell Protocol
4. File Transfer Protocol
5. Protocolo de transferencia de hipertexto / Protocolo seguro de transferencia de hipertexto
6. Trivial File Transfer Protocol
7. Secure Copy Protocol
8. TACACS+
9. RADIUS
10. Netflow
11. Network Time Protocol
12. Syslog

    Se deben tomar medidas para garantizar la supervivencia de los planos de administración y de control durante incidentes de seguridad. Si uno de estos planos es vulnerado con éxito, todos los planos pueden verse en peligro.

Administración de Contraseña

Las contraseñas controlan el acceso a recursos o a dispositivos. Esto se logra mediante la definición de una contraseña o secreto que se utiliza para autenticar las solicitudes. Cuando se recibe una solicitud para el acceso a un recurso o a un dispositivo, la solicitud exige la verificación de la contraseña y de la identidad, y el acceso se puede conceder, negar o limitar según el resultado de la verificación. Como práctica recomendada de seguridad, las contraseñas se deben administrar con un servidor de autenticación TACACS+ o RADIUS. Sin embargo, tenga en cuenta que, si fallan los servicios TACACS+ o RADIUS, aún se necesita una contraseña de acceso privilegiado configurada localmente. Un dispositivo puede también tener otra información de contraseña presente dentro de su configuración, como un clave NTP, una comunidad SNMP o una clave de Protocolo de Ruteo.

El comando enable secret se utiliza para establecer la contraseña que otorga acceso administrativo privilegiado al sistema Cisco IOS XE. El comando enable secret debe ser utilizado en lugar del comando enable password anterior. El comando enable password utiliza un algoritmo de cifrado vulnerable.

Si no se configura ningún comando enable secret y se configura una contraseña para la línea tty de la consola, la contraseña de la consola se puede utilizar para recibir el acceso privilegiado, incluso de una sesión tty (vty) virtual remota. Esta acción es casi seguro indeseada y es otro motivo por el cual se debe asegurar la configuración de un comando enable secret.

El comando de configuración global service password-encryption indica al software Cisco IOS XE que cifre las contraseñas, los secretos del Protocolo de autenticación por desafío mutuo (CHAP) y datos similares que se guardan en su archivo de configuración. Dicho cifrado es útil para evitar que observadores casuales lean las contraseñas, como, por ejemplo, cuando miran la pantalla durante la reunión de un administrador. No obstante, el algoritmo empleado por el comando service password-encryption es un simple cifrado Vigenère. El algoritmo no ha sido diseñado para proteger los archivos de configuración contra el grave análisis de, incluso, atacantes poco sofisticados y no debe ser utilizado con este fin. Cualquier archivo de configuración de Cisco IOS XE que contenga contraseñas cifradas debe tratarse con el mismo cuidado que se utiliza para una lista de texto sin cifrar de esas mismas contraseñas.

Mientras que este algoritmo de cifrado vulnerable no es utilizado por el comando enable secret, es utilizado por el comando de configuración global enable password, así como por el comando password line configuration. Las contraseñas de este tipo deben ser eliminadas y se debe utilizar el comando enable secret o la función Enhanced Password Security.

El comando enable secret y la función Enhanced Password Security utilizan Message Digest 5 (MD5) como hash de contraseñas. Este algoritmo ha tenido considerable revisión pública y no es reversible. Sin embargo, el algoritmo está sujeto a ataques de diccionario. En un ataque de diccionario, un atacante prueba todas las palabras de un diccionario o de otra lista de contraseñas candidatas para encontrar una coincidencia. Por lo tanto, los archivos de configuración se deben guardar con seguridad y compartir solamente con individuos de confianza.

Enhanced Password Security

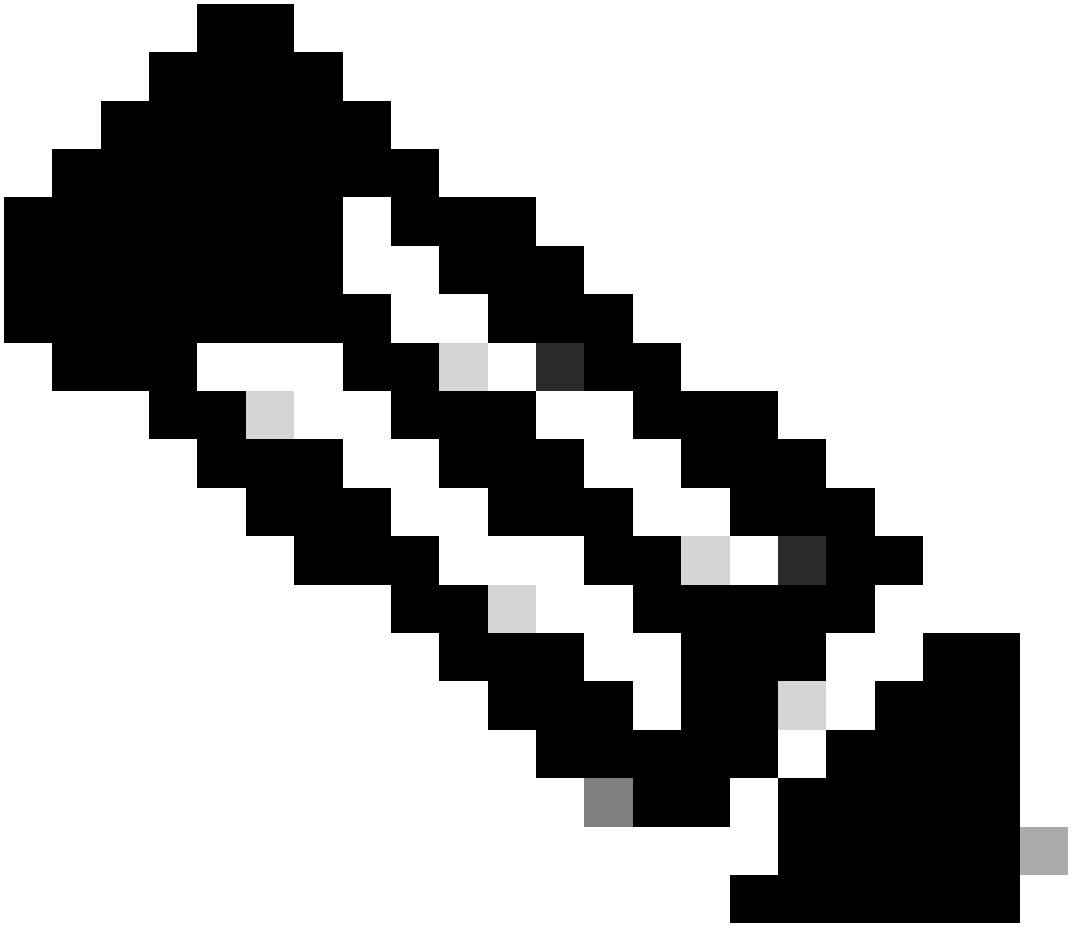
La función Enhanced Password Security, que ha funcionado desde la primera versión del software Cisco IOS XE versión 16.6.4, permite que un administrador configure el hash MD5 de contraseñas para el comando username. Antes de esta función, había dos tipos de contraseñas: Tipo 0, que es una contraseña de texto sin cifrar, y Tipo 7, que utiliza el algoritmo del cifrado Vigen re. La función Enhanced Password Security no se puede utilizar con protocolos que exigen que la contraseña de texto sin formato sea recuperable, como CHAP.

Para cifrar una contraseña de usuario con hash MD5, ejecute el comando de configuración global username secret.

username <name> secret <password>

Login Password Retry Lockout

La función Login Password Retry Lockout, que ha funcionado desde la primera versión del software Cisco IOS XE versión 16.6.4, permite bloquear una cuenta de usuario local después de un número configurado de intentos de inicio de sesión fallidos. Una vez que un usuario ha sido bloqueado, su cuenta queda bloqueada hasta que la desbloquee. Un usuario autorizado configurado con nivel de privilegio 15 no puede ser bloqueado con esta función. La cantidad de usuarios con el nivel de privilegio 15 debe ser mínima.



> Nota: los usuarios autorizados pueden bloquearse a sí mismos fuera de un dispositivo si se alcanza el número de intentos de inicio de sesión fallidos. Además, un usuario malicioso puede crear una condición de negación de servicio con intentos repetidos de autenticación con un nombre de usuario válido.

Este ejemplo muestra cómo habilitar la función Login Password Retry Lockout:

aaa new-model aaa local authentication tries max-fail <max-tries> aaa authentication login default local

username <name> secret <password>

Esta función también se aplica a los métodos de autenticación como CHAP y Password Authentication Protocol (PAP).

No Service Password-Recovery

En la versión 16.6.4 y posteriores del software Cisco IOS XE, la función No Service Password-

Recovery no permite que nadie con acceso a la consola acceda de forma insegura a la configuración del dispositivo y borre la contraseña. Tampoco permite que usuarios maliciosos cambien el valor del registro de configuración y accedan a NVRAM.

no service password-recovery

El software Cisco IOS XE proporciona un procedimiento de recuperación de contraseña que se basa en el acceso al modo de supervisión de ROM (ROMMON) y utiliza la tecla de interrupción durante el inicio del sistema. En ROMMON, el software del dispositivo puede volver a cargarse para iniciar una nueva configuración del sistema que incluye una nueva contraseña.

El procedimiento de recuperación de la contraseña actual permite que cualquier usuario con acceso a la consola acceda al dispositivo y a su red. La función de no recuperación de contraseña de servicio impide el empleo de la secuencia de la tecla Interrumpir y el ingreso a ROMMON durante la fase de inicio.

Si no se habilita la función No Service Password-Recovery en un dispositivo, se recomienda que se guarde una copia fuera de línea de la configuración del dispositivo y que se implemente una solución de archivado de configuración. Si es necesario recuperar la contraseña de un dispositivo Cisco IOS XE una vez habilitada esta función, se elimina toda la configuración.

Inhabilitación de Servicios No Utilizados

Como práctica recomendada de seguridad, todo servicio que no sea necesario debe ser inhabilitado. Estos servicios no necesarios, especialmente los que usan el protocolo UDP, son rara vez utilizados con fines legítimos, pero pueden usarse para lanzar ataques de denegación de servicio y otros ataques que también se frenan mediante el filtrado de paquetes.

Los servicios simples de TCP y de UDP deben ser inhabilitados. Estos servicios incluyen:

1. echo (número del puerto 7)
2. discard (número de puerto 9)
3. daytime (número de puerto 13)
4. chargen (número de puerto 19)

   Aunque las listas de acceso protegidas contra suplantación puedan evitar o hacer menos peligroso el abuso de los servicios simples, estos se deben inhabilitar en cualquier dispositivo al que se pueda acceder dentro de la red. Los servicios pequeños están inhabilitados de forma predeterminada en las versiones 16.6.4 y posteriores del software Cisco IOS XE. En las versiones anteriores del software, se pueden ejecutar los comandos de configuración global no service tcp-small-servers y no service udp-small-servers para inhabilitarlos.

   Esta es una lista de servicios adicionales que se deben inhabilitar si no se los utiliza:
5. Ejecute el comando de configuración global no ip finger para inhabilitar el servicio Finger. Las versiones posteriores a la 16.1 del software Cisco IOS XE desactivan este servicio de forma predeterminada.
6. Ejecute el comando de configuración global no ip bootp server para inhabilitar Bootstrap

Protocol (BOOTP). Las versiones posteriores a la 16.1 del software Cisco IOS XE desactivan este servicio de forma predeterminada.
7. En Cisco IOS XE Software Release 16.6.4 y versiones posteriores, ejecute el comando ip dhcp bootp ignore en el modo de configuración global para inhabilitar BOOTP. De esta manera, quedan habilitados los servicios de Dynamic Host Configuration Protocol (DHCP).
8. Los servicios de DHCP pueden ser inhabilitados si no se necesitan los servicios de retransmisión de DHCP. Ejecute el comando no service dhcp en modo de configuración global.
9. Ejecute el comando no mop enabled en modo de configuración de interfaz para inhabilitar el servicio de Maintenance Operation Protocol (MOP).
10. Ejecute el comando de configuración global no ip domain-lookup para inhabilitar los servicios de resolución del Sistema de Nombres del Dominio (DN).
11. Ejecute el comando no service pad en modo de configuración global para inhabilitar el servicio de Packet Assembler/Disassembler (PAD), que se utiliza para las redes X.25.
12. El servidor HTTP puede desactivarse con el comando no ip http server en el modo de configuración global, mientras que el servidor HTTP seguro (HTTPS) puede desactivarse con el comando de configuración global no ip http secure-server.
13. A menos que los dispositivos Cisco IOS XE recuperen configuraciones de la red durante el inicio, se debe utilizar el comando de configuración global no service config. Esto evita que el dispositivo Cisco IOS XE intente localizar un archivo de configuración en la red con TFTP.
14. Cisco Discovery Protocol (CDP) es un protocolo de red que se utiliza para descubrir otros dispositivos con CDP habilitado para la adyacencia de vecinos y la topología de red. CDP se puede utilizar por los sistemas de administración de red (NMS) o durante el troubleshooting. CDP se debe inhabilitar en todas las interfaces que estén conectadas con redes no confiables. Para ello, ejecute el comando de interfaz no cdp enable. De manera alternativa, el CDP se puede inhabilitar globalmente con el comando de configuración global no cdp run. Tenga en cuenta que CDP puede ser utilizado por un usuario malicioso para reconocimiento y mapping de red.
15. Link Layer Discovery Protocol (LLDP) es un protocolo de IEEE que se define en 802.1AB. LLDP es similar a CDP. Sin embargo, este protocolo permite la interoperabilidad entre los otros dispositivos que no admiten CDP. LLDP debe recibir el mismo tratamiento que CDP y se debe inhabilitar en todas las interfaces que se conecten con redes no confiables. Para ello, ejecute los comandos de configuración de interfaz no lldp transmit y no lldp receive. Ejecute el comando no lldp run global configurationpara inhabilitar LLDP globalmente. LLDP también puede ser utilizado por un usuario malicioso para reconocimiento y mapping de red.
16. Para los switches que soportan el arranque desde sdflash, la seguridad se puede mejorar arrancando desde flash y deshabilitando sdflash con el comando de configuración no sdflash.

Tiempo de Espera de EXEC

Para configurar el intervalo que el intérprete de comandos EXEC espera para la entrada del usuario antes de que termine una sesión, ejecute el comando de configuración de línea exec-timeout. El comando exec-timeout debe ser utilizado para cerrar las sesiones en las líneas vty o tty que quedan inactivas. De manera predeterminada, las sesiones se desconectan tras diez minutos de inactividad.

line con 0

exec-timeout <minutes> [seconds]

line vty 0 4

exec-timeout <minutes> [seconds]

Keepalives para Sesiones TCP

Los comandos de configuración global service tcp-keepalives-in y service tcp-keepalives-out permiten que un dispositivo envíe keepalives de TCP para sesiones de TCP. Esta configuración se debe utilizar para habilitar keepalives TCP en conexiones que entran al dispositivo y en conexiones que salen del dispositivo. Esto garantiza que el dispositivo en el extremo remoto de la conexión siga siendo accesible y que las conexiones semiabiertas o huérfanas se eliminen del dispositivo Cisco IOS XE local.

service tcp-keepalives-in

service tcp-keepalives-out

Uso de la interfaz de administración

Al plano de administración de un dispositivo se accede en banda o fuera de banda en una interfaz de administración física o lógica. Lo ideal es que existan tanto el acceso de administración en banda como el acceso de administración fuera de banda para cada dispositivo de red de modo que se pueda acceder al plano de administración durante interrupciones de la red.

Una de las interfaces más comunes que se utiliza para el acceso en banda a un dispositivo es la interfaz lógica Loopback. Las interfaces Loopback nunca dejan de funcionar, mientras que las interfaces físicas pueden cambiar de estado y quizá no se pueda acceder a la interfaz. Se recomienda agregar una interfaz Loopback en cada dispositivo como interfaz de administración y que se la utilice exclusivamente para el plano de administración. Esto permite que el administrador aplique las políticas en toda la red para el plano de administración. Una vez que la interfaz Loopback se configura en un dispositivo, puede ser utilizada por los protocolos del plano de administración, tales como SSH, SNMP y syslog, a fin de enviar y recibir el tráfico.

interface Loopback0

IP address 192.168.1.1 255.255.255.0

Notificaciones de Umbrales de Memoria

La función Memory Threshold Notification, agregada en la versión 16.6.4 del software Cisco IOS XE, permite mitigar las condiciones de memoria baja en un dispositivo. Esta función utiliza dos métodos para lograr esto: Memory Threshold Notification y Memory Reservation.

La función Memory Threshold Notification genera un mensaje de registro para indicar que la

memoria libre de un dispositivo se ha reducido por debajo del umbral configurado. Este ejemplo de configuración muestra cómo habilitar esta función con el comando de configuración global memory free low-watermark. Este comando habilita a un dispositivo para que genere una notificación cuando la memoria libre disponible se reduce por debajo del umbral especificado y para que vuelva a generar una notificación cuando la memoria libre disponible aumenta en un cinco por ciento más que el umbral especificado.

memory free low-watermark processor <threshold>

memory free low-watermark io <threshold>

El método Memory Reservation se utiliza de modo que haya memoria suficiente disponible para notificaciones cruciales. Este ejemplo de configuración demuestra cómo habilitar esta función. Esto garantiza que los procesos de administración continúen funcionando cuando se agota la memoria del dispositivo.

memory reserve critical <value>

Notificación de Umbrales de CPU

Introducida en la versión 16.6.4 del software Cisco IOS XE, la función CPU Thresholding Notification permite detectar y recibir notificaciones cuando la carga de la CPU en un dispositivo supera un umbral configurado. Cuando se supera el umbral, el dispositivo genera y envía un mensaje de trampa SNMP. El software Cisco IOS XE admite dos métodos de umbral de utilización de la CPU: umbral ascendente y umbral descendente.

Este ejemplo de configuración muestra cómo habilitar umbrales superiores e inferiores que accionan un mensaje de notificación del umbral del CPU:

snmp-server enable traps cpu threshold

snmp-server host <host-address> <community-string> cpu

process cpu threshold type <type> rising <percentage> interval <seconds> [caída <percentage> interval <seconds>]

process cpu statistics limit entry-percentage <number> [size <seconds>]

Network Time Protocol

El protocolo Network Time Protocol (NTP) no es un servicio particularmente peligroso, pero cualquier servicio innecesario puede representar un vector de ataque. Si se utiliza el protocolo NTP, es importante configurar explícitamente un origen de hora confiable y utilizar la autenticación adecuada. Se requiere un tiempo preciso y confiable para fines de syslog, como durante las investigaciones forenses de ataques potenciales, así como para la conectividad VPN exitosa que depende de los certificados para la autenticación de la Fase 1.

1. Zona horaria de NTP: Al configurar NTP, debe configurarse la zona horaria para que las marcas de tiempo se correlacionen bien. Estos son los dos métodos habituales para

configurar la zona horaria en los dispositivos de redes con presencia global. Un método es configurar todos los dispositivos de red con el Tiempo Universal Coordinado (UTC), previamente conocido como Tiempo Medio de Greenwich (GMT). El otro método es configurar los dispositivos de red con el huso horario local. Puede encontrar más información sobre esta función en la zona horaria del reloj en la documentación del producto de Cisco.

2. Autenticación de NTP: Si configura la autenticación de NTP, se garantiza que los mensajes de NTP se intercambien entre pares de NTP confiables.

   Configuración de ejemplo que utiliza autenticación NTP:

   Cliente:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

   (config)#ntp server 172.16.1.5 key 5 Server:

   (config)#ntp authenticate

   (config)#ntp authentication-key 5 md5 ciscotime

   (config)#ntp trusted-key 5

Acceso limitado a la red mediante ACL de infraestructura

Las listas de control de acceso a la infraestructura (iACL), creadas para evitar la comunicación directa no autorizada con dispositivos de red, constituyen uno de los controles de seguridad más cruciales que se puede implementar en las redes. Las ACL de infraestructura aprovechan la idea de que prácticamente todo el tráfico cruza la red y no se dirige a la red en sí misma.

Las iACL se crean y aplican para especificar las conexiones de hosts o redes que pueden acceder a los dispositivos de redes. Ejemplos comunes de estos tipos de conexión son eBGP, SSH y SNMP. Después de que se hayan permitido las conexiones necesarias, el resto del tráfico a la infraestructura se niega explícitamente. Todo el tráfico de tránsito que cruza la red y no se dirige a los dispositivos de la infraestructura se permite explícitamente.

Las iACL ofrecen protecciones que son relevantes tanto para el plano de administración como para el plano de control. La implementación de iACL se puede facilitar con el uso de un direccionamiento distinto para los dispositivos de la infraestructura de la red. Consulte Enfoque Orientado a la Seguridad para el Direccionamiento IP para obtener más información sobre las consecuencias en la seguridad del direccionamiento IP.

Este ejemplo de configuración de iACL ilustra la estructura que se debe utilizar como punto de partida cuando usted comienza el proceso de implementación de iACL:

ip access-list extended ACL-INFRASTRUCTURE-IN

— Permitir las conexiones necesarias para los protocolos de routing y la gestión de redes

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179

permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>

permit tcp host <trusted-management-stations> any eq 22

permit udp host <trusted-netmgmt-servers> any eq 161

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny ip any <infrastructure-address-space> <wildcard-mask>

— Permitir tráfico en tránsito

permit ip any any

Una vez creada, la iACL se debe aplicar a todas las interfaces que se encuentran con dispositivos que no forman parte de la infraestructura, que incluyen las interfaces que se conectan con otras organizaciones, segmentos de acceso remoto, segmentos de usuario y segmentos en centros de datos.

Consulte Protección del Núcleo: Listas de Control de Acceso para Protección de Infraestructura para obtener más información sobre las ACL de Infraestructura.

Filtrado de Paquetes ICMP

Internet Control Message Protocol (ICMP) ha sido diseñado como protocolo de control de IP. Como tal, los mensajes que transporta pueden tener ramificaciones de amplio alcance a los protocolos TCP e IP en general. Mientras que las herramientas de troubleshooting de la red ping y traceroute usan ICMP, rara vez se necesita la conectividad externa ICMP para el correcto funcionamiento de una red.

El software Cisco IOS XE proporciona funcionalidad para filtrar específicamente los mensajes ICMP por nombre o tipo y código. Esta ACL de ejemplo, que se debe utilizar con las entradas de control de acceso (ACE) de los ejemplos anteriores, permite pings de estaciones de administración y de servidores NMS confiables y bloquea el resto de los paquetes ICMP:

ip access-list extended ACL-INFRASTRUCTURE-IN

— Permitir eco ICMP (ping) desde estaciones de administración y servidores de confianza

permit icmp host <trusted-management-stations> any echo

permit icmp host <trusted-netmgmt-servers> any echo

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny ip any <infrastructure-address-space> <wildcard-mask>

— Permitir tráfico en tránsito

permit ip any any

Filtrar fragmentos IP

El proceso de filtrado para los paquetes de IP fragmentados puede constituir un desafío para los dispositivos de seguridad. Esto se debe a que la información de la Capa 4 que se utiliza para filtrar los paquetes TCP y UDP está solamente presente en el fragmento inicial. El software Cisco IOS XE utiliza un método específico para verificar los fragmentos no iniciales con respecto a las listas de acceso configuradas. El software Cisco IOS XE evalúa estos fragmentos no iniciales frente a la ACL e ignora cualquier información de filtrado de Capa 4. Esto hace que los fragmentos no iniciales sean evaluados solamente en la parte de la Capa 3 de cualquier ACE configurada.

En este ejemplo de configuración, si un paquete TCP que se dirige a 192.168.1.1 en el puerto 22 se fragmenta en tránsito, el fragmento inicial deja de funcionar como lo espera la segunda ACE según la información de la Capa 4 dentro del paquete. Sin embargo, la primera ACE permite todos los fragmentos restantes (no iniciales) y para ello se basa completamente en la información de la Capa 3 en el paquete y en la ACE. El escenario se muestra en esta configuración:

ip access-list extended ACL-FRAGMENT-EXAMPLE

permit tcp any host 192.168.1.1 eq 80

deny tcp any host 192.168.1.1 eq 22

Debido a la naturaleza no intuitiva del manejo de fragmentos, las ACL suelen permitir fragmentos IP inadvertidamente. La fragmentación también se usa con frecuencia para intentar evadir la detección mediante sistemas de detección de intrusión. Por estas razones los fragmentos IP se usan frecuentemente en ataques y deben ser filtrados explícitamente por encima de cualquier iACL configurada. Esta ACL de ejemplo incluye un filtrado completo de fragmentos IP. Las funciones de este ejemplo se deben utilizar junto con las funciones de los ejemplos anteriores.

ip access-list extended ACL-INFRASTRUCTURE-IN

— Denegar fragmentos IP que utilizan ACE específicos de protocolo para ayudar en

— clasificación del tráfico de ataque

deny tcp any any fragments

deny udp any any fragments

deny icmp any any fragments

deny ip any any fragments

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny ip any <infrastructure-address-space> <wildcard-mask>

— Permitir tráfico en tránsito

permit ip any any

Consulte Listas de control acceso y fragmentos de IP para ver más información sobre cómo actúan las ACL ante los paquetes de IP fragmentados.

ACL Support for Filtering IP Options

La versión 16.6.4 del software Cisco IOS XE agregó soporte para el uso de ACL para filtrar paquetes IP basados en las opciones IP que contiene el paquete. Las opciones IP representan un desafío de seguridad para los dispositivos de red porque se deben procesar como paquetes de excepción. Esto exige un nivel de esfuerzo del CPU que no es necesario para los paquetes típicos que cruzan la red. La presencia de opciones IP dentro de un paquete puede también indicar un intento de destruir los controles de seguridad en la red o de alterar de otra manera las características de tránsito de un paquete. Es por estas razones que los paquetes con opciones IP se deben filtrar en el borde de la red.

Este ejemplo se debe utilizar con las ACE de los ejemplos anteriores para incluir el filtrado completo de paquetes IP que contienen opciones IP:

ip access-list extended ACL-INFRASTRUCTURE-IN

— Denegar paquetes IP que contengan opciones IP

deny ip any any option any-options

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny ip any <infrastructure-address-space> <wildcard-mask>

— Permitir tráfico en tránsito

permit ip any any

Filtrado en ACL por el valor de TTL

La versión 16.6.4 del software Cisco IOS XE agregó soporte ACL para filtrar paquetes IP en función del valor de Tiempo de vida (TTL). Los dispositivos de red reducen el valor TTL de un datagrama IP a medida que un paquete fluye del origen al destino. Aunque los valores iniciales varíen según el sistema operativo, cuando el valor TTL de un paquete alcanza cero, se debe descartar el paquete. Los dispositivos donde el TTL llega a cero pierden los paquetes, y deben

generar y enviar a la fuente del paquete un mensaje de tiempo de ICMP agotado.

La generación y la transmisión de estos mensajes es un proceso de excepción. Los routers pueden cumplir esta función cuando la cantidad de paquetes de IP a punto de perderse es baja, pero, si la cantidad es elevada, la tarea de generar y transmitir estos mensajes puede consumir todos los recursos de la CPU. Esto genera un vector de ataque de negación de servicio. Por este motivo, los dispositivos deben fortalecerse para los ataques de denegación de servicio que emplean una gran cantidad de paquetes de IP a punto de perderse.

Se recomienda que las organizaciones filtren los paquetes IP con valores TTL bajos en el borde de la red. Si se filtran exhaustivamente los paquetes con valores TTL insuficientes para cruzar la red, disminuye la amenaza de ataques basados en TTL.

En este ejemplo, ACL filtra paquetes con valores TTL menores a seis. De esta manera se protege a las redes de hasta cinco saltos de ancho contra los ataques basados en el vencimiento de TTL.

ip access-list extended ACL-INFRASTRUCTURE-IN

— Denegar paquetes IP con valores TTL insuficientes para atravesar la red

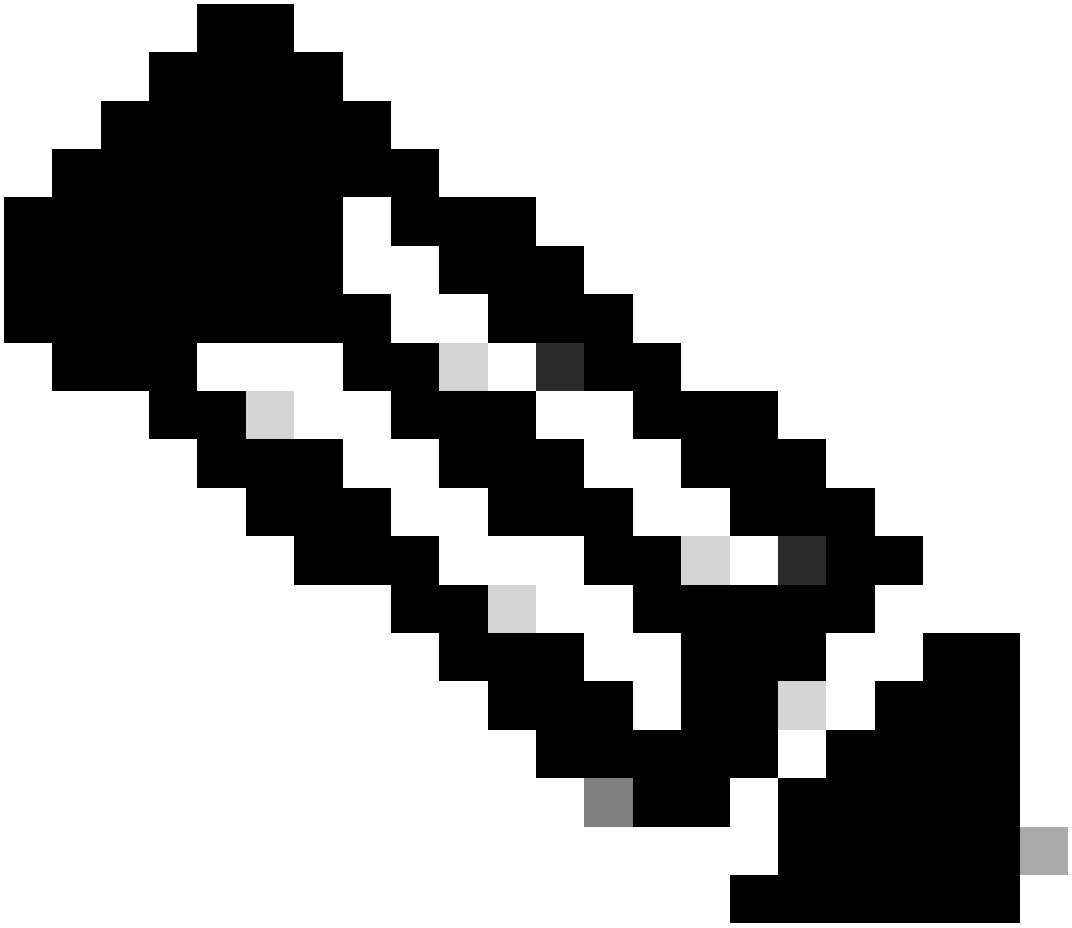
deny ip any any ttl lt 6

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny ip any <infrastructure-address-space> <mask>

— Permitir tráfico en tránsito

permit ip any any



Nota: Algunos protocolos hacen un uso legítimo de paquetes con valores TTL bajos. eBGP es uno de esos protocolos. Consulte Identificación y Disminución de Ataques Basados en el Vencimiento de TTL para obtener más información sobre la disminución de ataques que se basan en el vencimiento de TTL.

Proteja las sesiones de administración interactiva

Las sesiones de administración de dispositivos le permiten ver y recopilar información sobre un dispositivo y sus operaciones. Si esta información se divulga a un usuario malicioso, el dispositivo puede convertirse en blanco de ataque, verse en peligro o ser usado para realizar ataques adicionales. Cualquier persona con acceso privilegiado a un dispositivo tiene la capacidad para el control administrativo completo de ese dispositivo. Es fundamental proteger las sesiones de administración, a fin de no revelar información e impedir el acceso no autorizado.

Management Plane Protection

En la versión 16.6.4 y posteriores del software Cisco IOS XE, la función Management Plane Protection (MPP) permite que un administrador restrinja en qué interfaces puede recibir un dispositivo el tráfico de administración. De esta manera, el administrador tiene control adicional sobre un dispositivo y el modo de acceso a él.

En este ejemplo se ve cómo activar la MPP para solo permitir SSH y HTTPS en la interfaz de GigabitEthernet0/1:

host del plano de control

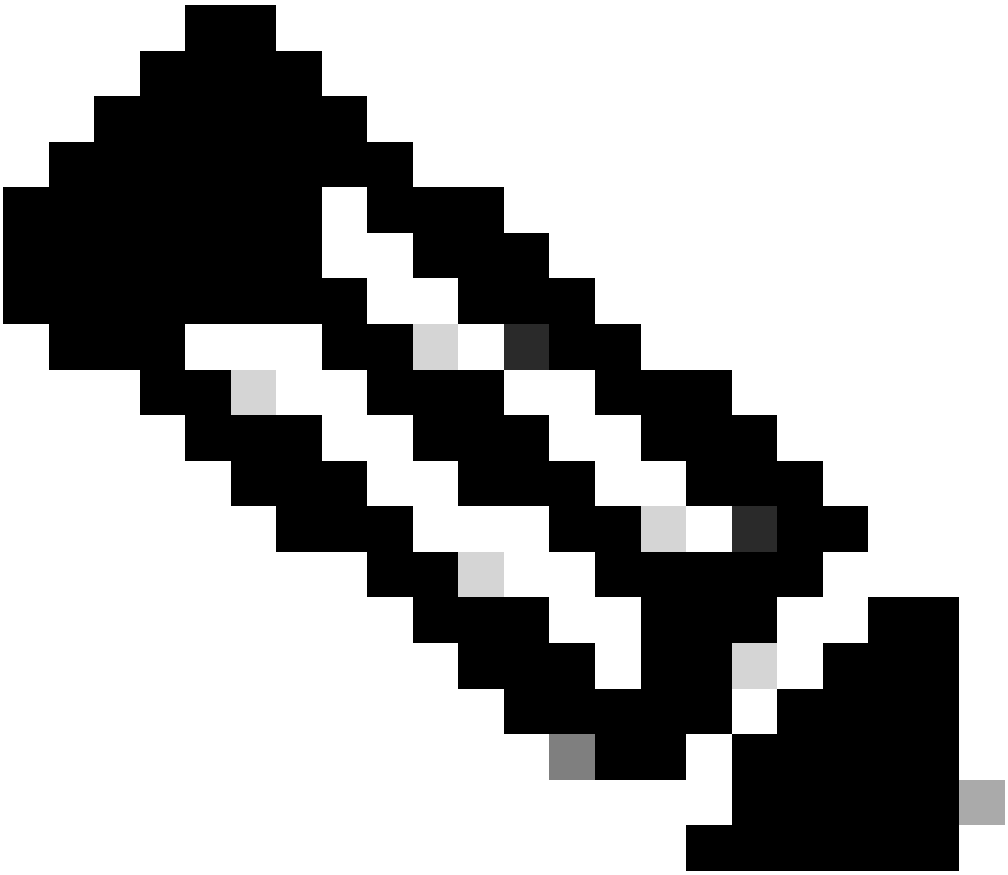
management-interface GigabitEthernet 0/1 allow ssh https

Función Control Plane Protection

La protección del plano de control (CPPr) se basa en la funcionalidad de la política del plano de control para restringir y controlar el tráfico del plano de control que se dirige al procesador de rutas del dispositivo IOS-XE. CPPr divide el plano de control en categorías de plano de control independientes que se conocen como subinterfaces. Existen tres subinterfaces de plano de control: Host, Transit y CEF-Exception. Además, CPPr incluye estas funciones adicionales para la protección del plano de control:

1. Filtrado de puertos: Esta función permite controlar o rechazar paquetes que vayan a puertos UDP y TCP cerrados o sin escucha.
2. Política de umbral de colas: Esta función limita la cantidad de paquetes de un protocolo especificado admitida en la cola de entrada de IP del plano de control.

   CPPr permite que los administradores clasifiquen, controlen y restrinjan el tráfico enviado a dispositivos con fines administrativos mediante la subinterfaz de host. Entre algunos ejemplos de paquetes que se clasifican para la categoría de subinterfaz host se incluyen el tráfico de administración, como SSH o Telnet, y los protocolos de ruteo.



Nota: CPPr no admite IPv6 y está restringido a la ruta de entrada IPv4.

Consulte Control Plane Policing para obtener más información sobre la función Cisco CPPr.

Encripte las sesiones de administración

Dado que en las sesiones de administración interactiva se puede revelar información, este tráfico debe encriptarse para que usuarios maliciosos no accedan a los datos transmitidos. La encriptación del tráfico permite conexiones de acceso remoto seguras con dispositivos. Si el tráfico para una sesión de administración se envía por la red en texto sin formato, un atacante puede obtener información confidencial sobre el dispositivo y la red.

Un administrador puede establecer una conexión de administración de acceso remoto cifrada y segura a un dispositivo con las funciones SSH o Protocolo seguro de transferencia de hipertexto (HTTPS). El software Cisco IOS XE es compatible con SSH versión 2.0 (SSHv2) y HTTPS, que utiliza Secure Sockets Layer (SSL) y Transport Layer Security (TLS) para la autenticación y el cifrado de datos.

El software Cisco IOS XE también es compatible con el protocolo de copia segura (SCP), que permite una conexión cifrada y segura para copiar configuraciones de dispositivos o imágenes de

software. El protocolo SCP depende de SSH.

Este ejemplo de configuración habilita SSH en un dispositivo Cisco IOS XE:

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

line vty 0 4

transport input ssh

Este ejemplo de configuración habilita los servicios de SCP:

ip scp server enable

Esto es un ejemplo de configuración para los servicios HTTPS:

crypto key generate rsa modulus 2048

ip http secure-server

SSHv2

La función SSHv2 se introdujo en Cisco IOS XE en la primera versión 16.6.4 que permite al usuario configurar SSHv2. SSH se ejecuta encima de una capa de transporte confiable y proporciona capacidades de autenticación y encripción potentes. El único transporte confiable que se define para el SSH es TCP. SSH proporciona una manera de acceder con seguridad y de ejecutar con seguridad comandos en otra computadora o en otro dispositivo por una red. La función Secure Copy Protocol (SCP) tunelada a través de SSH permite una transferencia de archivos segura.

Si el comando ip ssh version 2 no se configura explícitamente, Cisco IOS XE habilita la versión 1.99 de SSH. La versión 1.99 de SSH permite conexiones de SSHv1 y SSHv2. Se considera que SSHv1 es inseguro y puede generar efectos adversos en el sistema. Si SSH está habilitado, se recomienda inhabilitar SSHv1 mediante el uso del comando ip ssh version 2.

Este ejemplo de configuración habilita SSHv2 (con SSHv1 inhabilitado) en un dispositivo Cisco IOS XE:

hostname router

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh time-out 60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

ip ssh version 2

line vty 0 4

transport input ssh

Consulte Soporte Secure Shell Version 2 para obtener más información sobre el uso de SSHv2.

SSHv2 Enhancements for RSA Keys

Cisco IOS XE SSHv2 admite métodos de autenticación interactivos mediante teclado y basados en contraseña. Las función SSHv2 Enhancements for RSA Keys también admite la autenticación mediante clave pública RSA para el cliente y el servidor.

Para la autenticación de usuario, la autenticación de usuario basada en RSA utiliza una pareja de claves privada/pública asociadas con cada usuario para la autenticación. El usuario debe generar un par de claves privada/pública en el cliente y configurar una clave pública en el servidor SSH de Cisco IOS XE para completar la autenticación.

El usuario de SSH que intenta establecer las credenciales introduce una firma encriptada con la clave privada. La firma y la clave pública del usuario se envían al servidor SSH para la autenticación. El servidor SSH calcula un hash de la clave pública proporcionada por el usuario. Se emplea el hash para determinar si el servidor tiene una entrada que coincida. Si se halla una coincidencia, se efectúa la verificación de mensaje RSA con la clave pública. Por lo tanto, se autentica o se niega el acceso al usuario de acuerdo con la firma cifrada.

Para la autenticación del servidor, el cliente SSH de Cisco IOS XE debe asignar una clave de host para cada servidor. Cuando el cliente intenta establecer una sesión SSH con un servidor, recibe la firma del servidor como parte del mensaje de intercambio de claves. Si se activa en el cliente la marca de control estricto de clave de organizador, el cliente controla si se encuentra la entrada de clave de organizador correspondiente al servidor preconfigurado. Si se halla una coincidencia, el cliente intenta validar la firma con la clave de organizador del servidor. Si el servidor se autentica correctamente, el establecimiento de sesión continúa; de lo contrario, se termina y muestra un mensaje Error en la autenticación del servidor.

Este ejemplo de configuración habilita el uso de claves RSA con SSHv2 en un dispositivo Cisco IOS XE:

Configure un nombre de host para el dispositivo

hostname router

Configurar un nombre de dominio

ip domain-name example.com

Habilite el servidor SSH para la autenticación local y remota en el router que utiliza

el comando "crypto key generate".

Para la versión 2 de SSH, el tamaño del módulo debe ser al menos de 768 bits

crypto key generate rsa usage-keys label shkeys modulus 2048

Especifique el nombre del par de claves RSA (en este caso, "sshkeys") que se utilizará para SSH

ip ssh rsa keypair-name sshkeys

Configure un tiempo de espera ssh (en segundos).

El siguiente resultado habilita un tiempo de espera de 120 segundos para las conexiones SSH.

ip ssh time-out 120

Configure un límite de cinco reintentos de autenticación.

ip ssh authentication-retries 5

Configuración de SSH versión 2.

ip ssh version 2

Consulte Secure Shell Version 2 Enhancements for RSA Keys para obtener más información sobre el uso de claves RSA con SSHv2.

Este ejemplo de configuración permite que el servidor SSH de Cisco IOS XE realice la autenticación de usuario basada en RSA. La autenticación de usuario es exitosa si la clave pública RSA guardada en el servidor se verifica con la clave pública o la clave privada guardadas en el cliente.

Configure un nombre de host para el dispositivo.

hostname router

Configure un nombre de dominio.

ip domain name cisco.com

Genere pares de claves RSA que utilicen un módulo de 2048 bits.

crypto key generate rsa modulus 2048

Configure las claves SSH-RSA para la autenticación de usuario y servidor en el servidor SSH.

ip ssh pubkey-chain

Configure el nombre de usuario de SSH.

Configure las claves SSH-RSA para la autenticación de usuario y servidor en el servidor SSH.

ip ssh pubkey-chain

Configure el nombre de usuario de SSH.

username ssh-user

Especifique la llave pública RSA del peer remoto.

Debe configurar el comando key-string

(seguido de la clave pública RSA del par remoto) o el

comando key-hash (seguido del tipo de clave SSH y la versión).

Consulte Configuración del Servidor SSH de Cisco IOS XE para Realizar la Autenticación de Usuario Basada en RSA para obtener más información sobre el uso de claves RSA con SSHv2.

Este ejemplo de configuración permite que el cliente SSH de Cisco IOS XE realice la autenticación del servidor basada en RSA.

hostname router

ip domain-name cisco.com

Genere pares de llaves RSA.

crypto key generate rsa

Configure las claves SSH-RSA para la autenticación de usuario y servidor en el servidor SSH.

ip ssh pubkey-chain

Habilite el servidor SSH para la autenticación de clave pública en el router.

server SSH-server-name

Especifique la clave pública RSA del par remoto.

Debe configurar el comando key-string

(seguido de la clave pública RSA del par remoto) o thea

comando key-hash <key-type> <key-name> (seguido de la clave SSH

tipo y versión).

Asegúrese de que se realice la autenticación del servidor: la conexión es

finalizado en caso de fallo.

ip ssh stricthostkeycheck

Consulte Configuración del Cliente SSH de Cisco IOS XE para Realizar la Autenticación del Servidor Basada en RSA para obtener más información sobre el uso de claves RSA con SSHv2.

Puertos de Consola y Auxiliar

En los dispositivos Cisco IOS XE, los puertos de consola y auxiliares (AUX) son líneas asíncronas que se pueden utilizar para el acceso local y remoto a un dispositivo. Debe tener en cuenta que los puertos de consola de los dispositivos Cisco tienen privilegios especiales. Particularmente, estos privilegios permiten que un administrador realice el procedimiento de recuperación de contraseña. Para realizar la recuperación de contraseña, un atacante no autenticado necesitaría tener acceso al puerto de consola y la capacidad de interrumpir la energía al dispositivo o de hacer que el dispositivo colapse.

Los métodos usados para acceder el puerto de consola de un dispositivo se deben asegurar de la misma forma que se asegura el acceso privilegiado a un dispositivo. Los métodos utilizados para asegurar el acceso deben incluir el uso de AAA, exec-timeout y contraseñas del módem si un módem está conectado a la consola.

Si la recuperación de contraseña no es necesaria, un administrador puede quitar la capacidad de realizar el procedimiento de recuperación de contraseña que utiliza el comando de configuración global no service password-recovery; sin embargo, una vez que se ha habilitado el comando no service password-recovery, un administrador ya no puede realizar la recuperación de contraseña en un dispositivo.

En la mayoría de las situaciones, el puerto AUX de los dispositivos debe desactivarse para impedir el acceso no autorizado. Los puertos AUX pueden desactivarse mediante estos comandos:

line aux 0

 transport input none

 transport output none

 no exec exec-timeout 0 1

 no password

Control de Líneas vty y tty

Las sesiones de administración interactivas del software Cisco IOS XE utilizan tty o tty virtual (vty). Una línea tty es una línea asíncrona local a la cual se puede conectar un terminal para el acceso local al dispositivo o a un módem para el acceso por marcación a un dispositivo. Tenga en

cuenta que las líneas tty se pueden utilizar para conexiones a los puertos de consola de otros dispositivos. Esta función permite que un dispositivo con líneas tty funcione como servidor de consola donde se pueden establecer conexiones a través de la red a los puertos de consola de dispositivos conectados con las líneas tty. Las líneas tty para estas conexiones inversas a través de la red también deben ser controladas.

Una línea vty se utiliza para el resto de las conexiones de red remotas admitidas por el dispositivo, independientemente del protocolo (SSH, SCP o Telnet, por ejemplo). Para garantizar el acceso a un dispositivo a través de una sesión de administración local o remota, se deben implementar controles apropiados en las líneas vty y las líneas tty. Los dispositivos Cisco IOS XE tienen un número limitado de líneas vty; el número de líneas disponibles se puede determinar con el comando EXEC show line. Cuando todas las líneas de vty ya están usadas, no se puede establecer nuevas sesiones de administración, lo cual crea una condición de denegación de servicio para el acceso al dispositivo.

La forma más simple de controlar el acceso a una vty o una tty de un dispositivo es mediante el uso de la autenticación en todas las líneas sin importar la ubicación del dispositivo dentro de la red. Esto es crucial para las líneas vty porque a ellas se accede a través de la red. También se puede acceder mediante la red a líneas de tty conectadas a módems empleados para acceso remoto a dispositivos, o a líneas de tty conectadas a puertos de consolas de otros dispositivos. Se pueden aplicar otras formas de controles de acceso a vty y tty mediante los comandos de configuración transport input o access-class, mediante las funciones CoPP y CPPr, o aplicando listas de acceso en interfaces de dispositivos.

La autenticación se puede aplicar mediante AAA, que es el método recomendado de acceso autenticado a dispositivos, mediante la base de datos de usuarios locales, o mediante la autenticación de contraseña simple configurada directamente en las líneas de vty o tty.

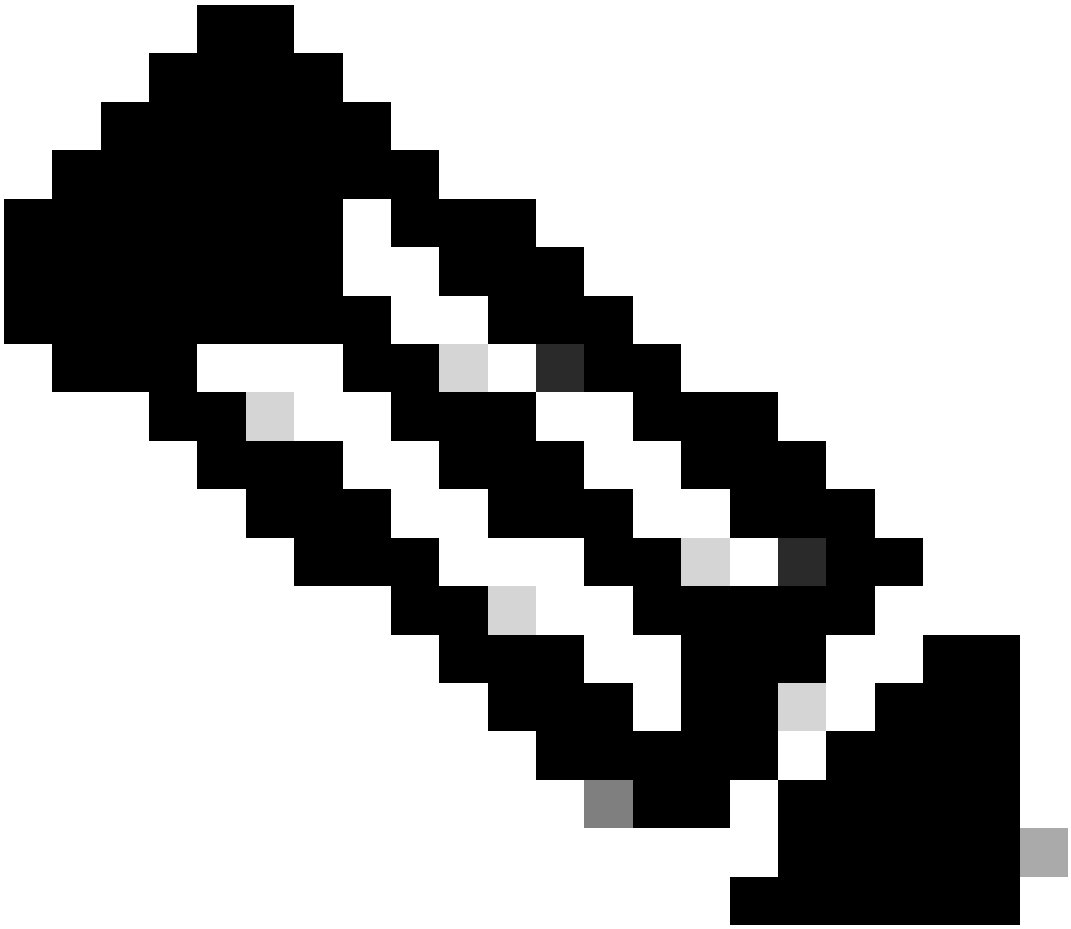
El comando exec-timeout debe ser utilizado para cerrar las sesiones en las líneas vty o tty que quedan inactivas. El comando service tcp-keepalives-in también debe emplearse para activar keepalives de TCP en conexiones entrantes a dispositivos. Esto garantiza que el dispositivo en el extremo remoto de la conexión siga siendo accesible y que las conexiones semiabiertas o huérfanas se eliminen del dispositivo IOS-XE local.

Control del Transporte para Líneas vty y tty

Un vty y tty se pueden configurar para aceptar solamente conexiones de administración de acceso remoto cifradas y seguras al dispositivo o a través del dispositivo si se utiliza como servidor de consola. Esta sección trata sobre las tty porque tales líneas se pueden conectar con los puertos de consola en otros dispositivos y, de esta manera, se puede acceder a ellas a través de la red. En un esfuerzo por evitar la divulgación de información o el acceso no autorizado a los datos que se transmiten entre el administrador y el dispositivo, se puede utilizar transport input ssh en lugar de protocolos de texto sin formato, como Telnet y rlogin. El comando de configuración transport input none puede configurarse en tty para desactivar el uso de la línea de tty con conexiones de consolas inversas.

Las líneas vty y las líneas tty permiten que un administrador se conecte con otros dispositivos.

Para limitar el tipo de transporte que un administrador puede utilizar para conexiones salientes, utilice el comando de configuración transport output line. Si las conexiones salientes no son necesarias, se puede utilizar transport output none. Sin embargo, si se permiten las conexiones salientes, se puede aplicar un método de acceso remoto cifrado y seguro para la conexión mediante el uso de transport output ssh.



> Nota: IPSec se puede utilizar para conexiones de acceso remoto seguras y cifradas a un dispositivo, si se admite. Si usted utiliza IPSec, este conjunto también agrega la sobrecarga del CPU adicional al dispositivo. Sin embargo, SSH se debe todavía implementar como el transporte, incluso cuando se utiliza IPSec.

Banners de Advertencia

En algunas jurisdicciones legales, puede ser imposible procesar a usuarios maliciosos y puede ser ilegal monitorearlos, a menos que se los haya notificado de que no tienen permitido emplear el sistema. Un método para proporcionar esta notificación es colocar esta información en un mensaje de banner que se configura con el comando banner login del software Cisco IOS XE.

Los requisitos de notificación legal son complejos, varían según la jurisdicción y la situación, y pueden discutirse con el asesor legal. Incluso dentro de las jurisdicciones, las opiniones legales pueden variar. En colaboración con un asesor, un banner puede proporcionar la siguiente información en forma parcial o total:

1. Notificación de que solamente el personal específicamente autorizado puede iniciar sesión o utilizar el sistema y quizás notificación de la información sobre quién puede autorizar el uso.
2. Notificación de que cualquier uso no autorizado del sistema es ilegal y de que puede estar sujeto a sanciones penales y civiles.
3. Notificación de que cualquier uso del sistema se puede registrar o monitorear sin nuevo aviso y que los registros resultantes se pueden utilizar como pruebas ante el tribunal.
4. Notificaciones específicas que exigen las leyes locales.

   Desde el punto de vista de la seguridad, en lugar de ser legal, un banner de inicio de sesión no puede contener ninguna información específica sobre el nombre del router, el modelo, el software o la propiedad. Los usuarios maliciosos pueden darle un uso indebido a esta información.

Autenticación, autorización y contabilidad

El marco de trabajo de autenticación, autorización y auditoría (AAA) es fundamental para proteger el acceso interactivo a dispositivos de redes. Este marco ofrece un entorno muy configurable que se puede acomodar a las necesidades de las redes.

autenticación TACACS+

TACACS+ es un protocolo de autenticación que los dispositivos Cisco IOS XE pueden utilizar para la autenticación de usuarios de administración en un servidor AAA remoto. Estos usuarios de administración pueden acceder al dispositivo IOS-XE a través de SSH, HTTPS, telnet o HTTP.

La autenticación TACACS+, más comúnmente conocida como autenticación AAA, le da a cada administrador de red la posibilidad de utilizar cuentas de usuarios individuales. Al no dependerse de una contraseña compartida, se mejora la seguridad de la red y se refuerza la responsabilidad individual.

RADIUS es un protocolo similar en su propósito a TACACS+; sin embargo, sólo cifra la contraseña enviada a través de la red. En cambio, TACACS+ encripta toda la carga útil de TCP, que incluye el nombre de usuario y la contraseña. Por esta razón, TACACS+ se puede utilizar en preferencia a RADIUS cuando TACACS+ es soportado por el servidor AAA. Consulte Comparación entre TACACS+ y RADIUS para obtener una comparación más detallada de estos dos protocolos.

La autenticación TACACS+ se puede habilitar en un dispositivo Cisco IOS XE con una configuración similar a este ejemplo:

aaa new-model

aaa authentication login default group tacacs+

tacacs server <server_name>

address ipv4 <tacacs_server_ip_address>

Key <key>

La configuración anterior se puede utilizar como punto de partida para una plantilla de autenticación AAA específica de una organización.

Una lista de métodos es una lista secuencial donde se describen los métodos de autenticación que se emplearán para autenticar a usuarios. Estas listas le permiten designar uno o más protocolos de seguridad para la autenticación y, por ende, garantizan un sistema de autenticación de respaldo por si fracasa el método inicial. El software Cisco IOS XE utiliza el primer método de la lista que acepta o rechaza correctamente a un usuario. Los métodos subsiguientes se intentan solamente si los métodos anteriores fallan debido a la falta de disponibilidad o a la configuración incorrecta del servidor.

Consulte Listas de Métodos con Nombre para la Autenticación para obtener más información sobre la configuración de Listas de Métodos con Nombre.

Autenticación Alternativa

Si todos los servidores TACACS+ configurados dejan de estar disponibles, un dispositivo Cisco IOS XE puede confiar en los protocolos de autenticación secundarios. Las configuraciones típicas incluyen el uso de las opciones de autenticación local o enable si todos los servidores TACACS+ configurados carecen de disponibilidad.

La lista completa de opciones para la autenticación en el dispositivo incluye enable, local y line. Cada uno de estas opciones tiene ventajas. Se prefiere el uso del comando enable secret porque el secreto se transforma en hash mediante un algoritmo unidireccional inherentemente más seguro que el algoritmo de cifrado empleado con las contraseñas de Tipo 7 para autenticación local o de línea.

Sin embargo, en las versiones del software Cisco IOS XE que admiten el uso de contraseñas secretas para usuarios definidos localmente, puede ser deseable recurrir a la autenticación local. Esto permite que se cree un usuario localmente definido para uno o más administradores de red. Si TACACS+ perdiera toda su disponibilidad, cada administrador puede utilizar su nombre de usuario local y su contraseña. Si bien esta acción amplía la responsabilidad individual de los administradores de redes en las interrupciones de TACACS+, aumenta significativamente la carga administrativa porque deben mantenerse las cuentas de usuarios locales en todos los dispositivos de redes.

Este ejemplo de configuración se basa en el ejemplo anterior de autenticación de TACACS+, para incluir autenticación de respaldo en la contraseña configurada de forma local con el comando enable secret:

enable secret <password>

aaa new-model

aaa authentication login default group tacacs+ enable

tacacs server <server_name>

address ipv4 <tacacs_server_ip_address>

Key <key>

Consulte Configuración de la Autenticación para obtener más información sobre el uso de la autenticación alternativa con AAA.

Uso de Contraseñas Tipo 7

Las contraseñas de Tipo 7, diseñadas originalmente para permitir la desencriptación rápida de contraseñas almacenadas, no constituyen un método seguro de almacenamiento de contraseñas. Hay muchas herramientas disponibles que pueden descifrar fácilmente estas contraseñas. Se puede evitar el uso de contraseñas de tipo 7 a menos que lo requiera una función que esté en uso en el dispositivo Cisco IOS XE.

El tipo 9 (cifrado) se puede utilizar siempre que sea posible:

username <username> privilege 15 algorithm-type scrypt secret <secret>

La eliminación de contraseñas de este tipo puede facilitarse con la autenticación AAA y el uso de la función Enhanced Password Security, que permite que las contraseñas secretas sean utilizadas con los usuarios que localmente se definen a través del comando de configuración global username. Si usted no puede evitar completamente el uso de contraseñas Tipo 7, tenga en cuenta que estas contraseñas son ofuscadas pero no cifradas.

Consulte la sección Fortalecimiento del plano de administración general en este documento para ver más información sobre la eliminación de las contraseñas de Tipo 7.

Autorización de Comandos con TACACS+

La autorización de comandos con TACACS+ y con AAA proporciona un mecanismo que permite o niega los comandos que ingresa un usuario administrativo. Cuando el usuario ingresa comandos EXEC, Cisco IOS XE envía cada comando al servidor AAA configurado. que utiliza sus políticas configuradas para permitir o negar el comando para ese usuario en particular.

Esta configuración se puede agregar al ejemplo de autenticación AAA anterior para implementar la autorización de comandos:

aaa authorization exec default group tacacs+ none

aaa authorization commands 0 default group tacacs+ none

aaa authorization commands 1 default group tacacs+ none

aaa authorization commands 15 default group tacacs+ none

Consulte Configuración de la Autorización para obtener más información sobre la autorización de comandos.

Contabilización de Comandos TACACS+

Cuando está configurada, la contabilización de comandos AAA envía información sobre cada comando EXEC que se ingresa a los servidores TACACS+ configurados. La información enviada al servidor de TACACS+ incluye el comando ejecutado, la fecha de ejecución y el usuario que introdujo el comando. Con RADIUS no se ofrece auditoría de comandos.

Este ejemplo de configuración habilita la contabilización de comandos AAA para los comandos EXEC ingresados en los niveles de privilegio cero, uno y 15. Esta configuración se basa en ejemplos anteriores que incluyen la configuración de los servidores TACACS.

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 0 default start-stop group tacacs+

aaa accounting commands 1 default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

Consulte Configuración de auditorías para ver más información sobre la configuración de las auditorías de AAA.

Servidores AAA Redundantes

Los servidores AAA que se aprovechan en un entorno pueden ser redundantes e implementarse de forma tolerante a fallos. Esto permite garantizar que el acceso de administración interactivo, como SSH, sea posible si un servidor AAA no está disponible.

Al designar o implementar una solución de servidor AAA redundante, recuerde lo siguiente:

1. disponibilidad de los servidores de AAA durante las posibles fallas de la red;
2. colocación geográficamente distribuida de los servidores de AAA;
3. Cargue en servidores AAA individuales de condiciones estables de falla y estado
4. latencia de red entre los servidores de acceso a la red y los servidores AAA;
5. sincronización de las bases de datos del servidor AAA.

Consulte Implementación de Servidores de Control de Acceso para obtener más información.

Fortalezca el protocolo simple de administración de redes

Esta sección resalta varios métodos que se pueden utilizar para asegurar la implementación de SNMP dentro de los dispositivos IOS-XE. Es fundamental fortalecer bien el SNMP, para proteger

la confidencialidad, la integridad, y la disponibilidad de los datos de redes y de los dispositivos de redes por donde pasan los datos. SNMP le brinda una gran cantidad de información sobre el estado de los dispositivos de red. Esta información se puede proteger de usuarios malintencionados que deseen aprovechar estos datos para realizar ataques contra la red.

Identificaciones de comunidad SNMP

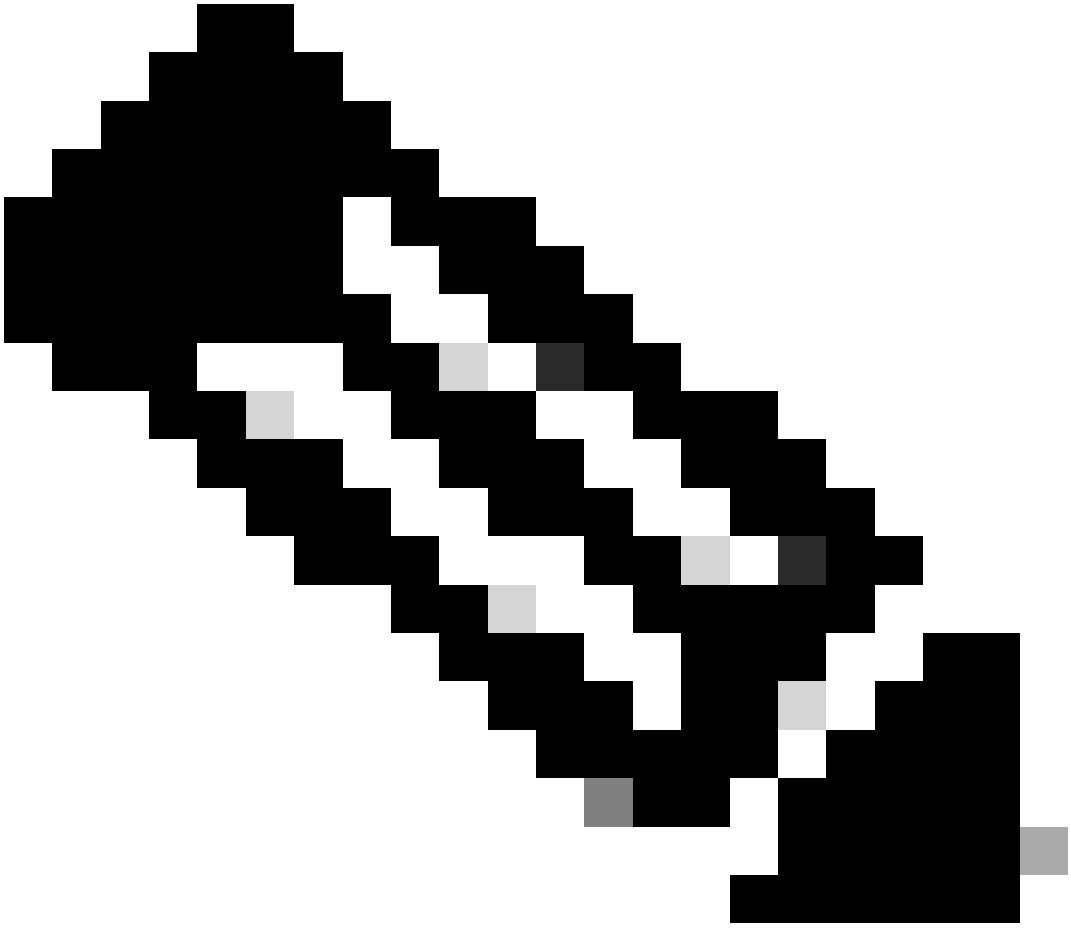
Las cadenas de comunidad son contraseñas que se aplican a un dispositivo IOS-XE para restringir el acceso, tanto de solo lectura como de lectura y escritura, a los datos SNMP del dispositivo. Estas cadenas de comunidad, como todas las contraseñas, se pueden elegir cuidadosamente para asegurarse de que no son triviales. Las cadenas de comunidad se pueden cambiar a intervalos regulares y de acuerdo con las políticas de seguridad de la red.

Por ejemplo, las cadenas se pueden cambiar cuando un administrador de red cambia de función o deja la empresa.

Estas líneas de configuración configuran una comunidad de solo lectura de READONLY y una cadena de comunidad de lectura y escritura de READWRITE:

snmp-server community READONLY RO

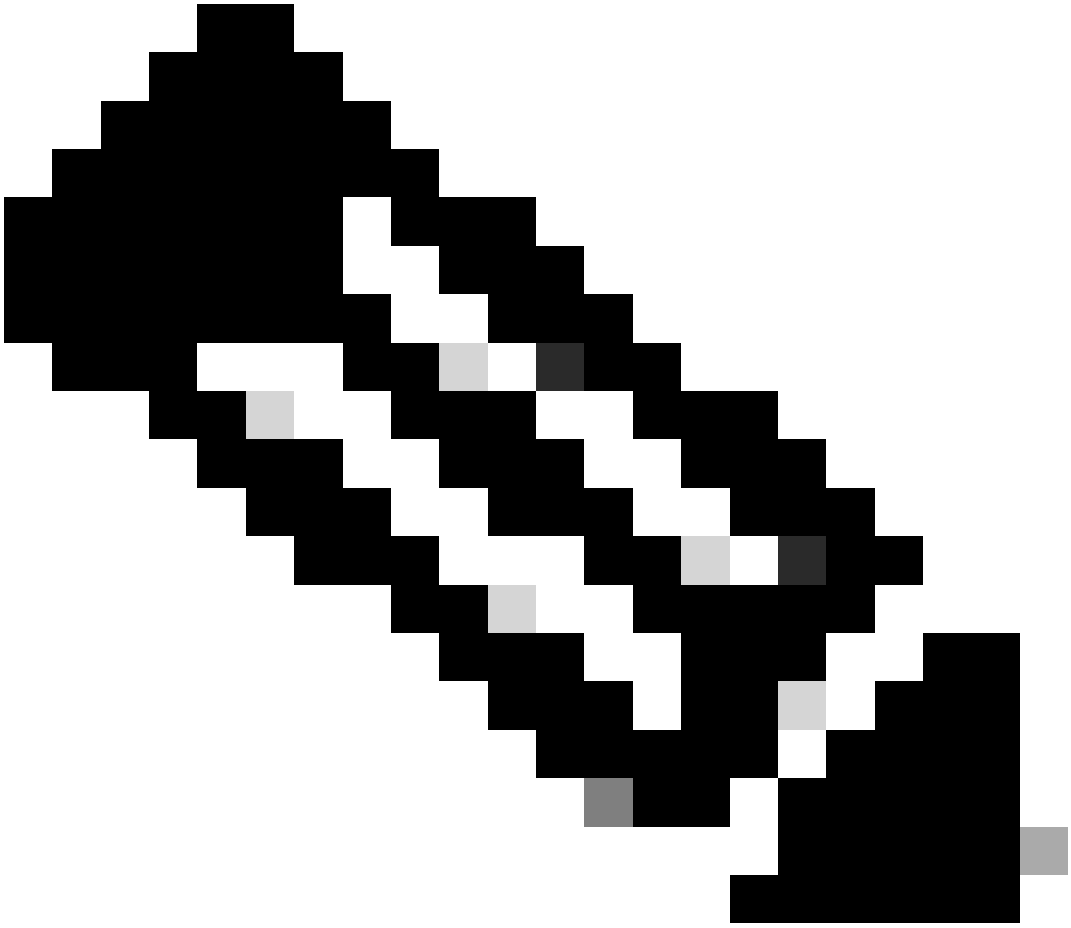
snmp-server community READWRITE RW



Nota: Los ejemplos de cadenas de comunidad anteriores se han elegido para explicar claramente el uso de estas cadenas. Para entornos de producción, las cadenas de comunidad se pueden elegir con precaución y pueden constar de una serie de símbolos alfabéticos, numéricos y no alfanuméricos. Consulte Recomendaciones para la Creación de Contraseñas Sólidas para obtener más información sobre la selección de contraseñas no triviales.

Comunidades SNMP con ACL

Además de la cadena de comunidad, se puede aplicar una ACL que restrinja aún más el acceso SNMP a un grupo seleccionado de direcciones IP de origen. Esta configuración restringe el acceso SNMP de sólo lectura a los dispositivos host finales que residen en el espacio de direcciones 192.168.100.0/24 y restringe el acceso SNMP de lectura y escritura sólo al dispositivo host final en 192.168.100.1.



Nota: Los dispositivos permitidos por estas ACL requieren la cadena de comunidad adecuada para acceder a la información SNMP solicitada.

---

access-list 98 permit 192.168.100.0 0.0.0.255

access-list 99 permit 192.168.100.1

snmp-server community READONLY RO 98

snmp-server community READWRITE RW 9

Consulte snmp-server community en la Referencia de Comandos de Administración de Redes de Cisco IOS XE para obtener más información sobre esta función.

ACL de Infraestructura

Las ACL de infraestructura (iACL) se pueden implementar para garantizar que solo los hosts finales con direcciones IP fiables puedan enviar tráfico SNMP a un dispositivo IOS-XE. Una iACL

puede contener una política que deniegue paquetes SNMP no autorizados en el puerto UDP 161.

Consulte la sección Limitar el Acceso a la Red con ACL de Infraestructura de este documento para obtener más información sobre el uso de iACL.

Vistas SNMP

Vistas SNMP son una función de seguridad que pueden permitir o negar el acceso a ciertas bases de información de administración (MIB) SNMP. Una vez que se crea una vista y se aplica a una cadena de comunidad con los comandos de configuración global snmp-server community community string view, si accede a los datos de MIB, se le restringen los permisos definidos por la vista. Se recomienda que, cuando sea apropiado, utilice vistas para limitar a los usuarios de SNMP a los datos que necesitan.

Este ejemplo de configuración restringe el acceso SNMP con la comunidad LIMITED a los datos de MIB situados en el grupo del sistema:

snmp-server view <view_name> <mib_view_family_name> [include/exclude]

snmp-server community <community_string>view <view_name> RO

Consulte Configuración de Soporte SNMP para obtener más información.

Versión 3 de SNMP

La versión 3 de SNMP (SNMPv3) se encuentra definida en RFC3410 , RFC3411 , RFC3412 , RFC3413 , RFC3414 y RFC3415 , además es un protocolo de interoperabilidad basado en estándares para la administración de red. SNMPv3 ofrece acceso seguro a dispositivos porque autentica y brinda la opción de encriptar paquetes en las redes. SNMPv3, cuando se admite, puede usarse para agregar otra capa de seguridad al implementar SNMP. SNMPv3 consiste en tres opciones de configuración primaria:

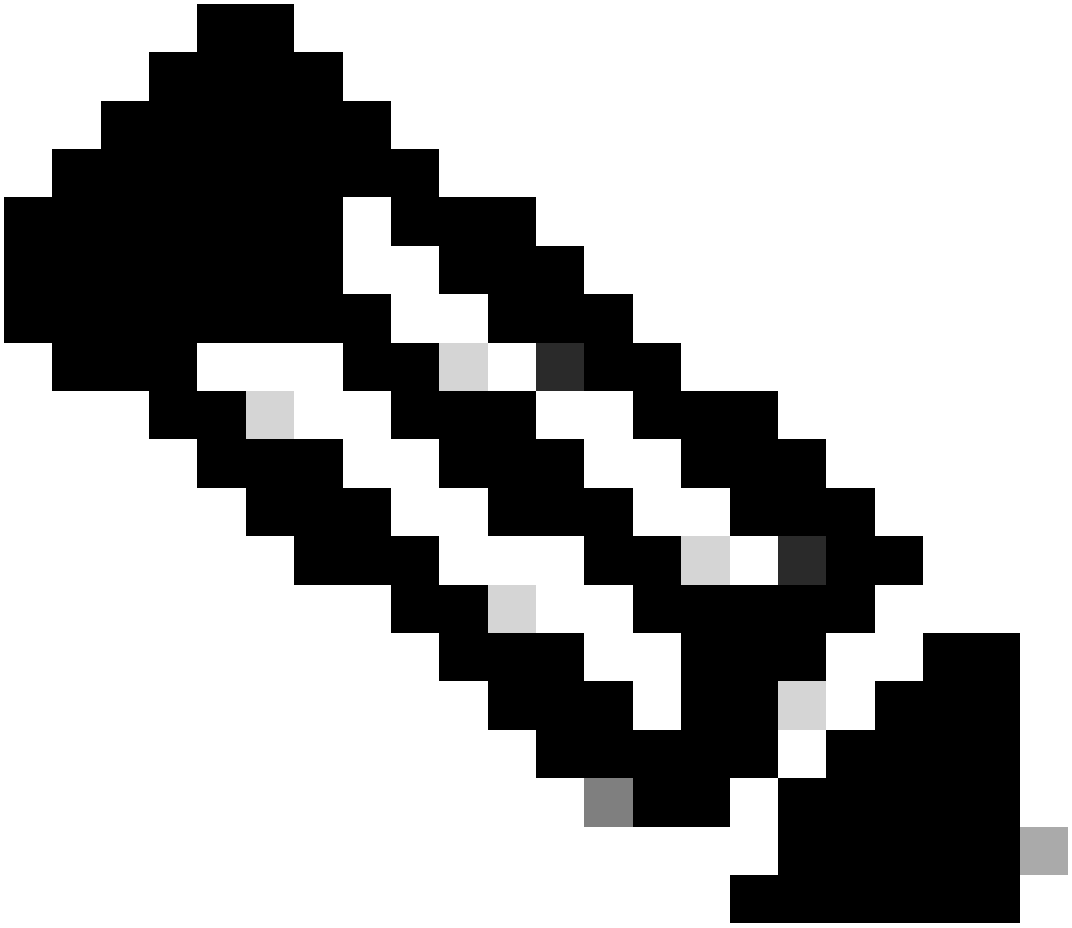
1. no auth - Este modo no requiere ninguna autenticación ni ningún cifrado de los paquetes SNMP.
2. auth - Este modo requiere autenticación del paquete SNMP sin encripción.
3. priv: Este modo requiere autenticación y cifrado (privacidad) de cada paquete SNMP.

   Debe existir un ID de motor autorizado para utilizar los mecanismos de seguridad SNMPv3 autenticación o autenticación y cifrado para manejar paquetes SNMP; de forma predeterminada, el ID de motor se genera localmente. El ID de motor se puede visualizar con el comando show snmp engineid tal y como se muestra en este ejemplo:

   router#show snmp engineID

ID del motor SNMP local: 800000090300000152BD35496

Puerto IP-addr de ID de motor remoto



Nota: Si se cambia el engineID, se deben reconfigurar todas las cuentas de usuario SNMP.

El siguiente paso es configurar un grupo SNMPv3. Este comando configura un dispositivo Cisco IOS XE para SNMPv3 con un grupo de servidores SNMP AUTHGROUP y habilita solamente la autenticación para este grupo con la palabra clave auth:

snmp-server group AUTHGROUP v3 auth

Este comando configura un dispositivo Cisco IOS XE para SNMPv3 con un grupo de servidores SNMP.

PRIVGROUP y habilita la autenticación y el cifrado para este grupo con la palabra clave priv:

snmp-server group PRIVGROUP v3 priv

Este comando configura a un usuario SNMPv3 snmpv3user con una contraseña de autenticación MD5 de authpassword y una contraseña de cifrado 3DES de privpassword:

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des privpassword

Tenga en cuenta que los comandos de configuración de usuario snmp-server no se muestran en la salida de configuración del dispositivo como lo requiere RFC 3414; por lo tanto, la contraseña de usuario no se puede ver en la configuración. Para ver los usuarios configurados, ingrese el comando show snmp user como se muestra en este ejemplo:

router#show snmp user

Nombre de usuario: snmpv3user ID del motor: 80000090300000152BD35496

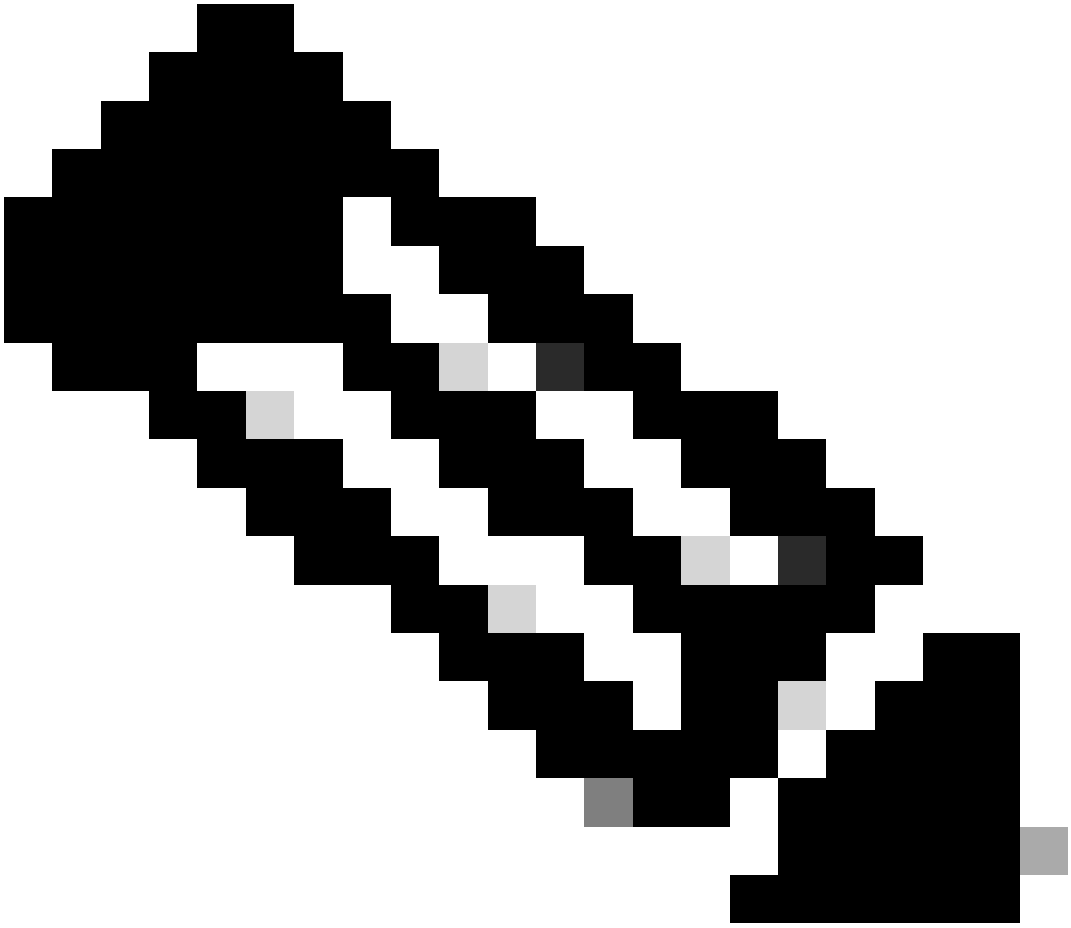
tipo de almacenamiento: activo no volátil

Protocolo de autenticación: MD5
Protocolo de privacidad: 3DES
Group-name: PRIVGROUP

Consulte Configuración de Soporte SNMP para obtener más información sobre esta función.

Management Plane Protection

La función Management Plane Protection (MPP) del software Cisco IOS XE se puede utilizar para ayudar a proteger SNMP porque restringe las interfaces a través de las cuales el tráfico SNMP puede terminar en el dispositivo. La función MPP permite que un administrador designe una o más interfaces como interfaces de administración. El tráfico de administración puede ingresar a un dispositivo solamente a través de estas interfaces de administración. Después de que se habilita la función MPP, ninguna interfaz, salvo las interfaces de administración designadas, acepta el tráfico de administración de red que se dirige al dispositivo.



Nota: MPP es un subconjunto de la función CPPr y requiere una versión de IOS que admita CPPr. Consulte Comprensión de Control Plane Protection para obtener más información sobre la función CPPr.

En este ejemplo, MPP se utiliza para restringir el acceso SNMP y SSH a solamente la interfaz FastEthernet0/0:

host del plano de control

management-interface FastEthernet0/0 allow ssh snmp

Consulte Guía para la Función Management Plane Protection para obtener más información.

Prácticas Recomendadas de Registro

El registro de eventos le proporciona visibilidad del funcionamiento de un dispositivo Cisco IOS XE y de la red en la que está implementado. El software Cisco IOS XE ofrece varias opciones de

registro flexibles que pueden ayudar a alcanzar los objetivos de visibilidad y gestión de la red de una organización.

Estas secciones proporcionan algunas prácticas recomendadas de registro básicas que pueden ayudar a un administrador a aprovechar el registro correctamente y minimizar el impacto del registro en un dispositivo Cisco IOS XE.

Envío de Registros a una Ubicación Central

Le aconsejamos que envíe la información de registro a un servidor syslog remoto. Esto hace posible correlacionar y auditar con más eficiencia los eventos de seguridad y redes en los dispositivos de redes. Tenga en cuenta que los mensajes de syslog son transmitidos de manera no confiable por UDP y en texto sin formato. Por esta razón, cualquier protección que una red ofrezca al tráfico de administración (por ejemplo, cifrado o acceso fuera de banda) se puede ampliar para incluir el tráfico syslog.

Este ejemplo de configuración configura un dispositivo Cisco IOS XE para enviar información de registro a un servidor syslog remoto:

logging host <ip-address>

Consulte Identificación de Incidentes Usando Firewall y Eventos Syslog del Router IOS-XE para obtener más información sobre la correlación de registros.

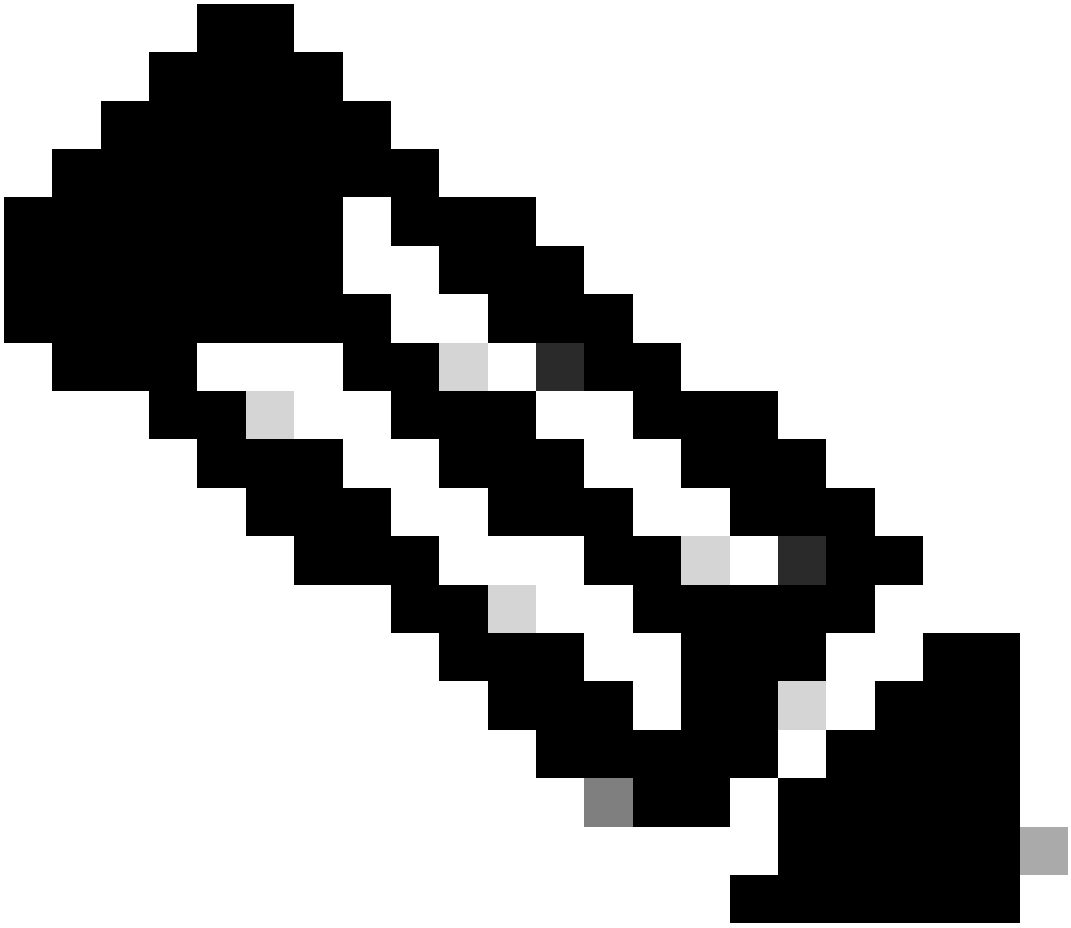
La función Logging to Local Nonvolatile Storage (ATA Disk) permite guardar los mensajes de registro del sistema en un disco flash ATA (Advanced Technology Attachment). Los mensajes guardados en una unidad ATA persisten después de que se reinicie un router.

Estas líneas de configuración configuran 134.217.728 bytes (128 MB) de mensajes de registro en el directorio syslog de la memoria flash ATA (disk0) y especifican un tamaño de archivo de 16.384 bytes:

logging buffered.

logging persistent url disk0:/syslog size 134217728 filesize 16384

Antes de que los mensajes de registro se escriban en un archivo del disco ATA, el software Cisco IOS XE comprueba si hay suficiente espacio en disco. Si no hay espacio suficiente, se elimina el archivo de los mensajes de registro más viejo (por fechado) y se guarda el archivo actual. El formato del nombre de archivo es log_month:day:year::time.



Nota: Una unidad flash ATA tiene un espacio en disco limitado y, por lo tanto, debe mantenerse para evitar un exceso de datos almacenados.

En este ejemplo se ve cómo copiar mensajes de registros de un disco flash ATA de router en un disco externo del servidor FTP 192.168.1.129 como parte del mantenimiento:

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

Refiérase a Registro en Almacenamiento No Volátil Local para obtener más información sobre esta función.

Nivel de Registro

A cada mensaje de registro generado por un dispositivo Cisco IOS XE se le asigna una de las ocho severidades que van desde el nivel 0, Emergencias, hasta el nivel 7, Depuración. A menos que se requiera específicamente, se recomienda evitar el registro en el nivel 7. El registro en el nivel 7 produce una carga de CPU elevada en el dispositivo que puede provocar inestabilidad en

el dispositivo y en la red.

El comando de configuración global logging trap level se emplea para especificar qué mensajes de registros enviar a los servidores syslog remotos. El nivel especificado indica el mensaje de nivel más bajo de gravedad que se envía. Para los registros almacenados en buffer, se utiliza el comando logging buffered level.

Este ejemplo de configuración limita los mensajes de registro que se envían a los servidores syslog remotos y al buffer de registro local a los niveles de gravedad del 6 (informativo) al 0 (emergencias):

logging trap 6

logging buffered 6

Inhabilitación de Registro en la Consola o en las Sesiones de Monitoreo

Con el software Cisco IOS XE, es posible enviar mensajes de registro a las sesiones de monitoreo -las sesiones de monitoreo son sesiones de administración interactivas en las que se ha emitido el comando EXEC terminal monitor- y a la consola. Sin embargo, esto puede elevar la carga de CPU de un dispositivo IOS-XE y, por lo tanto, no se recomienda. En cambio, se recomienda enviar la información de registros al búfer de registros local, que puede consultarse con el comando show logging.

Utilice los comandos de configuración global no logging console y no logging monitor para desactivar los registros en la consola y en las sesiones de monitoreo. Este ejemplo de configuración muestra el uso de estos comandos:

no logging console

no logging monitor

Consulte Referencia de Comandos de Administración de Redes de Cisco IOS XE para obtener más información sobre los comandos de configuración global.

Uso de Registros Almacenados en Buffer

El software Cisco IOS XE admite el uso de un búfer de registro local para que un administrador pueda ver los mensajes de registro generados localmente. El uso de registros almacenados en buffer es mucho más recomendado que el registro en la consola o en las sesiones de monitoreo.

Hay dos opciones de configuración que son relevantes al configurar el registro almacenado en buffer: el tamaño del buffer de registro y la gravedad del mensaje que se almacena en el buffer. El tamaño del buffer de registro se configura con el comando de configuración global logging buffered para el tamaño. La gravedad más baja incluida en el búfer se configura mediante el comando logging buffered severity. Un administrador puede ver el contenido del buffer de registro a través del comando EXEC show logging.

En este ejemplo se incluye la configuración de un búfer de registros de 16 384 bytes y una

gravedad de 6 (información), lo cual indica que se almacenan los mensajes que van del nivel 0 (emergencias) al 6 (información):

logging buffered 16384 6

Refiérase a Configuración de Cisco IOS XE para el Dispositivo de Destino de Visualización de Mensajes para obtener más información sobre el registro almacenado en buffer.

Configuración de la Interfaz de Origen de Registro

Para ofrecer un nivel superior de uniformidad al recopilar y consultar mensajes de registros, se recomienda configurar de manera estática una interfaz de fuentes de registros.

Con el comando logging source-interface interface, la configuración estática de una interfaz de origen de registro garantiza que la misma dirección IP aparezca en todos los mensajes de registro que se envían desde un dispositivo Cisco IOS individual. Para una mayor estabilidad, se le aconseja utilizar una interfaz Loopback como origen de registro.

En este ejemplo de configuración se ve el uso del comando de configuración global de interfaces logging source-interface para especificar que la dirección IP de la interfaz de loopback 0 se use con todos los mensajes de registros:

logging source-interface Loopback 0

Consulte Administrador de Syslog Integrado de Cisco IOS XE para obtener más información.

Configuración de Fechados de Registro

La configuración de fechados de registro lo ayuda a correlacionar los eventos en los dispositivos de red. Es importante implementar una configuración correcta y constante de los fechados de registro para asegurarse de que pueda correlacionar los datos de registro. Las marcas de tiempo de registro se pueden configurar para incluir la fecha y la hora con precisión de milisegundos, así como la zona horaria que se utiliza en el dispositivo.

Este ejemplo incluye la configuración de fechados de registro con la precisión de milisegundos dentro de la zona Tiempo Universal Coordinado (UTC):

service timestamps log datetime msec show-timezone

Si usted prefiere usar un estándar diferente al UTC para registrar la hora, usted puede configurar un huso horario local específico y configurar esa información para que esté presente en los mensajes de registro generados. Este ejemplo muestra la configuración de un dispositivo para la zona Tiempo Estándar del Pacífico (PST):

clock timezone PST -8

service timestamps log datetime msec localtime show-timezone

Gestión de la configuración del software Cisco IOS XE

El software Cisco IOS XE incluye varias funciones que pueden habilitar una forma de administración de la configuración en un dispositivo Cisco IOS XE. Estas funciones permiten archivar configuraciones, restaurar una configuración de modo que regrese a una versión anterior y crear un registro detallado de cambios en la configuración.

Configuration Replace y Configuration Rollback

En la versión 16.6.4 y posteriores del software Cisco IOS XE, las funciones Configuration Replace y Configuration Rollback permiten archivar la configuración del dispositivo Cisco IOS XE en el dispositivo. Las configuraciones archivadas, de forma manual o automática, se pueden usar para reemplazar la configuración en ejecución mediante el comando configure replace nombredearchivo. Este comando se opone al comando copy nombre de archivounning-config. El comando configure replace nombre de archivo reemplaza la configuración actual en comparación con la fusión realizada por el comando copy.

Se recomienda activar esta función en todos los dispositivos Cisco IOS XE de la red. Una vez hecho el reemplazo, el administrador puede archivar la configuración en ejecución mediante el comando EXEC con privilegios archive config. Las configuraciones archivadas se pueden ver mediante el comando EXEC show archive.

Este ejemplo ilustra la configuración de archivado automático de la configuración. También le indica al dispositivo Cisco IOS XE que almacene las configuraciones archivadas como archivos denominados archive-config-N en el sistema de archivos disk0:, que mantenga un máximo de 14 copias de seguridad y que archive una vez al día (1440 minutos) y cuando un administrador ejecute el comando EXEC write memory.

archivar

path disk0:archive-config

máximo 14

time-period 1440

Si bien en el archivo se admiten hasta 14 configuraciones de respaldo, se recomienda tener en cuenta el espacio necesario antes de emplear el comando maximum.

Función Exclusive Configuration Change Access

Añadida a la versión 16.6.4 del software Cisco IOS XE, la función Exclusive Configuration Change Access garantiza que solo un administrador realice cambios de configuración en un dispositivo Cisco IOS XE en un momento dado. Esta función ayuda a eliminar el impacto no deseable de cambios simultáneos realizados a componentes de la configuración relacionados. Esta función se configura con el comando de configuración global configuration mode exclusive y opera en uno de los dos modos: automático y manual. En el modo automático, la configuración se bloquea

automáticamente cuando un administrador ejecuta el comando EXEC configure terminal. En el modo manual, el administrador utiliza el comando configure terminal lock para bloquear la configuración al pasar al modo de configuración.

Este ejemplo ilustra la configuración de esta función para el bloqueo automático de la configuración:

configuration mode exclusive

Digitally Signed Cisco Software

Añadida en Cisco IOS XE Software Release 16.1 y versiones posteriores, la función Digitally Signed Cisco Software facilita el uso de Cisco IOS XE Software que está firmado digitalmente y, por lo tanto, es de confianza, con el uso de criptografía asimétrica segura (clave pública).

Una imagen con firma digital tiene un hash cifrado (con una clave privada). El dispositivo desencripta el hash con la clave pública correspondiente a partir de las claves que tiene almacenadas y también calcula su propio hash de la imagen. Si el hash descifrado coincide con el hash calculado de la imagen, la imagen no se ha alterado y es confiable.

Los claves de Digitally Signed Cisco Software son identificadas por tipo y versión. Los tipos de clave puede ser especial, producción o renovación. Los tipos producción y especial tienen una versión de la clave asociada que aumenta alfabéticamente cada vez que la clave se revoca o reemplaza. Tanto las imágenes ROMMON como las imágenes normales de Cisco IOS XE están firmadas con una clave especial o de producción cuando se utiliza la función Digitally Signed Cisco Software. La imagen de ROMMON se puede actualizar y debe firmarse con la misma clave que la imagen de producción especial cargada.

Este comando verifica la integridad de la imagen isr4300-universalk9.16.06.04.SPA.bin en flash con las claves en el almacén de claves del dispositivo:

show software authenticity file bootflash:isr4300-universalk9.16.06.04.SPA.bin

Consulte Digitally Signed Cisco Software para obtener más información sobre esta función.

Una nueva imagen (isr4300-universalk9.16.10.03.SPA.bin) se puede copiar a la memoria flash para cargarla y la firma de la imagen se verifica con la clave especial recién agregada

copy /verify tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin flash:

Configuration Change Notification and Logging

La función Configuration Change Notification and Logging, agregada en la versión 16.6.4 del software Cisco IOS XE, permite registrar los cambios de configuración realizados en un dispositivo Cisco IOS XE. El registro se mantiene en el dispositivo Cisco IOS XE y contiene la información del usuario de la persona que realizó el cambio, el comando de configuración ingresado y la hora en que se realizó el cambio. Esta función se activa mediante el comando de modo de configuración de registro logging enable configuration change. Los comandos opcionales

hide keys y logging size entries se utilizan para mejorar la configuración predeterminada, ya que impiden el registro de datos de contraseña y aumentan la longitud del registro de cambios.

Se recomienda que habilite esta funcionalidad para que el historial de cambios de configuración de un dispositivo Cisco IOS XE se pueda entender más fácilmente. Además, se recomienda utilizar el comando notify syslog configuration para activar la generación de mensajes de syslog al hacer cambios de configuración.

archivar

log config

logging enable

logging size 200

teclas ocultas

notify syslog

Una vez habilitada la función Configuration Change Notification and Logging, se puede utilizar el comando EXEC privilegiado show archive log config all para ver el registro de la configuración.

Plano de Control

Las funciones del plano de control constan de protocolos y procesos que comunican a los dispositivos de redes a fin de trasladar los datos de origen a destino. Esto incluye protocolos de ruteo, como Border Gateway Protocol, y otro protocolos como ICMP y Resource Reservation Protocol (RSVP).

Es importante que los eventos en los planos de datos y de administración no afecten negativamente al plano de control. Cuando un evento del plano de datos, como un ataque de DoS, afecta al plano de control, toda la red puede volverse inestable. Esta información sobre las funciones y configuraciones del software Cisco IOS XE puede ayudar a garantizar la resistencia del plano de control.

Consolidación del Plano de Control General

Es fundamental proteger el plano de control de un dispositivo de red porque este plano garantiza el mantenimiento y el funcionamiento de los planos de administración y de datos. Si el plano control llegara a ser inestable durante un incidente de seguridad, puede ser imposible que usted recupere la estabilidad de la red.

En muchos casos, se puede desactivar la recepción y la transmisión de determinados tipos de mensajes en interfaces, a fin de reducir la carga de CPU necesaria para procesar los paquetes innecesarios.

Mensajes de Redirección ICMP IP

Un mensaje de redirección ICMP puede ser generado por un router cuando un paquete se recibe y se transmite en la misma interfaz. En esta situación, el router reenvía el paquete y envía un mensaje de redirección ICMP al remitente del paquete original. Este comportamiento le permite al remitente saltear el router y reenviar los futuros paquetes directamente al destino (o a un router más cercano al destino). En una red IP que funciona sin inconvenientes, un router envía mensajes de redirección solamente a hosts en sus propias subredes locales. En otras palabras, las redirecciones ICMP nunca pueden ir más allá de un límite de Capa 3.

Existen dos tipos de mensajes de redirección ICMP: redirección para una dirección de host y redirección para una subred completa. Usuarios maliciosos podrían explotar la capacidad del router de enviar redireccionamientos de ICMP enviando paquetes al router de forma continua, lo cual obligaría al router a responder con mensajes de redireccionamiento de ICMP, y tendría un impacto adverso sobre la CPU y el rendimiento del router. Para evitar que el router envíe mensajes de redirección ICMP, utilice el comando de configuración de interfaz no ip redirects.

Mensajes ICMP de Destino Inalcanzable

El filtrado con una lista de acceso a la interfaz genera la transmisión de mensajes ICMP de destino inalcanzable al origen del tráfico filtrado. La generación de estos mensajes puede incrementar la utilización de la CPU en los dispositivos. En el software Cisco IOS XE, la generación de ICMP inalcanzable está limitada a un paquete cada 500 milisegundos de forma predeterminada. La generación de mensajes de ICMP inalcanzable puede desactivarse mediante el comando de configuración de interfaz no ip unreachables. El límite predeterminado de ICMP inalcanzables se puede modificar con el comando de configuración global ip icmp rate-limit unreachable interval-in-ms.

Proxy ARP

Proxy ARP es la técnica mediante la cual un dispositivo, generalmente un router, responde solicitudes del protocolo ARP dirigidas a otro dispositivo. Al falsificar su identidad, el router acepta la responsabilidad de rutear paquetes al destino real. Proxy ARP puede ayudar a las máquinas en una subred a alcanzar subredes remotas sin configurar el ruteo o un gateway predeterminado. El ARP proxy se define en el RFC 1027.

El uso de ARP de proxy tiene muchas desventajas. Puede generar un incremento del tráfico de ARP en el segmento de red, agotar los recursos y permitir ataques de intermediarios. Proxy ARP presenta un vector de ataque de agotamiento de recursos porque cada solicitud a la que se aplicó la técnica Proxy ARP consume un poco de memoria. Un atacante puede agotar la memoria disponible si envía una gran cantidad de solicitudes de ARP.

Estos ataques permiten que un host de la red falsifique la dirección MAC del router y entonces hosts no advertidos de esto le envíen tráfico al atacante. El ARP de proxy se puede desactivar mediante el comando de configuración de interfaz no ip proxy-arp.

Consulte Habilitación e Inhabilitación de Proxy ARP para obtener más información sobre esta función.

Mensajes de control NTP

Las consultas de mensajes de control NTP son una función de NTP que ayudó en las funciones de administración de red (NM) antes de que se crearan y utilizaran mejores NM. A menos que su organización siga utilizando NTP para las funciones de NM, las prácticas recomendadas de seguridad de la red son desactivarlas completamente juntas. Si los está utilizando, puede tratarse de un servicio del tipo solo red interna que está bloqueado por un firewall u otro dispositivo externo. Incluso se han eliminado de todas las versiones de IOS e IOS-XE excepto las estándar, ya que IOS-XR y NX-OS no las admiten.

Si decide desactivar esta función, el comando es

```
Router (config)# no ntp allow mode control
```

Este comando luego se muestra en running-config como no ntp allow mode control 0. Al hacer esto, ha deshabilitado los mensajes de control NTP en el dispositivo y protege el dispositivo de ataques.

Limite el impacto del tráfico del plano de control sobre la CPU

La protección del plano de control es crucial. Puesto que el rendimiento de la aplicación y la experiencia del usuario final pueden sufrir sin la presencia de tráfico de administración y de datos, la supervivencia del plano de control garantiza el mantenimiento y el funcionamiento de los otros dos planos.

Comprenda el tráfico del plano de control

Para proteger correctamente el plano de control del dispositivo Cisco IOS XE, es esencial comprender los tipos de tráfico que conmuta el proceso la CPU. Normalmente, el tráfico que se conmuta en el procesador puede ser de dos tipos diferentes. El primer tipo de tráfico se dirige al dispositivo Cisco IOS XE y debe ser manejado directamente por la CPU del dispositivo Cisco IOS XE. Este tráfico consiste en la categoría de tráfico de adyacencia de recepción. Este tráfico contiene una entrada en la tabla Cisco Express Forwarding (CEF), por la cual el siguiente salto de router es el propio dispositivo, lo cual se indica mediante el término "receive (recepción)" en la salida de CLI para show ip cef. Esta indicación se aplica a cualquier dirección IP que requiera una gestión directa por parte de la CPU del dispositivo Cisco IOS XE, que incluye direcciones IP de interfaz, espacio de direcciones de multidifusión y espacio de direcciones de difusión.

El segundo tipo de tráfico que maneja la CPU es el tráfico del plano de datos (tráfico con un destino más allá del propio dispositivo Cisco IOS XE) que requiere un procesamiento especial de la CPU. Aunque no se trata de una lista exhaustiva de CPU que afecta al tráfico del plano de datos, estos tipos de tráfico son conmutados por proceso y, por lo tanto, pueden afectar al funcionamiento del plano de control:

1. Registro de listas de control de acceso: El tráfico de registro de ACL consiste en los paquetes generados por coincidencias (permiso o denegación) de ACE donde se emplea la palabra clave log.

2. Reenvío de rutas inversas unicast (RPF unicast): Se emplea en combinación con una ACL y puede generar switching mediante proceso de determinados paquetes.
3. Opciones de IP: La CPU debe procesar todos los paquetes de IP que incluyan opciones.
4. Fragmentación: La CPU debe recibir y procesar todos los paquetes de IP que exijan fragmentación.
5. Tiempo de vida (TTL) agotado: Los paquetes con un valor de TTL inferior o igual a uno exigen el envío del mensaje Internet Control Message Protocol Time Exceeded (ICMP Type 11, Code 0) (Se agotó el tiempo del protocolo de mensajería de control de Internet, Tipo de ICMP 11, Código 0), lo cual genera el procesamiento por parte de la CPU.
6. ICMP inalcanzables: La CPU procesa los paquetes que resultan en mensajes de ICMP inalcanzable por routing, MTU o filtrado.
7. Tráfico que requiere una solicitud de ARP: La CPU debe procesar los destinos para los cuales no existe ninguna entrada de ARP.
8. Tráfico que no es de IP: La CPU procesa todo el tráfico que no es de IP.

   Esta lista detalla varios métodos para determinar qué tipos de tráfico son procesados por la CPU del dispositivo Cisco IOS XE:
9. El comando show ip cef brinda información sobre el siguiente salto para cada prefijo IP incluido en la tabla CEF. Como se indicó anteriormente, las entradas que contienen receive como salto siguiente se consideran adyacencias de recepción e indican que el tráfico debe enviarse directamente a la CPU.
10. El comando show interface switching brinda información sobre la cantidad de paquetes para la que el dispositivo hace switching por proceso.
11. El comando show ip traffic proporciona información sobre el número de paquetes IP: con un destino local (es decir, recibir tráfico de adyacencia) con opciones que requieren fragmentación que se envían al espacio de direcciones de difusión que se envían al espacio de direcciones de multidifusión.
12. El tráfico del tipo receive adjacency puede ser identificado con el uso del comando show ip cache flow. Cualquier flujo destinado al dispositivo Cisco IOS XE tiene una interfaz de destino (DstIf) de local.
13. Control Plane Policing se puede utilizar para identificar el tipo y la velocidad del tráfico que alcanza el plano de control del dispositivo Cisco IOS XE. Esta función se puede realizar con el uso de ACL de clasificación detalladas, de registro y del comando show policy-map control-plane .

ACL de Infraestructura

Las ACL de infraestructura (iACLs) limitan la comunicación externa con los dispositivos de la red.

Las ACL de infraestructura se tratan en detalle en la sección Acceso limitado a la red mediante ACL de infraestructura de este documento.

Se recomienda implementar iACL para proteger el plano de control de todos los dispositivos de redes.

ACL de recepción

Una rACL protege el dispositivo contra el tráfico dañino antes de que este afecte al procesador de ruta. Las ACL de recepción han sido diseñadas para solamente proteger el dispositivo en el cual se configuran; rACL no afectan el tráfico de tránsito. Como resultado, la dirección IP de destino cualquiera que se utilice en las entradas ACL de ejemplo sólo hace referencia a las direcciones IP físicas o virtuales del router. Las ACL de recepción también se consideran una práctica recomendada de seguridad de la red y pueden considerarse como una adición a largo plazo a una buena seguridad de la red.

Esta es la ACL de trayectoria de recepción que se escribe para permitir el tráfico SSH (TCP puerto 22) de hosts confiables en la red 192.168.100.0/24:

— Permitir SSH desde hosts de confianza permitidos al dispositivo.

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 2

— Denegar SSH de todas las otras fuentes al RP.

access-list 151 deny tcp any any eq 22

— permitir el resto del tráfico al dispositivo.

— según la política de seguridad y las configuraciones.

access-list 151 permit ip any any

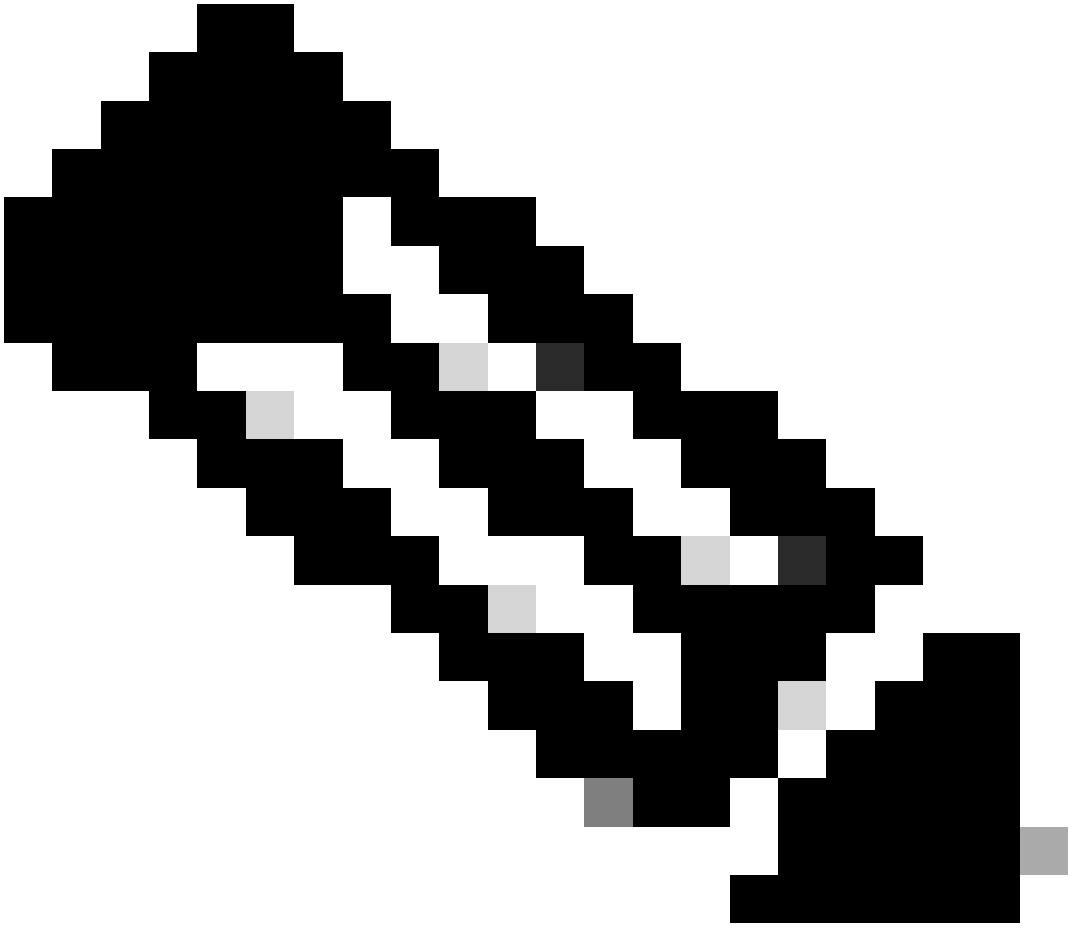
— aplique esta lista de acceso a la ruta de recepción.

ip receive access-list 151

Consulte Listas de Control de Acceso para ayudar a identificar y permitir el tráfico legítimo a un dispositivo y negar todos los paquetes no deseados.

CoPP

La función CoPP también puede usarse para restringir los paquetes de IP destinados a dispositivos de infraestructuras. En este ejemplo, sólo se permite que el tráfico SSH de hosts confiables llegue a la CPU del dispositivo Cisco IOS XE.



Nota: si se descarta el tráfico de direcciones IP desconocidas o no fiables, se puede evitar que los hosts con direcciones IP asignadas dinámicamente se conecten al dispositivo Cisco IOS XE.

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22

access-list 152 permit tcp any any eq 22

access-list 152 deny ip any

class-map match-all COPP-KNOWN-UNDESIRABLE match access-group 152

policy-map COPP-INPUT-POLICY class COPP-KNOWN-UNDESIRABLE drop

control-plane service-policy input COPP-INPUT-POLICY

En el ejemplo anterior de CoPP, en las entradas de ACL, los paquetes no autorizados que coincidían con la acción de permitir se desechaban mediante la función de rechazo de mapa de

políticas, mientras que los paquetes que coincidían con la acción de rechazar no se veían afectados por dicha función.

CoPP está disponible en la versión de software Cisco IOS XE.

Consulte Control Plane Policing para obtener más información sobre la configuración y el uso de la función CoPP.

Función Control Plane Protection

La protección del plano de control (CPPr), introducida en la versión 16.6.4 del software Cisco IOS XE, se puede utilizar para restringir o controlar el tráfico del plano de control que se dirige a la CPU del dispositivo Cisco IOS XE. Si bien es similar a la función CoPP, CPPr tiene la capacidad de restringir el tráfico de granularidad más fina. CPPr divide el plano de control general en tres categorías independientes, conocidas como subinterfaces. Las subinterfaces existen para las categorías de tráfico Host, Transit y CEF-Exception. Además, CPPr incluye estas funciones de protección del plano de control:

1. Filtrado de puertos: Esta función permite controlar y rechazar paquetes enviados a puertos UDP o TCP cerrados o sin escucha.
2. Umbral de colas: Esta función limita la cantidad de paquetes de un protocolo especificado admitida en la cola de entrada de IP del plano de control.

   Consulte Control Plane Protection y Comprensión de Control Plane Protection (CPPr) para obtener más información sobre la configuración y el uso de la función CPPr.

Limitadores de Velocidad Basados en Hardware

Las Supervisor Engine 32 y Supervisor Engine 720 de Cisco Catalyst 6500 Series admiten limitadores de velocidad basados en hardware (HWRL) específicos de cada plataforma para ciertos escenarios de networking especiales. Estos limitadores de la velocidad del hardware son conocidos como limitadores de velocidad para casos especiales porque abarcan un conjunto predefinido específico de escenarios de negación de servicio de IPv4, IPv6, unicast y multicast. Los HWRL pueden proteger el dispositivo Cisco IOS XE de una variedad de ataques que requieren que la CPU procese los paquetes.

Proteja el protocolo BGP

El protocolo Border Gateway Protocol (BGP) es la base de ruteo de Internet. Las organizaciones con requisitos no modestos de conectividad suelen emplear BGP. Los atacantes suelen apuntar al protocolo BGP por su ubicuidad y porque las organizaciones más pequeñas definen y olvidan las configuraciones de BGP. Sin embargo, hay muchas funciones de seguridad específicas de BGP que se pueden aprovechar para aumentar la seguridad de una configuración BGP.

Aquí se describen en términos generales funciones de seguridad más importantes de BGP. Según corresponda, se hacen recomendaciones para la configuración.

Protecciones de Seguridad Basadas en TTL

Cada paquete IP contiene un campo de 1 byte conocido como Tiempo de Vida (TTL). Cada dispositivo que un paquete del IP cruza reduce este valor en uno. El valor de inicio varía de acuerdo con el sistema operativo y normalmente va de 64 a 255. Un paquete se descarta cuando su valor TTL alcanza cero.

Existe una protección de seguridad TTL denominada Generalized TTL-based Security Mechanism (GTSM) o BGP TTL Security Hack (BTSH), que emplea el valor de TTL de los paquetes de IP para garantizar que los paquetes de BGP recibidos provengan de pares conectados directamente. Esta función a menudo requiere coordinación de los routers de peering; sin embargo, una vez habilitada, puede derrotar completamente muchos ataques basados en TCP contra BGP.

GTSM para BGP se activa mediante la opción ttl-security para el comando de configuración de router BGP neighbor. Este ejemplo ilustra la configuración de esta función:

router bgp <asn>

neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> ttl-security hops <hop-count>

A medida que se reciben paquetes BGP, se verifica el valor TTL y este debe ser mayor o igual 255 menos el hop-count especificado.

Autenticación de Peer BGP con MD5

La autenticación de pares con MD5 genera un resumen de MD5 para cada paquete enviado en sesiones de BGP. Específicamente, para generar el resumen, se utilizan partes de encabezados de IP y TCP, contenido TCP y una clave secreta.

El resumen creado se guarda en la opción Kind 19 de TCP, creada específicamente para este fin por RFC 2385. El speaker de BGP que recibe emplea el mismo algoritmo y la misma clave secreta para regenerar el resumen de mensajes. Si los resúmenes recibidos y computados no son idénticos, se descarta el paquete

La autenticación de pares con MD5 se configura mediante la opción password para el comando de configuración de router BGP neighbor. El uso de este comando se ilustra a continuación:

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> password <secret>

Consulte Autenticación de Router Vecino para obtener más información sobre la autenticación de peer BGP con MD5.

Configure el máximo de prefijos

Los prefijos BGP son guardados por un router en la memoria. Cuanto más prefijos debe guardar

un router, más memoria debe consumir el protocolo BGP. En algunas configuraciones, se puede almacenar un subconjunto de todos los prefijos de Internet, por ejemplo, en configuraciones que aprovechan sólo una ruta o rutas predeterminadas para las redes de usuario de un proveedor.

Para prevenir el agotamiento de la memoria, es importante configurar el número máximo de prefijos que acepta cada peer. Se recomienda que se configure un límite para cada peer BGP.

Cuando configura esta función con el comando de configuración de router BGP neighbor maximum-prefix, se requiere un argumento: el número máximo de prefijos que se aceptan antes de que se apague un par. Opcionalmente, se puede ingresar un número del 1 al 100. Este número representa el porcentaje del valor de prefijos máximo en el cual se envía un mensaje de registro.

router bgp <asn> neighbor <ip-address> remote-as <remote-asn>

neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>

Consulte Configuración de la Función de Número Máximo de Prefijos BGP para obtener más información sobre los prefijos máximos por peer.

Filtre los prefijos de BGP mediante listas de prefijos

Las listas de prefijos le permiten a un administrador de red aceptar o negar prefijos específicos que se envían o se reciben a través de BGP. Las listas de prefijos se pueden utilizar siempre que sea posible para garantizar que el tráfico de red se envíe por las rutas deseadas. Las listas de prefijos se pueden aplicar a cada par eBGP en las direcciones entrante y saliente.

Las listas de prefijos configuradas limitan los prefijos que se envían o se reciben a los permitidos específicamente por la política de ruteo de una red. Si esto no es factible debido al gran número de prefijos recibidos, se puede configurar una lista de prefijos para bloquear específicamente los prefijos malos conocidos. Estos prefijos malos conocidos incluyen redes y espacio de dirección IP sin asignar que RFC 3330 reserva para fines internos o de evaluación. Las listas de prefijos salientes se pueden configurar para permitir específicamente sólo los prefijos que una organización pretende anunciar.

Este ejemplo de configuración utiliza listas de prefijos para limitar las rutas que se aprenden y publican. Específicamente, la lista de prefijos BGP-PL-INBOUND permite el ingreso de solamente una ruta predeterminada, y el prefijo 192.168.2.0/24 es la única ruta permitida para ser publicada por BGP-PL-OUTBOUND.

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0

ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24

router bgp <asn>

neighbor <ip-address> prefix-list BGP-PL-INBOUND in

neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out

Consulte Filtrado de Rutas Salientes Basado en Prefijos para obtener una cobertura completa del filtrado de prefijos BGP.

Filtre los prefijos de BGP mediante listas de acceso a la ruta del sistema autónomo

Las listas de acceso de trayectoria del sistema autónomo BGP permiten que el usuario filtre los prefijos recibidos y publicados sobre la base del atributo AS-path de un prefijo. Esto se puede combinar con listas de prefijos para definir un buen conjunto de filtros.

En este ejemplo de configuración, se emplean listas de acceso a la ruta del sistema autónomo (SA) para solo admitir los prefijos entrantes originados por el SA remoto y los prefijos salientes originados por el SA local. Los prefijos que son originados por el resto de los sistemas autónomos se filtran y no se instalan en la tabla de ruteo.

ip as-path access-list 1 permit

ip as-path access-list 2 permit

router bgp <asn>

neighbor <ip-address> remote-as 65501

neighbor <ip-address> filter-list 1 in

neighbor <ip-address> filter-list 2 out

Proteja los protocolos de gateway interior

La capacidad de una red de reenviar correctamente el tráfico y de recuperarse de cambios en la topología o de fallas depende de una vista precisa de la topología, Para ofrecer esta vista, muchas veces puede ejecutarse un protocolo de gateway interior (IGP). De forma predeterminada, los protocolos IGP son dinámicos y descubren los routers adicionales que se comunican con el IGP en particular que se encuentra funcionando. Los protocolos IGP también descubren las rutas que se pueden utilizar durante una falla de link de la red.

Las siguientes subsecciones describen en términos generales las funciones de seguridad de IGP más importantes.

Cuando corresponda, se incluyen recomendaciones y ejemplos que abarcan Routing Information Protocol Version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP) y Open Shortest Path First (OSPF).

Autenticación y Verificación de Protocolo de Ruteo con Message Digest 5

Si no se logra asegurar el intercambio de información de ruteo, un atacante puede introducir información de ruteo falsa en la red. Mediante el uso de la autenticación de contraseña con

protocolos de ruteo entre routers, puede ayudar a la seguridad de la red. Sin embargo, puesto que esta autenticación se envía como texto sin formato, un atacante puede destruir este control de seguridad sin inconvenientes.

Cuando agrega capacidades de hash MD5 al proceso de autenticación, las actualizaciones de ruteo ya no contienen contraseñas de texto sin formato, y todo el contenido de la actualización de ruteo es más resistente a la manipulación. Sin embargo, la autenticación MD5 todavía puede sufrir ataques de fuerza bruta y de diccionario si se eligen contraseñas débiles. Se recomienda el uso de contraseñas con suficiente distribución al azar. Puesto que la autenticación MD5 es mucho más segura en comparación con la autenticación de contraseña, estos ejemplos son específicos para la autenticación MD5. También se puede utilizar IPSec para validar y asegurar protocolos de ruteo, pero estos ejemplos no detallan su uso.

EIGRP y RIPv2 utilizan Key Chains como parte de la configuración. Consulte clave para obtener más información sobre la configuración y el uso de Key Chains.

Este es un ejemplo de configuración para la autenticación del router EIGRP que utiliza MD5:

key chain <key-name>

key <key-identifier>

key-string <password>

interface <interface> ip authentication mode eigrp <as-number> md5

ip authentication key-chain eigrp <as-number> <key-name>

Esto es un ejemplo de configuración de la autenticación de router MD5 para RIPv2. RIPv1 no admite la autenticación.

key chain <key-name>

key <key-identifier>

key-string <password>

interface <interface> ip rip authentication mode md5

ip rip authentication key-chain <key-name>

Este es un ejemplo de configuración para la autenticación de router OSPF que utiliza MD5. OSPF no utiliza Key Chains.

interface <interface> ip ospf message-digest-key <key-id> md5 <password>

router ospf <process-id>

network 10.0.0.0 0.255.255.255 area 0 area 0 authentication message-digest

Consulte Configuración de OSPF para obtener más información.

Comando Passive-Interface

Las filtraciones de información, o la introducción de información falsa en un IGP, se pueden mitigar mediante el uso del comando passive-interface que ayuda a controlar el anuncio de la información de ruteo. Se recomienda que no publique ningún datos en las redes que están fuera de su control administrativo.

Este ejemplo demuestra el uso de esta función:

router eigrp <as-number> passive-interface default

no passive-interface <interface>

Filtrado de Rutas

Para reducir la probabilidad de introducir información de routing falsa en la red, debe emplear filtrado de routing. A diferencia del comando de configuración de ruta passive-interface, el ruteo ocurre en las interfaces una vez que se habilita el filtrado de rutas, pero la información que se publica o procesa es limitada.

Para EIGRP y RIP, al usar el comando distribute-list con la palabra clave out se limita la información difundida, mientras que la palabra clave in limita las actualizaciones procesadas. El comando distribute-list está disponible para OSPF, pero no evita que un router propague rutas filtradas. Se puede usar, en cambio, el comando area filter-list.

Este ejemplo de EIGRP filtra las publicaciones salientes con el comando distribute-list y una lista de prefijos:

ip prefix-list <list-name>

seq 10 permit <prefix>

router eigrp <as-number>

passive-interface default

no passive-interface <interface>

distribute-list prefix <list-name> out <interface>

Este ejemplo de EIGRP filtra las actualizaciones entrantes con una lista de prefijos:

ip prefix-list <list-name> seq 10 permit <prefix>

router eigrp <as-number>

passive-interface default

no passive-interface <interface>

distribute-list prefix <list-name> in <interface>

Consulte Filtrado de Rutas EIGRP para obtener más información sobre cómo controlar la publicidad y el procesamiento de las actualizaciones de ruteo.

En este ejemplo de OSPF, se emplea una lista de prefijos con el comando específico de OSPF area filter-list:

ip prefix-list <list-name> seq 10 permit <prefix>

router ospf <process-id>

area <area-id> filter-list prefix <list-name> in

Consumo de Recursos del Proceso de Ruteo

Los prefijos de protocolo de ruteo son guardados por un router en la memoria y el consumo de recursos aumenta con los prefijos adicionales que un router debe contener. Para evitar el agotamiento de recursos, es importante configurar el protocolo de ruteo para limitar el consumo de recursos. Esto es posible con OSPF si se emplea la función de protección de sobrecarga de base de datos de estado de enlaces.

Este ejemplo demuestra la configuración de la función de protección contra sobrecarga de base de datos de estado de link de OSPF:

router ospf <process-id> max-lsa <maximum-number>

Consulte Limitación del Número de LSA que se Generan Automáticamente para un Proceso OSPF para obtener más información sobre la protección contra sobrecarga de base de datos de estado de link de OSPF.

Proteja los protocolos de redundancia de primer salto

Estos protocolos FHRP ofrecen recuperabilidad y redundancia para dispositivos que actúan como gateways predeterminados. Esta situación y estos protocolos son corrientes en entornos en los que un par de dispositivos de la Capa 3 funciona como gateway predeterminado para un segmento de red o un conjunto de VLAN que contengan servidores o estaciones de trabajo.

Los protocolos Gateway Load-Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP) y Virtual Router Redundancy Protocol son FHRP. De forma predeterminada, estos protocolos se comunican con mensajes no autenticados. Este tipo de comunicación puede permitir que un atacante se haga pasar por un dispositivo que habla por FHRP para así asumir la función de gateway predeterminado en la red. Esta toma de posesión permitiría que un atacante realice un ataque por desconocido e intercepte todo el tráfico de usuario que sale de la red.

Para evitar este tipo de ataque, todos los FHRPs soportados por el software Cisco IOS XE incluyen una capacidad de autenticación con MD5 o cadenas de texto. Debido a la amenaza planteada por los FHRP no autenticados, se recomienda que las instancias de estos protocolos

utilicen autenticación MD5. Este ejemplo de configuración demuestra el uso de autenticación MD5 para GLBP, HSRP y VRRP:

interface FastEthernet 1

description *** GLBP Authentication ***

glbp 1 authentication md5 key-string <glbp-secret>

glbp 1 ip 10.1.1.1

interface FastEthernet 2

description *** Autenticación HSRP ***

standby 1 authentication md5 key-string <hsrp-secret>

standby 1 ip 10.2.2.1

interface FastEthernet 3

descripción *** Autenticación VRRP ***

vrrp 1 authentication md5 key-string <vrrp-secret>

vrrp 1 ip 10.3.3.1

Plano de Datos

Aunque el plano de datos sea responsable de transferir datos desde el origen hasta el destino, dentro del contexto de la seguridad, es el menos importante de los tres planos. Por este motivo, es importante priorizar la protección de los planos de control y administración por sobre el plano de datos al proteger dispositivos de redes.

Sin embargo, dentro del plano de datos, hay muchas funciones y opciones de configuración que pueden ayudar a asegurar el tráfico. En las secciones a continuación se detallan estas características y opciones para que pueda asegurar su red más fácilmente.

Consolidación del Plano de Datos General

La gran mayoría del tráfico del plano de datos fluye a través de la red según lo determinado por la configuración de ruteo de la red. Sin embargo, existen funciones de red IP que permiten alterar la trayectoria de los paquetes a través de la red. Funciones como las opciones de IP, específicamente la opción de ruteo de origen, representan un desafío de la seguridad en las redes de hoy.

El uso ACL de tránsito también es importante para la consolidación del plano de datos.

Para ver más información, consulte la sección Filtre el tráfico en tránsito con ACL de tránsito de

este documento.

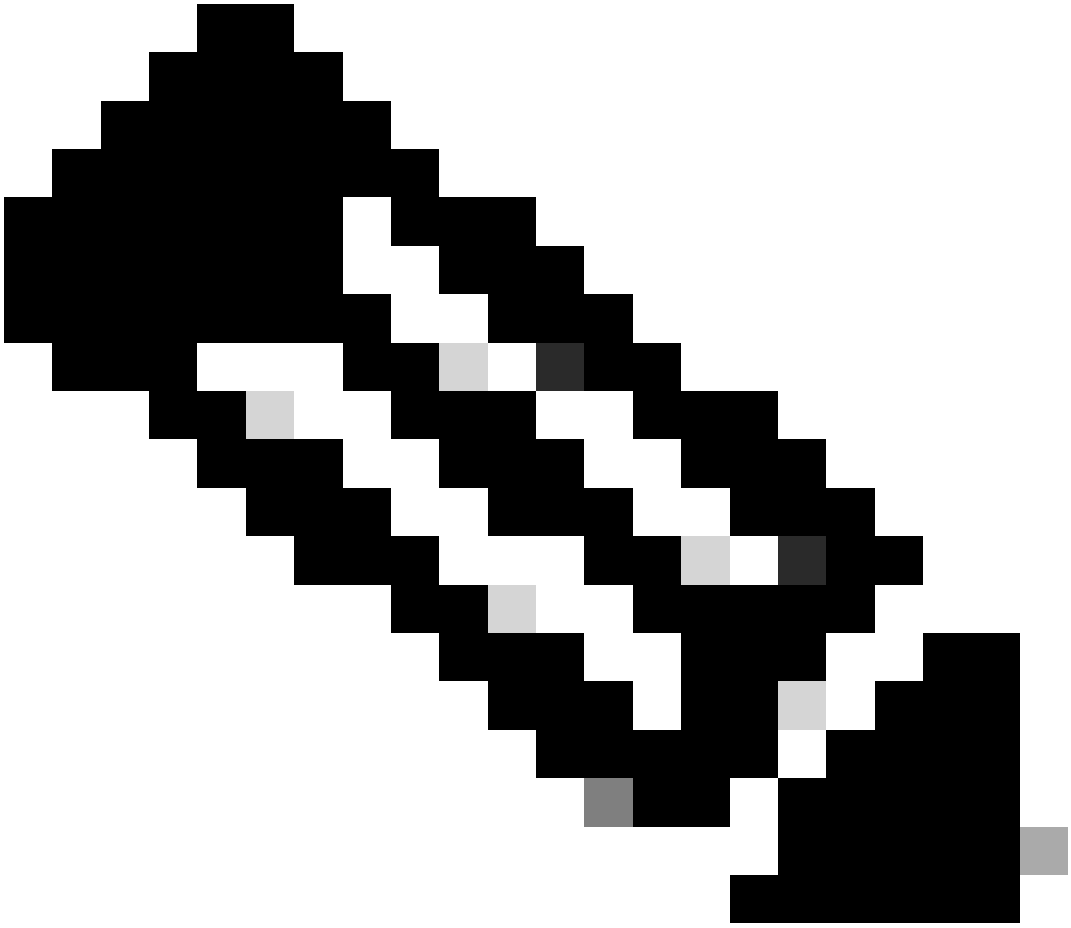
IP Options Selective Drop

Las opciones IP plantean dos problemas de seguridad. El tráfico que contiene opciones IP debe ser conmutado por proceso por los dispositivos Cisco IOS XE, lo que puede llevar a una carga de CPU elevada. Las opciones de IP también incluyen la posibilidad de alterar la ruta del tráfico por la red, lo cual podría permitir al tráfico sortear los controles de seguridad.

Debido a estos problemas, el comando de configuración global ip options {drop | ignore} se ha agregado a las versiones 16.6.4 y posteriores del software Cisco IOS XE. En la primera forma de este comando, ip options drop, se descartan todos los paquetes IP que contienen opciones IP recibidos por el dispositivo Cisco IOS XE. De esta manera se evita una carga elevada del CPU y la posible destrucción de los controles de seguridad que las opciones IP pueden habilitar.

La segunda forma de este comando, ip options ignore, configura el dispositivo Cisco IOS XE para ignorar las opciones IP que están contenidas en los paquetes recibidos. Si bien esto no disminuye las amenazas relacionadas con las opciones IP para el dispositivo local, es posible que los dispositivos de flujo descendente puedan verse afectados por la presencia de opciones IP. Es por esta razón que se recomienda firmemente la forma drop de este comando. Esto se demuestra en el ejemplo de configuración:

ip options drop



Nota: Algunos protocolos, por ejemplo el RSVP, hacen un uso legítimo de las opciones IP. El funcionamiento de estos protocolos se ve afectado por este comando.

Una vez que se ha habilitado la función IP Options Selective Drop, el comando EXEC show ip traffic puede ser utilizado para determinar el número de paquetes que se descartan debido a la presencia de opciones IP. Esta información está presente en el contador de forced drop.

Consulte ACL IP Options Selective Drop para obtener más información sobre esta función.

Inhabilitación de Ruteo de Origen de IP

El ruteo de origen de IP aprovecha las opciones Loose Source Route y Record Route conjuntamente o la opción Strict Source Route junto con Record Route para habilitar el origen del datagrama IP para especificar la trayectoria de red que toma un paquete. Se puede utilizar esta función para intentar rutear el tráfico alrededor de los controles de seguridad en la red.

Si las opciones IP no se inhabilitaron totalmente a través de la función IP Options Selective Drop,

es importante que se inhabilite el ruteo de origen de IP. El ruteo de origen IP, que está habilitado de forma predeterminada en todas las versiones del software Cisco IOS XE, se inhabilita mediante el comando de configuración global no ip source-route.

Este ejemplo de configuración ilustra el uso de este comando:

no ip source-route

Inhabilitación de Mensajes de Redirección ICMP

Los mensajes de redirección ICMP se utilizan para informar a un dispositivo de red una mejor trayectoria a un destino IP. De forma predeterminada, el software Cisco IOS XE envía una redirección si recibe un paquete que debe enrutarse a través de la interfaz que recibió.

En algunas situaciones, puede ser posible que un atacante haga que el dispositivo Cisco IOS XE envíe muchos mensajes de redirección ICMP, lo que resulta en una carga de CPU elevada. Por este motivo, se recomienda que la transmisión de mensajes de redirección ICMP se inhabilite. Los redireccionamientos de ICMP se desactivan mediante el comando de configuración de interfaz no ip redirects, como se muestra en el ejemplo de configuración:

interface FastEthernet 0

no ip redirects

Inhabilitación o Limitación de Broadcasts Dirigidos a IP

Los Broadcasts Dirigidos a IP permiten enviar un paquete de broadcast IP a una subred IP remota. Una vez que alcanza la red remota, el dispositivo IP de reenvío envía el paquete como broadcast de Capa 2 a todas las estaciones en la subred. Esta función de difusión dirigida se ha aprovechado como ayuda de amplificación y reflexión en varios ataques que incluyen el ataque smurf.

Las versiones actuales del software Cisco IOS XE tienen esta funcionalidad inhabilitada de forma predeterminada; sin embargo, se puede habilitar a través del comando de configuración de la interfaz ip directed-broadcast. Las versiones del software Cisco IOS XE anteriores a la 12.0 tienen esta funcionalidad habilitada de forma predeterminada.

Si una red requiere absolutamente la funcionalidad de broadcast dirigido, su uso puede ser controlado. Esto es posible mediante el uso de una lista de control de acceso como opción para el comando ip directed-broadcast. En este ejemplo de configuración, solo se permiten las transmisiones dirigidas de paquetes de UDP originados en la red de confianza 192.168.1.0/24:

access-list 100 permit udp 192.168.1.0 0.0.0.255 any

interface FastEthernet 0

ip directed-broadcast 100

Filtre el tráfico en tránsito con ACL de tránsito

Mediante las ACL de tránsito (tACL) se puede controlar qué tráfico transita por las redes. Estas listas se diferencian de las ACL de infraestructura que pretenden filtrar el tráfico que se dirige a la red en sí misma. El filtrado que ofrecen las tACL viene bien cuando se desea filtrar el tráfico destinado a un grupo en particular de dispositivos o el tráfico que transita por la red.

Tradicionalmente, los firewalls realizan este tipo de filtrado. Sin embargo, hay casos en los que puede ser beneficioso realizar este filtrado en un dispositivo Cisco IOS XE de la red, por ejemplo, en los que debe realizarse el filtrado pero no hay ningún firewall presente.

Las ACL de tránsito son también un lugar apropiado en el cual implementar las protecciones contra suplantación estáticas.

Para ver más información, consulte la sección Protecciones contra la suplantación de identidad de este documento.

Consulte Listas de Control de Acceso de Tránsito: Filtrado en el Borde para obtener más información sobre las tACL.

Filtrado de Paquetes ICMP

El protocolo Internet Control Message Protocol (ICMP) fue diseñado como protocolo de control para IP. Como tal, los mensajes que transmite pueden tener ramificaciones de largo alcance en los protocolos TCP e IP en general. ICMP es utilizado por las herramientas de troubleshooting de la red ping y traceroute, así como por Path MTU Discovery; sin embargo, la conectividad ICMP externa rara vez se necesita para el funcionamiento correcto de una red.

El software Cisco IOS XE proporciona funcionalidad para filtrar específicamente los mensajes ICMP por nombre o tipo y código. En este ejemplo de ACL, se permiten ICMP de redes de confianza, pero se bloquean todos los paquetes de ICMP de otras fuentes:

ip access-list extended ACL-TRANSIT-IN

— Permitir paquetes ICMP sólo de redes de confianza

permit icmp host <trusted-networks> any

— Denegar el resto del tráfico IP a cualquier dispositivo de red

deny icmp any any

Filtrar fragmentos IP

Como ya se detalló en este documento en la sección Acceso limitado a la red mediante ACL de infraestructura, el filtrado de paquetes de IP fragmentados puede constituir un desafío para los dispositivos de seguridad.

Dada la naturaleza no intuitiva del manejo de fragmentos, las ACL suelen permitir fragmentos de IP inadvertidamente. La fragmentación también se usa con frecuencia para intentar evadir la detección mediante sistemas de detección de intrusión. Es por estas razones que los fragmentos IP se utilizan a menudo en ataques y se pueden filtrar explícitamente en la parte superior de cualquier tACL configurada.

La ACL incluye un filtrado completo de fragmentos IP. La función ilustrada en este ejemplo se debe utilizar junto con la función de los ejemplos anteriores:

ip access-list extended ACL-TRANSIT-IN

— Denegar fragmentos IP que utilizan ACE específicos de protocolo para ayudar en

— clasificación del tráfico de ataque

deny tcp any any fragments

deny udp any any fragments

deny icmp any any fragments

deny ip any any fragments

Refiérase a Procesamiento de Fragmentos de la Lista de Acceso para obtener más información sobre el manejo de ACL de paquetes IP fragmentados.

ACL Support for Filtering IP Options

En la versión 16.6.4 y posteriores del software Cisco IOS XE, el software Cisco IOS XE admite el uso de ACL para filtrar paquetes IP basados en las opciones IP que contiene el paquete. La presencia de opciones IP dentro de un paquete puede indicar un intento de subvertir los controles de seguridad en la red o alterar de alguna otra manera las características de tránsito de un paquete. Es por estas razones que los paquetes con opciones IP se pueden filtrar en el borde de la red.

Este ejemplo se debe utilizar con el contenido de los ejemplos anteriores para incluir el filtrado de paquetes IP que contienen opciones IP:

ip access-list extended ACL-TRANSIT-IN

— Denegar paquetes IP que contengan opciones IP

deny ip any any option any-options

Protecciones Contra Suplantación

En muchos ataques, se falsifica la dirección IP de origen para ganar eficacia u ocultar el origen verdadero y así entorpecer el rastreo. El software Cisco IOS XE proporciona RPF unidifusión y protección de IP de origen (IPSG) para disuadir los ataques que se basan en la suplantación de la

dirección IP de origen. Además, las ACL y el ruteo nulo suelen implementarse como métodos manuales de prevención de la suplantación.

La protección de IP de origen reduce la suplantación de identidad en las redes bajo control administrativo directo, al verificar el puerto de switch, la dirección MAC y la dirección de origen. La función Unicast RPF proporciona verificación de la red de origen y puede reducir los ataques mediante suplantación de redes que no están bajo control administrativo directo. Port Security se puede utilizar para validar direcciones MAC en la capa de acceso. La inspección del protocolo de resolución de direcciones (ARP) dinámica (DAI) mitiga los vectores de ataque que contaminan ARP en los segmentos locales.

Unicast RPF

Unicast RPF permite que un dispositivo verifique que la dirección de origen de un paquete reenviado puede ser alcanzada a través de la interfaz que recibió el paquete. No debe utilizar Unicast RPF como la única protección contra suplantación. Los paquetes falsificados podrían entrar a la red a través de una interfaz RPFenabled de unidifusión si existe una ruta de retorno adecuada a la dirección IP de origen. Con RPF unicast, usted debe activar Cisco Express Forwarding en cada dispositivo, y la configuración se hace en cada interfaz.

RPF unidifusión se puede configurar en uno de dos modos: amplio o estricto. Si el ruteo es asimétrico, se prefiere el modo flexible porque se sabe que el modo estricto descarta paquetes en estas situaciones. Durante la configuración del comando de configuración de interfaz ip verify, la palabra clave any configura el modo flexible mientras que la palabra clave rx configura el modo estricto.

Este ejemplo ilustra la configuración de esta función:

ip cef

interface <interface>

ip verify unicast source reachable-via <mode>

Consulte Comprensión de Unicast Reverse Path Forwarding para obtener más información sobre la configuración y el uso de Unicast RPF.

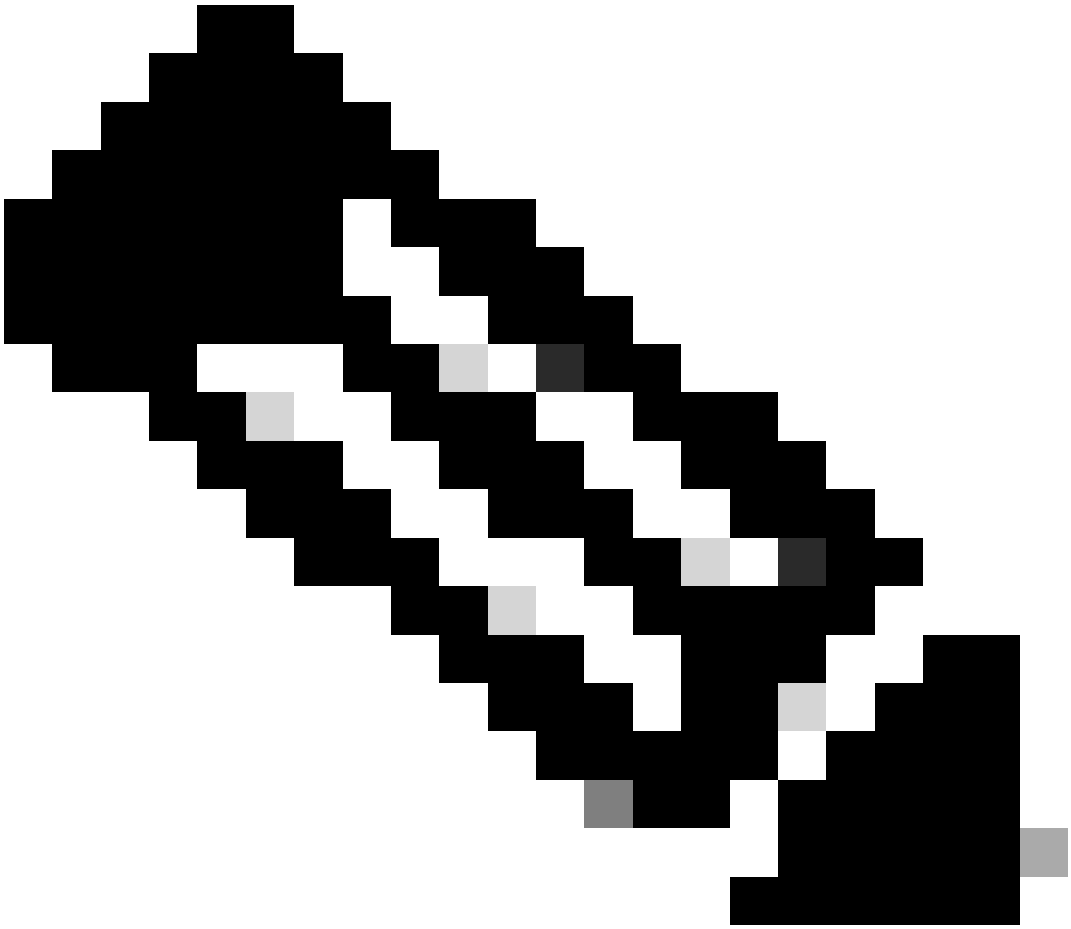
IP Source Guard

IP Source Guard es una función eficaz para la prevención de la suplantación que se puede utilizar si usted tiene control de las interfaces de la Capa 2. Esta función utiliza información obtenida de la serie de técnicas DHCP snooping para configurar dinámicamente una lista de control de acceso de puerto (PACL) en la interfaz de Capa 2 y niega cualquier tráfico de direcciones IP no asociadas en la tabla de enlace de origen IP.

IP Source Guard se puede aplicar a interfaces de la Capa 2 que pertenecen a VLAN con la función DHCP snooping habilitada. Estos comandos habilitan la función DHCP snooping:

ip dhcp snooping

ip dhcp snooping vlan <vlan-range>



> Nota: Para admitir IP Source Guard, el chasis/router necesita un módulo de switching de capa 2.

Port Security se puede habilitar con el comando de configuración ip verify source port security interface . Esto requiere el comando de configuración global ip dhcp snooping information option; además, el servidor DHCP debe admitir la opción DHCP 82.

Consulte IP Source Guard para obtener más información sobre esta función.

Seguridad de Puertos

Port Security se utiliza para reducir la suplantación de direcciones MAC en la interfaz de acceso. Port Security puede utilizar direcciones MAC (sticky) aprendidas dinámicamente para facilitar la configuración inicial. Una vez que la seguridad de puertos determina una infracción de MAC,

puede usar uno de los cuatro modos de infracción. a saber: protect, restrict, shutdown y shutdown VLAN. En los casos en que un puerto sólo proporciona acceso a una estación de trabajo con el uso de protocolos estándar, puede ser suficiente un número máximo de uno. Los protocolos que utilizan direcciones MAC virtuales, como HSRP, no funcionan cuando el número máximo se configura en uno.

interface <interface> switchport

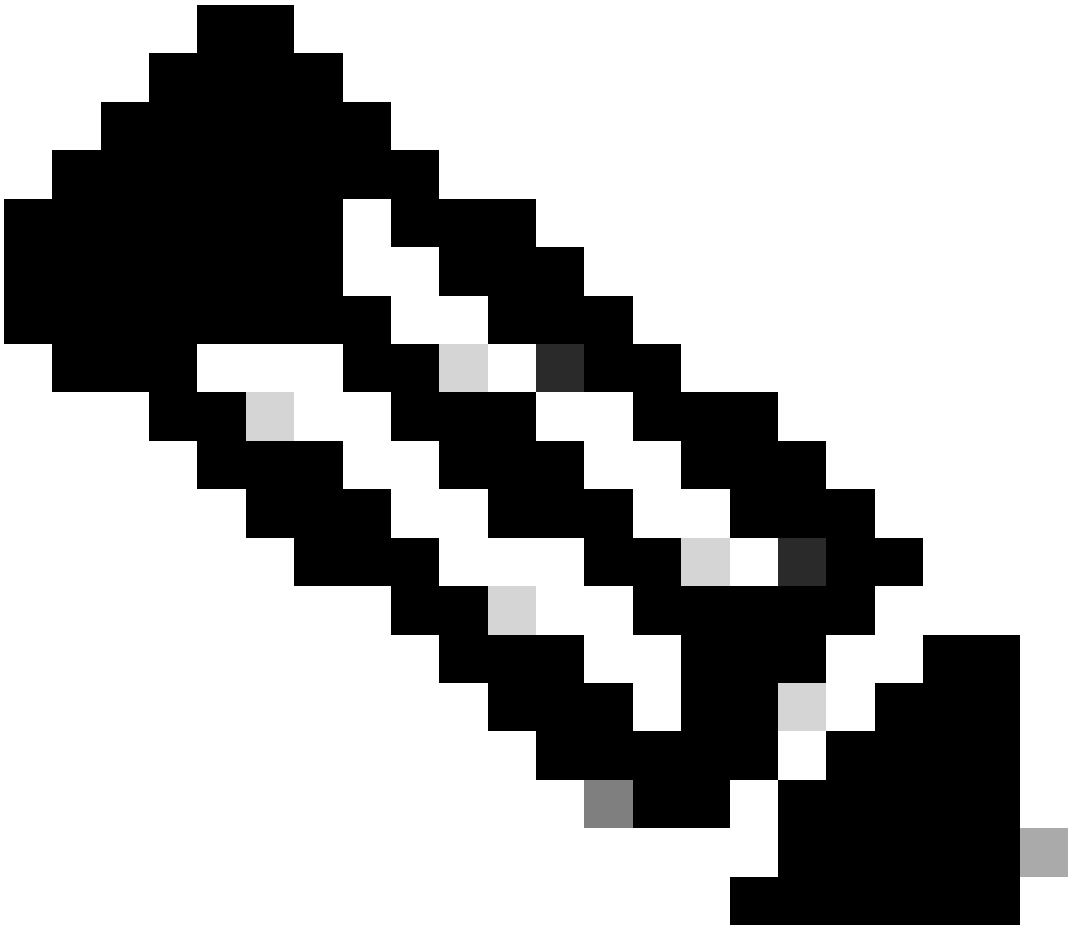
switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum <number>

switchport port-security violation <violation-mode>



Nota: Para admitir la seguridad de puertos, el chasis/router necesita un módulo de

---

switching de capa 2.

Consulte Configuración de la Seguridad de Puerto para obtener más información sobre la configuración de la Seguridad de Puerto.

ACL Contra Suplantación

Las ACL de configuración manual pueden brindar protección estática contra la suplantación de identidad para los ataques que emplean espacios conocidos de direcciones no utilizadas y no confiables. Comúnmente, estas ACL de protección contra suplantación se aplican al tráfico de ingreso en los límites de red como componente de una ACL más grande. Las ACL contra la suplantación de identidad exigen monitoreo regular porque pueden cambiar con frecuencia. Estos ataques pueden reducirse en el tráfico que se origina en la red local si se aplican ACL salientes que limiten el tráfico hacia direcciones locales válidas.

Este ejemplo demuestra cómo se pueden utilizar ACL para limitar la suplantación IP. Esta ACL se aplica al tráfico entrante en la interfaz deseada. Las ACE que componen esta ACL no son exhaustivas. Si usted configura estos tipos de ACL, busque una referencia actualizada que sea concluyente.

ip access-list extended ACL-ANTISPOOF-IN

deny ip 10.0.0.0 0.255.255.255 any

deny ip 192.168.0.0 0.0.255.255 any

interface <interface>

ip access-group ACL-ANTISPOOF-IN in

Consulte Configuración de ACL IPv4 para obtener más información sobre cómo configurar las Listas de Control de Acceso.

Limite el impacto del tráfico del plano de datos sobre la CPU

La función principal que desempeñan los routers y los switches es reenviar paquetes y tramas a través del dispositivo a los destinos finales. Estos paquetes, que transitan los dispositivos implementados en la red, pueden afectar el funcionamiento del CPU de un dispositivo. El plano de datos, que consiste en el tráfico que transita por el dispositivo de red, se puede proteger para garantizar el funcionamiento de los planos de gestión y control. Si el tráfico de tránsito puede hacer que un dispositivo procese el tráfico del switch, el plano de control de un dispositivo puede verse afectado, lo que puede provocar una interrupción operativa.

Funciones y Tipos de Tráfico que Afectan el CPU

Esta lista, aunque no sea exhaustiva, incluye los tipos de tráfico del plano de datos que requieren

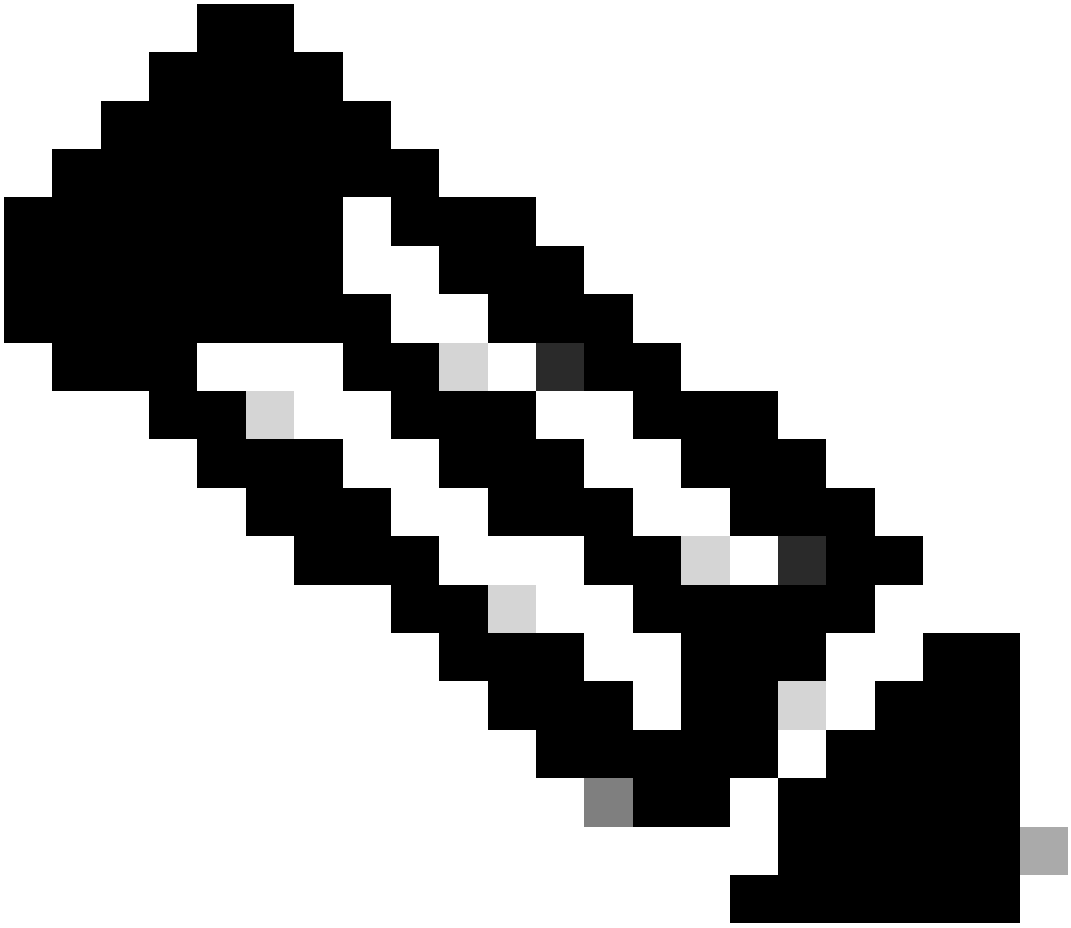
procesamiento especial del CPU y que el CPU conmuta en el procesador:

1. Registro de ACL: El tráfico de registro de ACL consiste en los paquetes generados por coincidencias (permiso o denegación) de ACE donde se emplea la palabra clave log.
2. Unicast RPF: El uso de Unicast RPF junto con una ACL puede dar lugar a la conmutación del proceso de ciertos paquetes.
3. Opciones de IP: La CPU debe procesar todos los paquetes de IP que incluyan opciones.
4. Fragmentación: La CPU debe recibir y procesar todos los paquetes de IP que exijan fragmentación.
5. Tiempo de vida (TTL) agotado: Los paquetes con un valor de TTL inferior o igual a 1 exigen el envío del mensaje Internet Control Message Protocol Time Exceeded (ICMP Type 11, Code 0) (Se agotó el tiempo del protocolo de mensajería de control de Internet, Tipo de ICMP 11, Código 0), lo cual genera el procesamiento por parte de la CPU.
6. ICMP inalcanzables: La CPU procesa los paquetes que resultan en mensajes de ICMP inalcanzable por routing, MTU o filtrado.
7. Tráfico que requiere una solicitud de ARP: La CPU debe procesar los destinos para los cuales no existe ninguna entrada de ARP.
8. Tráfico que no es de IP: La CPU procesa todo el tráfico que no es de IP.

   Consulte la sección Consolidación del Plano de Datos General este documento para obtener más información sobre la Consolidación del Plano de Datos.

Filtre por el valor de TTL

Puede utilizar la función ACL Support for Filtering on TTL Value, introducida en la versión 16.6.4 del software Cisco IOS XE, en una lista de acceso IP ampliada para filtrar paquetes según el valor TTL. Esta función se puede utilizar para proteger un dispositivo que recibe tráfico de tránsito y si el valor TTL es cero o uno. El filtrado de paquetes basado en valores TTL también se puede utilizar para garantizar que el valor TTL no sea inferior al diámetro de la red, por lo que protege el plano de control de los dispositivos de infraestructura descendentes de ataques de vencimiento TTL.



Nota: algunas aplicaciones y herramientas como traceroute utilizan paquetes de vencimiento TTL para fines de prueba y diagnóstico. Algunos protocolos, como IGMP, hacen un uso legítimo de un valor TTL de uno.

Este ejemplo de ACL crea una política que filtra paquetes IP si el valor TTL es inferior a 6.

— Cree una política ACL que filtre los paquetes IP con un valor TTL.

— inferior a 6

ip access-list extended ACL-TRANSIT-IN

deny ip any any ttl lt 6

permit ip any any

— Aplicar lista de acceso a la interfaz en la dirección de entrada.

interface GigabitEthernet 0/0

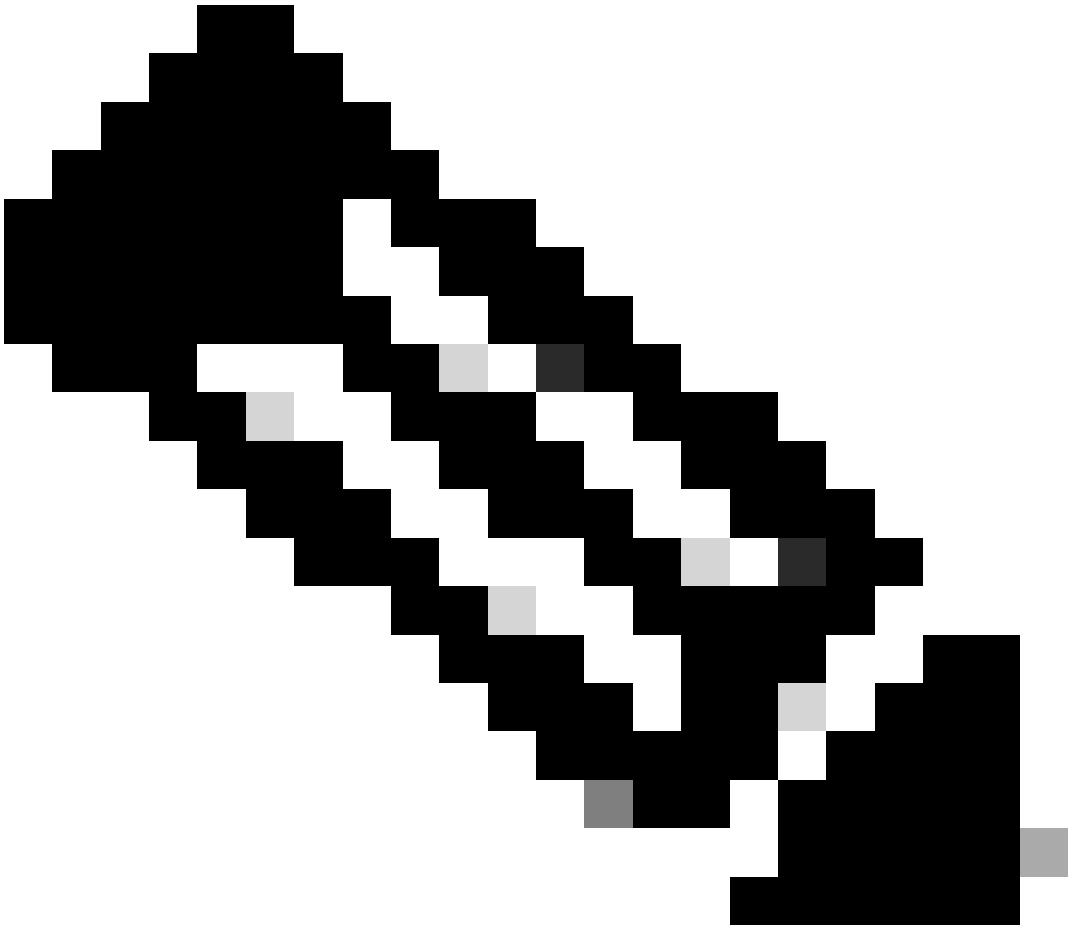
ip access-group ACL-TRANSIT-IN in

Consulte Identificación y Disminución de Ataques Basados en el Vencimiento de TTL para obtener más información sobre el filtrado de paquetes basado en el valor TTL.

Consulte ACL Support for Filtering on TTL Value para obtener más información sobre esta función.

Filtre por la presencia de opciones de IP

En Cisco IOS XE Software Release 16.6.4 y versiones posteriores, puede utilizar el Soporte ACL para la función de Filtrado de Opciones IP en una lista de acceso IP ampliada y con nombre para filtrar los paquetes IP con las opciones IP presentes. El filtrado de paquetes IP que se basan en la presencia de opciones IP también se puede utilizar para evitar que el plano de control de los dispositivos de infraestructura tenga que procesar estos paquetes en el nivel de CPU.



Nota: La función ACL Support for Filtering IP Options (Soporte de ACL para Filtrar Opciones IP) sólo se puede utilizar con ACL con nombre y ampliadas.

También se puede observar que RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP Versiones 2 y 3, y otros protocolos que utilizan paquetes de opciones IP no pueden funcionar correctamente si se descartan los paquetes para estos protocolos. Si estos protocolos están en uso en la red, se puede utilizar ACL Support for Filtering IP Options ; sin embargo, la función ACL IP Options Selective Drop podría descartar este tráfico y estos protocolos no pueden funcionar correctamente. Si no se usan protocolos que exijan opciones de IP, el método preferido para rechazar estos paquetes es el del rechazo selectivo de opciones de IP de ACL.

Este ejemplo de ACL crea una política que filtra los paquetes IP que contienen cualquier opción IP:

ip access-list extended ACL-TRANSIT-IN

deny ip any any option any-options

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN in

Este ejemplo ACL demuestra una política esa los paquetes del IP de los filtros con cinco opciones IP específicas. Se niegan los paquetes que contienen estas opciones:

1. 0 End of Options List (eool)
2. 7 Record Route (record-route)
3. 68 Time Stamp (timestamp)
4. 131 - Source ruta flexible (lsr)
5. 137 - Source ruta estricta (ssr)

ip access-list extended ACL-TRANSIT-IN

deny ip any any option eool

deny ip any any option record-route

deny ip any any option timestamp

deny ip any any option lsr

deny ip any any option ssr

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-IN in

Consulte la sección Consolidación del Plano de Datos General de este documento para obtener más información sobre la función ACL IP Options Selective Drop.

Otra función del software Cisco IOS XE que se puede utilizar para filtrar paquetes con opciones IP es CoPP. En la versión 16.6.4 y posteriores del software Cisco IOS XE, CoPP permite que un administrador filtre el flujo de tráfico de los paquetes del plano de control. Un dispositivo compatible con CoPP y ACL Support for Filtering IP Options, introducido en la versión 16.6.4 del software Cisco IOS XE, puede utilizar una política de lista de acceso para filtrar paquetes que contengan opciones IP.

Esta política de CoPP descarta los paquetes de tránsito recibidos por un dispositivo cuando hay alguna opción IP presente:

ip access-list extended ACL-IP-OPTIONS-ANY

permit ip any any option any-options

class-map ACL-IP-OPTIONS-CLASS

match access-group name ACL-IP-OPTIONS-ANY

policy-map COPP-POLICY

class ACL-IP-OPTIONS-CLASS

police 80000 compliance transmit exceeds drop

plano de control

service-policy input COPP-POLICY !

Esta política de CoPP descarta los paquetes de tránsito recibidos por un dispositivo cuando estas opciones IP están presentes:

1. 0 End of Options List (eool)
2. 7 Record Route (record-route)
3. 68 Time Stamp (timestamp)
4. 131 Loose Source Route (lsr)
5. 137 Strict Source Route (ssr)

```
ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
police 80000 compliance transmit exceeds drop

plano de control
service-policy input COPP-POLICY
```

En las políticas CoPP anteriores, las entradas de la lista de control de acceso (ACE) que coinciden con los paquetes con la acción permit hacen que estos paquetes sean descartados por la función drop de policy-map, mientras que los paquetes que coinciden con la acción deny (no se muestran) no se ven afectados por la función drop de policy-map.

Para ver más información sobre la función CoPP, consulte Implementación de políticas del plano de control.

Función Control Plane Protection

En la versión 16.6.4 y posteriores del software Cisco IOS XE, se puede utilizar la protección del plano de control (CPPr) para restringir o controlar el tráfico del plano de control por parte de la CPU de un dispositivo Cisco IOS XE. Si bien es similar a la CoPP, CPPr tiene la capacidad de restringir o supervisar el tráfico que utiliza una granularidad más fina que la CoPP. CPPr divide el plano de control agregado en tres categorías de plano de control independientes conocidas como subinterfaces: existen subinterfaces Host, Transit y CEF-Exception.

Esta política de CPPr descarta los paquetes de tránsito recibidos por un dispositivo si el valor TTL es inferior a 6 y los paquetes de tránsito o no tránsito recibidos por un dispositivo si el valor TTL es cero o uno. La política de CPPr también descarta los paquetes con opciones IP seleccionadas

recibidos por el dispositivo.

```
ip access-list extended ACL-IP-TTL-0/1
permit ip any any ttl eq 0 1
class-map ACL-IP-TTL-0/1-CLASS
match access-group name ACL-IP-TTL-0/1
ip access-list extended ACL-IP-TTL-LOW
permit ip any any ttl lt 6
class-map ACL-IP-TTL-LOW-CLASS
match access-group name ACL-IP-TTL-LOW
ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
policy-map CPPR-CEF-EXCEPTION-POLICY
class ACL-IP-TTL-0/1-CLASS
police 80000 compliance-action drop
class ACL-IP-OPTIONS-CLASS
police 8000 compliance-action drop
policy-map CPPR-TRANSIT-POLICY
class ACL-IP-TTL-LOW-CLASS
police 8000 compliance-action drop
```

tránsito del plano de control

```
service-policy input CPPR-TRANSIT-POLICY
```

En la política anterior de CPPr, en las entradas de la lista de control de acceso, los paquetes que coincidían con la acción de permitir se desechaban mediante la función de rechazo de mapa de políticas, mientras que los paquetes que coincidían con la acción de rechazar (no mostrados) no se veían afectados por dicha función.

Consulte Control Plane Policing para obtener más información sobre la función CPPr.

Identificación y Determinación del Origen del Tráfico

En ocasiones, debe identificar y rastrear rápidamente el tráfico de red, especialmente durante la respuesta a incidentes o cuando el rendimiento de la red es bajo. Las ACL de clasificación y NetFlow son los dos métodos principales para lograr esto con el software Cisco IOS XE. Netflow permite ver todo el tráfico en la red. Además, NetFlow se puede implementar con recopiladores que pueden proporcionar análisis automatizados y tendencias a largo plazo. Las ACL de clasificación son un componente de las ACL y requieren planificación previa para identificar tráfico específico e intervención manual durante el análisis. Las siguientes secciones proporcionan una breve descripción de cada función.

Netflow

Netflow realiza un seguimiento de los flujos de la red para identificar actividad de la red anómala y relacionada con la seguridad. Los datos de NetFlow se pueden ver y analizar mediante la CLI, o se pueden exportar a un recopilador de NetFlow gratuito o comercial para su agregación y análisis. Los colectores NetFlow, a través de la tendencia a largo plazo, pueden proporcionar análisis de uso y de comportamiento de la red. Netflow funciona realizando el análisis de atributos específicos dentro de los paquetes del IP y creando flujos. La versión 5 de Netflow es la versión de uso más frecuente, sin embargo, la versión 9 es más extensible. Se puede crear flujos de NetFlow con muestras de datos de tráfico en entornos de gran volumen.

CEF, o CEF distribuido, es un requisito previo para habilitar NetFlow. Netflow se puede configurar en routers y switches.

El siguiente ejemplo ilustra la configuración básica de esta función. En versiones anteriores del software Cisco IOS XE, el comando para habilitar NetFlow en una interfaz es ip route-cache flow en lugar de ip flow {ingress | egress}.

ip flow-export destination <ip-address> <udp-port>

ip flow-export version <version>

interface <interface>

ip flow <ingess|egress>

Este es un ejemplo del resultado de Netflow en la CLI. El atributo SrcIf puede ayudar en la determinación del origen del tráfico.

router#show ip cache flow IP packet size distribution (26662860 paquetes totales):

1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480

.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

000 000 001 007 039 000 000 000 000 000 000 000 000

Caché de IP Flow Switching, 4456704 bytes

55 activos, 65481 inactivos, 1014683 añadidos

41000680 sondeos ager, 0 errores de asignación de flujo

Tiempo de espera de flujos activos en 2 minutos

Límite de tiempo de flujos inactivos en 60 segundos

Caché de subflujo de IP, 336520 bytes

110 activos, 16274 inactivos, 2029366 añadidos, 1014683 añadidos al flujo

0 fallos de asignación, 0 liberación forzada de 1 fragmento, 15 fragmentos añadidos última eliminación de estadísticas nunca

Total de flujos de protocolo Paquetes bytes Paquetes activos (s) Inactivos (s)

-------- Flujos /Sec /Flow /Pkt /Sec /Flow /Flow

TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8

TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1

TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1

TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5

TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4

TCP-X 351 0.0 2 40 0.0 0.0 60.8

TCP-BGP 114 0.0 1 40 0.0 0.0 62.4

TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4

TCP-other 556070 0.6 8 318 6.0 8.2 38.3

UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1

UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6

UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2

UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8

UDP-otros 86247 0.1 226 29 24.0 31.4 54.3

ICMP 19989 0,0 37 33 0,9 26,0 53,9

IP-otros 193 0.0 1 22 0.0 3.0 78.2

Total: 1014637 1,2 26 99 32,8 13,8 43,9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts

Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3

Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9

Gi0/1 192.168.150.60 Local 192.168.206.20 01 000 0303 11

Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1

Consulte Flexible NetFlow para obtener más información sobre las capacidades de NetFlow.

ACL de Clasificación

Las ACL de clasificación permiten ver el tráfico que cruza una interfaz. Las ACL de clasificación no alteran la política de seguridad de una red y normalmente se construyen para clasificar protocolos, direcciones de origen o destinos individuales. Por ejemplo, una ACE que permite todo el tráfico se podría separar en protocolos o puertos específicos. Esta clasificación más granular del tráfico en ACE específicas puede ayudar a proporcionar una comprensión del tráfico de red porque cada categoría de tráfico tiene su propio contador de visitas. Un administrador también puede separar la negación implícita al final de una ACL en ACE granulares para ayudar a identificar los tipos de tráfico denegado.

Un administrador puede acelerar una respuesta a incidentes mediante el uso de ACL de clasificación con los comandos EXEC show access-list y clear ip access-list counters.

Este ejemplo ilustra la configuración de una ACL de clasificación para identificar el tráfico SMB antes de una negación predeterminada:

ip access-list extended ACL-SMB-CLASSIFY

remark Contenido existente de ACL

remark Clasificación del tráfico TCP específico de SMB

deny tcp any any eq 139

deny tcp any any eq 445

deny ip any any

Para identificar el tráfico que utiliza una ACL de clasificación, utilice el comando show access-list acl-name

comando EXEC. Los contadores ACL se pueden borrar con el comando EXEC clear ip access-list counters .

router#show access-list ACL-SMB-CLASSIFY Extended IP access list ACL-SMB-CLASSIFY

10 deny tcp any any eq 139 (10 coincidencias)

20 deny tcp any any eq 445 (9 coincidencias)

30 deny ip any any (184 coincidencias)

Consulte Comprensión del Registro de Listas de Acceso de Control para obtener más información sobre cómo habilitar las capacidades de registro en las ACL.

Control de Acceso con PACL

Las PACL se pueden aplicar solamente a la dirección entrante en las interfaces físicas de la Capa 2 de un switch. Similar a las VLAN maps, las PACL proporcionan control de acceso en tráfico no ruteado o de la Capa 2. La sintaxis para la creación de las PACL, que tienen precedencia sobre los mapas de VLAN y las ACL de routers, es la misma que para estas últimas. Si una ACL se aplica a un interfaz de Capa 2, se denomina PACL.

La configuración supone la creación de una ACL de MAC, IPv4 o IPv6 y su aplicación en la interfaz de capa 2.

En este ejemplo se emplea una lista de acceso ampliada determinada para ilustrar la configuración de esta función:

ip access-list extended <acl-name> permit <protocol> <source-address> <source-port> <destination-address> <destination-port> !

interface <type> <slot/port> switchport mode access switchport access vlan <vlan_number> ip access-group <acl-name> in !

Consulte la sección ACL de Puerto de Configuración de la Seguridad de la Red con ACL de Puerto para obtener más información sobre la configuración de las PACL.

VLAN aisladas

La configuración de una VLAN secundaria como VLAN aislada previene totalmente la comunicación entre los dispositivos en la VLAN secundaria. Solo puede haber una VLAN aislada por VLAN principal, y solo los puertos promiscuos pueden comunicarse con los puertos en una VLAN aislada. Las VLAN aisladas se pueden utilizar en redes no fiables, como las redes que admiten invitados.

Este ejemplo de configuración configura la red VLAN 11 como VLAN aislada y la asocia con la VLAN primaria (VLAN20). Este ejemplo también configura la interfaz FastEthernet 1/1 como puerto aislado en VLAN 11:

vlan 11 private-vlan alone

vlan 20 private-vlan primary private-vlan association 11

interface FastEthernet 1/1 description *** Port in Isolated VLAN *** switchport mode private-vlan host switchport private-vlan host-association 20 11

VLAN Comunitarias

Una VLAN secundaria que se configura como una VLAN comunitaria permite la comunicación entre los miembros de la VLAN y con cualquier puerto promiscuo en la VLAN primaria. Sin embargo, no hay comunicación posible entre dos VLAN comunitarias cualquiera o entre una VLAN comunitaria y una VLAN aislada. Las VLAN comunitarias se deben utilizar en casos en los que se agrupan servidores que necesitan conectividad mutua, pero no se necesita conectividad a todos los otros dispositivos en la VLAN. Este escenario es común en una red de acceso público o cuando, por ejemplo, los servidores proporcionan contenido a clientes poco confiables.

Este ejemplo configura una sola VLAN comunitaria y configura el puerto FastEthernet 1/2 del switch como miembro de esa VLAN. La VLAN comunitaria, VLAN 12, es una VLAN secundaria a la VLAN 20 primaria.

vlan 12 private-vlan community

vlan 20 private-vlan primary private-vlan association 12

interface FastEthernet 1/2 description *** Port in Community VLAN *** switchport mode private-vlan host switchport private-vlan host-association 20 12

Conclusión

Este documento le brinda una descripción general de los métodos que se pueden utilizar para asegurar un dispositivo del sistema Cisco IOS XE. Si usted asegura los dispositivos, aumenta la seguridad general de las redes que administra. En esta descripción general, se trata la protección de los planos de administración, de control y de datos; además se incluyen recomendaciones para la configuración. En la medida de lo posible, se brinda suficiente información detallada para la configuración de cada función asociada. Sin embargo, en todos los casos, se mencionan las referencias completas para brindarle la información necesaria para una evaluación adicional.

Reconocimientos

Algunas descripciones de funciones en este documento fueron escritas por los equipos de desarrollo de información de Cisco.

Apéndice: Lista de comprobación de consolidación de dispositivos de Cisco IOS XE

Esta lista de verificación es una colección de todos los pasos de consolidación que se presentan en esta guía.

Los administradores pueden utilizarlo como recordatorio de todas las funciones de refuerzo utilizadas y consideradas para un dispositivo Cisco IOS XE, incluso si una función no se implementó porque no se aplicó. Se recomienda a los administradores evaluar los riesgos de cada opción antes de implementarla.

Plano de Administración

1. Contraseñas
   Habilitar hash MD5 (opción secreta) para contraseñas de usuario local y habilitadasConfigurar el bloqueo de reintento de contraseñaDeshabilitar la recuperación de contraseña (considerar el riesgo)
2. Inhabilitación de servicios no utilizados
3. Configurar keepalives TCP para las sesiones de administración
4. Configurar notificaciones del umbral de CPU y de memoria
5. Configurar
   Notificaciones de umbral de memoria y CPU Memoria de reserva para el acceso a la consola Detector de fugas de memoria Detección de desbordamiento de búfer Recopilación de información de desperfecto mejorada
6. Utilizar iACL para restringir el acceso de administración
7. Filtrar (considerar el riesgo)
   Paquetes ICMPfragmentos IPopciones IPvalor TTL en paquetes
8. Función Control Plane Protection
   Configurar filtrado de puertosConfigurar umbrales de cola
9. Acceso de administración
   Utilizar Management Plane Protection para restringir las interfaces de gestiónEstablecer tiempo de espera execUtilizar un protocolo de transporte cifrado (como SSH) para el acceso CLIcontrolar el transporte para líneas vty y tty (opción de clase de acceso)Advertir que se utilizan banners
10. AAA
    Utilizar AAA para autenticación y reservaUtilizar AAA (TACACS+) para autorización de comandosUtilizar AAA para contabilidadUtilizar servidores AAA redundantes
11. SNMP (Protocolo de administración de red simple)
    Configurar comunidades SNMPv2 y aplicar ACLconfigurar SNMPv3
12. Registro
    Configurar el registro centralizadoEstablecer los niveles de registro para todos los componentes relevantesEstablecer la fuente de registroInterfazConfigurar granularidad de registro de fecha y hora
13. Administración de la Configuración
    Sustitución y reversiónAcceso exclusivo a cambios de configuraciónConfiguración de

flexibilidad del softwareNotificaciones de cambios de configuración.

Plano de Control

1. Inhabilitar (considerar el riesgo)
   ICMP redirectsICMP unreachablesProxy ARP
2. Configurar la autenticación NTP si se utiliza NTP
3. Configurar la función Control Plane Policing/Protection (filtrado de puerto, umbrales de cola)
4. Asegurar los protocolos de seguridad
   BGP (TTL, MD5, prefijos máximos, listas de prefijos, ACL de ruta del sistema)IGP (MD5, interfaz pasiva, filtrado de rutas, consumo de recursos)
5. Configurar limitadores de velocidad basados en hardware
6. Asegurar los Protocolos de Redundancia de Primer Salto (GLBP, HSRP, VRRP)

Plano de Datos

1. Configurar la función IP Options Selective Drop
2. Inhabilitar (considerar el riesgo)
   IP source routingIP Directed BroadcastsRedirecciones ICMP
3. Limitar broadcasts dirigidos a IP
4. Configurar TACL (considerar el riesgo)
   Filtrar ICMPFilter IP fragmentsFilter IP optionsFilter TTL values
5. Configurar las protecciones contra suplantación requeridas
   ACLprotección de IP de origenInspección dinámica de ARPseguridad de puertos RFP unidifusión
6. Función Control Plane Protection (cef-exception del plano de control)
7. Configurar Netflow y ACL de clasificación para la identificación del tráfico
8. Configurar ACL de control de acceso requeridas (VLAN maps, PACL, MAC)
9. Configurar VLAN privadas

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).