Guía de Cisco para fortalecer los dispositivos Cisco IOS

Contenido

Encripte las sesiones de administración
SSHv2
SSHv2 Enhancements for RSA Keys
Puertos de Consola y Auxiliar
Control de Líneas vty y tty
Control del Transporte para Líneas vty y tty
Banners de Advertencia
Autenticación, autorización y contabilidad
autenticación TACACS+
Autenticación Alternativa
Uso de Contraseñas Tipo 7
Autorización de Comandos con TACACS+
Contabilización de Comandos TACACS+
Servidores AAA Redundantes
Fortalezca el protocolo simple de administración de redes
Identificaciones de comunidad SNMP
Comunidades SNMP con ACL
ACL de Infraestructura
Vistas SNMP
Versión 3 de SNMP
Management Plane Protection
Prácticas Recomendadas de Registro
Envío de Registros a una Ubicación Central
Nivel de Registro
Inhabilitación de Registro en la Consola o en las Sesiones de Monitoreo
Uso de Registros Almacenados en Buffer
Configuración de la Interfaz de Origen de Registro
Configuración de Fechados de Registro
Administración de la Configuración de Cisco IOS Software
Configuration Replace y Configuration Rollback
Función Exclusive Configuration Change Access
Cisco IOS Software Resilient Configuration
Digitally Signed Cisco Software
Configuration Change Notification and Logging
Plano de Control
Consolidación del Plano de Control General
Mensajes de Redirección ICMP IP
Mensajes ICMP de Destino Inalcanzable
Proxy ARP
Limite el impacto del tráfico del plano de control sobre la CPU
Comprenda el tráfico del plano de control
ACL de Infraestructura
ACL de recepción
CoPP
Función Control Plane Protection

Limitadores de Velocidad Basados en Hardware
Proteja el protocolo BGP
Protecciones de Seguridad Basadas en TTL
Autenticación de Peer BGP con MD5
Configure el máximo de prefijos
Filtre los prefijos de BGP mediante listas de prefijos
Filtre los prefijos de BGP mediante listas de acceso a la ruta del sistema autónomo
Proteja los protocolos de gateway interior
Autenticación y Verificación de Protocolo de Ruteo con Message Digest 5
Comando Passive-Interface
Filtrado de Rutas
Consumo de Recursos del Proceso de Ruteo
Proteja los protocolos de redundancia de primer salto
Plano de Datos
Consolidación del Plano de Datos General
IP Options Selective Drop
Inhabilitación de Ruteo de Origen de IP
Inhabilitación de Mensajes de Redirección ICMP
Inhabilitación o Limitación de Broadcasts Dirigidos a IP
Filtre el tráfico en tránsito con ACL de tránsito
Filtrado de Paquetes ICMP
Filtrar fragmentos IP
ACL Support for Filtering IP Options
Protecciones Contra Suplantación
Unicast RPF
IP Source Guard
Seguridad de Puertos
Dynamic ARP Inspection
ACL Contra Suplantación
Limite el impacto del tráfico del plano de datos sobre la CPU
Funciones y Tipos de Tráfico que Afectan el CPU
Filtre por el valor de TTL
Filtre por la presencia de opciones de IP
Función Control Plane Protection
Identificación y Determinación del Origen del Tráfico
Netflow
ACL de Clasificación
Control de Acceso con VLAN Maps y Listas de Control de Acceso de Puerto
Control de Acceso con VLAN Maps
Control de Acceso con PACL
Control de Acceso con MAC
Uso de VLAN privadas
VLAN aisladas
VLAN Comunitarias
Puertos Promiscuos

Introducción

En este documento se presenta la información para ayudarlo a proteger sus dispositivos con sistemas Cisco IOS®, lo cual refuerza la seguridad general de su red. Este documento, que se basa en los tres planos en los cuales se pueden categorizar las funciones de un dispositivo de red, proporciona una descripción general de cada función incluida y referencias a documentación relacionada.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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

Antecedentes

Los tres planos funcionales de una red —plano de administración, plano de control y plano de datos— ofrecen diferentes funciones que se deben proteger.

- **Plano de administración:** Administra el tráfico enviado al dispositivo Cisco IOS y está compuesto por aplicaciones y protocolos como Shell seguro (SSH) y Protocolo simple de administración de redes (SNMP).

- **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).

- **Plano de datos:** Reenvía datos mediante un dispositivo de red. El plano datos no incluye el

tráfico que se envía al dispositivo IOS de Cisco 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 trate sobre la configuración segura de un dispositivo Cisco IOS, las configuraciones solas no aseguran totalmente 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. Los boletines y las respuestas de seguridad están disponibles en http://www.cisco.com/go/psirt.

Hay información adicional sobre estos medios de comunicación disponible en la Política de Vulnerabilidad 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 Determinación de Prioridad de los Riesgos para los Anuncios de Vulnerabilidad de la Seguridad a fin de obtener ayuda con 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 conocer mejor los eventos actuales, emergentes e históricos relativos a 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.

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

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 Proteja las sesiones de administración interactiva de este documento para ver más información sobre la administración segura de los dispositivos Cisco IOS.

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.

Encontrará más información sobre esta función en la sección Identificación y Determinación del Origen del Tráfico de este documento y en http://www.cisco.com/go/netflow (para clientes registrados solamente).

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 una configuración de un dispositivo Cisco IOS, dos aspectos adicionales de la administración de la configuración son fundamentales: seguridad y archivo de configuración.

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 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 usted utiliza para archivar las configuraciones de un dispositivo Cisco IOS debe ser asegurado. 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.

Estas secciones del documento abordan en detalle las funciones y las configuraciones de seguridad disponibles en Cisco IOS Software que ayudan a fortalecer el plano de administración.

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:

- Simple Network Management Protocol
- Telnet
- Secure Shell Protocol
- File Transfer Protocol
- Trivial File Transfer Protocol
- Secure Copy Protocol
- TACACS+
- RADIUS
- Netflow
- Network Time Protocol
- 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 con la definición de una contraseña o de un secreto que se utilice para autenticar 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 configurar la contraseña que concede acceso administrativo privilegiado al sistema Cisco IOS. 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** le indica a Cisco IOS Software que cifre las contraseñas, los secretos de Challenge Handshake Authentication Protocol (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 que contenga contraseñas cifradas debe tratarse con el mismo cuidado que se utiliza para una lista de texto sin formato 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, introducida en Cisco IOS Software Release 12.2(8)T, permite que un administrador configure el hash de contraseñas MD5 para el **comando username**. Antes de esta función, existían dos tipos de contraseñas: Tipo 0, que es una contraseña de texto no cifrado, y Tipo 7, que usa el algoritmo del cifrado Vigenère. 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>

!
```

Consulte Enhanced Password Security para obtener más información sobre esta función.

Login Password Retry Lockout

La función de bloqueo tras intentos fallidos de inicio de sesión agregada en la versión del software Cisco IOS 12.3(14)T le permite bloquear las cuentas de usuarios locales tras una cantidad configurable de intentos fallidos de inicio de sesión. 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.

Tenga en cuenta que los usuarios autorizados pueden bloquear su propio acceso a un dispositivo si alcanza el número configurado 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 attempts max-fail <max-attempts>
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 Cisco IOS Software Release 12.3(14)T y en versiones posteriores, la función No Service Password-Recovery no permite que ningún usuario con acceso a la consola acceda de manera 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 ofrece un procedimiento de recuperación de la contraseña accediendo al Modo de monitor de ROM (ROMMON) con la tecla Interrumpir durante la fase de 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 una vez que se habilita esta función, se elimina la configuración completa.

Consulte Ejemplo de configuración de ROMMON segura para ver más información sobre esta función.

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:

- echo (número del puerto 7)
- discard (número de puerto 9)
- daytime (número de puerto 13)
- 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 simples se inhabilitan de forma predeterminada en Cisco IOS Software Release 12.0 y versiones posteriores. 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:

- Ejecute el comando de configuración global **no ip finger** para inhabilitar el servicio Finger. Las versiones de Cisco IOS Software posteriores a 12.1(5) y a 12.1(5)T inhabilitan este servicio de forma predeterminada.
- Ejecute el comando de configuración global **no ip bootp server** para inhabilitar Bootstrap

Protocol (BOOTP).

- En Cisco IOS Software Release 12.2(8)T y versiones posteriores, ejecute el **comando ip dhcp bootp ignore** en modo de configuración global para inhabilitar BOOTP. De esta manera, quedan habilitados los servicios de Dynamic Host Configuration Protocol (DHCP).

- 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.

- Ejecute el **comando no mop enabled** en modo de configuración de interfaz para inhabilitar el servicio de Maintenance Operation Protocol (MOP).

- Ejecute el comando de configuración global **no ip domain-lookup** para inhabilitar los servicios de resolución del Sistema de Nombres del Dominio (DN).

- 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.

- 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**.

- A menos que los dispositivos Cisco IOS recuperen las configuraciones de la red durante el inicio, se debe utilizar el comando de configuración **no service config**. Esto impide que el dispositivo Cisco IOS intente hallar un archivo de configuración en la red con TFTP.

- 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.

- 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 configuration**para inhabilitar LLDP globalmente. LLDP también puede ser utilizado por un usuario malicioso para reconocimiento y mapping de red.

- Para el Switches que soporta el arranque del sdflash, la Seguridad puede ser aumentada iniciando del flash y inhabilitando el sdflash con el comando configuration de “ningún 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. Esta configuración garantiza que se pueda seguir accediendo al dispositivo en el extremo remoto de la conexión y que las conexiones semiabiertas o huérfanas sean eliminadas del dispositivo Cisco IOS 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

Con la función Memory Threshold Notification, agregada en Cisco IOS Software Release 12.3(4)T, usted puede atenuar las condiciones de poca memoria en un dispositivo. Esta función

emplea 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> !
```

Consulte Memory Threshold Notifications para obtener más información sobre esta función.

Notificación de Umbrales de CPU

Introducida en Cisco IOS Software Release 12.3(4)T, la función CPU Thresholding Notification le permite detectar y ser notificado si la carga del CPU en un dispositivo supera un umbral configurado. Cuando se supera el umbral, el dispositivo genera y envía un mensaje de trampa SNMP. Cisco IOS Software admite dos métodos de formación de umbrales para la utilización del CPU: umbral superior y umbral inferior.

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>
[falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

Consulte CPU Thresholding Notification para obtener más información sobre esta función.

Y

Memoria de reserva para acceso a la consola

En Cisco IOS Software Release 12.4(15)T y en versiones posteriores, la función Reserve Memory for Console Access se puede utilizar a fin de reservar bastante memoria para asegurar el acceso a la consola a un dispositivo Cisco IOS para fines de administración y de troubleshooting. Esta función es especialmente beneficiosa cuando el dispositivo funciona con poca memoria. Puede ejecutar el comando de configuración global **memory reserve console** para habilitar esta función. En este ejemplo se configura un dispositivo Cisco IOS para reservar 4096 kilobytes con este fin.

```
!
memory reserve console 4096
!
```

Consulte Reserve Memory for Console Access para obtener más información sobre esta función.

Detector de fugas de memoria

Introducida en Cisco IOS Software Release 12.3(8)T1, la función Memory Leak Detector le permite detectar agotamiento de memoria en un dispositivo. Se trata de una función que permite encontrar agotamiento en todos los bloques de memoria, los buffers de paquetes y tramos. El agotamiento de memoria es la asignación estática o dinámica de la memoria que no responde a ningún propósito útil. Esta función se centra en las asignaciones de memoria que son dinámicas. Usted puede utilizar el comando EXEC **show memory debug leaks** para detectar si existe un agotamiento de memoria.

Buffer Overflow: Detection and Correction of Redzone Corruption

En Cisco IOS Software Release 12.3(7)T y versiones posteriores, la función Buffer Overflow: Detection and Correction of Redzone Corruption se puede habilitar en un dispositivo para detectar y corregir un desbordamiento del bloque de memoria y para continuar con las operaciones.

Estos comandos de configuración global pueden ser utilizados para habilitar esta función. Una vez configurado, el comando **show memory overflow** se puede utilizar para visualizar las estadísticas de la detección y la corrección del desbordamiento del buffer.

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

Enhanced Crashinfo File Collection

La función Enhanced Crashinfo File Collection elimina automáticamente los viejos archivos crashinfo. Esta función, agregada en la versión del software Cisco IOS 12.3(11)T, permite que un dispositivo recupere espacio para crear nuevos archivos crashinfo cuando se bloquea. Esta función también permite que se guarde la configuración del número de archivos crashinfo.

```
!
exception crashinfo maximum files <number-of-files>
!
```

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. La hora exacta y confiable es necesaria para los fines de syslog, por ejemplo durante las investigaciones forenses de posibles ataques, así como para la conectividad VPN exitosa cuando se depende de certificados para la autenticación de Fase 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. Podrá encontrar más información sobre esta función en "huso horario del reloj" en la documentación del producto de Cisco.

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

Ejemplo de configuración mediante autenticación de 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
```

Servidor:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

Desactive Smart Install

Las mejores prácticas de seguridad relativas a la función Cisco Smart Install (SMI) dependen de cómo se emplee en cada entorno de cliente. Cisco distingue entre estos casos de uso:

- Clientes que no emplean la función Smart Install.
- Clientes que la emplean solo para implementación automatizada.
- Clientes que la emplean no solo para implementación automatizada (administración de imágenes y configuración).

En estas secciones se describen en detalle los escenarios:

- Clientes que no emplean la función Smart Install.
- Los clientes que no usan la función Cisco Smart Install, pero tienen una versión del software Cisco IOS y Cisco IOS XE donde está disponible el comando, deben desactivar la función mediante el comando **no vstack**.

> **Note**: El comando **vstack** se introdujo en la versión de Cisco IOS 12.2(55)SE03.

Este es un ejemplo de salida del comando **show vstack** en un switch Cisco Catalyst con la función

de cliente Smart Install desactivada:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Clientes que emplean la función Smart Install solo para implementación automatizada

Desactive la función de cliente Smart Install tras la instalación sin interacción, o emplee el comando **no vstack**.

Para propagar el comando **no vstack** en la red, use uno de estos métodos:

- Introduzca el comando **no vstack** en todos los switches clientes manualmente o mediante un script.
- Agregue el comando **no vstack** como parte de la configuración de Cisco IOS enviada a cada cliente de Smart Install durante la instalación sin interacción.
- En las versiones que no ofrecen el comando **vstack** (versión de Cisco IOS 12.2(55)SE02 y anteriores), aplique una lista de control de acceso (ACL) en los switches clientes para bloquear el tráfico del puerto TCP 4786.

Para activar la función de cliente Smart Install más adelante, introduzca el comando **vstack** en todos los switches clientes manualmente o mediante un script.

Clientes que emplean la función Smart Install no solo para implementación automatizada

Al diseñar arquitecturas de Smart Install, hay que tener cuidado de que solo la gente de confianza pueda acceder al espacio de la dirección IP de la infraestructura. En las versiones que no ofrecen el comando **vstack**, asegúrese de que solo el director de Smart Install tenga conectividad de TCP a todos los clientes de Smart Install en el puerto 4786.

Los administradores pueden usar estas mejores prácticas de seguridad para las implementaciones de Cisco Smart Install en dispositivos afectados:

- ACL de interfaz
- Políticas del plano de control (CoPP). Esta función no está disponible en todas las versiones del software Cisco IOS.

En este ejemplo se ve una ACL de interfaz donde la dirección IP del director de Smart Install es 10.10.10.1, mientras que la dirección IP del cliente de Smart Install es 10.10.10.200:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Esta ACL debe implementarse en todas las interfaces IP de todos los clientes. También se puede enviar mediante el director al implementar por primera vez los switches.

Para restringir aún más el acceso a todos los clientes de la infraestructura, los administradores pueden emplear estas mejores prácticas de seguridad en otros dispositivos de la red:

- Listas de control de acceso a la infraestructura (iACL)
- Listas de control de acceso a la VLAN (VACL)

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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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 la Protección de la Infraestructura para obtener más información sobre ACL a la 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 ofrece una función para filtrar específicamente los mensajes de 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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 emplea un método específico para buscar fragmentos no iniciales en las listas de acceso configuradas. Cisco IOS Software evalúa estos fragmentos no iniciales en relación con la ACL e ignora cualquier información de filtrado de la 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. Este escenario se muestra en esta configuración:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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

Cisco IOS Software Release 12.3(4)T incorporó soporte para el uso de ACL para filtrar paquetes IP sobre la base de 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Filtrado en ACL por el valor de TTL

En la versión del software Cisco IOS 12.4(2)T se ofrece en las ACL filtrado de paquetes de IP

basado en el 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 inferiores 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.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

> **Note**: Algunos protocolos hacen un uso legítimo de los paquetes con valores bajos de TTL. El protocolo eBGP es uno de ellos. 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.

Consulte Soporte ACL para Filtrar por Valor TTL para obtener más información sobre esta función.

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 del software Cisco IOS 12.4(6)T y posteriores, la función de protección del plano de administración (MPP) permite que los administradores definan en qué interfaces los dispositivos pueden recibir 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:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Consulte Management Plane Protection para más información sobre esta función.

Función Control Plane Protection

La función Control Plane Protection (CPPr) se basa en la función Control Plane Policing para restringir y supervisar el tráfico del plano de control que se dirige al procesador de ruta del dispositivo IOS. La función CPPr, agregada en Cisco IOS Software Release 12.4(4)T, divide el plano de control en categorías separadas que se conocen como subinterfaces. Existen tres subinterfaces del plano del control: Host, Transit y CEF-Exception. Además, CPPr incluye estas funciones adicionales para la protección del plano de control:

- **Filtrado de puertos:** Esta función permite controlar o rechazar paquetes que vayan a puertos UDP y TCP cerrados o sin escucha.

- **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.

> **Note**: CPPr no admite IPv6 y se ve limitado a la ruta de entrada IPv4.

Consulte Guía para la Función Control Plane Protection - 12.4T y Comprensión de Control Plane Protection para obtener más información sobre la función CPPr de Cisco.

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.

Los administradores pueden establecer conexiones de administración de acceso remoto seguras y encriptadas con dispositivos mediante las funciones SSH o HTTPS (Secure Hypertext Transfer Protocol). Cisco IOS Software es compatible con SSH versión 1.0 (SSHv1), con SSH versión 2.0 (SSHv2) y con HTTPS que utiliza Secure Sockets Layer (SSL) y Transport Layer Security (TLS) para la autenticación y el cifrado de datos. SSHv1 y SSHv2 no son compatibles. SSHv1 es inseguro y no está estandarizado, por lo cual no se recomienda si existe la opción de SSHv2.

El software Cisco IOS también admite Secure Copy Protocol (SCP), que permite una conexión encriptada y segura para copiar configuraciones de dispositivos o imágenes de software. El protocolo SCP depende de SSH. Este ejemplo de configuración habilita el protocolo SSH en un dispositivo Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Este ejemplo de configuración habilita los servicios de SCP:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Esto es un ejemplo de configuración para los servicios HTTPS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Consulte Configuración de Secure Shell en Routers y Switches que ejecutan Cisco IOS y Preguntas Frecuentes sobre Secure Shell (SSH) para obtener más información sobre la función SSH de Cisco IOS Software.

SSHv2

La función del soporte SSHv2 introducida en Cisco IOS Software Release 12.3(4)T permite que un usuario configure SSHv2. (El soporte SSHv1 fue implementado en una versión anterior de Cisco IOS Software). SSH se ejecuta sobre una capa de transporte confiable y ofrece sólidas capacidades de autenticación y cifrado. 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 no se configura explícitamente el comando **ip ssh version 2**, Cisco IOS activa 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 está activado SSH, se recomienda desactivar SSHv1 mediante el comando **ip ssh version 2**.

En este ejemplo de configuración se activa SSHv2 (con SSHv1 desactivado) en un dispositivo Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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

SSHv2 Enhancements for RSA Keys

La función SSHv2 de Cisco IOS admite los métodos de autenticación interactiva mediante teclado y basada 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 de SSH

de Cisco IOS 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 de servidor, el cliente SSH de Cisco IOS 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 con éxito, el establecimiento de sesión continúa; De lo contrario, se cancela la operación y se presenta el mensaje **Server Authentication Failed (Error de autenticación de servidor)**.

En este ejemplo de configuración se activa el uso de claves RSA con SSHv2 en un dispositivo Cisco IOS:

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

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

En este ejemplo de configuración se permite que el servidor de SSH de Cisco IOS realice la autenticación de usuario 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 a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
```

```
!

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

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

En este ejemplo de configuración se permite que el cliente de SSH de Cisco IOS realice la autenticación de servidor RSA.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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

Puertos de Consola y Auxiliar

En los dispositivos Cisco IOS, los puertos de consola y auxiliar (AUX) son líneas asincrónicas que se pueden utilizar para el acceso local o remoto a un dispositivo. Usted debe tener en cuenta que los puertos de consola en los dispositivos Cisco IOS 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 eliminar la capacidad de realizar el procedimiento de recuperación de contraseña con el comando de configuración global **no service password-recovery**. Sin embargo, una vez que se habilita 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:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Control de Líneas vty y tty

Las sesiones de administración interactivas en Cisco IOS Software utilizan una línea tty o una línea 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 tienen un número limitado de líneas vty; la cantidad de líneas disponible puede determinarse 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 se pueda seguir accediendo al dispositivo en el extremo remoto de la conexión y que las conexiones semiabiertas o huérfanas sean eliminadas del dispositivo Cisco IOS local.

Control del Transporte para Líneas vty y tty

Debe configurarse un vty y un tty para aceptar solo conexiones de administración de acceso remoto seguras y encriptadas a dispositivos o mediante dispositivos si se emplean como servidores de consolas. 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. Con el fin de evitar la divulgación de información o el acceso no autorizado a datos que se transmiten entre el administrador y el dispositivo, se debe utilizar **transport input ssh** en vez 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 debe utilizar el comando **transport output none**. Sin embargo, si se permiten conexiones salientes, se debe implementar un método de acceso remoto cifrado y seguro para la conexión con el uso de **transport output ssh**.

> **Note**: Puede usarse IPSec para conexiones de acceso remoto seguras y encriptadas a dispositivos, 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. Una forma de enviar esta notificación es incluir esta información en un banner que se configura con el comando banner login de Cisco IOS Software.

Los requisitos para las notificaciones legales son complejos, varían de acuerdo con la jurisdicción y la situación, y se deben tratar con un 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:

- 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.
- Notificación de que cualquier uso no autorizado del sistema es ilegal y de que puede estar sujeto a sanciones penales y civiles.
- 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.
- Notificaciones específicas que exigen las leyes locales.

De un punto de vista de la seguridad, más que desde el punto de vista legal, un banner de inicio de sesión no debe incluir 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 emplean los dispositivos Cisco IOS para autenticar a usuarios de administración a partir de un servidor AAA remoto. Estos usuarios de administración pueden acceder al dispositivo IOS 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 de finalidad similar a la de TACACS+; no obstante, solo encripta la contraseña enviada por la red. En cambio, TACACS+ encripta toda la carga útil de TCP, que incluye el nombre de usuario y la contraseña. Por esta razón, se recomienda el uso de TACACS+ en lugar de RADIUS cuando el servidor AAA admite el protocolo TACACS+. Consulte Comparación entre TACACS+ y RADIUS para obtener una comparación más detallada de estos dos protocolos.

La autenticación de TACACS+ se puede activar en los dispositivos Cisco IOS con una configuración similar a este ejemplo:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

La configuración anterior se puede utilizar como punto de partida para una plantilla de autenticación AAA específica de una organización. Consulte Autenticación, Autorización y Contabilización para obtener más información sobre la configuración de AAA.

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 emplea el primer método de la lista que logre aceptar o rechazar al 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 carecen de disponibilidad, un dispositivo Cisco IOS puede utilizar 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 de Cisco IOS Software que admiten el uso de contraseñas secretas para los usuarios localmente definidos, 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**:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
```

```
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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. Debe evitarse el uso de contraseñas Tipo 7, a menos que lo requiera una función en uso en el dispositivo Cisco IOS.

El tipo 9 (scrypt) debe ser utilizado siempre que sea posible:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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 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:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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 deben ser redundantes e implementados con tolerancia a fallas. 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:

- disponibilidad de los servidores de AAA durante las posibles fallas de la red;

- colocación geográficamente distribuida de los servidores de AAA;
- Cargue en servidores AAA individuales de condiciones estables de falla y estado
- latencia de red entre los servidores de acceso a la red y los servidores AAA;
- 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

En esta sección se resaltan varios métodos que se pueden utilizar para asegurar la implementación del protocolo SNMP dentro de los dispositivos IOS. 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. Hay que proteger esta información de los usuarios maliciosos que desean emplearla para lanzar ataques contra las redes.

Identificaciones de comunidad SNMP

Las comunidades son contraseñas que se aplican a un dispositivo IOS para restringir el acceso (de solo lectura y de lectura y escritura) a los datos SNMP en el dispositivo. Al igual que con todas las contraseñas, estas comunidades se deben elegir cuidadosamente para asegurarse de que no sean triviales. Se recomienda cambiar las comunidades regularmente y de acuerdo con las políticas de seguridad de la red. Por ejemplo, las comunidades se deben modificar cuando un administrador de red cambia los roles o deja la compañía.

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

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
```

```
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

> **Note**: Los ejemplos de cadenas de comunidad anteriores se eligieron para explicar con claridad el uso de estas cadenas. En los entornos de producción, las comunidades se deben elegir con cautela y deben incluir 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.

Consulte Referencia del Comando SNMP de IOS para obtener más información sobre esta función.

Comunidades SNMP con ACL

Además de la comunidad, se debe aplicar una ACL que restrinja aún más el acceso de SNMP a un grupo selecto de direcciones IP de origen. Esta configuración restringe el acceso de solo lectura de SNMP a los dispositivos host extremo que residen en el espacio de la dirección 192.168.100.0/24 y restringe el acceso de lectura y escritura de SNMP a solamente el dispositivo host extremo en 192.168.100.1.

> **Note**: Los dispositivos permitidos por estas ACL necesitan la cadena de comunidad correcta para acceder a la información de SNMP solicitada.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
```

```
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Para obtener más información sobre esta función, consulte Comunidad de servidores de snmp en la Guía de referencia de comandos de administración de redes de Cisco ISO.

ACL de Infraestructura

Se puede implementar ACL de infraestructura (iACL) para garantizar que solo los hosts finales con direcciones IP de confianza puedan enviar tráfico de SNMP a dispositivos IOS. Una iACL debe contener una política que niegue los paquetes SNMP no autorizados en el puerto UDP 161.

Consulte la sección Limitación del Acceso a la Red con Listas de Control de Acceso a la 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 una vista se crea y se aplica a una comunidad con los comandos de configuración global **snmp-server community** y **community-string view**, si usted accede a los datos de MIB, estará restringido a 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*:

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
```

```
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

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:

- **no auth**: Este modo no exige ninguna autenticación ni encriptación de paquetes de SNMP
- **auth**: Este modo exige la autenticación de los paquetes de SNMP sin encriptación
- **priv**: Este modo exige autenticación y encriptación (privacidad) de todos los paquetes de SNMP

Debe existir una ID de motor de autorización para utilizar los mecanismos de seguridad de SNMPv3 (autenticación, o bien, autenticación y encriptación) con los paquetes de SNMP; de manera 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
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

> **Note**: Si la ID de motor se modifica, deben reconfigurarse todas las cuentas de usuarios de SNMP.

El siguiente paso es configurar un grupo SNMPv3. Este comando configura los dispositivos Cisco IOS para SNMPv3 con un grupo de servidores SNMP AUTHGROUP y permite solo autenticación para este grupo con la palabra clave **auth**:

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Este comando configura los dispositivos Cisco IOS para SNMPv3 con un grupo de servidores SNMP PRIVGROUP, y permite autenticación y encriptación para este grupo con la palabra clave **priv**:

```
router#show snmp engineID
Local SNMP engineID: 80000090300000152BD35496
Remote Engine ID IP-addr Port
```

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

```
router#show snmp engineID
Local SNMP engineID: 80000090300000152BD35496
Remote Engine ID IP-addr Port
```

Observe que los comandos de configuración **snmp-server user** no aparecen en el resultado de la configuración del dispositivo según lo exige RFC 3414; por lo tanto, la contraseña del 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
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

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

Management Plane Protection

La función de protección del plano de administración (MPP) del software Cisco IOS puede emplearse para proteger el SNMP, ya que restringe las interfaces mediante las cuales el tráfico de 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.

Tenga en cuenta que el MPP es un subconjunto de la función CPPr y exige 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:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

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

Prácticas Recomendadas de Registro

El registro de eventos le permite ver el funcionamiento de un dispositivo Cisco IOS y la red en los cual está implementado. Cisco IOS Software ofrece varias opciones de registro flexibles que pueden ayudar a alcanzar las metas que tiene una organización con respecto a la administración y a la visibilidad de red.

Las secciones a continuación incluyen prácticas recomendadas de registro básicas que pueden ayudar a un administrador a aprovechar el registro con éxito y, al mismo tiempo, a minimizar el impacto que tiene el registro en un dispositivo Cisco IOS.

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 syslog son transmitidos de manera poco fiable por el protocolo UDP y en texto sin formato. Por este motivo, las protecciones que ofrecen las redes al tráfico de administración (por ejemplo, encriptación o acceso fuera de banda) deben ampliarse para incluir el tráfico de syslog.

En este ejemplo se configura un dispositivo Cisco IOS para enviar información de registros a un servidor syslog remoto:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

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

La función Logging to Local Nonvolatile Storage (ATA Disk), integrada en 12.4(15)T e introducida originalmente en 12.0(26)S, habilita el almacenamiento de los mensajes de registro del sistema en un disco Flash de conexión de tecnología avanzada (ATA). Los mensajes guardados en una unidad ATA persisten después de que se reinicie un router.

Estas líneas configuran 134 217 728 bytes (128 MB) de mensajes de registros al directorio de syslog del flash ATA (disk0), especificando un tamaño de archivo de 16 384 bytes:

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Antes de grabar los mensajes de registros en un archivo del disco ATA, el software Cisco IOS verifica que haya suficiente espacio en el 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 del archivo es log_month: **día: año:: hora**.

Note: Las unidades de memoria flash ATA tienen espacio limitado, por lo cual deben

mantenerse para no sobrescribir los 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
```

Consulte Registro en Almacenamiento No Volátil Local (disco ATA) para obtener más información sobre esta función.

Nivel de Registro

Cada mensaje del registro generado por un dispositivo Cisco IOS se asigna uno de ocho niveles de gravedad que van del nivel 0 (Emergencias) al nivel 7 (Debug). A menos que sea específicamente necesario, se le aconseja que evite el registro en el nivel 7 porque produce una carga del CPU elevada en el dispositivo que puede dar lugar a inestabilidad de la red y del dispositivo.

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):

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

Consulte Troubleshooting, Administración de Fallas y Registro para obtener más información.

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

Con el software Cisco IOS, se puede enviar mensajes de registros a la consola y a sesiones de monitoreo, que son sesiones de administración interactiva donde se ha emitido el comando EXEC **terminal monitor**. Sin embargo, esto puede elevar la carga de CPU de los dispositivos IOS y, por ende, 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:

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

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

Uso de Registros Almacenados en Buffer

Cisco IOS Software admite el uso de un buffer de registro local para que un administrador pueda

ver localmente los mensajes de registro generados. 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 relevantes al configurar el registro almacenado en buffer: el tamaño del buffer de registro y los niveles de gravedad de los mensajes que se guardan 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):

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

Consulte Referencia de Comandos de Administración de Red de Cisco IOS 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. Dicha configuración, que se realiza con el comando de interfaz **logging source-interface** , garantiza que la misma dirección IP aparezca en todos los mensajes de registro que se envíen 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:

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

Consulte Referencia de Comando de Cisco IOS 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. Los fechados de registro se deben configurar para incluir la fecha y hora con precisión de milisegundos y para incluir el huso horario que utiliza el dispositivo.

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

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

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):

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

Administración de la Configuración de Cisco IOS Software

Cisco IOS Software incluye varias funciones que pueden habilitar una forma de administración de la configuración en un dispositivo Cisco IOS. 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 del software Cisco IOS 12.3(7)T y las posteriores, las funciones de reemplazo de configuración y reversión de configuración le permiten archivar la configuración de dispositivos Cisco IOS en los dispositivos. 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 archivo***unning-config**. El comando **configure replace** *nombre de archivo* reemplaza la configuración actual en comparación con la fusión realizada por el comando copy.

Se recomienda que habilite esta función en todos los dispositivos Cisco IOS en 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. Este ejemplo le indica al dispositivo Cisco IOS que guarde las configuraciones archivadas como archivos con nombre *archived-config-N* en el disco 0: sistema de archivos, para mantener un máximo de 14 copias de respaldo y para archivar una vez por día (1440 minutos) y cuando un administrador publica el comando EXEC **write memory** .

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

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

La función Exclusive Configuration Change Access, agregada a Cisco IOS Software Release 12.3(14)T, garantiza que solamente un administrador haga cambios en la configuración de un dispositivo Cisco IOS 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 mediante el comando de configuración global **configuration mode exclusive** y opera en uno de 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:

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

Cisco IOS Software Resilient Configuration

En la versión del software Cisco IOS 12.3(8)T, la función de configuración de recuperabilidad permite almacenar de forma segura una copia de la imagen del software Cisco IOS y la configuración de dispositivo empleada actualmente por el dispositivo Cisco IOS. Cuando se habilita esta función, no es posible alterar o quitar estos archivos de respaldo. Se recomienda activar esta función para impedir que se eliminen estos archivos, ya sea por error o por ataques maliciosos.

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

Una vez que se habilita esta función, es posible restaurar una configuración eliminada o una imagen de Cisco IOS Software eliminada. El estado actual de esta función se puede consultar mediante el comando EXEC **show secure boot**.

Digitally Signed Cisco Software

En la versión del software Cisco IOS 15.0(1)M para los routers de las series Cisco 1900, 2900 y 3900 se agregó la función de software Cisco de firma digital, que permite emplear el software Cisco IOS de firma digital y, por ende, de confianza, mediante 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. Las imágenes de Cisco IOS regular y de ROMMON se firman con una clave de producción o especial al emplear la función de software Cisco de firma digital. 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 c3900-universalk9-mz.SSA en flash a partir de las claves almacenadas en el dispositivo:

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

La función Digitally Signed Cisco Software también fue integrada en Cisco IOS XE Release 3.1.0.SG para Cisco Catalyst 4500 E-Series Switches.

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

En la versión del software Cisco IOS 15.1(1)T y las posteriores, se introdujo el reemplazo de claves para esta función de firma digital. La función de reemplazo y revocación de claves reemplaza y elimina un clave que se utiliza para una verificación de Digitally Signed Cisco Software del almacenamiento de claves de una plataforma. Solamente las claves de tipo especial y de producción se pueden revocar en caso de que sea vean comprometidas.

Una nueva clave (de producción o especial) de una imagen (de producción o especial) viene en una imagen (de producción o revocación) empleada para revocar la clave de producción o especial anterior. La integridad de la imagen de revocación se verifica mediante una clave sustituta que viene prealmacenada en la plataforma. Las claves de renovación no cambian. Al revocar una clave de producción, tras cargarse la imagen de revocación, la nueva clave que lleva se agrega al almacén de claves y la correspondiente clave antigua puede revocarse, siempre y cuando se actualice la imagen de ROMMON y se arranque con la nueva imagen de producción. Al revocar una clave especial, se carga una imagen de producción. Esta imagen agrega la nueva clave especial y puede revocar la clave especial anterior. Tras actualizar ROMMON, se puede arrancar con la nueva imagen especial.

En este ejemplo se presenta la revocación de una clave especial. Estos comandos agregan la nueva clave especial al almacén de claves desde la imagen actual de producción, copian una nueva imagen de ROMMON (C3900_rom-monitor.srec.SSB) en el área de almacenamiento (usbflash0:), actualizan el archivo de ROMMON y revocan la antigua clave especial:

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

Luego se puede copiar una nueva imagen especial (c3900-universalk9-mz.SSB) en flash para cargarla, y la firma de la imagen se verifica mediante la clave especial recién agregada (.SSB):

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

La revocación y el reemplazo de claves no se ofrecen en los switches de la serie Catalyst 4500 E que emplean el software Cisco IOS XE, pero estos switches sí ofrecen la función de software Cisco de firma digital.

Consulte la sección Digitally Signed Cisco Software Key Revocation and Replacement de la guía Digitally Signed Cisco Software para obtener más información sobre esta función.

Configuration Change Notification and Logging

La función Configuration Change Notification and Logging, agregada en Cisco IOS Software Release 12.3(4)T, permite registrar los cambios realizados en la configuración de un dispositivo Cisco IOS. El registro se mantiene en el dispositivo Cisco IOS y contiene la información del usuario que hizo 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**. Las entradas de comando opcionales **hidekeys** y **logging size** se emplean para mejorar la configuración predeterminada, ya que impiden el registro de datos de contraseñas e incrementan la longitud del registro de cambios.

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

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/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. Si un evento del plano de datos, como un ataque de negación de servicio, afecta al plano de control, toda la red puede volverse inestable. La siguiente información sobre las configuraciones y las funciones de Cisco IOS Software puede ayudar a asegurar la resistencia del plano 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. Es decir, los mensajes de redirección ICMP nunca deben superar un límite de Capa 3.

Hay dos tipos de mensajes de redirección ICMP: mensaje de redirección para una dirección host y mensaje de 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 Cisco IOS Software, la generación de mensajes ICMP de destino inalcanzable se limita 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. El router "falsifica" su identidad para aceptar la responsabilidad de rutear los 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 de Proxy ARP para obtener más información sobre esta función.

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 como corresponde el plano de control de los dispositivos Cisco IOS, resulta esencial comprender los tipos de tráfico para los que la CPU hace switching mediante un proceso. Normalmente, el tráfico que se conmuta en el procesador puede ser de dos tipos diferentes. El primer tipo de tráfico es dirigido al dispositivo Cisco IOS y el CPU del dispositivo Cisco IOS debe manejarlo directamente. 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 es la misma para cualquier dirección IP que requiere el manejo directo de parte del CPU del dispositivo Cisco IOS, que incluye direcciones IP de la interfaz, espacio de dirección de multicast y espacio de dirección de broadcast.

El segundo tipo de tráfico que maneja la CPU es el del plano de datos (tráfico con un destino más allá del propio dispositivo Cisco IOS), el cual exige un procesamiento especial por parte de la CPU. Si bien esta no es una lista exhaustiva de tráfico del plano de datos que afecta al CPU, estos tipos de tráfico son conmutados en el procesador y pueden, por lo tanto, afectar el funcionamiento del plano de control:

- **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.

- **Reenvío de rutas inversas unicast (RPF unicast):** Se emplea en combinación con una ACL y puede generar switching mediante proceso de determinados paquetes.
- **Opciones de IP:** La CPU debe procesar todos los paquetes de IP que incluyan opciones.
- **Fragmentación:** La CPU debe recibir y procesar todos los paquetes de IP que exijan fragmentación.
- **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.
- **ICMP inalcanzables:** La CPU procesa los paquetes que resultan en mensajes de ICMP inalcanzable por routing, MTU o filtrado.
- **Tráfico que requiere una solicitud de ARP:** La CPU debe procesar los destinos para los cuales no existe ninguna entrada de ARP.
- **Tráfico que no es de IP:** La CPU procesa todo el tráfico que no es de IP.

Esta lista detalla varios métodos que permiten determinar qué tipos de tráfico procesa el CPU del dispositivo Cisco IOS:

- El comando **show ip cef** brinda información sobre el siguiente salto para cada prefijo IP incluido en la tabla CEF. Tal como se indicó previamente, las entradas que contienen el término receive como "Salto Siguiente" son consideradas receive adjacencies e indican que el tráfico se debe enviar directamente al CPU.
- El comando **show interface switching** brinda información sobre la cantidad de paquetes para la que el dispositivo hace switching por proceso.
- El comando **show ip traffic** brinda información sobre el número de paquetes IP:

  con un destino local (es decir, tráfico del tipo receive adjacency)con opcionesque requieren fragmentaciónque se envían al espacio de dirección de broadcastque se envían al espacio de dirección de multicast
- El tráfico del tipo receive adjacency puede ser identificado con el uso del **comando show ip cache flow**. Los flujos que se dirijan al dispositivo Cisco IOS tienen una interfaz de destino (DstIf) de *local*.
- **Control Plane Policing** se puede utilizar para identificar el tipo y la velocidad de tráfico que alcanza el plano de control del dispositivo Cisco IOS. 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

En el caso de plataformas distribuidas, las listas de control de acceso de recepción (rACL) pueden ser una opción para Cisco IOS Software Releases 12.0(21)S2 para 12000 (GSR), 12.0(24)S para 7500 y 12.0(31)S para 10720. 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 consecuencia, cualquier dirección IP de destino utilizada en las entradas de ACL del ejemplo a continuación solo hace referencia a la dirección IP física o virtual del router. Las ACL de recepción también se consideran una práctica recomendada de seguridad de la red y se deben tener en cuenta para una incorporación a largo plazo a fin de obtener 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:

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

Consulte GSR: Listas de Control de Acceso de Recepción para obtener ayuda con la identificación y el permiso del tráfico legítimo a un dispositivo y con la negación de 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, solamente el tráfico SSH de hosts confiables está permitido para alcanzar el CPU del dispositivo Cisco IOS.

> **Note**: Al rechazar el tráfico de direcciones IP desconocidas o poco confiables puede impedirse que hosts con direcciones IP dinámicas se conecten a los dispositivos Cisco IOS.

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

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.

La función CoPP está disponible en las versiones 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 y 12.4T de Cisco IOS Software.

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

Función Control Plane Protection

La función Control Plane Protection (CPPr), introducida en Cisco IOS Software Release 12.4(4)T, puede ser utilizada para restringir o supervisar el tráfico del plano de control de policía que se dirige al CPU del dispositivo Cisco IOS. 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:

- **Filtrado de puertos:** Esta función permite controlar y rechazar paquetes enviados a puertos UDP o TCP cerrados o sin escucha.

- **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 al dispositivo Cisco IOS contra una variedad de ataques que requieren que los paquetes sean procesados por el CPU.

Varios HWRL se encuentran habilitados de forma predeterminada. Consulte Configuraciones Predeterminadas de Limitador de Velocidad Basado en Hardware PFC3 para obtener más información.

Consulte Configuraciones Predeterminadas de Limitador de Velocidad Basado en Hardware PFC3 para obtener más información sobre HWRL.

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. Generalmente, esta función requiere la coordinación de los routers de peering; sin embargo, una vez habilitada, puede vencer totalmente muchos ataques basados de 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:

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

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:

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

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 guardar un subconjunto de todos los prefijos de Internet, como en configuraciones que utilizan solamente una ruta predeterminada o rutas para las redes de cliente 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.

Al configurar esta función con el comando de configuración de router BGP **neighbor maximum-prefix**, hace falta un argumento: el número máximo de prefijos que se aceptan antes de que se apague un peer. 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.

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

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. Siempre que sea posible deben usarse listas de prefijos, para garantizar que el tráfico de red se envíe por las rutas previstas. Las listas de prefijos se deben aplicar a cada peer eBGP en los directorios 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, una lista de prefijos se debe configurar 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 deben configurar para permitir específicamente solo los prefijos que una organización se propone publicar.

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.

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

Consulte Conexión con un Proveedor de Servicio Usando BGP Externo para obtener información completa sobre el 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.

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

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. Puede usar la autenticación de contraseña con los protocolos de ruteo entre routers para contribuir con 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.

Mediante la incorporación de capacidades de hash MD5 al proceso de autenticación, las actualizaciones de ruteo dejan de contener contraseñas de texto sin formato y el contenido entero de la actualización de ruteo se vuelve más resistente a las alteraciones. 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 de router EIGRP con MD5:

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

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

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

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

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

Consulte Configuración de OSPF para obtener más información.

Comando Passive-Interface

Las filtraciones de información o la introducción de información falsa en un IGP pueden ser atenuadas con el uso del **comando passive-interface** que contribuye con el control de la publicación 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:

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

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:

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

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

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

Consulte Configuración de funciones de routing de IP independientes del protocolo para ver más información sobre cómo controlar la difusión y el procesamiento de las actualizaciones de routing.

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

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

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:

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

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 impedir este tipo de ataques, todos los FHRP compatibles con el software Cisco IOS incluyen un recurso de autenticación con cadenas de texto o MD5. 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:

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

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 en el procesador por los dispositivos Cisco IOS, esto puede significar una carga elevada para el CPU. 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 Cisco IOS Software Releases 12.3(4)T, 12.0(22)S y 12.2(25)S. Con el primer formato de este comando, **ip options drop**, todos los paquetes de IP con opciones de IP recibidos por el dispositivo Cisco IOS se rechazan. 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 para ignorar las opciones IP 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:

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

Tenga en cuenta que algunos protocolos, como 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 de IP, habilitado de forma predeterminada en todas las versiones de Cisco IOS Software, se inhabilita con el comando de configuración global **no ip source-route**. Este ejemplo de configuración ilustra el uso de este comando:

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

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, Cisco IOS Software envía un mensaje de redirección si recibe un paquete que se debe rutear a través de la interfaz por la cual fue recibido.

En algunas situaciones, quizás sea posible que un atacante obligue al dispositivo Cisco IOS a enviar muchos mensajes de redireccionamiento de ICMP, lo cual eleva la carga de la CPU. 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:

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

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 broadcasts dirigidos ha sido aprovechada como ayuda de amplificación y reflexión en varios ataques, incluido el ataque smurf.

Las versiones actuales de Cisco IOS Software tienen esta función inhabilitada de forma predeterminada; sin embargo, puede ser habilitada con el comando de configuración de interfaz **ip directed-broadcast**. Las versiones de Cisco IOS Software anteriores a 12.0 tienen esta función habilitada de manera predeterminada.

Si una red requiere absolutamente la función de broadcasts dirigidos, su uso debe 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:

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

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 podría ser provechoso realizar este filtrado en un dispositivo Cisco IOS en la red, por ejemplo, si se debe realizar un filtrado pero no hay 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 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 transporta pueden tener ramificaciones de gran 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, rara vez se necesita la conectividad ICMP externa para el correcto funcionamiento de una red.

Cisco IOS Software proporciona una función para filtrar mensajes ICMP específicamente 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:

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

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 suelen usarse en ataques y se deben filtrar explícitamente en las tACL configuradas. La ACL que figura abajo incluye el filtrado completo de fragmentos IP. La función ilustrada en este ejemplo se debe utilizar junto con la función de los ejemplos anteriores:

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

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

En la versión del software Cisco IOS 12.3(4)T y las posteriores, el software admite el uso de ACL para filtrar los paquetes de IP según las opciones de IP que contengan. La presencia de opciones de IP dentro de los paquetes podría indicar un intento de sortear los controles de seguridad de la red o alterar las características del tránsito del 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 el contenido de los ejemplos anteriores para incluir el filtrado de paquetes IP que contienen opciones IP:

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

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 ofrece RPF unicast y protección de IP de origen (IPSG) para disuadir los ataques donde se falsifica 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 suplantados podrían ingresar a la red a través de una interfaz habilitada para Unicast RPF si existe una ruta de regreso

a la dirección IP de origen apropiada. Con RPF unicast, usted debe activar Cisco Express Forwarding en cada dispositivo, y la configuración se hace en cada interfaz.

Unicast RPF se puede configurar de dos maneras: flexible 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:

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

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:

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

Después de que se habilite la función DHCP snooping, estos comandos habilitan IPSG:

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

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 82 de DHCP.

Consulte Configuración de funciones de DHCP y de IP Source Guard para obtener más información sobre esta función.

Seguridad del puerto

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. Cuando un puerto brinda acceso a una sola estación de trabajo mediante el uso de protocolos estándar, un máximo de uno puede ser suficiente. Los protocolos que utilizan direcciones MAC virtuales, como HSRP, no funcionan cuando el número máximo se configura en uno.

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

Consulte Configuración de la seguridad de puertos para ver más información.

Dynamic ARP Inspection

La inspección dinámica de ARP (DAI) puede usarse para mitigar los ataques de contaminación de ARP en los segmentos locales. Un ataque mediante envenenamiento ARP es un método en el cual un atacante envía información sobre ARP falsificada a un segmento local. Esta información está pensada para dañar la caché de ARP de otros dispositivos. Un atacante utiliza a menudo el envenenamiento ARP para realizar un ataque por desconocido.

La función DAI intercepta y valida la relación de dirección de IP a MAC de todos los paquetes ARP en los puertos no confiables. En los entornos de DHCP, DAI emplea los datos generados por la función de detección DHCP. No se validan los paquetes ARP que se reciben en interfaces confiables y se descartan los paquetes no válidos en las interfaces no confiables. En entornos no DHCP, se necesita usar ACL ARP.

Estos comandos habilitan la función DHCP snooping:

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

Una vez habilitada la función DHCP snooping, estos comandos habilitan la función DAI:

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

En entornos no DHCP, se necesitan ACL ARP para habilitar la función DAI. Este ejemplo demuestra la configuración básica de DAI con ACL ARP:

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

DAi puede también ser habilitado encendido por la base de la interfaz soportada dondequiera que.

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

Consulte Configuración de Dynamic ARP Inspection para obtener más información sobre cómo configurar DAI.

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.

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

Consulte Configuración de ACL IP de Uso Frecuente para obtener más información sobre cómo configurar Listas de Control de Acceso.

Team Cymru se encarga de mantener la lista oficial de direcciones de Internet. Podrá encontrar información adicional sobre el filtrado de direcciones sin usar en la Página de Referencia de Bogon.

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 los dispositivos de redes, debe protegerse para garantizar el funcionamiento de los planos de administración y control. Si el tráfico de tránsito puede hacer que un dispositivo conmute el tráfico en el procesador, el plano de control de un dispositivo puede verse afectado y esto puede producir una interrupción en el funcionamiento operativo.

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:

- **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**.
- **RPF unicast:** Se emplea en combinación con una ACL y puede generar switching mediante proceso de determinados paquetes.
- **Opciones de IP:** La CPU debe procesar todos los paquetes de IP que incluyan opciones.
- **Fragmentación:** La CPU debe recibir y procesar todos los paquetes de IP que exijan fragmentación.
- **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.
- **ICMP inalcanzables:** La CPU procesa los paquetes que resultan en mensajes de ICMP inalcanzable por routing, MTU o filtrado.
- **Tráfico que requiere una solicitud de ARP:** La CPU debe procesar los destinos para los cuales no existe ninguna entrada de ARP.
- **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

Usted puede utilizar la función ACL Support for Filtering on TTL Value, introducida en Cisco IOS Software Release 12.4(2)T, en una lista de acceso IP ampliada para filtrar los paquetes en función del 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 los valores TTL también se puede utilizar para asegurarse de que el valor TTL no sea más bajo que el diámetro de la red, y de esta manera se protege el plano de control de los dispositivos de infraestructura de flujo descendente contra los ataques basados en vencimiento de TTL.

Tenga en cuenta que algunas aplicaciones y herramientas, como **traceroute**, utilizan los paquetes con vencimiento de TTL con fines de diagnóstico y de evaluación. 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.

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

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.

En la versión del software Cisco IOS 12.4(4)T y las posteriores, la concordancia flexible de paquetes (FPM) permite que el administrador compare bits de los paquetes de manera arbitraria. Esta política FPM descarta paquetes con un valor TTL inferior a seis.

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

Consulte Flexible Packet Matching, en la página de inicio Cisco IOS Flexible Packet Matching para obtener más información sobre la función.

Filtre por la presencia de opciones de IP

En la versión del software Cisco IOS 12.3(4)T y las posteriores, puede utilizar la función de filtrado de opciones de IP en una lista de acceso de IP ampliada y determinada, a fin de filtrar los paquetes de IP con opciones de IP presentes. El filtrado de paquetes IP que se basa en la presencia de opciones IP también se puede utilizar para evitar que el plano de control de dispositivos de infraestructura tenga que procesar estos paquetes en el CPU.

Tenga en cuenta que la función ACL Support for Filtering IP Options se puede utilizar solamente con ACL ampliadas y con nombre. Cabe señalar también que la ingeniería de tráfico de switching por etiquetas multiprotocolo, las versiones 2 y 3 de IGMP y otros protocolos que emplean paquetes de opciones IP quizás no funcionen bien si se rechazan sus paquetes. Si estos protocolos se utilizan en la red, entonces se puede usar la función ACL Support for Filtering IP Options; sin embargo, la función de rechazo selectivo de opciones de IP de ACL puede rechazar este tráfico, y estos protocolos quizás no funcionen bien. 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:

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

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:

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

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

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

Consulte Listas de Control de Acceso de Tránsito: Filtrado en el Borde para obtener más información sobre el filtrado de tráfico de borde y de tránsito.

Otra función que ofrece Cisco IOS Software y que se puede utilizar para filtrar los paquetes con opciones IP es CoPP. En la versión del software Cisco IOS 12.3(4)T y las posteriores, con CoPP el administrador puede filtrar el flujo de tráfico de los paquetes del plano de control. Un dispositivo compatible con CoPP y con ACL Support for Filtering IP Options, introducidos en Cisco IOS Software Release 12.3(4)T, puede utilizar una política de lista de acceso para filtrar los paquetes que contienen opciones IP.

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

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

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

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

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

En las políticas CoPP precedentes, las entradas de la lista de control de acceso (ACE) que coinciden con los paquetes mediante la acción *permit* producen que estos paquetes sean descartados por la función *drop* de policy-map, mientras que los paquetes que coinciden mediante la acción *deny* (no mostrada) 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 del software Cisco IOS 12.4(4)T y las posteriores, se puede emplear la protección del plano de control (CPPr) para restringir o controlar el tráfico del plano de control de la CPU de los dispositivos Cisco IOS. Si bien es similar a la función CoPP, CPPr tiene la capacidad de restringir el tráfico con granularidad más fina. CPPr divide el plano de control general en tres categorías independientes, conocidas como subinterfaces. Existen las 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.

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

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 Comprensión de la Protección del Plano de Control y Protección del Plano de Control para obtener más información sobre la función CPPr.

Identificación y Determinación del Origen del Tráfico

A veces, usted puede necesitar identificar y determinar rápidamente el origen del tráfico de la red, especialmente durante una respuesta a un incidente o un rendimiento deficiente de la red. Las ACL de clasificación y NetFlow son los dos métodos principales para lograr esto con el software Cisco IOS. Netflow permite ver todo el tráfico en la red. Además, Netflow se puede implementar con colectores que pueden proporcionar tendencia a largo plazo y análisis automatizado. 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.

Se necesita CEF o CEF distribuido para activar NetFlow. Netflow se puede configurar en routers y switches.

El siguiente ejemplo ilustra la configuración básica de esta función. En las versiones anteriores de Cisco IOS Software, el comando para habilitar el Netflow en una interfaz es **ip route-cache flow** en vez de **ip flow {ingress | egress}**.

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

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 total packets):
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

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /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-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 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 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Consulte Netflow de Cisco IOS para obtener más información sobre las capacidades de Netflow.

Consulte Introducción a Netflow de Cisco IOS: Una descripción Técnica General para obtener una descripción técnica general 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. El administrador también puede dividir la denegación implícita al final de una ACL en varias ACE, para identificar los tipos de tráficos denegados.

Un administrador puede acelerar una respuesta a un incidente usando 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:

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
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

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /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-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 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 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Para identificar el tráfico que utiliza una ACL de clasificación, utilice el comando EXEC **show access-list acl-name**. Los contadores de ACL pueden regresarse a cero mediante 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 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

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 VLAN Maps y Listas de Control de Acceso de Puerto

Las Listas de Control de Acceso a VLAN (VACL), o VLAN maps y ACL de puerto (PACL), proporcionan la capacidad de implementar control de acceso en tráfico no ruteado que está más cercano a los dispositivos extremos que las listas de control de acceso que se aplican a las interfaces ruteadas.

Las siguientes secciones proporcionan una descripción general de las funciones, las ventajas y los escenarios de uso potencial de las VACL y las PACL.

Control de Acceso con VLAN Maps

Las VACL, o VLAN maps que se aplican a todos los paquetes que ingresan en la VLAN, proporcionan la capacidad de implementar control de acceso en el tráfico intra-VLAN. Esto no es posible con las ACL de interfaces con routing. Por ejemplo, podría usarse un mapa de VLAN para impedir que los hosts de una misma VLAN se comuniquen entre sí, lo cual reduce la probabilidad de que gusanos o atacantes locales se aprovechen de un host en el mismo segmento de red. Para impedir que los paquetes usen una VLAN map, usted puede crear un lista de control de acceso (ACL) que coincida con el tráfico y, en la VLAN map, configurar la acción para descartarla. Una vez que se configura una lista de acceso VLAN map, todos los paquetes que ingresan a la LAN se evalúan secuencialmente en relación con VLAN map configurada. Las listas de acceso VLAN maps son compatibles con las listas de acceso IPv4 y MAC; sin embargo, no admiten registro ni ACL IPv6.

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

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
```

```
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

En este ejemplo se muestra el uso de un mapa de VLAN para denegar los puertos TCP 139 y 445, y el protocolo vines-ip:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Consulte Configuración de la Seguridad de la Red con ACL para obtener más información sobre la configuración de VLAN maps.

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:

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

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

Control de Acceso con MAC

Las listas de control de acceso MAC o las listas extendidas se pueden aplicar en la red IP con el uso de este comando en el modo de configuración de interfaz:

```
Cat6K-IOS(config-if)#mac packet-classify
```

> **Note**: Los paquetes de Capa 3 se deben clasificar como paquetes de Capa 2. El comando es compatible con Cisco IOS Software Release 12.2(18)SXD (para Sup 720) y Cisco IOS Software Release 12.2(33)SRA o versiones posteriores.

Este comando de interfaz debe ser aplicado en la interfaz de ingreso y le indica al motor de reenvío que no examine el encabezado IP. El resultado es que usted puede utilizar una lista de acceso MAC en el entorno IP.

Uso de VLAN privadas

Las VLAN privadas (PVLAN) son una función de seguridad de la Capa 2 que limita la conectividad entre las estaciones de trabajo o los servidores dentro de una VLAN. Sin las PVLAN, todos los dispositivos de las VLAN de la capa 2 pueden comunicarse libremente. Existen situaciones de networking en las que la seguridad puede ser ayudada mediante la limitación de la comunicación entre los dispositivos en una sola VLAN. Por ejemplo, las PVLAN sueles usarse para prohibir la comunicación entre los servidores en una subred de acceso público. Si un servidor se viera comprometido, la falta de conexión con los demás servidores por la aplicación de las PVLAN contribuiría a limitar el problema a ese servidor.

Hay tres tipos de VLAN privadas: VLAN aisladas, VLAN comunitarias y VLAN primarias. Para configurar PVLAN, se utiliza VLAN primarias y secundarias. La VLAN primaria contiene todos los puertos promiscuos, que se describen más adelante, e incluye una o más VLAN secundarias, que pueden ser VLAN aisladas o comunitarias.

VLAN aisladas

La configuración de una VLAN secundaria como VLAN aislada previene totalmente la comunicación entre los dispositivos en la VLAN secundaria. Quizás haya una sola VLAN aislada por cada VLAN principal, y solo los puertos promiscuos pueden comunicarse con los puertos de las VLAN aisladas. Las VLAN aisladas se deben utilizar en redes poco confiables como redes que admiten huéspedes.

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

```
Cat6K-IOS(config-if)#mac packet-classify
```

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.

```
Cat6K-IOS(config-if)#mac packet-classify
```

Puertos Promiscuos

Los puertos del switch que se colocan en la VLAN primaria se conocen como puertos promiscuos. Los puertos promiscuos pueden comunicarse con el resto de los puertos en las VLAN primaria y secundaria. Las interfaces de router o firewall son los dispositivos que se encuentran más

comúnmente en estas VLAN.

Este ejemplo de configuración combina los ejemplos de VLAN aislada y comunitaria anteriores y agrega la configuración de la interfaz FastEthernet 1/12 como puerto promiscuo:

```
Cat6K-IOS(config-if)#mac packet-classify
```

Al implementar las PVLAN, es importante asegurarse de que la configuración de la capa 3 admita las restricciones impuestas por las PVLAN y no permita que se sortee la configuración de las PVLAN. El filtrado de la capa 3 con un firewall o una ACL de router puede impedir que se sortee la configuración de las PVLAN.

Consulte VLAN Privadas (PVLAN): Puertos Promiscuos, VLAN Aislada y VLAN Comunitaria, en la página de inicio de Seguridad de LAN, para obtener más información sobre el uso y la configuración de VLAN Privadas.

Conclusión

Este documento le da una amplia descripción general de los métodos que se pueden utilizar para asegurar un dispositivo del sistema de Cisco IOS. 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 Verificación para la Consolidación de Dispositivo Cisco IOS

Esta lista de verificación es una colección de todos los pasos de consolidación que se presentan en esta guía. Los administradores pueden utilizarla como recordatorio de todas las funciones de consolidación utilizadas y consideradas para un dispositivo Cisco IOS, incluso si una función no fue implementada porque no correspondió. Se recomienda a los administradores evaluar los riesgos de cada opción antes de implementarla.

Plano de Administración

- Contraseñas

  Habilitar hash MD5 (opción de secreto) para contraseñas de usuario local y de habilitaciónConfigurar el bloqueo de nuevo intento de contraseñaInhabilitar la recuperación de contraseña (considerar el riesgo)

- Inhabilitación de servicios no utilizados
- Configurar keepalives TCP para las sesiones de administración
- Configurar notificaciones del umbral de CPU y de memoria
- Configurar

  Notificaciones de umbral de CPU y de memoriaMemoria de reserva para acceso a la consolaDetector de fugas de memoriaDetección del desbordamiento de bufferRecolección de archivos crashinfo mejorada
- Utilizar iACL para restringir el acceso de administración
- Filtrar (considerar el riesgo)

  Paquetes ICMPFragmentos IPOpciones IPValor TTL en los paquetes
- Función Control Plane Protection

  Configurar filtrado de puertoConfigurar umbrales de cola
- Acceso de administración

  Utilizar la función Management Plane Protection para restringir las interfaces de administraciónConfigurar el tiempo de espera de execUtilizar un protocolo de transporte cifrado (como SSH) para el acceso de CLIControlar el transporte para las líneas vty y tty (opción de clase de acceso)Usar banners de advertencia
- AAA

  Utilizar AAA para autenticación y autenticación alternativaUtilizar AAA (TACACS+) para autorización de comandosUtilizar AAA para contabilizaciónUtilizar servidores AAA redundantes
- SNMP

  Configurar comunidades SNMPv2 y aplicar ACLConfigurar SNMPv3
- Registro

  Configurar registro centralizadoConfigurar niveles de registro para todos los componentes relevantesConfigurar la interfaz de origen de registroConfigurar granularidad de fechado de registro
- Administración de la Configuración

Reemplazo y restauraciónFunción Exclusive Configuration Change AccessConfiguración de resistencia del softwareNotificaciones de cambios en la configuración

Plano de Control

- Inhabilitar (considerar el riesgo)

  Mensajes de redirección ICMPMensajes ICMP de Destino InalcanzableProxy ARP

- Configurar autenticación NTP si se está utilizando NTP
- Configurar la función Control Plane Policing/Protection (filtrado de puerto, umbrales de cola)
- Asegurar los protocolos de seguridad

  BGP (TTL, MD5, prefijos máximos, listas de prefijos, ACL de trayectoria del sistema)IGP (MD5, interfaz pasiva, filtrado de rutas, consumo de recursos)

- Configurar limitadores de velocidad basados en hardware
- Asegurar los Protocolos de Redundancia de Primer Salto (GLBP, HSRP, VRRP)

Plano de Datos

- Configurar la función IP Options Selective Drop
- Inhabilitar (considerar el riesgo)

  Ruteo de origen IPBroadcasts dirigidos a IPMensajes de redirección ICMP

- Limitar broadcasts dirigidos a IP
- Configurar TACL (considerar el riesgo)

  Filtrar ICMPFiltrar fragmentos IPFiltrar opciones IPFiltrar valores TTL

- Configurar las protecciones contra suplantación requeridas

  Listas de control de acceso (ACL)IP Source GuardDynamic ARP InspectionUnicast RPFSeguridad del puerto

- Función Control Plane Protection (cef-exception del plano de control)
- Configurar Netflow y ACL de clasificación para la identificación del tráfico
- Configurar ACL de control de acceso requeridas (VLAN maps, PACL, MAC)

- Configurar VLAN privadas