Guía de Cisco para endurecer los dispositivos Cisco IOS

Contenido

Cifre a 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
Fortifique el protocolo administración de red simple
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
Impacto del límite CPU del tráfico del plano del control
Entienda el tráfico del plano del control
ACL de Infraestructura
ACL de recepción
CoPP
Función Control Plane Protection

Introducción

Este documento describe la información para ayudarle a asegurar sus dispositivos del sistema del ® del Cisco IOS, que aumenta 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** - El plano de administración maneja el tráfico que se envía al dispositivo Cisco IOS y se compone de las aplicaciones y de los protocolos tales como Secure Shell (SSH) y Simple Network Management Protocol (SNMP).

- **Avión del control** - El avión del control de un dispositivo de red procesa el tráfico que es supremo mantener las funciones de la infraestructura de 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).

- **Avión de los datos** - De los datos del avión los datos adelante a través de 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 del Authentication, Authorization, and Accounting (AAA) es vital asegurar los dispositivos de red. 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. Vea la sección del autenticación, autorización y contabilidad de este documento para más información sobre cómo leverage el AAA.

Centralización de Monitoreo y Colección de Registros

Para ganar el conocimiento sobre la existencia, emergiendo, y los eventos históricos se relacionaron con los incidentes de seguridad, su organización debe tener una estrategia unificada para el registro de evento y la correlación. 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.

Vea la sección interactiva segura de las Sesiones de administración de este documento para 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 a las Sesiones de administración interactivas que utilizan SSH, así como estadística-recolectan con el SNMP o el 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 asegurar el plano de administración y el avión del control de un dispositivo, porque las operaciones del avión del control afectan directamente a las operaciones 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, observe que una contraseña localmente configurada para el acceso privilegiado todavía está necesitada en caso de error del TACACS+ o de servicios RADIUS. 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. Sin embargo, el algoritmo usado por el **comando service password-encryption** es un Vigen simple con referencia a la cifra. 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 sin cifrar, y tipo 7, que utiliza el algoritmo del Vigen con referencia a la cifra. 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 característica del cierre de la recomprobación de la contraseña de inicio de sesión, agregada en el Cisco IOS Software Release 12.3(14)T, permite que usted bloquee hacia fuera una cuenta de usuario local después de un número configurado de intentos de inicio de sesión fracasados. 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 Cisco IOS Software proporciona un procedimiento para recuperación de contraseña que confíe en el acceso al modo de monitor de ROM (ROMMON) usando la tecla de interrupción durante el inicio del sistema. En el ROMMON, el software del dispositivo se puede recargar para indicar una nueva configuración del sistema que incluya 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 ninguna característica del password-recovery del servicio previene la realización de la secuencia de la tecla BREAK y ingresar del ROMMON durante el inicio del sistema.

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.

Refiera al ejemplo de configuración seguro ROMMON para más información sobre esta característica.

Inhabilitación de servicios no utilizados

Como práctica recomendada de seguridad, todo servicio que no sea necesario debe ser inhabilitado. Utilizan para los propósitos legítimos pero pueden ser utilizados a estos servicios innecesarios, especialmente los que utilicen el User Datagram Protocol (UDP), infrecuentemente para poner en marcha el DOS y los otros ataques que son prevenidos de otra manera por 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 ser inhabilitado con el **comando no ip http server** en el modo de configuración global, y el servidor seguro HTTP (HTTPS) se puede inhabilitar con el **ningún ip http** comando global configuration del **servidor seguro**.

- 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 previene el dispositivo Cisco IOS de una tentativa de localizar un archivo de configuración en la red con el 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.

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. Por abandono, las sesiones son disconnected después de diez minutos de inactividad.

```
!

line con 0
exec-timeout <minutes> [seconds]
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

Keepalives para Sesiones TCP

El servicio TCP-Keepalives-en y los comandos global configuration del TCP-**Keepalives-hacia fuera del servicio** permiten a un dispositivo para enviar los keepalifes TCP para las sesiones 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 característica utiliza dos métodos para lograr esto: Memory Threshold Notification y Memory Reservation.

La función Memory Threshold Notification genera un mensaje de registro para indicar que la memoria libre de un dispositivo se ha reducido por debajo del umbral configurado. Este ejemplo de configuración muestra cómo habilitar esta función con el comando de configuración global

memory free low-watermark. Este comando habilita a un dispositivo para que genere una notificación cuando la memoria libre disponible se reduce por debajo del umbral especificado y para que vuelva a generar una notificación cuando la memoria libre disponible aumenta en un cinco por ciento más que el umbral especificado.

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

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

```
!
memory reserve critical <value> !
```

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 característica, agregada en el Cisco IOS Software Release 12.3(11)T, permite que un dispositivo reclame el espacio para crear los nuevos archivos CRASHINFO cuando el dispositivo causa un crash. 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.

- **Huso horario NTP** - Cuando usted configura el NTP, el huso horario necesita ser configurado para poder correlacionar exactamente los grupos fecha/hora. Hay generalmente dos acercamientos para configurar el huso horario para los dispositivos en una red con una

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 NTP** - Si usted configura autenticación NTP, ofrece la garantía que los mensajes NTP están intercambiados entre los pares de confianza NTP.

Configuración de muestra usando autenticación NTP:

Cliente:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

Servidor:

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

La neutralización Smart instala

Las mejores prácticas de la Seguridad alrededor de Cisco Smart instalan la característica (S I) dependen de cómo la característica se utiliza en un entorno del cliente específico. Cisco distingue estos casos del uso:

- Los clientes que no utilizan el Smart instalan la característica.
- Los clientes que leverage Smart instalan la característica solamente para el despliegue del cero-tacto.
- Los clientes que leverage Smart instalan la característica para más que el despliegue del cero-tacto (Administración de la configuración y de la imagen).

Estas secciones describen cada escenario detalladamente:

- Los clientes que no utilizan Smart instalan la característica.
- Los clientes que no utilizan Cisco Smart instalan la característica, y funcionan con una versión del Cisco IOS y el Software Cisco IOS XE donde está disponible el comando, debe inhabilitar Smart instala la característica con el **ningún** comando del **vstack**.

  Nota: El comando del **vstack** fue introducido en el Cisco IOS Release 12.2(55)SE03.

Ésta es salida de muestra del comando del **vstack de la demostración** en un Switch del Cisco Catalyst con Smart instala la función de cliente inhabilitada:

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

Los clientes que Leverage Smart instalan la característica solamente para el despliegue del Cero-tacto

Inhabilite Smart instalan la funcionalidad del cliente después de que la instalación del cero-tacto sea completa o no utilizan el **ningún** comando del **vstack**.

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

- No ingrese el **ningún** comando del **vstack** en todo el cliente conmuta manualmente o con un script.
- No agregue el **ningún** comando del **vstack** como parte de la configuración del Cisco IOS que se avanza en cada Smart instala al cliente como parte de la instalación del cero-tacto.
- En las versiones que no soportan el comando del **vstack** (versiones del Cisco IOS Release 12.2(55)SE02 y Anterior), aplique un Access Control List (ACL) en el Switches del cliente para bloquear el tráfico en el puerto TCP 4786.

Para habilitar el elegante instale la funcionalidad del cliente más adelante, ingrese el comando del **vstack** en todo el cliente conmuta manualmente o con un script.

Los clientes que Leverage Smart instalan la característica para más que el despliegue del Cero-tacto

En el diseño de un elegante instale la arquitectura, cuidado debe ser tomado tales que el espacio de IP Address de la infraestructura no es accesible a los partidos untrusted. En las versiones que no soportan el comando del **vstack**, asegúrese de que solamente Smart instale al director haga que la Conectividad TCP a todo el Smart instale a los clientes en el puerto 4786.

Los administradores pueden utilizar estas mejores prácticas de la Seguridad para Cisco Smart instalan las implementaciones en los dispositivos afectados:

- Interfaz ACL
- Políticas del plano de control (CoPP). Esta característica no está disponible en todas las versiones de Cisco IOS Software.

Este ejemplo muestra que una interfaz ACL con Smart instala al director dirección IP mientras que 10.10.10.1 y Smart instalan el dirección IP del cliente como 10.10.10.200:

```
ip access-list extended SMI_HARDENING_LIST
Permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
deny tcp any any eq 4786
permit ip any any
```

Este ACL se debe desplegar en todas las interfaces IP en todos los clientes. Puede también ser avanzado vía el director cuando el Switches primero se despliega.

Para restringir más lejos el acceso a todos los clientes dentro de la infraestructura, los administradores pueden utilizar estas mejores prácticas de la Seguridad en los otros dispositivos en la red:

- Listas de control de acceso de la infraestructura (iACLs)
- Listas de control de acceso del VLA N (VACL)

Acceso del límite a la red con la infraestructura ACL

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.

Un iACL se construye y se aplica para especificar las conexiones de los host o de las redes que necesitan ser permitidos a los dispositivos de red. Ejemplos comunes de estos tipos de conexión

son eBGP, SSH y SNMP. Después de que se hayan permitido las conexiones necesarias, el resto del tráfico a la infraestructura se niega explícitamente. Todo el tráfico de tránsito que cruza la red y no se dirige a los dispositivos de la infraestructura se permite explícitamente.

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

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

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit required connections for routing protocols and
!--- network management
!

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
permit tcp host <trusted-management-stations> any eq 22
permit udp host <trusted-netmgmt-servers> any eq 161
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

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

Consulte Protección del Núcleo: Listas de Control de Acceso para 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 Cisco IOS Software proporciona las funciones para filtrar específicamente los mensajes ICMP por nombre o teclear y cifrarlos. Esta ACL de ejemplo, que se debe utilizar con las entradas de control de acceso (ACE) de los ejemplos anteriores, permite pings de estaciones de administración y de servidores NMS confiables y bloquea el resto de los paquetes ICMP:

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!

permit icmp host <trusted-management-stations> any echo
permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Filtrar fragmentos IP

El procedimiento de filtrado para los paquetes del IP hechos fragmentos puede plantear un desafío a 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 Cisco IOS Software utiliza un método específico para marcar los fragmentos no iniciales contra las listas de acceso configurado. 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:

```
!

ip access-list extended ACL-FRAGMENT-EXAMPLE
permit tcp any host 192.168.1.1 eq 80
deny tcp any host 192.168.1.1 eq 22
!>
```

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

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!
```

```
deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Refiera a las listas de control de acceso y a los fragmentos IP para más información sobre cómo el ACL maneja los paquetes del IP hechos fragmentos.

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:

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets containing IP options
!

deny ip any any option any-options
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

Soporte ACL a filtrar en el valor de TTL

Soporte agregado Cisco IOS Software Release 12.4(2)T ACL para filtrar los paquetes del IP basados en el valor del Time to Live (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. El dispositivo que decrements TTL a cero, y por lo tanto cae el paquete, se requiere para generar y enviar un Time Exceeded Message ICMP a la fuente del paquete.

La generación y la transmisión de estos mensajes es un proceso de excepción. El Routers puede realizar esta función cuando el número de paquetes del IP que deban expirar es bajo, pero si el número de paquetes debido a expirar es alto, la generación y la transmisión de estos mensajes pueden consumir a todos los recursos de la CPU disponibles. Esto genera un vector de ataque de negación de servicio. Es por esta razón que los dispositivos necesitan ser endurecidos contra los ataques DOS que utilizan una alta velocidad de los paquetes del IP que deben expirar.

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.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets with TTL values insufficient to traverse the network
!

deny ip any any ttl lt 6
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

> Nota: Algunos protocolos hacen el uso legítimo de los paquetes con los 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.

Asegure a las Sesiones de administración interactivas

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 imprescindible asegurar a las Sesiones de administración para prevenir el acceso y el acceso no autorizado de la información.

Management Plane Protection

En el Cisco IOS Software Release 12.4(6)T y Posterior, la protección del plano de administración de la característica (MPP) permite que un administrador restrinja en qué tráfico de administración de las interfaces se puede recibir por un dispositivo. De esta manera, el administrador tiene control adicional sobre un dispositivo y el modo de acceso a él.

Este ejemplo muestra cómo permitir al MPP para permitir solamente SSH y el HTTPS en la interfaz GigabitEthernet0/1:

```
!

control-plane host
management-interface GigabitEthernet 0/1 allow ssh https
!
```

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:

- **característica de Puerto-filtración** - Esta característica prevé el policing o la caída de los paquetes que van a los puertos cerrados o NON-que escuchan TCP y UDP.

- **función de políticas del Cola-umbral** - Esta característica limita el número de paquetes para un protocolo especificado que se permitan en la cola de entrada IP del avión del control.

CPPr permite que un administrador clasifique, limpie, y restrinja el tráfico que se envía a un dispositivo para los fines de administración con la subinterfaz del host. Entre algunos ejemplos de paquetes que se clasifican para la categoría de subinterfaz host se incluyen el tráfico de administración, como SSH o Telnet, y los protocolos de ruteo.

> Nota: CPPr no soporta el IPv6 y se restringe a la trayectoria de la entrada del 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.

Cifre a las Sesiones de administración

Porque la información se puede divulgar en una Sesión de administración interactiva, este tráfico debe ser cifrado de modo que un usuario malintencionado no pueda acceder a los datos se transmiten que. La encripción del tráfico permite una conexión de acceso remoto segura al dispositivo. Si el tráfico para una sesión de administración se envía por la red en texto sin formato, un atacante puede obtener información confidencial sobre el dispositivo y la red.

Un administrador puede establecer haber cifrado y asegurar la Conexión de Administración del

Acceso Remoto a un dispositivo con las características de SSH o HTTPS (protocolo secure hypertext transfer). 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 estandardizado, así que no se recomienda si SSHv2 es una opción.

El Cisco IOS Software también soporta el protocolo de la Copia segura (SCP), que permite haber cifrado y una conexión segura para copiar las configuraciones del dispositivo o las imágenes del software. El protocolo SCP depende de SSH. Este ejemplo de configuración habilita el protocolo SSH en un dispositivo Cisco IOS:

```
!

ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1
!

line vty 0 4
transport input ssh
!
```

Este ejemplo de configuración habilita los servicios de SCP:

```
!

ip scp server enable
!
```

Esto es un ejemplo de configuración para los servicios HTTPS:

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

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 configuran al **comando 2 del verson del ssh del IP** explícitamente, después el Cisco IOS

habilita el SSH versión 1.99. El SSH versión 1.99 permite las conexiones SSHv1 y SSHv2. SSHv1 se considera ser inseguro y puede tener efectos adversos en el sistema. Si se habilita SSH, se recomienda para inhabilitar SSHv1 usando el comando de la **versión 2 del ssh del IP**.

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

```
!

hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1

!

ip ssh version 2

!

line vty 0 4
transport input ssh

!
```

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

SSHv2 Enhancements for RSA Keys

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 privado/un par clave público en el cliente y configurar una clave pública en el servidor SSH del Cisco IOS para completar la autenticación.

Un usuario de SSH que intenta establecer las credenciales proporciona una firma cifrada 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. El hash se utiliza para determinar si el servidor tiene una entrada que corresponda con. Si se encuentra una coincidencia, la verificación RSA-basada del mensaje se realiza 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 la clave de host estricta que marca el indicador se habilita en el cliente, el cliente marca si tiene la entrada de clave de host que corresponde al servidor preconfigurado. Si se encuentra una coincidencia, el cliente intenta validar la firma con la clave del host servidor. Si el servidor se autentica con éxito, el establecimiento de sesión continúa; si no se termina y visualiza un **mensaje fallido de la autenticación de servidor**.

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

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Specify the name of the RSA key pair (in this case, "sshkeys") to use for SSH
!

ip ssh rsa keypair-name sshkeys
!
! Enable the SSH server for local and remote authentication on the router using
! the "crypto key generate" command
! For SSH version 2, the modulus size must be at least 768 bits
!

crypto key generate rsa usage-keys label sshkeys modulus 2048
!
! Configure an ssh timeout (in seconds)
!
! The following enables a timeout of 120 seconds for SSH connections
!

ip ssh time-out 120
!
! Configure a limit of five (5) authentication retries
!

ip ssh authentication-retries 5
!
! Configure SSH version 2
!

ip ssh version 2
!
```

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

Este ejemplo de configuración permite al servidor SSH del Cisco IOS para realizar la autenticación de usuario RSA-basada. 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.

Este ejemplo de configuración permite al cliente SSH del Cisco IOS para realizar la autenticación de servidor RSA-basada.

```
!
!

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 auxiliar de un dispositivo se debe inhabilitar para prevenir el acceso no autorizado. Un puerto auxiliar se puede inhabilitar con estos comandos:

```
!

line aux 0
transport input none
transport output none
no exec
exec-timeout 0 1
no password
!
```

Control de Líneas vty y tty

Las sesiones de administración interactivas 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 se puede determinar con el comando show line exec. Cuando todas las líneas del vty son funcionando, las nuevas Sesiones de administración no pueden ser establecidas, que crea una condición DOS 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. Una línea equipo teleescritor que está conectada con un módem que se utilice para el Acceso Remoto al dispositivo, o una línea equipo teleescritor que está conectada con el puerto de la consola de otros dispositivos es también accesibles vía la red. Otras formas de vty y de controles de acceso equipo teleescritor se pueden aplicar con los comandos configuration de la **entrada de transporte** o de la acceso-**clase**, con el uso de las características de CoPP y de CPPr, o si usted aplica las Listas de acceso a las interfaces en el dispositivo.

La autenticación se puede aplicar con el uso del AAA, que es el método recomendado para el acceso autenticado a un dispositivo, con el uso de la base de datos de usuarios locales, o por la autenticación de contraseña simple configurada directamente en el vty o la línea equipo teleescritor.

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** debe también ser utilizado para habilitar los keepalifes TCP en las conexiones entrantes al dispositivo. 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

Un vty y un equipo teleescritor se deben configurar para validar cifrado solamente y asegurar las Conexiones de Administración del Acceso Remoto al dispositivo o a través del dispositivo si se utiliza como servidor de la consola. Esta sección trata sobre las tty porque tales líneas se pueden conectar con los puertos de consola en otros dispositivos y, de esta manera, se puede acceder a ellas a través de la red. 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. **La entrada de transporte ningunos** configuración se puede habilitar en un equipo teleescritor, que en efecto inhabilita el uso de la línea equipo teleescritor para las conexiones de la reverso-consola.

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**.

Nota: El IPSec puede ser utilizado para cifrado y asegurar las conexiones de acceso remoto a un dispositivo, si está soportado. 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 e ilegal monitorear a los usuarios malintencionados a menos que los hayan notificado que los no permiten para utilizar 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 del Authentication, Authorization, and Accounting (AAA) es crítico para asegurar el acceso interactivo a los dispositivos de red. El marco AAA proporciona un entorno altamente configurable que se pueda adaptar basó en las necesidades de la red.

autenticación TACACS+

El TACACS+ es un protocolo de autenticación que los dispositivos Cisco IOS pueden utilizar para la autenticación de los usuarios de administración contra un servidor de 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. Cuando usted no depende de una sola contraseña compartida, la Seguridad de la red se mejora y se consolida su responsabilidad.

El RADIUS es un protocolo similar en el propósito al TACACS+; sin embargo, cifra solamente la contraseña enviada a través de la red. En cambio, el TACACS+ cifra el entero carga útil de TCP, que incluye ambos el nombre de usuario y 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.

Autenticación de TACACS+ puede ser habilitado en un dispositivo Cisco IOS con una configuración similar a este ejemplo:

```
!

aaa new-model
aaa authentication login default group tacacs+
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

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 que describe los métodos de autentificación que se preguntarán para autenticar a un usuario. Las listas de métodos le permiten para señalar uno o más protocolos de Seguridad que se utilizarán para la autenticación, y aseguran así a sistema de respaldo para la autenticación en caso de que el método inicial falle. El Cisco IOS Software utiliza el primer método enumerado que valida o rechaza con éxito a un usuario. Los métodos subsiguientes se intentan solamente si los métodos anteriores fallan debido a la falta de disponibilidad o a la configuración incorrecta del servidor.

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

Autenticación Alternativa

Si todos los servidores TACACS+ configurados 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. El uso del secreto del permiso se prefiere porque el secreto se desmenuza con un algoritmo unidireccional que sea intrínsecamente más seguro que el algoritmo de encripción que se utiliza con las contraseñas del tipo 7 para la línea o la autenticación local.

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. Aunque esta acción aumente la responsabilidad de los administradores de la red en las caídas del sistema TACACS+, aumenta perceptiblemente la carga administrativa porque las cuentas de usuario local en todos los dispositivos de red deben

ser mantenidas.

Estructuras de este ejemplo de configuración sobre autenticación de TACACS+ el ejemplo anterior para incluir la autenticación del retraso a la contraseña que se configura localmente con el **comando enable secret**:

```
!

enable secret <password>
!

aaa new-model
aaa authentication login default group tacacs+ enable
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

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

Uso de Contraseñas Tipo 7

Diseñado originalmente para permitir el desciframiento rápido de las contraseñas salvadas, las contraseñas del tipo 7 no son una forma segura de almacenamiento de contraseña. 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.

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.

Vea el plano de administración general el endurecer de la sección de este documento para más información sobre el retiro de las contraseñas del 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:

```
!

aaa authorization exec default group tacacs none
aaa authorization commands 0 default group tacacs none
aaa authorization commands 1 default group tacacs none
aaa authorization commands 15 default group tacacs none
!
```

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

Contabilización de Comandos TACACS+

Cuando está configurada, la contabilización de comandos AAA envía información sobre cada comando EXEC que se ingresa a los servidores TACACS+ configurados. La información enviada al servidor TACACS+ incluye el comando ejecutado, la fecha que fue ejecutado, y el nombre de usuario del usuario que ingresa el comando. Las estadísticas del comando no se soportan con el RADIUS.

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

```
!

aaa accounting exec default start-stop group tacacs
aaa accounting commands 0 default start-stop group tacacs
aaa accounting commands 1 default start-stop group tacacs
aaa accounting commands 15 default start-stop group tacacs
!
```

Refiera a configurar explicando más información sobre la configuración de las estadísticas 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.

Cuando usted diseña o implementa una solución redundante del servidor de AAA, recuerde estas consideraciones:

- disponibilidad de los servidores de AAA durante las posibles fallas de la red;
- colocación geográficamente distribuida de los servidores de AAA;
- Cargue en los servidores de AAA individuales en de estado estacionario y las condiciones de error
- 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.

Fortifique el protocolo administración de red simple

En esta sección se resaltan varios métodos que se pueden utilizar para asegurar la implementación del protocolo SNMP dentro de los dispositivos IOS. Es crítico que el SNMP esté asegurado correctamente para proteger la confidencialidad, la integridad, y la Disponibilidad de los datos de red y de los dispositivos de red con los cuales estos datos transitan. SNMP le brinda

una gran cantidad de información sobre el estado de los dispositivos de red. Esta información se debe proteger contra los usuarios malintencionados que quieren leverage estos datos para realizar los ataques contra la red.

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*:

```
!

snmp-server community READONLY RO
snmp-server community READWRITE RW
!
```

> Nota: Los ejemplos anteriores de la cadena de comunidad se han elegido para explicar claramente 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.

> Nota: Los dispositivos que son permitidos por estos ACL requieren la cadena de comunidad apropiada para acceder la información de SNMP pedida.

```
!

access-list 98 permit 192.168.100.0 0.0.0.255
access-list 99 permit 192.168.100.1
!

snmp-server community READONLY RO 98
snmp-server community READWRITE RW 99
!
```

Refiera a la comunidad del SNMP-servidor en la referencia del comando management del Cisco IOS Network para más información sobre esta característica.

ACL de Infraestructura

La infraestructura ACL (iACLs) se puede desplegar para asegurarse de que solamente los host extremos con los IP Addresses de confianza pueden enviar el tráfico SNMP a un dispositivo 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*:

```
!

snmp-server view VIEW-SYSTEM-ONLY system include
!

snmp-server community LIMITED view VIEW-SYSTEM-ONLY RO
!
```

Consulte Configuración de Soporte SNMP para obtener más información.

Versión 3 de SNMP

La versión 3 de SNMP (SNMPv3) se encuentra definida en RFC3410 , RFC3411 , RFC3412 , RFC3413 , RFC3414 y RFC3415 , además es un protocolo de interoperabilidad basado en estándares para la administración de red. El SNMPv3 proporciona el acceso seguro a los dispositivos porque autentica y cifra opcionalmente los paquetes sobre la red. Donde soportado, el SNMPv3 se puede utilizar para agregar otra capa de Seguridad cuando usted despliega el SNMP. SNMPv3 consiste en tres opciones de configuración primaria:

- **ningún auth** - Este modo no requiere ninguna autenticación ni ningún cifrado de los paquetes snmp
- **auth** - Este modo requiere la autenticación del paquete snmp sin el cifrado
- **priv** - Este modo requiere la autenticación y el cifrado (aislamiento) de cada paquete snmp

Un ID del motor autoritario debe existir para utilizar los mecanismos de seguridad del SNMPv3 - autenticación o autenticación y cifrado - para manejar los paquetes 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
```

> Nota: Si se cambia el engineID, todas las cuentas de usuario SNMP deben ser configuradas de nuevo.

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

```
!
snmp-server group AUTHGROUP v3 auth
!
```

Este comando configura un dispositivo Cisco IOS para el SNMPv3 con un grupo de servidor SNMP PRIVGROUP y habilita la autenticación y el cifrado para este grupo con la **palabra clave priv**:

```
!
snmp-server group PRIVGROUP v3 priv
!
```

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

```
!

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

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: 80000009030000152BD35496
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 característica de la protección del plano de administración (MPP) en Cisco IOS Software se puede utilizar para ayudar al SNMP seguro porque restringe las interfaces a través de las cuales el tráfico SNMP puede terminar en el dispositivo. La función MPP permite que un administrador designe una o más interfaces como interfaces de administración. El tráfico de administración puede ingresar a un dispositivo solamente a través de estas interfaces de administración. Después de que se habilita la función MPP, ninguna interfaz, salvo las interfaces de administración designadas, acepta el tráfico de administración de red que se dirige al dispositivo.

Observe que el MPP es un subconjunto de la característica de CPPr y requiere una versión del IOS que soporte 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:

```
!
control-plane host
management-interface FastEthernet0/0 allow ssh snmp
!
```

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

Prácticas Recomendadas de Registro

El registro de eventos le 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 permite correlacionar y Auditar red y los eventos de seguridad a través de los dispositivos de red más con eficacia. 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, cualquier protección que una red permita al tráfico de administración (por ejemplo, cifrado o acceso fuera de banda) debe ser extendida para incluir el tráfico del Syslog.

Este ejemplo de configuración configura un dispositivo Cisco IOS para enviar la información de ingreso al sistema a un servidor del syslog remoto:

```
!
logging host <ip-address>
!
```

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.

Este las líneas de configuración configuran 134,217,728 bytes (128 MB) de los mensajes de registración al directorio del Syslog del flash ATA (disk0), especificando un tamaño del archivo de 16,384 bytes:

```
logging buffered
logging persistent url disk0:/syslog size 134217728 filesize 16384
```

Antes de que los mensajes de registración se escriban a un archivo en el disco ATA, el Cisco IOS Software marca si hay suficiente espacio en disco. Si no hay espacio suficiente, se elimina el archivo de los mensajes de registro más viejo (por fechado) y se guarda el archivo actual. El formato del nombre del archivo es log_month: **día: año:: tiempo**.

Nota: Memoria USB ATA ha limitado el espacio en disco y así las necesidades de ser mantenido para evitar sobregrabar los datos almacenados.

Este ejemplo muestra cómo copiar los mensajes de registración del disco Flash del router ATA a un disco externo en el servidor FTP 192.168.1.129 como parte de los procedimientos de 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 nivel de trampa de registro del comando global configuration se utiliza para especificar qué mensajes de registración se envían a los servidores del syslog remoto. El *nivel* especificado indica el mensaje de nivel más bajo de gravedad que se envía. Para los registros almacenados en buffer, se utiliza el **comando logging buffered level**.

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

```
!

logging trap 6
logging buffered 6
!
```

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 Cisco IOS Software, es posible enviar los mensajes del registro a las sesiones de monitoreo - las sesiones de monitoreo son las Sesiones de administración interactivas en quienes se ha publicado el **monitor de la terminal de** comando exec - y a la consola. Sin embargo, esto puede elevar carga de la CPU de un dispositivo IOS y por lo tanto no se recomienda. En lugar, le aconsejan enviar la información de ingreso al sistema al búfer del registro local, que se puede ver con el **comando show logging**.

Utilice los comandos global configuration **ninguna consola de registro** y **no logging monitor** para inhabilitar el registro a la consola y a las sesiones de monitoreo. Este ejemplo de configuración muestra el uso de estos comandos:

```
!

no logging console
no logging monitor
```

```
!
```
Consulte Referencia de Comandos de Administración de 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 buffer se configura con el comando mitigado registro de la gravedad. Un administrador puede ver el contenido del buffer de registro a través del **comando EXEC show logging**.

Este ejemplo de configuración incluye la configuración de memoria intermedia de registro de 16384 bytes, así como una gravedad de 6, informativa, que indica que los mensajes en los niveles 0 (emergencias) con 6 (informativo) están salvados:

```
!

logging buffered 16384 6
!
```
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 proporcionar un nivel creciente de estado coherente cuando usted recoge y revisa los mensajes del registro, le aconsejan configurar estáticamente una interfaz de origen del registro. 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.

Este ejemplo de configuración ilustra el uso del comando global configuration de la interfaz de la **interfaz de origen del registro** para especificar que la dirección IP de la interfaz del loopback0 esté utilizada para todos los mensajes del registro:

```
!
logging source-interface Loopback 0
!
```
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):

```
!
service timestamps log datetime msec show-timezone
!
```

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

```
!

clock timezone PST -8
service timestamps log datetime msec localtime show-timezone
!
```

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 el Cisco IOS Software Release 12.3(7)T y Posterior, el reemplace de la configuración y las características de la restauración no actualizada de la configuración permiten que usted archive la configuración de dispositivo Cisco IOS en el dispositivo. Salvado manualmente o automáticamente, las configuraciones en este archivo se pueden utilizar para substituir la Configuración actual de ejecución. por la **configuración substituyen el** comando filename. 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 que está habilitado, un administrador puede hacer la Configuración actual de ejecución. ser agregado al archivo con el comando privileged exec de los **config del archivo**. Las configuraciones archivadas se pueden ver con el comando exec del **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** .

```
!

archive
path disk0:archived-config
maximum 14
time-period 1440
write-memory
```

```
!
```

Aunque las funciones del archivo de configuración puedan salvar hasta 14 configuraciones de respaldo, le aconsejan considerar los requisitos de memoria antes de que usted utilice el comando **máximo**.

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 característica se configura con el modo **exclusivo del modo de configuración de** comando global configuration y actúa 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 lock configurado terminal** para bloquear la configuración cuando ingresa al modo de configuración.

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

```
!
configuration mode exclusive auto
!
```

Cisco IOS Software Resilient Configuration

Agregado en el Cisco IOS Software Release 12.3(8)T, la característica de configuración resistente permite salvar con seguridad una copia de la imagen del Cisco IOS Software y de la configuración del dispositivo que es utilizada actualmente por un dispositivo Cisco IOS. Cuando se habilita esta función, no es posible alterar o quitar estos archivos de respaldo. Le aconsejan permitir a esta característica para prevenir las tentativas inadvertidas y malévolas de borrar estos archivos.

```
!
secure boot-image
secure boot-config!
```

Una vez que se habilita esta función, es posible restaurar una configuración eliminada o una imagen de Cisco IOS Software eliminada. El estado de ejecución actual de esta característica puede ser visualizado con el comando exec **seguro del inicio de la demostración**.

Digitally Signed Cisco Software

Agregado en el Cisco IOS Software Release 15.0(1)M para Cisco 1900, 2900, y 3900 Series Router, la característica firmado digitalmente del software de Cisco facilita el uso del Cisco IOS Software se firma digitalmente y se confía en así que, con el uso de la criptografía asimétrica segura (de la clave pública).

Una imagen con firma digital tiene un hash cifrado (con una clave privada). Sobre el control, el dispositivo desencripta el hash con la clave pública correspondiente de las claves que tiene en su almacén dominante y también que 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. El ROMMON y las imágenes del Cisco IOS regulares se firman con una clave del special o de la producción cuando usted utiliza la característica firmado digitalmente del software de Cisco. La imagen ROMMON es mejorable y se debe firmar con la misma clave que el special o la imagen de producción se carga que.

Este comando verifica la integridad de la imagen c3900-universalk9-mz.SSA en el flash con las claves en el almacén de la clave del dispositivo:

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```

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 el Cisco IOS Software Release 15.1(1)T y Posterior, el reemplazo dominante para el software de Cisco firmado digitalmente fue introducido. 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 (special o producción) clave para la imagen a (special o producción) viene en la imagen a (producción o revocación) que se utiliza para revocar la clave anterior del special o de la producción. La integridad de imagen de la revocación se verifica con una clave de la renovación que venga depositado en la plataforma. Las claves de renovación no cambian. Cuando usted revoca una clave de la producción, después de que se cargue la imagen de la revocación, la nueva clave que lleva se agrega al almacén dominante y la vieja clave correspondiente puede ser revocada mientras se actualice la imagen ROMMON y se inicia la nueva imagen de producción. Cuando usted revoca una clave especial, se carga una imagen de producción. Esta imagen agrega la nueva clave especial y puede revocar la clave especial anterior. Después de que usted actualice el ROMMON, la nueva imagen especial puede ser iniciada.

Este ejemplo describe la revocación de una clave especial. Estos comandos add la nueva clave especial al almacén dominante de la imagen de producción actual, copian una nueva imagen ROMMON (C3900_rom-monitor.srec.SSB) a la área de almacenamiento (usbflash0:), actualizan el archivo ROMMON, y revocan la vieja clave especial:

```
software authenticity key add special
copy tftp://192.168.1.129/C3900_rom-monitor.srec.SSB usbflash0:
upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
software authenticity key revoke special
```

Una nueva imagen especial (c3900-universalk9-mz.SSB) se puede entonces copiar al flash que se cargarán y a la firma de la imagen se verifica con la clave especial nuevamente agregada (.SSB):

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```

La revocación y el reemplazo dominantes no se soporta en el Switches del E-series del Catalyst 4500 que funciona con el Software Cisco IOS XE, aunque este Switches soporte la característica firmado digitalmente del software de Cisco.

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. Estas funciones se habilitan con el comando configuration mode del maderero del cambio de configuración del **permiso del registro**. **Los hidekeys de los** comandos opcionales y las entradas del **tamaño del registro** se utilizan para mejorar la configuración predeterminada porque previenen el registro de los datos de la contraseña y aumentan la longitud del registro del cambio.

Se recomienda que habilite esta función para el historial de cambios en la configuración de un dispositivo Cisco IOS pueda entenderse más fácilmente. Además, le aconsejan utilizar el comando de **configuración de syslog de la notificación** para habilitar la generación de mensajes de Syslog cuando se realiza un cambio de configuración.

```
!

archive
log config
logging enable
logging size 200
hidekeys
notify syslog
!
```

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

Plano de Control

Las funciones planas del control consisten en los protocolos y los procesos que comunican entre los dispositivos de red para mover los datos desde la fuente al 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, usted puede inhabilitar a la recepción y la transmisión de los tipos determinados de mensajes en una interfaz para minimizar la cantidad carga de la CPU de eso se requiere 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. Un usuario malintencionado puede explotar la capacidad del router de enviar las redirecciones ICMP continuamente enviando los paquetes al router, que fuerza al router a responder con los mensajes de la redirección ICMP, y los resultados en un efecto adverso en el CPU y el funcionamiento 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 aumentar la utilización de la CPU en el dispositivo. 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 mensaje inalcanzable de ICMP puede ser inhabilitada con el **no ip unreachables del** comando interface configuration. La limitación de la tarifa del ICMP fuera de alcance se puede cambiar del valor por defecto con el intervalo-en-ms **inalcanzable del tarifa-límite ICMP del** comando de configuración global ip.

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.

Hay varias desventajas a la utilización del proxy ARP. Puede dar lugar a un aumento en la cantidad de tráfico ARP en el segmento de red y el agotamiento de recursos y los ataques del intermediario. 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 poder agotar toda la memoria disponible si envía un gran número de pedidos ARP.

Los ataques del intermediario habilitan un host en la red al spoof la dirección MAC del router, que da lugar a los host confiados que envían el tráfico al atacante. El proxy ARP se puede inhabilitar con el **no ip proxy-arp del** comando interface configuration.

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

Limite el impacto CPU del tráfico del plano del control

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.

Entienda el tráfico del plano del control

Para proteger correctamente el avión del control del dispositivo Cisco IOS, es esencial entender los tipos de tráfico que es proceso conmutado por el CPU. 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 la adyacencia de la recepción*. Este tráfico contiene una entrada en el tabla de Cisco Express Forwarding (CEF) por el que el salto siguiente del router sea el dispositivo sí mismo, que es indicado por el término recibe en la salida del **cef** CLI del **IP de la demostración**. 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 es manejado por el CPU es tráfico del plano de datos - trafique con un destino más allá del dispositivo Cisco IOS sí mismo - que requiere el proceso especial por el 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 la lista de control de acceso** - El tráfico del registro de ACL consiste en cualquier paquete que sea generado debido a una coincidencia (permit or deny) de ACE en las cuales se utilice la palabra clave del registro.

- **Unicast Reverse Path Forwarding (unicast RPF)** - El unicast RPF, usado conjuntamente con un ACL, puede dar lugar al process switching de ciertos paquetes.

- **Opciones IP** - Cualquier paquete del IP con las opciones incluidas se debe procesar por el CPU.

- **Fragmentación** - Cualquier paquete del IP que requiera la fragmentación se debe pasar al CPU para procesar.

- **Vencimiento del Tiempo para vivir (TTL)** - Los paquetes que tienen un valor de TTL inferior o igual uno requerir el tiempo del protocolo Protocolo de control de mensajes de Internet (ICMP) excedieron (el tipo 11 ICMP, el código 0) los mensajes que se enviarán, que resulta adentro procesamiento de la CPU.

- **ICMP fuera de alcance** - Los paquetes que dan lugar a los mensajes inalcanzables de ICMP debido a rutear, el MTU, o la filtración es procesados por el CPU.

- **Tráfico que requiere un pedido ARP** - Los destinos para los cuales una entrada ARP no existe requieren el proceso por el CPU.

- **Tráfico no IP** - Todo el tráfico no IP es procesado por el CPU.

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** proporciona la información sobre el número de paquetes que sean proceso conmutado por un dispositivo.

- 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. La infraestructura ACL se cubre extensivamente en el acceso del límite a la red con la sección de la infraestructura ACL de este documento.

Le aconsejan implementar los iACLs para proteger el avión del control de todos los dispositivos de red.

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:

```
!
!--- Permit SSH from trusted hosts allowed to the device.
!

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22
!
!--- Deny SSH from all other sources to the RP.
!

access-list 151 deny tcp any any eq 22
!
!--- Permit all other traffic to the device.
!--- according to security policy and configurations.
!

access-list 151 permit ip any any
!
!--- Apply this access list to the receive path.
!

ip receive access-list 151
!
```

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 característica de CoPP se puede también utilizar para restringir los paquetes del IP que se destinan al dispositivo de infraestructura. En este ejemplo, solamente el tráfico SSH de hosts confiables está permitido para alcanzar el CPU del dispositivo Cisco IOS.

> Nota: El tráfico de caída de los IP Addresses desconocidos o untrusted puede evitar que los host con los IP Addresses dinámico-asignados conecten con el dispositivo Cisco IOS.

```
!

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

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

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

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

En el ejemplo anterior de CoPP, las entradas ACL que hacen juego los paquetes no autorizados con la acción del permiso dan lugar a un descarte de estos paquetes por la función del descenso del directiva-mapa, mientras que los paquetes que hacen juego la acción de la negación no son afectados por la función del descenso del directiva-mapa.

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:

- **característica de Puerto-filtración** - Esta característica prevé limpiar y caer de los paquetes que se envían a los puertos cerrados o NON-que escuchan TCP o UDP.

- **característica de la Cola-formación de umbrales** - Esta característica limita el número de paquetes para un protocolo especificado que se permitan en la cola de entrada IP de la controle de plano.

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.

Asegure el BGP

El protocolo Border Gateway Protocol (BGP) es la base de ruteo de Internet. Como tal, cualquier organización con los requisitos de conectividad más que modestos utiliza a menudo el BGP. El BGP es apuntado por los atacantes debido a su ubicuidad y el *conjunto y olvida* a menudo la naturaleza de las configuraciones BGP en organizaciones más pequeñas. 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.

Conocido como ambos el corte TTL-basado generalizado del mecanismo de seguridad (GTSM) y de la Seguridad BGP TTL (BTSH), una protección de Seguridad TTL-basada leverages el valor de TTL de los paquetes del IP para asegurarse de que los paquetes BGP se reciben que son de un par directamente conectado. 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 el BGP se habilita con la opción de la TTL-**Seguridad** para el comando configuration **vecino del** router BGP. Este ejemplo ilustra la configuración de esta función:

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> ttl-security hops <hop-count>
!
```

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

Autenticación de Peer BGP con MD5

La autenticación de peer con el MD5 crea una publicación MD5 de cada paquete enviado como parte de una sesión 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 BGP de conversación de recepción utiliza el mismo algoritmo y clave secreta para regenerar la publicación de mensaje. Si los resúmenes recibidos y computados no son idénticos, se descarta el paquete.

La autenticación de peer con el MD5 se configura con la **opción de contraseña al** comando configuration **vecino del** router BGP. El uso de este comando se ilustra a continuación:

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> password <secret>
!
```

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

Configure los prefijos máximos

Los prefijos BGP son guardados por un router en la memoria. Cuanto más prefijos un router debe llevar a cabo, más memoria el BGP debe consumir. 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.

Cuando usted configura esta característica con el comando configuration **vecino del** router BGP del máximo-**prefijo**, se requiere 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.

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>
!
```

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

Filtre los prefijos BGP con las listas de prefijos

Las listas de prefijos le permiten a un administrador de red aceptar o negar prefijos específicos que se envían o se reciben a través de BGP. Las listas de prefijos se deben utilizar en lo posible para asegurarse que el tráfico de la red está enviado sobre las trayectorias 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.

```
!

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0
ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24
!

router bgp <asn>
neighbor <ip-address> prefix-list BGP-PL-INBOUND in
neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out
!
```

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

Filtre los prefijos BGP con las Listas de acceso de la trayectoria 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 utilizar conjuntamente con las listas de prefijos para establecer un conjunto robusto de los filtros.

Las aplicaciones de este ejemplo de configuración COMO Listas de acceso de la trayectoria para restringir los prefijos entrantes a ésos originaron por el telecontrol COMO y los prefijos salientes a ésos originaron por el sistema autónomo local. Los prefijos que son originados por el resto de los sistemas autónomos se filtran y no se instalan en la tabla de ruteo.

```
!

ip as-path access-list 1 permit ^65501$
ip as-path access-list 2 permit ^$
!

router bgp <asn>
neighbor <ip-address> remote-as 65501
neighbor <ip-address> filter-list 1 in
neighbor <ip-address> filter-list 2 out
!
```

Asegure los protocolos Interior Gateway Protocols

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, Usted puede ejecutar a menudo un Interior Gateway Protocol (IGP) en la orden proporciona esta visión. 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:

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip authentication mode eigrp <as-number> md5
ip authentication key-chain eigrp <as-number> <key-name>
!
```

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

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip rip authentication mode md5
ip rip authentication key-chain <key-name>
!
```

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

```
!

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

router ospf <process-id>
network 10.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
!
```

Consulte Configuración de OSPF para obtener más información.

Comando Passive-Interface

Las filtraciones de información o la introducción de información falsa en un IGP 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:

```
!

router eigrp <as-number>
passive-interface default
```

```
no passive-interface <interface>
!
```

Filtrado de Rutas

Para reducir la posibilidad que usted introduce la información de ruteo falsa en la red, usted debe utilizar el filtrado de Routes. 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 el EIGRP y el RIP, uso del **comando distribute-list** con los límites de la palabra clave de la **salida** se hace publicidad qué información, mientras que el uso del **en la** palabra clave limita se procesan qué actualizaciones. El **comando distribute-list** está disponible para OSPF, pero no evita que un router propague rutas filtradas. Se puede usar, en cambio, el **comando area filter-list**.

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

```
!

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

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> out <interface>
!
```

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

```
!

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

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> in <interface>
!
```

Refiera a configurar las características IP Routing Protocol-Independent para más información sobre cómo controlar la publicidad y a proceso de las actualizaciones de ruteo.

Este ejemplo OSPF utiliza una lista de prefijos con el **comando area filter-list OSPF-**específico:

```
!

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

router ospf <process-id>
area <area-id> filter-list prefix <list-name> in
!
```

Consumo de Recursos del Proceso de Ruteo

Los prefijos de protocolo de ruteo son guardados por un router en la memoria y el consumo de recursos aumenta con los prefijos adicionales que un router debe contener. Para evitar el

agotamiento de recursos, es importante configurar el protocolo de ruteo para limitar el consumo de recursos. Esto es posible con el OSPF si usted utiliza la característica de protección contra sobrecarga de la base de datos del estado del link.

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

```
!

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

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

Asegure los primeros protocolos de la redundancia de salto

Los primeros protocolos de la redundancia de salto (FHRPs) proporcionan la elasticidad y la Redundancia para los dispositivos que actúan como default gatewayes. 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. Por abandono, estos protocolos comunican con las comunicaciones del unauthenticated. 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 prevenir este tipo de ataque, todo el FHRPs que es soportado por el Cisco IOS Software incluye una capacidad de la autenticación con el MD5 o las cadenas de texto. Debido a la amenaza planteada por los FHRP no autenticados, se recomienda que las instancias de estos protocolos utilicen autenticación MD5. Este ejemplo de configuración demuestra el uso de autenticación MD5 para GLBP, HSRP y VRRP:

```
!

interface FastEthernet 1
description *** GLBP Authentication ***
glbp 1 authentication md5 key-string <glbp-secret>
glbp 1 ip 10.1.1.1
!

interface FastEthernet 2
description *** HSRP Authentication ***
standby 1 authentication md5 key-string <hsrp-secret>
standby 1 ip 10.2.2.1
!

interface FastEthernet 3
description *** VRRP Authentication ***
vrrp 1 authentication md5 key-string <vrrp-secret>
vrrp 1 ip 10.3.3.1
!
```

Plano de Datos

Aunque el plano de datos sea responsable de transferir datos desde el origen hasta el destino, dentro del contexto de la seguridad, es el menos importante de los tres planos. Es por esta razón que es importante proteger los aviones de la Administración y del control en la preferencia sobre el avión de los datos cuando usted asegura un dispositivo de red.

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.

Vea el tráfico de tránsito del filtro con transitar la sección ACL de este documento para más información.

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 IP también incluyen las funciones para alterar la trayectoria que el tráfico toma a través de la red, que potencialmente permite que derribe 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. En la primera forma de este comando, las **opciones del IP caen**, todos los paquetes del IP que contengan las opciones IP se caen que son recibidas por el dispositivo Cisco IOS. 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:

```
!
ip options drop
!
```

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:

```
!
no ip source-route
!
```

Inhabilitación de Mensajes de Redirección ICMP

Los mensajes de redirección ICMP se utilizan para informar a un dispositivo de red una mejor trayectoria a un destino IP. De forma predeterminada, 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, puede ser que sea posible que un atacante haga el dispositivo Cisco IOS enviar muchos mensajes de la redirección ICMP, que da lugar al elevado carga de la CPU. Por este motivo, se recomienda que la transmisión de mensajes de redirección ICMP se inhabilite. Las redirecciones ICMP se inhabilitan con el **comando no ip redirects de la** configuración de la interfaz, tal y como se muestra en del ejemplo de configuración:

```
!

interface FastEthernet 0
no ip redirects
!
```

Inhabilitación o Limitación de Broadcasts Dirigidos a IP

Los Broadcasts Dirigidos a IP permiten enviar un paquete de broadcast IP a una subred IP remota. Una vez que alcanza la red remota, el dispositivo IP de reenvío envía el paquete como broadcast de Capa 2 a todas las estaciones en la subred. Esta función de 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 con el uso de un Access Control List como opción al **comando ip directed-broadcast**. Este ejemplo de configuración limita los broadcastes dirigidos a esos paquetes UDP que originen en una red de confianza, 192.168.1.0/24:

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

interface FastEthernet 0
ip directed-broadcast 100
!
```

El tráfico de tránsito del filtro con transita los ACL

Es posible controlar qué tráfico transita la red con el uso transitan ACL (tACLs). Estas listas se diferencian de las ACL de infraestructura que pretenden filtrar el tráfico que se dirige a la red en sí misma. La filtración proporcionada por los tACLs es beneficiosa cuando es deseable al filtrar tráfico a un grupo determinado de dispositivos o de tráfico que transite 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.

Vea la sección contra spoofing de las protecciones de este documento para más información.

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. Este ejemplo ACL permite el ICMP de las redes de confianza mientras que bloquea todos los paquetes icmp de otras fuentes:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Permit ICMP packets from trusted networks only
!

permit icmp host <trusted-networks> any
!
!--- Deny all other IP traffic to any network device
!
```

```
deny icmp any any
!
```

Filtrar fragmentos IP

Según lo detallado previamente en el acceso del límite a la red con la sección de la infraestructura ACL de este documento, la filtración de los paquetes del IP hechos fragmentos puede plantear un desafío a 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:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
```

Refiera a las listas de control de acceso y a los fragmentos IP para más información sobre la dirección ACL de los paquetes del IP hechos fragmentos.

ACL Support for Filtering IP Options

En el Cisco IOS Software Release 12.3(4)T y Posterior, el Cisco IOS Software soporta el uso de los ACL de filtrar los paquetes del IP basados en las opciones IP que se contienen en el paquete. La presencia de opciones IP dentro de un paquete pudo indicar una tentativa de derribar los controles de seguridad en la red o de alterar de otra manera las características del transitar 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 el contenido de los ejemplos anteriores para incluir el filtrado de paquetes IP que contienen opciones IP:

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP packets containing IP options
!

deny ip any any option any-options
!
```

Protecciones Contra Suplantación

Mucho spoofing de la dirección IP de origen del uso de los ataques a ser eficaz o para encubrir la verdadera fuente de un ataque y para obstaculizar el traceback exacto. El Cisco IOS Software proporciona el unicast RPF y a la Protección de origen IP (IPSG) para disuadir los ataques que confían en el spoofing de la dirección IP de origen. Además, las ACL y el ruteo nulo suelen implementarse como métodos manuales de prevención de la suplantación.

La Protección de origen IP funciona para minimizar el spoofing para las redes que están bajo control administrativo directo por el puerto del switch de ejecución, el MAC address, y la verificación de 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. El examen del Address Resolution Protocol (ARP) dinámico (DAI) atenúa los vectores del ataque que utilizan el envenenamiento 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. El unicast RPF confía en usted para habilitar el Cisco Express Forwarding en cada dispositivo y se configura en una base del por interface.

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:

```
!

ip cef
!

interface <interface>
ip verify unicast source reachable-via <mode>
!
```

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

IP Source Guard

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

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

```
!

ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

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

```
!
interface <interface-id>
ip verify source
!
```

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 de Puertos

Port Security se utiliza para reducir la suplantación de direcciones MAC en la interfaz de acceso. Port Security puede utilizar direcciones MAC (sticky) aprendidas dinámicamente para facilitar la configuración inicial. Una vez que la Seguridad de puerto ha determinado una infracción MAC, puede utilizar uno de cuatro modos de la infracción. a saber: protect, restrict, shutdown y shutdown VLAN. En los casos cuando un puerto proporciona solamente el acceso para una estación de trabajo única con el uso de los protocolos estándars, un número 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.

```
!

interface <interface>
switchport
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum <number>
switchport port-security violation <violation-mode>
!
```

Refiera a configurar la Seguridad de puerto para más información sobre el confuration de la Seguridad de puerto.

Dynamic ARP Inspection

La inspección ARP dinámica (DAI) se puede utilizar para atenuar los ataques del envenenamiento 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 se diseña para corromper memoria caché ARP de los 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 del DHCP, DAI utiliza los datos que son generados por la característica del snooping del 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:

```
!
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

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

```
!
ip arp inspection vlan <vlan-range>
!
```

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

```
!

arp access-list <acl-name>
permit ip host <sender-ip> mac host <sender-mac>
!

ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

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

ACL Contra Suplantación

Los ACL manualmente configurados pueden proporcionar la protección contra spoofing estática contra los ataques que utilizan el espacio de la dirección inusitado y untrusted conocido. 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. Los ACL de antisimulaciones requieren la supervisión regular porque pueden cambiar con frecuencia. El spoofing se puede minimizar en el tráfico que origina de la red local si usted aplica los ACL salientes que limitan el tráfico a los direccionamientos de local válida.

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

```
!

ip access-list extended ACL-ANTISPOOF-IN
deny ip 10.0.0.0 0.255.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
!

interface <interface>
ip access-group ACL-ANTISPOOF-IN in
!
```

Consulte Configuración de ACL 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.

Impacto del límite CPU del tráfico del plano de los datos

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 avión de los datos, que consiste en el tráfico que transita el dispositivo de red, se debe asegurar para asegurar la operación de los aviones de la Administración y del 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 del registro de ACL consiste en cualquier paquete que sea generado debido a una coincidencia (permit or deny) de ACE en las cuales se utilice la palabra clave del **registro**.
- **Unicast RPF** - El unicast RPF usado conjuntamente con un ACL pudo dar lugar al process switching de ciertos paquetes.
- **Opciones IP** - Cualquier paquete del IP con las opciones incluidas se debe procesar por el CPU.
- **Fragmentación** - Cualquier paquete del IP que requiera la fragmentación se debe pasar al CPU para procesar.
- **Vencimiento del Tiempo para vivir (TTL)** - Los paquetes que tienen un valor de TTL inferior o igual 1 requerir el tiempo del protocolo Protocolo de control de mensajes de Internet (ICMP) excedieron (el tipo 11 ICMP, el código 0) los mensajes que se enviarán, que resulta adentro procesamiento de la CPU.
- **ICMP fuera de alcance** - Los paquetes que dan lugar a los mensajes inalcanzables de ICMP debido a rutear, al MTU o a la filtración son procesados por el CPU.
- **Tráfico que requiere un pedido ARP** - Los destinos para los cuales una entrada ARP no existe requieren el proceso por el CPU.
- **Tráfico no IP** - Todo el tráfico no IP es procesado por el CPU.

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

Filtre en 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.

```
!
!--- Create ACL policy that filters IP packets with a TTL value
!--- less than 6
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any ttl lt 6
permit ip any any
!
!--- Apply access-list to interface in the ingress direction
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

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

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

En el Cisco IOS Software Release 12.4(4)T y Posterior, el paquete flexible que corresponde con (FPM) permite que un administrador haga juego en los bits arbitrarios de un paquete. Esta política FPM descarta paquetes con un valor TTL inferior a seis.

```
!

load protocol flash:ip.phdf
!

class-map type access-control match-all FPM-TTL-LT-6-CLASS
match field IP ttl lt 6
!

policy-map type access-control FPM-TTL-LT-6-DROP-POLICY
class FPM-TTL-LT-6-CLASS
drop
!

interface FastEthernet0
service-policy type access-control input FPM-TTL-LT-6-DROP-POLICY
!
```

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

Filtre en la presencia de opciones IP

En el Cisco IOS Software Release 12.3(4)T y Posterior, usted puede utilizar el soporte ACL para la característica de filtración de las opciones IP en un Nombrado, lista de acceso IP ampliado para filtrar los paquetes del IP con las opciones 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. Debe también ser observado que RSVP, el Multiprotocol Label Switching Traffic Engineering, los IGMP versión 2 y 3, y otros protocolos que utilizan los paquetes de las opciones IP no pudieron poder funcionar correctamente si los paquetes para estos protocolos se caen. Si estos protocolos se utilizan en la red, entonces se puede usar la función ACL Support for Filtering IP Options; sin embargo, la característica selectiva del descenso de las opciones IP ACL podría caer este tráfico y estos protocolos no pudieron funcionar correctamente. Si no hay protocolos funcionando que requieren las opciones IP, el descenso selectivo de las opciones IP ACL es el método preferido para caer estos paquetes.

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

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option any-options
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

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

- 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)

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option eool
deny ip any any option record-route
deny ip any any option timestamp
deny ip any any option lsr
deny ip any any option ssr
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

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

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 el Cisco IOS Software Release 12.3(4)T y Posterior, CoPP permite que un administrador filtre el flujo de tráfico de paquetes del avión del 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:

```
!

ip access-list extended ACL-IP-OPTIONS-ANY
permit ip any any option any-options
!

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

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
drop
!

control-plane
service-policy input COPP-POLICY
!
```

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)

```
!

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

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

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
drop
!

control-plane
service-policy input COPP-POLICY
!
```

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.

Refiera a las Políticas del plano de control que despliegan para más información sobre la característica de CoPP.

Función Control Plane Protection

En el Cisco IOS Software Release 12.4(4)T y Posterior, controle la protección plana (CPPr) puede ser utilizado para tráfico del plano restringir o de control de policía por el CPU de un dispositivo 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.

```
!

ip access-list extended ACL-IP-TTL-0/1
permit ip any any ttl eq 0 1
!

class-map ACL-IP-TTL-0/1-CLASS
match access-group name ACL-IP-TTL-0/1
!

ip access-list extended ACL-IP-TTL-LOW
permit ip any any ttl lt 6
!

class-map ACL-IP-TTL-LOW-CLASS
match access-group name ACL-IP-TTL-LOW
!

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

```
!

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

policy-map CPPR-CEF-EXCEPTION-POLICY
class ACL-IP-TTL-0/1-CLASS
drop
class ACL-IP-OPTIONS-CLASS
drop
!

!-- Apply CPPr CEF-Exception policy CPPR-CEF-EXCEPTION-POLICY to
!-- the CEF-Exception CPPr sub-interface of the device

!

control-plane cef-exception
service-policy input CPPR-CEF-EXCEPTION-POLICY
!

policy-map CPPR-TRANSIT-POLICY
class ACL-IP-TTL-LOW-CLASS
drop
!

control-plane transit
service-policy input CPPR-TRANSIT-POLICY
!
```

En la directiva anterior de CPPr, las entradas del Access Control List que hacen juego los paquetes con la acción del permiso dan lugar a estos paquetes que son desechados por la función del descenso del directiva-mapa, mientras que los paquetes que hacen juego la acción de la negación (no mostrada) no son afectados por la función del descenso del directiva-mapa.

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. El Netflow y la clasificación ACL son los dos métodos principales para lograr esto con el Cisco IOS Software. 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 vía el CLI, o los datos se pueden exportar a un colector NetFlow del anuncio publicitario o del freeware para la agregación y el 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. Los flujos del Netflow se pueden crear con los datos del tráfico muestreados en los entornos en grandes cantidades.

El CEF, o el CEF distribuido, es un requisito previó a habilitar el 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 | salida}**.

```
!

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

interface <interface>
ip flow <ingess|egress>
!
```

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

```
router#show ip cache flow
IP packet size distribution (26662860 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. Un administrador pudo también separar el implícito niega en el final de un ACL en los ACE granulares para ayudar a identificar los tipos de tráfico denegado.

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:

```
!

ip access-list extended ACL-SMB-CLASSIFY
remark Existing contents of ACL
remark Classification of SMB specific TCP traffic
deny tcp any any eq 139
deny tcp any any eq 445
deny ip any any
!
```

Para identificar el tráfico que utiliza una ACL de clasificación, utilice el comando EXEC **show access-list acl-name**. Los contadores ACL se pueden borrar por con el comando exec **claro del ACL-**nombre de los **contadores de la lista de acceso del 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 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 los ACL en las interfaces ruteadas. Por ejemplo, una correspondencia del VLA N se pudo utilizar para prevenir los host que se contienen dentro del mismo VLA N de la comunicación con uno a, que reduce las oportunidades para que los atacantes o los gusanos locales exploten 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.

Este ejemplo utiliza una lista de acceso denominada extendida que ilustre la configuración de esta característica:

```
!

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

vlan access-map <name> <number>
match ip address <acl-name>
action <drop|forward>
!
```

Este ejemplo demuestra el uso de una correspondencia del VLA N para negar los puertos TCP 139 y 445 así como el protocolo VINES-IP:

```
!

ip access-list extended VACL-MATCH-ANY
permit ip any any
!

ip access-list extended VACL-MATCH-PORTS
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!

mac access-list extended VACL-MATCH-VINES
permit any any vines-ip
!

vlan access-map VACL 10
match ip address VACL-MATCH-VINES
action drop
!

vlan access-map VACL 20
match ip address VACL-MATCH-PORTS
action drop
!
```

```
vlan access-map VACL 30
match ip address VACL-MATCH-ANY
action forward
!

vlan filter VACL vlan 100
!
```

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. El sintaxis para la creación PACL, que toma la precedencia sobre las correspondencias y el router ACLS del VLA N, es lo mismo que el router ACLS. Si una ACL se aplica a un interfaz de Capa 2, se denomina PACL. La configuración implica la creación de un IPv4, del IPv6, o de MAC ACL y aplicación de ella al interfaz de capa 2.

Este ejemplo utiliza una lista de acceso denominada extendida para ilustrar la configuración de esta característica:

```
!

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

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

Consulte la sección ACL de puerto de Configuración de 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
```

> Nota: 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 del VLAN privado

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 los PVLAN, todos los dispositivos en un VLA N de la capa 2 pueden comunicar 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 único se compromete, la falta de Conectividad a otros servidores debido a la aplicación de los PVLAN pudo ayudar a limitar el compromiso al un 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. Pudo solamente haber un VLAN aislado por el VLAN principal, y solamente los puertos promiscuos pueden comunicar con los puertos en un VLAN aislado. 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:

```
!

vlan 11
private-vlan isolated
!

vlan 20
private-vlan primary
private-vlan association 11
!

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

VLAN Comunitarias

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

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

la VLAN 20 primaria.

```
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 12
!

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

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:

```
!

vlan 11
private-vlan isolated
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 11-12
!

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

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

interface FastEthernet 1/12
description *** Promiscuous Port ***
switchport mode private-vlan promiscuous
switchport private-vlan mapping 20 add 11-12
!
```

Cuando usted implementa los PVLAN, es importante asegurarse de que la configuración de la capa 3 en el lugar soporta las restricciones que son impuestas por los PVLAN y no permite para que la configuración de PVLAN sea derribada. La capa 3 que filtra con un router ACL o el Firewall puede prevenir la subversión de la configuración de 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.

Acuses de recibo

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. Aconsejan los administradores evaluar cada opción para su riesgo potencial antes de que implementen la opción.

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

  ACLIP Source GuardDynamic ARP InspectionUnicast RPFSeguridad de 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