Mejore la Seguridad en el CSS11000 y el CSS11500

Contenido

Introducción

Este documento proporciona la información sobre las configuraciones de la configuración de Cisco que pueden mejorar la Seguridad en el Switch del Cisco Content Services (CSS) 11000 o CSS11500. Este documento describe las configuraciones de la configuración básica que son casi universal aplicables en las redes del IP y cubre algunos artículos inesperados cuyo usted debe ser consciente.

Este documento no presenta una lista exhaustiva de estos elementos, ni se puede la información en el documento substituir para el conocimiento de parte del administrador de la red. El documento sirve como recordatorio de los elementos que se olvidan a veces.

Este documento menciona solamente los comandos que son importantes en las redes del IP. Muchos de los servicios que usted puede habilitar en el CSS requieren la correcta configuración de seguridad. Sin embargo, este documento se centra en la información para los servicios que se habilitan por abandono o que son habilitados casi siempre por los usuarios y que puede requerir la incapacidad o la reconfiguración.

Algunas de las configuraciones predeterminadas en el software de Cisco WebNS existen por los motivos históricos. Estas configuraciones eran aplicables cuando fueron elegidas, pero serían probablemente diferentes si los nuevos valores por defecto fueron elegidos hoy. Otros valores por defecto son aplicables para la mayoría de los sistemas, pero pueden crear los riesgos de seguridad si estos valores por defecto se utilizan en los dispositivos esos crean a la parte de una defensa del perímetro de red. Todavía otros valores por defecto son requeridos realmente por los estándares, pero no son siempre deseables de un punto de vista de la seguridad.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Administración de Contraseña

Las contraseñas y la información propietaria similar, tal como cadenas de comunidad del Simple Network Management Protocol (SNMP), son la forma de defensa principal contra el acceso no autorizado a su CSS. La mejor forma de administrar a la mayoría de las contraseñas es mantenerlas en un TACACS+ o en un servidor de autenticación RADIUS. Sin embargo, casi cada CSS todavía tiene una contraseña localmente configurada para el acceso privilegiado. El CSS puede también incluir la otra información de contraseña en el archivo de configuración. Cualquier contraseña que se configure en el texto claro aparece en la configuración cifrada con el Data Encryption Standard (DES).

Perfiles de usuario local

Esta lista describe los perfiles de usuario local:

- *Administrador* — El perfil del administrador incluye estos privilegios:Acceso al menú Offline Diagnostics MonitorAcceso total a la línea de comandoAcceso de directorio completoEstas configuraciones se pueden configurar de la línea de comando o del menú Offline Diagnostics Monitor.
- *Técnico* — El perfil del técnico incluye estos privilegios:Acceso total a la línea de comandoAcceso de directorio completoEstas configuraciones se pueden configurar con el uso de la línea de comando. No utilice el perfil del técnico para los fines administrativos CSS.
- *Superusuario* — El perfil del superusuario incluye estos privilegios:Acceso total a la línea de comandoLa capacidad de salvar las restricciones del acceso de directorioEstas configuraciones se pueden configurar con el uso de la línea de comando.
- *Usuario* — El perfil del usuario no puede realizar los cambios de configuración e incluye las restricciones del acceso de directorio. Estas configuraciones se pueden configurar con el uso de la línea de comando.

Cuando usted publica el **comando restrict user-database**, usted aplica las restricciones del acceso de directorio en cada usuario. Los niveles del usuario solamente del administrador y del técnico pueden realizar estas acciones:

- Quite el **comando restrict user-database**.
- Cambie el **comando local user-database**.
- Publique el **comando clear running-config**.

Control del acceso interactivo

Cualquier usuario que pueda iniciar sesión a un CSS puede el mostrar información que el público general no necesita necesariamente ver. En algunos casos, un usuario que puede iniciar sesión al CSS puede utilizar el CSS como retransmisión para los otros ataques de red. Un usuario que tiene el acceso privilegiado al CSS puede configurar de nuevo el CSS. Para prevenir el acceso inapropiado, usted necesita controlar los inicios de sesión interactivo al CSS.

Aunque la mayoría del acceso interactivo se inhabilite por abandono, hay excepciones. Las excepciones más obvias son sesiones interactivas directamente de los terminales asincróno conectado, tales como el terminal de la consola, y acceso al puerto de administración Ethernet.

Refiera a configurar los métodos de Acceso Remoto CSS para más información sobre cómo

controlar el acceso interactivo al CSS.

Puertos de consola

Un elemento importante a recordar es que el puerto de la consola de un dispositivo de Cisco tiene privilegios especiales. Particularmente, suponga que alguien envía un carácter ESC (escape) al puerto de la consola cuando el funcionamiento de los diagnósticos del POSTE. Después de que una reinicialización, esta persona pueda utilizar fácilmente el procedimiento para recuperación de contraseña para tomar el control del sistema. Los atacantes que pueden interrumpir el poder o inducen una caída del sistema, y que tienen acceso al puerto de la consola a través de un terminal cableada, de un módem, de un servidor terminal, o de un poco de otro dispositivo de red, pueden tomar el control del sistema. Estos atacantes pueden tomar el control incluso si no tienen acceso físico al sistema o a la capacidad de iniciar sesión al sistema normalmente.

Por lo tanto, cualquier módem o dispositivo de red que den el acceso al puerto de consola de Cisco se debe asegurar a un estándar que sea comparable a la Seguridad que se utiliza para el acceso privilegiado al CSS. Al mínimo, cualquier módem de la consola debe ser de un tipo que pueda requerir al usuario de marcación manual suministrar una contraseña para el acceso, y la contraseña del módem debe ser manejada cuidadosamente.

Acceso interactivo general

Hay más maneras de conseguir las conexiones interactivas a un CSS que los usuarios puede realizar. Usted puede utilizar estos métodos para manejar el CSS:

- Telnet
- Host del shell seguro (SSH)
- SNMP
- Consola
- FTP
- XML
- Administración de la Web

Publique el **comando restrict** para habilitar o inhabilitar. El CSS todavía escucha en el puerto determinado, pero cierra la conexión. De modo que los paquetes no golpeen estos puertos, configure las cláusulas del Access Control List (ACL) para negar los paquetes.

Es difícil ser cierto que todos los modos posibles de acceso se han bloqueado. En la mayoría de los casos, los administradores deben utilizar una cierta clase de mecanismo de autenticación para aseegurarse que los logines en todas las líneas son controlados. Los administradores deben asegurarse de que los logines estén controlados incluso en las máquinas que se suponen para ser inaccesibles de las redes no confiables.

Control del acceso a la consola

Por abandono, la consola autentica contra los perfiles del usuario localmente configurados. Para activar el TACACS+ o la autenticación de RADIUS, publique el comando global de la **autenticación de la consola** y las opciones asociadas.

Control del vtys

Por abandono, el vtys autentica contra los perfiles del usuario localmente configurados. Para activar el TACACS+ o la autenticación de RADIUS, publique el comando global de la **autenticación virtual** y las opciones asociadas.

Soporte de SSH

Si su software support un protocolo de acceso encriptado tal como SSH, Cisco recomienda que usted habilita solamente ese protocolo y inhabilita el acceso de Telnet cuando usted quiere utilizar al servidor SSH. Para habilitar el daemon ssh (SSHD), usted necesita una licencia del servidor del SSHD, que habilita la funcionalidad SSHD en el estándar y las versiones mejoradas del software CSS. Publique los **comandos sshd**. Refiera a configurar los Network Protocol CSS para más información.

Nota: Soporte del SSH versión 1 encendido en 4.01. Soporte del SSH versión 2 encendido en 5.20.

RADIUS

A partir de la versión 5.00 y posterior, usted puede configurar el CSS para utilizar el RADIUS para la autenticación de usuario. Para configurar el CSS para la autenticación de RADIUS, refiera a configurar los perfiles del usuario y los parámetros CSS.

Nota: Un usuario/un perfil del grupo requiere solamente los atributos de RADIUS de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF), tipo de servicio [006] = administrativo.

Esta lista identifica los códigos del mensaje del debug:

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

Para ver los debugs que se asocian a los inicios de sesión en RADIUS, publique estos comandos:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Éste es un ejemplo de un debug de la autenticación satisfactoria:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Éste es un ejemplo de una autenticación que falló debido a un nombre de usuario incorrecto o una contraseña:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Éste es un ejemplo de una autenticación que falló porque no configuran al tipo de servicio del atributo de RADIUS 006 del perfil del usuario:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

TACACS+

En la versión 5.03 y posterior, usted puede configurar el CSS para utilizar el TACACS+ para la autenticación de usuario. Para configurar el CSS para autenticación de TACACS+, refiera a los Release Note para el Cisco CSS 11000 series.

Para ver los debugs que se asocian a los logines TACACS+, publique estos comandos:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Éste es un ejemplo de un debug de la autenticación satisfactoria:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Éste es un ejemplo de una autenticación fallida debido a un nombre de usuario incorrecto o una contraseña:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Banners de Advertencia

En algunas jurisdicciones, usted puede facilitar grandemente el proceso de civil y/o el proceso penal de los crackers que se rompen en sus sistemas si usted proporciona un banner que informe a los usuarios no autorizados que su uso es desautorizado. Otras jurisdicciones prohíben el monitor de las actividades incluso de los usuarios no autorizados a menos que usted haya tomado las medidas para notificar a los usuarios de su intento para hacer tan. Una manera de proporcionar esta notificación es ponerlo en un mensaje del anuncio. Usted puede configurar un mensaje del anuncio con el **comando set banner** CSS. Este comando fue introducido en 5.03.

Los requisitos de notificación legal son complejos y varían en cada jurisdicción y situación. Incluso dentro de las jurisdicciones, las opiniones legales varían. Discuta este problema con su asesor legal. En cooperación con el consejo, considere cuáles de estos avisos de poner en su banner:

- Un aviso que estado específicamente solamente el personal autorizado es iniciar sesión a o utiliza el sistema y quizás la información sobre quién puede autorizar el uso.
- Un aviso que cualquier uso no autorizado del sistema es ilegal y puede estar conforme a civil y/o a las sanciones penales.
- Un aviso que cualquier uso del sistema puede ser registrado o ser monitoreado sin previó aviso y que los registros resultantes se pueden utilizar como pruebas ante el tribunal.
- Avisos específicos que son requeridos por las legislaciones locales.

Por las razones de la Seguridad (bastante que legal), no incluya en su anuncio de inicio de sesión esta información sobre su CSS:

- Nombre
- Modelo

- Software que se ejecuta
- Propietario

Servicios de administración configurados normalmente

Muchos usuarios manejan sus redes con el uso de los protocolos con excepción del inicio de sesión remoto interactivo. Para este fin, los protocolos más comunes son SNMP y HTTP. La mayoría de la opción segura no es habilitar estos protocolos en absoluto. Sin embargo, si usted ha habilitado uno de los protocolos, asegúrelo como esta sección describe.

SNMP

El SNMP es muy ampliamente utilizado para el dispositivo de red que monitorea y, con frecuencia, para los cambios de configuración. El SNMP tiene dos revisiones, SNMPv1 y SNMPv2 estándar importantes. Su CSS admite la versión SNMP 2C (SNMPv2C), que se conoce como SNMP basado en la Comunidad. El CSS genera los desvíos en el formato del SNMPv1.

Para controlar el acceso SNMP al CSS, publique el **comando no restrict snmp** y el **comando restrict snmp**. El acceso con el SNMP se habilita por abandono. Si usted inhabilita el acceso con el SNMP, el CSS todavía escucha en el puerto determinado 1, pero cierra la conexión. Configure las cláusulas ACL para negar los paquetes de modo que los paquetes no golpeen el puerto SNMP.

Desafortunadamente, el SNMPv1 y el SNMPv2C utilizan un esquema de autenticación muy débil que se base en una cadena de comunidad. La autenticación asciende a una contraseña corregida que se transmita sobre la red sin el cifrado. Si usted debe utilizar el SNMPv2C, tenga cuidado de elegir las cadenas de comunidad indeterminadas (y no utilice, por ejemplo, el público o el soldado). Si en todo el posible, evite el uso de las mismas cadenas de comunidad para todos los dispositivos de red. Utilice una diversa cadena o cadenas para cada dispositivo, o por lo menos para la cada área de la red. No utilice de la misma forma un string (cadena de caracteres) de sólo lectura y uno de sólo escritura. Si es posible, haga la interrogación periódica SNMPv2C con una cadena de comunidad de sólo lectura. Las cadenas de lectura/escritura del uso solamente para real escriben las operaciones.

El SNMPv2C no es conveniente de utilizar a través del Internet pública por estas razones:

- El SNMPv2C utiliza las cadenas de autentificación de texto claro.
- El SNMPv2C es un protocolo de transacción de basado en datagrama que es fácilmente spoofed.
- La mayoría de las implementaciones de SNMP envía esas cadenas repetidas veces como parte de las consultas periódicas.

Considere cuidadosamente las implicaciones antes de que usted utilice el SNMPv2C a través del Internet pública.

En la mayoría de las redes, los mensajes SNMP legítimos vienen solamente de las ciertas estaciones de administración. Si los mensajes SNMP legítimos vienen solamente de las ciertas estaciones de administración en su red, considere el uso de los ACL que se aplican a los VLAN de circuitos para negar los mensajes SNMP no solicitados.

Las estaciones de administración SNMP a veces tienen inmensas bases de datos de

autenticación de información, tal como cadenas de comunidad. Esta información puede proporcionar el acceso a muchos CSS y a otros dispositivos de red. Esta concentración de información hace que la administración de SNMP coloca un objetivo natural para el ataque. Asegure la estación de la administración de SNMP por consiguiente.

HTTP

La configuración remota de soporte del CSS vía el protocolo HTTP con el uso de los documentos del Lenguaje de marcado extensible (XML). En la WebNS versión 4.10 o anterior, usted puede alcanzar el acceso a las interfaces de usuario de la Administración de dispositivos de WebNS en el texto claro si usted hojea al puerto TCP 8081. El acceso HTTP es generalmente equivalente al acceso interactivo al CSS. El protocolo de autenticación que se utiliza para el HTTP es equivalente al envío de una contraseña de texto sin cifrar a través de la red. Desafortunadamente, no hay disposición eficaz en el HTTP para basado en el desafío o las contraseñas de USO único. Por lo tanto, el HTTP es relativamente una elección riesgosa para el uso a través del Internet pública.

Si usted elige utilizar el HTTP para la Administración, restrinja el acceso a los IP Addresses apropiados con el uso de los ACL que se aplican a los VLAN de circuitos. Para controlar el acceso HTTP XML al CSS, publique el **comando no restrict xml** y el **comando restrict xml**. En versiones posteriores de WebNS, el comando ha cambiado al **estado red-MGT** *[neutralización | permiso]*. El acceso con HTTP XML se inhabilita por abandono. Para controlar el acceso del usuario de la Administración de dispositivos HTTP WebNS, publique el **comando no restrict web-mgmt** y el **comando restrict web-mgmt**. La interfaz de usuario de la Administración de dispositivos de WebNS se inhabilita por abandono. Usted debe configurar el **comando no restrict xml** y el **comando no restrict web-mgmt** para hojear al CSS en el puerto 8081.

En la versión 5.00 y posterior, si usted HTTP-hojea a la dirección de circuito en el puerto 8081, reorientan al navegador para utilizar el HTTPS y para conectar con la misma dirección de circuito.

HTTPS

La configuración remota de soporte del CSS con el protocolo seguro HTTP (HTTPS). Este Secure Socket Layer (SSL) protege las Transferencias de datos (que pueden incluir las contraseñas) entre la interfaz de usuario de la Administración de dispositivos de WebNS y su buscador Web.

Para controlar el acceso del usuario de la Administración de dispositivos HTTPS WebNS, publique el **comando no restrict web-mgmt** y el **comando restrict web-mgmt**. La interfaz de usuario de la Administración de dispositivos de WebNS se inhabilita por abandono. Si se inhabilita, el CSS continúa escuchando en el puerto determinado pero cierra la conexión. De modo que los paquetes no golpeen el puerto TCP 443 SSL, configure las cláusulas ACL para negar los paquetes.

Administración y acceso interactivo sobre el Internet (y otras redes no confiables)

Muchos usuarios manejan sus CSS remotamente, y esto es a veces realizado sobre Internet. Todo acceso remoto sin cifrar implica algunos riesgos, pero el acceso mediante una red pública como Internet es particularmente peligroso. Todos los planes de administración remota, que incluyen el acceso interactivo, el HTTP, y el SNMP, son vulnerables.

Los ataques que esta sección discute son los relativamente sofisticados, pero ellos están de ninguna manera fuera del alcance de los crackers de hoy. Los proveedores de red pública que toman las medidas de seguridad apropiada pueden frustrar a menudo estos atacantes. Evalúe su nivel de confianza en las medidas de seguridad que todos los proveedores que llevan su uso del tráfico de administración. Incluso si usted confía en sus proveedores, toma por lo menos algunos pasos para protegerse contra los resultados de cualquier equivocaciones que estos proveedores pudieran incurrir en.

Todas las precauciones en esta sección aplican tanto a los host en cuanto al CSS. Mientras que este documento discute cómo proteger las sesiones de conexión al sistema CSS, también miran en el uso de los mecanismos análogos para proteger sus host si usted administra esos host remotamente. La administración de Internet remota es útil, pero requiere la atención apropiada a la Seguridad.

Sabueso del paquete

Los crackers se rompen con frecuencia en los ordenadores que los Proveedores de servicios de Internet poseen, o en los ordenadores en otras Redes grandes. Los crackers instalan los programas del sabueso de paquete, que monitorean el tráfico que pasa a través de la red. Estos programas del sabueso de paquete roban los datos, tales como contraseñas y cadenas de comunidad SNMP. Los operadores de la red han comenzado a mejorar su Seguridad, que hace este hurto más difícil. Sin embargo, este hurto sigue siendo relativamente común. Además del riesgo de los intrusos exteriores, el personal de ISP poco escrupuloso puede también instalar los succionadores. Cualquier contraseña que se envíe sobre un canal sin encripción es en peligro, que incluye el login y las contraseñas habilitadas para sus CSS.

Si usted puede, evitar registrar en su CSS con el uso de cualquier protocolo sin encripción sobre cualquier red no confiable. Si su software CSS la soporta, utilice un protocolo de inicio de sesión encriptado tal como SSH.

Si usted no tiene acceso a un Remote Access Protocol cifrado, otra posibilidad es utilizar un sistema de contraseñas de USO único tal como S/KEY o OPIE, así como un TACACS+ o un servidor de RADIUS, para controlar los inicios de sesión interactivo y el acceso privilegiado a su CSS. La ventaja es que una contraseña robada es inútil. Una contraseña robada es hecha inválida por la misma sesión en quien se roba. Los datos que se transmiten en la sesión y no relacionado con las contraseñas siga siendo disponible para los cotillas, solamente muchos programas del sniffer se configuran para concentrar en las contraseñas.

Si usted debe enviar a las sesiones telnets de las contraseñas sobre texto sin cifrar, cambie sus contraseñas con frecuencia. y mucha atención de la paga a la trayectoria que sus sesiones atraviesan.

Otros peligros del acceso a Internet

Además de los sabuesos de paquete, la Administración del internet remoto de un CSS presenta estos riesgos de seguridad:

- Para manejar un CSS sobre Internet, usted debe permitir que por lo menos algunos host de Internet tengan acceso al CSS. Estos host pueden ser comprometidos, o sus direccionamientos pueden ser spoofed. Cuando usted permite el acceso interactivo de Internet, usted hace a su seguridad dependa, no sólo en sus propias medidas antispoofing,

pero en las medidas antispoofing de los proveedores de servicio que están implicados.Usted puede reducir estos peligros si usted realiza estas acciones:Aseegurese que todos los host que se permiten para iniciar sesión a su CSS están bajo su propio control.Utilice los protocolos de inicio de sesión encriptados con la autenticación robusta.

- A veces, el acceso a una conexión TCP no encriptada (tal como una sesión telnet) es posible obtener. Alguien que consigue el acceso a este tipo de sesión puede tomar realmente el control lejos de un usuario se abra una sesión que. Tales ataques no son casi tan comunes como el paquete sencillo que huele y pueden ser complejos montar. Sin embargo, tales ataques son posibles, y un atacante que tiene su red específicamente en la mente mientras que una blanco puede utilizarlos. La única solución real al problema de robo de sesión es utilizar un Management Protocol fuertemente autenticado, cifrado.
- Los ataques de la negación de servicio (DOS) son relativamente comunes en Internet. Si su red está bajo ataque DOS, usted puede no poder alcanzar su CSS para recoger la información o tomar la acción defensiva. Incluso un ataque en la red algún otro puede empeorar el Acceso de administración a su propia red. Aunque usted pueda tomar las medidas para hacer su red más resistente a los ataques DOS, la única defensa real contra este riesgo es tener un separado, canal de administración fuera de banda (tal como un módem de marcación manual) para el uso en las emergencias.

Registro

Los Ciscos CSS pueden el registrar información sobre una variedad de eventos, muchos cuyo tenga importancia por su relación con la seguridad. Los registros pueden ser inestimables para la caracterización y la respuesta a los incidentes de seguridad. Usted puede publicar el **comando logging subsystem** para habilitar abre una sesión el CSS. El nivel de registro predeterminado es warning-4 para todos los subsistemas.

Publique estos comandos para que la orden de apertura de sesión del subsistema recoja esta información:

- Ingresos del usuario al sistema
- Logoutes
- Autenticación RADIUS
- autenticación TACACS+

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Nota: El comando netman subsystem cubre los debugs TACACS+.

De un punto de vista de la seguridad, los eventos más importantes que el Registro del sistema registra generalmente incluyen estos eventos:

- Cambios de estado de la interfaz
- Cambios a la configuración del sistema
- Coincidencias ACL

```
logging subsystem netman level info-6
!--- Note that the default logging level is warning-4, which does !--- not appear in the
```

```
configuration. logging commands enable
logging subsystem acl level debug-7
```

El Monitoreo remoto (RMON) le permite monitorea y analiza remotamente la actividad de los paquetes en los accesos de Ethernet CSS. El RMON también permite la configuración de la alarma para el monitor de los objetos de MIB y permite que la configuración de evento le notifique de estas condiciones de alarmar. Un evento RMON es la acción que ocurre cuando se acciona una alarma RMON asociada. Usted puede configurar un evento de la alarma tales que, cuando ocurre un evento de la alarma, genera un o ambo elementos:

- Un evento del registro
- Un desvío a una estación de administración de red SNMP

Salve la información de registro

Por abandono, el CSS guarda los mensajes del registro del inicio y del evento del subsistema a los archivos del registro en el duro o el disco Flash. El contenido de estos archivos se registra en el texto ASCII. Usted puede también configurar el CSS para enviar los mensajes del registro a una sesión CSS activa, a la dirección de correo electrónico, o a otro sistema del host.

El tamaño máximo de un archivo del registro local es 50 MB para los sistemas disco-basados duros y el 10 MB para los sistemas disco-basados Flash.

Los mensajes del registro del subsistema son los eventos del subsistema que ocurren durante la operación del CSS. El CSS guarda estos mensajes en el archivo de sys.log. El CSS crea este archivo cuando ocurre el primer evento del subsistema que debe ser registrado. El CSS determina que los mensajes de subsistema a registrar por su nivel de registro configurado.

La mayoría de las instalaciones más grandes tienen los servidores de Syslog. Usted puede publicar el **comando logging host** para enviar la información de ingreso al sistema a una daemon del Syslog en el sistema del host. Incluso si usted tiene un servidor de Syslog, usted debe todavía habilitar el registro local al disco.

Todos los registros son con impresión horaria con el mes, día, y miden el tiempo al segundo. Si usted configura una fuente de la hora común tal como protocolo de tiempo de la red sencillo (SNTP) para sus registros, usted puede seguir más fácilmente la secuencia de eventos registrados. Para configurar al servidor SNTP en el CSS, publique el **comando sntp**. El SNTP fue introducido en el código 5.00.

Registre las violaciones de lista de acceso

Si usted utiliza los ACL al filtrar tráfico que accede las direcciones de circuito o los direccionamientos de la regla de contenido IP virtual (VIP), usted puede elegir registrar los paquetes que violan sus criterios del filtro. Para habilitar la apertura de sesión de la cláusula ACL, publique el **comando clause - log enable**. También, publique el **comando logging subsystem acl level debug-7**. El CSS registra esta información:

- Protocolo
- Puerto de origen
- Puerto de destino
- Dirección IP de origen
- Dirección IP de destino

Intente evitar la configuración del registro para las entradas ACL que hacen juego muy un gran número de paquetes. Esta configuración hace los archivos del registro crecer excesivamente grandes y puede cortar en el rendimiento del sistema.

Usted puede también utilizar el registro de ACL para caracterizar el tráfico que se asocia a los ataques a la red. En este caso, usted configura el registro de ACL para registrar el tráfico sospechoso. Usted puede caracterizar en el router Cisco en el lado de Internet del CSS para hacer un ACL a mano. Refiera a caracterizar y a localizar las inundaciones de paquetes usando los routeres Cisco para más información.

Nota: El CSS ACL se aplica solamente en los paquetes de entrada. El ACL no marca los paquetes que son salientes de una interfaz.

Asegure el Routing IP

Esta sección discute algunas medidas de seguridad básica que se relacionen con la manera de la cual del router los paquetes del IP adelante. Refiera al esencial del ISP de Cisco - El IOS esencial ofrece cada ISP debe considerar para más información sobre estos problemas.

Por abandono, una configuración del CSS:

- Restringe el número de paquetes SYN que vayan a un VIP antes de que el CSS lo registre como ataque DOS**Nota:** Este comportamiento no puede ser inhabilitado.
- Niega los broadcastes dirigidos
- Niega los paquetes con el mismo IP Address de origen y de destino
- Niega los IP Addresses del origen de multidifusión
- Niega a puerto de origen o de destino 0 paquetes

Antispoofing

Muchos ataques a la red confían en un atacante que falsifique, o las parodias, las direcciones de origen de los datagramas IP. Algunos ataques confían en el spoofing para que el ataque trabaje. Los otros ataques son mucho más duros de localizar si los atacantes pueden utilizar el direccionamiento algún otro en vez de su propio direccionamiento. Por lo tanto, prevenir el spoofing dondequiera que sea posible tiene valor para los administradores de la red.

Antispoofing debe ser hecho en cada punta en la red donde está práctica. Pero antispoofing es generalmente el más fácil de hacer y el más eficaz en las fronteras entre los bloqueos de dirección grandes o entre los dominios de la Administración de red. Antispoofing en cada router en una red es generalmente poco práctico porque la determinación cuyo las direcciones de origen pueden aparecer legítimo en cualquier interfaz dada es difícil.

Si usted es un Proveedor de servicios de Internet (ISP), usted puede encontrar que protección efectiva contra falsificación, así como otras medidas de seguridad eficaces, las causas costosas, los suscriptores con problema para llevar su negocio otros proveedores. Si usted es un ISP, tenga especialmente cuidado de aplicar los controles antispoofing en los pools de marcado manual y otros puntos de conexión del usuario final.

Nota: Refiera al RFC 2267 .

Los administradores del escudo de protección corporativo o los routeres perimetrales instalan a

veces las medidas antispoofing de modo que los host en Internet no puedan asumir a las direcciones del host interno. Sin embargo, los host internos pueden todavía asumir a las direcciones del host en Internet. Intente prevenir el spoofing en las ambas direcciones. Hay por lo menos tres buenas razones para instalar antispoofing en las ambas direcciones en un escudo de protección de organización:

- Tientan a los usuarios internos menos para intentar poner en marcha los ataques a la red y menos probable tener éxito si intentan.
- Los host internos que se configuran mal accidentalmente son menos probables causar el problema para los sitios remotos. Por lo tanto, son menos probables generar la insatisfacción del cliente.
- Muchas veces los intrusos exteriores entran a las redes como plataformas de lanzamiento para otros ataques. Estos intrusos pueden estar menos interesados en una red con protección de simulación saliente.

Antispoofing con los ACL

Desafortunadamente, simplemente a los comandos list que proporcionan la protección contra simulación apropiada no es práctica. La configuración ACL depende demasiado de la red individual. El objetivo básico es desechar los paquetes que llegan en las interfaces que no son trayectos viables de las direcciones de origen supuestas de esos paquetes. Por ejemplo, en un dos-circuito CSS que conecte un bloque de servidores con Internet, usted quiere desechar cualquier datagrama que llegue en el circuito de Internet, pero tiene un campo de dirección de origen que demande que vino de una máquina en el bloque de servidores.

Semejantemente, usted quiere desechar cualquier datagrama que llegue en la interfaz que está conectada con el bloque de servidores, pero que tiene un campo de dirección de origen que demande que vino de una máquina fuera del bloque de servidores. Si los recursos de la CPU permiten, aplique antispoofing en cualquier circuito donde está posible una determinación de qué tráfico puede llegar legítimo.

Los ISP que llevan el tráfico de tránsito pueden haber limitado las oportunidades de configurar los ACL antispoofing, pero tales ISP pueden filtrar generalmente fuera del tráfico que demanda originar dentro del espacio de la dirección de ese ISP.

Los filtros antispoofing se deben construir generalmente con las entradas ACL. Los paquetes se deben filtrar en los circuitos a través de los cuales los paquetes llegan. El CSS puede aplicar solamente los ACL a los paquetes de entrada.

Cuando existen los ACL antispoofing, deben rechazar siempre los datagramas con el broadcast o las direcciones de origen multicast. Por abandono, el CSS niega estos datagramas. Los ACL antispoofing deben también rechazar los datagramas que tienen el Loopback Address reservado como dirección de origen. Además, usted debe generalmente hacer que un ACL antispoofing filtre hacia fuera todo el Internet Control Message Protocol (ICMP) reorienta, sin importar la dirección de origen o de destino. El CSS ACL no permite que usted especifique el tipo ICMP para negar. En lugar, publique el **comando no redirects** para configurar todos los IP Address de circuito para no validar las redirecciones ICMP. Éstos son los comandos:

```
clause # deny any 127.0.0.0 255.0.0.0 destination any
clause # deny any 0.0.0.0 0.0.0.0 destination any
```

Nota: La cláusula # niega cualquier comando any del destino de 0.0.0.0 0.0.0.0 filtra hacia fuera

los paquetes de muchos clientes del Bootstrap Protocol (BOOTP) /DHCP. Por lo tanto, el comando no es apropiado en todos los entornos.

Control de los broadcastes dirigidos

Extremadamente común y ataques populares DOS del smurf, y algunos ataques relacionados, broadcastes dirigidos por IP del uso. Por abandono, el CSS se configura con el **comando no ip subnet-broadcast**, que niega los broadcastes dirigidos.

Un broadcast dirigido por IP es un datagrama que se envía a la dirección de broadcast de una subred a la cual la máquina remitente no se asocie directamente. El broadcast dirigido se rutea a través de la red como paquete de unidifusión hasta que el broadcast dirigido llegue la subred de destino. En la subred, el broadcast dirigido se convierte en un broadcast de la capa de link. Debido a la naturaleza de la arquitectura del IP Addressing, solamente el router más reciente o acoda 3 que el dispositivo de red en el encadenamiento puede identificar concluyente un broadcast dirigido. Este dispositivo es el que está conectado directamente con la subred de destino. Algunas veces las difusiones directas se utilizan con objetivos legítimos, pero tal uso no es habitual fuera de la industria de servicios financieros.

En un ataque smurf, el atacante envía los pedidos de eco ICMP de una dirección de la fuente falsificada a una dirección de broadcast dirigido. Como consecuencia, todos los host en la subred de destino envían las contestaciones a la fuente falsificada. Cuando un atacante envía una secuencia continua de ese pedido, el atacante puede crear una secuencia de respuesta mucho más grande, que puede inundar totalmente al host cuyo se falsifica direccionamiento.

Refiera a más último de los establecimientos de rechazo del servicio: Descripción e información del “Smurfing” para minimizar los efectos para que una estrategia bloquee los ataques smurf en algunos routeres de escudo de protección (que depende del diseño de red). El documento también proporciona la información general en el ataque smurf.

Integridad del trayecto

Muchos ataques dependen de la capacidad de influenciar las trayectorias que los datagramas toman a través de la red. Si los crackers controlan la encaminamiento, hay una ocasión que pueden spoof el direccionamiento de la máquina de otro usuario y tener el tráfico de retorno enviado a ellos. En algunos casos, los crackers pueden interceptar y los leeres datos que se piensan para algún otro. La encaminamiento se puede también interrumpir puramente para los propósitos DOS.

Ruteo de origen IP

Protocolo IP soporta los opciones de Source Routing que permiten que el remitente de un IP datagram controle la ruta que el datagrama toma hacia el destino final, y generalmente, la ruta que cualquier contestación toma. Estas opciones rara vez se utilizan para fines legítimos en redes reales. Algunas más viejas instrumentaciones de IP no procesan los paquetes Source-Routed correctamente. Alguien puede enviar los datagramas con los opciones de Source Routing y, para causar un crash posiblemente las máquinas que ejecutan estas implementaciones.

El CSS se configura por abandono con el **comando no ip source-route set**. El CSS nunca adelante un paquete del IP que lleva un opción de Source Routing. Deje el comando default configurado a menos que usted sepa que su red necesita el Source Routing.

Mensajes de redirección ICMP

Un mensaje de la redirección ICMP da instrucciones un nodo extremo para utilizar a un router específico como la trayectoria a un destino determinado. En una red del IP que funcione correctamente, un router envía reorienta solamente a los host en las subredes locales del router. El nodo extremo nunca envía una reorientación, y la reorienta nunca atraviesa más de un salto de la red. Sin embargo, un atacante puede violar estas reglas, y algunos ataques se basan en estas reglas. Filtre hacia fuera las redirecciones ICMP entrantes en las interfaces de entrada de cualquier router que mienta en una frontera entre los dominios administrativos. Además, usted puede tener cualquier ACL que se aplique en el lado de entrada de una interfaz del router de Cisco filtre hacia fuera todas las redirecciones ICMP. Esto que filtra no causa ningún efecto en el funcionamiento en una red que se configure correctamente.

Este tipo de filtración previene reorienta solamente los ataques que los atacantes remotos ponen en marcha. Además, los atacantes pueden utilizar reorientan para causar el problema significativo si el host del atacante está conectado directamente con el mismo segmento que un host que esté bajo ataque.

Por abandono, el CSS se configura para validar reorienta en cada IP Address de circuito se configure que. Publique el **comando no redirect** bajo IP Address de circuito para apagar esta función.

Autenticación y filtrado del protocolo de ruteo

Si usted utiliza un Dynamic Routing Protocol que soporte la autenticación, habilite esa autenticación. La autenticación previene algunos ataques maliciosos en la infraestructura de ruteo y puede también ayudar a prevenir que los dispositivos ficticios mal configurado en la red pueden estropear.

Por las mismas razones, los proveedores de servicio y otros operadores de las Redes grandes pueden considerar el uso del filtrado de Routes. Con el filtrado de Routes, los routeres de la red no validan claramente la información de ruteo incorrecta. Para el filtrado de Routes, utilice el parámetro de la distribuir-**lista** en el comando. El uso excesivo de filtrado de Routes puede destruir las ventajas del Dynamic Routing. Pero el uso selectivo ayuda a menudo a prevenir los malos resultados. Por ejemplo, si usted utiliza un Dynamic Routing Protocol para comunicar con una red del cliente del stub, no valide ninguna rutas de ese cliente con excepción de las rutas al espacio de la dirección que usted ha delegado realmente al cliente.

El CSS no puede las rutas de filtro. En lugar, routing peer de la configuración del CSS con esta función.

Este documento no proporciona la Instrucción detallada en la configuración de la autenticación de ruteo y del filtrado de Routes. Tal documentación está en el cisco.com y a otra parte disponible. Usted puede referir al esencial del ISP de Cisco del documento - el IOS esencial ofrece cada ISP debe considerar. Debido a la complejidad, la búsqueda experimentó el consejo si usted es un novato antes de que usted configure estas características en las redes importantes.

Administración de sobrecarga’

Muchos ataques DOS confían en las inundaciones de paquetes inútiles. Estas inundaciones congestionan los links de redes, reducen la velocidad de los hosts, y también pueden sobrecargar

los routers. La configuración correcta del router puede reducir el impacto de tales saturaciones.

Una parte importante de administración de inundaciones es la conciencia de donde las mermas en el rendimiento pueden ocurrir. Si una inundación sobrecarga una línea T1, filtre hacia fuera la inundación en el router en el extremo de origen de la línea. Hay poco o nada de efecto si usted filtra en el extremo de destino en este caso. Si el router sí mismo es la mayoría del componente de red sobrecargado, usted puede hacer las materias peores si usted filtra las protecciones que ponen los pedidos excesivos en el router. Tenga esto presente cuando usted considera una implementación de las sugerencias en esta sección.

Inundación de tránsito

Usted puede utilizar las características de Cisco QoS en el Routers por aguas arriba del ® del Cisco IOS para proteger el CSS, los host, y los links contra algunas clases de inundaciones. Desafortunadamente, este documento no proporciona un tratamiento general de esta clase de administración de inundación. También, la protección depende pesadamente del ataque. El único simple, consejo pertinente es generalmente utilizar el Espera equitativa ponderada (WFQ) dondequiera que los recursos de la CPU puedan soportar el WFQ. El WFQ es el valor por defecto para las líneas de los seriales de baja velocidad en versiones del Cisco IOS Software posteriores. Las otras funciones del interés posible incluyen:

- Committed Access Rate (CAR)
- Control de tráfico genérico (GTS)
- El formar la cola a medida

A veces, usted puede configurar estas características cuando bajo ataque activo.

El CSS puede reducir el impacto de los ataques de inundación SYN en el VIP y los servidores reales. Por abandono, el CSS restringe el número de SYN y de entradas en contacto de tres vías incompletas y las registra como ataques DOS.

Refiera a la información de referencia de seguridad para más información.

Servicios posiblemente innecesarios

Como regla general, inhabilite cualquier servicio innecesario en cualquier router que sea accesible de una red potencialmente hostil. Los servicios que esta sección enumera son a veces útiles. Pero inhabilite estos servicios si no están en el uso activo.

SNTP

El SNTP no es especialmente peligroso, pero cualquier servicio innecesario puede presentar un trayecto de penetración. Si usted utiliza realmente el SNTP, esté seguro de configurar explícitamente la fuente horaria de confianza. El SNTP no utiliza la autenticación. Una corrupción de la base de tiempo es una buena manera de derribar ciertos protocolos de Seguridad. El mejor método es utilizar una fuente que sea interna y menos probable ser spoofed.

Cisco Discovery Protocol

El Cisco Discovery Protocol (CDP), que fue introducido en WebNS 5.10, se utiliza para algunas funciones de administración de red. El CDP es peligroso porque cualquier sistema en un

segmento directamente conectado puede realizar estas acciones:

- Aprenda que el router es un dispositivo de Cisco
- Determine el número de modelo y la versión de software que los funcionamientos

Un atacante puede utilizar esta información para diseñar los ataques contra el CSS. La información CDP está accesible sólo para los sistemas conectados directamente. El CSS hace publicidad solamente de la información CDP. El CSS no escucha. Usted puede publicar el comando global configuration del **no cdp run** para inhabilitar el protocolo CDP. Usted no puede inhabilitar el CDP en el CSS sobre una base del por interface.

Estancia actualizada

Como todo el software, el software de Cisco WebNS tiene bug. Algunos de estos errores tienen consecuencias en la seguridad. Además, los nuevos ataques continúan siendo inventados. Y el comportamiento que era considerado correcto cuando un software fue escrito puede tener efectos nocivos cuando el comportamiento se explota deliberadamente.

Cuando se encuentra gran vulnerabilidad de la nueva seguridad en un producto Cisco, generalmente Cisco emite una nota de asesoramiento acerca de la vulnerabilidad. Refiera a la política de información de la vulnerabilidad de seguridad sobre el proceso con el cual se publican estos avisos. Refiera a los Security Advisory para los avisos.

Casi cualquier conducta inesperada de cualquier software puede crear un riesgo de seguridad en alguna parte. Bug de la mención de las recomendaciones solamente que tienen implicaciones directas para la seguridad del sistema. Usted puede aumentar su Seguridad si usted mantiene su software actualizado, incluso en ausencia de cualquier Security Advisory.

Algunos problemas de seguridad no son el resultado de los bug de software, y los administradores de la red deben permanecer enterados de las tendencias en los ataques. Hay varios sitios web, listas de correo de Internet, y grupos de noticias de Usenet que se refieren a estas tendencias.

Información Relacionada

- RFC 2267
- Security Advisory
- Directiva de la vulnerabilidad de seguridad
- Información de referencia de seguridad
- Configurar los Network Protocol CSS
- Configurar los métodos de Acceso Remoto CSS
- Configurar los perfiles del usuario y los parámetros CSS
- Release Notes
- Caracterización y seguimiento de la inundación de paquetes usando routers de Cisco
- Esencial del ISP de Cisco - El IOS esencial ofrece cada ISP debe considerar
- El más último de los establecimientos de rechazo del servicio: Descripción e información del “Smurfing” para minimizar los efectos
- Soporte Técnico y Documentación - Cisco Systems