ASA: Envíe el tráfico de la red del ASA al ejemplo de configuración CSC-SSM

Contenido

Introducción

Este documento proporciona una configuración de muestra para que cómo envíe el tráfico de la red del dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA) al módulo de Servicios de seguridad contento de la Seguridad y del control (CSC-SSM).

El CSC-SSM proporciona la protección contra los virus, el spyware, el Spam, y el otro tráfico no deseado. Logra esto analizando el tráfico FTP, HTTP, POP3, y S TP que es desviado a él por el dispositivo de seguridad adaptante. Para forzar el ASA para desviar el tráfico al CSC-SSM, usted necesita utilizar el Marco de políticas modular.

Refiera al ASA: Envíe el tráfico de la red del ASA al ejemplo de configuración AIP SS para enviar el tráfico de la red que pasa a través del dispositivo de seguridad adaptante de las 5500 Series de Cisco ASA (ASA) al módulo avanzado del (IPS) del módulo de Servicios de seguridad del examen y de la prevención (AIP-SSM).

Nota: El CSC-SSM puede analizar el tráfico FTP, HTTP, POP3, y S TP solamente cuando el puerto destino del paquete que pide la conexión es el puerto conocido para el protocolo especificado. El CSC-SSM puede analizar solamente estas conexiones:

- Conexiones FTP abiertas al puerto TCP 21
- Conexiones HTTP abiertas al puerto TCP 80
- Conexiones POP3 abiertas al puerto TCP 110
- Conexiones SMTP abiertas al puerto TCP 25

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Una comprensión básica de cómo configurar la versión de software 7.1 de los funcionamientos de las 5500 Series de Cisco ASA y posterior.
- El CSC-SSM ha estado instalado.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5520 con la versión de software 7.1 y posterior
- CSC-SSM-10 con la versión de software 6.1

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El CSC-SSM mantiene un archivo que contenga los perfiles de la firma del contenido sospechoso, actualizado regularmente de un servidor de actualización en Trend Micro. El CSC-SSM analiza el tráfico que recibe del dispositivo de seguridad adaptante y lo compara al contento lo perfila obtiene de Trend Micro. Él entonces adelante contenido legítimo encendido al dispositivo de seguridad adaptante para rutear, o los bloques y los informes contentan que es sospechoso.

Por abandono, CSC-SSM viene con una licencia baja que proporcione estas características:

- Detecta y toma la acción en los virus y el malware en el tráfico de la red
- Los bloques comprimidos o los archivos muy grandes que se exceden especificaron los parámetros
- Las exploraciones para y quitan el spyware, el adware, y otros tipos de grayware

Además, si se equipa de a más la licencia, también realiza estas tareas:

- Reduce el Spam y lo protege contra el fraude del phishing en su tráfico S TP y POP3
- Configura los filtros contentos que le permiten para permitir o para prohibir el tráfico del correo electrónico que contiene las palabras claves o las frases
- Filtros/bloques URL que usted no quisiera que los usuarios accedieran, o URL que se saben para haber ocultado o los propósitos malévolos

Nota: El CSC-SSM puede analizar las transferencias de archivos FTP solamente cuando el examen FTP se habilita en el ASA. Por abandono, se habilita el examen FTP.

Nota: El CSC-SSM no puede apoyar a la falla de estado porque el CSC-SSM no mantiene la información de conexión, y por lo tanto no puede proporcionar la unidad de transmisión por falla con la Información requerida para la falla de estado. Se caen las conexiones que un CSC-SSM está analizando cuando el dispositivo de seguridad en el cual el CSC-SSM está instalado falla. Cuando el dispositivo de seguridad adaptante espera llega a ser activo, adelante el tráfico analizado al CSC-SSM y las conexiones se reajusta.

Configurar

En una red en la cual el dispositivo de seguridad adaptante se despliegue con el CSC-SSM, usted configura el dispositivo de seguridad adaptante para enviar al CSC-SSM solamente los tipos de tráfico que usted quiere ser analizado.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

ASA - Diagrama de flujo del CSC SS

Este diagrama muestra el flujo de tráfico dentro del ASA y de CSC-SSM:

En este ejemplo, los clientes pueden ser los usuarios de la red que acceden un sitio web, descargan los archivos de un servidor FTP, o extraen el correo de un servidor POP3.

En esta configuración, éste es cómo los flujos de tráfico:

1. El cliente inicia una petición.
2. El dispositivo de seguridad adaptante recibe la petición y adelante la a Internet.
3. Cuando se extrae el contenido solicitado, el dispositivo de seguridad adaptante determina si sus políticas de servicio definen este tipo de contenido como uno que se deba desviar al CSC-SSM para explorar, y lo hacen tan si es apropiado.
4. El CSC-SSM recibe el contenido del dispositivo de seguridad adaptante, lo analiza y lo compara a su última actualización de los filtros del contenido de Trend Micro.
5. Si el contenido es sospechoso, el CSC-SSM bloquea el contenido y señala el evento. Si el contenido no es sospechoso, el CSC-SSM adelante el contenido solicitado de nuevo al dispositivo de seguridad adaptante para rutear.

Configuración inicial del CSC

En la configuración inicial, varios parámetros necesitan ser configurados. Aseegurese le haber recopilado la información requerida para estos parámetros antes de que usted comience.

Como el primer paso para configurar el CSC-SSM, inicie el ASDM de Cisco. Por abandono, usted puede acceder el CSC-SSM a través del IP Address de administración del ASA en https://192.168.1.1/. Usted necesita asegurarse de que su PC y la interfaz de administración del ASA estén en la misma red. Alternativamente, usted puede descargar el activador de ASDM para los accesos subsiguientes.

Configure estos parámetros con el ASDM:

1. Una vez en la ventana ASDM principal, elija la **configuración > Trend Micro contentan la Seguridad > la configuración del Asisitente** y hacen clic al **asistente para la configuración del lanzamiento**.
2. **Clave de activación:**El primer paso para obtener la clave de activación es identificar el Product Authorization Key (PAK) enviada junto con el producto. Contiene un código de barras y 11 caracteres hexadecimales. Por ejemplo, un PAK de la muestra puede ser 120106C7D4A.Utilice el PAK para registrar el CSC-SSM en la página web del registro de la licencia del producto (clientes registrados solamente). Después de que usted se registre, usted recibe las claves de activación por el email.
3. **Parámetros IP del puerto de administración:**Especifique la dirección IP, el netmask y el Gateway IP Address para la interfaz de administración del CSC.**Servidores DNS** — Dirección IP para el servidor DNS principal.
4. **Host y Domain Name** — Especifique un nombre del host así como el Domain Name del CSC-SSM.**Dominio entrante** — Domain Name usado por el mail server local como el entrante dominio de correo electrónico.**Nota:** Las directivas antispam se aplican solamente al tráfico del email que entran en este dominio.**Configuraciones de la notificación** — Dirección

de correo electrónico del administrador y el dirección IP del servidor y el puerto del email que se utilizarán para las notificaciones.

5. **Parámetros del acceso del host de administración:**Ingrese el IP Address y la máscara para cada subred y recíbalos que deba tener Acceso de administración al CSC-SSM.**Nota:** Por abandono, todas las redes tienen Acceso de administración al CSC-SSM. Por motivos de seguridad, Cisco recomienda que usted restringe el acceso a las subredes o a los host de administración específicos.
6. **Nueva contraseña para CSC-SSM:**Cambie la contraseña predeterminada, `Cisco`, a una nueva contraseña para el Acceso de administración.
7. En el paso 6 del asistente para la configuración del CSC, especifique el tipo de tráfico que se analizará.El dispositivo de seguridad adaptante desvía los paquetes al CSC-SSM después de que las políticas del firewall sean aplicadas pero antes de los paquetes salga la interfaz de egreso. Por ejemplo, los paquetes que son bloqueados por una lista de acceso no se remiten al CSC-SSM.Configure las políticas de servicio para especificar qué tráfico debe desviar el dispositivo de seguridad adaptante al CSC-SSM. El CSC-SSM puede analizar el tráfico HTTP, POP3, FTP, y S TP enviado a los puertos conocidos para esos protocolos.Para simplificar el proceso de la configuración inicial, este procedimiento crea una directiva de servicio global que desvíe todo el tráfico para los protocolos admitidos al CSC-SSM, entrante y saliente. Porque analizar todo el tráfico que venga a través del dispositivo de seguridad adaptante puede reducir el funcionamiento del dispositivo de seguridad adaptante y del CSC-SSM, usted quiere revisar esta política de seguridad más adelante. Por ejemplo, no es generalmente necesario analizar todo el tráfico que venga de su red interna porque viene de una fuente confiable. Si usted refina las políticas de servicio de modo que el CSC-SSM explore solamente el tráfico de las fuentes untrusted, usted puede alcanzar sus metas de la Seguridad y maximizar el funcionamiento del dispositivo de seguridad adaptante y del CSC-SSM.Complete estos pasos para crear una directiva de servicio global que identifique el tráfico que se analizará:El tecleo **agrega** para agregar un tipo nuevo de tráfico.Elija **global de la** lista desplegable de la interfaz.Salga de la fuente y de los Campos Destination fijados a **ningunos**.En el servicio sea, haga clic el botón de radio de los **puntos de suspensión (...)**. En este cuadro de diálogo, elija un servicio predefinido o el tecleo **agrega** para definir un nuevo servicio.En si el indicador luminoso LED amarillo de la placa muestra gravedad menor del CSC falla, después el área, elija si el dispositivo de seguridad adaptante si el tráfico seleccionado del permit or deny si el CSC-SSM es inasequible.Haga Click en OK para volver a la selección del tráfico para la ventana de la exploración del CSC.Haga clic en Next (Siguiente).
8. En el paso 7 del asistente para la configuración del CSC, ajustes de la configuración del estudio que usted ingresó para el CSC-SSM.Si le satisfacen con estas configuraciones, clic en Finalizar.El ASDM muestra un mensaje que indique que el dispositivo del CSC es activo ahora.Por abandono, el CSC-SSM se configura para realizar las exploraciones contentas de la Seguridad habilitadas por la licencia que usted compró, que puede incluir el contra virus, el anti-Spam, el anti-phishing, y el filtrado de contenido. También se configura para conseguir las actualizaciones periódicas del servidor de actualización de Trend Micro.Si estuvo incluido en la licencia usted compró, usted puede crear las configuraciones personalizadas para el bloqueo de URL y el Filtrado de URL, así como el email y los parámetros FTP. Vea el guía del administrador de la Seguridad y del control SS del contenido de Cisco para más información.

Cómo configurar el ASA para desviar el tráfico a CSC-SSM

Para forzar el ASA para desviar el tráfico al CSC-SSM, usted necesita utilizar el Marco de políticas modular. Complete estos pasos para lograr la identificación y la diversión del tráfico a CSC-SSM:

1. Cree una lista de acceso que haga juego el tráfico que usted quiere analizado por el CSC-SSM, para desviar el tráfico a CSC-SSM, con el comando **ampliado lista de acceso**:`hostname(config)#`**`access-list acl-name extended {deny | permit}`** *`protocol src_ip mask dest_ip mask operator port`*
2. Cree una correspondencia de la clase para identificar el tráfico que se debe desviar al CSC-SSM con el **comando class-map**:`hostname(config)#`**`class-map`** *`class_map_name`*
3. Una vez en el modo de la configuración de asignación de la clase, utilice el **comando access-list de la coincidencia** para identificar el tráfico con el uso de la lista de acceso especificada previamente:`hostname(config-cmap)#`**`match access-list`** *`acl-name`* `hostname(config-cmap)#`**`exit`**
4. Cree una correspondencia de políticas para enviar el tráfico al CSC-SSM con el **comando policy-map**:`hostname(config)#`**`policy-map`** *`policy_map_name`*
5. Una vez en el modo de la configuración de correspondencia de políticas, utilice el **comando class** para especificar la correspondencia de la clase, creada previamente, que identifica el tráfico que se analizará:`hostname(config-pmap)#`**`class`** *`class_map_name`*
6. Una vez en el modo de configuración de clase de la correspondencia de políticas, usted puede configurar éstos:Si usted quiere aplicar un límite del por-cliente para las conexiones simultáneas que el dispositivo de seguridad adaptante desvía al CSC-SSM, utilice el **comando connection del conjunto**, como sigue:`hostname(config-pmap-c)#`**`set connection per-client-max`** *`n`* donde está las conexiones simultáneas `n` máximas el dispositivo de seguridad adaptante permite cada cliente. Este comando evita que un solo cliente abuse de los servicios del CSC-SSM o de cualquier servidor protegido por el SS, que incluye la prevención de las tentativas en los ataques DOS en el HTTP, el FTP, el POP3, o los servidores SMTP que el CSC-SSM protege.Utilice el comando del **csc** para controlar cómo el ASA maneja el tráfico cuando el CSC-SSM es inasequible:`hostname(config-pmap-c)#`**`csc`** *`{fail-close | fail-open}`* donde el fracaso-*cierre* especifica que el ASA debe bloquear el tráfico si el CSC-SSM falla y en cambio, fracaso-*abierto* especifica que el ASA debe permitir el tráfico si el CSC-SSM falla.**Nota:** Esto se aplica al tráfico seleccionado por la correspondencia de la clase solamente. El otro tráfico no enviado al CSC-SSM no es afectado por un error CSC-SSM.
7. Pasado, aplique la correspondencia de políticas global o a una interfaz específica con el **comando service-policy**:`hostname(config-pmap-c)#`**`service-policy`** *`policy_map_name [global | interface interface_ID]`* donde está el nombre el `interface_id` asignado a la interfaz con el **comando nameif**.**Nota:** Se permite solamente una política global. Usted puede reemplazar la política global en una interfaz con la aplicación de una política de servicio a esa interfaz. Usted puede aplicar solamente una correspondencia de políticas a cada interfaz.

Diagrama de la red

Este diagrama es un ejemplo de un ASA 5500 configurado para estos parámetros:

El resumen del diagrama de la red ilustra éstos:

- Conexión HTTP a las redes externas
- Conexión FTP de los clientes dentro del dispositivo de seguridad a los servidores fuera del

dispositivo de seguridad
- Clientes POP3 de los clientes dentro del dispositivo de seguridad a los servidores fuera del dispositivo de seguridad.
- Conexiones SMTP entrantes señaladas al mail server interior

Configuración ASA

ASA5520

```
ciscoasa(config)#show running-config : Saved : ASA
Version 8.0(2) ! hostname ciscoasa domain-name
Security.lab.com enable password 2kxsYuz/BehvglCF
encrypted no names dns-guard ! interface
GigabitEthernet0/0 speed 100 duplex full nameif outside
security-level 0 ip address 172.30.21.222 255.255.255.0
! interface GigabitEthernet0/1 description INSIDE nameif
inside security-level 100 ip address 192.168.5.1
255.255.255.0 ! !--- Output suppressed access-list csc-
acl remark Exclude CSC module traffic from being scanned
access-list csc-acl deny ip host 10.89.130.241 any !---
In order to improve the performance of the ASA and CSC
Module. !--- Any traffic from CSC Module is excluded
from the scanning. access-list csc-acl remark Scan Web &
Mail traffic access-list csc-acl permit tcp any any eq
www access-list csc-acl permit tcp any any eq smtp
access-list csc-acl permit tcp any any eq pop3 ! !---
All Inbound and Outbound traffic for WEB, Mail services
is scanning. access-list csc-acl-ftp permit tcp any any
eq ftp !--- All Inbound and Outbound traffic for FTP
service is scanning. class-map csc-class match access-
list csc-acl ! class-map csc-ftp-class match access-list
csc-acl-ftp ! policy-map global_policy class csc-class
csc fail-open class csc-ftp-class csc fail-open policy-
map global_policy class inspection_default !--- Inspect
FTP traffic for scanning. inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect icmp inspect http service-
policy global_policy global !--- Output suppressed
```

Home Page del CSC

Configuración del CSC

Trend Micro InterScan para Cisco CSC-SSM proporciona la protección para los protocolos importantes del tráfico, tales como el tráfico S TP, HTTP, y FTP, así como POP3, para asegurarse de que los empleados no introducen accidentalmente los virus de sus cuentas de correo electrónico personales.

Elija la **configuración > Trend Micro contentan la Seguridad** para abrir el CSC-SSM. Del menú de la configuración, elija de estas opciones de configuración:

- **CSC puesto** — Inicia al asistente para la configuración para instalar y para configurar el CSC-SSM
- **Red** — Exploración, archivo que bloquea, Filtrado de URL, y bloqueo de URL de la red de las configuraciones

- **Correo** — El analizar de las configuraciones, filtrado de contenido, y prevención del Spam para el email entrante y saliente S TP y POP3
- **Transferencia de archivos** — Exploración y bloqueo del archivo de las configuraciones
- **Actualizaciones** — Actualizaciones de los horario para los componentes contentos de la exploración de la Seguridad, por ejemplo, archivo del modelo del virus, motor de la exploración, y así sucesivamente

Las opciones de la red, del correo, de la transferencia de archivos, y de las actualizaciones se describen más detalladamente en estos capítulos:

- Correo — Configurando el tráfico de correo S TP y POP3
- Red y transferencia de archivos — Configurar tráfico del (FTP) de la red (HTTP) y de la transferencia de archivos
- Actualizaciones — Manejo de las actualizaciones y de las interrogaciones del registro

Este ejemplo muestra cómo configurar un CSC-SSM para analizar el mensaje SMTP entrante a la red de la red interna.

Los mensajes SMTP entrantes se desvían al CSC-SSM para analizar. En este ejemplo, todo el tráfico del exterior para acceder el mail server interior (192.168.5.2/24) para los servicios SMTP se desvía al CSC-SSM.

```
access-list csc_inbound extended permit tcp any host 192.168.5.2 eq smtp
```

Estas configuraciones predeterminadas le dan una cierta protección para su tráfico del email después de que usted instale Trend Micro InterScan para Cisco CSC-SSM.

Configuración S TP

Configuración de Trend Micro S TP

Complete estos pasos para configurar el CSC-SSM para analizar el mensaje SMTP entrante usando el ASDM:

1. Elija la **configuración > Trend Micro contentan la Seguridad > el correo** en el ASDM y hacen clic la **exploración entrante de la configuración** para visualizar la ventana de la exploración/de la blanco del mensaje entrante S TP.
2. La ventana le lleva a **Trend Micro InterScan para el** prompt de inicio de sesión de **Cisco CSC-SSM**. Ingrese la contraseña CSC-SSM.
3. La ventana de la exploración del mensaje entrante S TP tiene estas tres opiniones:DestinoAcciónNotificaciónUsted puede conmutar entre las opiniones si usted hace clic la lengueta apropiada para la información que usted quiere. El nombre activo de la lengueta aparece en el texto marrón; los nombres inactivos de la lengueta aparecen en el texto negro. Utilice las tres lenguetas para configurar la exploración del virus del tráfico entrante S TP.Haga clic la **blanco** para permitir que usted defina el alcance de la actividad sobre el cual se actúa.La exploración del mensaje entrante S TP se habilita por abandono.
4. En la sección predeterminada de la exploración, **todos los archivos scannable** se seleccionan por abandono. Analiza sin importar las Extensiones del nombre del archivo.
5. Configure el **archivo comprimido** S TP **que dirige** para el correo entrante.Configuración para saltar la exploración de los archivos comprimidos cuando uno de éstos es verdad:La cuenta

descomprimida del archivo es mayor de 200.El tamaño del archivo descomprimido excede el 20 MB.El número de capas de la compresión excede de tres.La relación de transformación descomprimida o del archivo comprimido del tamaño es mayor de 100 a 1.Los archivos comprimidos se exceden especificado analizando los criterios.Modifique los parámetros predeterminados de la cuenta descomprimida del archivo como 300 y descomprimió el tamaño del archivo como 30 MB.

6. En la **exploración para la** sección del **Spyware/de Grayware de** estas ventanas, que fue mostrada en el paso 5, elija los tipos de grayware que usted quiere detectado por Trend Micro InterScan para Cisco CSC-SSM. Vea la ayuda en línea para una descripción de cada tipo de grayware enumerado.Haga clic la **salvaguardia** para habilitar la nueva configuración
7. Haga clic la lengueta de la **acción**, que permite que usted defina Paso a seguir cuando se detecta una amenaza. Los ejemplos de las acciones son limpios o cancelación.Estos valores son acción predeterminada tomada para los correos entrantes.**Para los mensajes con el virus/la** sección de la **detección de Malware** — limpie el mensaje o la conexión en los cuales el malware fue detectado, y si el mensaje o la conexión es uncleanable, borrela.**Para el Spyware/las detecciones de Grayware** — Éstos son los archivos que se entregarán si los mensajes SMTP en los cuales se detecta el spyware o el grayware.**Salvaguardia del** tecleo para habilitar la nueva configuración
8. Haga clic la lengueta de la **notificación**, que permite que usted componga un mensaje de notificación, así como defina quién se notifica del evento y de la acción.Si le satisfacen con la configuración predeterminada de la notificación, no se requiere ninguna otra acción. Pero, usted puede revisar las opciones de notificación y decidir si usted quiere cambiar los valores por defecto. Por ejemplo, usted puede enviar una notificación al administrador cuando un riesgo de seguridad se ha detectado en un correo electrónico. Para el S TP, usted puede también notificar el remitente o al beneficiario.Marque los cuadros del **administrador** y del **beneficiario** para la notificación por correo electrónico. Usted puede también adaptar el texto predeterminado en el mensaje de notificación algo más apropiado para su organización por ejemplo en esta captura de pantalla.
9. En la sección **en línea de las notificaciones de la** ventana, elija uno de las opciones de la lista, ni, o de ambas.En nuestro ejemplo, elija el **mensaje libre del riesgo** y teclee su propio mensaje en el campo proporcionado.Haga clic la **salvaguardia** para habilitar la nueva configuración.

Configuración HTTP

El analizar

Después de la instalación, por abandono su tráfico HTTP y FTP se analiza para los virus, los gusanos, y los Trojans. El Malware tal como spyware y el otro grayware requieren un cambio de configuración antes de que se detecten.

Estas configuraciones predeterminadas le dan una cierta protección para su red y el tráfico FTP después de que usted instale Trend Micro InterScan para Cisco CSC-SSM. Usted puede cambiar estas configuraciones. Por ejemplo, usted puede preferir utilizar la exploración por la opción de las Extensiones de archivo especificado bastante que todos los archivos Scannable para la detección del malware. Antes de que usted realice los cambios, revise la ayuda en línea para más información sobre estas selecciones.

Después de la instalación, es posible que usted quiere poner al día los ajustes de la configuración adicionales para obtener la protección máxima para su red y el tráfico FTP. Si usted compró la licencia más, que le da derecho a recibir el bloqueo de URL, anti-phishing, y las funciones del Filtrado de URL, usted debe configurar estas características adicionales.

Complete estos pasos para configurar el CSC-SSM para analizar el mensaje HTTP con el ASDM:

1. Haga clic la red (HTTP) en la página de Trend Micro, y esta ventana de la exploración del mensaje de la red tiene cuatro opiniones:DestinoExploración del webmailAcciónNotificaciónHaga clic la lengueta apropiada para la información que usted quiere para conmutar entre las opiniones. El nombre activo de la lengueta aparece en el texto marrón; los nombres inactivos de la lengueta aparecen en el texto negro. Utilice todas las lenguetas para configurar la exploración del virus del tráfico de la Web.Haga clic la **blanco** para permitir que usted defina el alcance de la actividad sobre el cual está ser actuada.La exploración del mensaje HTTP se habilita por abandono.Habilitado con el uso de **todos los archivos Scannable** como el método de la exploración.Archivo comprimido de la red (HTTP) que dirige para descargar de la red — configurada para saltar la exploración de los archivos comprimidos cuando uno de éstos es verdad:La cuenta descomprimida del archivo es mayor de 200.El tamaño del archivo descomprimido excede el 30 MB.El número de capas de la compresión excede de tres.La relación de transformación descomprimida o del archivo comprimido del tamaño es mayor de 100 a 1.Para la **exploración del webmail** — Configurado para analizar los sitios del webmail para Yahoo, AOL, el MSN, y Google.
2. **Dirección grande del archivo**Las lenguetas de la blanco en las ventanas de la exploración HTTP y de la exploración FTP permiten que usted defina el tamaño de la descarga más grande que usted quiere analizado. Por ejemplo, usted puede especificar que una descarga bajo el 20 MB está analizada, solamente una descarga más grande que el 20 MB no se analiza.Además, usted puede:Especifique las descargas grandes que se entregarán sin analizar, que puede introducir un riesgo de seguridad.Especifique que las descargas mayores que el límite especificado están borradas.Por abandono, el software CSC-SSM especifica que los archivos más pequeños que el 50 MB están analizados. Modifiqúese como 75 MB. Los archivos que son 75 MB y más grandes se entregan sin analizar al cliente solicitante.**Exploración diferida**La característica que analiza diferida no se habilita por abandono. Cuando está habilitada, esta característica permite que usted comience a descargar los datos sin analizar la descarga entera. La exploración diferida permite que usted comience a ver los datos sin una espera prolongada mientras que se analiza el conjunto de información entero.**Nota:** Si usted no habilita la opción que analiza diferida, después usted puede hacer frente a una actualización fracasada a través del módulo del CSC.**Nota:** Cuando se habilita la exploración diferida, la porción unscanned de información puede introducir un riesgo de seguridad.**Nota:** Trafique que los movimientos con el HTTPS no se pueden analizar para los virus y otras amenazas por el software CSC-SSM.Si la exploración diferida no se habilita, el contenido entero de la descarga debe ser analizado antes de que se presente usted. Pero, un cierto software de cliente puede medir el tiempo hacia fuera debido al tiempo requerido para recoger los suficientes paquetes de red para componer los archivos completos para analizar. Esta tabla resume las ventajas y desventajas de cada método.**Exploración para el Spyware y Grayware**Grayware es una categoría de software que puede ser legítima, indeseada, o malévola. A diferencia de las amenazas tales como virus, gusanos, y Trojans, el grayware no infecta, replica, o destruye los datos, sino que puede violar su aislamiento. Los ejemplos del grayware incluyen el

spyware, el adware, y las herramientas del Acceso Remoto.La detección del Spyware o del grayware no se habilita por abandono. Usted debe configurar la esta característica en estas ventanas para detectar el spyware y otras formas de spyware y el otro grayware en su red y transferencia de archivos trafican:**Salvaguardia del** tecleo para poner al día su configuración.

3. Usted puede conmutar a la lengueta del **webmail de la exploración** para analizar los sitios del webmail para Yahoo, AOL, el MSN, y Google.**Nota:** Si usted elige para analizar solamente el webmail, la exploración HTTP se restringe a los sitios especificada en la lengueta de la exploración del webmail de la red (HTTP) > exploración > ventana de la exploración HTTP. El otro tráfico HTTP no se analiza. Se analizan los sitios configurados hasta que usted los quite cuando usted hace clic el icono de Trashcan.En el **campo de nombre**, ingrese el nombre exacto del Web site, una palabra clave URL, y una cadena para definir el sitio de Webmail.**Nota:** Las conexiones a los mensajes que se manejan en el webmail se analizan.**Salvaguardia del** tecleo para poner al día su configuración.
4. Usted puede conmutar a la lengueta de la **acción** para la configuración del virus/de la detección de Malware y del Spyware/de las detecciones de Grayware.Las descargas de la red (HTTP) para los archivos en los cuales se detecta el virus/el malware — limpian el archivo descargado o el archivo en los cuales el malware fue detectado. Si es uncleanable, borre el archivo.El (FTP) de las descargas y de las transferencias de archivos de la red (HTTP) para los archivos en los cuales se detecta el spyware o el grayware — los archivos se borra.
5. Las descargas de la red (HTTP) cuando se detecta el malware — una notificación en línea se insertan en el navegador, que estado que Trend Micro InterScan para CSC-SSM ha analizado el archivo que usted intenta transferir, y han detectado un riesgo de seguridad.

Bloqueo del archivo

En el menú desplegable izquierdo, **bloqueo del** clic en Archivo.

Esta característica se habilita por abandono; sin embargo, usted debe especificar los tipos de archivos que usted quiere bloqueado. El bloqueo del archivo le ayuda a aplicar sus directivas de la organización para el uso de Internet y otros recursos de computación durante el WorkTime. Por ejemplo, su compañía no permite descargar de la música, debido a las cuestiones legales así como los problemas de la productividad del empleado.

- En la lengueta de la blanco de la ventana del bloqueo de archivo, marque la casilla de verificación **ejecutable** para bloquear el .exe.
- Usted puede especificar los tipos de archivo adicionales por la extensión del nombre del archivo. Marque la casilla de verificación de las **Extensiones de archivo especificado del bloque** para habilitar esta característica.
- Entonces, ingrese los tipos de archivo adicionales en las extensiones de archivo para bloquear el campo, y el haga click en Add En el ejemplo, se bloquean los archivos .mpg.**Salvaguardia del** tecleo cuando le acaban para poner al día la configuración.

Marque el cuadro de las **notificaciones del administrador** para enviar los mensajes predeterminados en el cuadro de texto.

Haga clic la lengueta de la **notificación** para el mensaje de alerta.

Bloqueo de URL

Esta sección describe la característica del bloqueo de URL e incluye estos temas:

- Bloqueo del vía la lengueta de la lista local
- Bloqueo del vía la lengueta del archivo del modelo (PhishTrap)

Nota: Esta característica requiere la licencia más.

La característica del bloqueo de URL le ayuda a evitar que los empleados accedan los sitios web prohibidos. Por ejemplo, es posible que usted quiere bloquear algunos sitios porque las directivas en su organización prohíben el acceso a fechar los servicios, los servicios en línea de las compras, o los sitios ofensivos.

Usted puede también bloquear los sitios que se conocen para perpetrar el fraude, tal como phishing. El phishing es una técnica usada por los criminales que envían los correos electrónicos que aparecen ser de una organización legítima, que le solicitan revelar la información privada tal como números de cuenta del banco. Esta imagen muestra un ejemplo de un correo electrónico usado para el phishing.

Por abandono, se habilita el bloqueo de URL. Pero, solamente los sitios en el archivo del modelo de TrendMicro PhishTrap se bloquean hasta que usted especifique los sitios adicionales para bloquear.

Bloqueo del vía la lengueta de la lista local

Complete estos pasos para configurar el bloqueo de URL del vía la lengueta de la lista local:

1. Elija la **configuración > Trend Micro contentan la Seguridad > la red** en el ASDM y hacen clic el **bloqueo de URL de la configuración** para visualizar la ventana del bloqueo de URL.
2. En vía la lengueta de la lista local de la ventana del bloqueo de URL, teclee los URL que usted quiere bloquear en el campo de la coincidencia. Usted puede especificar el nombre exacto del sitio web, una palabra clave URL, y una cadena.
3. Haga clic el **bloque** después de que cada entrada para mover el URL a la lista del bloque. El tecleo **no bloquea** para agregar la entrada para bloquear las excepciones de la lista para especificar su entrada como excepción. Sigue habiendo las entradas según lo bloqueado o las excepciones hasta que usted las quite.**Nota:** Usted puede también importar una lista del bloque y de la excepción. El archivo importado debe estar en un formato específico. Vea la ayuda en línea para las instrucciones.

Bloqueo del vía la lengueta del archivo del modelo (PhishTrap)

Complete estos pasos para configurar el archivo URL que bloquea del vía la lengueta del archivo del modelo (PhishTrap):

1. Elija la **configuración > Trend Micro contentan la Seguridad > la red** en el ASDM y hacen clic el link del **bloqueo de URL de la configuración** para visualizar la ventana del bloqueo de URL.
2. Entonces haga clic **vía la** lengueta del **archivo del modelo (PhishTrap)**.
3. Por abandono, el archivo del modelo de Trend Micro PhishTrap detecta y bloquea los sitios conocidos del phishing, los sitios del spyware, los sitios del cómplice del virus que son sitios asociados a los exploits sabidos, y la enfermedad vectors, que son los sitios web que existen

solamente para los propósitos malévolos. Utilice el someter el phishing potencial URL a los campos de TrendLabs para someter los sitios que usted piensa debe ser agregado al archivo del modelo de PhishTrap. TrendLabs evalúa el sitio y puede agregar el sitio a este archivo si se autoriza tal acción.
4. Haga clic la lengueta de la **notificación** para revisar el texto del mensaje predeterminado que aparece en el navegador cuando una tentativa se hace para acceder un sitio bloqueado. La ayuda en línea muestra un ejemplo. Resaltela y redefina para personalizar el mensaje predeterminado.
5. Haga clic la **salvaguardia** cuando le acaban para poner al día la configuración.

Filtrado de URL

Hay la sección importante dos que se discutirá aquí.

- Configuraciones de filtración
- Reglas para filtrosLos URL definidos en las ventanas del bloqueo de URL descritas previamente se permiten siempre o se rechazan siempre. La característica del Filtrado de URL, sin embargo, permite que usted filtre los URL en las categorías, que usted puede programar para permitir el acceso durante ciertas épocas, definidas como tiempo libre, y rechaza el acceso durante el WorkTime.**Nota:** Esta característica requiere la licencia más.Éstas son las seis categorías del Filtrado de URL:Compañía-prohibidoNo trabajo relacionadoTemas de investigaciónFunción de negocioCliente definidoOtros

Por abandono, los sitios compañía-prohibidos se bloquean durante los tiempos del trabajo y libres.

Configuraciones de filtración

Complete estos pasos para configurar la característica del Filtrado de URL:

1. Elija la **configuración > Trend Micro contentan la Seguridad > la red** en el ASDM y hacen clic las **configuraciones del Filtrado de URL de la configuración** para visualizar la ventana de configuración del Filtrado de URL.
2. En las categorías lengueta URL, revise las subcategorías enumeradas y las clasificaciones predeterminadas asignadas a cada categoría para ver si las asignaciones son apropiadas para su organización. Por ejemplo, las drogas ilegales son una subcategoría de la categoría Compañía-prohibida. Si su organización es una compañía de servicios financieros, es posible que usted quiere dejar esta categoría clasificada según lo compañía-prohibido. Marque la casilla de verificación de las **drogas ilegales** para habilitar la filtración para los sitios relacionados con las drogas ilegales. Pero, si su organización es una autoridad competente, usted debe reclasificar la subcategoría de las drogas ilegales a la categoría de la función de negocio. Vea la ayuda en línea para más información sobre la reclasificación.
3. Después de que usted haya revisado y haya refinado las clasificaciones de la subcategoría, marque la subcategoría asociada para habilitar todas las subcategorías para las cuales usted quiere la filtración realizada.
4. Si hay sitios dentro de algunas de las subcategorías habilitadas que usted no quiere filtrado, haga clic la lengueta de las **excepciones del Filtrado de URL**.
5. Teclee los URL que usted quiere excluir de la filtración en el campo de la coincidencia. Usted puede especificar el nombre exacto del sitio web, una palabra clave URL, y una

cadena.
6. El tecleo **agrega** después de que cada entrada para mover el URL al no filtre la lista siguiente de los sitios. Sigue habiendo las entradas como excepciones hasta que usted las quite.**Nota:** Usted puede también importar una lista de la excepción. El archivo importado debe estar en un formato específico. Vea la ayuda en línea para las instrucciones.
7. Haga clic la lengueta del **horario** para definir los días de la semana y las horas del día que se debe considerar WorkTime. El tiempo no señalado como WorkTime se señala automáticamente como tiempo libre.
8. **Salvaguardia del** tecleo para poner al día la configuración del Filtrado de URL.
9. Haga clic la lengueta de la **reclasificación URL** para someter los URL sospechados a TrendLabs para la evaluación.

Reglas para filtros

Después de que usted haya asignado las subcategorías URL a las categorías correctas para su organización, las excepciones definidas (eventualmente), y creado el trabajo y el tiempo libre programa, asigne las reglas para filtros que determinan cuando una categoría está filtrando.

Complete estos pasos para asignar las reglas de Filtrado de URL:

1. Elija la **configuración > Trend Micro contentan la Seguridad > la red** en el ASDM y hacen clic las **reglas de Filtrado de URL de la configuración** conectan para visualizar la ventana de las reglas de Filtrado de URL.
2. Para cada uno de las seis categorías principales, especifique si los URL en esa categoría están bloqueados, y si es así durante el tiempo del WorkTime, libre, o ambos. Vea la ayuda en línea para más información.
3. Haga clic la **salvaguardia** para poner al día la configuración.**Nota:** Para que el Filtrado de URL trabaje correctamente, el módulo CSC-SSM debe poder enviar los pedidos de HTTP al servicio de Trend Micro. Si se requiere un proxy de HTTP, elija la **actualización > las configuraciones de representación** para configurar la configuración de representación. El componente del Filtrado de URL no soporta el proxy SOCKS4.

Configuración FTP

Configuración de Trend Micro FTP

Después de la instalación, por abandono su tráfico FTP se analiza para los virus, los gusanos, y los Trojans. El Malware tal como spyware y el otro grayware requieren un cambio de configuración antes de que se detecten.

El analizar del (FTP) de la transferencia de archivos de las transferencias de archivos — Habilitado usando todos los archivos Scannable como el método de la exploración.

Complete los pasos dados en el **archivo que bloquea la** página para el tráfico HTTP.

Complete los pasos dados en el **archivo que bloquea la** página para el tráfico HTTP.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Aunque, el OIT se pueda utilizar para ver un análisis de algunas **salidas del comando show**, estos **comandos show** no son actualmente compatibles con esta herramienta.

- **módulo show** — Para marcar el estatus de un SS, por ejemplo:`ciscoasa#show module Mod Card Type Model Serial No. --- ---------- ---------- -------- 0 ASA 5520 Adaptive Security Appliance ASA5520 JMX090000B7 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20 JAF10333331 Mod MAC Address Range Hw Version Fw Version Sw Version --- ---------- ---------- ---------- 0 0014.c482.5151 to 0014.c482.5155 1.1 1.0(10)0 8.0(2) 1 000b.fcf8.012c to 000b.fcf8.012c 1.0 1.0(10)0 Trend Micro InterScan Security Module Version 6.0 Mod SSM Application Name Status SSM Application Version --- ---------- ---------- ---------- 1 Trend Micro InterScan Security Up Version 6.0 Mod Status Data Plane Status Compatibility --- ---------- ---------- ---------- 0 Up Sys Not Applicable 1 Up Up`
- **detalles del módulo show 1** — Utilice la palabra clave de los **detalles** para ver la información adicional para el SS, por ejemplo:`ciscoasa#show module 1 details Getting details from the Service Module, please wait... ASA 5500 Series Security Services Module-20 Model: ASA-SSM-20 Hardware version: 1.0 Serial Number: JAF10333331 Firmware version: 1.0(10)0 Software version: Trend Micro InterScan Security Module Version 6.0 App. name: Trend Micro InterScan Security Module App. version: Version 6.0 Data plane Status: Up Status: Up HTTP Service: Up Mail Service: Up FTP Service: Up Activated: Yes Mgmt IP addr: 172.30.21.235 Mgmt web port: 8443`
- **el slot_num del módulo show se recupera** — Determina si hay una configuración de la recuperación para el SS. Si una configuración de la recuperación existe para el SS, el ASA lo visualiza. Por ejemplo:`ciscoasa#show module 1 recover Module 1 recover parameters. . . Boot Recovery Image: Yes Image URL: tftp://10.21.18.1/ids-oldimg Port IP Address: 172.30.21.10 Port Mask: 255.255.255.0 Gateway IP Address: 172.30.21.254`

Refiera a verificar la configuración inicial para más información sobre cómo verificar que Trend Micro InterScan para Cisco CSC-SSM actúe correctamente.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. Refiera a resolver problemas Trend Micro InterScan para el CSC SS de Cisco para más información sobre cómo resolver problemas más en CSC-SSM.

Acceso a internet

Problema

El CSC no puede acceder Internet a través de la interfaz de administración ASA **o el** CSC no puede conseguir las actualizaciones del servidor de la tendencia a través de Internet.

Solución

Las configuraciones de la interfaz de administración con la **Administración-solamente** ordenan y hacen que solamente valida el tráfico a o desde el ASA, **no con él**. Quite tan el comando de la **Administración-solamente** y la sentencia NAT para el tráfico del Administración-a-exterior después permite que Internet para que el CSC se ponga al día.

Spam que no es detectado

Problema

El CSC no puede detectar el SPAM.

Solución

Usted tiene que habilitar la opción del anti-Spam, que no se habilita por abandono. La licencia más debe ser instalada, y las configuraciones DNS deben estar correctas para el network basado, reputación del correo electrónico del anti-Spam a funcionar correctamente. Refiera a habilitar el Spam S TP y POP3 que filtra para más información.

Autorice los errores de violación

Problema

El módulo del CSC muestra los errores de violación de la licencia y señala más host que cuál está en la red. `La infracción de la licencia se ha detectado en el InterScan para el` error del `CSC SS` se considera en el módulo del CSC. ¿Cómo puede este error ser resuelto?

Solución

Mueva todas las interfaces excepto Exterior-WAN (nivel de seguridad 0) a los mayores niveles de seguridad.

Problema de rendimiento

Problema

El tráfico entrante S TP ha llegado a ser muy lento. El mail server interior consigue a veces la respuesta del servidor que toma un par de minutos o de dos para recibir.

Solución

Usted se ejecuta posiblemente en la lentitud en el tráfico debido a los **paquetes defectuosos**. Intente este ejemplo, que puede resolver el problema.

```
!--- Creates a new tcp map and allows for 100 out of order packets tcp-map localmap queue-limit
100 !--- This is the class that defines traffic to sent to the csc-module. The name you use can
be different. Sets the localmap parameters to flow matching the class map. policy-map
global_policy class csc-class set connection advanced-options localmap
```

Problema

La exploración HTTP no trabajó y visualizó este error:

```
Error: Failed to rate URL, rc=-723
```

Solución

Se genera este mensaje de error cuando el CSC-SSM tiene problema en entrar en contacto los servidores de Trend Micro. Esto puede suceder cuando hay tiempo de espera en la red o si el

CSC-SSM está demasiado ocupado manejar los pedidos de conexión. Las conexiones simultáneas máximas en el CSC-SSM-10 son cerca de 500. En este caso para el periodo especificado, el número de conexiones ha superado posiblemente el límite máximo. Refiera al cuadro 2 en las 5500 Series módulo de Servicios de seguridad contento de la Seguridad de Cisco ASA y del control para más información sobre los límites de la conexión.

Una solución alternativa posible para esto es limitar las conexiones simultáneas. Refiera a las conexiones del límite con el CSC SS para más información.

Envíe por correo electrónico el problema

Problema

La negación en los correos electrónicos no se puede quitar de los correos si es necesario y también las fuentes no se pueden cambiar en la negación del correo electrónico. ¿Por qué hace esto sucede?

Solución

No es posible quitar la negación de algunos de los correos electrónicos salientes en CSC-SSM. También, usted no puede cambiar la fuente de la negación puesto que no se soporta en CSC-SSM.

Problema del tráfico

Problema

Usted no puede parar el tráfico del envío del ASA a CSC-SSM. ¿Cómo puede esto ser resuelta?

Solución

Para parar el tráfico del envío al ASA de CSC-SSM, el administrador debe quitar la política de servicio de la interfaz con el ningún comando service-policy:

```
hostname(config-pmap-c)#no service-policy policy_map_name [global | interface interface_ID]
```

Problema de la actualización del modelo de Grayware

Problema

Este mensaje de error es módulo abierto una sesión del CSC.

```
GraywarePattern: Actualización del modelo: Incapaz de conseguir la información del modelo.
Actualización del modelo: El archivo de la descarga era fracasado para ActiveUpdate no podía
desabrochar los paquetes descargados de la corrección. Archivo zip puede ser corrompido. Esto
puede suceder debido a una conexión de red inestable. Intente por favor descargar el archivo
otra vez. El código de error es 24.

AntiVirusPattern: Actualización del modelo: El archivo de la descarga era fracasado para
ActiveUpdate no podía desabrochar los paquetes descargados de la corrección. Archivo zip puede
ser corrompido. Esto puede suceder debido a una conexión de red inestable. Intente por favor
descargar el archivo otra vez. El código de error es 24.
```

¿Cómo puede este mensaje de error ser resuelto?

Solución

Este problema se relaciona con el Id. de bug Cisco CSCtc37947 (clientes registrados solamente) y el Id. de bug Cisco CSCsk10777 (clientes registrados solamente). Vuelva a sentar el CSC-SSM o actualice el código a 6.2.x para resolver este problema. También el retiro de los archivos temporales creados para la actualización auto en la cuenta raíz del CSC puede resolver el problema. Recomience los servicios después de que usted vuelva a sentar CSC-SSM o actualice el código.

El HTTPS trafica el problema

Problema

Usted no puede bloquear el tráfico HTTPS con CSC-SSM. ¿Cómo puede el tráfico HTTPS ser bloqueado?

Solución

El CSC-SSM no puede bloquear el tráfico HTTPS porque no puede profundamente examinar el paquete debido a la encripción de SSL en él.

Incapaz de desviar el tráfico del examen del CSC

El tráfico se puede desviar del examen del CSC si usted agrega los enunciados de negación para los rangos de red en la pregunta al ACL usado para que el tráfico coincidente pase al módulo.

Incapaz de registrar todo el tráfico HTTP que pasa con CSC-SSM

El CSC no puede registrar todo el tráfico sino solamente la información de las visualizaciones del bloque/de las tentativas filtradas.

Error mientras que actualiza el CSC

`El [ERR-PAT-0002] el sistema de la actualización no puede descomprimir el archivo de la actualización, y no puede continuar. Este mensaje está para los objetivos de hacer un diagnóstico solamente. Clientes - entre en contacto por favor el` mensaje de error del `Soporte técnico` aparece cuando usted actualiza el CSC. Se considera este mensaje de error cuando el archivo del **.bin** se utiliza en vez del archivo **.package**. El problema no ocurre cuando se utiliza el archivo **.package**.

Error mientras que CSC que pone al día automáticamente las firmas

Problema:

Cuando el CSC hace la actualización automática, consiguió este mensaje.

```
el modelo 17462 del Anti-Spam fue descargado y instalado con éxito. Incapaz de copiar el
archivo. Usted debe copiar manualmente el archivo /opt/trend/isvw/temp/AU/piranhacache/ * a la
trayectoria /opt/trend/isvw/lib/mail/cache.
```

Solución:

Esto es un bug conocido del problema con el código de Trendmicro del CSC. Un bug se ha clasifiado para esto y para los detalles completos. Refiera al Id. de bug Cisco CSCtc37947 (clientes registrados solamente). Actualice el CSC a 6.3.1172(2) o más adelante para librarse del problema.

El módulo del CSC no puede mostrar los Syslog

Problema:

Después de actualizar a 6.3.1172.4, el servicio de LogServer en el módulo del CSC pudo fallar y el administrador recibe esta notificación por correo electrónico: `LogServer ha parado recientemente en InterScan para el CSC SS. Entre en contacto por favor el soporte de cliente para la ayuda.`

Solución:

Hay dos opciones como solución alternativa:

1. Instale el arreglo de la estructura de la ingeniería.Entre en contacto el TAC de Cisco (clientes registrados solamente) para la información sobre cómo instalar esta estructura.
2. Rehaga la imagen el dispositivo a una versión anterior.Refiera a rehacer la imagen el CSC-SSM para toda la información sobre este proceso.

Refiera al Id. de bug Cisco CSCtl21378 (clientes registrados solamente) para más información.

El servidor de registro del CSC se ejecuta en el Loop infinito y para precipitadamente

Problema:

El servidor de registro del módulo del CSC se ejecuta en un Loop infinito y para precipitadamente.

Solución:

Este problema es debido al Id. de bug Cisco CSCtl21378. Refiera a CSCtl21378 (clientes registrados solamente) para más información.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Refiera a resolver problemas Trend Micro InterScan para Cisco CSC-SSM para más información sobre cómo resolver problemas las diversas aplicaciones el CSC-SSM.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **arranque del módulo del debug** — Mensajes del debug de las demostraciones sobre el proceso de arranque SS.
- **el módulo 1 del módulo del hw apaga** — Apague el SS
- **módulo 1 del módulo del hw reajustado** — Reajuste el SS

Nota: `El %ASA-3-421001: El flujo TCP de inside:172.22.50.112/1718 a outside:XX.XX.XX.XX/80 se salta porque la Seguridad contenta y la placa de control tiene mensaje fallido` es un mensaje del registro que aparece cuando el módulo del CSC llega a ser totalmente insensible.

Nota: Utilice este comando para reajustar el módulo.

```
ASA#hw-module module 1 reset The module in slot 1 should be shut down before resetting it or
loss of configuration may occur. Reset module in slot 1? [confirm] (Confirm it at this point by
'return'.)
```

Refiera al guía de referencia de comandos para más información sobre este comando.

Información Relacionada

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 - Soporte de productos
- Seguridad del contenido de Cisco y guía del administrador del control SS, 6.2
- Seguridad del contenido de Cisco y guía del administrador del control SS
- Cisco Adaptive Security Device Manager - Soporte de productos
- Soporte Técnico y Documentación - Cisco Systems