El filtro CSC-SSM URL falla con Corte-por la autenticación de representación configurada en el ASA en línea

Contenido

Introducción

Este documento describe el problema cuando el filtro URL falla en el módulo de Servicios de seguridad contento de la Seguridad y del control (CSC-SSM) cuando corte-por la autenticación de representación se configura en el dispositivo de seguridad adaptante (ASA) o un dispositivo entre el puerto de administración CSC-SSM y Internet.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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

Convenciones

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

Condiciones/entorno

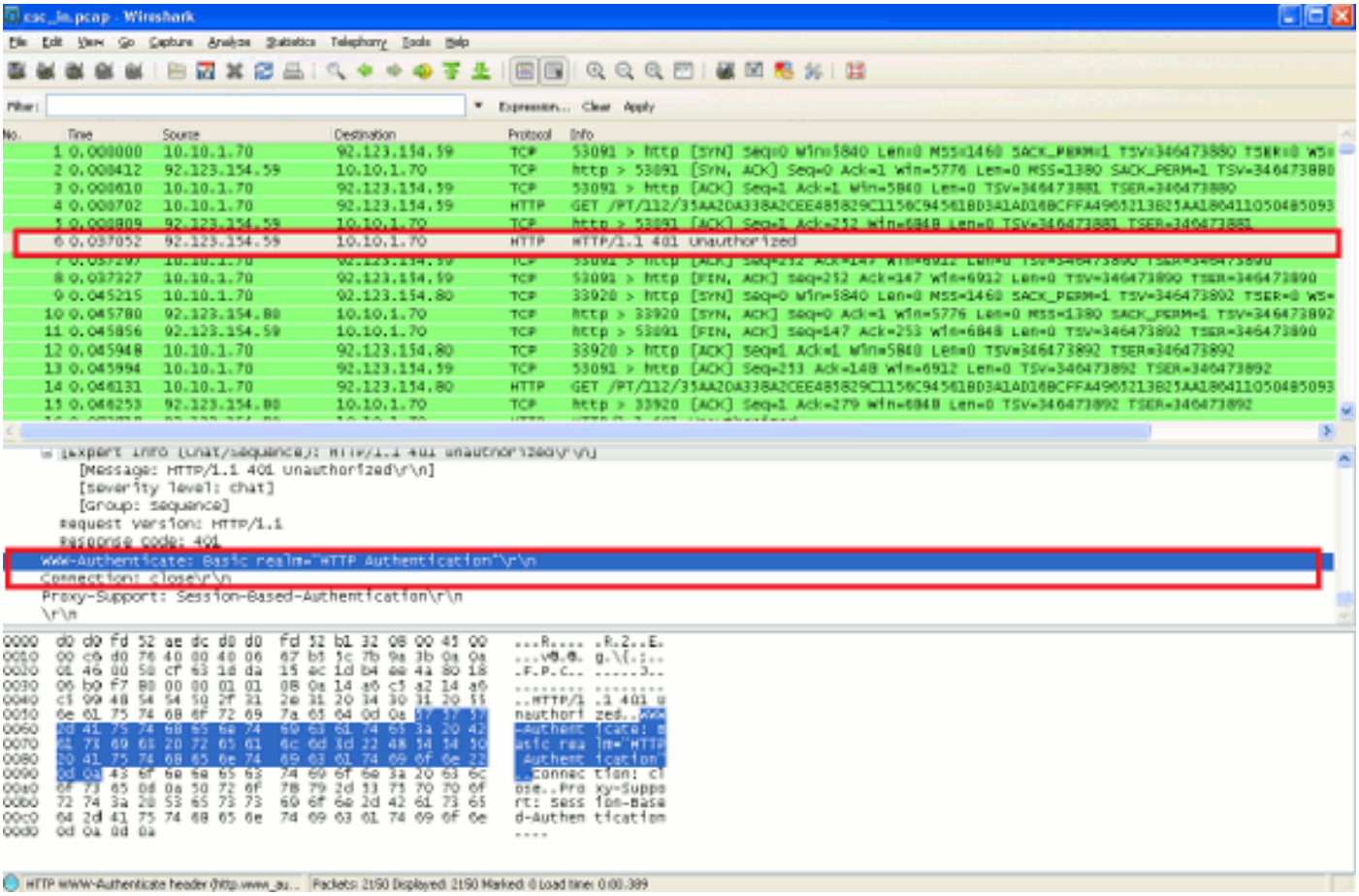
El Authentication, Authorization, and Accounting (AAA) corte-por la autenticación de representación se configura en un ASA que esté en la trayectoria entre el puerto de administración del módulo del CSC y Internet.

Problema

Los sitios web URL-no se filtran con el CSC-SSM y el CSC-SSM HTTP. Los registros muestran los mensajes similares a éstos:

```
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> Get URL Category returned [-1],
    with category 0 = [0] and rating = [0]
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> URLFilteringScanTask:PerformPreScanTask
    - URL rating failed, has to let it go
2011/04/28 14:55:04 GMT+01:00  <6939-1376041904> add result=1 server=
```

El problema se identifica fácilmente después de que recojan a las capturas de paquetes a y desde el puerto de administración CSC-SSM en la interfaz interior ASA. En el ejemplo abajo, la dirección IP de la red interna es 10.10.1.0/24 y la dirección IP del módulo del CSC es 10.10.1.70. La dirección IP 92.123.154.59 es la dirección IP de uno de los servidores de la clasificación de Trend Micro.



Cuando el módulo del CSC mira para determinar la categoría que cierto URL baja en, el módulo del CSC debe pedir a la tendencia las informaciones al servidor micro de la clasificación acerca

de ese URL específico. Las fuentes CSC-SSM esta conexión de su propio IP Address de administración y él utilizan el TCP/80 para la comunicación. En la visualización de la pantalla arriba, el apretón de manos de tres vías completa con éxito entre el servidor de la clasificación de Trend Micro y el CSC-SSM. El CSC-SSM ahora envía una petición get al servidor y recibe un" mensaje desautorizado "HTTP/1.1 401 generado por el ASA (o el otro dispositivo de red en línea) que hace corte-por el proxy.

En este ejemplo ASA, el AAA corte-por la autenticación de representación se configura con estos comandos:

```
aaa authentication match inside_authentication inside AUTH_SERV access-list
inside_authentication extended permit tcp any any
```

Estos comandos requieren el ASA indicar a todos los usuarios en el interior (debido al "tcp cualquier" en la autenticación ACL) para que la autenticación que vaya a cualquier sitio web. El IP Address de administración CSC-SSM es 10.10.1.70, que pertenece a la misma subred como el de la red interna ahora está conforme a esta directiva. Como consecuencia, el ASA considera el CSC-SSM ser apenas otro host en la red interna y lo desafía para un nombre de usuario y contraseña. Desafortunadamente, el CSC-SSM no se diseña para proporcionar la autenticación cuando intenta alcanzar los servidores de la clasificación de Trend Micro para la clasificación de los URL. Puesto que el CSC-SSM falla la autenticación, el ASA envía un" mensaje desautorizado "HTTP/1.1 401 al módulo. La conexión se cierra y el URL en la pregunta no es clasificado con éxito por el módulo del CSC.

Solución

Utiliza esta solución para resolver el problema.

Ingrese estos comandos de eximir el IP Address de administración CSC-SSM de la autenticación:

```
access-list inside_authentication extended deny tcp host 10.10.1.70 any access-list
inside_authentication extended permit tcp any any
```

El puerto de administración CSC-SSM necesita tener acceso totalmente sin obstáculo a Internet. No debe pasar a través de ningunos filtros o revisiones de seguridad que pudieron prevenir el acceso a Internet. También, no debe tener que autenticar, de ninguna manera, de obtener el acceso a Internet.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems