Errores debido del aborto de TLS del Módulo de servicios NGFW al error del error o de la validación de certificado del apretón de manos

Contenido

Introducción

Este documento describe cómo resolver problemas un problema determinado con el acceso a los sitios web HTTPS-basados a través del Módulo de servicios del Firewall de la última generación de Cisco (NGFW) con el desciframiento habilitado.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Procedimientos de apretón de manos de Secure Sockets Layer (SSL)
- Certificados SSL

Componentes Utilizados

La información en este documento se basa en el Módulo de servicios de Cisco NGFW con la versión 9.2.1.2(52) del administrador de seguridad de la prima de Cisco (PRSM).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El desciframiento es una característica que permite al Módulo de servicios NGFW para desencriptar los flujos SSL-cifrados (y examinar la conversación que se cifra de otra manera) y para aplicar las directivas en el tráfico. Para configurar esta característica, los administradores deben configurar un certificado del desciframiento en el módulo NGFW, que se presenta a los sitios web HTTPS-basados acceso al cliente en lugar del certificado de servidor original.

Para que el desciframiento trabaje, el módulo NGFW debe confiar en el certificado servidor-presentado. Este documento explica los escenarios cuando el contacto SSL falla entre el Módulo de servicios NGFW y el servidor, que hace ciertos sitios web HTTPS-basados fallar cuando usted intenta alcanzarlos.

Con el fin de este documento, estas directivas se definen en el Módulo de servicios NGFW con PRSM:

- **Directivas de la identidad**: No hay directivas definidas de la identidad.
- **Políticas de descifrado**: **La Decrypt-toda** directiva utiliza esta configuración:
- **Políticas de acceso**: No hay políticas de acceso definidas.
- **Configuraciones del desciframiento**: Este documento asume que un **certificado del desciframiento** está configurado en el Módulo de servicios NGFW y que los clientes lo confían en.

Cuando una política de descifrado se define en el Módulo de servicios NGFW y se configura según lo descrito previamente, el Módulo de servicios NGFW intenta interceptar todo el tráfico SSL-cifrado a través del módulo y desencriptar.

> Nota: Una explicación gradual de este proceso está disponible en la sección desencriptada del flujo de tráfico del guía del usuario para ASA CX y del administrador de seguridad primero 9.2 de Cisco.

Esta imagen representa la Secuencia de eventos:

En esta imagen, **A** es el cliente, **B** es el Módulo de servicios NGFW, y el **C** es el servidor HTTPS. Por los ejemplos proporcionados en este documento, el servidor HTTPS-basado es Cisco Adaptive Security Device Manager (ASDM) en un dispositivo de seguridad adaptante de Cisco (ASA).

Hay dos factores importantes sobre este proceso que usted deba considerar:

- En el segundo paso del proceso, el servidor debe validar una de las habitaciones de la cifra

SSL que son presentadas por el Módulo de servicios NGFW.

- En el cuarto paso del proceso, el Módulo de servicios NGFW debe confiar en el certificado que es presentado por el servidor.

Problema

Si el servidor no puede validar las cifras unas de los SSL que son presentadas por el Módulo de servicios NFGW, usted recibe un mensaje de error similar a esto:

Es importante tomar la nota de la información de detalles del error (resaltada), que muestra:

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

Cuando usted ve el archivo de **/var/log/cisco/tls_proxy.log** en el archivo de los diagnósticos del módulo, estos mensajes de error aparecen:

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

Solución

Una posible causa para este problema es que una licencia del Triple Data Encryption Standard/del Advanced Encryption Standard (3DES/AES) (designada a menudo el k9) no está instalada en el módulo. Usted puede descargar la licencia del k9 para el módulo sin la carga y cargarla vía PRSM.

Si persiste el problema después de que usted instale la licencia 3DES/AES, después obtenga a las capturas de paquetes para el contacto SSL entre el Módulo de servicios NGFW y el servidor, y entre en contacto al Administrador del servidor para habilitar las cifras apropiadas SSL en el servidor.

Problema

Si el Módulo de servicios NGFW no confía en el certificado que es presentado por el servidor, después usted recibe un mensaje de error similar a esto:

Es importante tomar la nota de la información de detalles del error (resaltada), que muestra:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Cuando usted ve el archivo de **/var/log/cisco/tls_proxy.log** en el archivo de los diagnósticos del módulo, estos mensajes de error aparecen:

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa
```

```
2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

Solución

Si el módulo no puede confiar en el certificado del servidor SSL, usted debe importar el certificado de servidor en el módulo con PRSM para asegurarse de que el proceso del contacto SSL es acertado.

Complete estos pasos para importar el certificado de servidor:

1. Desvíe el Módulo de servicios NGFW cuando usted accede el servidor para descargar el certificado vía un navegador. Una manera de desviar el módulo es crear una política de descifrado que no desencripte el tráfico a ese servidor determinado. Este vídeo le muestra cómo crear la directiva:

   Éstos son los pasos que se muestran en el vídeo:

   Para acceder el PRSM en el CX, navegue a **https:// <IP_ADDRESS_OF_PRSM>**. Este ejemplo utiliza **https://10.106.44.101**.

   Navegue a las **configuraciones > a las directivas/a las configuraciones > a las políticas de descifrado** en el PRSM.

   Haga clic el icono que está situado cerca de la esquina superior izquierda de la pantalla y elija el **agregar sobre la** opción de la **directiva** para agregar una directiva al top de la lista.

   Nombre la directiva, deje la fuente como **ningunos**, y cree un objeto del **grupo de red CX**. Nota: Recuerde incluir la dirección IP del servidor HTTPS-basado. En este ejemplo, una dirección IP de **172.16.1.1** se utiliza.Choose **no desencripta** para la acción.

   Salve la directiva y confíe los cambios.
2. Descargue el certificado de servidor a través de un navegador y carguelo al Módulo de servicios NGFW vía PRSM, tal y como se muestra en de este vídeo:

   Éstos son los pasos que se muestran en el vídeo:

   Una vez que se define la directiva anterior-mencionada, utilice a un navegador para navegar al servidor HTTPS-basado que se abre a través del Módulo de servicios NGFW.
   Nota: En este ejemplo, la versión 26.0 de Firefox del Mozilla se utiliza para navegar al servidor (un ASDM en un ASA) con el URL **https://172.16.1.1**.Valide la advertencia de seguridad si una surge y agregue una excepción de seguridad.

Haga clic el pequeño icono bloqueo-formado situado a la izquierda de la barra de dirección. La ubicación de este icono varía basado en el navegador se utiliza que y la versión.

Haga clic el botón del **certificado de la visión** y entonces el botón de la **exportación** bajo lengueta de los detalles después de que usted seleccione el certificado de servidor.

Salve el certificado en su máquina personal en una ubicación de su opción.

El registro en el PRSM y hojea a las **configuraciones > a los Certificados**.

El tecleo **I quiere a… > Import Certificate (Importar certificado)** y eligió el certificado de servidor anterior-descargado (del paso 4).

Salve y confíe los cambios. Una vez completo, el Módulo de servicios NGFW debe confiar en el certificado que es presentado por el servidor.

3. Quite la directiva que fue agregada en el paso 1. El Módulo de servicios NGFW puede ahora completar el apretón de manos con éxito con el servidor.

Información Relacionada

- Guía del usuario para ASA CX y administrador de seguridad 9.2 de la prima de Cisco
- Soporte Técnico y Documentación - Cisco Systems