Solución de problemas de actualización de fuentes de inteligencia de seguridad en Firepower Management Center

Contenido

Introducción

Este documento describe cómo resolver problemas con las actualizaciones de la fuente de inteligencia de seguridad.

Background

La fuente de inteligencia de seguridad se compone de varias listas actualizadas periódicamente de direcciones IP que tienen una reputación deficiente, según lo determinado por Cisco Talos Security Intelligence and Research Group (Talos). Es importante mantener la información de inteligencia actualizada periódicamente para que un sistema Cisco Firepower pueda utilizar información actualizada con el fin de filtrar el tráfico de red.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Management Center
- Fuente de inteligencia de seguridad

Componentes Utilizados

La información de este documento se basa en un Cisco Firepower Management Center que ejecuta la versión 5.2 o posterior del software.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Se produce un error en la actualización de la fuente de inteligencia de seguridad. Puede verificar el fallo mediante la GUI web o la CLI (se explica con más detalle en las siguientes secciones).

Verifique el problema desde la GUI web

Cuando se produce un error en la actualización de la fuente de inteligencia de seguridad, Firepower Management Center muestra alertas de estado.

Verifique el problema desde la CLI

Para determinar la causa raíz de un fallo de actualización con la fuente de inteligencia de seguridad, introduzca este comando en la CLI de Firepower Management Center:

```
admin@Sourcefire3D:~$ cat /var/log/messages
```

Busque cualquiera de estas advertencias en los mensajes:

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

Solución

Termina estos pasos de progresión para resolver problemas el problema:

1. Compruebe que el **intelligence.sourcefire.com** está activo. Vaya a https://intelligence.sourcefire.com en un explorador.

2. Acceda a la CLI de Firepower Management Center mediante Secure Shell (SSH).

3. Ping intelligence.sourcefire.com desde Firepower Management Center:

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verifyyou receive an output similar
   to this:

   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ifyou do not receive a
   response similar to that shown, then you can have an outbound connectivity issue, or you do
   not have a route to intelligence.sourcefire.com.
   ```

4. Resolver el nombre de host para intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com
```

Verifique que reciba una respuesta similar a la siguiente:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

Nota: El resultado anterior utiliza el servidor del sistema de nombres de dominio público (DNS) de Google como ejemplo. La salida depende de los ajustes de DNS configurados en **System > Local > Configuration**, bajo el **Network** sección. Si no recibe una respuesta similar a la mostrada, asegúrese de que la configuración de DNS es correcta.**Precaución**: el servidor utiliza un esquema de direcciones IP de ordenamiento cíclico para el balanceo de carga, la tolerancia a fallos y el tiempo de actividad. Por lo tanto, las direcciones IP pueden cambiar y Cisco recomienda que el firewall se configure con un **CNAME** en lugar de una dirección IP.

5. Compruebe la conectividad con intelligence.sourcefire.com con el uso de Telnet:

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

Verifique que reciba un resultado similar a este:

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

Nota: Si puede completar el segundo paso correctamente pero no puede establecer una conexión Telnet con **intelligence.sourcefire.com** a través del puerto 443, puede tener una regla de firewall que bloquee el puerto 443 saliente para intelligence.sourcefire.com.

6. Vaya a **System > Local > Configuration** y verifique la configuración de proxy del **Manual Proxy** configuración bajo el **Network** sección.

Nota: Si este proxy realiza una inspección de Secure Sockets Layer (SSL), debe establecer una regla de omisión que omita el proxy para **intelligence.sourcefire.com**.

7. Pruebe si puede realizar una HTTP GET solicitud contra intelligence.sourcefire.com:

```
admin@Firepower:~sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
```

```
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Nota: La carita sonriente al final del curl La salida del comando indica una conexión exitosa.**Nota**: Si utiliza un proxy, el curl requiere un nombre de usuario. El comando es **curl -U <user> -vvk** https://intelligence.sourcefire.com. Además, después de introducir el comando, se le solicitará que introduzca la contraseña de proxy.

8. Verifique que el tráfico HTTPS utilizado para descargar la fuente de inteligencia de seguridad no pase a través de un descifrador SSL. Para verificar que no se produce descifrado SSL, valide la información del certificado de servidor en el resultado del paso 6. Si el certificado de servidor no coincide con lo que se muestra en el ejemplo siguiente, puede tener un descifrador SSL que renuncie al certificado. Si el tráfico pasa a través de un descifrador SSL, debe omitir todo el tráfico que va a intelligence.sourcefire.com.

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
```

```
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Nota: se debe omitir el descifrado SSL para la fuente de inteligencia de seguridad porque el descifrado SSL envía al Firepower Management Center un certificado desconocido en el protocolo de enlace SSL. El certificado enviado a Firepower Management Center no está firmado por una CA de confianza de Sourcefire, por lo que la conexión no es de confianza.

Información Relacionada

- Automatic Error al descargar la actualización en un FirePOWER Management Center
- Direcciones de servidor necesarias para las operaciones de protección frente a malware avanzado (AMP)
- Puertos de comunicación necesarios para el funcionamiento del sistema Firepower
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).