Errores de la actualización de la alimentación de la inteligencia de Seguridad del Troubleshooting en el centro de administración de FireSIGHT

Contenido

Introducción

Este documento describe cómo resolver problemas los problemas con las actualizaciones de la alimentación de la inteligencia de Seguridad. La alimentación de la inteligencia de Seguridad se comprende de varias listas regularmente actualizadas de IP Addresses que tengan reputaciones pobres, según lo determinado por la inteligencia de Seguridad de Cisco Talos y el grupo de investigación (Talos). Es importante mantener la alimentación de la inteligencia puesta al día regularmente de modo que un sistema de Cisco FireSIGHT pueda utilizar la información actualizada para filtrar su tráfico de la red.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Centro de administración de Cisco FireSIGHT
- Alimentación de la inteligencia de Seguridad

Componentes Utilizados

La información en este documento se basa en un centro de administración de Cisco FireSIGHT que ejecute la versión de software 5.2 o más adelante.

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.

Problema

Un error de la actualización de la alimentación de la inteligencia de Seguridad ocurre. Usted puede verificar el error vía la red GUI o el CLI (explicado más lejos en las secciones que siguen).

Verifique el problema de la red GUI

Cuando ocurre el error de la actualización de la alimentación de la inteligencia de Seguridad, el centro de administración de FireSIGHT visualiza las alertas de la salud.

Verifique el problema del CLI

Para determinar la causa raíz de un incidente de la actualización con la alimentación de la inteligencia de Seguridad, ingrese este comando en el CLI del centro de administración de FireSIGHT:

```
admin@Sourcefire3D:~$

cat /var/log/messages
```

Busque para 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. Verifique que el sitio de *intelligence.sourcefire.com* sea activo. Navegue a https://intelligence.sourcefire.comin a un navegador. Usted debe recibir una cara sonriente, que indica que el sitio está vivo.

2. Acceda el CLI del centro de administración de FireSIGHT vía el Secure Shell (SSH).

3. Haga ping *intelligence.sourcefire.com del* centro de administración de FireSIGHT:

   ```
   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.com
   ```

   Usted debe recibir una salida similar a esto:

   ```
   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ms
   ```

Si usted no recibe una respuesta similar a ésa mostrada, después usted puede ser que tenga un problema de conectividad saliente o usted no tiene una ruta a *intelligence.sourcefire.com.*

4. Resuelva el nombre de host para *intelligence.sourcefire.com*:

```
admin@Firepower:~$

sudo

nslookup intelligence.sourcefire.com
```

Usted debe recibir una respuesta similar a esto:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

Note: La salida ya mencionada utiliza el servidor del sistema del nombre del public domain de Google (DNS) como un ejemplo. La salida depende de las configuraciones DNS que se configuran en el **sistema > el Local > configuración**, bajo sección de la *red*. Si usted no recibe una respuesta similar a ésa mostrada, después asegúrese de que las configuraciones DNS estén correctas.**Caution**: El servidor utiliza un esquema circular de la dirección IP para el Equilibrio de carga, la tolerancia de fallas, y el uptime. Por lo tanto, los IP Addresses pudieron cambiar, y Cisco recomienda que el Firewall esté configurado con un *CNAME* en vez de una dirección IP.

5. Marque la Conectividad a *intelligence.sourcefire.com* con el uso de Telnet:

```
admin@Firepower:~$

 sudo telnet intelligence.sourcefire.com 443
```

Usted debe recibir una salida similar a esto:

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

Note: Si usted puede completar el segundo paso con éxito pero no puede a Telnet a *intelligence.sourcefire.com* sobre el puerto 443, usted puede ser que tenga una regla de firewall que bloquea el puerto 443 saliente para *intelligence.sourcefire.com*.

6. Navegue al **sistema > al Local > a la configuración** y verifique las configuraciones de representación del *Configuración manual del proxy* bajo sección de la *red*.
Note: Si este proxy hace el examen de Secure Sockets Layer (SSL), usted debe poner en el lugar una regla de puente que desvíe el proxy para *intelligence.sourcefire.com*.
7. Pruebe si usted puede realizar una *petición get HTTP* 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
```

Note: La cara sonriente en el extremo de la salida de comando del *rizo* indica una conexión satisfactoria.**Note**: Si usted utiliza un proxy, el comando del *rizo* requiere un nombre de usuario. El comando será **rizo - <user> U - vvk** https://intelligence.sourcefire.com. Además, después de que usted ingrese el comando, le indican ingresa la contraseña del proxy.

8. Verifique que el tráfico HTTPS que se utiliza para descargar la alimentación de la inteligencia de Seguridad no pase con un decryptor SSL. Para verificar que ocurra ningún descifrado SSL, valide la información del certificado de servidor en la salida del paso 6. Si el certificado de servidor no hace juego eso visualizada en el ejemplo que sigue, después usted puede ser que tenga un decryptor SSL que dimite el certificado. Si el tráfico pasa con un decryptor SSL, usted debe desviar todo el tráfico que vaya 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
```

Note: El descifrado SSL se debe desviar para la alimentación de la inteligencia de Seguridad porque el decryptor SSL envía el centro de administración de FireSIGHT un certificado desconocido en el contacto SSL. El certificado que se envía al centro de administración de FireSIGHT no es firmado por un CA Sourcefire-de confianza, así que la conexión es untrusted.

Información Relacionada

- Error automático de la actualización de la descarga en un centro de administración de FireSIGHT
- Direccionamientos del servidor requerido para las operaciones avanzadas de la protección de Malware (AMP)
- Puertos de comunicación requeridos para la operación del sistema de FireSIGHT
- Soporte Técnico y Documentación - Cisco Systems