Solucionar problemas de "error de configuración de nube" en dispositivos Firepower

Contenido

Introducción

Este documento describe escenarios comunes donde el sistema Firepower activa la alerta de estado "Actualizaciones de datos de amenazas - Configuración de nube de Cisco - Fallo".

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Sistema Firepower
- Integración en la nube
- Resolución DNS y conectividad proxy
- Integración con Cisco Threat Response (CTR)

Componentes Utilizados

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

- Firepower Management Center (FMC) versión 6.4.0 o posterior
- Firepower Threat Defense (FTD) o Firepower Sensor Module (SFR) versión 6.4.0 o posterior
- Cisco Secure Services Exchange (SSE)
- Portal Cisco Smart Account

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

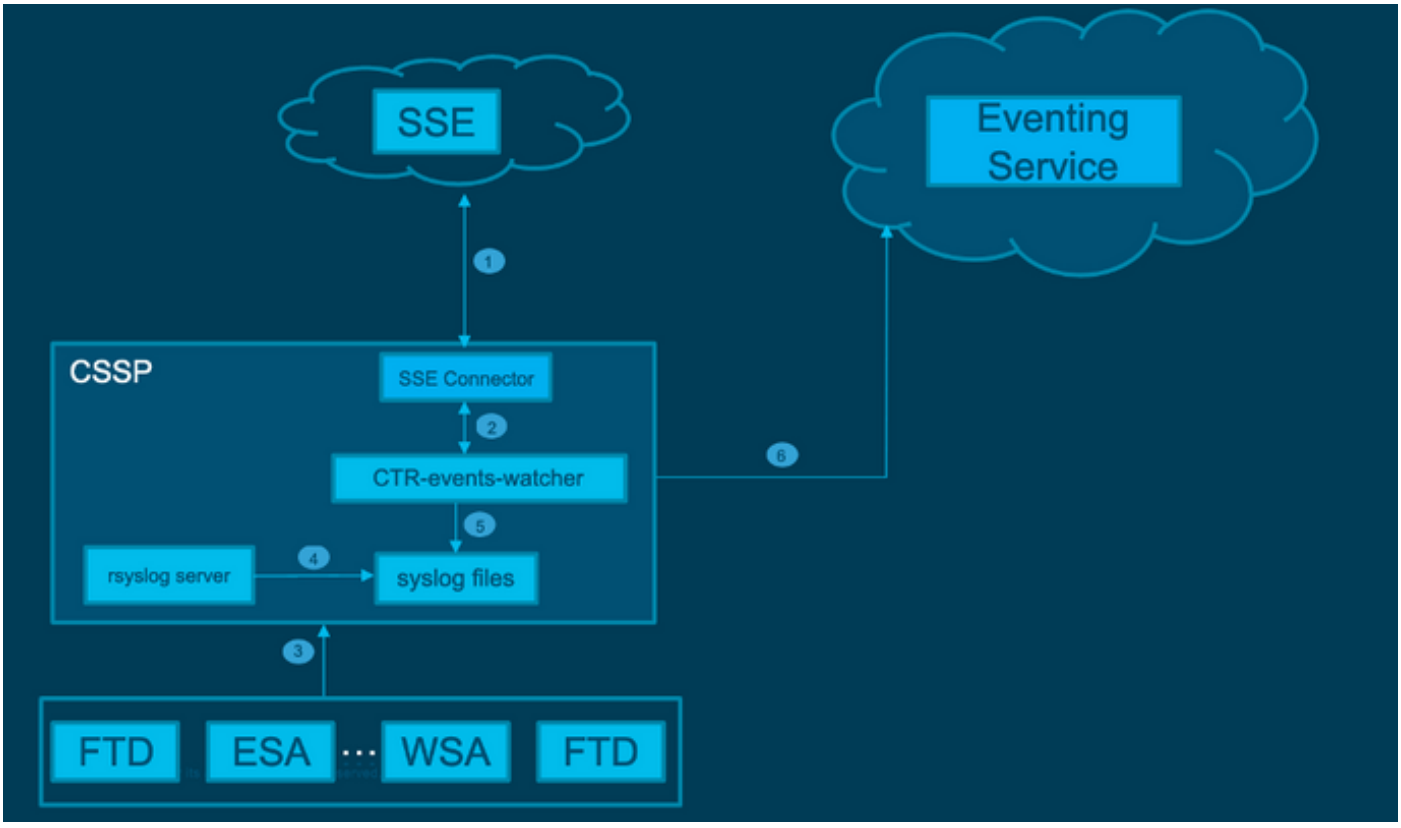
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se observa el error de configuración de la nube porque el FTD no puede comunicarse con api-sse.cisco.com. que es el sitio al que deben llegar los dispositivos Firepower para integrarse con los servicios SecureX y en la nube.

Esta alerta forma parte de la función Rapid Threat Containment (RTC), que está activada de forma predeterminada en las nuevas versiones de Firepower, en las que el FTD debe poder hablar con api-sse.cisco.com en Internet. Si esta comunicación no está disponible, el módulo de supervisión de estado del FTD muestra este mensaje de error.

Diagrama de la red



Problema

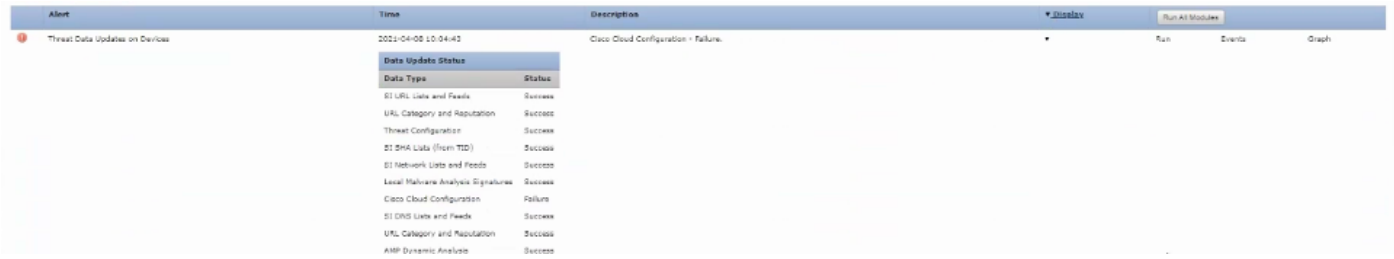
Como el Id. de bug de mejora de Cisco CSCvr46845 describe cuando el sistema Firepower activa la alerta de estado "Cisco Cloud Configuration - Failure" la mayor parte del tiempo, el problema está relacionado con la conectividad entre FTD y api-sse.cisco.com. Sin embargo, la alerta es muy genérica y no es de mucha ayuda enfocar la resolución de problemas necesaria ya que puede señalar varios problemas, incluso si todavía se trata de conectividad, pero en un contexto diferente.

Hay dos escenarios posibles principales:

Escenario 1. La integración en la nube no está habilitada. Si hay alguna integración en la nube, se esperaría por completo recibir esta alerta. Porque no se permite la conectividad con el portal de la nube.

Situación hipotética 2. La integración en la nube está habilitada. En este caso, es necesario llevar a cabo un análisis más detallado para descartar diferentes circunstancias que impliquen una falla de conectividad.

El ejemplo de alerta de falla de estado se muestra en la siguiente imagen:



Ejemplo de alerta de falla de estado

Troubleshoot

Solución para la situación 1. Se observa el error de configuración de la nube porque el FTD no puede comunicarse con https://api-sse.cisco.com/

Para desactivar la alerta de "Error en la configuración de la nube de Cisco", navegue hasta **Sistema > Estado > Política > Editar política > Actualizaciones de datos de amenazas en dispositivos > Seleccione Habilitado (Desactivado) > Guardar política y salir**. Estas son las pautas de referencia para la configuración en línea.

Solución para la situación 2. Cuándo se debe habilitar la integración en la nube.

Principales comandos útiles para la resolución de problemas:

```
curl -v -k https://api-sse.cisco.com <-- To verify connection with the external site
nslookup api-sse.cisco.com <-- To dicard any DNS error
/ngfw/etc/sf/connector.properties <-- To verify is configure properly the FQDN settings
lsof -i | grep conn <-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED
```

Opción 1. Configuración de DNS ausente

Paso 1. Verifique que los servidores DNS estén configurados en el FTD. Si no hay configuraciones DNS, puede proceder de la siguiente manera:

```
> show network
```

Paso 2. Agregue servidores DNS con el comando:

```
> configure network dns servers dns_ip_addresses
```

Después de configurar el DNS, la alerta de estado se corrige y el dispositivo se muestra como correcto. Podría tardar un tiempo en reflejarse el cambio y establecer los servidores DNS adecuados configurados.

Opción 2. El DNS del cliente no pudo resolver https://api-sse.cisco.com

Pruebe con el comando **curl**. Si el dispositivo no puede alcanzar el sitio en la nube, recibirá un resultado similar a este ejemplo.

```
FTD01:/home/ldap/abbac# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

> **Sugerencia**: comience con el mismo método de solución de problemas que en la opción 1. Verifique primero que la configuración DNS esté configurada correctamente. Puede observar un problema de DNS después de ejecutar el comando curl.

Una salida de rizo buena y correcta debe ser la siguiente:

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api-sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 30 Dec 2020 21:41:15 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
```

```
<ETag: "5fb40950-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src https: ;
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<X-Frame-Options: SAMEORIGIN
<Strict-Transport-Security: max-age=31536000; includeSubDomains
<
* Connection #0 to host api-sse.cisco.com left intact
Forbidden
```

Diríjase al nombre de host del servidor.

```
# curl -v -k https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
 CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

Utilice las herramientas básicas de conectividad como los comandos **nslookup, telnet** y **ping** para verificar, así como la resolución de DNS correcta para el sitio de la nube de Cisco.

> **Nota**: los servicios en la nube de Firepower deben tener una conexión saliente a la nube en el puerto 8989/tcp.

Aplique nslookup a los hostnames del servidor.

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com

root@fp:/home/admin# nslookup api-sse.cisco.com
Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 10.234.20.16
```

En el caso de problemas de conexión a AMP Cloud, puede deberse a la resolución de DNS. Verifique la configuración de DNS o realice nslookup desde el FMC.

```
nslookup api.amp.sourcefire.com
```

TELNET

```
root@fp:/home/admin# telnet api-sse.cisco.com 8989
```

```
root@fp:/home/admin# telnet api-sse.cisco.com 443
root@fp:/home/admin# telnet cloud-sa.amp.cisco.com 443
```

Ping

```
root@fp:/home/admin# ping api-sse.cisco.com
```

Más opciones de solución de problemas

Verifique las propiedades del conector en **/ngfw/etc/sf/connector.properties**. Debe ver esta salida con el puerto de conector correcto (8989) y el connector_fqdn con la URL correcta.

```
root@Firepower-module1:sf# cat /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions
connector_fqdn=api-sse.cisco.com
```

Puede consultar la Guía de configuración de Firepower para obtener una mejor referencia.

Problemas conocidos

ID de bug de Cisco CSCvs05084 FTD Falla de configuración de nube de Cisco debido a proxy

ID de bug de Cisco CSCvp56922 Use la API update-context sse-connector para actualizar el nombre de host y la versión del dispositivo

Error de ID de error de Cisco CSCvu02123 DOC: actualizar URL accesible desde dispositivos Firepower a SSE en la guía de configuración de CTR

Cisco bug ID CSCvr46845 ENH: El mensaje de estado "Cisco Cloud Configuration - Failure" necesita mejora

[Vídeo] Firepower: registro de FMC en SSE

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).