Fehlerbehebung bei "Cloud-Konfigurationsfehler" auf FirePOWER-Geräten

Inhalt

Einleitung

In diesem Dokument werden häufige Szenarien beschrieben, in denen das FirePOWER-System eine Statusmeldung auslöst: "Threat Data Updates - Cisco Cloud Configuration - Failure" (Aktualisierung von Bedrohungsdaten - Cisco Cloud-Konfiguration - Fehler).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER-System
- Cloud-Integration
- DNS-Auflösung und Proxy-Konnektivität
- Integration von Cisco Threat Response (CTR)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER Management Center (FMC) Version 6.4.0 oder höher
- Firepower Threat Defense (FTD) oder Firepower Sensor Module (SFR) Version 6.4.0 oder höher
- Cisco Secure Services Exchange (SSE)

- Cisco Smart Account-Portal

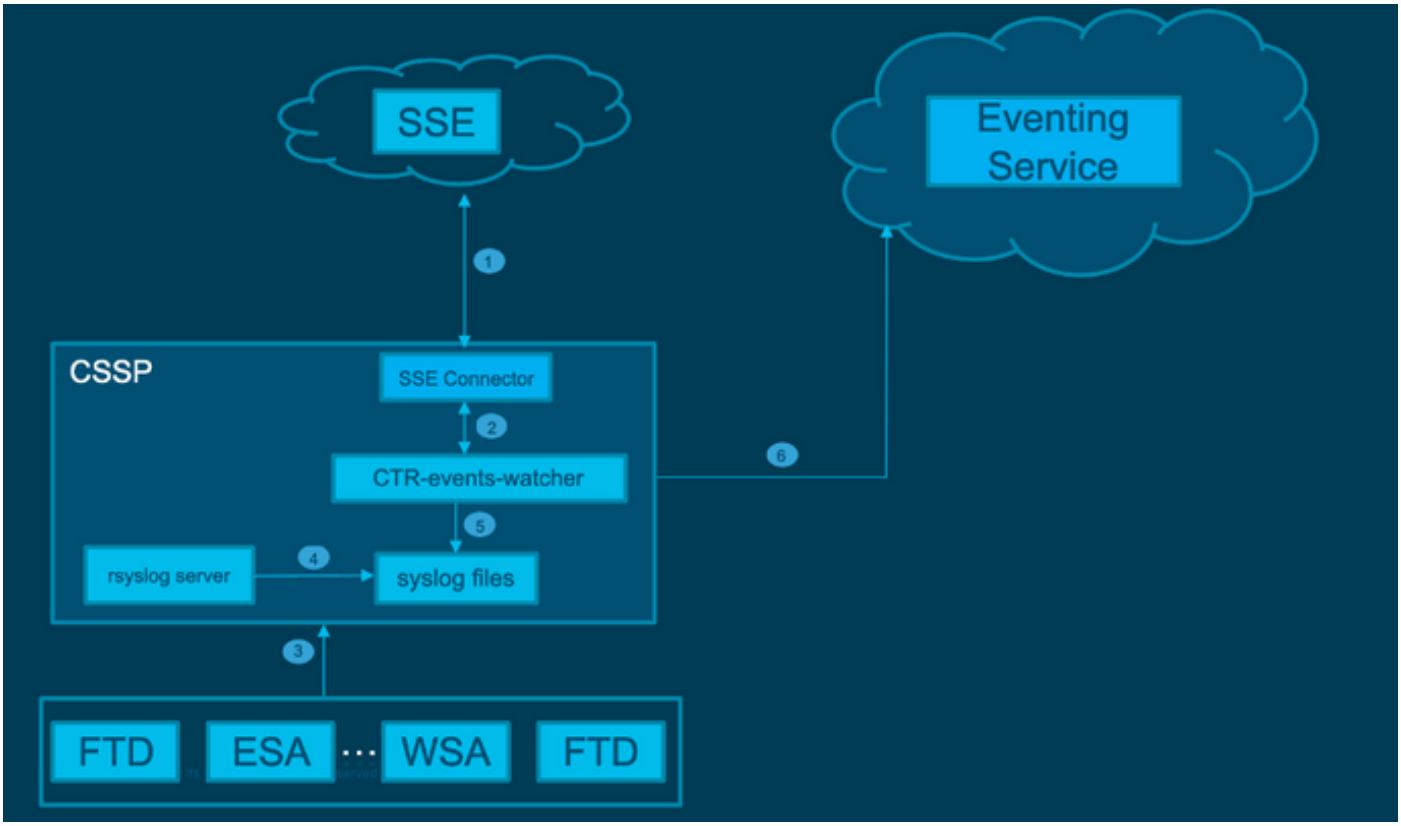
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Der Cloud-Konfigurationsfehler wurde beobachtet, da die FTD nicht mit api-sse.cisco.com kommunizieren kann. Dies ist der Standort, den die FirePOWER-Geräte erreichen müssen, um die SecureX- und Cloud-Services zu integrieren.

Diese Warnung ist Teil der Rapid Threat Containment (RTC)-Funktion, die standardmäßig für die neuen Firepower-Versionen aktiviert ist. Die FTD muss in der Lage sein, im Internet mit api-sse.cisco.com zu sprechen. Wenn diese Kommunikation nicht verfügbar ist, zeigt das FTD-Statusüberwachungsmodul diese Fehlermeldung an.

Netzwerkdiagramm



Problem

Wie die Enhancement Cisco Bug-ID CSCvr46845 beschreibt, wenn das FirePOWER-System die Warnmeldung "Cisco Cloud Configuration - Failure" auslöst, hängt das Problem meistens mit der Verbindung zwischen FTD und api-sse.cisco.com zusammen. Die Warnmeldung ist jedoch sehr allgemein gehalten, und es ist nicht sehr hilfreich, sich auf die erforderliche Fehlerbehebung zu konzentrieren, da sie auf verschiedene Probleme hinweisen kann, auch wenn es sich dabei um die Verbindung handelt, jedoch in einem anderen Kontext.

Es gibt zwei mögliche Hauptszenarien:

Szenario 1. Cloud-Integration ist nicht aktiviert. Bei Cloud-Integration wird diese Warnung voraussichtlich vollständig ausgegeben. Weil die Verbindung zum Cloud-Portal nicht zulässig ist.

Szenario 2. Cloud-Integration ist aktiviert. In diesem Fall muss eine detailliertere Analyse durchgeführt werden, um unterschiedliche Umstände auszuschließen, die einen Verbindungsausfall mit sich bringen.

Ein Beispiel für eine Warnmeldung bei einem Systemausfall wird im nächsten Bild angezeigt:

Beispiel für eine Warnmeldung bei einem Systemausfall

Fehlerbehebung

Lösung für Szenario 1. Der Cloud-Konfigurationsfehler wurde beobachtet, weil die FTD nicht mit https://api-sse.cisco.com/ kommunizieren kann.

Um die Warnmeldung "Cisco Cloud-Konfigurationsfehler" zu deaktivieren, navigieren Sie zu **System > Health > Policy > Edit policy > Threat Data Updates on Devices > Choose Enabled (Off) > Save policy and Exit**. Hier finden Sie die Referenzrichtlinien für die Inline-Konfiguration.

Lösung für Szenario 2. Wenn die Cloud-Integration aktiviert werden muss.

Hilfreiche Hauptbefehle für die Fehlerbehebung:

```
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
```

Option 1: DNS-Konfiguration fehlt

Schritt 1: Überprüfen Sie, ob die DNS-Server auf dem FTD konfiguriert sind. Wenn keine DNS-Konfigurationen vorhanden sind, können Sie wie folgt vorgehen:

```
> show network
```

Schritt 2: Fügen Sie mit dem folgenden Befehl DNS-Server hinzu:

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

Nach der Konfiguration des DNS wird die Integritätswarnung behoben, und das Gerät wird als fehlerfrei angezeigt. Es kann eine Weile dauern, bis die Änderung übernommen und die richtigen DNS-Server konfiguriert werden.

Option 2: Der Kunden-DNS konnte https://api-sse.cisco.com nicht auflösen.

Testen Sie mit dem **curl-**Befehl. Wenn das Gerät den Cloud-Standort nicht erreichen kann, erhalten Sie eine Ausgabe ähnlich diesem Beispiel.

```
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'
```

> **Tipp:** Beginnen Sie mit der Fehlerbehebung auf die gleiche Weise wie bei Option 1. Überprüfen Sie zunächst, ob die DNS-Konfiguration richtig eingestellt ist. Sie können ein DNS-Problem feststellen, nachdem der curl-Befehl ausgeführt wurde.

Eine gute und korrekte Curl-Ausgabe muss wie folgt aussehen:

```
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
```

Zum Server-Hostnamen wechseln.

```
# 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):
```

Verwenden Sie die grundlegenden Verbindungstools wie **nslookup, telnet** und **ping**, um die richtige DNS-Auflösung für die Cisco Cloud-Website zu überprüfen.

> **Hinweis**: FirePOWER Cloud-Services müssen über eine ausgehende Verbindung zur Cloud auf Port 8989/tcp verfügen.

Wenden Sie nslookup auf die Server-Hostnamen an.

```
# 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
```

Bei Verbindungsproblemen mit der AMP Cloud kann dies auf eine DNS-Auflösung zurückzuführen sein. Überprüfen Sie die DNS-Einstellungen, oder führen Sie nslookup vom FMC aus.

```
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
```

Weitere Optionen zur Fehlerbehebung

Überprüfen Sie die Konnektoreigenschaften unter **/ngfw/etc/sf/connector.properties**. Sie müssen diese Ausgabe mit dem richtigen Anschluss (8989) und connector_fqdn mit der richtigen URL sehen.

```
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
```

Weitere Informationen finden Sie im Firepower-Konfigurationsleitfaden.

Bekannte Probleme

Cisco Bug-ID CSCvs05084 FTD Cisco Cloud-Konfigurationsfehler aufgrund des Proxys

Cisco Bug-ID CSCvp56922 Update-Context Sse-Connector-API zur Aktualisierung von Hostname und Version des Geräts verwenden

Cisco Bug-ID CSCvu02123 DOC Bug: Update URL erreichbar von FirePOWER Devices zu SSE im CTR Konfigurationsleitfaden

Cisco Bug-ID CSCvr46845 ENH: Integritätsmeldung "Cisco Cloud Configuration - Failure" muss verbessert werden

[Video] FirePOWER - FMC bei SSE registrieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.