Probleemoplossing "Cloud-configuratiefout" op FirePOWER-apparaten

Inhoud

Inleiding

In dit document worden veel voorkomende scenario's beschreven waarin het FirePOWER-systeem de melding "Threat Data Updates - Cisco Cloud Configuration - Failure" activeert.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower System
- Cloudintegratie
- DNS-resolutie- en proxyconnectiviteit
- Cisco Threat Response (CTR)-integratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center (FMC) versie 6.4.0 of hoger
- Firepower Threat Defence (FTD) of Firepower Sensor Module (SFR) versie 6.4.0 of hoger
- Cisco Secure Services Exchange (SSE)
- Cisco Smart Account-portal

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

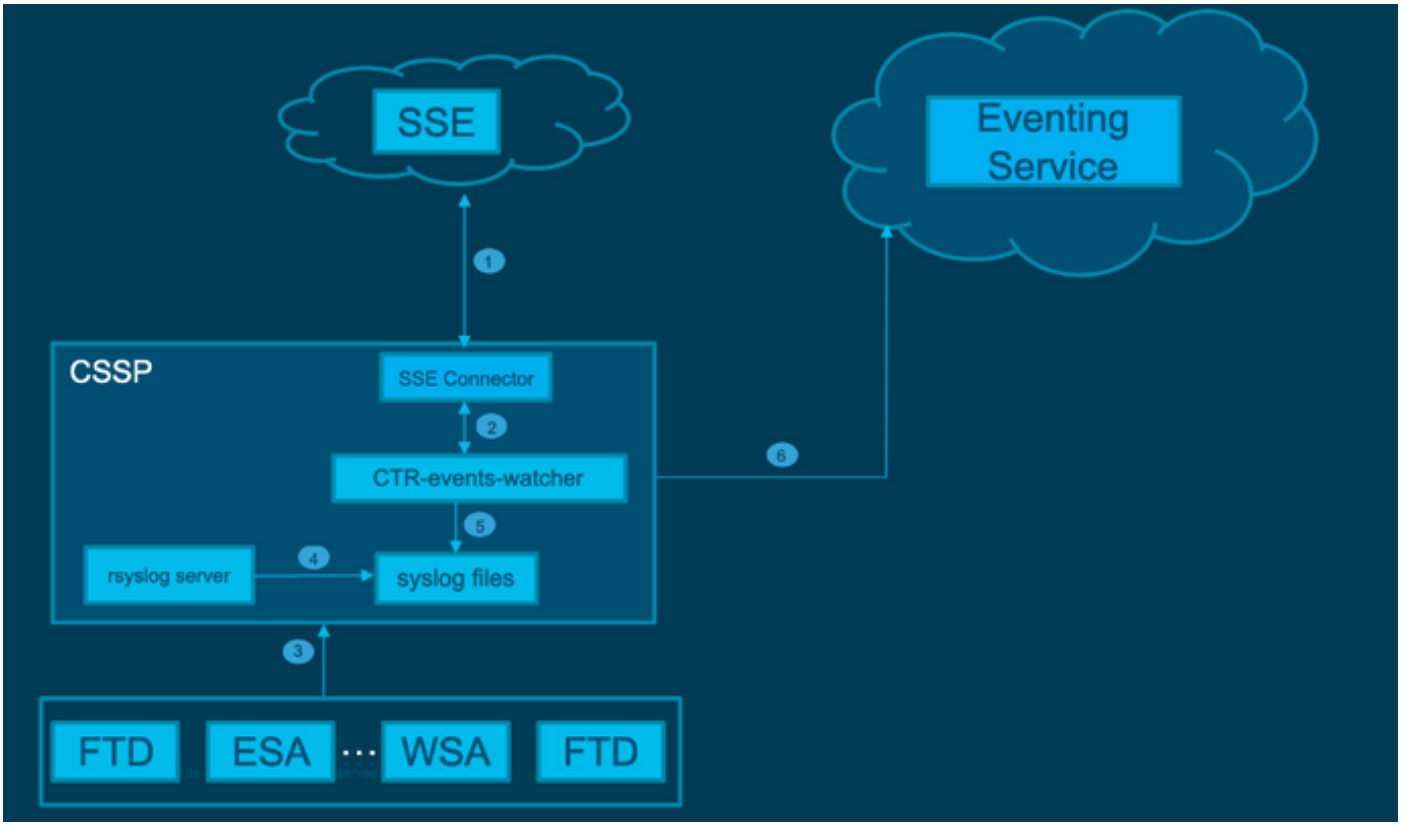
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Cloud Configuration-fout wordt waargenomen omdat de FTD niet kan communiceren met api-se.cisco.com. dat is de site die de FirePOWER-apparaten moeten bereiken om te kunnen integreren met de SecureX- en Cloud-services.

Deze waarschuwing maakt deel uit van de functie Rapid Threat Containment (RTC), die standaard is ingeschakeld voor de nieuwe FirePOWER-versies, waarin de FTD op het internet moet kunnen praten met api-sse.cisco.com. Indien deze mededeling niet beschikbaar is, wordt deze foutmelding weergegeven in de gezondheidsmonitormodule van de FTD.

Netwerkdiagram



Probleem

Zoals wordt beschreven in de Cisco bug-id van Enhancement CSCvr46845 wanneer het FirePOWER-systeem de Health Alert "Cisco Cloud Configuration - Failure" activeert, is het probleem meestal gerelateerd aan de connectiviteit tussen FTD en api-sse.cisco.com. De waarschuwing is echter erg algemeen en het is niet erg nuttig om de nodige probleemoplossing te focussen, aangezien deze kan wijzen op verschillende problemen, zelfs als het nog steeds gaat over connectiviteit, maar in een andere context.

Er zijn twee belangrijke mogelijke scenario's:

Scenario 1. Cloudintegratie is niet ingeschakeld. Als er een Cloud Integration is, dan wordt

volledig verwacht om deze waarschuwing te krijgen. Omdat de verbinding met het cloudportaal niet is toegestaan.

Scenario 2. Cloudintegratie is ingeschakeld. In dit geval, is het noodzakelijk om een meer gedetailleerde analyse uit te voeren om verschillende omstandigheden uit te sluiten die een connectiviteitsmislukking impliceren.

Het volgende voorbeeld van een waarschuwing voor gezondheidsfouten wordt weergegeven in de volgende afbeelding:

Voorbeeld van waarschuwing voor gezondheidsfouten

Problemen oplossen

Oplossing voor scenario 1. De fout in de cloudconfiguratie wordt opgemerkt omdat de FTD niet kan communiceren met https://api-sse.cisco.com/

Als u de waarschuwing "Cisco Cloud Configuration-Failure" wilt uitschakelen, gaat u naar **Systeem > Gezondheid > Beleid > Beleid > Beleid bewerken > Updates van bedreigingsgegevens op apparaten > Ingeschakeld (Uit) kiezen > Beleid opslaan en afsluiten**. Hier zijn de referentierichtlijnen voor inline configuratie.

Oplossing voor scenario 2. Wanneer de cloudintegratie moet worden ingeschakeld.

Belangrijkste nuttige opdrachten voor probleemoplossing:

```
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
```

Optie 1. DNS-configuratie ontbreekt

Stap 1. Controleer of DNS-servers zijn geconfigureerd op de FTD. Als er geen DNS-configuraties zijn, kunt u als volgt te werk gaan:

```
> show network
```

Stap 2. Voeg DNS-servers toe met de opdracht:

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

Na het configureren van de DNS wordt de waarschuwing hersteld en wordt het apparaat als gezond weergegeven. Het zou een tijdje kunnen duren om de verandering te weerspiegelen en de juiste DNS servers te configureren.

Optie 2. De klant DNS kon geen oplossing vinden op https://api-sse.cisco.com

Test met de **krulopdracht** . Als het apparaat de cloudsite niet kan bereiken, ontvangt u een uitvoer vergelijkbaar met dit voorbeeld.

```
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'
```

> **Tip**: begin met dezelfde probleemoplossing als in optie 1. Controleer eerst of de DNS-configuratie juist is ingesteld. U kunt een DNS probleem opmerken nadat het de krulopdracht in werking stelt.

Een goede en correcte kruloutput moet als volgt zijn:

```
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
```

Curl naar de server hostnaam.

```
# 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):
```

Gebruik de basisconnectiviteitstools, zoals de opdrachten **nslookup, telnet** en **ping** om te verifiëren en de juiste DNS-resolutie voor de Cisco Cloud-site.

> **Opmerking**: Firepower Cloud Services moet uitgaande verbinding met de cloud hebben op poort 8989/tcp.

Pas nslookup op de server hostnames toe.

```
# 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
```

Voor verbindingsproblemen met AMP Cloud kan dit te wijten zijn aan DNS-resolutie. Controleer de DNS-instellingen of zoek de gegevens op via het VCC.

```
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
```

Meer opties voor probleemoplossing

Controleer de eigenschappen van de connector onder **/ngfw/etc/sf/connector.properties**. U moet deze uitvoer zien met de juiste connector (8989) en connector_fqdn met de juiste URL.

```
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
```

U kunt de Firepower Configuration Guide raadplegen voor meer informatie.

Bekende problemen

Cisco bug-id CSCvs05084 FTD Cisco Cloud Configuration-fout vanwege proxy

Cisco bug-id CSCvp5692 API voor update-context connector gebruiken om hostnaam en versie van apparaat bij te werken

Cisco bug-id CSCvu02123 DOC-bug: update URL bereikbaar van FirePOWER Devices naar SSE in de CTR-configuratiehandleiding

Cisco bug-id CSCvr46845 ENH: gezondheidsbericht 'Cisco Cloud Configuration - Failure' moet worden verbeterd

[Video] Firepower - Registreer FMC in SSE

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.