Risoluzione dei problemi relativi a "Cloud Configuration Failure" sui dispositivi Firepower

Sommario

Introduzione

Questo documento descrive gli scenari comuni in cui il sistema Firepower attiva l'avviso di integrità: Threat Data Updates - Cisco Cloud Configuration - Failure.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center
- Firepower Threat Defense
- Modulo sensore Firepower
- Integrazione cloud
- Risoluzione DNS e connettività proxy
- Integrazione Cisco Threat Response (CTR)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

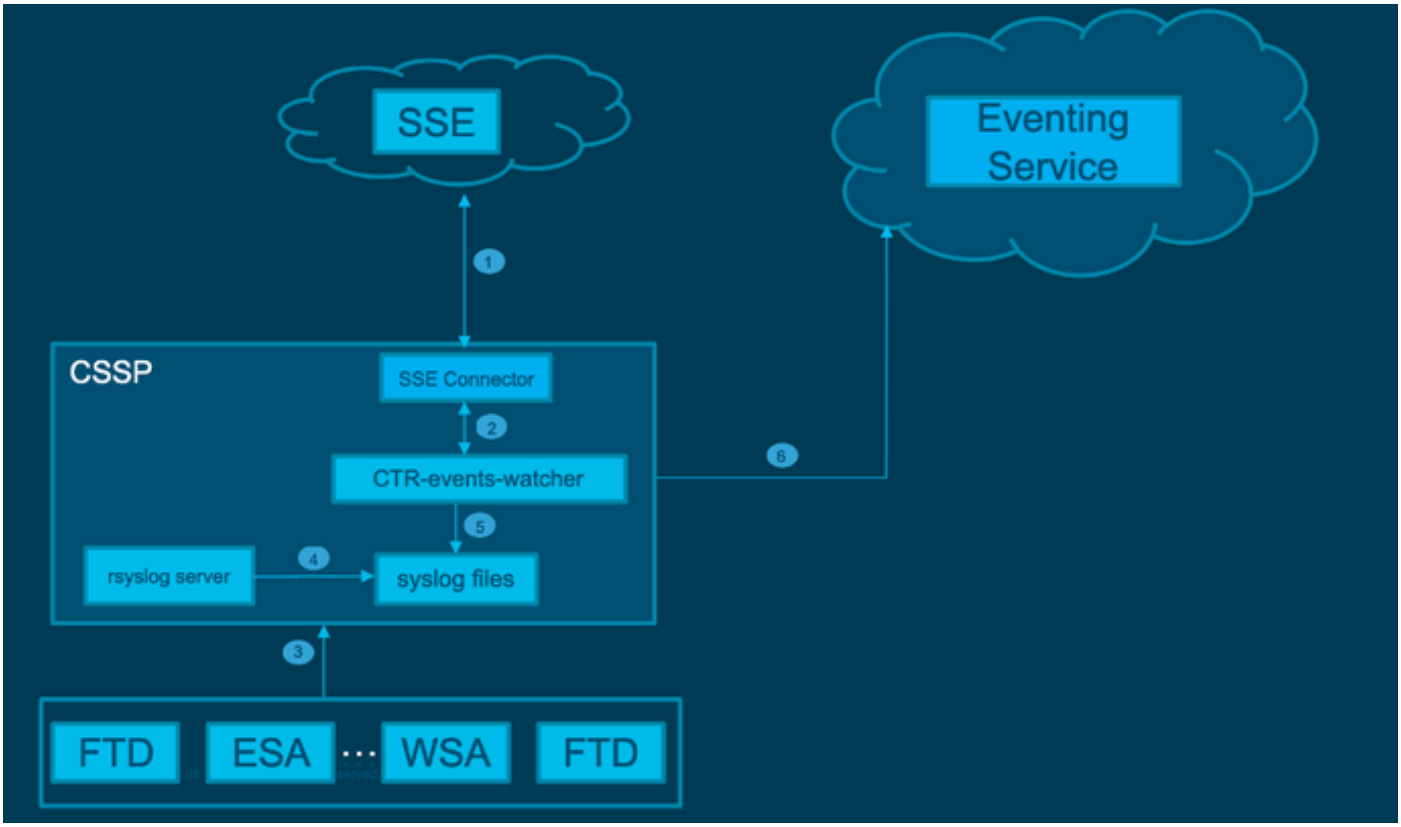
Si è verificato un errore di configurazione cloud perché l'FTD non è in grado di comunicare con api-sse.cisco.com.

Questo è il sito che i dispositivi Firepower devono raggiungere per integrarsi con i servizi SecureX e Cloud.

Questo avviso fa parte della funzionalità Rapid Threat Container (RTC). Questa funzione è abilitata per impostazione predefinita nelle nuove versioni di Firepower, in cui l'FTD deve essere in grado di parlare con api-sse.cisco.com su Internet.

Se questa comunicazione non è disponibile, il modulo di monitoraggio dell'integrità FTD visualizza questo messaggio di errore: Threat Data Updates - Cisco Cloud Configuration - Failure

Esempio di rete



Problema

L'ID bug Cisco CSCvr46845 spiega che quando il sistema Firepower attiva l'avviso di integrità Configurazione cloud Cisco - Errore, il problema è spesso correlato alla connettività tra FTD e api-sse.cisco.com.

Tuttavia, l'avviso è molto generico e può indicare vari problemi, anche se ancora relativi alla connettività, ma in un contesto diverso.

Esistono due scenari principali:

Scenario 1. Se l'integrazione cloud non è abilitata, questo avviso è previsto perché la connettività al portale cloud non è consentita.

Scenario 2. Nel caso in cui l'integrazione cloud sia abilitata, è necessario eseguire un'analisi più dettagliata per eliminare le circostanze che comportano un errore di connettività.

L'esempio di avviso di errore di integrità viene mostrato nell'immagine seguente:

Esempio di avviso di errore di integrità

Risoluzione dei problemi

Soluzione per lo scenario 1. L'errore di configurazione del cloud è stato osservato perché l'FTD non è in grado di comunicare con https://api-sse.cisco.com/

Per disabilitare l'avviso di errore di configurazione del cloud Cisco, selezionare Sistema > Integrità > Criteri > Modifica criterio > Aggiornamenti dati minaccia sui dispositivi. Scegliere Attivato (Disattivato), Salva criterio ed Esci.

Di seguito sono riportate le linee guida di riferimento per la configurazione inline.

Soluzione per lo scenario 2. Quando è necessario abilitare l'integrazione cloud.

Comandi utili per la risoluzione dei problemi:

<#root>

```
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
```

Opzione 1. Configurazione DNS assente

Passaggio 1. Verificare che i DNS siano configurati nell'FTD. Se non sono disponibili configurazioni DNS, procedere come segue:

```
> show network
```

Passaggio 2. Aggiungere DNS con il comando:

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

Dopo aver configurato il DNS, l'avviso di integrità viene corretto e il dispositivo risulta integro. L' è un breve intervallo di tempo prima che la modifica venga riflessa e che i server DNS corretti siano configurati.

Opzione 2. Il DNS del cliente non è stato in grado di risolvere https://api-sse.cisco.com

Provare con il comando curl. Se il dispositivo non riesce a raggiungere il sito cloud, è presente un output simile a questo esempio.

<#root>

```
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'
```

Suggerimento: iniziare con lo stesso metodo di risoluzione dei problemi dell'opzione 1. Verificare innanzitutto che la configurazione DNS sia impostata correttamente. Si è verificato un problema DNS dopo l'esecuzione del comando curl.

L'output della curva corretto deve essere il seguente:

<#root>

```
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 sul nome host del server.

<#root>

```
#
```

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):
```

Utilizzare gli strumenti di connettività di base, ad esempio i comandi nslookup, telnet e ping, per verificare e anche la risoluzione DNS corretta per il sito Cisco Cloud.

Nota: i servizi cloud Firepower devono avere una connessione in uscita al cloud sulla porta 8989/tcp.

Applicare nslookup ai nomi host del server.

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

<#root>

```
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
```

I problemi di connessione a AMP Cloud potrebbero essere dovuti alla risoluzione DNS. Verificare le impostazioni DNS o eseguire nslookup dal CCP.

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

Telnet

<#root>

```
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>

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

Altre opzioni di risoluzione dei problemi

Verificare le proprietà del connettore in /ngfw/etc/sf/connector.properties. Questo output deve essere visualizzato con la porta del connettore corretta (8989) e il connettore_fqdn con l'URL corretto.

<#root>

```
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

Per ulteriori informazioni, consultare la Guida alla configurazione di Firepower.

Problemi noti

ID bug Cisco CSCvs05084 FTD Errore di configurazione Cisco Cloud a causa di un proxy

ID bug Cisco CSCvp56922 Uso dell'API del connettore sse update-context per aggiornare il nome host e la versione del dispositivo

ID bug Cisco CSCvu02123 DOC Bug: Update URL reachable from Firepower Devices to SSE (Aggiornamento URL raggiungibile dai dispositivi Firepower a SSE) nella guida alla configurazione di CTR

ID bug Cisco CSCvr46845 ENH: Messaggio integrità Configurazione Cisco Cloud - Miglioramento errori

[Video] Firepower - Registra FMC in SSE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).