Dépannage de " ; Cloud Configuration Failure" ; sur les périphériques Firepower

Table des matières

Introduction

Ce document décrit des scénarios courants où le système Firepower déclenche l'alerte d'intégrité « Mises à jour des données de menace - Configuration du cloud Cisco - Échec ».

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système Firepower
- Intégration du cloud
- Résolution DNS et connectivité proxy
- Intégration de Cisco Threat Response (CTR)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Management Center (FMC) version 6.4.0 ou ultérieure
- Firepower Threat Defense (FTD) ou Firepower Sensor Module (SFR) version 6.4.0 ou

ultérieure
- Cisco Secure Services Exchange (SSE)
- Portail Cisco Smart Account

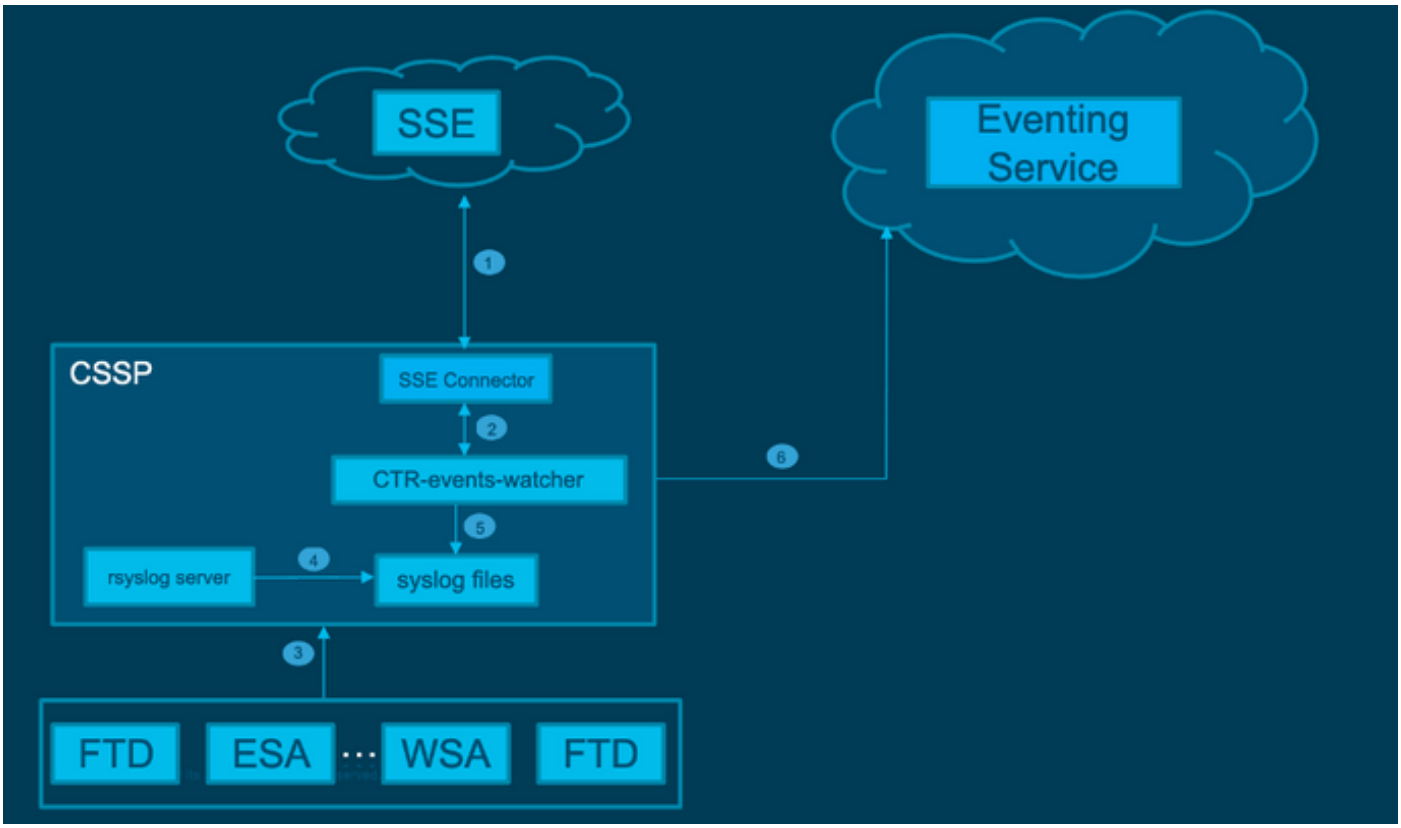
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'erreur de configuration du cloud est observée parce que le FTD n'est pas en mesure de communiquer avec api-sse.cisco.com. qui est le site que les périphériques Firepower doivent atteindre afin de s'intégrer avec les services SecureX et Cloud.

Cette alerte fait partie de la fonctionnalité de confinement rapide des menaces (RTC), qui est activée par défaut sur les nouvelles versions de Firepower, dans laquelle le FTD doit pouvoir communiquer avec api-sse.cisco.com sur Internet. Si cette communication n'est pas disponible, le module Health Monitor du FTD affiche ce message d'erreur.

Diagramme du réseau



Problème

Comme l'amélioration Cisco bug ID CSCvr46845 décrit lorsque le système Firepower déclenche l'alerte d'intégrité « Cisco Cloud Configuration - Failure » la plupart du temps, le problème est lié à la connectivité entre FTD et api-sse.cisco.com. Cependant, l'alerte est très générique et il n'est

pas d'une grande aide de concentrer le dépannage nécessaire car elle peut pointer vers divers problèmes, même s'il s'agit toujours de connectivité, mais dans un contexte différent.

Il existe deux principaux scénarios possibles :

Scénario 1. L'intégration cloud n'est pas activée. En cas d'intégration du cloud, cette alerte devrait être émise. Parce que la connectivité au portail cloud n'est pas autorisée.

Scénario 2. L'intégration cloud est activée. Dans ce cas, il est nécessaire d'effectuer une analyse plus détaillée pour exclure différentes circonstances impliquant une panne de connectivité.

L'exemple d'alerte de défaillance d'intégrité est illustré dans l'image suivante :

Exemple d'alerte de défaillance sanitaire

Dépannage

Solution pour le scénario 1. L'erreur de configuration du cloud est observée car le FTD ne peut pas communiquer avec https://api-sse.cisco.com/

Pour désactiver l'alerte « Échec de la configuration du cloud Cisco », accédez à System > Health > Policy > Edit policy > Threat Data Updates on Devices > Choose Enabled (Off) > Save Policy and Exit. Voici les instructions de référence pour la configuration en ligne.

Solution pour le scénario 2. Lorsque l'intégration au cloud doit être activée.

Principales commandes utiles pour le dépannage :

<#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
```

Option 1. Configuration DNS absente

Étape 1. Vérifiez que les serveurs DNS sont configurés sur le FTD. S'il n'existe aucune configuration DNS, procédez comme suit :

```
> show network
```

Étape 2. Ajoutez des serveurs DNS à l'aide de la commande :

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

Une fois le DNS configuré, l'alerte d'intégrité est corrigée et le périphérique apparaît sain. Cela peut prendre un certain temps pour refléter la modification et configurer les serveurs DNS appropriés.

Option 2. Le DNS du client n'a pas pu résoudre https://api-sse.cisco.com

Testez avec la commande curl. Si le périphérique ne peut pas atteindre le site cloud, vous recevez un résultat similaire à celui de cet exemple.

```
<#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'
```

> Conseil : commencez par la même méthode de dépannage que dans l'option 1. Vérifiez d'abord que la configuration DNS est correctement définie. Vous pouvez remarquer un problème DNS après l'exécution de la commande curl.

Une sortie de boucle correcte et correcte doit être la suivante :

```
<#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
```

Accédez au nom d'hôte du serveur.

```
<#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):
```

Utilisez les outils de connectivité de base tels que les commandes nslookup, telnet et ping pour vérifier ainsi que la résolution DNS correcte pour le site cloud Cisco.

> Remarque : les services cloud Firepower doivent disposer d'une connexion sortante au cloud sur le port 8989/tcp.

Appliquez nslookup aux noms d'hôte du serveur.

```
# 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
```

Pour les problèmes de connexion au cloud AMP, cela peut être dû à la résolution DNS. Vérifiez les paramètres DNS ou effectuez la commande nslookup à partir du FMC.

```
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
```

Autres options de dépannage

Vérifiez les propriétés du connecteur sous /ngfw/etc/sf/connector.properties. Vous devez voir cette sortie avec le port de connecteur correct (8989) et le connector_fqdn avec l'URL correcte.

<#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
```

Vous pouvez vous référer au Guide de configuration de Firepower pour une meilleure référence.

Problèmes identifiés

ID de bogue Cisco CSCvs05084 FTD Échec de la configuration du cloud Cisco en raison d'un proxy

ID de bogue Cisco CSCvp56922 Utilisez l'API update-context sse-connector pour mettre à jour le nom d'hôte et la version du périphérique

Bogue CSCvu02123 DOC de l'ID de bogue Cisco : Mise à jour de l'URL accessible à partir de Firepower Devices vers SSE dans le guide de configuration CTR

Bogue Cisco ID CSCvr46845 ENH : le message d'intégrité « Cisco Cloud Configuration - Failure » doit être amélioré

[Vidéo] Firepower : enregistrement de FMC dans SSE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.