Troubleshoot "Cloud Configuration Failure" on Firepower Devices

Contents

Introduction

This document describes common scenarios where the Firepower System triggers Health Alert: **Threat Data Updates - Cisco Cloud Configuration - Failure**.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- **Firepower Management Center**
- **Firepower Threat Defense**
- **Firepower Sensor Module**
- Cloud Integration
- DNS resolution and proxy connectivity
- **Cisco Threat Response** (CTR) Integration

Components Used

The information in this document is based on these software and hardware versions:

- **Firepower Management Center** (FMC) version 6.4.0 or later
- **Firepower Threat Defense** (FTD) or **Firepower Sensor Module** (SFR) version 6.4.0 or later
- **Cisco Secure Services Exchange** (SSE)
- **Cisco Smart Account Portal**

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

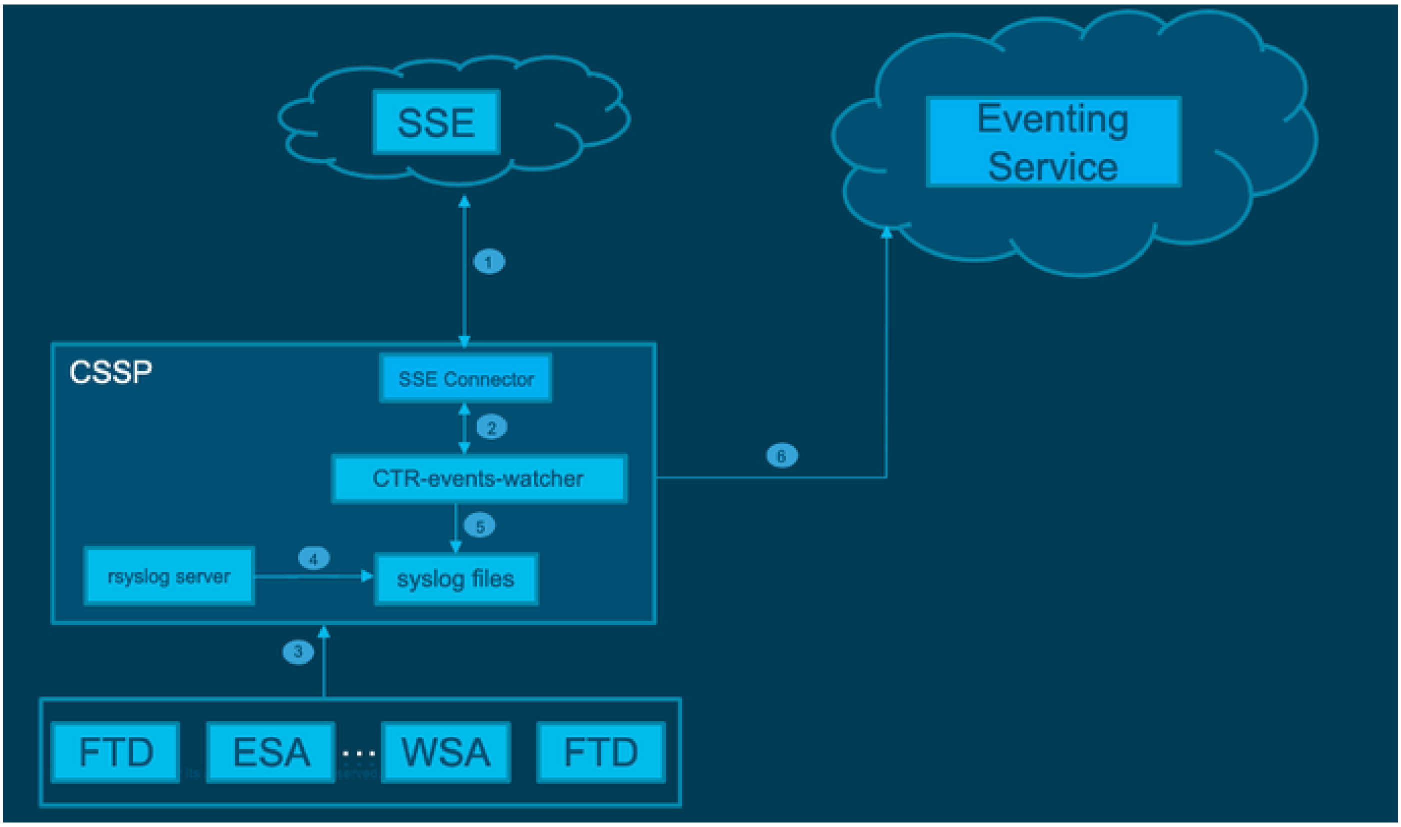
The **Cloud Configuration** error is observed because the FTD is unable to communicate with api-sse.cisco.com.

This is the site that the **Firepower** devices need to reach in order to integrate with the SecureX and Cloud services.

This alert is part of the **Rapid Threat Containment** (RTC) feature. This feature is enabled by default on the new Firepower versions, wherein the FTD needs to be able to talk to api-sse.cisco.com on the internet.

If this communication is not available, the FTD health monitor module displays this error message: **Threat Data Updates - Cisco Cloud Configuration - Failure**

Network Diagram



Problem

Cisco bug ID CSCvr46845 explains that when the **Firepower System** triggers the Health Alert **Cisco Cloud Configuration - Failure**, the issue is frequently related to connectivity between FTD and api-sse.cisco.com.

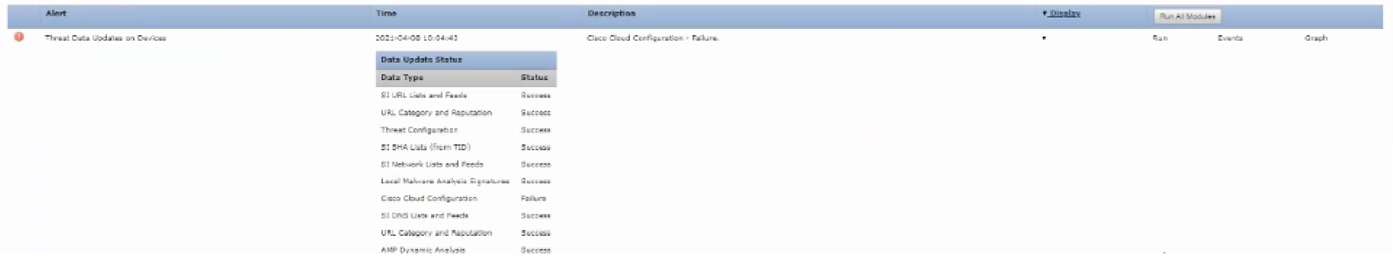
However, the alert is very generic and it can point to various problems, even if still about connectivity, but in a different context.

There are two main possible scenarios:

Scenario 1. In the case where **Cloud Integration** is not enabled, this alert is expected because the connectivity to the cloud portal is not allowed.

Scenario 2. In the case where **Cloud Integration** is enabled, it is necessary to carry out a more detailed analysis to eliminate circumstances that involve a connectivity failure.

Health Failure Alert Example is shown in the next image:



Alert	Time	Description
Threat Data Updates on Devices	2021-04-08 10:04:43	Cisco Cloud Configuration - Failure.

Data Update Status

Data Type	Status
SI URL Lists and Feeds	Success
URL Category and Reputation	Success
Threat Configuration	Success
SI SHA Lists (from TID)	Success
SI Network Lists and Feeds	Success
Local Malware Analysis Signatures	Success
Cisco Cloud Configuration	Failure
SI DNS Lists and Feeds	Success
URL Category and Reputation	Success
AMP Dynamic Analysis	Success

Health Failure Alert Example

Troubleshoot

Solution for Scenario 1. The cloud configuration error is observed because the FTD is unable to communicate with https://api-sse.cisco.com/

To Disable the **Cisco Cloud Configuration-Failure** alert, navigate to **System > Health > Policy > Edit policy > Threat Data Updates on Devices.** Choose **Enabled (Off), Save Policy** and **Exit**.

Here are the reference guidelines for inline configuration.

Solution for Scenario 2. When the cloud integration must be enabled.

Helpful commands for troubleshooting:

```
<#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. DNS Configuration Absent

Step 1. Verify that DNS are configured on the FTD. If there are no DNS configurations, proceed as follows:

```
> show network
```

Step 2. Add DNS with the command:

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

After configuring the DNS, the health alert is fixed and the device is shown as healthy. The is a brief time lapse before the change is reflected the proper DNS servers are configured.

Option 2. The Customer DNS could not Resolve https://api-sse.cisco.com

Test with the **curl** command. If the device cannot reach the cloud site, there is an output similar to this example.

<#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'
```

Tip: Start with the same method to troubleshoot as in Option 1. Verify first that the DNS configuration is properly set. You can notice a DNS issue after it runs the curl command.

A correct **curl** output must be as follows:

<#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 to the server hostname.

<#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):
```

Use the basic connectivity tools like the **nslookup**, **telnet**, and **ping** commands to verify as well as the correct DNS resolution for the Cisco Cloud site.

Note: Firepower Cloud Services must have outbound connection to the cloud on port 8989/tcp.

Apply **nslookup** to the server hostnames.

```
# 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
```

Connection issues to **AMP Cloud** are possibly due to DNS resolution. Verify the DNS settings or do **nslookup** from the 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
```

More Troubleshoot Options

Verify the connector properties under **/ngfw/etc/sf/connector.properties**. You must see this output with the correct connector port (8989) and the connector_fqdn with the correct URL.

<#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
```

For more information, refer to the Firepower Configuration Guide.

Known Issues

Cisco bug ID CSCvs05084 FTD Cisco **Cloud Configuration Failure** due to proxy

Cisco bug ID CSCvp56922 Use update-context sse-connector API to update device hostname and version

Cisco bug ID CSCvu02123 DOC Bug: Update URL reachable from Firepower Devices to SSE in the CTR configuration guide

Cisco bug ID CSCvr46845 ENH: Health message **Cisco Cloud Configuration - Failure** needs improvement

[Video] Firepower - Register FMC into SSE