"Cisco Cloud Configuration - Failure" 문제 해결 - Firepower 디바이스에 대한 위협 데이터 업데이트 알림

목차

소개

이 문서에서는 Firepower System에서 상태 알림 "위협 데이터 업데이트 - Cisco 클라우드 컨피그레이션 - 실패"를 트리거하는 가장 일반적인 시나리오와 알림을 해결하고 제거하기 위해 여러 솔루션을 사용하여 문제를 해결하는 다양한 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 시스템
- 클라우드 통합
- DNS 확인 및 프록시 연결
- Cisco CTR(Threat Response) 통합

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 6.4.0 이상의 FMC(Firepower Management Center)
- 버전 6.4.0 이상의 FTD(Firepower Threat Defense) 또는 SFR(Firepower Sensor Module)

- Cisco SSE(Secure Services Exchange)
- Cisco Smart Account 포털

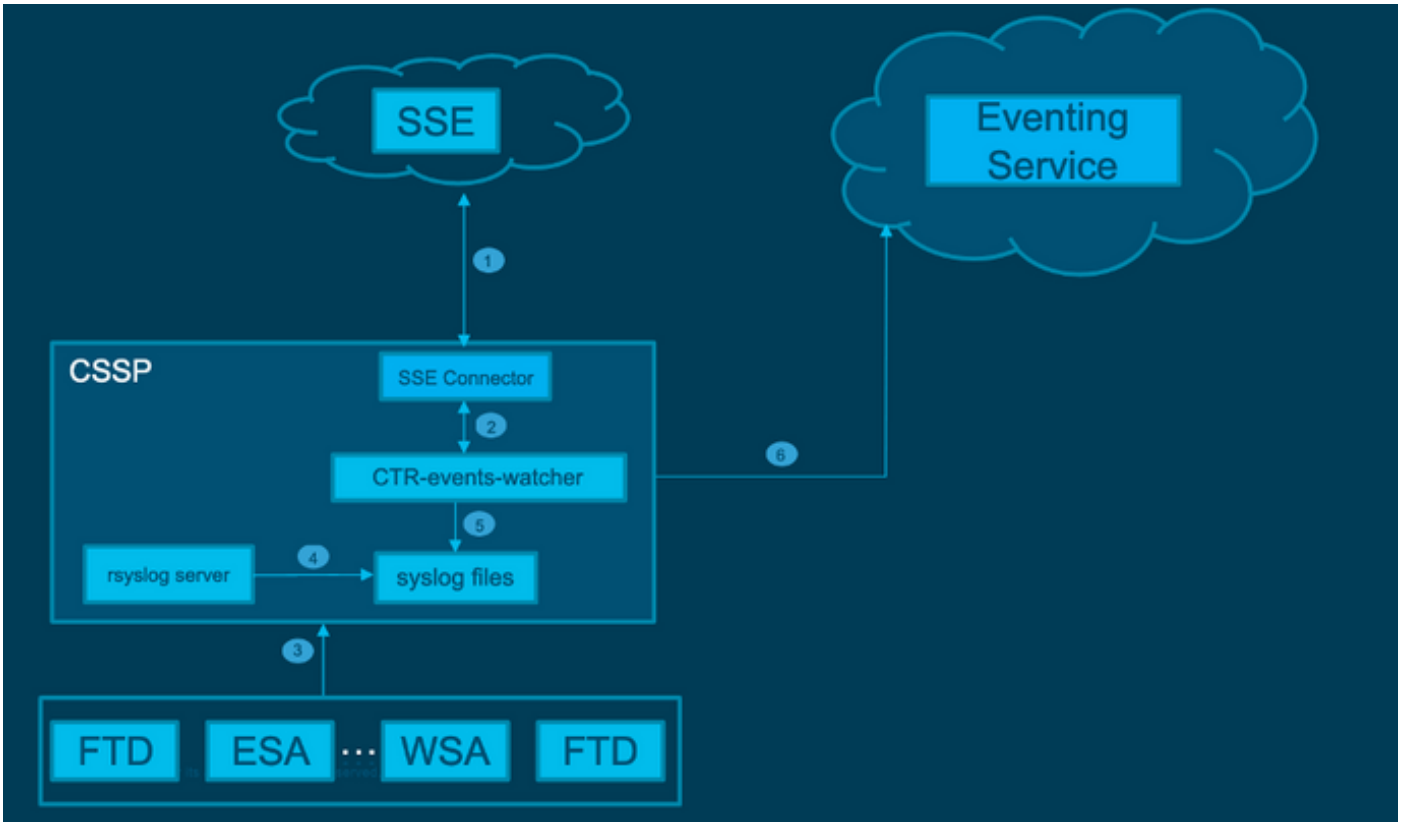
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FTD가 "https://api-sse.cisco.com"과 통신할 수 없기 때문에 클라우드 컨피그레이션 오류가 발생합니다. FirePOWER 디바이스가 SecureX 및 클라우드 서비스와 통합하기 위해 도달해야 하는 사이트는 어디입니까?

이 알림은 RTC(Rapid Threat Containment) 기능의 일부로, 새로운 Firepower 버전에서 기본적으로 활성화되어 있으며 FTD가 인터넷의 'api-sse.cisco.com'과 통신할 수 있어야 합니다. 이 통신을 사용할 수 없는 경우 FTD의 상태 모니터 모듈에 이 오류 메시지가 표시됩니다.

네트워크 다이어그램



문제

개선 사항 Cisco 버그 ID CSCvr46845는 Firepower System에서 상태 알림 "Cisco Cloud Configuration - Failure"를 트리거하는 시점을 설명하며, 대부분의 경우 문제가 FTD와 api-sse.cisco.com 간의 연결과 관련이 있습니다. 그러나 이 경고는 매우 일반적이며, 연결에 대한 문제가 있더라도 다른 맥락에서 다양한 문제를 가리킬 수 있으므로 필요한 트러블슈팅에 집중하는 데 큰 도움이 되지 않습니다.

가능한 시나리오는 크게 두 가지입니다.

시나리오 1. 클라우드 통합이 활성화되지 않았습니다. 클라우드 통합이 있을 경우 이 알림을 받을 것으로 예상됩니다. 클라우드 포털에 연결할 수 없기 때문입니다.

시나리오 2. 클라우드 통합이 활성화됩니다. 이 경우 연결 실패가 수반되는 서로 다른 상황을 배제하기 위해 보다 세밀한 분석을 수행할 필요가 있다.

상태 실패 알림 예는 아래 이미지에 나와 있습니다.

상태 실패 알림 예

문제 해결

시나리오 1의 해결책. FTD가 https://api-sse.cisco.com/과 통신할 수 없기 때문에 클라우드 구성 오류가 발생합니다

"Cisco Cloud Configuration-Failure" 알림을 비활성화합니다. **System > Health > Policy > Edit policy > Threat Data Updates on Devices > Enabled (Off) > Save Policy and Exit를 선택합니다**." 인라인 컨피그레이션에 대한 참조 지침은 다음과 같습니다.

시나리오 2. 클라우드 통합을 활성화해야 하는 경우.

문제 해결에 유용한 주요 명령:

```
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
```

옵션 1. DNS 구성 누락

1단계. DNS 컨피그레이션이 없는 경우 FTD에 DNS 서버가 구성되어 있는지 확인하고 다음과 같이 진행합니다.

```
> show network
```

2단계. 명령을 사용하여 DNS 서버를 추가합니다

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

DNS를 구성하면 상태 알림이 고정되어 디바이스가 정상으로 표시됩니다. 변경 사항을 반영하고 구성된 적절한 DNS 서버를 설정하는 데 시간이 걸릴 수 있습니다.

옵션 2. 고객 DNS가 https://api-sse.cisco.com을 확인할 수 없습니다.

curl 명령으로 테스트합니다. 디바이스가 클라우드 사이트에 도달할 수 없는 경우 아래 예와 유사한 출력이 표시됩니다

```
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'
```

> **팁:** 위의 옵션 1과 동일한 트러블슈팅 방법으로 시작하여 먼저 DNS 컨피그레이션이 제대로 설정되었는지 확인합니다. curl 명령을 실행한 후 DNS 문제를 확인할 수 있습니다.

올바른 컬 출력은 다음과 같이 표시되어야 합니다.

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.6.187.110...
* Connected to api-sse.cisco.com (52.6.187.110) 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
```

서버 호스트 이름으로 컬링

```
# curl -v -k https://cloud-sa.amp.cisco.com
*   Trying 52.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (52.21.117.50) 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):
```

nslookup, telnet 및 **ping 명령**과 같은 기본 연결 **툴**을 사용하여 Cisco 클라우드 사이트에 대한 올바른 DNS 확인 여부를 확인합니다.

> **참고:** Firepower Cloud Services는 포트 **8989/tcp**에서 클라우드에 대한 아웃바운드 연결이 있어야 합니다.

서버 호스트 이름에 nslookup 적용

```
# 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: 52.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 18.234.20.16
```

AMP 클라우드에 대한 연결 문제 DNS 확인 때문일 수 있습니다. DNS 설정을 확인하거나 FMC에서 nslookup을 수행합니다.

```
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
```

핑

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

추가 문제 해결 옵션

/ngfw/etc/sf/connector.properties에서 커넥터 속성을 **확인합니다**. 아래와 같이 올바른 커넥터 포트(8989)와 올바른 URL의 **connector_fqdn**을 출력해야 합니다.

```
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
```

자세한 내용은 Firepower 컨피그레이션 가이드를 참조하십시오.

알려진 문제

프록시로 인한 CSCvs05084 FTD Cisco Cloud Configuration Failure

CSCvp56922 update-context sse-connector API를 사용하여 디바이스 호스트 이름 및 버전 업데이트

CSCvu02123 문서 버그: CTR 컨피그레이션 가이드에서 Firepower 디바이스에서 SSE로 연결 가능한 URL 업데이트

CSCvr46845 ENH: 상태 메시지 'Cisco Cloud Configuration - Failure' 개선 필요

[비디오] Firepower - FMC를 SSE에 등록

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.