CTR과의 FMC 통합 문제 해결

목차

소개

이 문서에서는 CTR(Cisco Threat Response)과의 통합을 위해 FMC(Firepower Management Center) 또는 FTD(Firepower Threat Defense) 디바이스에서 SSE(Security Services Exchange) 커넥터 프로세스가 비활성화될 때 문제를 해결하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC
- FTD
- CTR 통합

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.4.0 이상의 FMC
- 소프트웨어 버전 6.4.0 이상의 FTD
- Cisco Security Services Exchange

- CTR 계정

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

배경 정보

SSEC커넥터

SSEConnector는 SSE 포털에 디바이스를 등록하6.4.0 Firepower 디바이스의 프로세스입니다.Cisco 클라우드 컨피그레이션이 On 또는 Off로 설정된 경우 FMC는 모든 관리되는 FTD에 브로드캐스트합니다.Cisco Cloud가 활성화되면 SSEConnector 서비스는 SSE 포털과 Firepower 디바이스 간의 통신을 시작합니다.각 FTD는 SSE 포털에 디바이스를 통합할 수 있는 등록 토큰을 FMC에 요청합니다.이 통합 후에는 디바이스에서 SSE 컨텍스트가 활성화되고 EventHandler가 Cisco 클라우드에 침입 이벤트를 전송하도록 재구성됩니다.

CTR

Threat Response는 여러 Cisco Security 제품 간의 통합을 지원하고 자동화하는 위협 인시던트 대응 오케스트레이션 허브입니다.Threat Response는 다음과 같은 주요 보안 작업을 가속화합니다.탐지, 조사, 교정이 Cisco의 통합 보안 아키텍처의 핵심입니다.

Threat Response의 목표는 네트워크 운영 팀과 사고 대응자가 Cisco와 타사에서 수집 및 사용할 수 있는 모든 위협 인텔리전스를 통해 네트워크의 위협을 이해할 수 있도록 지원하는 것입니다.

하지만 무엇보다 Threat Response는 보안 툴의 복잡성을 줄이고 위협을 식별하고 사고 대응을 가속화하기 위해 설계되었습니다.

Threat Response는 통합 플랫폼(https://visibility.amp.cisco.com/)입니다. 이 시스템은 "모듈"을 통해 작동하며, 이는 서로 다른 통합 시스템(예: Threat Grid 또는 AMP)과의 통신을 처리하는 독립적인 코드 부분입니다. 이러한 모듈은 통합 시스템에서 제공할 수 있는 세 가지 기능(보완, 로컬 컨텍스트 및 응답)을 모두 처리합니다.

CTR은 어떤 용도로 사용할 수 있습니까?

- 사고 대응
- 조사
- 위협 추적
- 인시던트 관리

관찰 가능한 모듈을 검색할 때 구성된 모든 모듈은 해당 관찰 가능한 모든 레코드를 검색할 책임이 있는 시스템에 대해 묻습니다.그런 다음 제공된 응답을 가져와 Threat Response로 다시 전달한 다음 모든 모듈(이 경우 Stealthwatch 모듈)에서 수집된 결과를 가져와 데이터를 정렬하고 구성하고 그래프로 표시합니다.

CTR을 다른 제품과 통합하려면 두 개의 포털 "https://castle.amp.cisco.com/"(Castle) 및 "https://admin.sse.itd.cisco.com/app/devices"(Security Services Exchange)가 더 필요합니다.

성 포털

여기에서 Cisco 보안 어카운트를 관리할 수 있습니다.

Cisco 보안 어카운트를 사용하면 Cisco 보안 포트폴리오 내에서 여러 애플리케이션을 관리할 수 있습니다.라이센스 자격에 따라 다음과 같은 항목이 포함될 수 있습니다.

- AMP for Endpoints
- 위협 그리드
- 위협 대응

보안 서비스 교환 포털

이 포털은 CTR 포털의 확장으로, CTR 포털에 등록된 디바이스를 관리할 수 있으므로 제품을 통합하는 데 필요한 토큰을 생성할 수 있습니다.

Security Services Exchange는 다음과 같은 제품 및 기능을 포함하여 특정 Cisco 보안 제품을 Cisco Threat Response와 통합할 때 장치, 서비스 및 이벤트 관리를 제공합니다.

- Cisco Threat Response와 통합된 Security Management Appliance 목록을 관리합니다.
- 통합 Cisco Firepower 디바이스에서 이벤트 데이터를 수집하여(자동 또는 수동으로) Cisco Threat Response로 전달합니다.

문제 해결

클라우드 서비스가 활성화되었는지 확인

먼저 FMC에서 **System > Licenses > Smart Licenses**에서 평가 모드가 아닌지 확인합니다.

지금 Smart Software Satellite 탭의 **System > Integration에서** 선택한 옵션이 **Cisco Smart Software Manager에 직접** 연결되는지 확인합니다. 이 기능은 Air-Gapped 환경에서 지원되지 않습니다.

Cloud Services(**클라우드 서비스**) 탭에서 System(**시스템**) > **Integration(통합)**으로 이동하고 **Cisco Cloud Event Configuration(Cisco 클라우드 이벤트 컨피그레이션)** 옵션이 켜져 있는지 확인합니다.

FMC/FTD와 SSE 포털 간의 연결 확인

IP가 변경될 수 있으므로 다음 URL을 허용해야 합니다.

미국 지역

- api-sse.cisco.com
- est.sco.cisco.com(지역 간 공통)
- mx*.sse.itd.cisco.com(현재 mx01.sse.itd.cisco.com만 해당)
- dex.sse.itd.cisco.com(고객 성공)
- eventing-ingest.sse.itd.cisco.com(CTR 및 CDO용)

EU 지역

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com(지역 간 공통)
- mx*.eu.sse.itd.cisco.com(현재 mx01.eu.sse.itd.cisco.com만 해당)

- dex.eu.sse.itd.cisco.com(고객 성공)
- eventing-ingest.eu.sse.itd.cisco.com(CTR 및 CDO용)

APJ 지역

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com(지역 간 공통)
- mx*.apj.sse.itd.cisco.com(현재 mx01.apj.sse.itd.cisco.com만 해당)
- dex.apj.sse.itd.cisco.com(고객 성공 기준)
- eventing-ingest.apj.sse.itd.cisco.com(CTR 및 CDO용)

FMC와 FTD 모두 관리 인터페이스의 SSE URL에 연결해야 하며, 연결을 테스트하려면 루트 액세스 권한이 있는 Firepower CLI에 다음 명령을 입력합니다.

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

각 명령을 실행한 후에는 연결 끝 부분, 즉 **호스트 "URL"**에 대한 **연결 #0이 그대로 유지된 상태로** 이 줄**을** 표시해야 합니다.

연결이 시간 초과되거나 출력에 이 회선을 수신하지 못하는 경우 관리 인터페이스가 이러한 URL에 액세스할 수 있는지, 디바이스와 이러한 URL 간의 연결을 차단하거나 수정하는 업스트림 디바이스가 없는지 확인하십시오.

다음 명령을 사용하여 인증서 검사를 우회할 수 있습니다.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) 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, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* 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 S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (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, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

참고:403 Forbidden 메시지는 테스트를 통해 전송된 매개변수가 SSE에서 기대하는 것이 아니지만 이를 통해 연결을 검증할 수 있습니다.

SSEConnector 상태 확인

아래와 같이 커넥터 속성을 확인할 수 있습니다.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

SSConnector와 EventHandler 간의 연결을 확인하기 위해 이 명령을 사용할 수 있습니다. 이는 잘못된 연결의 예입니다.

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

설정된 연결의 예에서는 스트림 상태가 연결되어 있음을 확인할 수 있습니다.

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

SSE 포털 및 CTR로 전송된 데이터 확인

FTD 디바이스에서 TCP 연결을 확인하기 위해 이벤트를 전송하려면 https://eventing-ingest.sse.itd.cisco.com을 사용하여 설정해야 합니다. 이것은 SSE 포털과 FTD 간에 설정되지 않은 연결의 예입니다.

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

connector.log 로그에서 다음을 수행합니다.

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **참고:**표시된 IP 주소가 18.205.49.246 및 18.205.49.246에 속할 수 있습니다. 따라서 IP 주소 대신 URL을 기반으로 SSE 포털에 대한 트래픽을 허용하는 것이 좋습니다.

이 연결이 설정되지 않으면 이벤트가 SSE 포털로 전송되지 않습니다. 이것은 FTD와 SSE 포털 간에 설정된 연결의 예입니다.

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

일반적인 문제

6.4로 업그레이드한 후 SSE 커넥터는 SSE 포털과 통신하지 않습니다.Connector.log가 이벤트와 유사한 오류를 제공합니다. (*Service).Start] ZeroMQ PUSH 끝점에 연결할 수 없습니다 .\"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\"(으)로 전화를 걸 수 없습니다.unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock을 사용하여연결:해당 파일이나 디렉토리가 없습니다.\n"

SSEConnector 서비스를 다시 시작합니다.

1) sudo pmtool disablebyid SSEConnector

2) sudo pmtool enablebyid SSEConnector

3) 디바이스를 재시작합니다.다시 시작하면 디바이스가 클라우드에 통신합니다.

중요 로그 파일 위치

디버그 로그 - 성공한 연결 또는 실패 메시지를 표시합니다.

```
/ngfw/var/log/connector/connector.log
```

구성 설정

```
/ngfw/etc/sf/connector.properties
```

구성 설정

```
curl localhost:8989/v1/contexts/default
```

관련 정보

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- 기술 지원 및 문서 – Cisco Systems