Fehlerbehebung bei der FMC-Integration mit CTR

Inhalt

Einführung

In diesem Dokument werden die Schritte zur Fehlerbehebung für den Security Services Exchange (SSE) Connector-Prozess beschrieben, wenn dieser auf dem FirePOWER Management Center (FMC)- oder FirePOWER Threat Defense (FTD)-Geräten für die Integration mit Cisco Threat Response (CTR) deaktiviert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FMC
- FTD
- CTR-Integration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FMC auf Software Version 6.4.0 oder höher
- FTD auf Software ab Version 6.4.0
- Cisco Security Services Exchange
- CTR-Konto

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

SSEConnector

SSEConnector ist ein Prozess auf den FirePOWER-Geräten nach 6.4.0, der die Geräte in das SSE-Portal einträgt. Das FMC sendet an alle verwalteten FTDs, wenn die Cisco Cloud-Konfiguration auf Ein oder Aus eingestellt ist. Sobald die Cisco Cloud aktiviert ist, beginnt der SSEConnector-Dienst die Kommunikation zwischen dem SSE-Portal und den FirePOWER-Geräten. Jede FTD fordert das FMC auf, ein Registrierungstoken zu verwenden, das die Integration der Geräte in das SSE-Portal ermöglicht. Nach dieser Integration wird der SSE-Kontext auf den Geräten aktiviert, und der EventHandler wird neu konfiguriert, um Intrusion Events an die Cisco Cloud zu senden.

CTR

Threat Response ist ein Orchestrierungs-Hub für die Reaktion auf Bedrohungen, der Integrationen über mehrere Cisco Security-Produkte hinweg unterstützt und automatisiert. Die Reaktion auf Bedrohungen beschleunigt wichtige Sicherheitsaufgaben: Erkennung, Untersuchung und Beseitigung von Bedrohungen und ist ein Eckpfeiler unserer integrierten Sicherheitsarchitektur.

Ziel von Threat Response ist es, Netzwerkbetriebsteams und Incident Response-Teams dabei zu unterstützen, Bedrohungen im Netzwerk mithilfe der gesammelten und kombinierten Threat-Intelligence von Cisco und Drittanbietern zu verstehen.

Die Threat Response ist jedoch mehr als alles andere darauf ausgelegt, die Komplexität von Sicherheitstools zu reduzieren, Bedrohungen zu identifizieren und die Reaktion auf Vorfälle zu beschleunigen.

Threat Response ist eine Integrationsplattform (https://visibility.amp.cisco.com/). Das System arbeitet mit "Modulen", bei denen es sich um unabhängige Codeelemente handelt, die die Kommunikation mit verschiedenen integrierten Systemen (z. B. Threat Grid oder AMP) behandeln. Diese Module behandeln alle drei Funktionen, die ein integriertes System bieten kann (Anreicherung, lokaler Kontext und Reaktion).

Wofür kann CTR verwendet werden?

- Reaktion auf Vorfälle
- Untersuchungen
- Nachverfolgung von Bedrohungen
- Incident-Management

Wenn Sie nach einem beobachtbaren Gerät suchen, fragen alle von Ihnen konfigurierten Module

die Systeme, für die sie verantwortlich sind, nach einem Datensatz dieser Beobachtungsdaten zu suchen. Anschließend senden sie die bereitgestellten Antworten an Threat Response. Anschließend werden die gesammelten Ergebnisse aus allen Modulen (in diesem Fall das Stealthwatch-Modul) erfasst und sortiert und in einem Diagramm angezeigt.

Zur Integration von CTR in verschiedene Produkte sind zwei weitere Portale beteiligt: "https://castle.amp.cisco.com/" (Castle) und "https://admin.sse.itd.cisco.com/app/devices" (Security Services Exchange)

Schloss Portal

Hier können Sie die Cisco Sicherheitskonten verwalten:

Mit einem Cisco Security-Konto können Sie mehrere Anwendungen innerhalb des Cisco Security-Portfolios verwalten. Entsprechend Ihren Lizenzierungsansprüchen können Sie Folgendes tun:

- AMP für Endgeräte
- Threat Grid
- Reaktion auf Bedrohungen

Exchange-Portal für Sicherheitsdienste

Dieses Portal ist eine Erweiterung des CTR-Portals, in dem Sie die im CTR-Portal registrierten Geräte verwalten können. Hier können Sie die Token erstellen, die für die Integration der Produkte erforderlich sind.

Security Services Exchange bietet Geräte-, Service- und Ereignismanagement, wenn Sie bestimmte Cisco Security-Produkte in Cisco Threat Response integrieren, einschließlich der folgenden Produkte und Funktionen:

- Verwalten Sie die Liste der Security Management Appliances, die in Cisco Threat Response integriert werden.
- Sammeln Sie Ereignisdaten von integrierten Cisco FirePOWER-Geräten, um diese (automatisch oder manuell) an Cisco Threat Response weiterzuleiten.

Fehlerbehebung

Überprüfen der Aktivierung von Cloud-Services

Prüfen Sie im FMC zunächst **System > Licenses > Smart Licenses (System> Licenses> Smart Licenses (SmartLicenses)**, wenn Sie sich nicht im Evaluierungsmodus befinden.

Überprüfen Sie jetzt unter **System > Integration** auf der Registerkarte **Smart Software Satellite**, dass die ausgewählte Option **direkt mit Cisco Smart Software Manager verbunden** ist, da diese Funktion in einer Air-Gap-Umgebung nicht unterstützt wird.

Navigieren Sie auf der Registerkarte **Cloud-Services** zu **System > Integration**, und überprüfen Sie, ob die **Cisco Cloud Event Configuration** (Konfiguration von Cisco Cloud-Ereignissen) aktiviert ist.

Überprüfung der Verbindung zwischen FMC/FTD und SSE-Portal

Diese nächsten URLs müssen zulässig sein, da sich IPs ändern können:

Region USA

- api-sse.cisco.com
- est.sco.cisco.com (länderübergreifend)
- mx*.sse.itd.cisco.com (derzeit nur mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (für den Erfolg von Kunden)
- eventing-ingest.sse.itd.cisco.com (für CTR und CDO)

Region EU

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (länderübergreifend)
- mx*.eu.sse.itd.cisco.com (derzeit nur mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (für den Erfolg von Kunden)
- eventing-ingest.eu.sse.itd.cisco.com (für CTR und CDO)

Region APJ

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (länderübergreifend)
- mx*.apj.sse.itd.cisco.com (derzeit nur mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (für den Erfolg des Kunden)
- eventing-ingest.apj.sse.itd.cisco.com (für CTR und CDO)

Sowohl FMC als auch FTD benötigen eine Verbindung zu den SSE-URLs ihrer Management-Schnittstelle. Um die Verbindung zu testen, geben Sie diese Befehle in der FirePOWER-CLI mit Root-Zugriff ein:

```
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
```

Nachdem jeder Befehl ausgeführt wurde, muss diese Zeile am Ende der Verbindung angezeigt werden: **Verbindung Nr. 0 zum Hosten von "URL" intakt**.

Wenn die Verbindung abgelaufen ist oder Sie diese Leitung nicht in der Ausgabe erhalten, überprüfen Sie bitte, ob den Verwaltungsschnittstellen der Zugriff auf diese URLs gestattet ist und dass es keine Upstream-Geräte gibt, die die Verbindung zwischen den Geräten und diesen URLs blockieren oder ändern.

Die Zertifikatsüberprüfung kann mit dem folgenden Befehl umgangen werden:

```
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;
```

> **Hinweis:** Sie erhalten die 403 Forbidden-Meldung, da die vom Test gesendeten Parameter nicht den Erwartungen von SSE entsprechen, aber dies erweist sich als ausreichend, um die Verbindung zu validieren.

Überprüfung des Status von SSEConnector

Sie können die Anschlusseigenschaften wie unten beschrieben überprüfen.

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

Mit diesem Befehl können Sie die Verbindung zwischen dem SSConnector und dem EventHandler überprüfen. Dies ist ein Beispiel für eine fehlerhafte Verbindung:

```
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
```

Im Beispiel einer eingerichteten Verbindung sehen Sie, dass der Streamstatus verbunden ist:

```
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
```

Überprüfung der an das SSE-Portal und CTR gesendeten Daten

Um Ereignisse vom FTD-Gerät an SEE senden zu können, muss eine TCP-Verbindung mit https://eventing-ingest.sse.itd.cisco.com eingerichtet werden. Dies ist ein Beispiel für eine Verbindung, die nicht zwischen dem SSE-Portal und dem FTD hergestellt wurde:

```
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)
```

In den Connector.log-Protokollen:

```
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"
```

> **Hinweis:** Beachten Sie, dass die angezeigten IP-Adressen 18.205.49.246 und 18.205.49.246 zu https://eventing-ingest.sse.itd.cisco.com gehören können, deshalb wird empfohlen, den Datenverkehr zum SSE-Portal auf URL anstatt auf IP-Adressen zuzulassen.

Wenn diese Verbindung nicht hergestellt wird, werden die Ereignisse nicht an das SSE-Portal gesendet. Dies ist ein Beispiel für eine bestehende Verbindung zwischen dem FTD und dem SSE-Portal:

```
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)
```

Häufige Probleme

Nach dem Upgrade auf 6.4 kommuniziert der SSE-Connector nicht mehr mit dem SSE-Portal.

Connector.log stellt Fehler bereit, die Ereignissen ähneln:(*Service).Start] Konnte keine Verbindung zum ZeroMQ-PUSH-Endpunkt herstellen: konnte nicht zu \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\" gewählt werden: dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: verbinden: keine solche Datei oder kein Verzeichnis\n"

Starten Sie den SSEConnector-Dienst neu:

1) sudo pmtool disabyid SSEConnector

2) sudo pmtool enable yid SSEConnector

3) Starten Sie das Gerät neu. Beim Neustart kommuniziert das Gerät mit der Cloud.

Wichtige Speicherorte für Protokolldateien

Debug-Protokolle - Zeigt erfolgreiche Verbindungs- oder Fehlermeldungen an

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

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

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

Zugehörige Informationen

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Technischer Support und Dokumentation für Cisco Systeme