Dépanner l'intégration FMC avec CTR

Contenu

Introduction

Ce document décrit les étapes à suivre pour dépanner le processus du connecteur SSE (Security Services Exchange) lorsqu'il devient désactivé sur les périphériques FMC (Firepower Management Center) ou FTD (Firepower Threat Defense) pour l'intégration avec Cisco Threat Response (CTR).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FMC
- FTD
- Intégration CTR

Components Used

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

- FMC sur la version logicielle 6.4.0 ou ultérieure

- FTD sur la version logicielle 6.4.0 ou ultérieure
- Cisco Security Services Exchange
- Compte CTR

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

SSEConnector

SSEConnector est un processus sur les périphériques Firepower après 6.4.0 qui inscrit les périphériques dans le portail SSE. Le FMC diffuse sur tous les FTD gérés lorsque la configuration du cloud Cisco est activée ou désactivée. Une fois le cloud Cisco activé, le service SSEConnector démarre la communication entre le portail SSE et les périphériques Firepower. Chaque FTD demande au FMC un jeton d'enregistrement permettant l'intégration des périphériques dans le portail SSE. Après cette intégration, le contexte SSE est activé sur les périphériques et EventHandler est reconfiguré pour envoyer des événements d'intrusion au cloud Cisco.

CTR

Threat Response est un concentrateur d'orchestration de la réponse aux incidents, qui prend en charge et automatise les intégrations sur plusieurs produits de sécurité Cisco. La réponse aux menaces accélère les principales tâches de sécurité : la détection, l'investigation et la correction, et constitue une pierre angulaire de notre architecture de sécurité intégrée.

L'objectif de Threat Response est d'aider les équipes chargées des opérations réseau et les intervenants en cas d'incident à comprendre les menaces sur leur réseau grâce à l'ensemble des informations collectées et combinées disponibles auprès de Cisco et de tiers.

Mais avant tout, Threat Response est conçu pour réduire la complexité des outils de sécurité, aider à identifier les menaces et accélérer la réponse aux incidents.

Threat Response est une plate-forme d'intégration (https://visibility.amp.cisco.com/). Le système fonctionne via " " de modules, qui sont des éléments de code indépendants qui gèrent les communications avec différents systèmes intégrés (par exemple Threat Grid ou AMP). Ces modules gèrent les 3 fonctions qu'un système intégré peut fournir (enrichissement, contexte local et réponse).

Àquoi peut servir CTR ?

- Réponse aux incidents
- Enquêtes
- Recherche de menaces
- Gestion des incidents

Lorsque vous recherchez un observable, tous vos modules configurés demandent aux systèmes pour lesquels ils sont responsables de rechercher n'importe quel enregistrement de ces observables. Ils prennent ensuite les réponses fournies et les redirigent vers Threat Response, puis ils prennent les résultats collectés de tous les modules (dans ce cas le module Stealthwatch), et trient et organisent les données et les affichent dans un graphique.

Pour intégrer CTR à différents produits sont impliqués deux portails supplémentaires “ https://castle.amp.cisco.com/ ” (Castle) et “ https://admin.sse.itd.cisco.com/app/devices ” (Security Services Exchange)

Portail du château

Vous pouvez ici gérer les comptes de sécurité Cisco :

Un compte de sécurité Cisco vous permet de gérer plusieurs applications au sein du portefeuille de sécurité Cisco. En fonction de vos droits de licence, ceci peut inclure :

- AMP pour les points terminaux
- Grille contre les menaces (Threat Grid)
- Réponse aux menaces

Portail Exchange des services de sécurité

Ce portail est une extension du portail CTR, où vous pouvez gérer les périphériques qui ont été enregistrés dans le portail CTR, de sorte que vous pouvez ici créer les jetons nécessaires à l'intégration des produits.

Security Services Exchange fournit une gestion des périphériques, des services et des événements lorsque vous intégrez certains produits de sécurité Cisco à Cisco Threat Response, notamment les produits et fonctionnalités suivants :

- Gérez la liste des appliances de gestion de la sécurité qui s'intègrent à Cisco Threat Response.
- Collecter les données d'événements des périphériques Cisco Firepower intégrés, en vue de les transmettre (automatiquement ou manuellement) à Cisco Threat Response.

Dépannage

Vérifier que les services cloud sont activés

Sur FMC, vérifiez d'abord sur **System > Licenses > Smart Licenses** que vous n'êtes pas en mode évaluation.

Vérifiez maintenant, sous **System > Integration** sur l'onglet **Smart Software Satellite**, que l'option sélectionnée est **Connexion directe à Cisco Smart Software Manager**, car cette fonctionnalité n'est pas prise en charge dans un environnement à aplatissement.

Accédez à **System > Integration** sous l'onglet **Cloud Services** et vérifiez que l'option **Cisco Cloud Event Configuration** est activée.

Vérifier la connectivité entre FMC/FTD et SSE Portal

Les URL suivantes doivent être autorisées car les adresses IP peuvent changer :

Région des États-Unis

- api-sse.cisco.com
- est.sco.cisco.com (commun à toutes les régions)
- mx*.sse.itd.cisco.com (actuellement uniquement mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (pour la réussite du client)
- eventing-ingest.sse.itd.cisco.com (pour CTR et CDO)

Région UE

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (commun à toutes les régions)
- mx*.eu.sse.itd.cisco.com (actuellement uniquement mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (pour la réussite du client)
- eventing-ingest.eu.sse.itd.cisco.com (pour CTR et CDO)

Région APJ

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (commun à toutes les régions)
- mx*.apj.sse.itd.cisco.com (actuellement uniquement mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (pour la réussite du client)
- eventing-ingest.apj.sse.itd.cisco.com (pour CTR et CDO)

FMC et FTD ont tous deux besoin d'une connexion aux URL SSE sur leur interface de gestion, pour tester la connexion, entrez ces commandes sur l'interface de ligne de commande Firepower avec accès racine :

```
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
```

Une fois chaque commande exécutée, vous devez voir cette ligne autour de la fin de la connexion : **Connection #0 to host « URL » laissé intact**.

Si la connexion expire ou si vous ne recevez pas cette ligne sur le résultat, vérifiez que les interfaces de gestion sont autorisées à accéder à ces URL et qu'il n'y a aucun périphérique en amont qui bloque ou modifie la connexion entre les périphériques et ces URL.

La vérification du certificat peut être ignorée avec cette commande :

```
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;
```

> **Note**: Vous recevez le message 403 Interdit, car les paramètres envoyés à partir du test ne correspondent pas aux attentes de SSE, mais cela se révèle suffisant pour valider la connectivité.

Vérifier l'état de SSEConnector

Vous pouvez vérifier les propriétés du connecteur comme ci-dessous.

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

Afin de vérifier la connectivité entre SSConnector et EventHandler, vous pouvez utiliser cette commande, voici un exemple de mauvaise connexion :

```
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
```

Dans l'exemple d'une connexion établie, vous pouvez voir que l'état du flux est connecté :

```
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
```

Vérifier les données envoyées au portail SSE et au CTR

Pour envoyer des événements du périphérique FTD à SEE, une connexion TCP doit être établie avec https://eventing-ingest.sse.itd.cisco.com Voici un exemple de connexion non établie entre le portail SSE et le FTD :

```
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)
```

Dans les journaux connector.log :

```
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"
```

> **Note**: Notez que les adresses IP affichées 18.205.49.246 et 18.205.49.246 appartiennent à https://eventing-ingest.sse.itd.cisco.com peut changer, c'est pourquoi la recommandation est d'autoriser le trafic vers SSE Portal en fonction de l'URL au lieu des adresses IP.

Si cette connexion n'est pas établie, les événements ne sont pas envoyés au portail SSE, ceci est un exemple de connexion établie entre le FTD et le portail SSE :

```
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)
```

Problèmes courants

Après la mise à niveau vers la version 6.4, le connecteur SSE ne communique pas avec le portail SSE. Connector.log fournit des erreurs similaires aux événements : (*Service).Start] Impossible de se connecter au point de terminaison ZeroMQ PUSH : impossible de composer le numéro \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\" : composer unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock : connexion : aucun fichier ou répertoire de ce type\n »

Redémarrez le service SSEConnector :

1) sudo pmtool disablebyid SSEConnector

2) sudo pmtool enablebyid SSEConnector

3) Redémarrez le périphérique. Au redémarrage, le périphérique communique avec le cloud.

Emplacements importants des fichiers journaux

Journaux de débogage - Affiche les messages de connexion ou d'échec réussis

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

Paramètres de configuration

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

Paramètres de configuration

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

Informations connexes

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Support et documentation techniques - Cisco Systems