Dépannage de l'intégration de Secure Firewall avec Security Services Exchange

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Dépannage
  - Connectivité
  - Inscription
    - Vérification de l'enregistrement
    - Vérification du côté de Security Services Exchange
  - Événements
  - Dépanner les événements non traités dans Security Services Exchange

Introduction

Ce document décrit comment dépanner l'intégration de Cisco Secure Firewall avec Security Services Exchange (SSX).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Centre de gestion du pare-feu sécurisé (FMC)
- Pare-feu sécurisé Cisco

Composants utilisés

- Cisco Secure Firewall - 7.6.0
- Centre de gestion du pare-feu sécurisé (FMC) - 7.6.0
- Services de sécurité eXchange (SSX)

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.

Dépannage

Connectivité

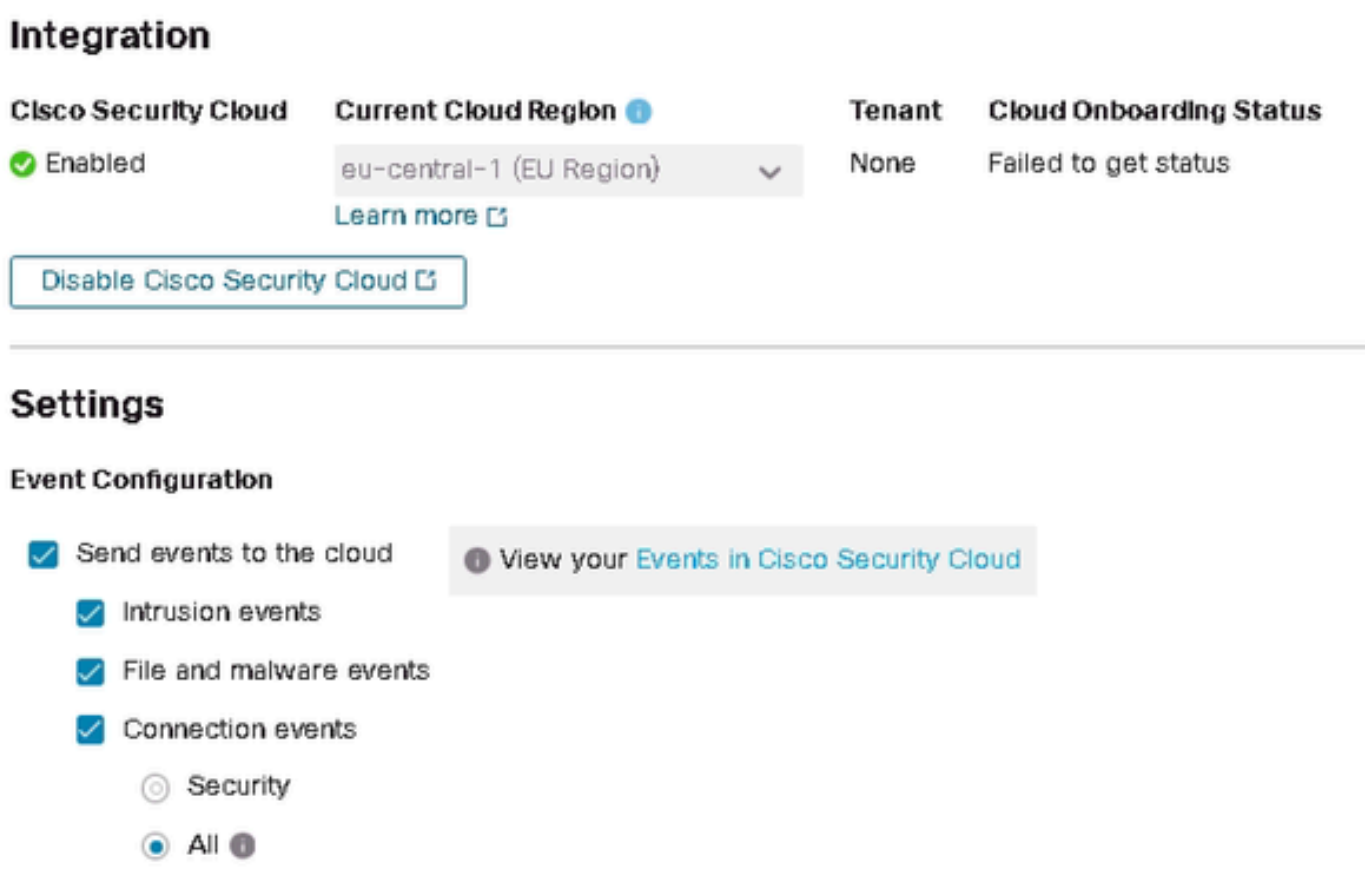
La principale condition est d'autoriser le trafic HTTPS vers ces adresses à partir du périphérique d'enregistrement :

- Région US :
  - api-sse.cisco.com
  - mx*.sse.itd.cisco.com
  - dex.sse.itd.cisco.com
  - eventing-ingest.sse.itd.cisco.com
  - registration.us.sse.itd.cisco.com
  - defenseorchestrator.com
  - edge.us.cdo.cisco.com
- Région de l'UE :
  - api.eu.sse.itd.cisco.com
  - mx*.eu.sse.itd.cisco.com
  - dex.eu.sse.itd.cisco.com
  - eventing-ingest.eu.sse.itd.cisco.com
  - registration.eu.sse.itd.cisco.com
  - defenseorchestrator.eu
  - edge.eu.cdo.cisco.com
- Région Asie (APJC) :
  - api.apj.sse.itd.cisco.com
  - mx*.apj.sse.itd.cisco.com
  - dex.apj.sse.itd.cisco.com
  - eventing-ingest.apj.sse.itd.cisco.com
  - registration.apj.sse.itd.cisco.com
  - apj.cdo.cisco.com
  - edge.apj.cdo.cisco.com

- Région Australie :
  - api.aus.sse.itd.cisco.com
  - mx*.aus.sse.itd.cisco.com
  - dex.au.sse.itd.cisco.com
  - eventing-ingest.aus.sse.itd.cisco.com
  - registration.au.sse.itd.cisco.com
  - aus.cdo.cisco.com
- Région Inde :
  - api.in.sse.itd.cisco.com
  - mx*.in.sse.itd.cisco.com
  - dex.in.sse.itd.cisco.com
  - eventing-ingest.in.sse.itd.cisco.com
  - registration.in.sse.itd.cisco.com
  - in.cdo.cisco.com

Inscription

L'enregistrement de Secure Firewall à Security Services Exchange s'effectue dans Secure Firewall Management Center, dans Integration > Cisco Security Cloud.



Ces résultats indiquent que la connexion au cloud Cisco a été établie.

<#root>

```
root@firepower:~#
netstat -anlp | grep EventHandler_SSEConnector.sock

unix 3 [ ] STREAM CONNECTED 133064 4159/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

<#root>

```
root@firepower:~#
lsof -i | grep conn

connector 5301 www 6u IPv4 471679686 0t0 TCP firepower:53080->ec2-35-158-61-95.eu-central-1.compute.amaz
connector 5301 www 8u IPv6 104710 0t0 TCP *:8989 (LISTEN)
```

Les journaux d'enregistrement sont stockés dans /var/log/connector/.

Vérification de l'enregistrement

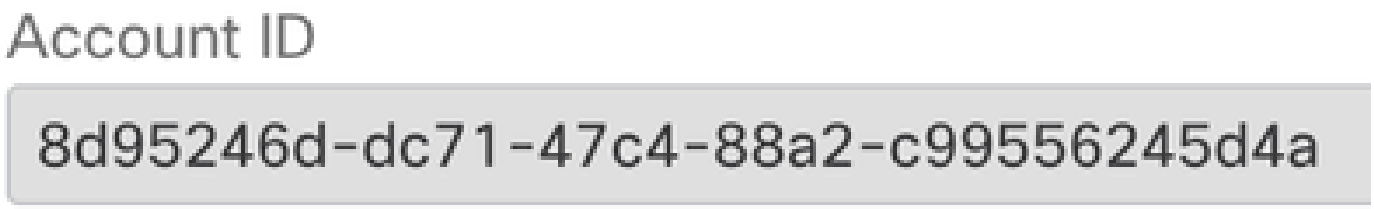
Une fois l'enregistrement réussi du côté du pare-feu sécurisé, un appel d'API à localhost : 8989/v1/contextes/default/tenant peut être effectué pour obtenir le nom et l'ID du locataire Security Services Exchange.

<#root>

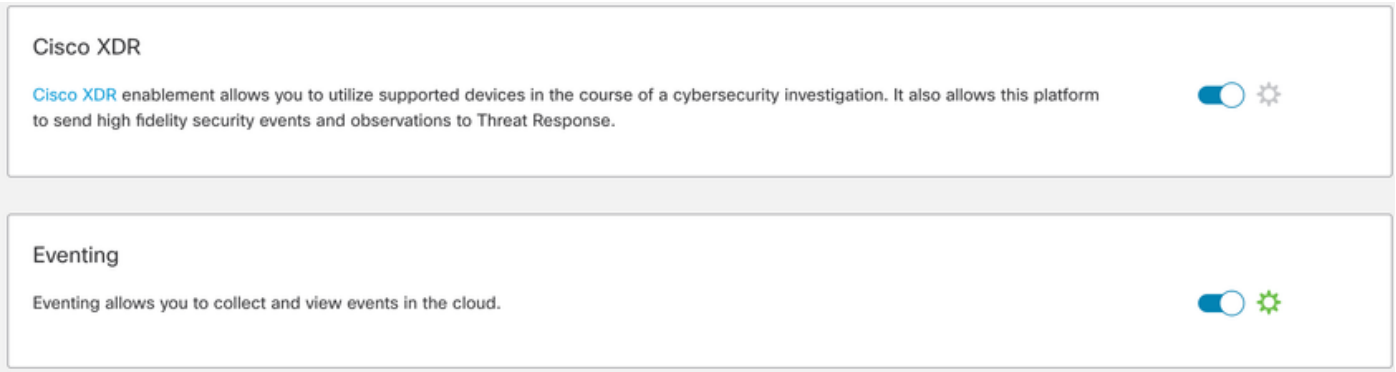
```
root@firepower:~#
curl localhost:8989/v1/contexts/default/tenant

{"registeredTenantInfo":{"companyId":"601143","companyName":"lab","domainName":"tac.cisco.com","id":"56
"Cisco - lab"
,"id":
"8d95246d-dc71-47c4-88a2-c99556245d4a"
,"spId":"AMP-EU"}]}
```

Vérification du côté de Security Services Exchange

Dans Security Services Exchange, accédez au nom d'utilisateur dans le coin supérieur droit et cliquez sur User Profile (Profil utilisateur) pour confirmer que l'ID de compte correspond à l'ID de locataire obtenu précédemment dans Secure Firewall.



Dans l'onglet Cloud Services, vous devez activer l'option Event. En outre, le commutateur Cisco XDR doit être activé en cas d'utilisation de cette solution.



L'onglet Devices contient la liste des appliances enregistrées.

Une entrée pour chaque périphérique est extensible et contient les informations suivantes :

- ID de périphérique - dans le cas du pare-feu sécurisé, cet ID peut être trouvé en interrogeant curl -s http://localhost:8989/v1/contexts/default | grep deviceId
- Date d'enregistrement
- Adresse IP
- Version du connecteur SSX
- Dernière modification

Événements

L'onglet Événements nous permet d'effectuer les actions sur les données qui ont été envoyées par Secure Firewall et qui sont traitées et affichées dans Security Services Exchange.

1. Filtrer la liste des événements et créer et enregistrer des filtres,
2. Afficher ou masquer les colonnes supplémentaires du tableau,
3. Examinez les événements envoyés par les périphériques Secure Firewall.

Dans l'intégration entre Secure Firewall et Security Services Exchange, ces types d'événements sont pris en charge :

Type d'événement	Version du périphérique de défense contre les menaces pris en charge pour une intégration directe	Version du périphérique Threat Defense pris en charge pour l'intégration Syslog
Événements d'intrusion	6.4 et versions ultérieures	6.3 et versions ultérieures
Événements de connexion de priorité élevée : • Événements de connexion liés à la sécurité. • Événements de connexion liés aux fichiers et aux programmes malveillants. • Événements de connexion liés aux événements d'intrusion.	6.5 et versions ultérieures	Non pris en charge
Événements liés aux fichiers et aux programmes malveillants	6.5 et versions ultérieures	Non pris en charge

Dépanner les événements non traités dans Security Services Exchange

Dans le cas de l'observation d'événements spécifiques dans le Centre de gestion du pare-feu sécurisé, il peut être nécessaire de déterminer si les événements correspondent aux conditions (celles liées aux événements d'intrusion, de fichier/programme malveillant et de connexion) à traiter et à afficher dans l'échange de services de sécurité.

Confirmation que des événements sont envoyés au cloud en interrogeant localhost : 8989/v1/contextes/default il est possible de déterminer si des événements sont envoyés au cloud.

<#root>

```
root@firepower:~#

curl localhost:8989/v1/contexts/default



...

"statistics": {
 "client": [
  {
   "type": "Events",
   "statistics": {
   "ZmqStat": {
   "LastCloudConnectSuccess": "2025-01-21T10:03:13.779677978Z",
   "LastCloudConnectFailure": "2025-01-20T10:54:43.552112185Z",
   "LastCloudDisconnect": "2025-01-20T11:35:44.606352271Z",

   "TotalEventsReceived": 11464,



   "TotalEventsSent": 11463

...
```

Le nombre d'événements reçus dans TotalEventsReceived signifie les événements applicables pour l'envoi à l'échange de services de sécurité traités par Secure Firewall.

Le nombre d'événements envoyés dans TotalEventsSent signifie des événements envoyés au cloud Cisco.

Si des événements sont détectés dans le Centre de gestion du pare-feu sécurisé, mais pas dans l'échange de services de sécurité, les journaux d'événements disponibles dans /ngfw/var/sf/detection_engine/<engine>/ doivent être vérifiés.

Sur la base d'un horodatage, décodez un journal d'événements spécifique en utilisant u2dump :

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
```

```
u2dump unified_events-1.log.1736964974 > ../fulldump.txt
```

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-1#
```

```
cd ../instance-2
```

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
```

```
ls -alh | grep unified_events-1.log.1736
```

```
-rw-r--r-- 1 root root 8.3K Jan 5 08:19 unified_events-1.log.1736064964
-rw-r--r-- 1 root root 5.0K Jan 7 23:23 unified_events-1.log.1736292107
-rw-r--r-- 1 root root 16K Jan 10 03:17 unified_events-1.log.1736393796
-rw-r--r-- 1 root root 4.7K Jan 12 16:02 unified_events-1.log.1736630477
-rw-r--r-- 1 root root 4.8K Jan 13 11:10 unified_events-1.log.1736766628
-rw-r--r-- 1 root root 5.5K Jan 14 22:41 unified_events-1.log.1736865732
-rw-r--r-- 1 root root 5.5K Jan 15 18:27 unified_events-1.log.1736964964
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081/instance-2#
```

```
u2dump unified_events-1.log.1736964964 >> ../fulldump.txt
```

- Événements d'intrusion

Tous les événements d'intrusion sont traités et affichés dans SSX et XDR. Assurez-vous que dans les journaux décodés, cet événement spécifique contient un indicateur :

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#
```

```
grep -i "ips event count: 1" fulldump.txt
```

```
IPS Event Count: 1
```

- Événements relatifs aux fichiers et aux programmes malveillants

En fonction des exigences de la plate-forme Security Services Exchange, seuls les événements avec un sous-type d'événement spécifique sont traités et affichés.

<#root>

```
"FileEvent":
 {
   “Subtypes”:
   {
     “FileLog”:
     {
     “Unified2ID”: 500,
     “SyslogID”: 430004
     },

     “FileMalware”:
```

```
    {
    “Unified2ID”: 502,

    “SyslogID”: 430005
    }
  }
}
```

Par conséquent, il ressemble à ce qui suit dans ces journaux décodés :

<#root>

```
root@firepower:/ngfw/var/sf/detection_engines/4ca2e696-0996-11ed-be66-77bcdf78a081#
cat fulldump.txt | grep -A 11 "Type: 502"


Type: 502(0x000001f6)


Timestamp: 0
Length: 502 bytes
Unified 2 file log event Unified2FileLogEvent
FilePolicy UUID: f19fb202-ac9e-11ef-b94a-c9dafad481cf
Sensor ID : 0
Connection Instance : 1
Connection Counter : 5930
Connection Time : 1736964963
File Event Timestamp : 1736964964
Initiator IP : 192.168.100.10
Responder IP : 198.51.100.10
```

- Événements de connexion

Concernant les événements de connexion, il n'existe aucun sous-type. Toutefois, si un événement de connexion comporte l'un de ces champs, il est considéré comme un événement de veille de sécurité et il est traité plus avant dans Security Services Exchange.

· URL_SI_Category

· Catégorie_SI_DNS

· IP_ReputationSI_Category

Remarque : Si des événements de fichiers/programmes malveillants ou de connexion sont détectés dans Secure Firewall Management Center, ne contiennent pas les sous-types ou paramètres mentionnés dans les journaux d'événements unifiés décodés avec u2dump, cela signifie que ces événements spécifiques ne sont pas traités et affichés dans Security

---

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.