Fehlerbehebung bei der Integration einer sicheren Firewall in Security Services Exchange

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Integration von Cisco Secure Firewall in Security Services Exchange (SSX) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Secure Firewall Management Center (FMC)
- Sichere Firewall von Cisco

Verwendete Komponenten

- Cisco Secure Firewall - 7.6.0
- Secure Firewall Management Center (FMC) - 7.6.0
- Security Services eXchange (SSX)

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 möglichen Auswirkungen aller Befehle kennen.

Fehlerbehebung

Konnektivität

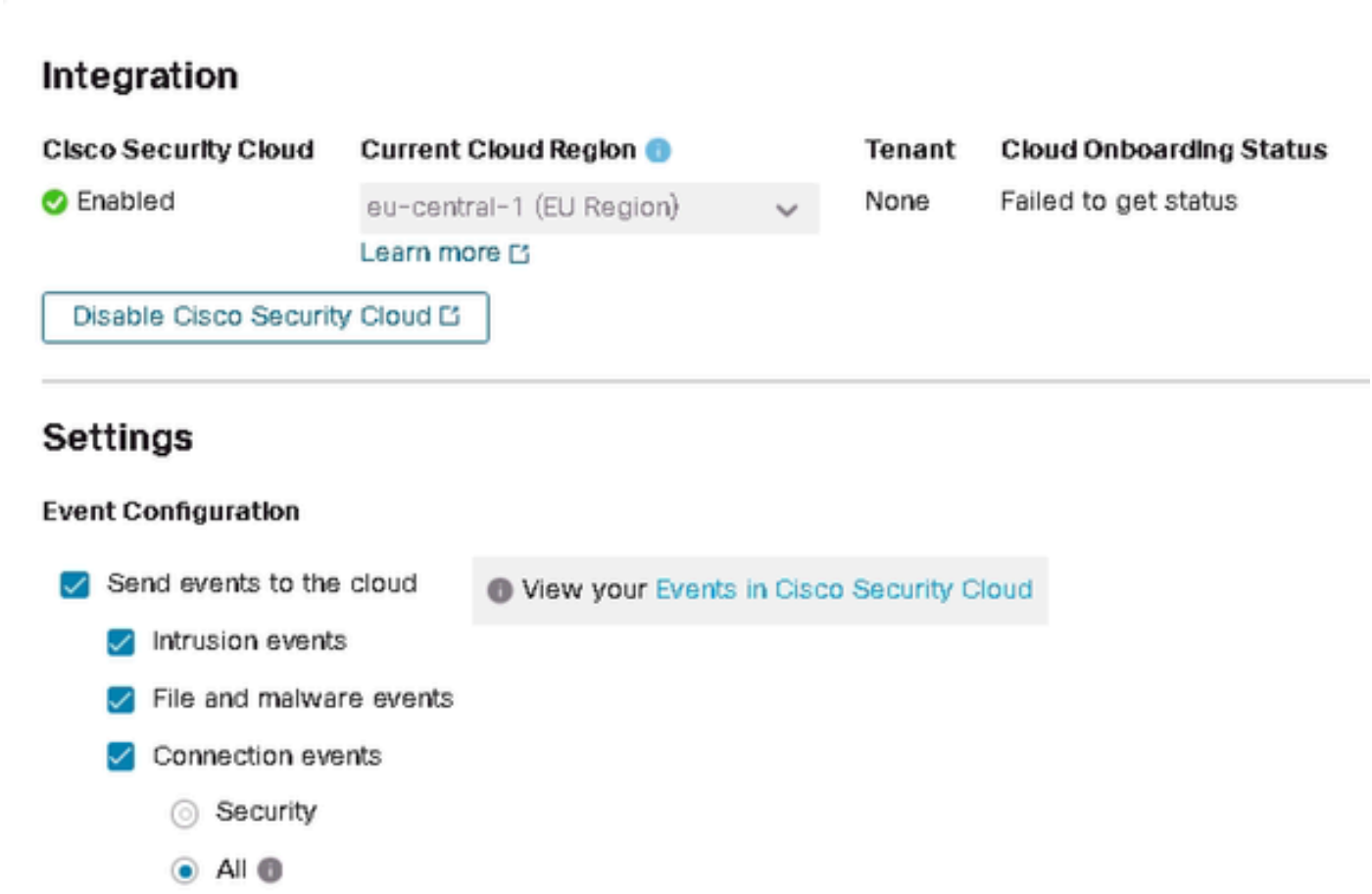
Die Hauptanforderung besteht darin, den HTTPS-Datenverkehr von dem registrierenden Gerät an diese Adressen zuzulassen:

- Region USA:
    - 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
- EU-Region:
    - 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
- Region Asien (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
- Region Australien:
    - 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
- Region Indien:
    - 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

Registrierung

Die Registrierung von Secure Firewall to Security Services Exchange erfolgt im Secure Firewall Management Center unter Integration > Cisco Security Cloud.



Diese Ausgaben zeigen an, dass eine erfolgreiche Verbindung zur Cisco Cloud hergestellt wurde.

<#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.ama
connector 5301 www 8u IPv6 104710 0t0 TCP *:8989 (LISTEN)
```

Registrierungsprotokolle werden in /var/log/connector/ gespeichert

Überprüfen der Registrierung

Nach erfolgreicher Registrierung auf Seiten der sicheren Firewall kann ein API-Aufruf an localhost:8989/v1/contexts/default/tenant ausgeführt werden, um den Namen und die ID des Security Services Exchange-Tenants zu erhalten.

<#root>

root@firepower:~#

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

{"registeredTenantInfo":{"companyId":"601143","companyName":"lab","domainName":"tac.cisco.com","id":"56

"Cisco - lab"

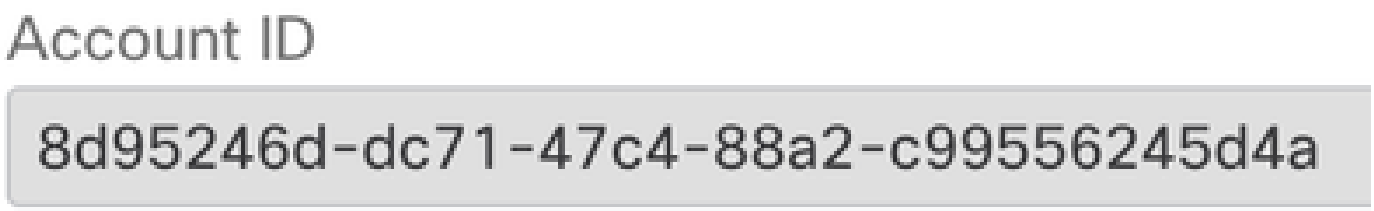
,"id":

"8d95246d-dc71-47c4-88a2-c99556245d4a"

,"spId":"AMP-EU"}]}

Überprüfung auf der Seite des Security Services Exchange

Navigieren Sie in Security Services Exchange zum Benutzernamen in der rechten oberen Ecke, und klicken Sie auf User Profile (Benutzerprofil), um zu bestätigen, dass die Konto-ID mit der zuvor in Secure Firewall abgerufenen Tenant-ID übereinstimmt.



Auf der Registerkarte "Cloud-Services" muss "Eventing" aktiviert sein. Außerdem muss bei Verwendung dieser Lösung der Cisco XDR-Switch aktiviert werden.

Die Registerkarte Geräte enthält eine Liste der registrierten Appliances.

Ein Eintrag für jedes Gerät kann erweitert werden und enthält folgende Informationen:

- Geräte-ID - im Fall von Secure Firewall kann diese ID durch Abfragen von curl -s gefunden werden: http://localhost:8989/v1/contexts/default | grep deviceId
- Datum der Eintragung
- IP-Adresse
- Version des SSX-Connectors
- Letzte Änderung

Events

Auf der Registerkarte "Ereignisse" können Sie die Aktionen für die Daten ausführen, die von der sicheren Firewall gesendet und in Security Services Exchange verarbeitet und angezeigt werden.

1. Filtern der Ereignisliste und Erstellen und Speichern von Filtern
2. Zusätzliche Tabellenspalten ein- oder ausblenden,
3. Überprüfen Sie die Ereignisse, die von sicheren Firewall-Geräten gesendet wurden.

Bei der Integration von Secure Firewall und Security Services Exchange werden die folgenden Ereignistypen unterstützt:

Ereignistyp	Unterstützte Threat Defense-Geräteversion für direkte Integration	Unterstützte Version des Threat Defense-Geräts für die Syslog-Integration
Angriffsereignisse	6.4 und höher	6.3 und höher
Verbindungsereignisse mit hoher Priorität: • Sicherheitsbezogene Verbindungsereignisse. • Verbindungsereignisse im Zusammenhang mit Datei- und Malware-Ereignissen. • Verbindungsereignisse im Zusammenhang mit Zugriffsversuchen.	6.5 und höher	Nicht unterstützt
Datei- und Malware-Ereignisse	6.5 und höher	Nicht unterstützt

Fehlerbehebung bei Ereignissen, die nicht in Security Services Exchange verarbeitet wurden

Bei der Beobachtung bestimmter Ereignisse im Secure Firewall Management Center kann es erforderlich sein, festzustellen, ob die Ereignisse den Bedingungen (die mit Angriffen, Datei-/Malware- und Verbindungsereignissen zusammenhängen) entsprechen, die in Security Services Exchange verarbeitet und angezeigt werden sollen.

Wenn Sie bestätigen, dass Ereignisse an die Cloud gesendet werden, indem Sie localhost:8989/v1/contexts/default abfragen, kann bestimmt werden, ob Ereignisse an die Cloud gesendet werden.

<#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

...
```

Die Anzahl der in TotalEventsReceived empfangenen Ereignisse bezieht sich auf Ereignisse, die zum Senden an das von der sicheren Firewall verarbeitete Security Services Exchange erforderlich sind.

Die Anzahl der in TotalEventsSent gesendeten Ereignisse bezieht sich auf Ereignisse, die an Cisco Cloud gesendet wurden.

Bei Ereignissen, die im Secure Firewall Management Center, aber nicht im Security Services Exchange auftreten, müssen die in /ngfw/var/sf/detection_engines/<engine>/ verfügbaren Ereignisprotokolle überprüft werden.

Basierend auf einem Zeitstempeldekodierungsereignisprotokoll mit 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
```

- Angriffsereignisse

Alle Angriffsereignisse werden in SSX und XDR verarbeitet und angezeigt. Stellen Sie sicher, dass in decodierten Protokollen das jeweilige Ereignis ein Flag enthält:

<#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
```

- Datei- und Malware-Ereignisse

Basierend auf den Anforderungen der Exchange-Plattform für Sicherheitsdienste werden nur Ereignisse mit einem bestimmten Ereignisuntertyp verarbeitet und angezeigt.

<#root>

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

```
    {
 “Unified2ID”: 502,

    “SyslogID”: 430005
    }
  }
 }
```

Daher sieht es in diesen decodierten Protokollen wie folgt aus:

<#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
```

- Verbindungsereignisse

In Bezug auf Verbindungsereignisse gibt es keine Untertypen. Wenn ein Verbindungsereignis jedoch eines dieser Felder enthält, wird es als Sicherheitsinformationsereignis betrachtet und in der Sicherheitsdiensteaustausch-Datenbank weiter verarbeitet.

- URL_SI_Category
- DNS_SI_Category
- IP_ReputationSI_Category

Anmerkung: Wenn Datei-/Malware- oder Verbindungsereignisse, die im Secure Firewall Management Center erkannt wurden, keine erwähnten Untertypen oder Parameter in den mit u2dump decodierten Unified Event Logs enthalten, bedeutet dies, dass diese spezifischen Ereignisse nicht verarbeitet und in Security Services Exchange angezeigt

---

werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.