Probleemoplossing voor beveiligde firewallintegratie met Security Services Exchange

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij de integratie van Cisco Secure Firewall met Security Services Exchange (SSX).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Secure Firewall Management Center (FMC)
- Cisco Secure-firewall

Gebruikte componenten

- Cisco Secure-firewall - 7.6.0
- Secure Firewall Management Center (FMC) - 7.6.0
- Security Services Exchange (SX)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleemoplossing

Connectiviteit

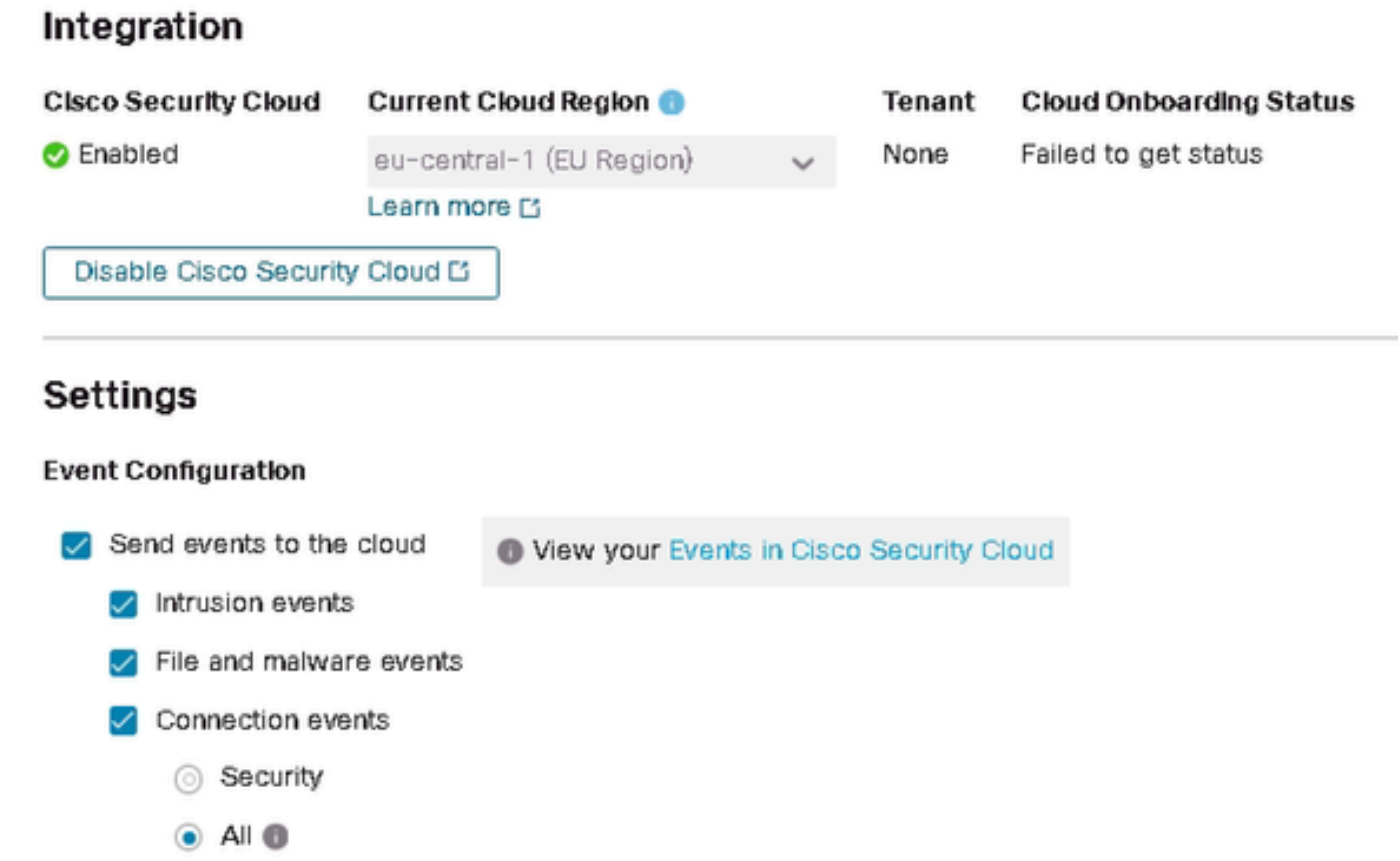
De belangrijkste eis is dat HTTPS-verkeer vanaf het registratieapparaat naar deze adressen wordt toegestaan:

- Amerikaanse regio:
    - 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-regio:
    - 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
- Regio Azië (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
- Regio Australië:
    - 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
- Regio India:
    - 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

Registratie

De registratie van Secure Firewall to Security Services Exchange wordt uitgevoerd in Secure Firewall Management Center, in Integratie > Cisco Security Cloud.



Deze uitgangen geven een succesvolle verbinding aan met Cisco Cloud.

<#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)
```

Registratielogboeken worden opgeslagen in /var/log/connector/.

Verificatie van de registratie

Als de registratie aan de kant van Secure Firewall succesvol is, kan een API-oproep naar localhost:8989/v1/contexten/default/tenant worden uitgevoerd om de naam en ID van de medewerker van Security Services Exchange te verkrijgen.

<#root>

root@firepower:~#

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

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

"Cisco - lab"

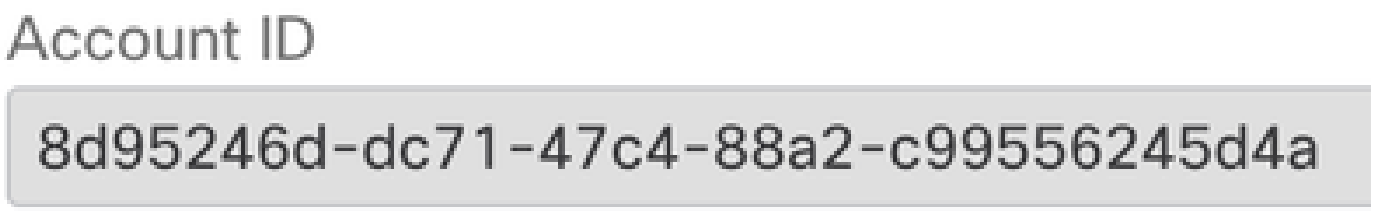
,"id":

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

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

Verificatie aan de kant van Security Services Exchange

In Security Services Exchange navigeer naar de gebruikersnaam in de rechterbovenhoek en klik op Gebruikersprofiel om te bevestigen dat de account-ID overeenkomt met de huurder-ID die eerder in Secure Firewall is verkregen.



In het tabblad Cloud Services is het vereist om Event ingeschakeld te hebben. Ook moet Cisco XDR switch ingeschakeld zijn als u deze oplossing gebruikt.

Het tabblad Apparaten bevat een lijst van geregistreerde apparaten.

Een ingang voor elk apparaat is uitbreidbaar en bevat deze informatie:

- Apparaat-ID - in het geval van Secure Firewall kan deze ID worden gevonden door curl -s http://localhost:8989/v1/contexts/default te bevragen | grep deviceID
- Registratiedatum
- IP-adres
- Versie SSX-connector
- Laatste wijziging

Gebeurtenissen

Op het tabblad Gebeurtenissen kunnen we de acties uitvoeren op de gegevens die door Secure Firewall zijn verzonden en die worden verwerkt en weergegeven in Security Services Exchange.

1. Filter de lijst van gebeurtenissen en maak en sla filters op.
2. Extra tabelkolommen tonen of verbergen,
3. Bekijk de gebeurtenissen die zijn verzonden vanaf Secure Firewall-apparaten.

In integratie tussen Secure Firewall en Security Services Exchange worden deze eventypen ondersteund:

Type gebeurtenis	Ondersteunde Threat Defense Device versie voor directe integratie	Versie Ondersteund Threat Defense Device voor systeemintegratie
Inbraakgebeurtenissen	6.4 en hoger	6.3 en hoger
Prioritaire verbindingsgebeurtenissen: • Beveiligingsgerelateerde verbindingsgebeurtenissen. • Verbindingsgebeurtenissen die verband houden met gebeurtenissen in bestanden en malware. • Verbindingsgebeurtenissen die verband houden met inbraakgebeurtenissen.	6.5 en hoger	Niet ondersteund
Evenementen met bestanden en malware	6.5 en hoger	Niet ondersteund

Probleemoplossing voor gebeurtenissen die niet in Security Services Exchange zijn verwerkt

Bij het observeren van specifieke gebeurtenissen in het Secure Firewall Management Center kan worden vereist dat wordt bepaald of gebeurtenissen overeenkomen met de voorwaarden (die met betrekking tot Inbraakgebeurtenissen, gebeurtenissen in File/Malware en Verbindingsgebeurtenissen) die moeten worden verwerkt en weergegeven in de Security Services Exchange.

Bevestiging dat gebeurtenissen naar de cloud worden verzonden door localhost:8989/v1/contexten/default kan worden bepaald of gebeurtenissen naar de cloud worden verzonden.

<#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

...
```

Het aantal gebeurtenissen ontvangen in TotalEventsReceived betekent gebeurtenissen die van toepassing zijn voor het verzenden naar de Security Services Exchange verwerkt door Secure Firewall.

Het aantal gebeurtenissen dat is verzonden in TotalEventsSent staat voor gebeurtenissen die zijn verzonden naar Cisco Cloud.

In het geval van gebeurtenissen die worden gezien in het Secure Firewall Management Center, maar niet in de Security Services Exchange, moeten gebeurtenissenlogboeken die beschikbaar zijn in /ngfw/var/sf/detectie_engines/<engine>/, worden geverifieerd.

Gebaseerd op een tijdstempel decodeer specifiek gebeurtenislogboek met 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
```

- Inbraakgebeurtenissen

Alle inbraakgebeurtenissen worden verwerkt en weergegeven in SX en XDR. Zorg ervoor dat in gedecodeerde logbestanden die specifieke gebeurtenis een vlag bevat:

<#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
```

- Evenementen in File en Malware

Gebaseerd op de eisen van het platform van de Uitwisseling van de Diensten van de Veiligheid slechts worden de gebeurtenissen met specifiek Subtype van Gebeurtenis verwerkt en getoond.

<#root>

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

```
"FileMalware":

    {
"Unified2ID": 502,

    "SyslogID": 430005
    }
  }
}
```

Daarom lijkt het op deze gedecodeerde logboeken:

<#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
```

- Verbindingsgebeurtenissen

Met betrekking tot Verbindingsgebeurtenissen, zijn er geen subtypes. Echter, als een verbinding gebeurtenis een van deze velden heeft, wordt het beschouwd als een Security Intelligence-gebeurtenis en wordt het verder verwerkt in de Security Services Exchange.

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

Opmerking: Als gebeurtenissen van File/Malware of Connection die in Secure Firewall Management Center worden gezien, geen vermelde subtypes of parameters in de met u2dump gedecodeerde unified gebeurtenissenlogboeken bevatten, betekent dit dat deze

---

specifieke gebeurtenissen niet worden verwerkt en weergegeven in Security Services Exchange

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.