Security Services Exchange와의 보안 방화벽 통합 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

문제 해결

- 연결
- 등록
  - 등록 확인
  - Security Services Exchange 측에서 확인
- 이벤트
- Security Services Exchange에서 처리되지 않은 이벤트 문제 해결

소개

이 문서에서는 Cisco Secure Firewall과 SSX(Security Services Exchange)의 통합 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- FMC(Secure Firewall Management Center)
- Cisco 보안 방화벽

사용되는 구성 요소

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제 해결

연결

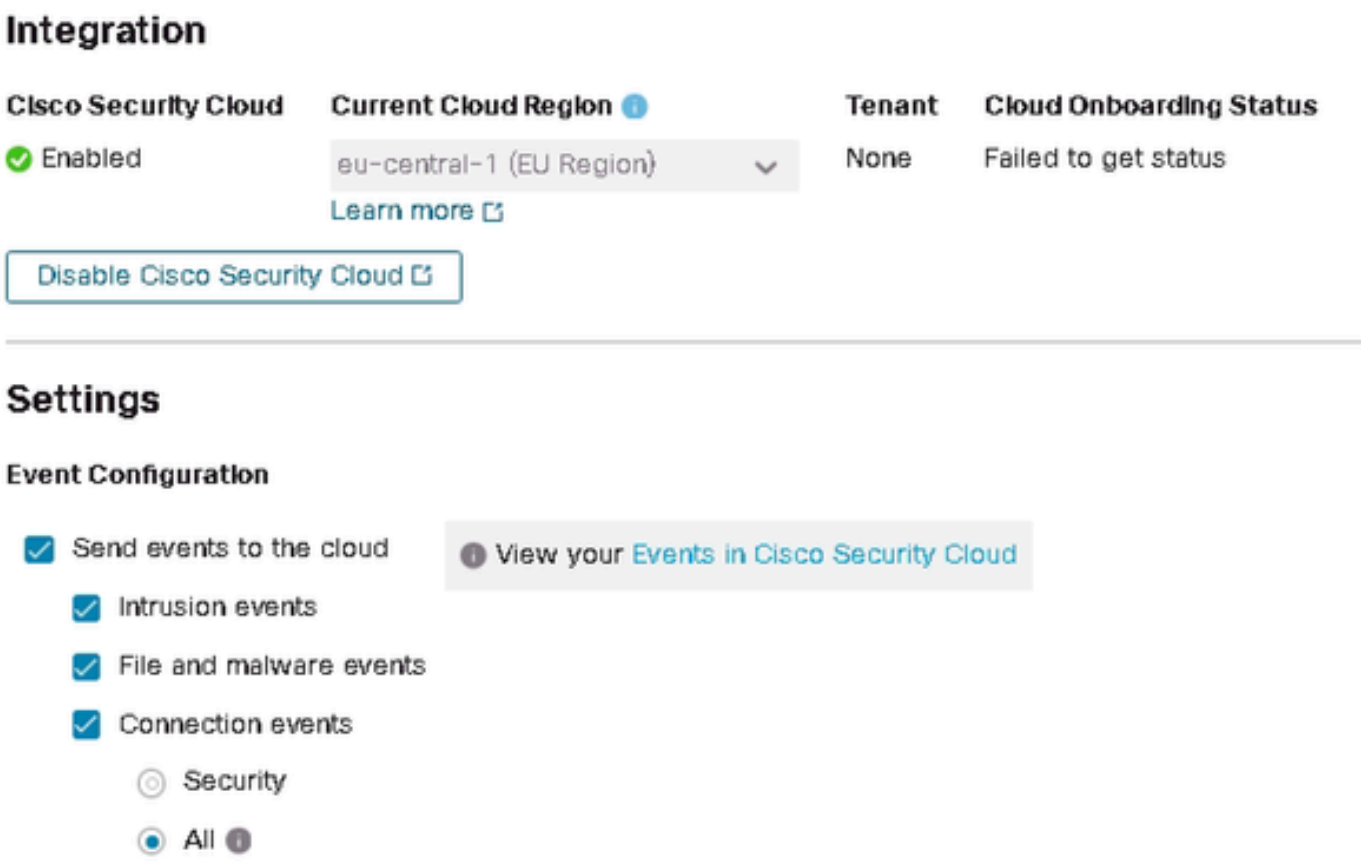
주요 요구 사항은 등록 디바이스에서 이러한 주소로 향하는 HTTPS 트래픽을 허용하는 것입니다.

- 미국 지역:
  - 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.com을 참조하십시오.
  - defenseorchestrator.com
  - edge.us.cdo.cisco.com을 참조하십시오.
- 유럽 지역:
  - api.eu.sse.itd.cisco.com을 참조하십시오.
  - mx*.eu.sse.itd.cisco.com
  - dex.eu.sse.itd.cisco.com을 참조하십시오.
  - eventing-ingest.eu.sse.itd.cisco.com을 참조하십시오.
  - registration.eu.sse.itd.cisco.com을 참조하십시오.
  - defenseorchestrator.eu
  - edge.eu.cdo.cisco.com을 참조하십시오.
- 아시아(APJC) 지역:
  - 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

- 호주 지역:
    - api.aus.sse.itd.cisco.com
    - mx*.aus.sse.itd.cisco.com
    - dex.au.sse.itd.cisco.com을 참조하십시오.
    - eventing-ingest.aus.sse.itd.cisco.com
    - registration.au.sse.itd.cisco.com을 참조하십시오.
    - aus.cdo.cisco.com
- 인도 지역:
    - api.in.sse.itd.cisco.com을 참조하십시오.
    - mx*.in.sse.itd.cisco.com
    - dex.in.sse.itd.cisco.com을 참조하십시오.
    - eventing-ingest.in.sse.itd.cisco.com을 참조하십시오.
    - registration.in.sse.itd.cisco.com을 참조하십시오.
    - in.cdo.cisco.com

등록

Secure Firewall을 Security Services Exchange에 등록하는 방법은 Secure Firewall Management Center, Integration > Cisco Security Cloud에서 수행합니다.



이러한 출력은 Cisco Cloud에 성공적으로 연결되었음을 나타냅니다.

<#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)
```

등록 로그는 /var/log/connector/에 저장됩니다.

등록 확인

보안 방화벽 측에서 등록이 성공하면 보안 서비스 교환 테넌트 이름 및 ID를 얻기 위해 localhost:8989/v1/contexts/default/tenant에 대한 API 호출을 수행할 수 있습니다.

<#root>

root@firepower:~#

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

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

"Cisco - lab"

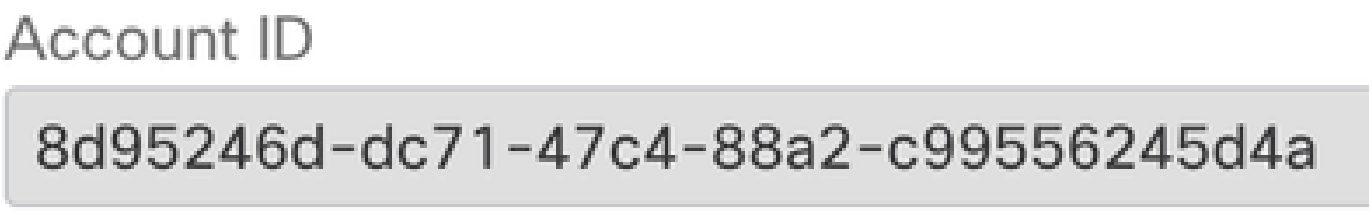
,"id":

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

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

Security Services Exchange 측에서 확인

Security Services Exchange의 오른쪽 상단 모서리에 있는 사용자 이름으로 이동한 다음 User Profile(사용자 프로필)을 클릭하여 계정 ID가 보안 방화벽에서 이전에 얻은 테넌트 ID와 일치하는지 확인합니다.



Cloud Services(클라우드 서비스) 탭에서는 Eventing(이벤트 처리)을 활성화해야 합니다. 또한 이 솔루션을 사용할 경우 Cisco XDR 스위치를 켜야 합니다.

Devices 탭은 등록된 어플라이언스의 목록을 포함합니다.

각 디바이스에 대한 항목은 확장 가능하며 다음 정보를 포함합니다.

- Device ID(디바이스 ID) - Secure Firewall(보안 방화벽)의 경우 curl -s

http://localhost:8989/v1/contexts/default에 쿼리하면 이 ID를 찾을 수 있습니다. | grep deviceId
- 등록 날짜
- IP 주소
- SSX 커넥터 버전
- 마지막 수정

이벤트

Events(이벤트) 탭에서는 Secure Firewall에서 전송한 데이터 및 Security Services Exchange에서 처리 및 표시되는 데이터에 대한 작업을 수행할 수 있습니다.

1. 이벤트 목록을 필터링하고 필터를 생성 및 저장합니다.
2. 추가 테이블 열을 표시하거나 숨깁니다.
3. Secure Firewall 디바이스에서 전송된 이벤트를 검토합니다.

Secure Firewall과 Security Services Exchange의 통합에서 다음 이벤트 유형이 지원됩니다.

이벤트 유형	직접 통합을 위해 지원되는 Threat Defense 디바이스 버전	Syslog 통합을 위해 지원되는 위협 방어 디바이스 버전
침입 이벤트	6.4 이상	6.3 이상
우선 순위가 높은 연결 이벤트: • 보안 관련 연결 이벤트. • 파일 및 악성코드 이벤트와 관련된 연결 이벤트입니다. • 침입 이벤트와 관련된 연결 이벤트.	6.5 이상	지원되지 않음
파일 및 악성코드 이벤트	6.5 이상	지원되지 않음

Security Services Exchange에서 처리되지 않은 이벤트 문제 해결

Secure Firewall Management Center에서 특정 이벤트를 관찰하는 경우, 이벤트가 Security Services Exchange에서 처리 및 표시할 조건(침입, 파일/악성코드 및 연결 이벤트와 관련된 조건)과 일치하는지 여부를 확인해야 합니다.

localhost:8989/v1/contexts/default를 쿼리하여 이벤트가 클라우드로 전송되는지 확인합니다. 이벤트가 클라우드로 전송되는지 여부를 확인할 수 있습니다.

<#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
...
```

TotalEventsReceived에서 수신된 이벤트 수는 보안 방화벽에서 처리한 보안 서비스 교환으로 전송할 수 있는 이벤트를 의미합니다.

TotalEventsSent에서 전송된 이벤트 수는 Cisco Cloud로 전송된 이벤트를 의미합니다.

Secure Firewall Management Center에 이벤트가 표시되지만 Security Services Exchange에는 표시되지 않는 경우, /ngfw/var/sf/detection_engines/<engine>/ 의 이벤트 로그를 확인해야 합니다.

u2dump를 사용하여 타임스탬프 디코드 특정 이벤트 로그 기반:

<#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

- 침입 이벤트

모든 침입 이벤트는 SSX 및 XDR에서 처리되고 표시됩니다. 디코딩된 로그에서 특정 이벤트에 플래그가 포함되어 있는지 확인합니다.

<#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
```

- 파일 및 악성코드 이벤트

Security Services Exchange 플랫폼 요구 사항에 따라 특정 이벤트 하위 유형의 이벤트만 처리 및 표시됩니다.

<#root>

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

“FileMalware”:

```
     {
```

“Unified2ID”: 502,

```
     “SyslogID”: 430005
     }
   }
 }
```

따라서 이러한 디코딩된 로그에서는 다음과 같습니다.

<#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
```

- 연결 이벤트

연결 이벤트와 관련해서는 하위 유형이 없습니다. 그러나 연결 이벤트에 이러한 필드가 있으면 보안 인텔리전스 이벤트로 간주되며 Security Services Exchange에서 더 자세히 처리됩니다.

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

참고: Secure Firewall Management Center에 표시되는 파일/악성코드 또는 연결 이벤트에 u2dump로 디코딩된 통합 이벤트 로그에 언급된 하위 유형 또는 매개변수가 포함되어 있지 않은 경우, 이는 이러한 특정 이벤트가 처리되지 않고 Security Services Exchange에 표시되지 않음을 의미합니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.