Solucione problemas de integração segura de firewall com o Security Services Exchange

Contents

Introdução

Este documento descreve como solucionar problemas de integração do Cisco Secure Firewall com o Security Services Exchange (SSX).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Centro de gerenciamento seguro de firewall (FMC)
- Firewall seguro da Cisco

Componentes Utilizados

- Cisco Secure Firewall - 7.6.0
- Centro de gerenciamento de firewall seguro (FMC) - 7.6.0
- Security Services eXchange (SSX)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Troubleshooting

Conectividade

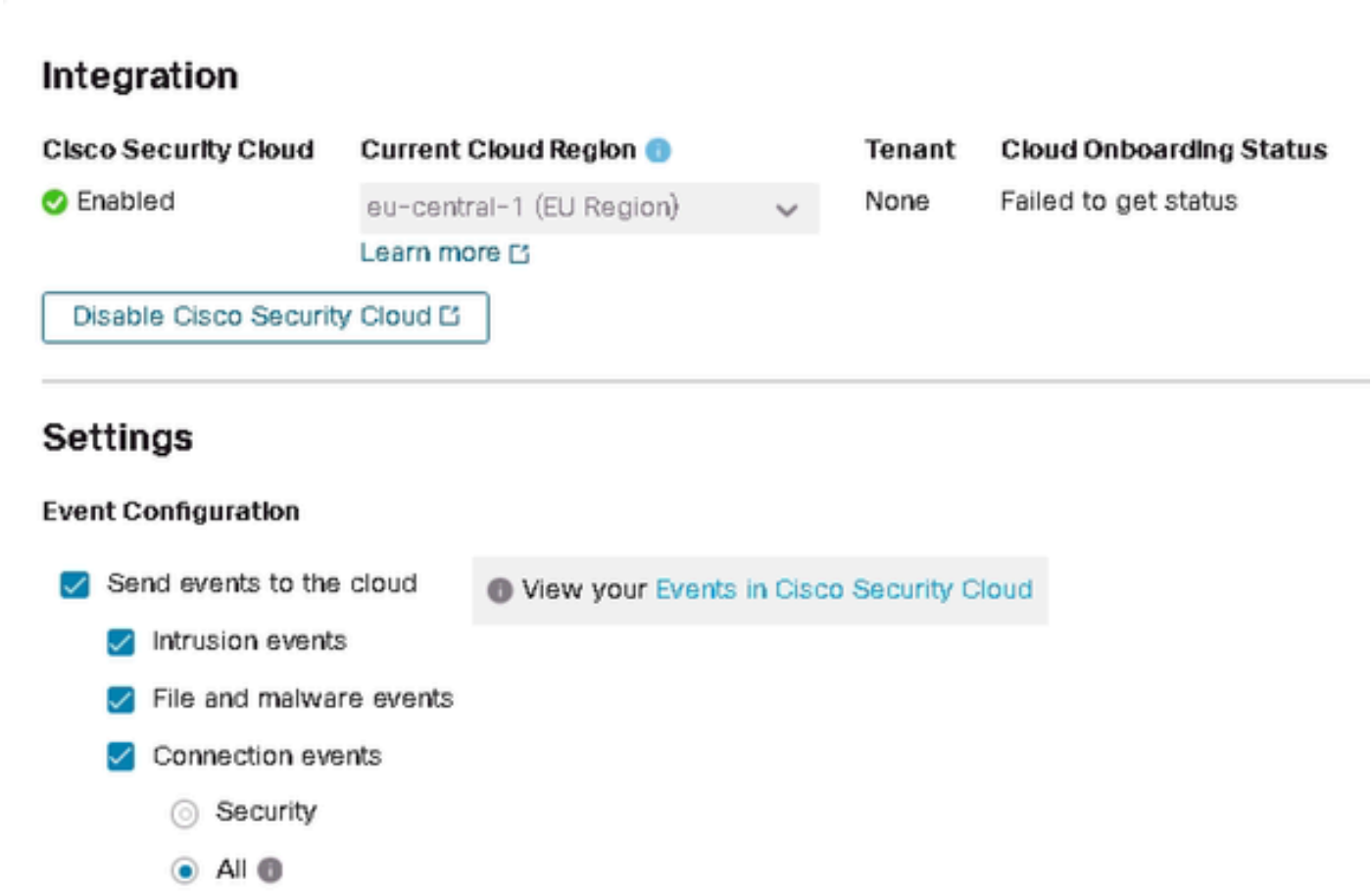
O principal requisito é permitir o tráfego HTTPS para esses endereços do dispositivo de registro:

- Região dos EUA:
    - 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
- Região da 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
- Região da Ásia (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
- Região da Austrália:
    - 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
- Região da Índia:
    - 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

Registro

O registro do Secure Firewall para o Security Services Exchange é feito no Secure Firewall Management Center, em Integração > Cisco Security Cloud.



Essas saídas indicam uma conexão bem-sucedida estabelecida com o 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)
```

Os registros de registro são armazenados em /var/log/connector/.

Verificando o registro

Quando o registro for bem-sucedido no lado do Firewall Seguro, uma chamada de API para localhost:8989/v1/contexts/default/tenant poderá ser realizada para obter o nome e a ID do locatário do 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"

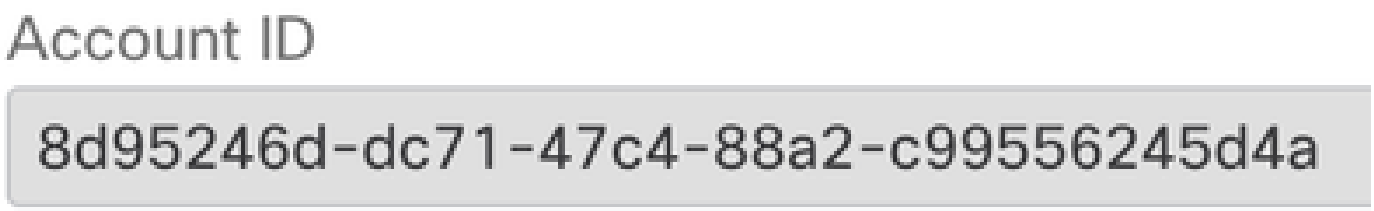
,"id":

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

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

Verificação no lado do Security Services Exchange

Em Security Services Exchange, navegue até o nome de usuário no canto superior direito e clique em User Profile (Perfil do usuário) para confirmar se a ID da conta corresponde à ID do locatário obtida antes no Secure Firewall.



Na guia Cloud Services, é necessário ter Eventing habilitado. Além disso, o switch Cisco XDR deve ser ligado no caso de utilizar esta solução.

A guia Dispositivos contém uma lista de dispositivos registrados.

Uma entrada para cada dispositivo é expansível e contém estas informações:

- ID do dispositivo - no caso do Firewall seguro, essa ID pode ser encontrada consultando curl -s http://localhost:8989/v1/contexts/default | grep deviceId
- Data de registro
- IP Address
- versão do conector SSX
- Última modificação

Events

A guia Eventos nos permite executar as ações nos dados que foram enviados pelo Secure Firewall e que são processados e exibidos no Security Services Exchange.

1. Filtrar a lista de eventos e criar e salvar filtros,
2. Mostrar ou ocultar colunas adicionais da tabela,
3. Revise os eventos enviados dos dispositivos com firewall seguro.

Na integração entre o Secure Firewall e o Security Services Exchange, há suporte para estes tipos de eventos:

Tipo de evento	Versão do dispositivo Threat Defense suportada para integração direta	Versão do dispositivo Threat Defense suportada para integração de Syslog
Eventos de intrusão	6.4 e mais recente	6.3 e posterior
Eventos de conexão de alta prioridade: • Eventos de conexão relacionados à segurança. • Eventos de conexão relacionados a eventos de arquivo e malware. • Eventos de conexão relacionados a eventos de invasão.	6.5 e posterior	Not Supported
Eventos de arquivos e malware	6.5 e posterior	Not Supported

Solucionar eventos não processados no Security Services Exchange

No caso da observação de eventos específicos no Secure Firewall Management Center, pode ser necessário determinar se os eventos correspondem às condições (aquelas relacionadas a eventos de Intrusão, Arquivo/Malware e Conexão) a serem processados e exibidos no Security Services Exchange.

A confirmação de que os eventos estão sendo enviados para a nuvem consultando localhost:8989/v1/contexts/default pode ser determinada se os eventos estão sendo enviados para a nuvem.

<#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

...
```

O número de eventos recebidos em TotalEventsReceived significa eventos aplicáveis para enviar ao Security Services Exchange processados pelo Firewall Seguro.

O número de eventos enviados em TotalEventsSent significa eventos enviados para a Nuvem da Cisco.

No caso de eventos vistos no Secure Firewall Management Center, mas não no Security Services Exchange, os registros de eventos disponíveis em /ngfw/var/sf/detection_engines/<engine>/ devem ser verificados.

Com base em um log de eventos específico de decodificação de carimbo de data/hora usando 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
```

- Eventos de intrusão

Todos os eventos de intrusão são processados e exibidos no SSX e no XDR. Certifique-se de que, em logs decodificados, esse evento específico contenha um flag:

<#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
```

- Eventos de arquivo e malware

Com base nos requisitos da plataforma Security Services Exchange, somente eventos com Subtipo de evento específico estão sendo processados e exibidos.

<#root>

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

```
    {
 “Unified2ID”: 502,

    “SyslogID”: 430005
    }
  }
 }
```

Portanto, ele se parece com estes logs decodificados:

<#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
```

- Eventos de conexão

Com relação aos eventos de conexão, não há subtipos. No entanto, se um evento de conexão tiver qualquer um desses campos, ele será considerado um evento de Inteligência de segurança e será processado posteriormente no Security Services Exchange.

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

Note: Se os eventos File/Malware ou Connection vistos no Secure Firewall Management Center, não contiverem subtipos ou parâmetros mencionados nos registros de eventos unificados decodificados com u2dump, isso significa que esses eventos específicos não estão sendo processados e exibidos no Security Services Exchange

---

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.