Solución de problemas de integración de firewall seguro con Security Services Exchange

Contenido

Introducción

Este documento describe cómo resolver problemas de integración de Cisco Secure Firewall con Security Services Exchange (SSX).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Centro de gestión de firewall seguro (FMC)
- Firewall seguro de Cisco

Componentes Utilizados

- Firewall seguro de Cisco - 7.6.0
- Secure Firewall Management Center (FMC): 7.6.0
- Intercambio de servicios de seguridad (SSX)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Resolución de problemas

Conectividad

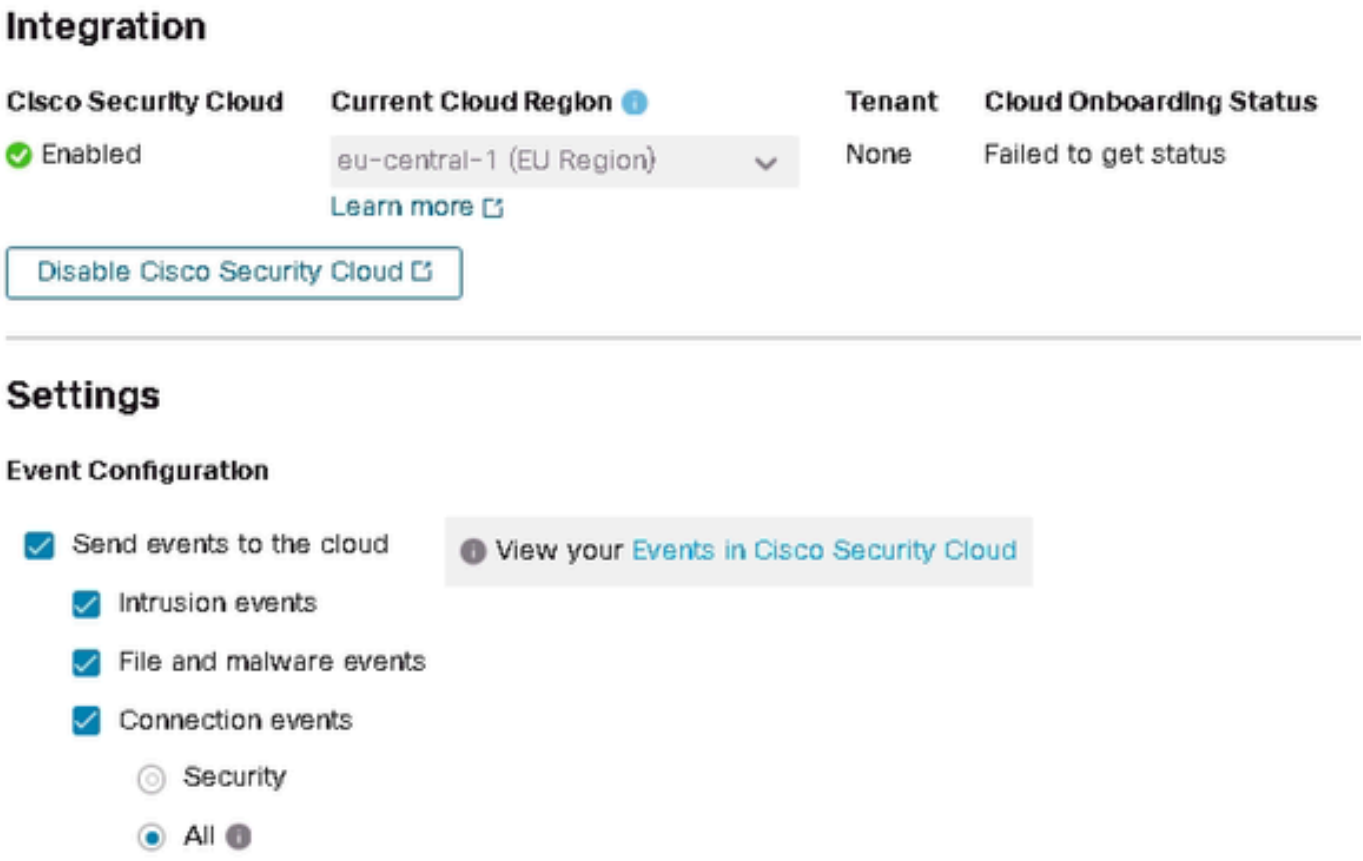
El requisito principal es permitir el tráfico HTTPS hacia estas direcciones desde el dispositivo de registro:

- Región de EE. UU.
    - 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
- Región de la 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
- Región de Asia (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
- Región de Australia:
    - 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
- Región de la 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

Registro

El registro de Secure Firewall a Security Services Exchange se realiza en Secure Firewall Management Center, en Integración > Cisco Security Cloud.



Estos resultados indican una conexión correcta establecida con la nube de Cisco.

<#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)
```

Los registros de registro se almacenan en /var/log/connector/.

Verificación del registro

Una vez que el registro es correcto en el lado de Secure Firewall, se puede realizar una llamada API a localhost:8989/v1/contexts/default/tenant para obtener el nombre y la ID del arrendatario de 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"

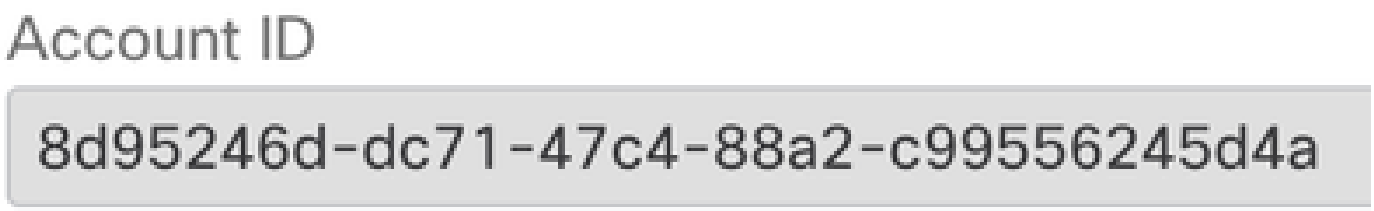
,"id":

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

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

Verificación en el lado de Security Services Exchange

En Security Services Exchange, desplácese hasta el nombre de usuario de la esquina superior derecha y haga clic en User Profile (Perfil de usuario) para confirmar que la ID de cuenta coincide con la ID de arrendatario obtenida anteriormente en Secure Firewall.



En la pestaña Servicios en la nube, es necesario tener Eventos habilitados. Además, el switch Cisco XDR debe estar encendido en caso de utilizar esta solución.

La ficha Devices contiene una lista de dispositivos registrados.

Se puede ampliar una entrada para cada dispositivo que contiene la siguiente información:

- Device ID (ID de dispositivo): en el caso de Secure Firewall, este ID se puede encontrar consultando curl -s http://localhost:8989/v1/contexts/default | grep deviceId
- Fecha de registro
- IP Address
- versión del conector SSX
- Última modificación

Events

La ficha de eventos nos permite realizar las acciones sobre los datos enviados por Secure Firewall y que se procesan y muestran en Security Services Exchange.

1. Filtrar la lista de eventos y crear y guardar filtros,
2. Mostrar u ocultar columnas de tabla adicionales,
3. Revise los eventos enviados desde los dispositivos de firewall seguro.

En la integración entre Secure Firewall y Security Services Exchange, se admiten estos tipos de eventos:

Tipo de Evento	Versión del dispositivo compatible Threat Defence para integración directa	Versión del dispositivo compatible Threat Defence para la integración de Syslog
Eventos de intrusión	6.4 y posteriores	6.3 y posteriores
Eventos de conexión de alta prioridad: • Eventos de conexión relacionados con la seguridad. • Eventos de conexión relacionados con archivos y eventos de malware. • Eventos de conexión relacionados con eventos de intrusión.	6.5 y posteriores	No soportados
Eventos de archivos y malware	6.5 y posteriores	No soportados

Solucionar problemas de eventos no procesados en el intercambio de servicios de seguridad

En el caso de la observación de eventos específicos en Secure Firewall Management Center, puede ser necesario determinar si los eventos coinciden con las condiciones (las relacionadas con los eventos de intrusión, archivo/malware y conexión) que se procesarán y mostrarán en Security Services Exchange.

Confirmación de que los eventos se están enviando a la nube consultando localhost:8989/v1/contexts/default. Se puede determinar si los eventos se están enviando a la nube.

<#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

...
```

El número de eventos recibidos en TotalEventsReceived significa eventos aplicables para el envío a Security Services Exchange procesados por Secure Firewall.

El número de eventos enviados en TotalEventsSent significa eventos enviados a la nube de Cisco.

En caso de que se observen eventos en Secure Firewall Management Center, pero no en Security Services Exchange, los registros de eventos disponibles en /ngfw/var/sf/detection_engine/<engine>/ deben verificarse.

Basado en un registro de eventos específico de decodificación de marca de tiempo 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 intrusión

Todos los eventos de intrusión se procesan y muestran en SSX y XDR. Asegúrese de que en los registros descodificados ese evento específico contenga un indicador:

<#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 archivos y malware

Según los requisitos de la plataforma Security Services Exchange, solo se procesan y muestran los eventos con un subtipo de evento específico.

<#root>

```
"FileEvent":
 {
   “Subtypes”:
   {
     “FileLog”:
     {
```

```
    “Unified2ID”: 500,
    “SyslogID”: 430004
    },
“FileMalware”:
    {
“Unified2ID”: 502,
    “SyslogID”: 430005
    }
  }
}
```

Por lo tanto, se ve como en estos registros 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 conexión

En cuanto a los eventos de conexión, no hay subtipos. Sin embargo, si un evento de conexión tiene cualquiera de estos campos, se considera un evento de inteligencia de seguridad y se procesa más adelante en el intercambio de servicios de seguridad.

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

Nota: Si los eventos de archivo/malware o de conexión que se ven en Secure Firewall Management Center no contienen los subtipos o parámetros mencionados en los registros de eventos unificados descodificados con u2dump, significa que estos eventos específicos no se procesan ni se muestran en Security Services Exchange

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).