Risoluzione dei problemi relativi all'integrazione di Secure Firewall con Security Services Exchange

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di integrazione di Cisco Secure Firewall con Security Services Exchange (SSX).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Centro gestione firewall protetto (FMC)
- Cisco Secure Firewall

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Risoluzione dei problemi

Connettività

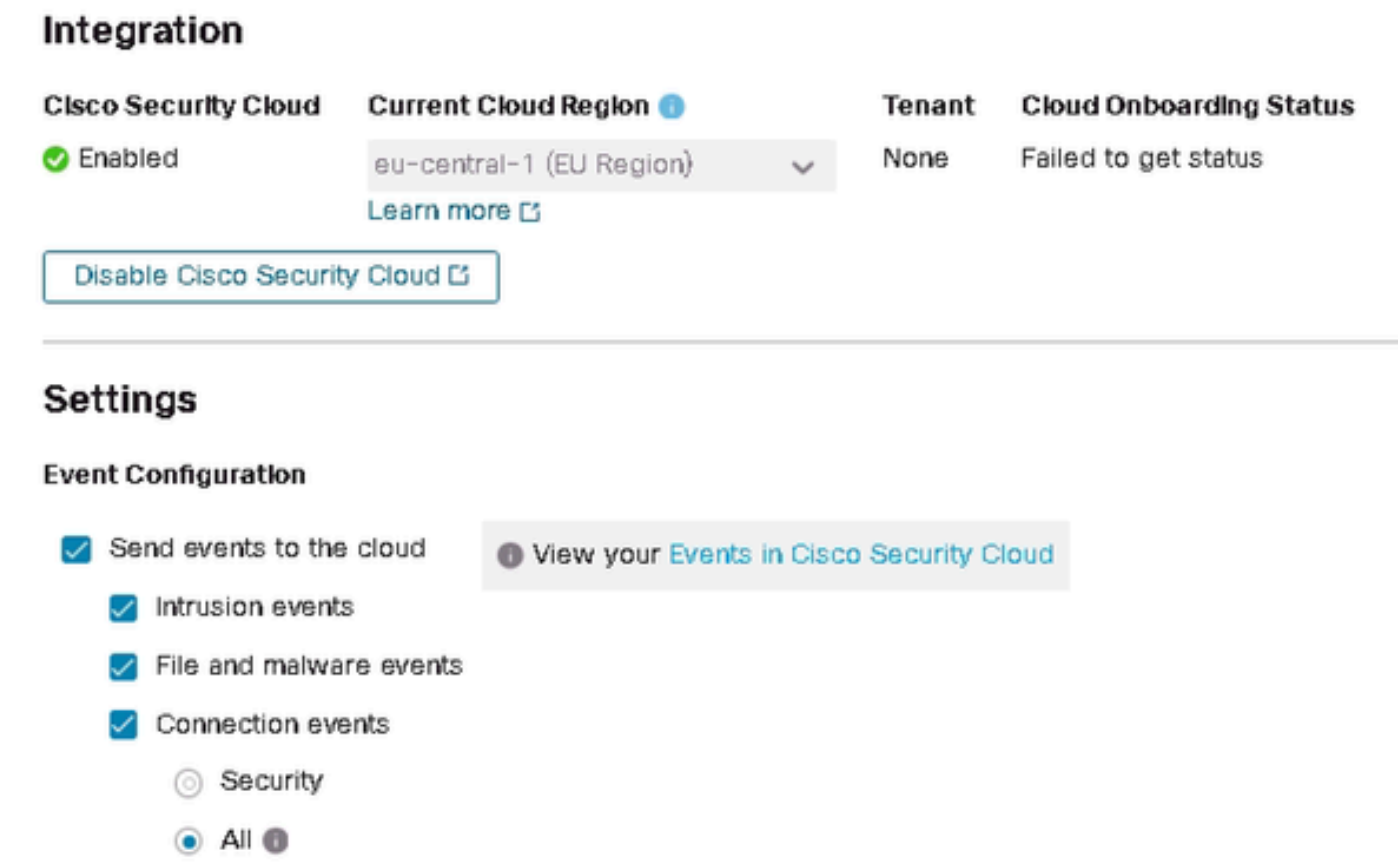
Il requisito principale è consentire il traffico HTTPS verso questi indirizzi dal dispositivo di registrazione:

- Regione 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
- Regione 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
- Regione 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
- Regione 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
- Regione 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

Registration

La registrazione di Secure Firewall in Security Services Exchange viene eseguita in Centro gestione Secure Firewall, in Integrazione > Cisco Security Cloud.



Questi output indicano che la connessione a Cisco Cloud è stata stabilita.

<#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)
```

I registri di registrazione sono memorizzati in /var/log/connector/.

Verifica della registrazione

Una volta completata la registrazione sul lato Secure Firewall, è possibile eseguire una chiamata API a localhost:8989/v1/contests/default/tenant per ottenere il nome e l'ID del tenant di 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"

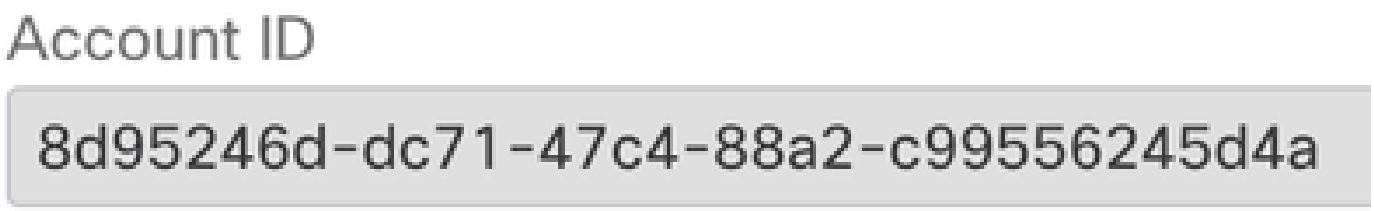
,"id":

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

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

Verifica sul lato Exchange dei servizi di sicurezza

In Servizi di sicurezza, passare al nome utente nell'angolo superiore destro e fare clic su Profilo utente per verificare che l'ID account corrisponda all'ID tenant ottenuto in precedenza in Secure Firewall.



Nella scheda Servizi cloud, è necessario che Eventing sia abilitato. Inoltre, per utilizzare questa soluzione, è necessario attivare lo switch Cisco XDR.

La scheda Dispositivi contiene un elenco degli accessori registrati.

Una voce per ciascun dispositivo è espandibile e contiene le seguenti informazioni:

- ID periferica - nel caso di Secure Firewall questo ID può essere trovato interrogando curl -s http://localhost:8989/v1/contexts/default | grep ID dispositivo
- Data di registrazione
- Indirizzo IP
- Versione connettore SSX
- Ultima modifica

Eventi

La scheda Eventi consente di eseguire le azioni sui dati inviati da Secure Firewall ed elaborati e visualizzati in Security Services Exchange.

1. Filtrare l'elenco degli eventi e creare e salvare filtri,
2. Visualizzare o nascondere colonne aggiuntive della tabella.
3. Controllare gli eventi inviati dai dispositivi Secure Firewall.

Nell'integrazione tra Secure Firewall e Security Services Exchange sono supportati i seguenti tipi di evento:

Tipo di evento	Versione del dispositivo di difesa dalle minacce supportata per l'integrazione diretta	Versione del dispositivo Threat Defense supportata per l'integrazione Syslog
Eventi intrusione	6.4 e successive	6.3 e successive
Eventi di connessione ad alta priorità: • Eventi di connessione relativi alla sicurezza. • Eventi di connessione correlati a eventi di file e malware. • Eventi di connessione correlati a eventi di intrusione.	6.5 e successive	Non supportata
Eventi file e malware	6.5 e successive	Non supportata

Risoluzione dei problemi relativi agli eventi non elaborati in Security Services

Exchange

In caso di osservazione di eventi specifici nel Centro gestione firewall protetto, può essere necessario determinare se gli eventi soddisfano le condizioni (relative agli eventi di intrusione, file/malware e connessione) da elaborare e visualizzare in Security Services Exchange.

Conferma dell'invio degli eventi al cloud eseguendo una query su localhost:8989/v1/contests/default. È possibile determinare se gli eventi vengono inviati al cloud.

<#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

...
```

Il numero di eventi ricevuti in TotalEventsReceived indica gli eventi applicabili per l'invio a Security Services Exchange elaborati da Secure Firewall.

Il numero di eventi inviati in TotalEventsSent indica gli eventi inviati a Cisco Cloud.

Nel caso di eventi rilevati nel Centro gestione firewall sicuro, ma non in Security Services Exchange, è necessario verificare i registri eventi disponibili in /ngfw/var/sf/detection_engine/<engine>/.

In base a un timestamp decodificare il registro eventi specifico utilizzando 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
```

- Eventi intrusione

Tutti gli eventi di intrusione vengono elaborati e visualizzati in SSX e XDR. Verificare che nei registri decodificati l'evento specifico contenga un 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
```

- Eventi file e malware

In base ai requisiti della piattaforma Exchange dei servizi di sicurezza, vengono elaborati e visualizzati solo gli eventi con sottotipo di evento specifico.

<#root>

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

```
    {
    "Unified2ID": 502,

    "SyslogID": 430005
    }
  }
}
```

Pertanto, il file registro è simile a quanto riportato di seguito:

<#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
```

- Eventi connessione

Per quanto riguarda gli eventi di connessione, non esistono sottotipi. Tuttavia, se un evento di connessione dispone di uno di questi campi, viene considerato un evento di Security Intelligence e viene ulteriormente elaborato in Security Services Exchange.

· URL_SI_Category

· DNS_SI_Category

· IP_ReputationSI_Category

Nota: Se gli eventi relativi a file, malware o connessione visualizzati in Centro gestione firewall protetto non contengono i sottotipi o i parametri indicati nei registri eventi unificati decodificati con u2dump, significa che tali eventi specifici non vengono elaborati e visualizzati in Exchange Servizi di sicurezza

---

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).