أستكشاف أخطاء تكامل جدار الحماية الآمن مع تبادل خدمات الأمان وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء تكامل جدار الحماية الآمن من Cisco وإصلاحها باستخدام تبادل خدمات الأمان (SSX).

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- مركز إدارة جدار الحماية الآمن (FMC)
- جدار الحماية الآمن من Cisco

المكونات المستخدمة

- Cisco Secure Firewall - 7.6.0
- مركز إدارة جدار الحماية الآمن (FMC) - 7.6.0
- تبادل خدمات الأمان (SSX)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

أستكشاف الأخطاء وإصلاحها

الاتصال

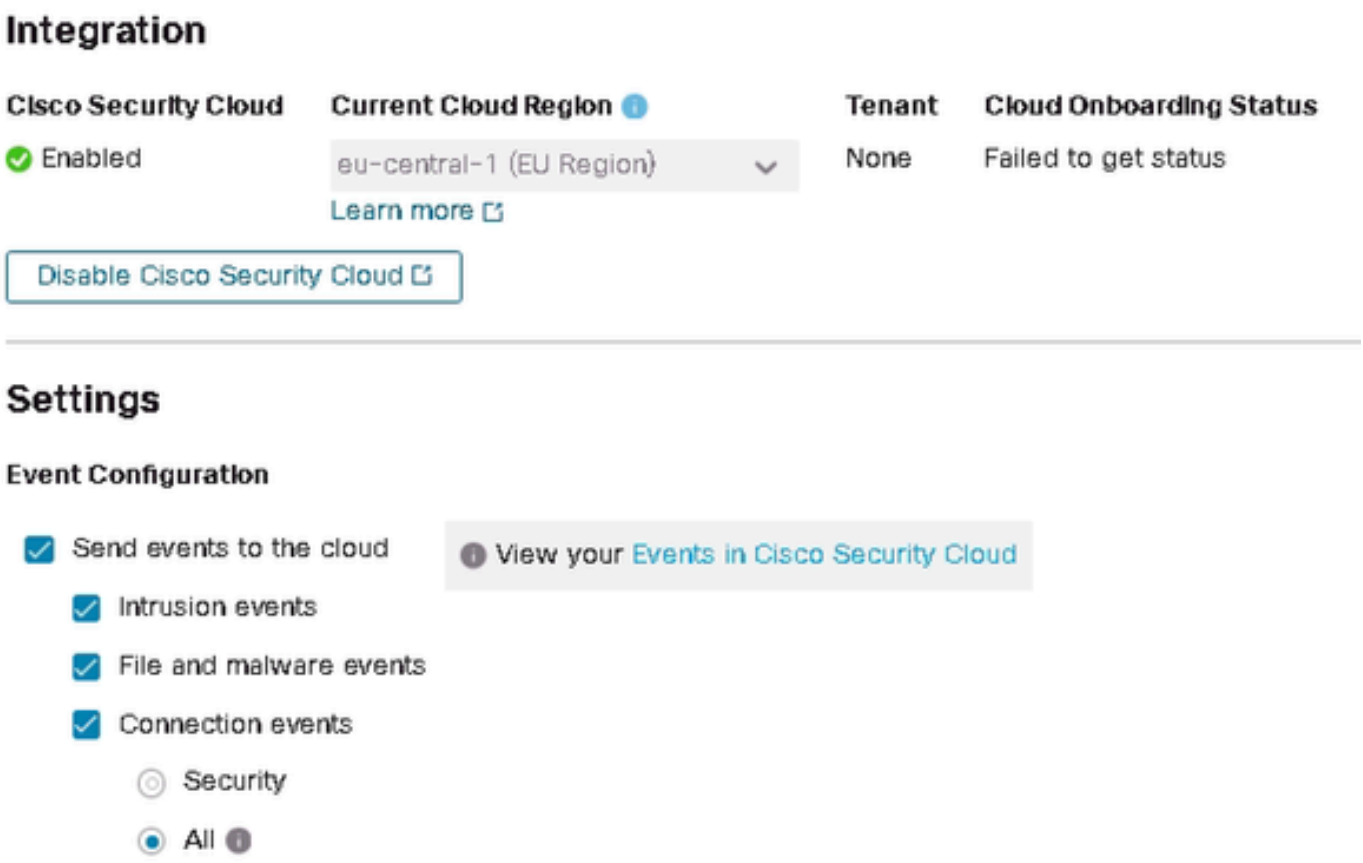
المتطلب الرئيسي هو السماح لحركة مرور HTTPS تجاه هذه العناوين من جهاز التسجيل:

- المنطقة الأمريكية:
  - 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
- منطقة الاتحاد الأوروبي:
  - 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
- منطقة آسيا (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

- منطقة اوستراليا:
  - 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
- منطقة الهند:
  - 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

التسجيل

يتم تسجيل جدار الحماية الآمن إلى تبادل خدمات الأمان في مركز إدارة جدار الحماية الآمن، في الدمج > Cisco Security Cloud.



تشير هذه المخرجات إلى اتصال ناجح تم إنشاؤه إلى 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)
```

يتم تخزين سجلات التسجيل في /var/log/connector/.

التحقق من التسجيل

بمجرد نجاح التسجيل على جانب "جدار الحماية الآمن"، يمكن إجراء إستدعاء API إلى المضيف المحلي:8989/v1/context/default/tenant للحصول على اسم ومعرف مستأجر 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"}]}

التحقق من جانب تبادل خدمات الأمان

في Security Services Exchange انتقل إلى اسم المستخدم الموجود في الركن العلوي الأيسر وانقر فوق ملف تعريف المستخدم لتأكيد تطابق معرف الحساب مع معرف المستأجر الذي تم الحصول عليه من قبل في جدار الحماية الآمن.

في علامة التبويب خدمات السحابة، يلزم أن يكون Eventing متاحا. أيضا، يجب تشغيل محول Cisco XDR في حالة إستخدام هذا الحل.

تحتوي علامة التبويب الأجهزة على قائمة بالأجهزة المسجلة.

مدخل لكل جهاز قابل للتوسيع ويحتوي على المعلومات التالية:

- معرف الجهاز - في حالة جدار الحماية الآمن، يمكن العثور على هذا المعرف من خلال الاستعلام عن curl -s http://localhost:8989/v1/contexts/default | GREP DeviceId
- تاريخ التسجيل
- عنوان IP
- إصدار موصل SSX
- آخر تعديل

الأحداث

تسمح لنا علامة التبويب الأحداث بتنفيذ الإجراءات على البيانات التي تم إرسالها بواسطة "جدار الحماية الآمن" والتي تمت معالجتها وعرضها في "تبادل خدمات الأمان".

1. تصفية قائمة الأحداث وإنشاء عوامل التصفية وحفظها،
2. إظهار أعمدة الجدول الإضافية أو إخفاؤها،
3. مراجعة الأحداث المرسلة من أجهزة جدار الحماية الآمن.

في الدمج بين جدار الحماية الآمن وخدمات الأمان تبادل خدمات الأمان يتم دعم أنواع الأحداث التالية:

نوع الحدث	نسخة جهاز الدفاع المدعومة للتكامل المباشر	إصدار جهاز الدفاع عن التهديد المدعوم لتكامل Syslog
أحداث التطفل	6.4 ومتأخر	6.3 والإصدارات اللاحقة
أحداث اتصال ذات أولوية عالية: • أحداث الاتصال المتعلقة بالأمان. • أحداث الاتصال المتعلقة بأحداث الملفات والبرامج الضارة. • أحداث الاتصال المتعلقة بأحداث التطفل.	الإصدار 6.5 والإصدارات الأحدث	غير مدعومة
أحداث الملفات والبرامج الضارة	الإصدار 6.5 والإصدارات الأحدث	غير مدعومة

أستكشاف الأحداث وإصلاحها التي لم تتم معالجتها في تبادل خدمات الأمان

في حالة مراقبة أحداث معينة في "مركز إدارة جدار الحماية الآمن"، يمكن الطلب لتحديد ما إذا

كانت الأحداث تتطابق مع الشروط (كل الملفات/البرامج المتعلقة بأحداث التطفل والملفات المكتشفة في تبادل خدمات الأمان والتي سيتم معالجتها وعرضها في الواجهة الرسومية).

تأكيد إرسال الأحداث إلى السحابة عن طريق الاستعلام عن localhost:8989/v1/contexts/default عن السحابة أم لا. يمكن تحديد ما إذا كانت الأحداث يتم إرسالها إلى السحابة

<#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

...

TotalEventsReceived يعني عدد الأحداث المتلقاة في الأحداث القابلة للتطبيق للإرسال إلى "تبادل خدمات الأمان" التي تمت معالجتها بواسطة "جدار الحماية الآمن".

TotalEventsSent يعني عدد الأحداث التي تم إرسالها في الأحداث التي تم إرسالها إلى Cisco Cloud.

في حالة الأحداث التي يتم رؤيتها في مركز إدارة جدار الحماية الآمن، ولكن ليس في تبادل خدمات الأمان، يجب التحقق من سجلات الأحداث المتوفرة في /ngfw/var/sf/detection_engines/<engine>/.

استنادا إلى سجل حدث محدد لفك ترميز الطابع الزمني باستخدام 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
```

- أحداث التطفل

تتم معالجة جميع أحداث التطفل وعرضها في كل من SSX و XDR. تأكد من إحتواء حدث معين في السجلات التي تم فك ترميزها على عالمة:

<#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
```

- أحداث الملفات والبرامج الضارة

استنادا إلى متطلبات النظام الأساسي لتبادل خدمات الأمان، تتم معالجة الأحداث ذات النوع الفرعي للحدث المحدد وعرضها فقط.

<#root>

```
"FileEvent":
 {
   “Subtypes”:
   {
     “FileLog”:
     {
     “Unified2ID”: 500,
     “SyslogID”: 430004
     },
 “FileMalware”:
     {
 “Unified2ID”: 502,
```

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

لذلك، يبدو في هذه السجلات المشفرة:

<#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
```

- أحداث الاتصال

فيما يتعلق بأحداث الاتصال، لا توجد أنواع فرعية. ومع ذلك، إذا كان حدث الاتصال يحتوي على أي من هذه الحقول، فإنه يعتبر حدث إستخبارات أمنية ويتم معالجته بشكل أكبر في تبادل خدمات الأمان.

· URL_SI_Category

· DNS_SI_Category

· IP_REPUTATIONsi_Category

ملاحظة: إذا كانت أحداث "الملف/البرامج الضارة" أو "الاتصال" التي تمت رؤيتها في "مركز إدارة جدار الحماية الآمن" لا تحتوي على الأنواع الفرعية أو المعلومات المذكورة في سجلات "الأحداث الموحدة" التي تم فك ترميزها باستخدام ميزة U2Dump، فهذا يعني أنه لم تتم معالجة هذه الأحداث المحددة وعرضها في تبادل خدمات الأمان

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).