أستكشاف أخطاء SecureX وإصلاحها باستخدام جدار الحماية الآمن 7.1 والإصدارات الأقدم

المحتويات

المقدمة

يصف هذا المستند المشاكل المتعلقة ب SecureX مع دمج جدار الحماية الآمن من Cisco - الإصدارات 7.1 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- مركز إدارة Firepower (FMC)
- جدار الحماية الآمن من Cisco
- المحاكاة الافتراضية الاختيارية للصور

المكونات المستخدمة

- Cisco Secure Firewall - 6.5
- مركز إدارة Firepower (FMC) - 6.5
- تبادل خدمات الأمان (SSE)
- SecureX
- وابة الترخيص Smart
- الاستجابة للتهديدات من Cisco (CTR)

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

اكتشاف مشاكل الاتصال

يمكنك اكتشاف مشاكل اتصال عامة من **action_queue.log** ملف. في حالات الفشل، يمكنك رؤية مثل هذه السجلات الموجودة في الملف:

```
ActionQueueScrape pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --
connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --capath
/ngfw/etc/sf/keys/fireamp/thawte_roots -f
https://api.eu.sse.itd.cisco.com/providers/sse/api/v1/regions) Failed, curl returned 28 at
/ngfw/usr/local/sf/lib/perl/5.10.1/SF/System.pmline 10477.
```

في هذه الحالة، يعني **الرمز** 28 انتهاء مهلة العملية والتحقق من الاتصال بالإنترنت.

هناك أيضا **الرمز** 6 الذي يعني مشاكل في تحليل DNS

مشكلات الاتصال بسبب تحليل خادم اسم المجال (DNS)

الخطوة 1. تحقق من أن الاتصال يعمل بشكل صحيح.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

تظهر المخرجات أن الجهاز غير قادر على حل URL .

في هذه الحالة، تحقق من تكوين خادم DNS المناسب. يمكن التحقق من صحته باستخدام **nslookup** من CLI الخبير:

```
root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached
```

يظهر الإخراج أنه لم يتم الوصول إلى DNS الذي تم تكوينه. لتأكيد إعدادات DNS، أستخدم **show network** :

```
> show network
===============[ System Information ]===============
Hostname : ftd01
DNS Servers : x.x.x.10
Management port : 8305
IPv4 Default route
Gateway : x.x.x.1

=====================[ eth0 ]=====================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : x:x:x:x:9D:A5
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : x.x.x.27
```

```
Netmask : 255.255.255.0
Broadcast : x.x.x.255
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ Proxy Information ]================
State : Disabled
Authentication : Disabled
```

في هذا المثال، تم إستخدام خادم DNS غير الصحيح. تغيير إعدادات DNS باستخدام هذا الأمر:

```
> configure network dns x.x.x.11
```

وبعد ذلك، يمكن إختبار الاتصال مرة أخرى. هذه المرة، نجح الاتصال.

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
```

```
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

مشاكل التسجيل إلى بوابة SSE

كل من FMC و **Cisco Secure Firewall** يلزم وجود اتصال بمحددات مواقع المعلومات (URL) الخاصة ب SSE على واجهة الإدارة الخاصة بها.

لاختبار الاتصال، أدخل هذه الأوامر على **Firepower CLI** مع الوصول الجذري:

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

يمكن تجاوز التحقق من الشهادة بهذا الأمر:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
```

```
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; ,;
```

ملاحظة: 403 Forbidden الرسالة تعني أن المعلمات المرسلة من الاختبار ليست ما يتوقعه SSE، ولكن هذا يثبت بما فيه الكفاية للتحقق من الاتصال.

التحقق من حالة SsecConnector

تحقق من خصائص الموصل كما هو موضح.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

للتحقق من الاتصال بين SSEConnector و EventHandler، أستخدم هذا الأمر. هذا مثال على اتصال سيئ:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

في مثال الاتصال الثابت، تحقق من اتصال حالة الدفق:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

التحقق من البيانات المرسلة إلى بوابة SSE و CTR

للإرسال أحداث من جهاز جدار الحماية الآمن من Cisco إلى SSE، يلزم إنشاء اتصال TCP مع https://eventing-ingest.sse.itd.cisco.com

هذا مثال على اتصال لم يتم إنشاؤه بين بوابة SSE وجدار حماية Cisco الآمن:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

في **connector.log** السجلات:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
```

```
events:connectWebSocket] dial tcp x.x.x.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp x.x.x.234:443: getsockopt: connection timed out"
```

ملاحظة: لاحظ أن عناوين IP المعروضة x.x.x.246 و 1x.x.x.246 تنتمي إلى https://eventing-ingest.sse.itd.cisco.com يحتمل أن يتم تغييرها. تتمثل التوصية في السماح بحركة المرور إلى مدخل SSE استنادا إلى URL بدلا من عناوين IP.

إذا لم يتم إنشاء هذا الاتصال، فلن يتم إرسال الأحداث إلى بوابة SSE. هذا مثال على اتصال ثابت بين جدار الحماية الآمن من Cisco وبوابة SSE:

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP x.x.x.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

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).