Risoluzione dei problemi relativi a SecureX con Secure Firewall 7.1 e versioni precedenti

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Risoluzione dei problemi

- Rileva problemi di connettività
- Problemi di connettività dovuti alla risoluzione DNS (Domain Name Server)

Introduzione

In questo documento vengono descritti i problemi relativi a SecureX con l'integrazione di Cisco Secure Firewall - versioni 7.1 e precedenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center (FMC)
- Cisco Secure Firewall
- Virtualizzazione delle immagini opzionale

Componenti usati

- Cisco Secure Firewall - 6.5
- Firepower Management Center (FMC) - 6.5
- SSE (Security Services Exchange)
- SecureX
- Portale delle licenze Smart
- Cisco Threat Response (CTR)

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

Rileva problemi di connettività

È possibile rilevare problemi di connettività generici dal **action_queue.log** file. In caso di errori, è possibile visualizzare tali registri nel file:

ActionQueueScrape pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 10

In questo caso, **il codice 28** indica che l'operazione è scaduta e che è stata verificata la connettività a Internet.

C'è anche il **codice 6** che significa problemi con la risoluzione DNS

Problemi di connettività dovuti alla risoluzione DNS (Domain Name Server)

Passaggio 1. Verificare che la connettività funzioni correttamente.

```
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'
```

L'output mostra che il dispositivo non è in grado di risolvere l'URL .

In questo caso, verificare che sia configurato il server DNS corretto. Può essere convalidato con una richiesta **nslookup** dalla CLI degli esperti:

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

L'output mostra che il DNS configurato non è raggiunto. Per confermare le impostazioni DNS, utilizzare il **show network** comando:

```
> 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
```

In questo esempio è stato utilizzato il server DNS errato. Modificare le impostazioni DNS con questo comando:

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

In seguito, sarà possibile testare nuovamente la connettività. Questa volta, la connessione è riuscita.

```
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;

Problemi di registrazione nel portale SSE

Sia FMC che **Cisco Secure Firewall** necessitano di una connessione agli URL SSE sull'interfaccia di gestione.

Per eseguire il test della connessione, immettere i seguenti comandi sul comando **Firepower CLI** con accesso root:

<#root>

curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/

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

Il controllo del certificato può essere ignorato con questo comando:

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; ,;
```

Nota: il **403 Forbidden** messaggio indica che i parametri inviati dal test non sono quelli previsti da SSE, ma questo è sufficiente per convalidare la connettività.

Verifica stato SSEConnector

Verificare le proprietà del connettore come illustrato.

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

Per verificare la connettività tra SSEConnector e EventHandler, utilizzare questo comando. Questo è un esempio di connessione errata:

```
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
```

Nell'esempio di una connessione stabilita, verificare che lo stato del flusso sia connected (connesso):

```
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
```

Verifica dei dati inviati al portale SSE e al CTR

Per inviare eventi dal dispositivo Cisco Secure Firewall a SSE, è necessario stabilire una connessione TCP con **https://eventing-ingest.sse.itd.cisco.com**

Questo è un esempio di connessione non stabilita tra il portale SSE e Cisco Secure Firewall:

```
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)
```

Nei **connector.log** registri:

```
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: ge
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: g
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: g
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: g
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: g
```

Nota: si noti che gli indirizzi IP visualizzati x.x.x.246 e 1x.x.x.246 appartengono a **https://eventing-ingest.sse.itd.cisco.com e** potrebbero essere modificati. Si consiglia di consentire il traffico sul portale SSE in base all'URL anziché agli indirizzi IP.

Se la connessione non viene stabilita, gli eventi non vengono inviati al portale SSE. Questo è un esempio di connessione stabilita tra Ciscp Secure Firewall e il portale 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)
```

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).