Integration und Fehlerbehebung von SecureX mit Firepower Threat Defense (FTD)

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten **Konfiguration** Lizenzierung Verknüpfen Sie Ihre Konten mit SSE, und registrieren Sie die Geräte. Registrierung der Geräte für SSE Konfigurieren benutzerdefinierter Dashboards auf SecureX Überprüfung Fehlerbehebung Erkennen von Verbindungsproblemen Verbindungsprobleme aufgrund der DNS-Auflösung Registrierungsprobleme beim SSE-Portal Überprüfung des Status von SSEConnector Überprüfung der an das SSE-Portal und CTR gesendeten Daten Video

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zur Integration, Verifizierung und Fehlerbehebung von SecureX mit Firepower Firepower Threat Defense (FTD).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Management Center (FMC)
- FirePOWER Threat Defense (FTD)
- Optionale Virtualisierung von Bildern

Verwendete Komponenten

- Firepower Threat Defense (FTD) 6.5
- FirePOWER Management Center (FMC) 6.5
- Security Services Exchange (SSE)
- SecureX

• Smart-Lizenzportal

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Lizenzierung

Rollen virtueller Kunden:

Nur der Virtual Account Admin oder der Smart Account Admin haben die Berechtigung, das Smart Account mit dem SSE-Konto zu verknüpfen.

Schritt 1: Um die Smart Account-Rolle zu validieren, navigieren Sie zu **software.cisco.com**, und wählen Sie im **Administrationsmenü die Option Smart Account verwalten aus**.



Schritt 2: Um die Benutzerrolle zu validieren, navigieren Sie zu **Users**, und überprüfen Sie, ob unter Roles (Rollen) die Konten auf Virtual Account Administrator (Virtual Account Administrator) festgelegt sind, wie im Bild gezeigt.

Cisco So	Zisco Software Central > Manage Smart Account > Users									
Account	Account Properties Virtual Accounts Users Custom Tags Requests Account Agreements Event Log									
Users	Users									
Use	user Groups									
	Add Users Remov	re Selected Export Selected			_					
	User ↑	Email	Organization	Account Access	F	Role	User Group	Actions		
	danieben				•		•	•		
	Daniel Benitez danleben	danieben@cisco.com	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	s V	Smart Account Administrator Virtual Account Administrator		Remove		
	1 User									

Schritt 3: Stellen Sie sicher, dass das Virtual Account (Virtuelles Konto), das für die Verknüpfung auf SSE ausgewählt ist, die Lizenz für die Sicherheitsgeräte enthält, wenn ein Konto, das keine Sicherheitslizenz enthält, auf SSE verknüpft ist, die Sicherheitsgeräte und das Ereignis nicht im SSE-Portal angezeigt werden.

8	Inventory Convert to Smart Licensing Reports	Preferences On-Prem Acco	ounts Activity			
ua	I Account: Mex-AMP TAC -	set Log				13 Minor Hide /
,0	Wailable Actions + Manage License Tags	License Reservation	G		Search by License	By Name By Ta
	License	Billing	Purchased	In Use	Balance Alerts	Actions
	FPR1010 URL Filtering	Prepaid	10	0	+ 10	Actions
	FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1	Actions
	FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1	Actions
	FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1	Actions
	HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2	Actions
	ISE Apex Session Licenses	Prepaid	1	0	+ 1	Actions
	ISE Base Session Licenses	Prepaid	10	0	+ 10	Actions
	ISE Plus License	Prepaid	10	0	+ 10	Actions
	Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9	Actions
	Terrest Defense With all Terrest Protection	Prepaid	10		+ 9	Actions

Schritt 4: Um zu überprüfen, ob das FMC für das richtige virtuelle Konto registriert wurde, navigieren Sie zu **System>Licenses>Smart License (System > Lizenzen > Smart License):**

Smart License Status			Cisco Smart Software Manager	
Usage Authorization:	0	Authorized (Last Synchronized On Jun 10 2020)		
Product Registration:	0	Registered (Last Renewed On Jun 10 2020)		
Assigned Virtual Account:		Mex-AMP TAC		
Export-Controlled Features:		Enabled		
Cisco Success Network:		Enabled (1)		
Cisco Support Diagnostics:		Disabled (1)		

Smart Licenses

License Type/Device Name	License Status							
> 🟳 Firepower Management Center Virtual (1)	0							
> 🔑 Base (1)	0							
> 🟳 Malware (1)	0							
> 🖓 Threat (1)	0							
> 🔑 URL Filtering (1)	0							
> 🖓 AnyConnect Apex (1)	0							
> 🖓 AnyConnect Plus (1)	0							
AnyConnect VPN Only (0)								
Note: Container Instances of same blade share feature licenses								

Verknüpfen Sie Ihre Konten mit SSE, und registrieren Sie die Geräte.

Schritt 1: Wenn Sie sich bei Ihrem SSE-Konto anmelden, müssen Sie Ihr Smart Account mit Ihrem SSE-Konto verknüpfen. Dazu müssen Sie auf das Toolsymbol klicken und Link Accounts auswählen.

0	*	Danie	l Benitez 🗸
Link Smart/Vir	tual Acco	unts	
Link CDO Acc	ount		
Downloads			
)

Sobald das Konto verknüpft ist, wird der Smart Account mit allen virtuellen Accounts auf dem Konto angezeigt.

Registrierung der Geräte für SSE

Schritt 1: Stellen Sie sicher, dass diese URLs in Ihrer Umgebung zugelassen sind:

Region USA

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

Region EU

- api.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com

Region APJ

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

Schritt 2: Melden Sie sich mit folgender URL beim SSE-Portal an: <u>https://admin.sse.itd.cisco.com,</u> navigieren Sie zu **Cloud Services,** und aktivieren Sie beide Optionen **Eventing** und **Cisco SecureX**, wie im nächsten Bild gezeigt:

CISCO Security Services Exchange	Devices Cloud Services Events Audit Log	
Cloud Services for Sourcefire Suppor		
	Cisco SecureX threat response Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.	•
	Eventing Eventing allows you to collect and view events in the cloud.	•

Schritt 3: Melden Sie sich beim FirePOWER Management Center an, navigieren Sie zu System>Integration>Cloud Services, aktivieren Sie Cisco Cloud Event Configuration und wählen Sie die Ereignisse aus, die Sie an die Cloud senden möchten:

Overview Analysis Policies Devices Objects AMP	Intelligence	Configuration Lieure Domaine Totogration	Deploy 0 System Help
Cloud Services Realms Identity Sources eStre	eamer Host Input Client Smart Software Satellite		
	URL Filtering Last URL Filtering Update: Nov 29, 2019 2:31 PM Update Now	AMP for Networks Last Local Malware Detection Update: Nov 28, 2019 3:31 PM	
	Enable Automatic Updates Query Cisco Cloud for Unknown URLs Cached URLs Expire Never C Discute URL categories and reputations	 Enable Automatic Local Malware Detection Updates Share URI from Malware Events with Cisco Use Legacy Port 32137 for AMP for Networks 	
	Save	Save	
	Cisco Cloud Region	Cisco Cloud Event Configuration	
	Region us-east-1 (US Region) This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.	 Send high priority Connection Events to the cloud Send File and Malware Events to the cloud Send Intrusion Events to the cloud Click here to view your Cisco Cloud configuration. Click here to view your events in Cisco Threat Response. 	
	Save	Save	

Schritt 4: Sie können zum SSE-Portal zurückkehren und überprüfen, ob jetzt die für SSE

angemeldeten Geräte angezeigt werden:

II-LIF Sacurity Services Exchange Devices Dend Services Events Audit Log									
Devices for Sou	Devices for Sourcefire Support								
Y (0, mer.x) 0 Rows Selected									
	35		Name A	Туре	Version	Status	Description		
	~	1	frepower	Cisco Firepower Threat Defense for VMWare	6.5.0	O Registered	27 frepower (FMC managed)		
	Created: 202	5/72e5//7 0-06-10 19:51:46 UTC	a	P Address 27			Connector Version:		
0	~	2	MEX-AMP-FMC	Cisco Firepower Management Center for VMW.	. 6.5.0	Registered	24 MDX-AMP-FMC		
	Created: 2020	c865776 0-06-10 20:17:37 UTC	2	P Address 24			Connector Version:		
Page Size: 25 ~	Total Entries: 2								

Die Ereignisse werden von den FTD-Geräten gesendet. Navigieren Sie zum **Event** im SSE-Portal, um die von den Geräten an SSE gesendeten Ereignisse zu überprüfen, wie im Bild gezeigt:

cisco	Isco Devices Exchange Devices Cloud Services Events Audit Log								• *		
Event Stream for Sourcefire Support											
	▼ Q. Enter filter criteria ~ 108/04/2020, 18:50 - 08/05/2020, 18:50 ×										
0	0 Rows Selected										
		Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Reporting Device ID	Source IP	
		Neutral	° No	.252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	09d441eedce5	100	
			° No	.145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	09d441eedce5	100	
		Unknown	° No	.100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	09d441eedce5	100	
		Neutral	° No	252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	09d441eedce5	100	

Konfigurieren benutzerdefinierter Dashboards auf SecureX

Schritt 1: Um Ihr Dashboard zu erstellen, klicken Sie auf das Symbol **+ New Dashboard** (Neues Dashboard). Wählen Sie einen Namen und eine Kachel aus, die Sie für das Dashboard verwenden möchten, wie im Bild gezeigt:

Create Dashboard	×
Dashboard Name	_
Test Dashboard	
Available Tiles	
> AMP Global Intelligence	
> AMP for Endpoints-mshukur (RO)	
> Email Security Appliance	
> Email Security Appliance esa03	
> E FMC 6.5.0	
> E Firepower	
> E Firepower - Mosterbe	
> E Firepower CSSP	
Firepower danieben	
Event Summary A set of metrics summarizing Firepower event activity in your organization	•
Incident Promotion Reason	
A set of metrics summarizing Firepower incident activity in your organization	•
Taios IP Reputation	
A set of metrics summarizing Talos disposition activity in your organization	•
Intrusion Top Attackers	-
List of top attackers for intrusion events in your organization	
Intrusion Top Targets	-
List of top targets for intrusion events in your organization	•
	Save

Schritt 2: Anschließend können Sie die von SSE aufgefüllten Dashboard-Informationen anzeigen. Sie können eine der erkannten Bedrohungen auswählen, und das SSE-Portal startet mit dem Ereignistypfilter:

Dashboard Integrations Orchestration Administration								
Applications & Integrations	Firepower + No	w Dashboard				Customize	Timeframe 🗸 🌒	News ->
 Applications 	Event Summary Fire	power danieben		Last 90 Days > I	Incident Promotion Reason Firepower daniebe	m	Last 90 Days > II	X Welcome to SecureX
Tr Launch					Talos Disposition (0)			Maximize your experience by reviewing these key topics:
	m 5.831	₩5.813	⊊18		User Promoted (0)			About SecureX
Sse Security Services Exchange	Total ES	Intrusion E3 Ma	alware El Security	Intelligence 🖾	Category: IP (0)			Configure Integrations Configure Dashboards and Tiles
 Wy leterarities 					Security Intelligence			Activate Orchestration
					Category: DNS (0)	14		Navigate SecureX
Amp Launch Links					Category: URL (0)			SecureX Ribbon
ALE for Enderlinks Edule					 Intrusion Rules Category (0) 			til: Cisco Security
Amp Launch Links					Malware Threat Score (0)			Securing the remote work erwironment
AMP for Endpoints-mshukur (RO) Launch Links					Custom IP Address (14)			As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?
AMP for Endpoints_segararo								Talos Intelligence
	0	۵ ۵	0	Ó,	۵ ۵۵ ۸	C	0 0	Threat Roundup for May 1 to May 8 Today, Talos is publishing a glimpse
Esa Links	Talos IP Reputation	Firepower danieben		Last 90 Days > II	Intrusion Top Attackers Firepower danieben		Last 30 Days > O E	into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn't meant to be an in
Esa Email Security Appliance - Pratham								Talos Intelligence
Links	¢0	€17 Ø1,8	19 ~0	+ 2,692				Vulnerability Spotlight: Remote code
Esa Email Security Appliance esa03 Links	Poor L3 Que:	stionable E3 Neutra	al 🖾 Favorable 🗅	Good 🗅				execution vulnerabilities in Adobe Cinco Talos recently discovered two remote code execution vulnerabilities in Adobe Acrobat Reader. Acrobat supports a number of features, including the ability to
Links								tat: Cisco Security
Secure 🗙 🏭 Home							111 🖪 🖻 🤉 🤇 Enter	logs, IPs, domains, etc. 🛛 🗔 🗘 +

Überprüfung

Überprüfen Sie, ob die FTDs Ereignisse (Malware oder Eindringversuche) generieren. Navigieren Sie zu Analyse>Dateien>Malware-Ereignisse, für Angriffsversuche navigieren Sie zu Analysis > Intrusion > Events.

Validieren Sie, ob die Ereignisse im SSE-Portal registriert werden, wie im Abschnitt 4 "Geräte für SSE registrieren" erwähnt.

Überprüfen Sie, ob Informationen im SecureX-Dashboard angezeigt werden, oder überprüfen Sie die API-Protokolle, damit Sie den Grund für einen möglichen API-Fehler sehen können.

Fehlerbehebung

Erkennen von Verbindungsproblemen

Sie können generische Verbindungsprobleme in der Datei action_queue.log erkennen. Im Fehlerfall werden solche Protokolle in der Datei angezeigt:

```
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.
```

In diesem Fall bedeutet Exit Code 28, dass der Vorgang abgelaufen ist, und wir sollten die Verbindung zum Internet überprüfen. Möglicherweise sehen Sie auch den Exitcode 6, was Probleme mit der DNS-Auflösung bedeutet.

Verbindungsprobleme aufgrund der DNS-Auflösung

Schritt 1: Überprüfen Sie, ob die Verbindung ordnungsgemäß funktioniert.

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'
Die obige Ausgabe zeigt dass das Gerät die URL htt

Die obige Ausgabe zeigt, dass das Gerät die URL <u>https://api-sse.cisco.com</u> nicht auflösen kann. In diesem Fall müssen wir überprüfen, ob der richtige DNS-Server konfiguriert ist. Sie kann mithilfe einer Instant-Übersetzung der CLI des Experten validiert werden:

root@ftd01:~# nslookup api-sse.cisco.com

;; connection timed out; no servers could be reached

Die obige Ausgabe zeigt, dass der konfigurierte DNS nicht erreicht ist. Verwenden Sie den Befehl show network (Netzwerk anzeigen), um die DNS-Einstellungen zu bestätigen:

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

In diesem Beispiel wurde der falsche DNS-Server verwendet. Sie können die DNS-Einstellungen mit dem folgenden Befehl ändern:

> configure network dns x.x.x.11
Nachdem diese Verbindung erneut getestet werden kann, ist die Verbindung erfolgreich.

```
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;</pre>
```

Registrierungsprobleme beim SSE-Portal

Sowohl FMC als auch FTD benötigen eine Verbindung zu den SSE-URLs ihrer Management-Schnittstelle. Um die Verbindung zu testen, geben Sie diese Befehle in der FirePOWER-CLI mit Root-Zugriff ein:

```
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
Die Zertifikatsüberprüfung kann mit dem folgenden Befehl umgangen werden:
```

```
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
anvwav.
>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;
```

Hinweis: Sie erhalten die 403 Forbidden-Meldung, da die vom Test gesendeten Parameter nicht den Erwartungen von SSE entsprechen, aber dies erweist sich als ausreichend, um die Verbindung zu validieren.

Überprüfung des Status von SSEConnector

Sie können die Anschlusseigenschaften wie gezeigt überprüfen.

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

Mit diesem Befehl können Sie die Verbindung zwischen dem SSConnector und dem EventHandler überprüfen. Dies ist ein Beispiel für eine fehlerhafte Verbindung:

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

Im Beispiel einer eingerichteten Verbindung sehen Sie, dass der Streamstatus verbunden ist:

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

Überprüfung der an das SSE-Portal und CTR gesendeten Daten

Um Ereignisse vom FTD-Gerät an SEE senden zu können, muss eine TCP-Verbindung mit

https://eventing-ingest.sse.itd.cisco.com eingerichtet werden. Dies ist ein Beispiel für eine Verbindung, die nicht zwischen dem SSE-Portal und dem FTD hergestellt wurde:

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)

In den Connector.log-Protokollen:

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.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"
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"
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"

Hinweis: Beachten Sie, dass die angezeigten IP-Adressen x.x.x.246 und 1x.x.x.246 <u>https://eventing-ingest.sse.itd.cisco.com</u> gehören können. Aus diesem Grund wird empfohlen, den Datenverkehr zum SSE-Portal anhand von URL anstelle von IP-Adressen zuzulassen.

Wenn diese Verbindung nicht hergestellt wird, werden die Ereignisse nicht an das SSE-Portal gesendet. Dies ist ein Beispiel für eine festgestellte Verbindung zwischen FTD und SSE-Portal:

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)

Video