Fehlerbehebung bei fehlgeschlagenen Sicherheitsinformations-Feed-Updates im Firepower Management Center

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Probleme mit Aktualisierungen des Sicherheitsinformations-Feeds beheben.

Hintergrund

Der Sicherheitsinformations-Feed besteht aus mehreren regelmäßig aktualisierten Listen von IP-Adressen mit schlechter Reputation, die von der Cisco Talos Security Intelligence and Research Group (Talos) ermittelt wurden. Der Intelligence Feed muss regelmäßig aktualisiert werden, damit ein Cisco FirePOWER-System aktuelle Informationen nutzen kann, um den Netzwerkverkehr zu filtern.

Voraussetzungen

Anforderungen

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

- Cisco FirePOWER Management Center
- Sicherheitsinformationen-Feed

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco FirePOWER Management Center, auf dem die Softwareversion 5.2 oder höher ausgeführt wird.

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 möglichen Auswirkungen aller Befehle kennen.

Problem

Fehler beim Aktualisieren des Sicherheitsinformations-Feeds. Sie können den Fehler entweder über die Web-GUI oder die CLI überprüfen (weitere Informationen hierzu finden Sie in den folgenden Abschnitten).

Überprüfen des Problems über die Web-Benutzeroberfläche

Wenn die Aktualisierung des Sicherheitsinformations-Feeds fehlschlägt, zeigt das FirePOWER Management Center Statuswarnungen an.

Überprüfen des Problems über die CLI

Geben Sie den folgenden Befehl in die CLI des FirePOWER Management Center ein, um die Ursache eines Update-Fehlers mit dem Sicherheitsinformations-Feed zu ermitteln:

```
admin@Sourcefire3D:~$ cat /var/log/messages
```

Suchen Sie in den Meldungen nach einer der folgenden Warnungen:

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

Lösung

Führen Sie die folgenden Schritte aus, um das Problem zu beheben:

1. Prüfen Sie, ob **intelligence.sourcefire.com** Standort ist aktiv. Navigieren Sie in einem Browser zu https://intelligence.sourcefire.com.

2. Zugriff auf die CLI des FirePOWER Management Center über Secure Shell (SSH)

3. Ping intelligence.sourcefire.com vom FirePOWER Management Center:

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verifyyou receive an output similar
   to this:
   ```

   ```
   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ifyou do not receive a
   response similar to that shown, then you can have an outbound connectivity issue, or you do
   not have a route to intelligence.sourcefire.com.
   ```

4. Auflösen des Hostnamens für intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com
```

Vergewissern Sie sich, dass Sie eine ähnliche Antwort erhalten:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

Hinweis: Die oben genannte Ausgabe verwendet als Beispiel den Google-DNS-Server (Public Domain Name System). Die Ausgabe hängt von den DNS-Einstellungen ab, die unter System > Local > Configuration konfiguriert wurden. **Network** Abschnitt. Wenn Sie keine Antwort erhalten, die der angezeigten ähnelt, stellen Sie sicher, dass die DNS-Einstellungen korrekt sind.Achtung: Der Server verwendet ein Rundlauf-IP-Adressenschema für Lastenausgleich, Fehlertoleranz und Betriebszeit. Aus diesem Grund können sich die IP-Adressen ändern. Cisco empfiehlt, die Firewall mit einem **CNAME** anstelle einer IP-Adresse.

5. Überprüfen Sie die Verbindung zu intelligence.sourcefire.com mithilfe von Telnet:

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

Überprüfen Sie, ob Sie eine Ausgabe ähnlich dieser erhalten:

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

Hinweis: Wenn Sie den zweiten Schritt erfolgreich abschließen können, aber nicht in der Lage sind, Telnet i**ntelligence.sourcefire.com** über Port 443 können Sie eine Firewall-Regel einrichten, die Port 443 für ausgehende intelligence.sourcefire.com.

6. Navigieren Sie zu System > Local > Configuration, und überprüfen Sie die Proxyeinstellungen des **Manual Proxy** Konfiguration unter **Network** Abschnitt.
Hinweis: Wenn dieser Proxy die SSL-Überprüfung (Secure Sockets Layer) durchführt, müssen Sie eine Umgehungsregel festlegen, die den Proxy für umgeht. **intelligence.sourcefire.com**.
7. Testen Sie, ob Sie HTTP GET Antrag auf intelligence.sourcefire.com:

```
admin@Firepower:~sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
```

```
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Hinweis: Das Smiley-Gesicht am Ende des curl gibt eine erfolgreiche Verbindung an.**Hinweis**: Wenn Sie einen Proxy verwenden, curl erfordert einen Benutzernamen. Der Befehl lautet **curl -U <Benutzer> -vvk** https://intelligence.sourcefire.com. Nachdem Sie den Befehl eingegeben haben, werden Sie aufgefordert, das Proxy-Kennwort einzugeben.

8. Vergewissern Sie sich, dass der HTTPS-Datenverkehr, der zum Herunterladen des Sicherheitsinformations-Feeds verwendet wird, nicht über einen SSL-Entschlüsseler verläuft. Um sicherzustellen, dass keine SSL-Entschlüsselung erfolgt, überprüfen Sie die Informationen des Serverzertifikats in der Ausgabe von Schritt 6. Wenn das Serverzertifikat nicht mit dem übereinstimmt, was im folgenden Beispiel angezeigt wird, können Sie einen SSL-Entschlüsseler verwenden, der das Zertifikat zurückweist. Wenn der Datenverkehr einen SSL-Entschlüsseler durchläuft, müssen Sie den gesamten Datenverkehr, der an intelligence.sourcefire.com.

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
```

```
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Hinweis: Die SSL-Entschlüsselung muss für den Sicherheitsinformations-Feed umgangen werden, da der SSL-Entschlüsseler dem FirePOWER Management Center ein unbekanntes Zertifikat im SSL-Handshake sendet. Das an das FirePOWER Management Center gesendete Zertifikat wird nicht von einer Sourcefire-vertrauenswürdigen Zertifizierungsstelle signiert, sodass die Verbindung nicht vertrauenswürdig ist.

Zugehörige Informationen

- Auto (automatisch)dramatisch Update-Fehler in einem FirePOWER Management Center herunterladen
- Erforderliche Serveradressen für AMP-Vorgänge (Advanced Malware Protection)
- Erforderliche Kommunikations-Ports für FirePOWER-Systembetrieb
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.