Dépannage des échecs de mise à jour du flux Security Intelligence sur Firepower Management Center

Table des matières

Introduction

Ce document décrit comment résoudre les problèmes liés aux mises à jour du flux Security Intelligence.

Fond

Le flux Security Intelligence se compose de plusieurs listes régulièrement mises à jour d'adresses IP qui ont une mauvaise réputation, comme déterminé par le groupe Cisco Talos Security Intelligence and Research (Talos). Il est important de mettre régulièrement à jour le flux d'informations pour qu'un système Cisco Firepower puisse utiliser des informations à jour afin de filtrer le trafic réseau.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center
- Flux Security Intelligence

Composants utilisés

Les informations contenues dans ce document sont basées sur un Cisco Firepower Management Center qui exécute le logiciel version 5.2 ou ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Une erreur de mise à jour du flux Security Intelligence se produit. Vous pouvez vérifier l'échec à l'aide de l'interface utilisateur graphique Web ou de l'interface de ligne de commande (expliquée plus en détail dans les sections suivantes).

Vérification du problème à partir de l'interface utilisateur graphique Web

En cas d'échec de la mise à jour du flux Security Intelligence, Firepower Management Center affiche des alertes d'intégrité.

Vérification du problème à partir de la CLI

Afin de déterminer la cause première d'un échec de mise à jour avec le flux Security Intelligence, entrez cette commande dans la CLI de Firepower Management Center :

<#root>

```
admin@Sourcefire3D:~$
```

cat /var/log/messages

Recherchez l'un de ces avertissements dans les messages :

```
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
```

Solution

Suivez ces étapes afin de résoudre ce problème :

1. Vérifiez que le **intelligence.sourcefire.com** Le site est actif. Accédez à https://intelligence.sourcefire.com dans un navigateur.

2. Accédez à l'interface de ligne de commande de Firepower Management Center par Secure Shell (SSH).

3. Ping intelligence.sourcefire.com depuis Firepower Management Center :

   <#root>

   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.verify

   you 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 simil

4. Résolvez le nom d'hôte pour intelligence.sourcefire.com:

   <#root>

   admin@Firepower:~$

   sudo

   nslookup intelligence.sourcefire.com

   Vérifiez que vous recevez une réponse similaire à celle-ci :

   ```
   Server: 8.8.8.8
   Address: 8.8.8.8#53

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

Remarque : le résultat ci-dessus utilise le serveur DNS (Public Domain Name System) de Google comme exemple. Le résultat dépend des paramètres DNS configurés dans System > Local > Configuration, sous le **Network** de l'Aide. Si vous ne recevez pas de réponse similaire à celle affichée, vérifiez que les paramètres DNS sont corrects.

> Attention : le serveur utilise un schéma d'adresses IP round-robin pour l'équilibrage de charge, la tolérance aux pannes et la disponibilité. Par conséquent, les adresses IP peuvent changer et Cisco recommande de configurer le pare-feu avec un **CNAME** au lieu d'une adresse IP.

5. Vérifiez la connectivité avec intelligence.sourcefire.com avec l'utilisation de Telnet :

<#root>

```
admin@Firepower:~$
```

sudo telnet intelligence.sourcefire.com 443

Vérifiez que vous recevez un résultat similaire à celui-ci :

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

> Remarque : si vous réussissez la deuxième étape mais que vous ne parvenez pas à établir une connexion Telnet avec i**ntelligence.sourcefire.com** sur le port 443, une règle de pare-feu peut bloquer le port 443 sortant pour intelligence.sourcefire.com.

6. Accédez à System > Local > Configuration et vérifiez les paramètres proxy de l' **Manual Proxy** configuration sous la **Network** de l'Aide.

> Remarque : si ce proxy effectue une inspection SSL (Secure Sockets Layer), vous devez mettre en place une règle de contournement qui contourne le proxy pour **intelligence.sourcefire.com.**

7. Testez si vous pouvez effectuer une HTTP GET demande contre intelligence.sourcefire.com:

<#root>

```
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
```

Remarque : le visage souriant à la fin de la curl indique que la connexion a réussi.

Remarque : si vous utilisez un proxy, le curl nécessite un nom d'utilisateur. La commande est curl -U <user> -vvk https://intelligence.sourcefire.com. En outre, après avoir entré la commande, vous êtes invité à entrer le mot de passe proxy.

---

8. Vérifiez que le trafic HTTPS utilisé pour télécharger le flux Security Intelligence ne passe pas par un déchiffreur SSL. Afin de vérifier qu'aucun déchiffrement SSL ne se produit, validez les informations de certificat de serveur dans le résultat de l'étape 6. Si le certificat du serveur ne correspond pas à ce qui est affiché dans l'exemple ci-dessous, vous pouvez disposer

d'un décrypteur SSL qui abandonne le certificat. Si le trafic passe par un décrypteur SSL, vous devez contourner tout le trafic qui va à intelligence.sourcefire.com.

<#root>

```
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
```

Remarque : le déchiffrement SSL doit être contourné pour le flux Security Intelligence, car le déchiffreur SSL envoie au Firepower Management Center un certificat inconnu dans la connexion SSL. Le certificat envoyé au Centre de gestion Firepower n'est pas signé par une autorité de certification de confiance Sourcefire, de sorte que la connexion n'est pas approuvée.

Informations connexes

- « Auto »pneumatique Échec de la mise à jour du téléchargement sur Firepower Management Center
- Adresses de serveur requises pour les opérations Advanced Malware Protection (AMP)
- Ports de communication requis pour le fonctionnement du système Firepower
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.