Dépannez les pannes de mise à jour de flux de renseignements de sécurité au centre de Gestion de FireSIGHT

Contenu

Introduction

Ce document décrit comment dépanner des questions avec des mises à jour de flux de renseignements de sécurité. Le flux de renseignements de sécurité est composé de plusieurs listes d'adresses IP régulièrement à jour qui ont des réputations pauvres, comme déterminé par les renseignements de sécurité de Cisco Talos et l'organisme de recherche (Talos). Il est important de conserver le flux d'intelligence régulièrement mis à jour de sorte qu'un système de Cisco FireSIGHT puisse employer les informations à jour afin de filtrer votre trafic réseau.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Centre de Gestion de Cisco FireSIGHT
- Flux de renseignements de sécurité

Composants utilisés

Les informations dans ce document sont basées sur un centre de Gestion de Cisco FireSIGHT qui exécute la version de logiciel 5.2 ou plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Une panne de mise à jour de flux de renseignements de sécurité se produit. Vous pouvez vérifier la panne par l'intermédiaire du GUI de Web ou du CLI (expliqué plus loin dans les sections qui suivent).

Vérifiez le problème du GUI de Web

Quand la panne de mise à jour de flux de renseignements de sécurité se produit, le centre de Gestion de FireSIGHT affiche des alertes de santés.

Vérifiez le problème du CLI

Afin de déterminer la cause principale d'une panne de mise à jour avec le flux de renseignements de sécurité, sélectionnez cette commande dans le CLI du centre de Gestion de FireSIGHT :

```
admin@Sourcefire3D:~$

cat /var/log/messages
```

Recherchez l'un ou l'autre 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 site d'*intelligence.sourcefire.com* est en activité. Naviguez vers https://intelligence.sourcefire.comin un navigateur. Vous devriez recevoir une face souriante, qui indique que le site est vivant.

2. Accédez au CLI du centre de Gestion de FireSIGHT par l'intermédiaire du Protocole Secure Shell (SSH).

3. Ping *intelligence.sourcefire.com du* centre de Gestion de FireSIGHT :

   ```
   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.com
   ```

   Vous devriez recevoir un résultat semblable à ceci :

   ```
   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ms
   ```

   Si vous ne recevez pas une réponse semblable à cela affichée, alors vous pourriez avoir un

problème de connectivité sortant ou vous n'avez pas une artère à *intelligence.sourcefire.com.*

4. Résolvez l'adresse Internet pour *intelligence.sourcefire.com* :

```
admin@Firepower:~$

sudo

nslookup intelligence.sourcefire.com
```

Vous devriez recevoir une réponse semblable à ceci :

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

Note: La sortie mentionnée ci-dessus utilise le serveur de Name System de domaine public de Google (DN) comme exemple. La sortie dépend des configurations de DN qui sont configurées dans le **système > les gens du pays > la configuration**, sous la section de *réseau*. Si vous ne recevez pas une réponse semblable à cela affichée, alors assurez-vous que les configurations de DN sont correctes.**Attention** : Le serveur utilise un schéma circulaire d'adresse IP pour l'Équilibrage de charge, la tolérance aux pannes, et la disponibilité. Par conséquent, les adresses IP pourraient changer, et Cisco recommande que le Pare-feu soit configuré avec un *CNAME* au lieu d'une adresse IP.

5. Vérifiez la Connectivité à *intelligence.sourcefire.com* avec l'utilisation du telnet :

```
admin@Firepower:~$

 sudo telnet intelligence.sourcefire.com 443
```

Vous devriez recevoir un résultat semblable à ceci :

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

Note: Si vous pouvez se terminer la deuxième étape avec succès mais ne pouvez pas au telnet à *intelligence.sourcefire.com* au-dessus du port 443, vous pourriez avoir une règle de Pare-feu qui bloque le port 443 sortant pour *intelligence.sourcefire.com*.

6. Naviguez vers le **système > les gens du pays > la configuration** et vérifiez les paramètres de proxy de la *configuration de proxy manuelle* sous la section de *réseau*.
Note: Si ce proxy fait l'inspection de Secure Sockets Layer (SSL), vous devez mettre en place une règle de contournement que saute le proxy pour *intelligence.sourcefire.com*.
7. Testez si vous pouvez effectuer une *requête HTTP GET* contre *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
```

Note: La face souriante à l'extrémité de la sortie de commande de *boucle* indique une connexion réussie.**Note**: Si vous utilisez un proxy, la commande de *boucle* exige un nom d'utilisateur. La commande sera **boucle - <user> U - vvk** https://intelligence.sourcefire.com. Supplémentaire, après que vous sélectionniez la commande, vous êtes incité entrez le mot de passe de proxy.

8. Vérifiez que le trafic HTTPS qui est utilisé afin de télécharger le flux de renseignements de sécurité ne traverse pas un decryptor SSL. Afin de vérifier qu'aucun déchiffrement SSL ne se produit, validez les informations de certificat de serveur dans la sortie de l'étape 6. Si le certificat de serveur n'apparie pas cela affiché dans l'exemple qui suit, alors vous pourriez avoir un decryptor SSL qui démissionne le certificat. Si le trafic traverse un decryptor SSL, vous devez sauter tout les trafic qui va à *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
```

Note: Le déchiffrement SSL doit être sauté pour le flux de renseignements de sécurité parce que le decryptor SSL envoie au centre de Gestion de FireSIGHT un certificat inconnu dans la prise de contact SSL. Le certificat qui est envoyé au centre de Gestion de FireSIGHT n'est pas signé par un CA Sourcefire-fait confiance, ainsi la connexion est non approuvé.

Informations connexes

- Panne automatique de mise à jour de téléchargement à un centre de Gestion de FireSIGHT
- Adresses du serveur requises pour des exécutions avancées de protection de malware (AMP)
- Ports de transmission requis pour l'exploitation du système de FireSIGHT
- Support et documentation techniques - Cisco Systems