Problemen oplossen bij het bijwerken van de security intelligentie op het Firepower Management Center

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met de updates van Security Intelligence.

Achtergrond

De Security Intelligence Feed bestaat uit verschillende regelmatig bijgewerkte lijsten van IP-adressen met een slechte reputatie, zoals bepaald door de Cisco Talos Security Intelligence and Research Group (Talos). Het is belangrijk dat de intelligentiefeed regelmatig wordt bijgewerkt, zodat een Cisco Firepower System actuele informatie kan gebruiken om uw netwerkverkeer te filteren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firepower Management Center
- Security Intelligence-feed

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco Firepower Management Center dat software versie 5.2 of hoger uitvoert.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Er is een fout opgetreden in de update van de Security Intelligence. U kunt de fout verifiëren via de web GUI of de CLI (zie de volgende secties voor meer informatie).

Controleer het probleem via de Web GUI

Wanneer de updatefout van de Security Intelligence optreedt, wordt in het Firepower Management Center gezondheidswaarschuwingen weergegeven.

Controleer het probleem vanuit de CLI

Voer deze opdracht in de CLI van het Firepower Management Center om de basisoorzaak van een update met de Security Intelligence Feed te achterhalen:

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

Zoek naar een van deze waarschuwingen in de berichten:

```
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
```

Oplossing

Voltooi de volgende stappen om het probleem op te lossen:

1. Controleer of de **intelligence.sourcefire.com** site is actief. Navigeer naar https://intelligence.sourcefire.comin een browser.

2. Toegang tot de CLI van het Firepower Management Center door Secure Shell (SSH).

3. Ping intelligence.sourcefire.com Vanuit 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. Los de hostnaam op voor intelligence.sourcefire.com:

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

Controleer of u een soortgelijke reactie hebt ontvangen:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

Opmerking: De eerder genoemde uitvoer gebruikt bijvoorbeeld de server van Google Public Domain Name System (DNS). De uitvoer is afhankelijk van de DNS-instellingen die zijn geconfigureerd in **System > Local > Configuration**, onder de **Network** doorsnede. Als u geen reactie ontvangt gelijkend op die getoond, dan zorg ervoor dat de DNS instellingen correct zijn.**Waarschuwing**: de server maakt gebruik van een round-robin IP-adresschema voor taakverdeling, fouttolerantie en uptime. Daarom kunnen de IP-adressen worden gewijzigd en Cisco raadt aan de firewall met een **CNAME** in plaats van een IP adres.

5. Controleer de aansluitingen op intelligence.sourcefire.com met het gebruik van Telnet:

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

Controleer of u een uitvoer ontvangt die vergelijkbaar is met deze:

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

Opmerking: als u de tweede stap succesvol kunt uitvoeren maar er niet in kunt slagen om Telnet te gebruiken i**ntelligence.sourcefire.com** via poort 443 kunt u een firewallregel hebben die poort 443 uitgaand blokkeert voor intelligence.sourcefire.com.

6. Navigeer naar **Systeem > Lokaal > Configuratie** en controleer de proxy-instellingen van het **Manual Proxy** configuratie onder de **Network** doorsnede.
   Opmerking: als deze proxy Secure Sockets Layer (SSL)-inspectie uitvoert, moet u een omzeilingsregel invoeren die de proxy voor **intelligence.sourcefire.com**.
7. Testen als u een HTTP GET verzoek tegen 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
```

Opmerking: Het smiley gezicht aan het einde van de curl opdrachtoutput geeft een succesvolle verbinding aan.**Opmerking**: als u een proxy gebruikt, curl Het bevel vereist een gebruikersbenaming. De opdracht is **curl -U <user> -vvk** https://intelligence.sourcefire.com. Bovendien, nadat u het bevel ingaat, wordt u ertoe aangezet om het volmachtswachtwoord in te gaan.

8. Controleer of het HTTPS-verkeer dat wordt gebruikt om de Security Intelligence-feed te downloaden, niet via een SSL-decryptor verloopt. Om te controleren of er geen SSL-decryptie optreedt, valideert u de informatie over het servercertificaat in de uitvoer van stap 6. Als het Servercertificaat niet overeenkomt met wat in het volgende voorbeeld wordt weergegeven, kunt u een SSL-decryptor hebben die het certificaat afgeeft. Als het verkeer door een SSL-decryptor loopt, moet u al het verkeer dat naar 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
```

Opmerking: de SSL-decryptie moet worden overgeslagen voor de Security Intelligence Feed omdat de SSL-decryptor het Firepower Management Center een onbekend certificaat in de SSL-handdruk stuurt. Het certificaat dat naar het Firepower Management Center wordt verzonden, is niet ondertekend door een op Sourcefire vertrouwde certificeringsinstantie, zodat de verbinding niet betrouwbaar is.

Gerelateerde informatie

- Automatiek Downloadupdate mislukking op een Firepower Management Center
- Vereiste serveradressen voor Advanced Malware Protection (AMP)
- Vereiste communicatiepoorten voor de werking van het FirePOWER System
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.