Risoluzione dei problemi relativi agli errori di aggiornamento dei feed di Security Intelligence in Firepower Management Center

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli aggiornamenti dei feed di Security Intelligence.

Sfondo

Il feed di intelligence per la sicurezza è composto da diversi elenchi di indirizzi IP con reputazione scadente aggiornati regolarmente, come determinato dal Cisco Talos Security Intelligence and Research Group (Talos). È importante mantenere il feed di intelligence aggiornato regolarmente in modo che un sistema Cisco Firepower possa usare le informazioni aggiornate per filtrare il traffico della rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center
- Feed per la Security Intelligence

Componenti usati

Per questo documento, è stato usato un Cisco Firepower Management Center con software versione 5.2 o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Si è verificato un errore di aggiornamento del feed di Security Intelligence. È possibile verificare l'errore dalla GUI Web o dalla CLI (illustrata più avanti nelle sezioni che seguono).

Verifica del problema dalla GUI Web

Quando si verifica un errore durante l'aggiornamento del feed di Security Intelligence, Firepower Management Center visualizza gli avvisi di integrità.

Verifica del problema dalla CLI

Per determinare la causa principale di un errore di aggiornamento con il feed di Security Intelligence, immettere questo comando nella CLI di Firepower Management Center:

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

Cercare uno di questi avvisi nei messaggi:

```
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
```

Soluzione

Per risolvere il problema, completare i seguenti passaggi:

1. Verificare che il **intelligence.sourcefire.com** è attivo. Passare a https://intelligence.sourcefire.com in un browser.

2. Accedere alla CLI di Firepower Management Center tramite Secure Shell (SSH).

3. Ping intelligence.sourcefire.com da 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. Risolvi il nome host per intelligence.sourcefire.com:

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

Verificare di aver ricevuto una risposta simile alla seguente:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

Nota: nell'output sopra riportato viene utilizzato come esempio il server DNS (Public Domain Name System) di Google. L'output dipende dalle impostazioni DNS configurate in **Sistema > Locale > Configurazione**, in **Network** sezione. Se non si riceve una risposta simile a quella visualizzata, verificare che le impostazioni DNS siano corrette.**Attenzione**: il server utilizza uno schema di indirizzi IP round robin per il bilanciamento del carico, la tolleranza di errore e i tempi di attività. Pertanto, gli indirizzi IP possono essere modificati e Cisco consiglia di configurare il firewall con un **CNAME** anziché un indirizzo IP.

5. Verificare la connettività a intelligence.sourcefire.com con l'uso di Telnet:

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

Verificare di ricevere un output simile al seguente:

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

Nota: se è possibile completare correttamente il secondo passaggio ma non è possibile eseguire la connessione Telnet a **intelligence.sourcefire.com** sulla porta 443, è possibile avere una regola del firewall che blocchi la porta 443 in uscita per intelligence.sourcefire.com.

6. Selezionare **Sistema > Locale > Configurazione** e verificare le impostazioni proxy del **Manual Proxy** configurazione in **Network** sezione.
Nota: se il proxy esegue l'ispezione SSL (Secure Sockets Layer), è necessario implementare una regola di bypass che ignori il proxy per **intelligence.sourcefire.com**.
7. Verificare se è possibile eseguire una HTTP GET richiesta contro 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
```

Nota: lo smile alla fine del curl l'output del comando indica che la connessione è riuscita.**Nota**: se si utilizza un proxy, curl richiede un nome utente. Il comando è **curl -U <utente> -vk** https://intelligence.sourcefire.com. Inoltre, dopo aver immesso il comando, viene richiesto di immettere la password proxy.

8. Verificare che il traffico HTTPS utilizzato per scaricare il feed di Security Intelligence non passi attraverso un decrittografatore SSL. Per verificare che non venga eseguita alcuna decrittografia SSL, convalidare le informazioni sul certificato server nell'output del passaggio 6. Se il certificato del server non corrisponde a quello visualizzato nell'esempio seguente, è possibile disporre di un decrittografatore SSL che rinuncia al certificato. Se il traffico passa attraverso un decrittatore SSL, è necessario ignorare tutto il traffico diretto a 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
```

Nota: la decrittografia SSL deve essere ignorata per il feed di Security Intelligence, in quanto il decrittografatore SSL invia al centro Firepower Management un certificato sconosciuto nell'handshake SSL. Il certificato inviato al Centro gestione Firepower non è firmato da una CA attendibile di Sourcefire, pertanto la connessione non è attendibile.

Informazioni correlate

- Automatico Download dell'aggiornamento non riuscito in un centro di gestione Firepower
- Indirizzi server richiesti per le operazioni Advanced Malware Protection (AMP)
- Porte di comunicazione necessarie per il funzionamento del sistema Firepower
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).