排除FireSIGHT管理中心上的安全情報源更新故障

目錄

簡介

本文說明如何解決安全情報源更新的問題。安全情報源由多個定期更新的信譽不良的IP地址清單組成，這些清單由思科Talos安全情報和研究小組(Talos)確定。 定期更新情報源非常重要，以便Cisco FireSIGHT系統可以使用最新資訊來過濾網路流量。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco FireSIGHT管理中心
- 安全情報源

採用元件

本文檔中的資訊基於運行軟體版本5.2或更高版本的Cisco FireSIGHT管理中心。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題

發生安全情報源更新失敗。您可以通過Web GUI或CLI驗證故障（在後面的章節中進一步說明）。

從Web GUI驗證問題

當安全情報源更新失敗時，FireSIGHT管理中心會顯示運行狀況警報。

從CLI驗證問題

要確定安全情報源更新失敗的根本原因，請在FireSIGHT管理中心的CLI中輸入以下命令：

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

在郵件中搜尋以下任一警告：

```
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
```

解決方案

完成以下步驟即可解決此問題：

1. 驗證*intelligence.sourcefire.com站點*是否處於活動狀態。在瀏覽器中導航至 https://intelligence.sourcefire.com。您應該會看到一張笑臉，表示該網站已啟動。

2. 通過安全外殼(SSH)訪問FireSIGHT管理中心的CLI。

3. 從FireSIGHT管理中心ping *intelligence.sourcefire.com*:

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.com
   ```

   您應該會收到類似以下的輸出：

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

   如果您沒有收到與所示類似的響應，則可能是出站連線有問題，或者您沒有通往intelligence.sourcefire.com的路*由。*

4. 解析*intelligence.sourcefire.com的主機名*:

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

   您應該會收到類似以下的回覆：

   ```
   Server: 8.8.8.8
   Address: 8.8.8.8#53

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

   附註：上述輸出使用Google公共域名系統(DNS)伺服器作為示例。輸出取決於*網路*部分下**System > Local > Configuration**中配置的DNS設定。如果您沒有收到與所示類似的響應，請確保DNS設定正確。**注意**：伺服器使用循環IP地址模式進行負載平衡、容錯和正常運行時間。因此，IP地址可能會改變，思科建議使用*CNAME*而不是IP地址配置防火牆。
5. 使用Telnet檢查與*intelligence.sourcefire.com*的連線：

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

您應該會收到類似以下的輸出：

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

附註：如果能夠成功完成第二步，但無法通過埠443通過Telnet訪問 *intelligence.sourcefire.com*，則您可能具有防火牆規則，該規則會阻止 *intelligence.sourcefire.com*的埠443出站。

6. 導覽至**System > Local > Configuration**，然後在*Network*部分下驗證*Manual Proxy*配置的代理設定。

   附註：如果此代理執行安全套接字層(SSL)檢查，則必須設定繞過 *intelligence.sourcefire.com代理的繞行規則*。

7. 測試是否可以對*intelligence.sourcefire*.com*執行HTTP GET請求*:

```
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
```

附註：*curl*命令輸出末尾的笑臉表示連線成功。**註**：如果您使用代理，則*curl命令*需要使用者名稱。命令將為curl -U <user> -vvk https://intelligence.sourcefire.com。此外，輸入命令後，系統會提示您輸入代理密碼。

8. 驗證用於下載安全情報源的HTTPS流量是否未通過SSL解密器。若要驗證是否未發生SSL解密，請驗證步驟6輸出中的伺服器證書資訊。如果伺服器證書與以下示例中顯示的不匹配，則您可能具有重新簽名證書的SSL解密器。如果流量通過SSL解密器，則必須繞過發往*intelligence.sourcefire.com*的所有流量。

```
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
```

附註：安全情報源必須繞過SSL解密，因為SSL解密器在SSL握手中向FireSIGHT管理中心傳送未知證書。傳送到FireSIGHT管理中心的證書未由Sourcefire信任的CA簽名，因此連線不受信任。

相關資訊

- FireSIGHT管理中心上的自動下載更新失敗
- 高級惡意軟體防護(AMP)操作所需的伺服器地址
- FireSIGHT系統運行所需的通訊埠
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。