排除故障安全智能源FireSIGHT管理中心的更新失败

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[问题](#)
[验证从Web GUI的问题](#)
[验证从CLI的问题](#)
[解决方案](#)
[相关信息](#)

简介

本文描述如何排除故障与安全智能源更新的问题。包括有恶劣的名誉IP地址的几有规律地更新的列表，如思科Talos安全智能和研究小组取决于安全智能源(Talos)。保留智能源有规律地更新是重要的，以便思科FireSIGHT系统能使用最新信息为了过滤您的网络流量。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科FireSIGHT管理中心
- 安全智能源

使用的组件

本文档中的信息根据运行软件版本5.2或以上的Cisco FireSIGHT管理中心。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

安全智能源更新失败发生。您能通过Web GUI或CLI验证失败(解释进一步在跟随)的部分。

验证从Web GUI的问题

当安全智能源更新失败发生时， FireSIGHT管理中心显示健康警报。

验证从CLI的问题

为了确定一更新失败的根本原因有安全智能源的，请输入此命令到FireSIGHT管理中心的CLI ：

```
admin@Sourcefire3D:~$

cat /var/log/messages
```

搜索在消息的这些警告之一：

```
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
```

解决方案

完成以下步骤以解决该问题：

1. 验证*intelligence.sourcefire.com*站点是活跃的。导航对https://intelligence.sourcefire.comin浏览器。您应该接收一个兴高采烈的表面，表明站点实际。

2. 通过安全壳SSH访问FireSIGHT管理中心的CLI。

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

   ```
   admin@Sourcefire3D:~$

   sudo ping intelligence.sourcefire.com
   ```

   您应该收到输出类似于此：

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

   如果不收到答复类似于显示的那，则您也许有出站连通性问题或您没有一个路由对*intelligence.sourcefire.com*。

4. 解决*intelligence.sourcefire.com的*主机名：

   ```
   admin@Firepower:~$

   sudo

   nslookup intelligence.sourcefire.com
   ```

   您应该收到答复类似于此：

```
Server: 8.8.8.8
Address: 8.8.8.8#53

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

Note:上述输出使用谷歌公共域名称系统(DNS)服务器为例。输出取决于在**系统>本地>配置方面**配置的DNS设置，在*网络*部分下。如果不收到答复类似于显示的那，则请保证DNS设置正确。**Caution**:服务器使用一循环IP地址模式负载均衡、容错和正常运行。所以， IP地址也许更改，并且思科建议防火墙配置与*CNAME*而不是IP地址。

5. 检查连接对*intelligence.sourcefire.com*与使用Telnet ：

```
admin@Firepower:~$

 sudo telnet intelligence.sourcefire.com 443
```

您应该收到输出类似于此：

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

Note:如果能成功地完成第二步，但是无法远程登录到在端口443的*intelligence.sourcefire.com*，您也许有阻塞端口443出站为*intelligence.sourcefire.com的*防火墙规则。

6. 导航对**系统>本地>配置**并且验证*手工代理配置的*代理设置在*网络*部分下。
   Note:如果此代理执行安全套接字协议层(SSL)检查，您必须进行绕过*intelligence.sourcefire.com的*代理的旁路规则。
7. 测试您是否可执行*HTTP GET*请求*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:兴高采烈的表面在*卷毛*命令输出结束时指示一个成功的连接。**Note**: 如果使用一个代理，*卷毛*命令要求用户名。命令将是**卷毛- U <user> - vvk** https://intelligence.sourcefire.com。另外，在您输入命令后，您是被提示的回车代理密码。

8. 验证HTTPS流量使用为了下载的安全智能源不穿过SSL decryptor。为了验证SSL解密不发生，请验证服务器证书信息在从步骤6.的输出中。如果服务器证书不匹配在跟随的示例显示的那，则您也许有辞去证书的SSL decryptor。 如果流量穿过SSL decryptor，您必须绕过去*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
```

Note:因为SSL decryptor发送FireSIGHT管理中心在SSL握手的一未知证书必须为安全智能源绕过SSL解密。发送对FireSIGHT管理中心的证书没有由Sourcefire委托CA，因此连接签字不信任。

相关信息

- FireSIGHT管理中心的自动下载更新失败
- 先进的恶意软件保护(AMP)操作的所需的服务器地址
- FireSIGHT系统操作的需要的通信端口
- 技术支持和文档 - Cisco Systems