排除Firepower管理中心上的安全情报源更新故障

目录

简介

本文档介绍如何解决安全情报源更新的问题。

背景

安全情报源由多个定期更新的信誉不佳的IP地址列表组成，这些列表由思科Talos安全情报和研究小组(Talos)确定。定期更新情报源非常重要，以便Cisco Firepower系统可以使用最新信息来过滤网络流量。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower管理中心
- 安全情报源

使用的组件

本文档中的信息基于运行软件版本5.2或更高版本的Cisco Firepower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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

发生安全情报源更新故障。您可以通过Web GUI或CLI验证故障（在后面的章节中进一步说明）。

从Web GUI验证问题

当安全情报源更新失败时，Firepower管理中心会显示运行状况警报。

从CLI验证问题

要确定安全情报源更新故障的根本原因，请在Firepower管理中心的CLI中输入以下命令：

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

在邮件中搜索以下警告之一：

```
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** 站点处于活动状态。在浏览器中导航至 https://intelligence.sourcefire.com。
2. 通过安全外壳(SSH)访问Firepower管理中心的CLI。
3. ping intelligence.sourcefire.com 从Firepower管理中心：

   ```
   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. 解析主机名 intelligence.sourcefire.com：

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

   验证您收到类似以下内容的响应：

   ```
   Server: 8.8.8.8
   Address: 8.8.8.8#53

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

   注意：上述输出以Google公共域名系统(DNS)服务器为例。输出取决于**System > Local > Configuration**中配置的DNS设置。 **Network** 部分。如果您没有收到与所示类似的响应，请确保DNS设置正确。**注意**：服务器使用轮询IP地址方案来实现负载均衡、容错和正常运行时间。因

此，IP地址可以更改，思科建议防火墙配置有 **CNAME** 而不是IP地址。

5. 检查与 intelligence.sourcefire.com 使用Telnet:

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

验证您收到类似以下内容的输出：

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

注：如果您可以成功完成第二步，但无法通过Telnet访问 **intelligence.sourcefire.com** 通过端口443，您可以拥有防火墙规则来阻止端口443的出站 intelligence.sourcefire.com.

6. 导航到**System > Local > Configuration**，并验证 **Manual Proxy** 配置 **Network** 部分。

注意：如果此代理执行安全套接字层(SSL)检测，则必须设置绕过代理的旁路规则 **intelligence.sourcefire.com**.

7. 测试您是否能执行 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
```

注意：位于屏幕末尾的笑脸 curl 命令输出表示连接成功。**注意**：如果您使用代理， curl 命令需要用户名。命令为**curl -U <user> -vvk** https://intelligence.sourcefire.com。此外，输入命令后，系统会提示您输入代理密码。

8. 验证用于下载安全情报源的HTTPS流量未通过SSL解密器。要验证不发生SSL解密，请验证步骤6输出中的服务器证书信息。如果服务器证书与以下示例中显示的内容不匹配，则您可以让一个SSL解密器对证书进行重新签名。 如果流量通过SSL解密器，则必须绕过所有流向的流量 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
```

注意：安全情报源必须绕过SSL解密，因为SSL解密器在SSL握手中向Firepower管理中心发送未知证书。发送到Firepower管理中心的证书未由Sourcefire信任的CA签名，因此连接不受信任。

相关信息

- 自动matic Firepower管理中心下载更新失败
- 高级恶意软件防护(AMP)操作所需的服务器地址
- Firepower系统运行所需的通信端口
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。