Contents

Introduction

This document describes how to troubleshoot issues with Security Intelligence Feed updates. The Security Intelligence Feed is comprised of several regularly updated lists of IP addresses that have poor reputations, as determined by the Cisco Talos Security Intelligence and Research Group (Talos). It is important to keep the intelligence feed regularly updated so that a Cisco FireSIGHT System can use up-to-date information in order to filter your network traffic.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco FireSIGHT Management Center
- Security Intelligence Feed

Components Used

The information in this document is based on a Cisco FireSIGHT Management Center that runs software Version 5.2 or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problem

A Security Intelligence Feed update failure occurs. You can verify the failure via either the web GUI or the CLI (explained further in the sections that follow).

Verify the Problem from the Web GUI

When the Security Intelligence Feed update failure occurs, the FireSIGHT Management Center displays health alerts.

Verify the Problem from the CLI

In order to determine the root cause of an update failure with the Security Intelligence Feed, enter this command into the CLI of the FireSIGHT Management Center:

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

Search for either of these warnings in the messages:

```
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
```

Solution

Complete these steps in order to troubleshoot the problem:

1. Verify that the *intelligence.sourcefire.com* site is active. Navigate to **https://intelligence.sourcefire.com**in a browser. You should receive a smiley face, which indicates that the site is live.

2. Access the CLI of the FireSIGHT Management Center via Secure Shell (SSH).

3. Ping *intelligence.sourcefire.com* from the FireSIGHT Management Center:

   `admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.com`You should receive an output similar to this:

   `64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ms`If you do not receive a response similar to that shown, then you might have an outbound connectivity issue or you do not have a route to *intelligence.sourcefire.com.*

4. Resolve the hostname for *intelligence.sourcefire.com*:

   `admin@Firepower:~$ sudonslookup intelligence.sourcefire.com`You should receive a response similar to this:

   ```
   Server: 8.8.8.8
   Address: 8.8.8.8#53

   Name: intelligence.sourcefire.com
   ```

   `Address: xxx.xxx.xx.x` **Note**: The aforementioned output uses the Google Public Domain Name System (DNS) Server as an example. The output depends on the DNS settings that are configured in **System > Local > Configuration**, under the *Network* section. If you do not receive a response similar to that shown, then ensure that the DNS settings are correct.**Caution**: The server uses a round-robin IP address schema for load balancing, fault-tolerance, and uptime. Therefore, the IP addresses might change, and Cisco recommends

that the firewall be configured with a *CNAME* instead of an IP address.

5. Check the connectivity to *intelligence.sourcefire.com* with the use of Telnet:

   `admin@Firepower:~$` **`sudo telnet intelligence.sourcefire.com 443`**You should receive an output similar to this:

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

   Note: If you are able to complete the second step successfully but are unable to Telnet to *intelligence.sourcefire.com* over port 443, you might have a firewall rule that blocks port 443 outbound for *intelligence.sourcefire.com*.
6. Navigate to **System > Local > Configuration** and verify the proxy settings of the *Manual Proxy* configuration under the *Network* section.
   Note: If this proxy does Secure Sockets Layer (SSL) inspection, you must put into place a bypass rule that bypasses the proxy for *intelligence.sourcefire.com*.
7. Test whether you can perform an *HTTP GET* request against *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: The smiley face at the end of the *curl* command output indicates a successful connection.**Note**: If you use a proxy, the *curl* command requires a username. The command will be **curl -U <user> -vvk https://intelligence.sourcefire.com**. Additionally, after you enter the command, you are prompted enter the proxy password.

8. Verify that the HTTPS traffic that is used in order to download the Security Intelligence feed does not pass through an SSL decryptor. In order to verify that no SSL decryption occurs, validate the Server Certificate information in the output from Step 6. If the Server Certificate does not match that displayed in the example that follows, then you might have an SSL decryptor that resigns the certificate. If the traffic passes through an SSL decryptor, you must bypass all of the traffic that goes to *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: The SSL decryption must be bypassed for the Security Intelligence Feed because the SSL decryptor sends the FireSIGHT Management Center an unknown certificate in the SSL handshake. The certificate that is sent to the FireSIGHT Management Center is not signed by a Sourcefire-trusted CA, so the connection is untrusted.

Related Information

- **Automatic Download Update Failure on a FireSIGHT Management Center**
- **Required Server Addresses for Advanced Malware Protection (AMP) Operations**
- **Required Communication Ports for FireSIGHT System Operation**
- **Technical Support & Documentation - Cisco Systems**