ESA with AMP Receives "The File Reputation service is not reachable" Error

Contents

Introduction

This document describes the alert attributed to the Cisco Email Security Appliance (ESA) with Advanced Malware Protection (AMP) enabled, where the service is unable to communicate over port 32137 or 443 for File Reputation.

Correct the "The File Reputation service is not reachable" Error Received for AMP

AMP was released for use on the ESA in AsyncOS Version 8.5.5 for Email Security. With AMP licensed and enabled on the ESA, administrators receive this message:

```
The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

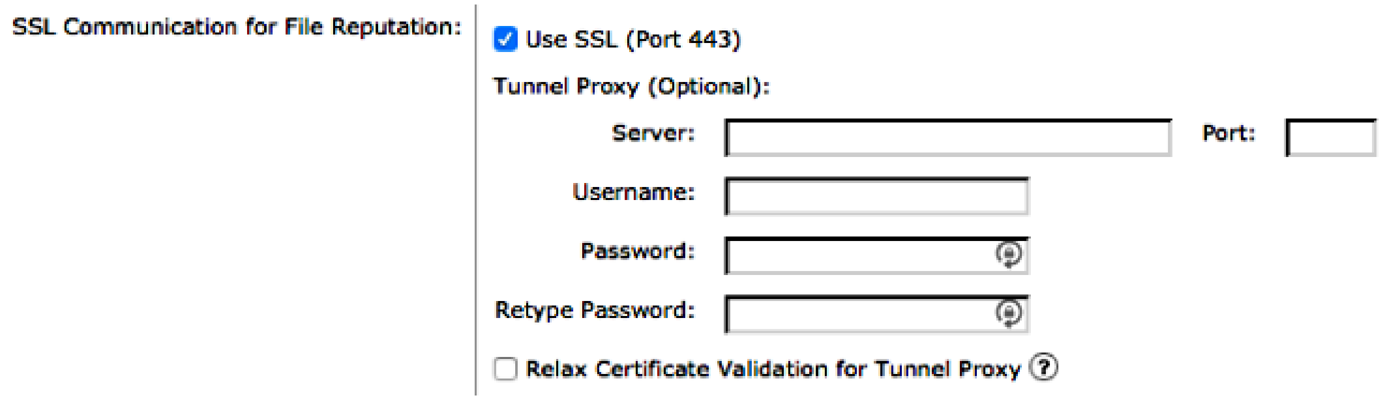
The AMP service might be enabled, but probably does not communicate on the network via port 32137 for File Reputation.

If that is the case, the ESA administrator can choose to have File Reputation communicate over port 443.

In order to do so, run **ampconfig > advanced** from the CLI and be sure that **Y** is selected for *Do you want to enable SSL communication (port 443) for file reputation? [N]*>:

```
(Cluster example.com)> ampconfig

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud
[1]>
```

If you use the GUI, choose **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (drop-down)** and ensure the **Use SSL** checkbox is checked as shown here:



SSL Communication for File Reputation:

☑ Use SSL (Port 443)

Tunnel Proxy (Optional):

Server: Port:

Username:

Password:

Retype Password:

□ Relax Certificate Validation for Tunnel Proxy

Commit any and all changes to the configuration.

Finally, review the current AMP log in order to see the service and connectivity success or failure. You can accomplish this from the CLI with **tail amp**.

Prior to changes made to **ampconfig > advanced**, you would have seen this in the AMP logs:

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

After the change is made to **ampconfig > advanced**, you see this in the AMP logs:

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

The **amp_watchdog.txt** file as shown in the previous example will run every 10 minutes and be tracked in the AMP log. This file is part of the keep-alive for AMP.

A normal query in the AMP log against a message with the configured file type(s) for File Reputation and File Analysis would be similar to this:

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

With this log information, the administrator should be able to correlate the Message ID (MID) in the mail logs.

Troubleshoot

Review firewall and network settings in order to ensure that SSL communication is opened for these:

Port	Protocol	In/Out	Hostname	Description
443	TCP	Out	As configured in Security Services > File Reputation and Analysis, Advanced section.	Access to cloud servi for file analysis.
32137	TCP	Out	As configured in Security Services > File Reputation and Analysis, Advanced section, Advanced section, Cloud Server Pool parameter.	Access to cloud servi order to obtain file reputation.

You can test basic connectivity from your ESA to the cloud service over 443 via Telnet in order to ensure that your appliance can successfully reach the AMP services, File Reputation, and File Analysis.

> **Note**: The addresses for File Reputation and File Analysis are configured on the CLI with **ampconfig > advanced** or from the GUI with **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (drop-down)**.

> **Note**: If utilizing a tunnel proxy between the ESA and File Reputation server(s), you may be required to enable the option to Relax Certificate Validation for Tunnel Proxy. This option is provided to skip standard certificate validation if the tunnel proxy server's certificate is not signed by a root authority trusted by the ESA. For instance, select this option if using a self-signed certificate on a trusted internal tunnel proxy server.

File Reputation example:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

File Analysis example:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

If the ESA is able to telnet to the file reputation server, and there is not an upstream proxy decrypting the connection, then the applaince may need to be re-registered with Threat Grid. On the ESA CLI there is a hidden command:

```
10.0.0-125.local> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> ampregister

AMP registration initiated.
```

Related Information

- ESA Advanced Malware Protection (AMP) Test
- ESA User Guides
- ESA FAQ: What is a Message ID (MID), Injection Connection ID (ICID), or Delivery Connection ID (DCID)?
- How do I search and view the mail logs on the ESA?
- Technical Support & Documentation - Cisco Systems