ESA mit AMP empfängt Fehler "Der Dateireputations-Service ist nicht erreichbar"

Inhalt

Einleitung

In diesem Dokument wird die Warnung beschrieben, die der Cisco E-Mail Security Appliance (ESA) mit aktiviertem Advanced Malware Protection (AMP) zugewiesen wurde, wenn der Service nicht über Port 32137 oder 443 für die Dateireputation kommunizieren kann.

Korrigieren Sie den Fehler "Der Dateireputations-Service ist nicht erreichbar", der für AMP empfangen wurde.

AMP wurde für die Verwendung auf der ESA in AsyncOS Version 8.5.5 für Email Security veröffentlicht. Wenn AMP auf der ESA lizenziert und aktiviert ist, erhalten Administratoren die folgende Meldung:

```
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
```

Der AMP-Dienst ist möglicherweise aktiviert, kommuniziert aber wahrscheinlich nicht im Netzwerk über Port 32137 für die Dateireputation.

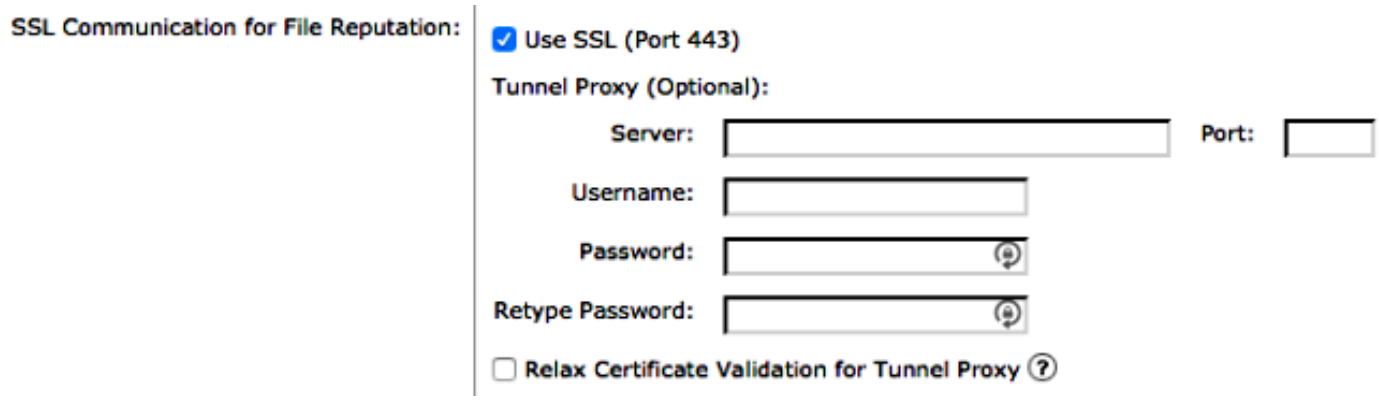
In diesem Fall kann der ESA-Administrator festlegen, dass die Dateireputation über Port 443 kommuniziert.

Führen Sie dazu **ampconfig > advanced** aus der CLI aus, und stellen Sie sicher, dass **Y** für *Do you want to enable SSL communication (port 443) for file reputation* ausgewählt ist. *[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]>
```

Wenn Sie die GUI verwenden, wählen Sie **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (Dropdown-Liste) aus,** und stellen Sie sicher, dass das Kontrollkästchen **SSL verwenden** wie hier dargestellt aktiviert ist:



Bestätigen Sie alle Konfigurationsänderungen.

Überprüfen Sie abschließend das aktuelle AMP-Protokoll, um festzustellen, ob der Service erfolgreich war oder die Verbindung fehlschlug. Dies kann über die CLI mit **Tail Amp** erreicht werden.

Vor den Änderungen an **ampconfig > advanced** hätten Sie Folgendes in den AMP-Protokollen gesehen:

```
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.
```

Nachdem die Änderung an "**ampconfig > advanced**" vorgenommen wurde, wird dies in den AMP-Protokollen angezeigt:

```
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
```

Die Datei **amp_watchdog.txt**, wie im vorherigen Beispiel gezeigt, wird alle 10 Minuten ausgeführt und im AMP-Protokoll nachverfolgt. Diese Datei ist Teil des Keepalives für AMP.

Eine normale Abfrage im AMP-Protokoll für eine Nachricht mit den konfigurierten Dateitypen für Dateireputation und Dateianalyse wäre ähnlich:

```
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
```

Mit diesen Protokollinformationen sollte der Administrator in der Lage sein, die Nachrichten-ID (MID) in den Mail-Protokollen zu korrelieren.

Fehlerbehebung

Überprüfen Sie die Firewall- und Netzwerkeinstellungen, um sicherzustellen, dass die SSL-Kommunikation für diese Geräte geöffnet ist:

Anschluss	Protokolle	Ein/Aus	Hostname	Beschreibung
443	TCP	Aus	Wie unter Sicherheitsdienste > Dateireputation und -analyse, Erweitert konfiguriert.	Zugriff auf Cloud-Serv zur Dateianalyse
32137	TCP	Aus	Wie konfiguriert unter Sicherheitsdienste > Dateireputation	Zugriff auf Cloud-Serv

	und -analyse, Erweitert, Erweitert, Cloud Server Pool-Parameter.	um Dateireputation zu erhalten

Sie können die grundlegende Verbindung von Ihrer ESA zum Cloud-Service über 443 via Telnet testen, um sicherzustellen, dass Ihre Appliance die AMP-Services, die Dateireputation und die Dateianalyse erfolgreich erreichen kann.

> **Hinweis:** Die Adressen für Dateireputation und Dateianalyse werden in der CLI mit "**ampconfig" > "advanced"** oder in der GUI mit "**Security Services" > "File Reputation and Analysis" > "Edit Global Settings" > "Advanced" (Dropdown-Liste) konfiguriert**.

> **Anmerkung:** Wenn Sie einen Tunnelproxy zwischen der ESA und dem/den Dateireputations-Server(n) verwenden, müssen Sie möglicherweise die Option zum Entspannen der Zertifikatvalidierung für den Tunnelproxy aktivieren. Diese Option wird bereitgestellt, um die Standardzertifikatvalidierung zu überspringen, wenn das Zertifikat des Tunnelproxyservers nicht von einer von der ESA vertrauenswürdigen Stammautorisierung signiert ist. Wählen Sie diese Option beispielsweise aus, wenn Sie ein selbstsigniertes Zertifikat auf einem vertrauenswürdigen internen Tunnelproxyserver verwenden.

Beispiel für Dateireputation:

```
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.
```

Beispiel für Dateianalyse:

```
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.
```

Wenn die ESA eine Telnet-Verbindung zum Dateireputations-Server herstellen kann und es keinen Upstream-Proxy gibt, der die Verbindung entschlüsselt, muss die Appliance möglicherweise bei Threat Grid neu registriert werden. In der ESA-CLI gibt es einen verborgenen Befehl:

```
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.
```

Zugehörige Informationen

- ESA Advanced Malware Protection (AMP)-Test
- ESA-Benutzerhandbücher
- Häufig gestellte Fragen zur ESA: Was ist eine Message ID (MID), Injection Connection ID (ICID) oder Delivery Connection ID (DCID)?
- Wie kann ich die E-Mail-Protokolle auf der ESA suchen und anzeigen?
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.