ESA met AMP Ontvangt "The File Reputation service is not reach" Fout

Inhoud

Inleiding

Dit document beschrijft de waarschuwing die is toegewezen aan de Cisco Email Security Applicatie (ESA) met Advanced Malware Protection (AMP) ingeschakeld, waarbij de service niet kan communiceren via poort 32137 of 443 voor bestandsnaam.

Corrigeer de "File Reputation service is not reach able" fout ontvangen voor AMP

AMP is vrijgegeven voor gebruik op de ESA in AsyncOS Versie 8.5.5 voor Email Security. Met AMP gelicentieerd en ingeschakeld op de ESA, ontvangen beheerders dit bericht:

```
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
```

De AMP-service kan zijn ingeschakeld, maar communiceert waarschijnlijk niet op het netwerk via poort 32137 voor bestandsnaam.

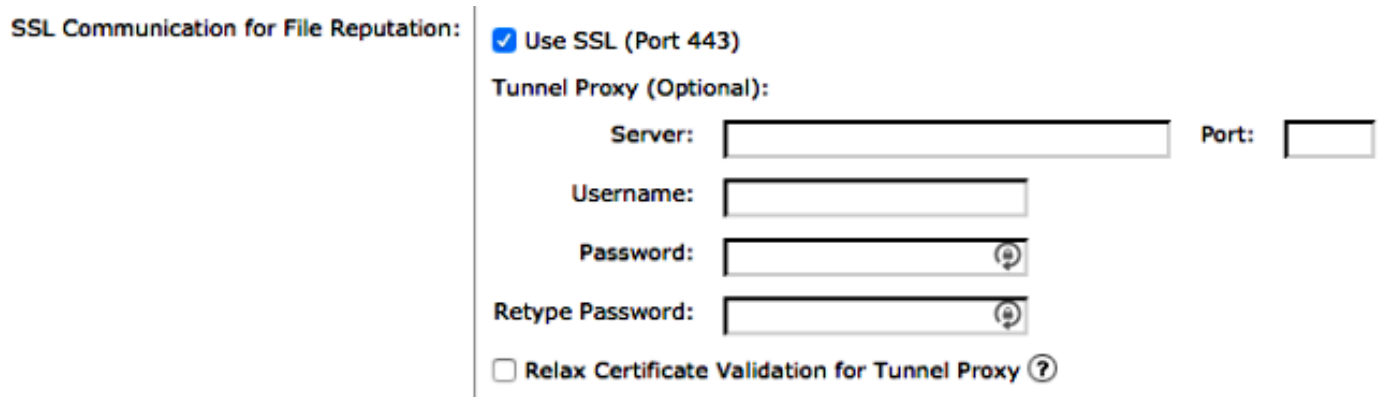
Als dat het geval is, kan de ESA-beheerder ervoor kiezen om File Reputation te laten communiceren via poort 443.

Om dit te doen, voer **ampconfig > geavanceerde** van de CLI uit en zorg ervoor dat **Y** is geselecteerd voor *Wilt u SSL communicatie (poort 443) inschakelen voor bestandsreputatie? [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]>
```

Als u de GUI gebruikt, kies **Security Services > File Reputation and Analysis > Global Settings > Advanced (Geavanceerd) bewerken** en zorg ervoor dat het selectievakje **Use SSL (SSL)** is ingeschakeld zoals hier wordt getoond:



Voer alle wijzigingen in de configuratie uit.

Tot slot, herzie het huidige AMP logboek om de dienst en connectiviteitssucces of mislukking te zien. Je kunt dit bereiken vanuit de CLI met **staartversterker**.

Voorafgaand aan veranderingen die aan **ampconfig > geavanceerd worden** aangebracht, zou u dit in de logboeken van AMP gezien hebben:

```
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.
```

Nadat de verandering in **ampconfig > geavanceerde** wordt aangebracht, ziet u dit in de logboeken van AMP:

```
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
```

Het bestand **amp_watchdog.txt**, zoals in het vorige voorbeeld, wordt elke 10 minuten uitgevoerd en in het AMP-logbestand gevolgd. Dit bestand maakt deel uit van de keep-living voor AMP.

Een normale query in het AMP-logbestand tegen een bericht met het ingestelde bestandstype(n) voor bestandsnaam en bestandanalyse is vergelijkbaar met dit:

```
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
```

Met deze loggegevens moet de beheerder de Berichtid (MID) in de e-maillogbestanden kunnen correleren.

Problemen oplossen

Bekijk de firewall- en netwerkinstellingen om er zeker van te zijn dat SSL-communicatie voor deze functies wordt geopend:

Port	Protocol	In/Uit	Hostname	Beschrijving
443	TCP	Uit	Zoals geconfigureerd in Security Services > File Reputation and Analysis, Advanced.	Toegang tot cloudser voor bestandsanalyse
32137	TCP	Uit	Zoals geconfigureerd in Security Services > File Reputation and Analysis, Advanced-sectie, Advanced-sectie, Cloud Server Pool-parameter.	Toegang tot cloudser om de reputatie van bestanden te verkrijg

U kunt de basisconnectiviteit van uw ESA met de cloudservice via Telnet testen om ervoor te zorgen dat uw apparaat met succes de AMP-services, File Reputation en File Analysis kan bereiken.

> **Opmerking**: de adressen voor bestandsreputatie en bestandsanalyse zijn geconfigureerd op de CLI met **ampconfig > advanced** of vanuit de GUI met **Security Services > File Reputation and Analysis > Global Settings > Advanced (drop-down)**.

> **Opmerking:** Als u gebruik maakt van een tunnelproxy tussen de ESA en File Reputation server(s), kan het nodig zijn om de optie in te schakelen om certificaatvalidatie voor tunnelproxy te ontkoppelen. Deze optie wordt geboden om standaard certificaatsvalidatie over te slaan als het certificaat van de tunnelproxy server niet is ondertekend door een basisautoriteit die door de ESA wordt vertrouwd. Selecteer deze optie bijvoorbeeld als u een zelfondertekend certificaat gebruikt op een vertrouwde interne tunnelproxyserver.

Voorbeeld reputatie bestand:

```
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.
```

Voorbeeld bestandsanalyse:

```
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.
```

Als de ESA in staat is om te telnet naar de file reputation server, en er is geen upstream proxy decrypting de verbinding, dan moet het apparaat mogelijk opnieuw worden geregistreerd bij Threat Grid. Op de ESA CLI staat een verborgen opdracht:

```
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.
```

Gerelateerde informatie

- ESA Advanced Malware Protection
- ESA-gebruikershandleidingen
- Veelgestelde vragen over ESA: Wat is een Message ID (MID), Injection Connection ID (ICID) of Delivery Connection ID (DCID)?
- Hoe zoek en bekijk ik de mail logboeken op de ESA?
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.