El ESA con AMP recibe el error "El servicio de reputación de archivos no está disponible".

Contenido

Introducción

Este documento describe la alerta atribuida al dispositivo de seguridad Cisco Email Security Appliance (ESA) con la protección frente a malware avanzado (AMP) habilitada, donde el servicio no puede comunicarse a través del puerto 32137 o 443 para la reputación de archivos.

Corrija el error "No se puede acceder al servicio de reputación de archivos" recibido para AMP

AMP se publicó para su uso en ESA en AsyncOS versión 8.5.5 para Email Security. Con la licencia de AMP y activada en el ESA, los administradores reciben este mensaje:

```
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
```

Es posible que el servicio AMP esté activado, pero es probable que no se comunique en la red a través del puerto 32137 para Reputación de archivos.

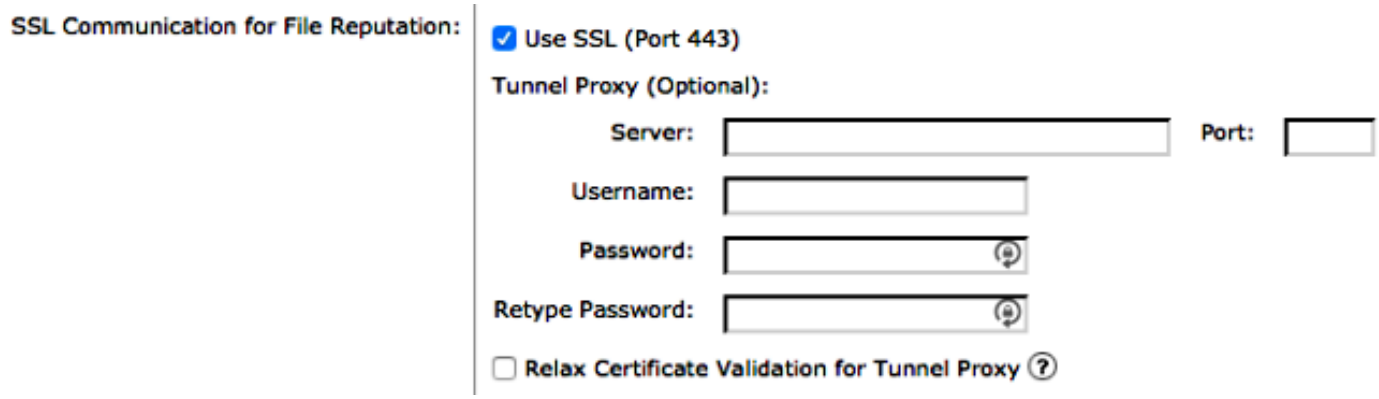
Si ese es el caso, el administrador ESA puede elegir que Reputación de archivos se comunique a través del puerto 443.

Para hacerlo, ejecute **ampconfig > advanced** desde la CLI y asegúrese de que **Y** esté seleccionado para *¿Desea habilitar la comunicación SSL (puerto 443) para la reputación del archivo? [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]>
```

Si utiliza la GUI, elija **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (desplegable)** y asegúrese de que la casilla de verificación **Use SSL** esté marcada como se muestra aquí:



Realice todos los cambios en la configuración.

Por último, revise el registro de AMP actual para ver si el servicio y la conectividad se han realizado correctamente o no. Puede lograr esto desde la CLI con **tail amp**.

Antes de realizar cambios en **ampconfig > advanced**, habría visto esto en los registros de AMP:

```
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.
```

Después de realizar el cambio en **ampconfig > advanced**, verá esto en los registros de 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
```

El archivo **amp_watchdog.txt** como se muestra en el ejemplo anterior se ejecutará cada 10 minutos y se realizará un seguimiento en el registro de AMP. Este archivo forma parte del keepalive de AMP.

Una consulta normal en el registro de AMP con un mensaje con los tipos de archivo configurados para Reputación de archivos y Análisis de archivos sería similar a la siguiente:

```
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
```

Con esta información de registro, el administrador debe poder correlacionar el ID de mensaje (MID) en los registros de correo.

Troubleshoot

Revise los parámetros de red y firewall para asegurarse de que la comunicación SSL está abierta para:

Puerto	Protocolo	Entrada/Salida	Hostname	Descripción
443	TCP	FUERA	Según la configuración de Servicios de seguridad > Reputación y análisis de archivos, sección Avanzadas.	Acceso a servicios en nube para el análisis archivos.
32137	TCP	FUERA	Según la configuración de Servicios de seguridad > Reputación y análisis de archivos, sección Avanzadas, sección Avanzadas, parámetro Pool de servidores en la	Acceso a servicios en nube para obtener reputación de archivo

nube.

Puede probar la conectividad básica de su ESA al servicio en la nube a través de 443 a través de Telnet para asegurarse de que su dispositivo puede alcanzar con éxito los servicios de AMP, Reputación de archivos y Análisis de archivos.

> **Nota**: las direcciones de Reputación de archivos y Análisis de archivos se configuran en la CLI con **ampconfig > advanced** o desde la GUI con **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (desplegable)**.

> **Nota:** Si utiliza un proxy de túnel entre el ESA y los servidores de Reputación de Archivos, es posible que deba habilitar la opción Relax Certificate Validation for Tunnel Proxy. Esta opción se proporciona para omitir la validación de certificados estándar si el certificado del servidor proxy de túnel no está firmado por una autoridad raíz en la que confía el ESA. Por ejemplo, seleccione esta opción si utiliza un certificado autofirmado en un servidor proxy de túnel interno de confianza.

Ejemplo de Reputación de archivos:

```
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.
```

Ejemplo de análisis de archivos:

```
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.
```

Si el ESA puede establecer una conexión telnet con el servidor de reputación de archivos y no hay un proxy upstream que descifre la conexión, es posible que sea necesario volver a registrar el dispositivo con Threat Grid. En la ESA CLI hay un comando oculto:

```
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.
```

Información Relacionada

- Prueba de protección frente a malware avanzado (AMP) de ESA
- Guías de usuario ESA
- PREGUNTAS FRECUENTES DE ESA: ¿Qué es un ID de mensaje (MID), un ID de conexión de inyección (ICID) o un ID de conexión de entrega (DCID)?
- ¿Cómo puedo buscar y ver los registros de correo en el ESA?
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).