Contenido

Introducción

Este documento describe la alerta atribuida al dispositivo de seguridad del correo electrónico de Cisco (ESA) con la protección avanzada de Malware (amperio) habilitada en él donde el servicio no comunica sobre el puerto 443 para Secure Sockets Layer (SSL).

Corrija “el servicio de la reputación del archivo en la nube es” error inalcanzable recibido para el amperio

El amperio fue liberado para el uso en el ESA en la versión 8.5.5 y posterior de AsyncOS. Con el amperio autorizado y habilitado en el ESA, los administradores reciben este mensaje:

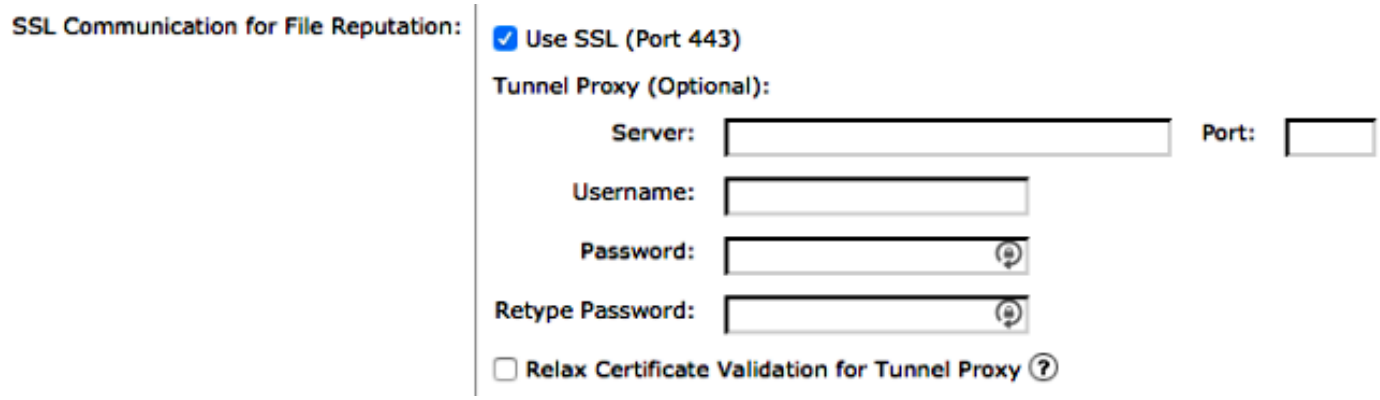
El servicio amperio se pudo habilitar, pero no comunica probablemente sobre el puerto 443.

¿Para asegurar que el amperio comunica sobre 443, ejecute el **ampconfig > avanzado del** CLI y esté seguro que **Y** está seleccionada para **usted quiere habilitar la comunicación SSL (puerto 443) para la reputación del archivo? [y] >**:

```
> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>
```

```
Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

Si usted utiliza el GUI, haga clic los **Servicios de seguridad > la reputación del archivo y el análisis > edita las configuraciones globales > avanzó (descenso-abajo)** y se asegura que la casilla de verificación del **uso SSL** está habilitada como se muestra aquí:



Confíe cualquiera y todos los cambios para su configuración.

Finalmente, revise el registro actual amperio para ver el servicio y el éxito o el error de la Conectividad. Usted puede lograr esto del CLI con el **amperio de la cola.**

Antes de los cambios realizados al **ampconfig > avanzó**, usted habría visto esto en los registros amperio:

```
> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced
```

```
Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

Después de que el cambio se realice al **ampconfig > avanzado**, usted ve esto en los registros amperio:

```
> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

Enter heartbeat interval?
[15]>

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

```
Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

El archivo de **amp_watchdog.txt** visualiza cada 10 minutos en los registros. Este archivo es parte del señal de mantenimiento para el amperio.

En los registros amperio, una interrogación normal sería similar a esto:

```
> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]>

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

Enter file analysis server URL?
[https://intel.api.sourcefire.com]>

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

Con esta información, usted debe poder correlacionar el ID del mensaje (MEDIADOS DE) en los registros del correo.

Troubleshooting

Firewall y configuraciones de red del estudio para asegurar que la comunicación SSL está abierta para éstos:

Puerto	Protocolo	In/out	Nombre del host	Descripción
443	TCP	Hacia fuera	Como está configurado en los Servicios de seguridad > la reputación y el análisis del archivo, sección avanzada.	Acceso para nublarse los servicios para el análisis archivo.
32137	TCP	Hacia fuera	Como está configurado en los Servicios de seguridad > la reputación y el análisis del archivo, sección avanzada, sección avanzada, parámetro del pool del servidor de la nube.	Acceso para nublarse los servicios para obtener la reputación del archivo.

Usted puede probar la conectividad básica de su ESA al servicio de la nube sobre 443 vía Telnet para asegurarse de que su dispositivo puede alcanzar con éxito los servicios amperio.

> Nota: Los direccionamientos para la reputación del archivo y el análisis del archivo se configuran en el CLI con el **ampconfig > avanzado**, o del GUI con los **Servicios de seguridad > la reputación y el análisis del archivo > edite las configuraciones globales > avanzado (descenso-abajo)**.

Clasifíe el ejemplo de la reputación:

```
ironport:service 36] telnet cloud-sa.amp.sourcefire.com 443
Trying 184.73.186.190...
Connected to cloud-sa.amp.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Clasifíe el ejemplo del análisis:

```
ironport:service 37] telnet intel.api.sourcefire.com 443
Trying 198.148.79.52...
Connected to intel.api.sourcefire.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Información Relacionada

- Prueba avanzada de la protección ESA Malware (amperio)
- Guías del usuario ESA
- ESA FAQ: ¿Cuál es un ID del mensaje (MEDIADOS DE), el ID de conexión de la inyección (ICID), o el ID de conexión de la salida (DCID)?
- ¿Cómo busco y ver el correo abre una sesión el ESA?