Integre la nube privada de terminales seguros con una Web y un correo electrónico seguros

Contenido

Introducción

En este documento se describen los pasos necesarios para integrar la nube privada de terminal seguro con el dispositivo web seguro (SWA) y el gateway de correo electrónico seguro (ESA).

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

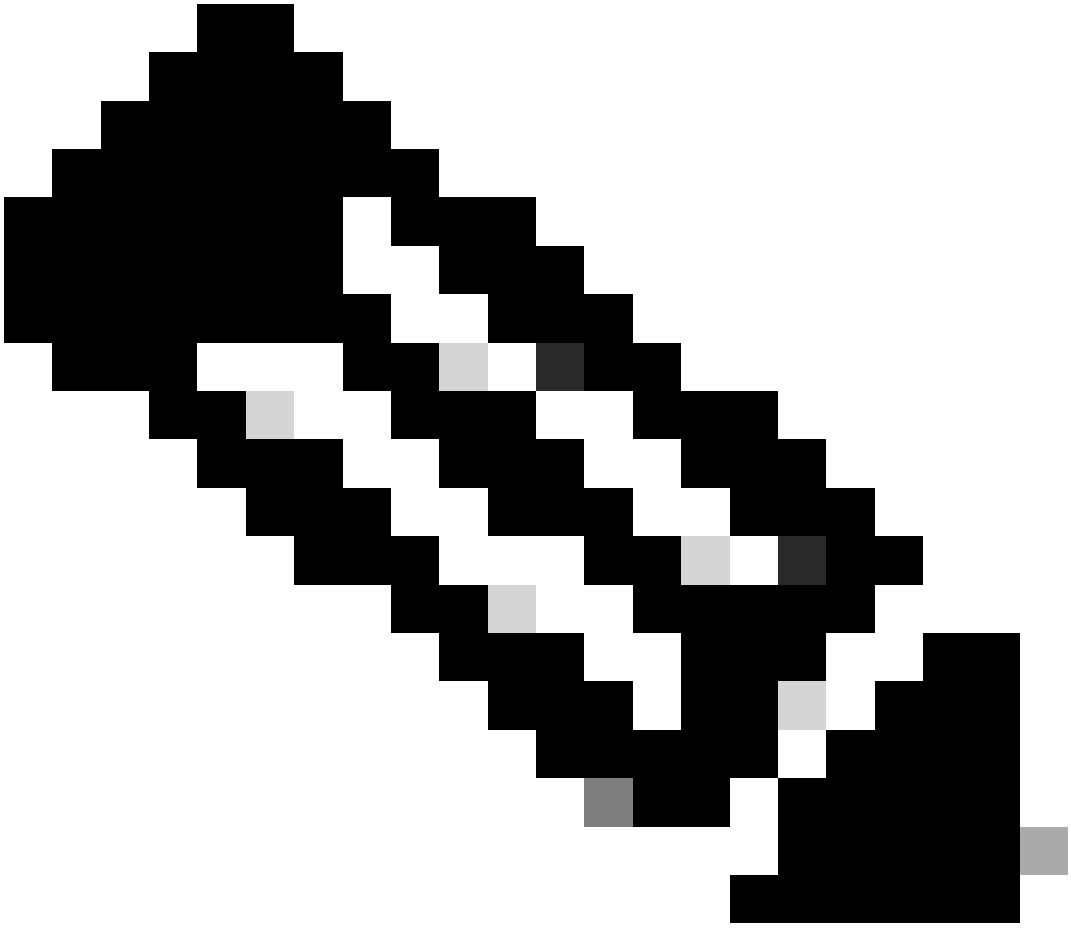
- AMP para terminales seguros para nube privada virtual
- Dispositivo web seguro (SWA)
- Gateway de correo electrónico seguro

Componentes Utilizados

SWA (Secure Web Appliance) 15.0.0-322

AMP para nube privada virtual 4.1.0_202311092226

Secure Email Gateway 14.2.0-620



Nota: La documentación es válida para variaciones físicas y virtuales de todos los productos involucrados.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comprobaciones de verificación antes de proceder a la integración

1. Compruebe si **Secure Endpoint Private Cloud/SWA/Secure Email Gateway** dispone de las licencias necesarias. Puede comprobar la clave de característica **SWA/Secure Email** o comprobar que la licencia inteligente está habilitada.
2. El proxy HTTPS debe estar activado en SWA si tiene previsto inspeccionar el tráfico HTTPS. Debe descifrar el tráfico HTTPS para poder realizar cualquier comprobación de reputación de archivos.
3. Se deben configurar el appliance AMP para nube privada/nube privada virtual y todos los

certificados necesarios. Consulte la guía de certificados VPC para obtener información sobre la verificación.

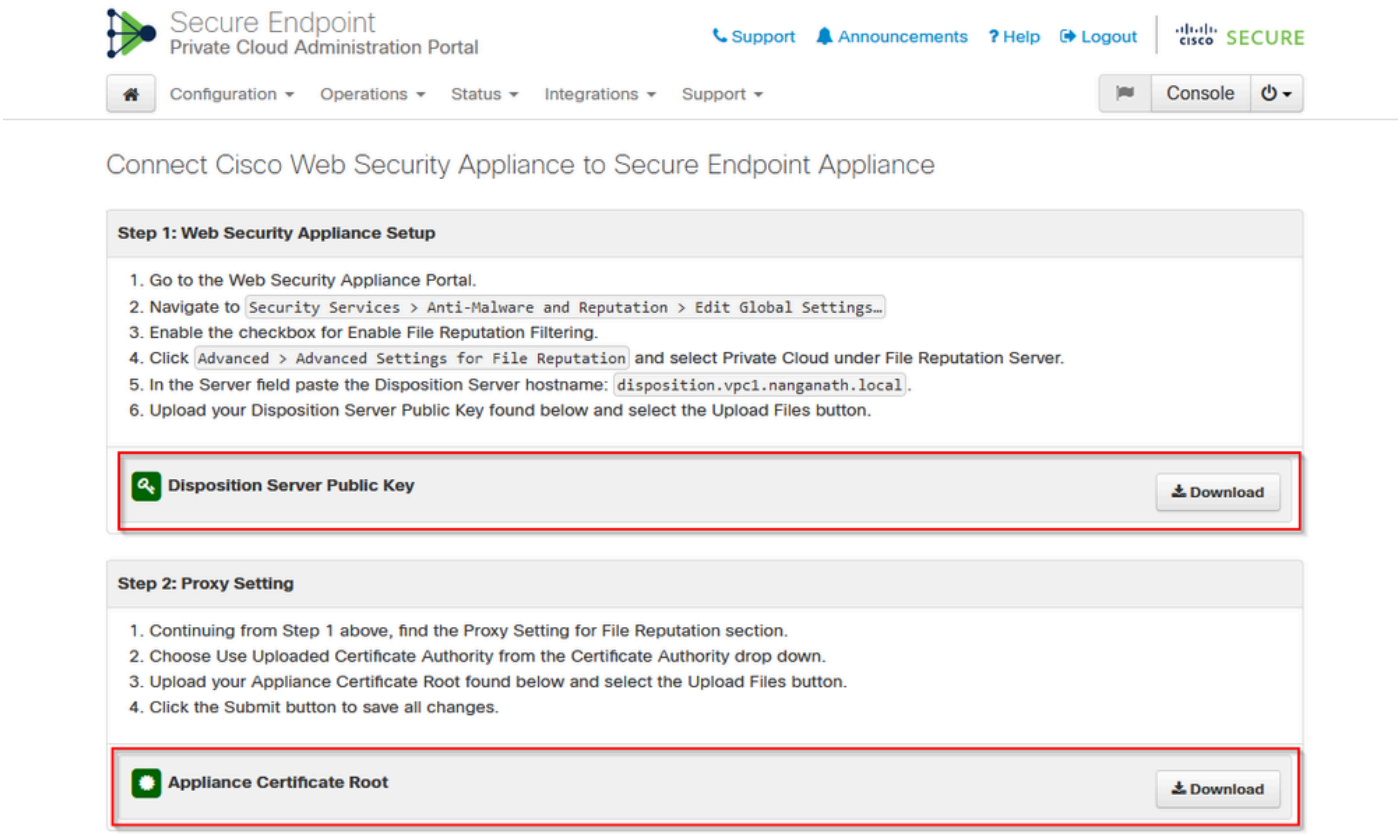
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html

4. Todos los nombres de host de los productos deben poder resolverse mediante DNS. Esto es para evitar cualquier problema de conectividad o problemas de certificados mientras se integra. En la nube privada de Secure Endpoint, la interfaz Eth0 es para el acceso de administrador y Eth1 debe poder conectarse con los dispositivos de integración.

Procedimiento

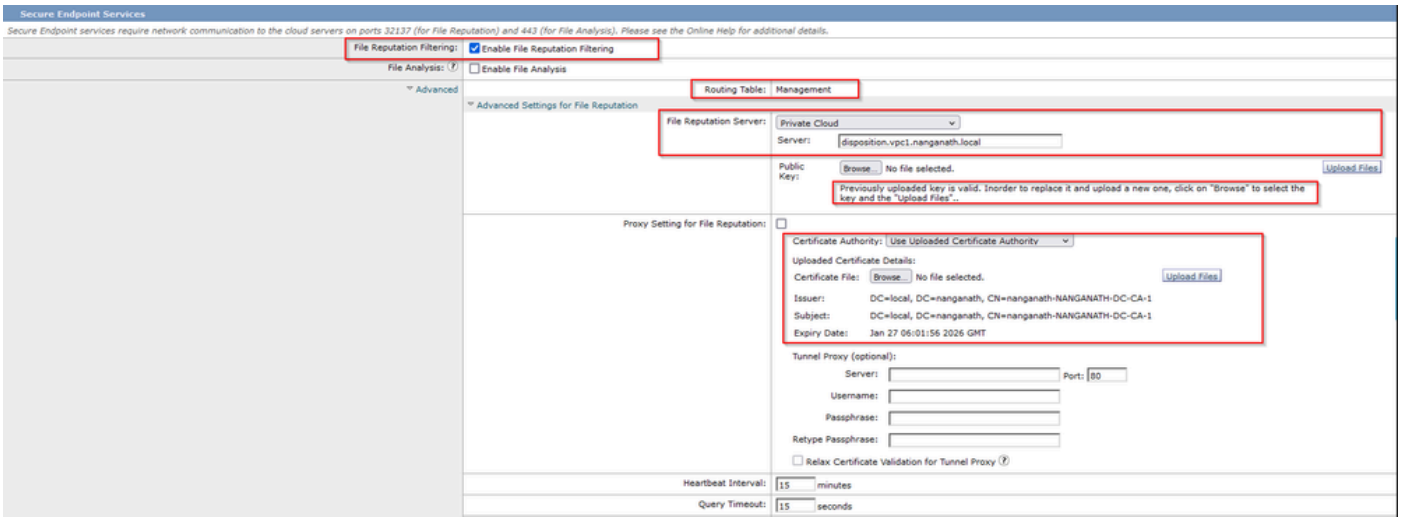
Configuración de la nube privada de terminal seguro

1. Inicie sesión en el **Secure Endpoint VPC admin portal.**
2. Vaya a **“Configuration”** > **“Services”** > **“Disposition Server”** > Copiar el nombre de host del servidor de disposición (también se puede obtener desde el tercer paso) .
3. Vaya a .**“Integrations”** > **“Web Security Appliance”**
4. Descargue el **“Disposition Server Public Key” & “Appliance Certificate Root”** .
5. Vaya a .**“Integrations”** > **“Email Security Appliance”**
6. Seleccione la versión de su ESA y descargue las opciones "Disposition Server Public Key" (Clave pública del servidor de disposición) y "Appliance Certificate Root" (Raíz del certificado del dispositivo).
7. Por favor, guarde el certificado y la clave a salvo. Debe cargarse en SWA/Secure Email más tarde.



Configuración del dispositivo web seguro

1. Vaya a **SWA GUI > "Security Services" > "Anti-Malware and Reputation" > Edit Global Settings**
2. En la sección "Secure Endpoint Services" puede ver la opción "Enable File Reputation Filtering" (Activar filtrado de reputación de archivos) y "Check" (Comprobar). Esta opción muestra un nuevo campo "Advanced" (Avanzado).
3. Seleccione "Nube privada" en File Reputation Server.
4. Proporcione el nombre de host del servidor de disposición de la nube privada como "Servidor".
5. Cargue la clave pública que descargó anteriormente. Haga clic en Cargar archivos.
6. Existe la opción de cargar la autoridad de certificación. Elija "Usar autoridad de certificación cargada" en el menú desplegable y cargue el certificado de CA que descargó anteriormente.
7. Envíe el cambio
8. Confirme el cambio



Configuración de Cisco Secure Email

1. Acceda a **Secure Email GUI > Security Services" > "File Reputation and Analysis" > Edit Global Settings > "Enable" or "Edit Global Settings"**

2. Seleccione "Nube privada" en File Reputation Server

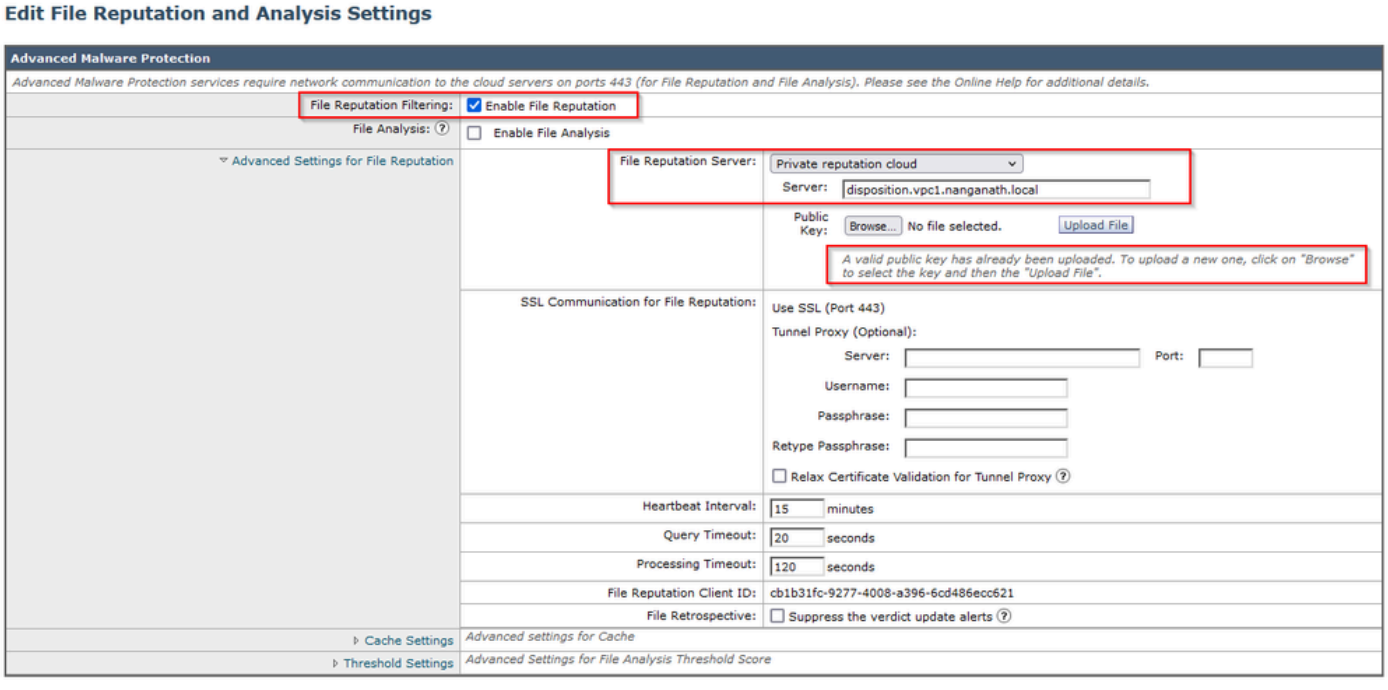
3. Proporcione el nombre de host del servidor de disposición de la nube privada como "Servidor".

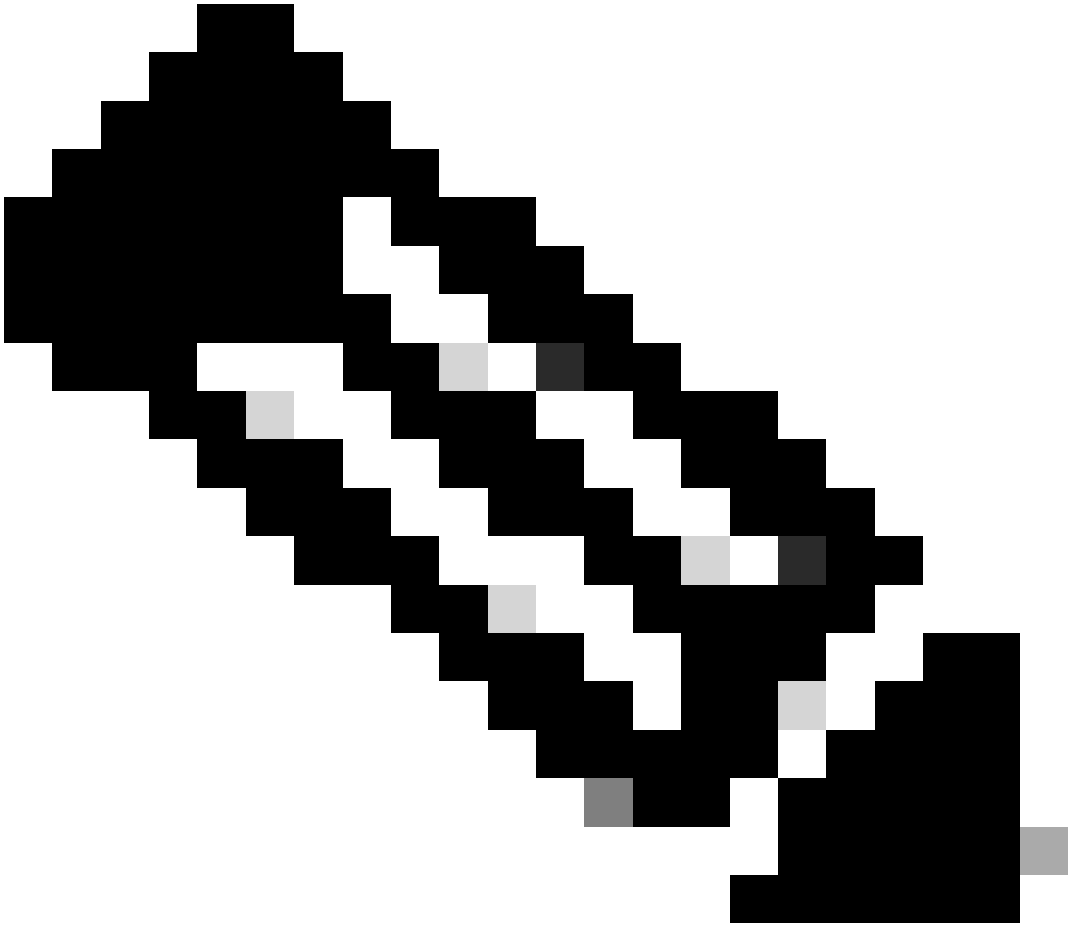
4. Cargue la clave pública que hemos descargado anteriormente. Haga clic en Cargar archivos.

5. Cargue la autoridad certificadora. Elija "Usar autoridad de certificación cargada" en el menú desplegable y cargue el certificado de CA que descargó anteriormente.

6. Ejecute el cambio

7. Confirme el cambio





Nota: Cisco Secure Web Appliance y Cisco Secure Email Gateway se basan en AsyncOS y comparten casi los mismos registros cuando se inicializa la reputación del archivo. El registro de AMP se puede observar en los registros de AMP de Secure Web Appliance o Secure Email Gateway (registros similares en ambos dispositivos). Esto solo indica que el servicio se ha inicializado en el SWA y el gateway de correo electrónico seguro. No indicó que la conectividad fuera completamente exitosa. Si hay algún problema de conectividad o de certificado, puede ver errores después del mensaje "Reputación de archivos inicializada". Principalmente, indica un error de "error inalcanzable" o "certificado no válido".

Los pasos para obtener registros de AMP desde la Web segura y el correo electrónico

1. Inicie sesión en la CLI de SWA/Secure Email Gateway y escriba el comando "**grep**"

2. Seleccione **"amp" or "amp_logs"**

3. Deje todos los demás campos tal como están y escriba "Y" para finalizar los registros. Siga los registros para mostrar los eventos en directo. Si está buscando eventos antiguos, puede escribir la fecha en "expresión regular"

```
Tue Feb 20 18:17:53 2024 Info:  connecting to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info:  connected to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info:  File reputation service initialized successfully
Tue Feb 20 18:17:53 2024 Info:  The following file type(s) can be sent for File Analysis:Executables, Document,
Microsoft Documents, Database, Miscellaneous, Encoded and Encrypted, Configuration, Email, Archived and compress
ed. To allow analysis of new file type(s), go to Security Services > File Reputation and Analysis.
```

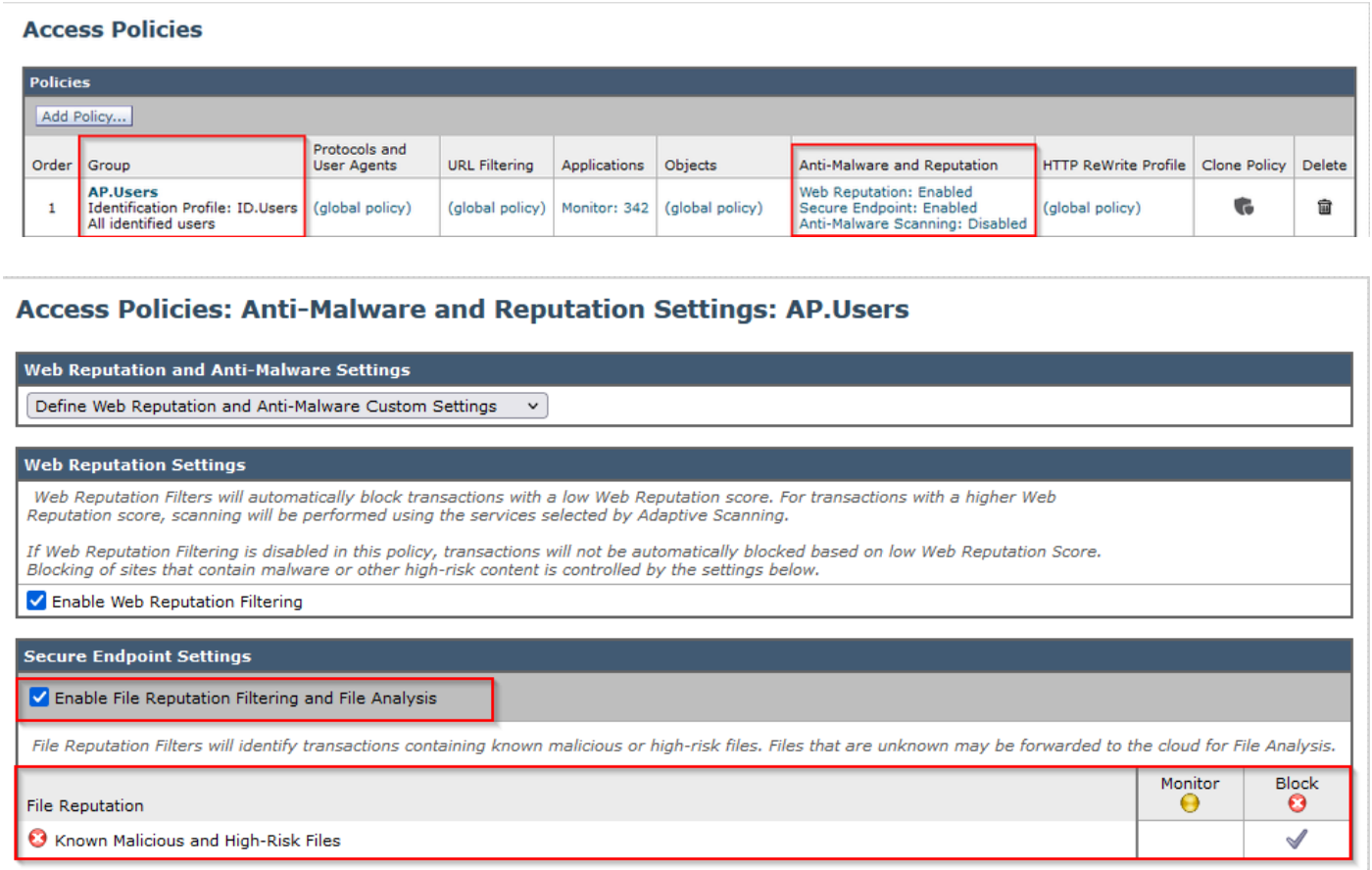
Prueba de la integración entre el dispositivo web seguro y la nube privada de terminal seguro.

No existe ninguna opción directa para probar la conectividad desde SWA. Debe inspeccionar los registros o alertas para comprobar si hay algún problema.

Para simplificar el proceso, estamos probando una URL HTTP en lugar de HTTPS. Tenga en cuenta que debe descifrar el tráfico HTTPS para realizar cualquier comprobación de reputación de archivos.

La configuración se realiza en la política de acceso de SWA y se aplica el análisis de AMP.

Nota: Revise la guía del usuario de SWA para saber cómo configurar las políticas en Cisco Secure Web Appliance.



Se intentó descargar un archivo malicioso "Bombermania.exe.zip" de Internet a través del dispositivo web seguro de Cisco. El registro muestra que el archivo malicioso está BLOQUEADO.

Registros de acceso SWA

Los registros de acceso se pueden obtener mediante estos pasos.

1. Inicie sesión en SWA y escriba el comando "**grep**"

2. Seleccione "**accesslogs**"

3. Si desea agregar cualquier "expresión regular" como la IP del cliente, menciónelo.

4. Escriba "Y" para finalizar el registro

1708320236.640 61255 10.106.37.205 TCP_DENIED/403 2555785 GET http://static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsF - DEFAULT_PARENT/bgl11-lab-wsa-2.cisco.com application/zip BLOCK_AMP_RESP_12-AP.Users-ID.Users-NONE-NONE-NONE-DefaultGroup-NONE <"IW_comp",3.7,1,"-",-,-,-,1,"-,-,-"-,-","-","-" "-",-,-,"IW_comp",-,"AMP High Risk","Computers and Internet","-","Unknown","Unknown","-","-",333.79,0,-,"-","-",37,"Win.Ransomware.Protected::Trojan.Agent.talos",0,0,"Bombermania.exe.zip","46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8",3,-"-",-,-> -

TCP_DENIED/403 —> SWA denegó esta solicitud GET HTTP.

BLOCK_AMP_RESP —> La solicitud GET HTTP se bloqueó debido a la respuesta de AMP.

Win.Ransomware.Protected::Trojan.Agent.talos —> Nombre de la amenaza

Bombermania.exe.zip —> Nombre de archivo que hemos intentado descargar

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —> valor SHA del archivo

Registros de AMP SWA

Los registros de AMP se pueden obtener mediante estos pasos.

1. Inicie sesión en SWA y escriba el comando "**grep**"

2. Seleccione "**amp_logs**"

3. Deje todos los demás campos tal como están y escriba "Y" para finalizar los registros. Siga los registros para mostrar los eventos en directo. Si está buscando eventos antiguos, puede escribir la fecha en "expresión regular"

'verdict_from': 'Nube' Parece ser lo mismo para nubes privadas y públicas. No lo confunda con un veredicto de la nube pública.

Lun 19 Feb 10:53:56 2024 Depuración: Veredicto ajustado - {'category': 'amp', 'spyname': 'Win.Ransomware.Protected::Trojan.Agent.talos', 'original_verdict': 'MALICIOUS', 'analysis_status':

18, 'verdict_num': 3, 'analysis_score': 0, 'upload': False, 'file_name': 'Bombermania.exe.zip', 'verdict_source': Ninguno, 'extract_file_verdict_list': '', 'verdict_from': 'Cloud', 'analysis_action': 2, 'file_type': 'application/zip', 'score': 0, 'upload_reason': 'File type is not configured for sandboxing', 'sha256': '46ee42fb79a161bf3763e8e34a047018bd 16d8572f8d31c2cdecae3d2e7a57a8', 'verdict_str': 'MALICIOUS', 'malicioso_child': None}

Registros de eventos de nube privada de terminal seguro

Los registros de eventos están disponibles en **/data/cloud/log**

Puede buscar el evento con el SHA256 o mediante la "ID de cliente de reputación de archivo" del SWA. "ID de cliente de Reputación de archivos" está presente en la página de configuración de AMP del SWA.

pv - Versión de protocolo, 3 indica TCP

ip: ignore este campo porque no hay garantía de que este campo indique la dirección IP real del cliente que realizó la consulta de reputación

uu: ID de cliente de reputación de archivos en WSA/ESA

SHA256 - SHA256 del archivo

dn: el nombre de la detección

n - 1 si AMP nunca ha visto el hash de archivos, 0 en caso contrario.

rd - Disposición de respuesta. aquí 3 significa DISP_MALICIOUS

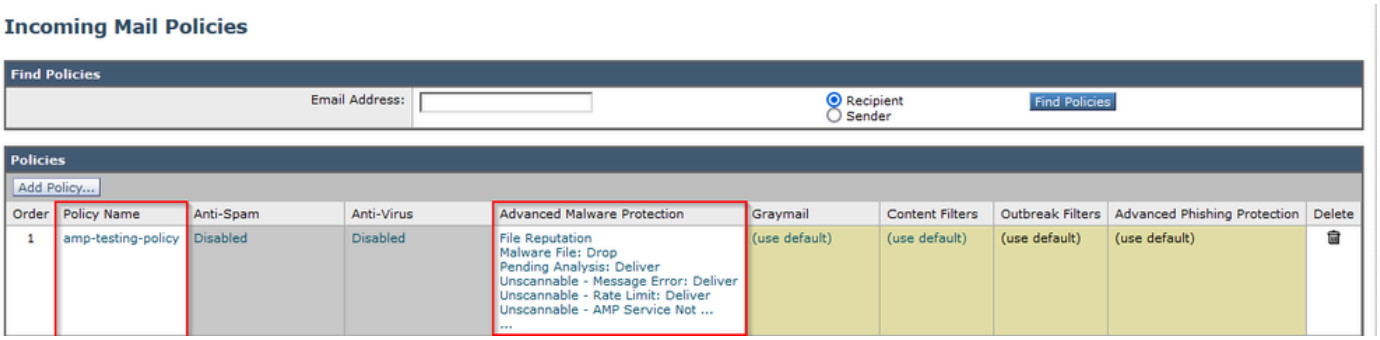
1 DISP_UNKNOWN Se desconoce la disposición del archivo.
2 DISP_CLEAN Se cree que el archivo es benigno.
3 DISP_MALICIOUS Se cree que el archivo es malicioso.
7 DISP_UNSEEN La disposición del archivo es desconocida y es la primera vez que vemos el archivo.
13 DISP_BLOCK No se debe ejecutar el archivo.
14 DISP_IGNORE XXX
15 DISP_CLEAN_PARENT Se cree que el archivo es benigno, por lo que cualquier archivo malicioso que cree debe tratarse como desconocido.
16 DISP_CLEAN_NFM Se cree que el archivo es benigno, pero el cliente debe supervisar el tráfico de red.

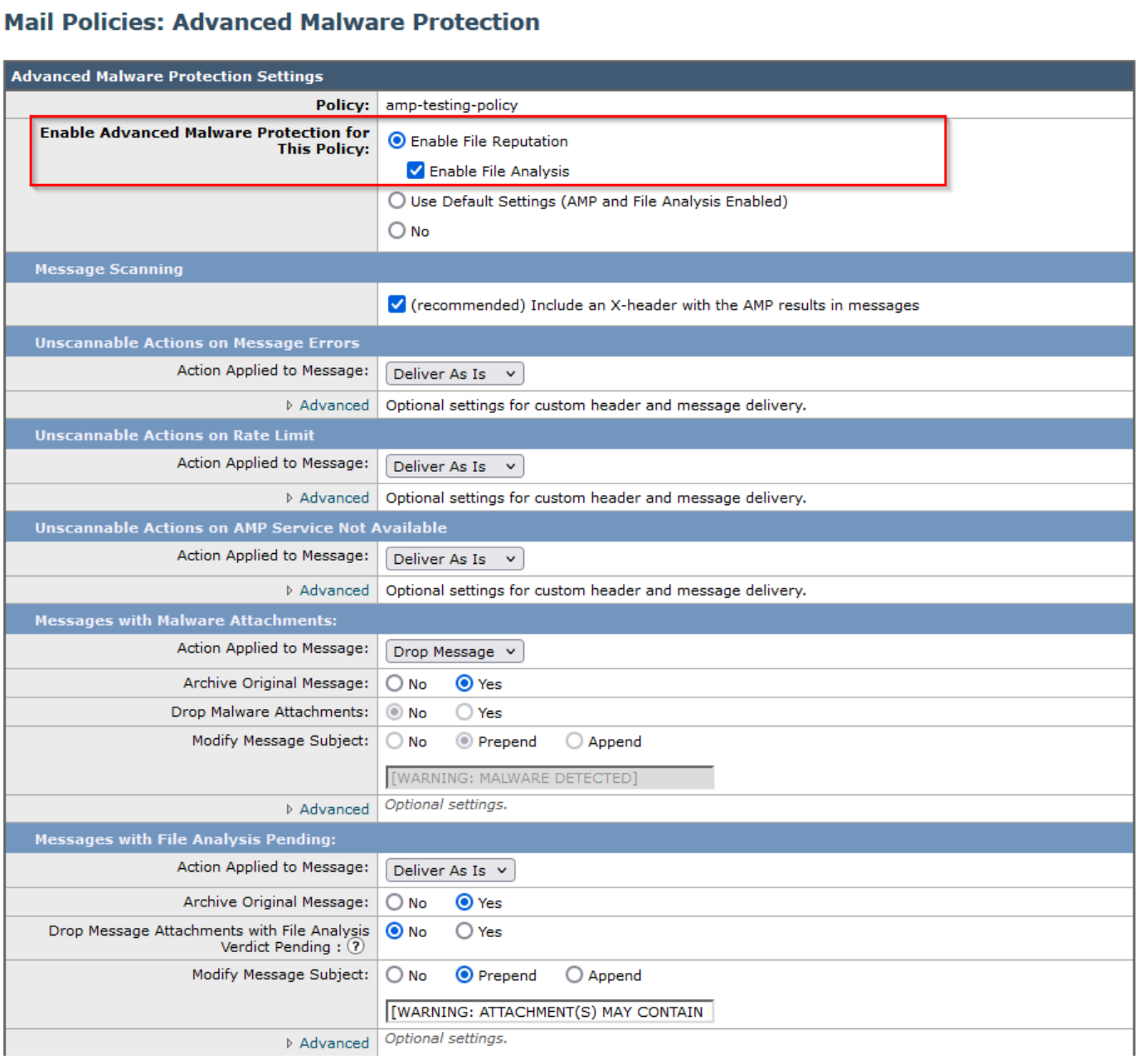
Prueba de la integración entre Secure Email y la nube privada de AMP

No existe ninguna opción directa para probar la conectividad desde el gateway de correo electrónico seguro. Debe inspeccionar los registros o alertas para comprobar si hay algún

problema.

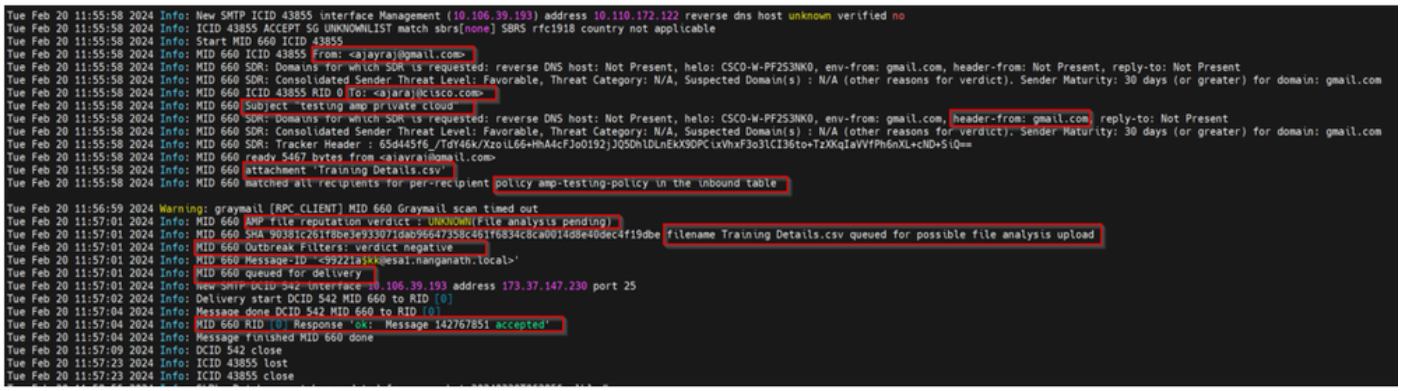
La configuración se realiza en la directiva de correo entrante de correo electrónico seguro para aplicar el análisis de AMP.





ESA probado con un archivo no malintencionado. Este es un archivo CSV.

Correo electrónico seguro mail_logs



Registros de AMP de correo electrónico seguro

Mar Feb 20 11:57:01 2024 Info: Respuesta recibida para la consulta de reputación de archivos desde la nube. Nombre de archivo = Detalles de formación.csv, MID = 660, Disposición = ARCHIVO DESCONOCIDO, Malware = Ninguno, Puntuación del análisis = 0, sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe, upload_action = Se recomienda enviar el archivo para su análisis, veredicto t_source = AMP, categorías_sospechosas = Ninguna

Registros de eventos de Secure Endpoint Private Cloud

{"pv":3,"ip":"10.106.72.238","si":0,"ti":14,"tv":6,"qt":42,"pr":1,"ets":1708410419,"ts":1708410366,"tsns":299
9277-4008-a396-6cd4
86ecc621","ai":1,"aptus":295,"ptus":2429102,"spero":{"h":"00","fa":0,"fs":0,"ft":0,"hd":1},"sha256":{"h":"903
0014D8E40DEC4F19DBE","fa":0,"fs":0,"ft":0,"hd":1},"hord":[32,4],"rd":1,"ra":1,"n":0}

rd - 1 DISP_UNKNOWN. Se desconoce la disposición del archivo.

Problemas habituales observados que provocan errores de integración

1. Elegir la "tabla de routing" incorrecta en SWA o correo electrónico seguro. El dispositivo integrado debe poder comunicarse con la interfaz Eth1 de la nube privada de AMP.
2. El nombre de host de VPC no se puede resolver mediante DNS en SWA o Secure Email, lo que provoca un fallo al establecer la conexión.
3. El CN (nombre común) del certificado de disposición de VPC debe coincidir con el nombre de host de VPC, así como con el mencionado en SWA y Secure Email Gateway.
4. El uso de una nube privada y un análisis de archivos en la nube no es un diseño compatible. Si utiliza un dispositivo en las instalaciones, el análisis de archivos y la reputación deben ser un servidor en las instalaciones.
5. Asegúrese de que no haya ningún problema de sincronización horaria entre la nube privada de AMP y SWA, Secure Email.
6. El valor predeterminado del límite de escaneo de objetos del motor DVS de SWA es 32 MB.

Ajuste esta configuración si desea analizar archivos más grandes. Tenga en cuenta que se trata de una configuración global que afecta a todos los motores de análisis, como Webroot, Sophos, etc.

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).