Configuración de la integración de la protección frente a malware avanzado (AMP) SD-WAN y solución de problemas

Contenido

Introducción

Este documento describe cómo configurar y resolver problemas de la integración de protección frente a malware avanzado (AMP) de Cisco SD-WAN en un router SD-WAN Cisco IOS® XE.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Advanced Malware Protection (AMP)
- Red de área extensa definida por software (SD-WAN) de Cisco

Componentes Utilizados

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.

Descripción general de soluciones

Componentes

La integración de AMP de SD-WAN es una parte integral de la solución de seguridad de extremo de SD-WAN que tiene como objetivo la visibilidad y la protección de los usuarios en una sucursal frente al malware.

Consta de los siguientes componentes del producto:

- **Router de extremo WAN en una sucursal.** Se trata de un router Cisco IOS® XE en modo de controlador con funciones de seguridad en un contenedor UTD
- **Nube de AMP.** La infraestructura de nube de AMP responde a las consultas de hash de archivos con una disposición
- **ThreatGrid**. La infraestructura de nube que puede probar un archivo para detectar malware potencial en un entorno aislado.

Estos componentes funcionan conjuntamente para ofrecer estas funciones clave para AMP:

- **Evaluación de reputación de archivos**

El proceso de hash SHA256 utilizado para comparar el archivo con el servidor en la nube de protección frente a malware avanzado (AMP) y acceder a su información de inteligencia de amenazas. La respuesta puede ser Limpia, Desconocida o Malintencionada. Si la respuesta es Unknown (Desconocido) y se configura File Analysis (Análisis de archivos), el archivo se envía automáticamente para su posterior análisis.

- **Análisis de archivos**

Se envía un archivo desconocido a la nube de ThreatGrid (TG) para su detonación en un entorno aislado. Durante la detonación, el espacio aislado captura artefactos y observa los comportamientos del archivo y, a continuación, asigna una puntuación global al archivo. Según las observaciones y la puntuación, Threat Grid puede cambiar la respuesta ante amenazas a Limpia o Malintencionada. Las conclusiones de ThreatGrid se devuelven a la nube de AMP para que todos los usuarios de AMP estén protegidos frente al malware recién descubierto.

- **Retrospección**

Mantiene información sobre los archivos, incluso después de que se descargan, podemos informar sobre los archivos que se determinó que eran maliciosos después de que se descargaron. La disposición de los archivos podría cambiar en función de la nueva inteligencia de amenazas que ha obtenido la nube de AMP. Esta reclasificación genera notificaciones retrospectivas automáticas.

Actualmente, la SD-WAN con integración de AMP admite la inspección de archivos para los protocolos:

- HTTP
- SMTP
- IMAP
- POP3
- FTP
- SMB

Nota: La transferencia de archivos sobre HTTPS sólo se soporta con el proxy SSL/TLS .

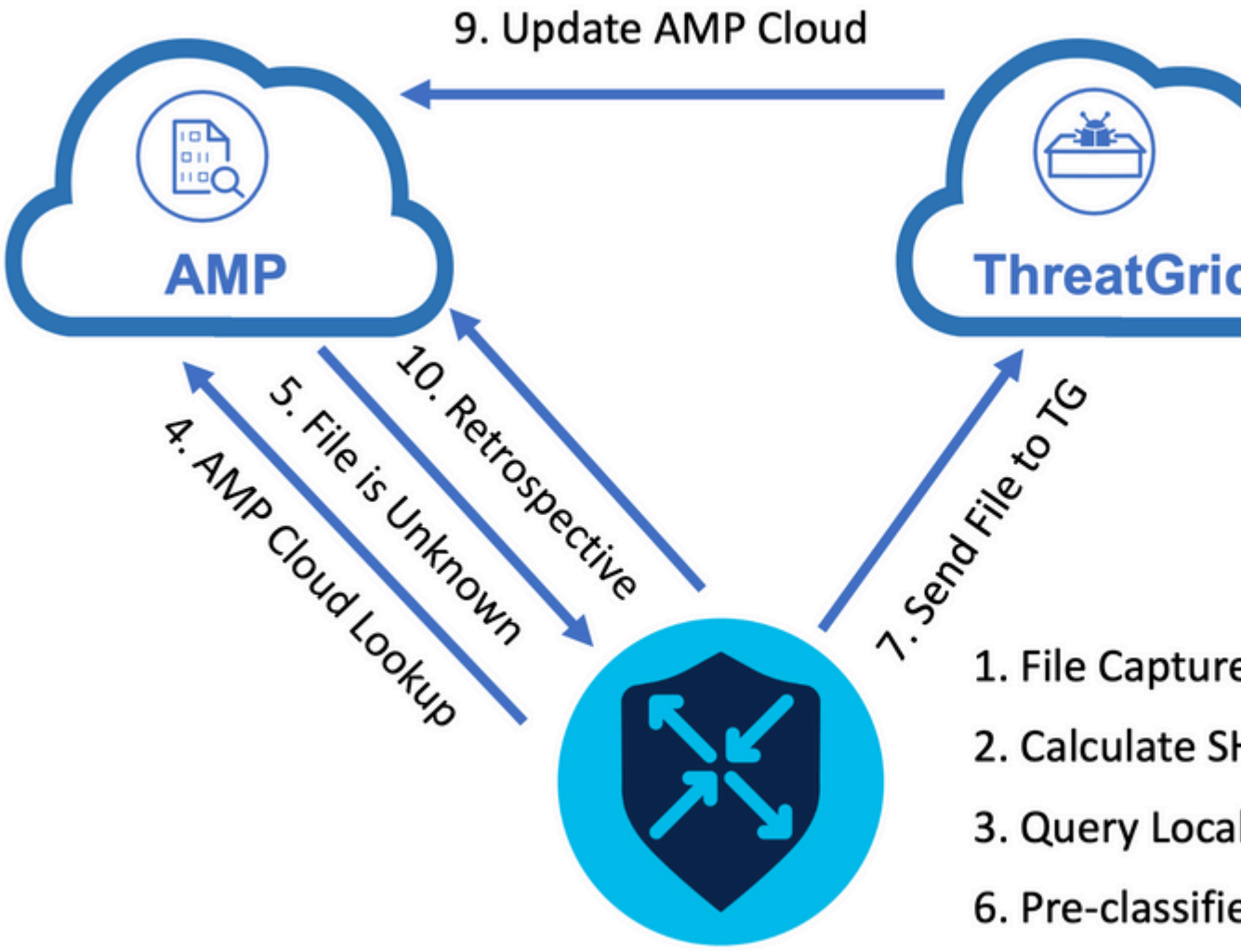
Nota: El análisis de archivos solo se puede realizar en un archivo completo, y no en un archivo dividido en contenido parcial. Por ejemplo, cuando un cliente HTTP solicita contenido parcial con el encabezado Range y devuelve ***contenido parcial de HTTP/1.1 206.*** En este caso, dado que el hash parcial del archivo es significativamente diferente del archivo completo, Snort omite la inspección del

---

archivo para el contenido parcial.

Flujo de funciones

La imagen muestra el flujo de alto nivel para la integración de AMP de SD-WAN cuando es necesario enviar un archivo a ThreatGrid para su análisis.



Para el flujo indicado:

1. El contenedor UTD captura la transferencia de archivos para los protocolos compatibles con AMP.
2. Se calcula el hash SHA256 para el archivo.
3. El hash SHA256 calculado se consulta con el sistema de caché local en UTD para ver si la disposición ya se conoce y si el TTL de caché no ha caducado.
4. Si no hay ninguna coincidencia con la caché local, el hash SHA256 se busca en la nube de AMP para obtener una disposición y una acción de devolución.
5. Si la disposición es UNKNOWN y la acción de respuesta es ACTION_SEND, el archivo se ejecuta a través del sistema de preclasificación en UTD.
6. El pre-clasificador determina el tipo de archivo y también valida si el archivo contiene contenido activo.
7. Si se cumplen ambas condiciones, el archivo se envía a ThreatGrid.
8. ThreatGrid activa el archivo en un espacio aislado y le asigna una puntuación de amenaza.

9. ThreatGrid actualiza la nube de AMP basándose en la evaluación de amenazas.
10. El dispositivo perimetral solicita a la nube de AMP información retrospectiva en función del intervalo de latidos de 30 minutos.

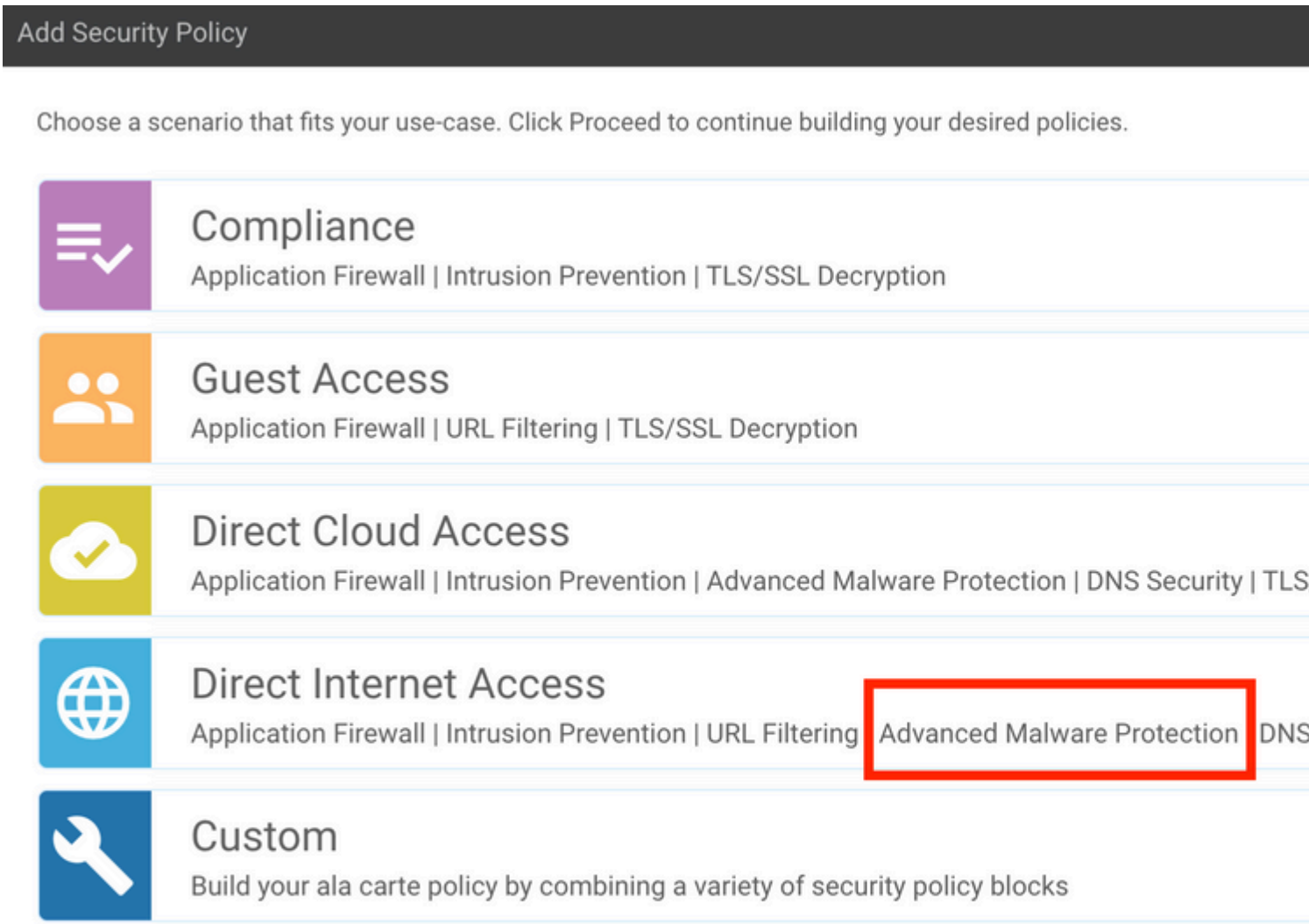
Configuración de la integración de AMP de SD-WAN

Nota: Se debe cargar una imagen virtual de seguridad en vManage antes de configurar la función de AMP. Para obtener más información, navegue hasta Imagen virtual de seguridad .

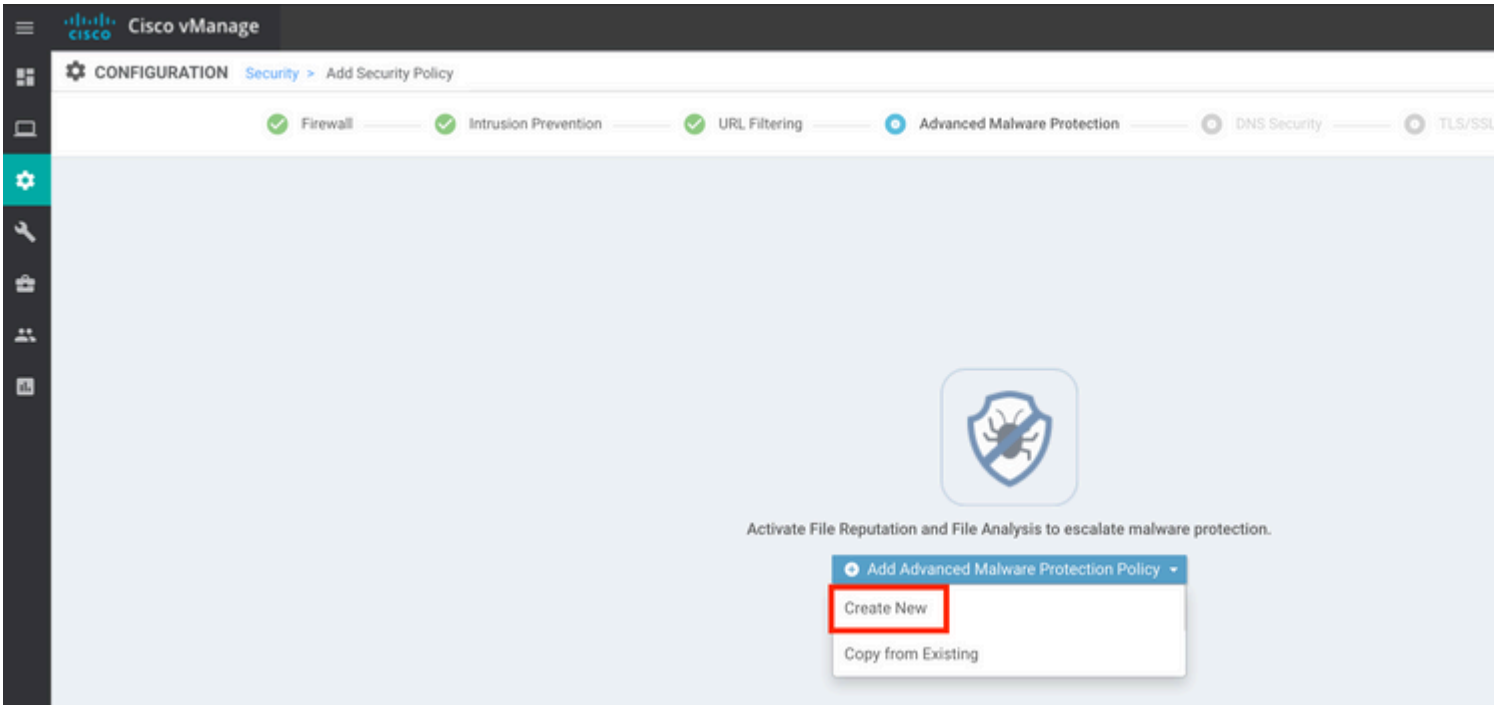
Nota: Revise este documento para ver los requisitos de red para que la conectividad de AMP/ThreatGrid funcione correctamente: Direcciones IP/Nombres de host requeridos por AMP/TG

Configurar la política de seguridad desde vManage

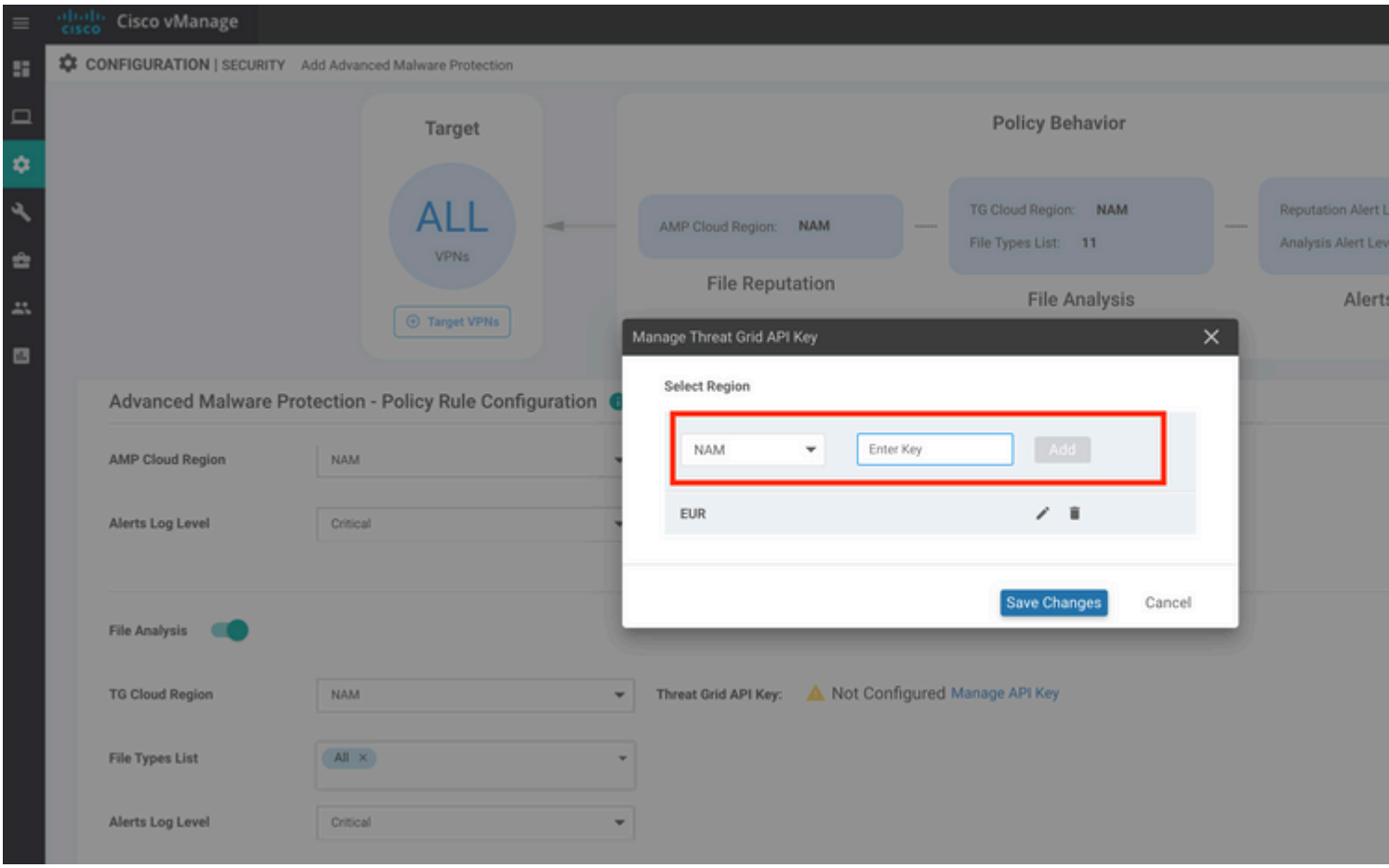
Para habilitar AMP, vaya a **Configuration** -> **Security** -> **Add Security Policy**. Seleccione Direct Internet Access (Acceso directo a Internet) y seleccione **Proceed (Continuar)** como se muestra en la imagen.



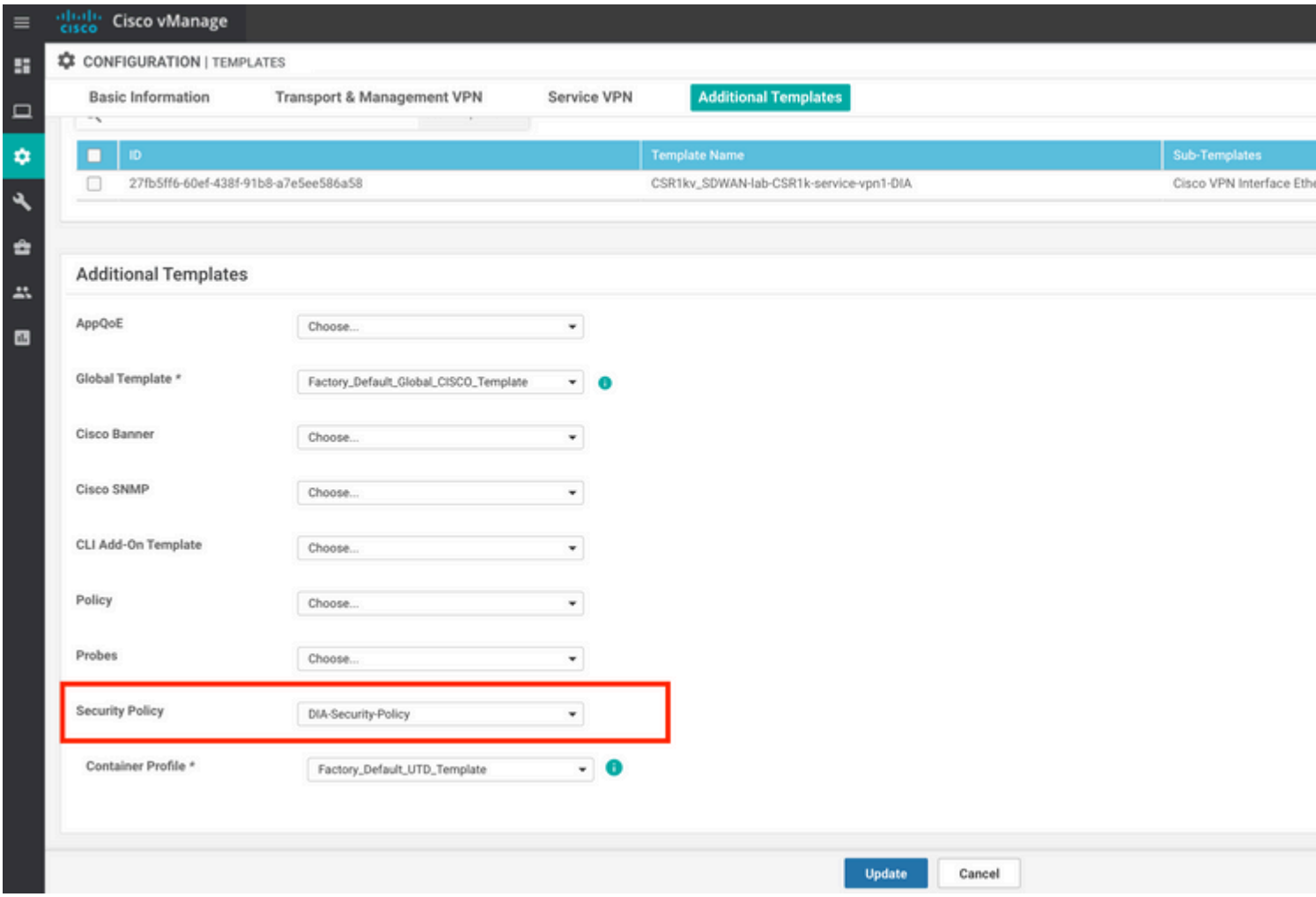
Configure las funciones de seguridad como desee hasta que acceda a la función de protección frente a malware avanzado. Agregue una nueva política de protección frente a malware avanzado.



Proporcione un nombre de directiva. Seleccione una de las regiones globales de la nube de AMP y active Análisis de archivos. Para el análisis de archivos con ThreatGrid utilizado, elija una de las regiones de nube de TG e introduzca la clave de la API de ThreatGrid, que se puede obtener del portal de ThreatGrid en **Mi cuenta de ThreatGrid.**



Una vez hecho esto, guarde la política y agregue esta política de seguridad a la plantilla Device bajo **Additional Templates** -> **Security Policy**, como se muestra en la imagen.



Configure el dispositivo con la plantilla de dispositivo actualizada.

Verificación

Una vez que la plantilla de dispositivo se envía correctamente al dispositivo de extremo, la configuración de AMP se puede verificar desde la CLI del router de extremo:

<#root>

```
branch1-edge1#show sdwan running-config | section utd
app-hosting appid utd
 app-resource package-profile cloud-low
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
!
app-vnic gateway1 virtualportgroup 1 guest-interface 1
 guest-ipaddress 192.0.2.2 netmask 255.255.255.252
!
 start
utd multi-tenancy
utd engine standard multi-tenancy
threat-inspection profile IPS_Policy_copy
threat detection
policy balanced
logging level notice
!
```

```
utd global
 file-reputation
  cloud-server cloud-isr-asn.amp.cisco.com
  est-server cloud-isr-est.amp.cisco.com
!
file-analysis
 cloud-server isr.api.threatgrid.com
 apikey 0 <redacted>
!
!
file-analysis profile AMP-Policy-fa-profile
 file-types
  pdf
  ms-exe
  new-office
  rtf
  mdb
  mscab
  msole2
  wri
  xlw
  flv
  swf
!
 alert level critical
!
file-reputation profile AMP-Policy-fr-profile
 alert level critical
!
file-inspection profile AMP-Policy-fi-profile


analysis profile AMP-Policy-fa-profile


 reputation profile AMP-Policy-fr-profile


!
policy utd-policy-vrf-1
 all-interfaces
 file-inspection profile AMP-Policy-fi-profile
 vrf 1
 threat-inspection profile IPS_Policy_copy
exit
policy utd-policy-vrf-global
 all-interfaces
```

```
 file-inspection profile AMP-Policy-fi-profile


 vrf global
exit
no shutdown
```

Troubleshoot

La integración de AMP de SD-WAN implica muchos componentes, tal y como se describe. Por lo tanto, cuando se trata de solucionar problemas, es fundamental poder establecer algunos puntos de demarcación clave para reducir el problema a los componentes del flujo de funciones:

1. **vManage.** ¿Puede vManage trasladar correctamente la política de seguridad con la política de AMP al dispositivo periférico?
2. **Borde**. Una vez que la política de seguridad se aplica correctamente en el perímetro, ¿captura el router el archivo sujeto a la inspección de AMP y lo envía a la nube de AMP/TG?
3. **nube de AMP/TG.** Si el perímetro ha enviado el archivo a AMP o TG, ¿obtiene la respuesta que necesita para tomar una decisión de permitir o rechazar?

Este artículo está pensado para centrarse en el dispositivo de extremo (2) con las diversas herramientas de plano de datos disponibles para ayudar a solucionar problemas con la integración de AMP en el router de extremo de la WAN.

Flujo general de solución de problemas

Utilice este flujo de trabajo de alto nivel para solucionar rápidamente los problemas de los distintos componentes relacionados con la integración de AMP con un objetivo clave que permita establecer el punto de demarcación del problema entre el dispositivo de extremo y la nube de AMP/TG.

1. ¿Se aplica correctamente la política de AMP al dispositivo periférico?
2. Compruebe el estado general del contenedor UTD.
3. Compruebe la reputación del archivo y analice el estado del cliente en el perímetro.
4. Compruebe si la transferencia de archivos se desvía al contenedor. Esto se puede hacer con el seguimiento de paquetes de Cisco IOS® XE.
5. Verifique para confirmar que el perímetro se comunica correctamente con la nube de AMP/TG. Esto se puede hacer con herramientas como EPC o packet-trace.
6. Asegúrese de que UTD crea una caché local basada en la respuesta de AMP.

Estos pasos de solución de problemas se examinan en detalle en este documento.

Problemas de inserción de políticas en vManage

Como se muestra en la configuración de políticas de AMP, la política de AMP es bastante sencilla sin contar con muchas opciones de configuración. A continuación se indican algunos aspectos comunes que se deben tener en cuenta:

1. vManage debe poder resolver los nombres DNS de la nube de AMP y ThreatGrid para el acceso a la API. Si se produce un error en la configuración del dispositivo en vManage después de agregar la directiva AMP, compruebe si hay errores en **/var/log/nms/vmanage-server.log**.
2. Como se indica en la guía de configuración, el nivel de registro de alertas ha dejado el nivel crítico predeterminado, o Advertencia si está justificado. Se debe evitar el registro de nivel de información, ya que puede tener un impacto negativo en el rendimiento.

Para verificarlo, acceda a neo4j DB y vea el contenido de la tabla vmanagedbAPIKEYNODE.

```
neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +----------
----------
----------+ | n | +----------
----------+ | (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
"$CRYPT_CLUSTER$IbGLEMGlYMNRy1s9P+WcfA==$dozo7tmRP1+HrvEnXQr4x1VxSViYkKwQ4HBAlhXWOtQ=", deviceID:
"CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455"}) | +----------
----------
-----+
```

Integración de AMP en el router de extremo de Cisco

Comprobar el estado del contenedor UTD

Utilice los comandos show utd para verificar el estado general del contenedor UTD:

```
show utd engine standard config
show utd engine standard status
show platform hardware qfp active feature utd config
show platform hardware qfp active feature utd stats
show app-hosting detail appid utd
show sdwan virtual-application utd
```

Comprobar el estado de AMP de UTD

Asegúrese de que la inspección de archivos está habilitada:

<#root>

```
branch1-edge1#show sdwan utd dataplane config
 utd-dp config context 0
 context-flag 25427969
 engine Standard
 state enabled
 sn-redirect fail-open
 redirect-type divert
 threat-inspection not-enabled
 defense-mode not-enabled
 domain-filtering not-enabled
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled

utd-dp config context 1
 context-flag 25559041
 engine Standard
 state enabled
```

```
 sn-redirect fail-open
 redirect-type divert
 threat-inspection enabled
 defense-mode IDS
 domain-filtering not-enabled
 url-filtering not-enabled
 all-interface enabled
 file-inspection enabled
```

Verifique que la conexión a la nube de AMP esté activa:

<#root>

```
branch1-edge1#show utd engine standard status file-reputation
File Reputation Status:
        Process:
Running

        Last known status: 2021-06-17 16:14:20.357884-0400 [info] AMP module version 1.12.4.999
```

<#root>

```
branch1-edge1#show sdwan utd file reputation
utd-oper-data utd-file-reputation-status version 1.12.4.999
utd-oper-data utd-file-reputation-status status utd-file-repu-stat-connected

utd-oper-data utd-file-reputation-status message "Connected to AMP Cloud!"
```

Verifique que la conexión a ThreatGrid esté activa:

<#root>

```
branch1-edge1#show utd engine standard status file-analysis
File Analysis Status:
        Process:
Running

        Last Upload Status: No upload since process init
```

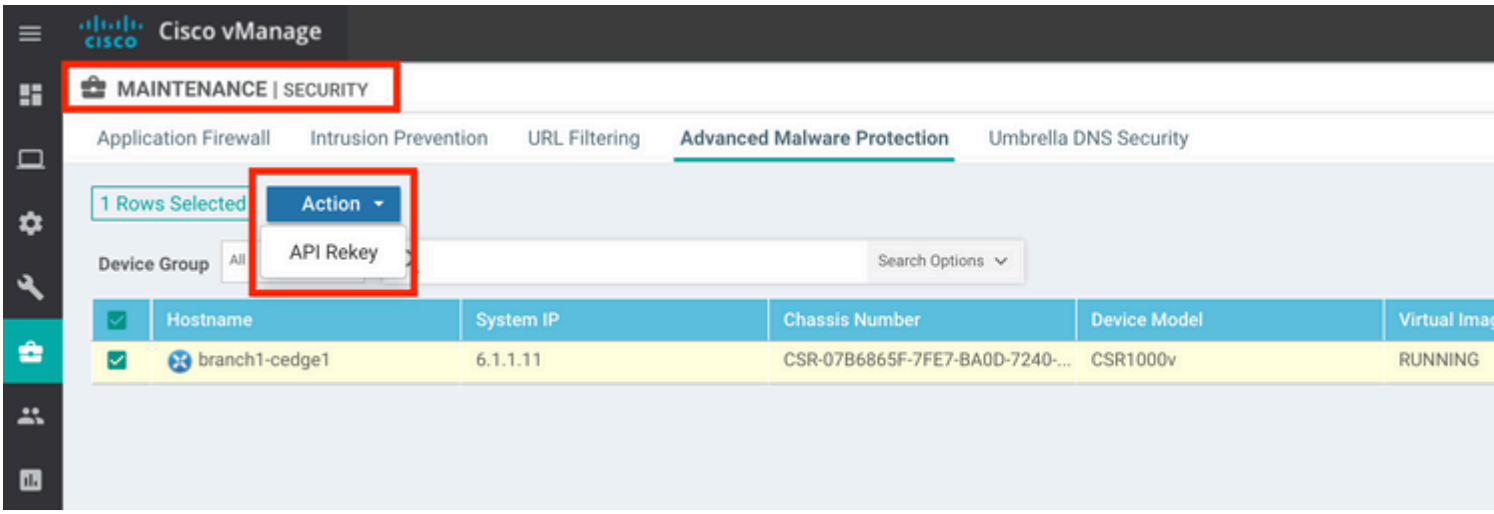
<#root>

```
branch1-edge1#show sdwan utd file analysis
utd-oper-data utd-file-analysis-status status tg-client-stat-up

utd-oper-data utd-file-analysis-status backoff-interval 0
```

```
utd-oper-data utd-file-analysis-status message "TG Process Up"
```

Si el proceso ThreatGrid no muestra el estado Up (Activo), puede resultar útil volver a crear la clave de la API. Para activar una nueva clave de API, navegue hasta **Mantenimiento** -> **Seguridad**:



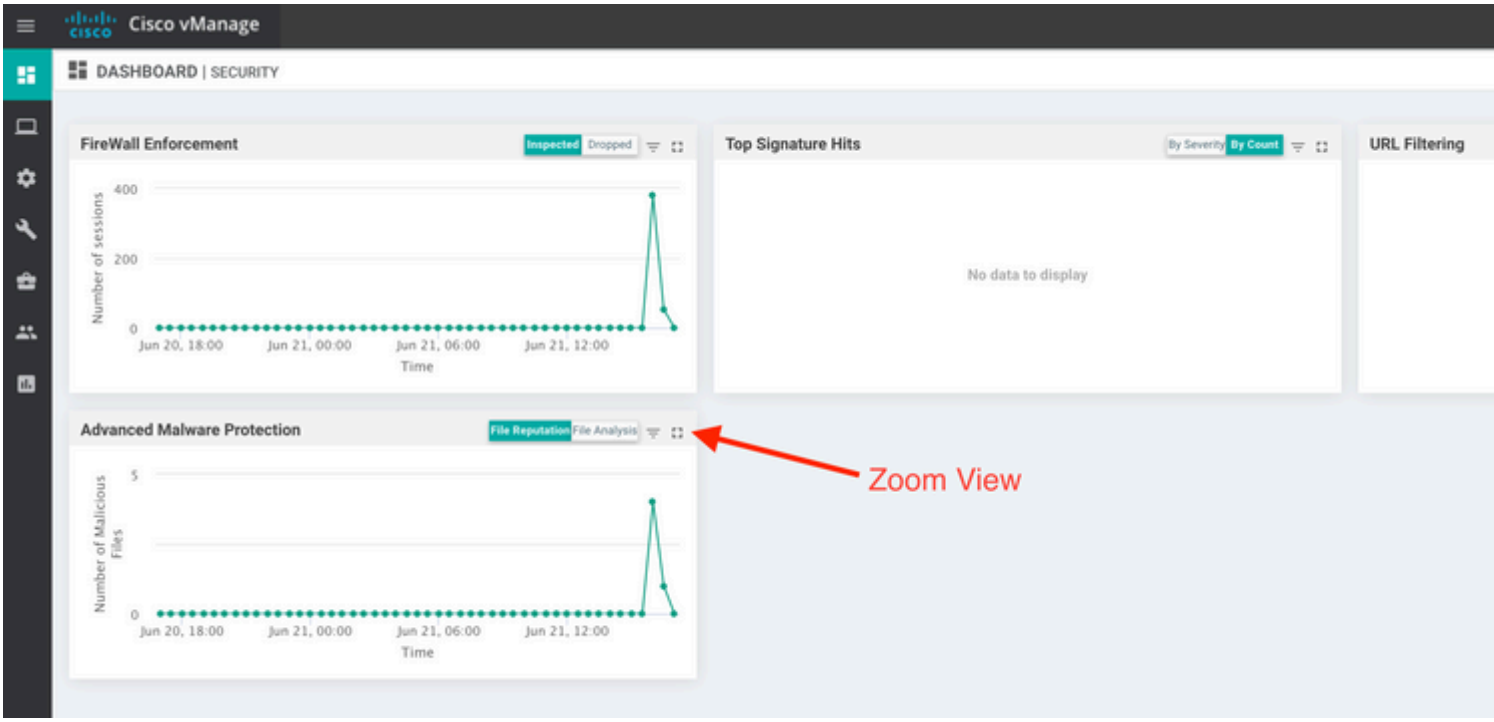
Nota: Una regeneración de clave de API activa una inserción de plantilla en el dispositivo.

Supervisión de actividad de AMP en router de extremo de WAN

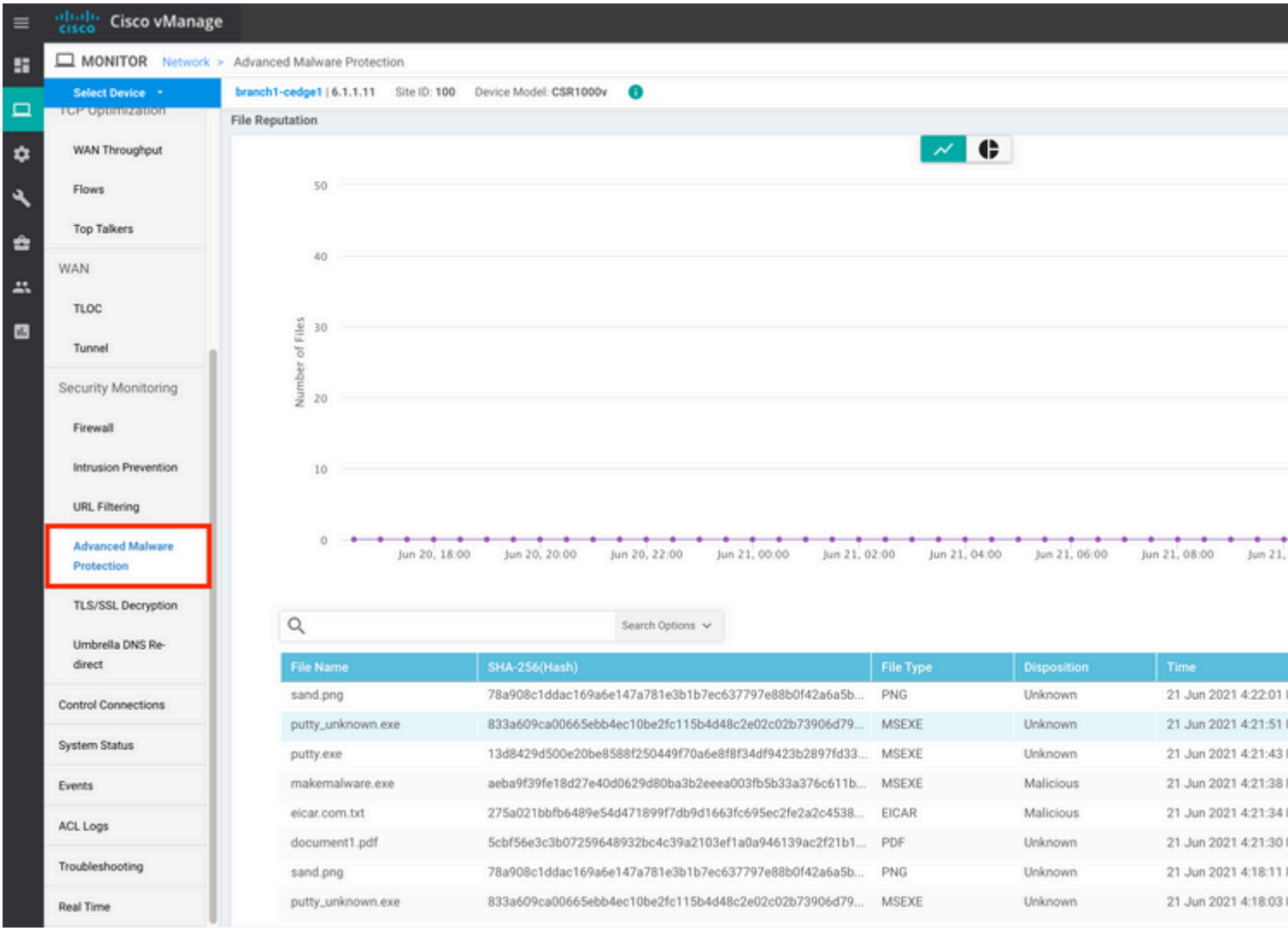
vManage

En vManage, las actividades del archivo de AMP se pueden supervisar desde el panel de seguridad o desde la vista de dispositivo.

Panel de seguridad:



Vista del dispositivo:



CLI

Comprobar estadísticas de reputación de archivos:

```
branch1-edge1#show utd engine standard statistics file-reputation
File Reputation Statistics
--------------------------
File Reputation Clean Count:            1
File Reputation Malicious Count:        4
File Reputation Unknown Count:         44
File Reputation Requests Error:         0
File Reputation File Block:             4
File Reputation File Log:              45
```

Comprobar estadísticas de análisis de archivos:

```
branch1-edge1#show utd engine standard statistics file-analysis
File Analysis Statistics
```

```
------------------------
File Analysis Request Received:         2
File Analysis Success Submissions:      2
File Analysis File Not Interesting:     0
File Analysis File Whitelisted:         0
File Analysis File Not Supported:       0
File Analysis Limit Exceeding:          0
File Analysis Failed Submissions:       0
File Analysis System Errors:            0
```

Nota: se pueden obtener estadísticas internas adicionales con el comando ***show utd engine standard statistics file-reputation vrf global internal***.

Comportamiento del plano de datos

El tráfico del plano de datos sujeto a la inspección de archivos según la política de AMP configurada se desvía al contenedor UTD para su procesamiento. Esto se puede confirmar con un seguimiento de paquetes utilizado. Si el tráfico no se desvía correctamente al contenedor, no se puede realizar ninguna de las acciones de inspección de archivos posteriores.

Caché de archivos locales de AMP

El contenedor UTD tiene una caché local de hash SHA256, tipo de archivo, disposición y acción basados en resultados de búsquedas anteriores en la nube de AMP. El contenedor solo solicita una disposición de la nube de AMP si el hash de archivo no está en la caché local. La caché local tiene un TTL de 2 horas antes de que se elimine la caché.

```
branch1-edge1#show utd engine standard cache file-inspection
Total number of cache entries: 6
File Name|                      SHA256|             File Type|        Disposition|         action|
-------------------------------------------------------------------------------------------------------
sand.png              78A908C1DDAC169A                    69                  1               1
putty.exe             13D8429D500E20BE                    21                  1               2
makemalware.exe       AEBA9F39FE18D27E                    21                  3               2
putty_unknown.exe     833A609CA00665EB                    21                  1               2
document1.pdf         5CBF56E3C3B07259                   285                  1               1
eicar.com.txt         275A021BBFB6489E                   273                  3               2
```

Código de disposición de AMP:

```
0 NONE
1 UNKNOWN
2 CLEAN
3 MALICIOUS
```

Código de acción de AMP:

```
0 UNKNOWN
```

```
1 ALLOW
2 DROP
```

Para obtener el hash SHA256 completo para los archivos, que es muy importante para resolver problemas de un veredicto de archivo específico, utilice la opción de detalle del comando:

```
branch1-edge1#show utd engine standard cache file-inspection detail
SHA256: 78A908C1DDAC169A6E147A781E3B1B7EC637797E88B0F42A6A5B59810B8E7EE5
amp verdict: unknown
amp action: 1
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 0
file name: sand.png
filetype: 69
create_ts: 2021-06-21 16:58:1624309104
sig_state: 3
-----------------------------------------------------------------------------------------
SHA256: 13D8429D500E20BE8588F250449F70A6E8F8F34DF9423B2897FD33BBB8712C5F
amp verdict: unknown
amp action: 2
amp disposition: 1
reputation score: 0
retrospective disposition: 0
amp malware name:
file verdict: 1
TG status: 7
file name: putty.exe
filetype: 21
create_ts: 2021-06-21 16:58:1624309107
sig_state: 3
-----------------------------------------------------------------------------------------
SHA256: AEBA9F39FE18D27E40D0629D80BA3B2EEEA003FB5B33A376C611BB4D8FFD03A6
amp verdict: malicious
amp action: 2
amp disposition: 3
reputation score: 95
retrospective disposition: 0
amp malware name: W32.AEBA9F39FE-95.SBX.TG
file verdict: 1
TG status: 0
file name: makemalware.exe
filetype: 21
create_ts: 2021-06-21 16:58:1624309101
sig_state: 3
<SNIP>
```

Para eliminar las entradas de caché local del motor UTD, utilice el comando:

```
clear utd engine standard cache file-inspection
```

Ejecutar depuración UTD

Los debugs utd se pueden habilitar para resolver problemas de AMP:

```
debug utd engine standard file-reputation level info
debug utd engine standard file-analysis level info
debug utd engine standard climgr level info
```

El resultado de la depuración se puede recuperar directamente desde el shell del sistema en **/tmp/rp/trace/vman_utd_R0-0.bin**, o copiar el archivo de seguimiento en el sistema de archivos del router con los pasos:

```
branch1-edge1#app-hosting move appid utd log to bootflash:
Successfully moved tracelog to bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
branch1-edge1#
```

Para ver el registro de seguimiento de UTD:

```
branch1-edge1#more /compressed bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
<snip>
2021-06-22 10:35:04.265:(#1):SPP-FILE-INSPECTION File signature query: sig_state = 3
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION start_time : 1624372489, current_time : 1624372504,Diff
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_node_exists:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Signature not found in cache
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION file_type_id = 21
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Write to cbuffer
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Sent signature lookup query to Beaker
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION File Name = /putty_unknown.exe, file_name = /putty_unkn
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_extract_filename :: Extracted filename 'putty_unkno
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_add:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_allocate:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Return FILE_VERDICT_PENDING
<SNIP>
```

> **Nota**: En 20.6.1 y versiones posteriores, la forma de recuperar y ver los tracelogs utd está en línea con el flujo de trabajo de seguimiento estándar con **show logging process vman module utd** ... comando.

Verificar la comunicación del perímetro a la nube

Para verificar que el dispositivo periférico se comunica con la nube de AMP/TG, se puede utilizar EPC en el router de extremo de la WAN para confirmar que existe comunicación bidireccional hacia/desde los servicios en la nube:

```
branch1-edge1#show monitor capture amp parameter
```

```
monitor capture amp interface GigabitEthernet1 BOTH
monitor capture amp access-list amp-cloud
monitor capture amp buffer size 10
monitor capture amp limit pps 1000
```

Problemas relacionados con AMP y TG Cloud

Una vez que se confirma, el dispositivo periférico captura correctamente el archivo y lo envía a AMP/TG para su análisis, pero el veredicto es incorrecto, requiere la solución de problemas de AMP o la nube de Threatgrid, que está fuera del alcance de este documento. La información es importante cuando se presentan problemas de integración:

- Organización de cuentas ThreatGrid
- Grupo fecha/hora
- Device Analysis ID (por ejemplo, CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455), es el número de chasis del router de extremo de la WAN.
- Hash SHA256 completo para el archivo en cuestión

Información Relacionada

- Guía de configuración de seguridad de SD-WAN
- Portal de ThreatGrid
- 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).