Solucionar problemas de acceso al sitio web de SWG de gateway web segura

Contenido

Introducción

Este documento describe la metodología estructurada para diagnosticar problemas de acceso al sitio web cuando se enruta a través de un proxy basado en la nube (gateway web seguro/SWG), pero no cuando se utiliza el acceso directo a Internet (DIA).

- Alcance: Se aplica a Cisco Umbrella SIG y Cisco Secure Access.

Requisitos previos y advertencias importantes

- Verifique que se realice toda la resolución de problemas en los problemas reproducibles.
- Recopile un archivo HAR (HTTP Archive) y una captura de paquetes (PCAP) simultánea para proporcionar datos precisos para el análisis.
- Los cambios en las políticas de proxy (por ejemplo, omitir el descifrado o la inspección) pueden afectar a la condición en materia de seguridad; aplique solo para la resolución de problemas o como se recomienda.

Identificar errores de nivel de proxy

Entre los indicadores de interferencia de proxy habituales se incluyen:

- 502 Puerta de enlace incorrecta
- 515 Certificado ascendente no fiable
- 517 Certificado ascendente revocado
- 403 Prohibido
- Certificados revocados
- Discordancias de conjunto de cifrado
- Tiempos de espera de conexión del sitio web

Metodología de Troubleshooting

Paso 1: Confirmar que el tráfico atraviesa el proxy

- Recolección de datos: Genere un archivo HAR y PCAP cuando se produzca el problema.
- Análisis de encabezado: Inspeccione el encabezado Via en las respuestas HTTP. La presencia de `s_proxy` (proxy Nginx) o `m_proxy` (servicio de proxy modular/MPS) confirma que el tráfico está proxy.
- Transmisión TCP: En Wireshark, siga la secuencia TCP para asegurarse de que la conexión es a la IP del proxy, no a la IP de destino.

Paso 2: Verificar estado de descifrado de TLS

- Inspección del explorador: Haga clic en el icono de candado de la barra de direcciones del explorador. Si el certificado raíz de acceso seguro de Cisco aparece en la cadena de certificados, la inspección HTTPS está activa.
- Validación: Haga referencias cruzadas a los encabezados Via en los archivos HAR/PCAP.
- Comando OpenSSL: Para inspeccionar cadenas de certificados:
  `openssl s_client -connect www.example.com:443 -showcerts`
  Este comando comprueba la cadena de certificados presentada por el servidor. Ejecutarlo desde una máquina que atraviese el proxy para validación directa.

Paso 3: Aislamiento y proceso de eliminación

1. Fase A: inspección de prueba de HTTPS (capa Nginx):
   - Agregue el dominio problemático a la lista "No descifrar" del SWG.
   - Mantenga activada la función Inspección de archivos.
   - Si se resuelve el problema: La causa raíz es probablemente la inspección SSL/TLS de Nginx. Analice el PCAP para detectar discrepancias de cifrado o problemas de SNI. Utilice `curl` con y sin proxy para comparar el comportamiento.
   - Si el problema persiste: Vaya a la fase B.
2. Fase B - Inspección del archivo de prueba (capa de exploración):
   - Desactive la inspección de archivos para el tráfico específico.
   - Si se resuelve el problema: La causa principal se encuentra en el motor de análisis de archivos. Revise PCAP y HAR, reproduzca en laboratorio y determine si un archivo específico o una firma de análisis provoca el problema.
   - Si no se resuelve: póngase en contacto con el servicio de asistencia para obtener registros y conclusiones completos.

Problemas comunes y códigos de error

515 Certificado ascendente no fiable

Este error se produce cuando el proxy SWG no puede validar el certificado del servidor de destino. Las causas incluyen cadenas de certificados caducadas, autofirmadas o incompletas.

- Inspección HTTPS ACTIVADA + Inspección de archivos ACTIVADA: El sitio web funciona; no hay errores de certificado.
- Inspección de HTTPS activada + Inspección de archivos desactivada: 515 error se observa, concordancia de informe del usuario.
- Inspección HTTPS DESACTIVADA + Inspección de archivos DESACTIVADA (dominio en la lista No descifrar): No se observaron problemas.

Detalles técnicos: El proxy Nginx puede fallar si el servidor ascendente depende de la obtención de acceso a información de autoridad (AIA) para los certificados intermedios que faltan, ya que Nginx no maneja AIA tan correctamente como el servicio proxy de escaneo de archivos. Los desajustes de SNI y SAN durante el intercambio de señales TLS también pueden desencadenar fallas.

517 Certificado ascendente revocado

El error 517 significa que la verificación CRL u OCSP del proxy SWG encontró el certificado del servidor ascendente revocado.

- Resolución de problemas: Utilice herramientas externas como SSL Labs u OpenSSL para confirmar el estado de revocación.
- Documentación:
  - Error 517 de solución de problemas de Cisco: certificado ascendente revocado
  - Comprender los errores comunes de certificados y protocolos

Opciones de manejo de errores de certificados

Cisco Secure Access introducirá una nueva función llamada "Opciones de gestión de errores de certificados" para la derivación de errores granulares sin desactivar por completo el descifrado. Los dominios que activan errores de certificado debido a la inspección se pueden administrar mediante esta función en lugar de las listas generales "No descifrar".
Esta función existe en Umbrella SIG a partir de hoy. Detalles de solicitudes de características

para CSA.

502 Puerta de enlace incorrecta

El error 502 indica que el proxy SWG recibió una respuesta no válida del servidor ascendente mientras actuaba como intermediario.

-Velocidad de descarga: Cliente a proxy SWG
-Hacia el procesador: Proxy SWG a servidor de destino

El error siempre está en la conexión ascendente, debido a errores de protocolo, reinicios de TCP o encabezados mal formados.

Frecuentes 502 Causas

- Paquetes de cifrado SWG no compatibles
- Solicitud de autenticación de certificado de cliente
- Encabezados agregados por el proxy SWG

Conjuntos Cipher No Soportados

Causa: El servidor requiere un cifrado no compatible con SWG (por ejemplo, TLS_CHACHA20_POLY1305_SHA256).
Resolución: Agregue el dominio a la lista de descifrado selectivo.

Comandos de prueba:
Con proxy:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vv -k "https://www.cnn.com" >> null
```

Sin proxy:

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vv -o /dev/null -k -L www.cnn.com
```

Windows:

```
curl -vv -o null -k -L www.cnn.com
```

Solicitud de autenticación de certificado de cliente

Causa: El servidor ascendente requiere certificados de cliente, que SWG no admite.
Resolución: Omita el dominio del proxy mediante la lista de gestión de dominios externos (Umbrella SIG) o omita el proxy seguro (Cisco Secure Access). Omitir la inspección HTTPS por sí solo es insuficiente.

Encabezados agregados por proxy

Causa: Algunos servidores rechazan las solicitudes con el encabezado X-Forwarded-For (XFF) agregado por SWG cuando la inspección HTTPS está habilitada.
Resolución: Comparar el comportamiento con/sin HTTPS y la inspección de archivos. Si el error solo ocurre cuando XFF está presente, es probable que el servidor web esté mal configurado.

Ejemplo:
`curl https://www.xyz.com -k –header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Código de estado: %{http_code}" -s`
Código de estado: 502
`curl https://www.xyz.com -k -o /dev/null -w "Código de estado: %{http_code}" -s`
Código de estado: 200

El encabezado XFF se agrega para la geolocalización. Si el servidor no puede procesarlo, se produce un error 502.

Archivos dañados o PUA potencialmente no deseados

Si SWG no puede analizar un archivo mediante la inspección de archivos (por ejemplo, archivos protegidos, solicitados por intervalo o dañados), bloquea la descarga y genera informes - Bloqueado - Aplicación potencialmente no deseada (archivo protegido)

- Resolución de problemas: Capture un HAR durante el evento de bloqueo. Utilice Omitir seguridad como solución temporal. Si el archivo está dañado o es malicioso, debe corregirse en el origen.

Categorías potencialmente dañinas y bloques de reputación

- Utilice Talos para comprobar la reputación web (WBRS). Si un dominio se clasifica erróneamente, envíe una solicitud COG Jira a Talos para su revisión. Talos clasificado como seguro o favorable pero todavía bloque SWG entonces necesitamos comprobar de Beaker

servicio de SWG.

Acceso denegado por Akamai para las IP de salida de SWG

- SWG utiliza IP de salida compartidas. Si los servicios de reputación de IP (por ejemplo, Brightcloud) los ponen en la lista negra, es posible que se deniegue el acceso a determinados sitios.

Problemas conocidos: Inicio de sesión en Youtube Bot y vídeo no disponibles

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).