Solución de problemas de acceso al sitio web SWG

Contenido

Introducción

Este documento describe cómo resolver problemas de acceso al sitio web observados con el proxy de gateway web segura (SWG) de Umbrella.

Antecedentes

Supongamos que el sitio web www.xyz.com no es accesible a través del proxy SWG y cuando los usuarios intentan acceder a Internet directamente (sin que Umbrella SWG esté en la imagen), funciona bien. Revisemos varios síntomas y diferentes tipos de mensajes de error notificados cuando el sitio web es inaccesible a través de SWG. Los más comunes son 502 mal gateway, 502 no pudo retransmitir el mensaje de error ascendente, certificado ascendente revocado, acceso denegado 403 prohibido, discrepancia de cifrados ascendentes, sitio web solo expiró después de girar durante algún tiempo o similar.

Error "Acceso denegado 403" debido a bloqueo ascendente

El servidor web o el lado ascendente está bloqueando o limitando nuestros rangos de IP de salida de proxy SWG. Por ejemplo, Akamai WAF ha incluido en la lista de bloqueos un par de rangos de IP de salida SWG. Para resolver este problema, la única opción es ponerse en contacto con los administradores del sitio web y hacer que desbloqueen nuestros rangos de IP. Hasta entonces, puede omitir SWG utilizando la lista de gestión de dominios externos para las implementaciones

de archivos SWG y PAC de Anyconnect. En resumen, este tipo de problema no se debe al proxy en sí, sino a la incompatibilidad entre el proxy y los servidores web. Aquí está el link para hacer referencia al KB específicamente para el error "Acceso denegado 403" debido al bloqueo de IP de salida.

Además, este es el enlace que cubre algunas posibles razones por las que Akamai ha bloqueado las direcciones IP listadas.

Error "Acceso denegado 403" debido a un problema de Java

No se puede acceder al sitio web y se produce el mensaje "Acceso denegado o 403 prohibido: error de gateway de seguridad de la nube de Umbrella" cuando la solicitud se envía a través del proxy SWG MPS con la configuración de inspección de archivos activada. Sin embargo, si la inspección de archivos está desactivada, los sitios web se cargan correctamente. O si ponemos el sitio web en el descifrado de bypass, los sitios web se cargan correctamente.

Causa principal del problema de alto nivel

¿Qué es el problema relacionado con Java con MPS?

El sitio o servidor web en cuestión devuelve una advertencia de TLS con respecto a la alerta SNI o SSL al proxy después de que el proxy intente conectarse al servidor. Básicamente, esto sucede después de que se envía el saludo del cliente. El proxy MPS (que se basa en Java y, como tal) por diseño, trata cualquier alerta de TLS con "Nombre no reconocido" en el campo de descripción como un error durante el análisis de SNI y finaliza la transacción. Encontrará más información aquí

Tenga en cuenta que no se trata de un problema de SWG o proxy MPS. Esta es una de las incompatibilidades con SWG o cualquier otro proxy debido a una configuración incorrecta en el lado del servidor. Los navegadores suelen ignorar esta advertencia, pero SWG u otro filtro de seguridad de contenido trata la advertencia SSL como un error fatal y finaliza la sesión, lo que da como resultado 403 páginas de error prohibidas para los usuarios. También puede reportar el error 502 Bad Gateway, pero con la mayoría de los ejemplos lo que hemos visto es el error 403 prohibido, como se muestra en esta imagen.

Como MPS funciona en la capa de aplicación, tiene poco o ningún control sobre cómo la capa TLS maneja la transacción en función de las alertas generadas en el protocolo TLS. Es responsabilidad del servidor asegurarse de que sus terminales/certificados TLS estén configurados correctamente. Consulte este enlace, por favor.

Para reducir o resolver el problema, se puede señalar fácilmente desde el laboratorio SSL.

15152060146964

Cuando se accede al sitio web sin el proxy SWG en el medio o se omite la inspección HTTPS de SWG, el sitio web funciona porque el navegador ignora la alerta de nombre SNI no reconocido y continúa comunicándose con el servidor web.

En el momento de escribir este artículo, la solución alternativa recomendada es la mejor mitigación que podemos sugerirle. En un futuro próximo, gracias a la nueva arquitectura de proxy, podremos resolver estos problemas con más facilidad.

Resolución

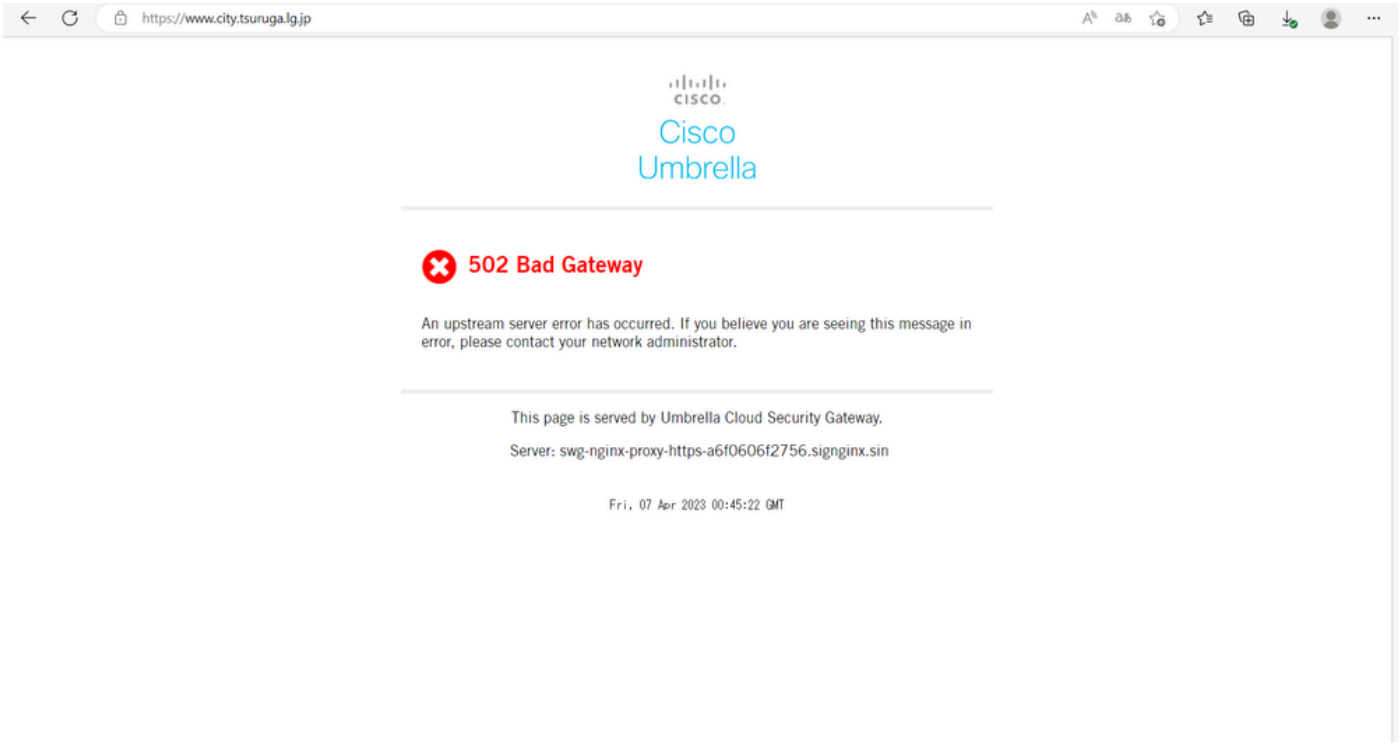
1. Desactivar el descifrado para los dominios afectados - O
2. Agregue el dominio a una lista de destino y asocie una regla de permiso (si confía en el sitio)

¿Qué es 502 Bad Gateway?

Un error 502 Bad Gateway significa que el servidor estaba actuando como un gateway o proxy y recibió una respuesta no válida del servidor ascendente. Cuando el usuario intenta acceder al sitio web a través de SWG Proxy, se producen dos flujos de comunicación.

a) Cliente —> Conexión proxy (Flujo descendente)
b) Proxy—> End web server connection (Upstream)

502 Se produce un error de gateway incorrecto entre el proxy SWG (MPS, Nginx) y la conexión del servidor final.



15026978020884

Factores comunes para 502 Bad Gateway

1. Paquetes Cipher SWG no compatibles

2. Solicitud de autenticación de certificado de cliente

3. Encabezados añadidos o eliminados por el proxy SWG

Paquetes de cifrado SWG no compatibles

Supongamos que un servidor web informa de conjuntos de cifrado SWG no admitidos durante la negociación TLS. Tenga en cuenta que el proxy SWG MPS (servicio de proxy modular) no admite el conjunto de cifrado TLS_CHACHA20_POLY1305_SHA256. Tenga en cuenta que hay un artículo separado para cubrir conjuntos cifrados compatibles con SWG y TLS. Podemos identificar fácilmente este problema revisando otros paquetes capturados durante el intercambio de conjuntos de cifrado en saludo del cliente y saludo del servidor. Como paso para la resolución de problemas, utilice el comando CURL que exige el uso de cifrados específicos para reducir el problema y confirmar que se debe a conjuntos de cifrado, como se muestra en los ejemplos 1 y 2.

Ejemplo de Comandos Curl:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
```

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

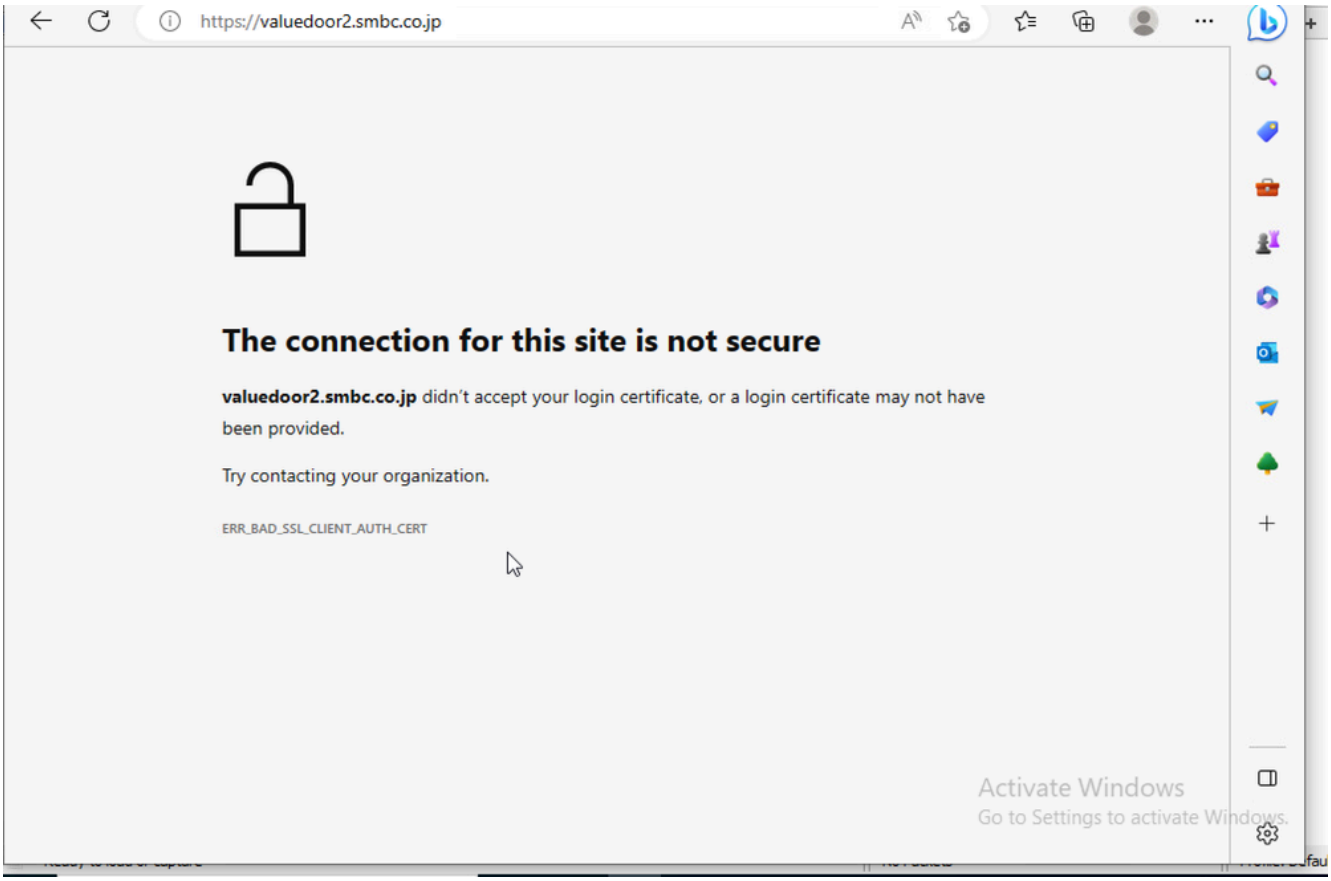
```
 - curl -vvv -o null -k -L www.cnn.com
```

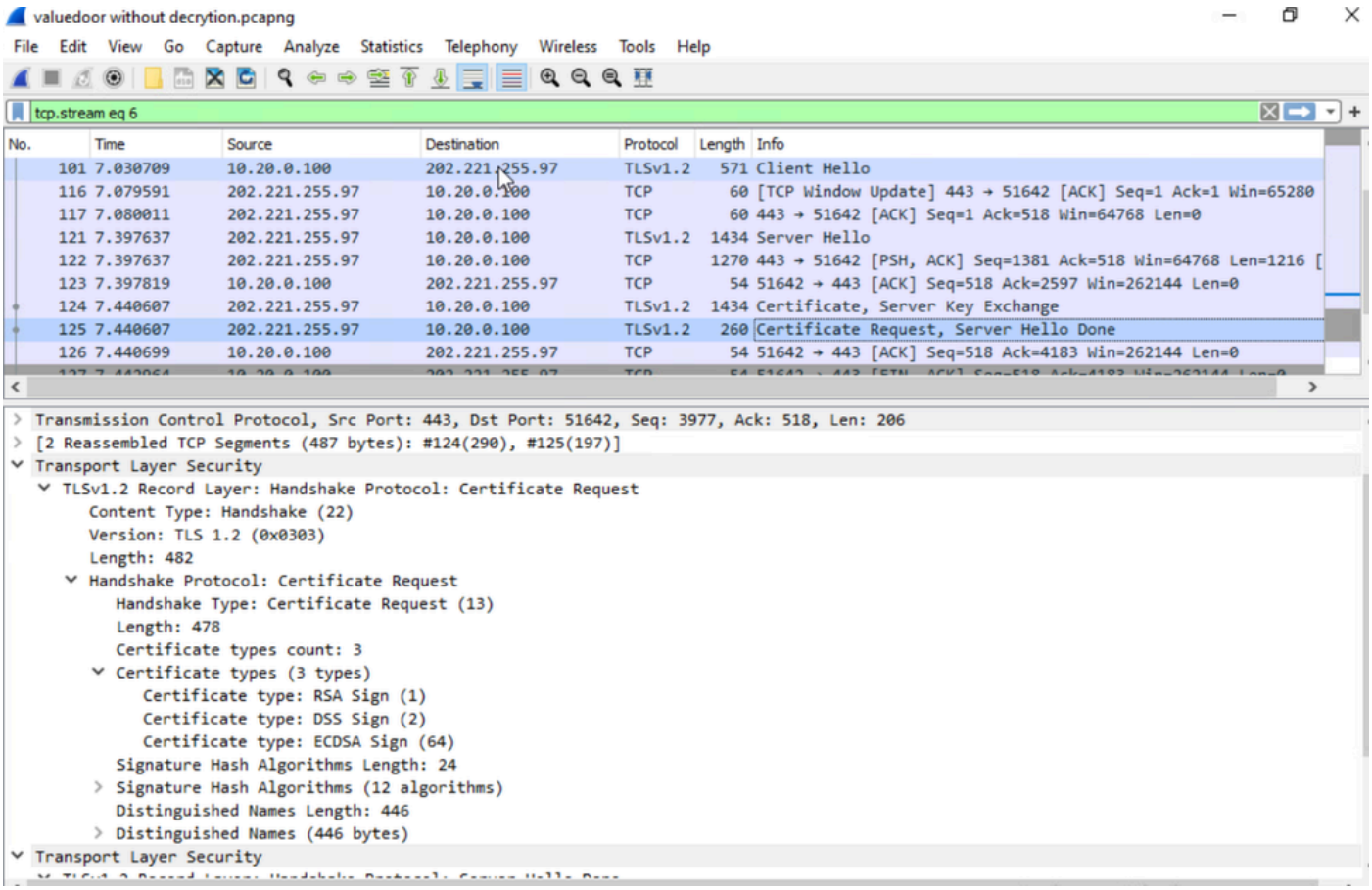
Resolución

Para resolver el problema, omita la inspección del sitio web problemático mediante la lista de descifrado selectivo.

Solicitud de autenticación de certificado de cliente

Durante el intercambio de señales TLS entre el proxy SWG y el flujo ascendente, el servidor web ascendente espera la autenticación del certificado de cliente. Dado que la autenticación de certificados de cliente no es compatible, necesitamos omitir esos dominios del proxy usando la lista de administración de dominios externos, y omitir solo la inspección https no es suficiente. Por ejemplo: https://valuedoor2.smbc.co.jp.

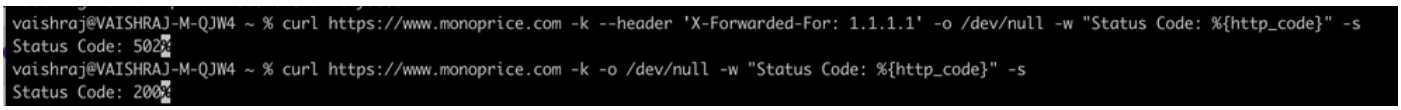




15027192992276

Encabezados agregados por proxy

El servidor web informa de un error de gateway 502 incorrecto debido al encabezado X-Forward-For (XFF) agregado por el proxy SWG cuando la inspección https está habilitada. Podemos reducir fácilmente la mayoría de los problemas de gateway 502 defectuosos solucionando primero el problema con o sin inspección https, y con o sin inspección de archivos para descartar el problema de escaneo de archivos con proxy MPS.



15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

Utilizamos el encabezado XFF cuando la inspección HTTPS está activada, de modo que el servidor ascendente puede proporcionar un contenido de geolocalización óptimo basado en la IP del cliente (que proporciona la ubicación física del usuario).

Cuando la inspección HTTPS no está habilitada, el proxy no agrega este encabezado, por lo que no hay un error 502 Bad Gateway. Este no es un problema de proxy SWG . Este error se debe a que el servidor web ascendente está mal configurado para no admitir el encabezado XFF estándar.

Resolución

Para resolver el problema, omita la inspección HTTPS para dominios específicos mediante listas de descifrado selectivo.

- 517 Certificado ascendente revocado
- Errores de certificado y protocolo TLS
- Seleccionar SWG DC manualmente para pruebas internas

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).