Error De Secure Access 502 Para Sitios Bancarios Después De La Autenticación

Contenido

Problema

Los usuarios informaron haber recibido un código de error HTTP de gateway incorrecto 502 después de autenticarse satisfactoriamente en FCBanking. El proceso de autenticación se completó correctamente, permitiendo a los usuarios ingresar sus credenciales de inicio de sesión, sin embargo, el navegador mostró un error 502 bad gateway inmediatamente después de la autenticación.

El dominio para FCBanking y su categoría relevante estaban exentos del descifrado SSL e IPS y este cambio de configuración no resolvió el error 502 HTTP. El problema se produjo de forma intermitente y solo se resolvió después de omitir el acceso seguro por completo para el dominio FCBanking. El análisis de archivos HAR reveló 502 errores en el destino de 'my.fcbanking.com' y los registros de búsqueda de actividad no mostraron los 502 errores que se capturaron en el archivo HAR, lo que indica que estos errores se estaban produciendo en un nivel de dispositivo intermedio.

Entorno

- Cisco Secure Access: acceso a Internet (módulo de roaming, VA, DNS, SWG, PAC, IPS, certificados)
- Topología de red: User PC > Switch > Catalyst SD-WAN Router > Internet local o túnel CSA
- Perímetro Catalyst SD-WAN configurado con regla de política de aplicaciones para enviar todo el tráfico de los puertos 80 y 443 a través del acceso directo a Internet (DIA) sin pasar por el grupo de túnel de red (NTG)
- Cisco Secure Client se basa en una lista de desvío para determinar el enrutamiento del tráfico a Secure Access
- Dominio bancario: fcbanking.com y subdominios asociados (my.fcbanking.com,

treasury.fcbanking.com)

Resolución

La resolución principal implica agregar el dominio bancario para omitir completamente el acceso seguro, lo que permite que el tráfico fluya directamente a Internet mientras se mantiene la seguridad de la capa DNS.

Paso 1: Agregar dominio principal a lista de desvío

- Agregue fcbanking.com a la lista bypass proxy only en la configuración de Secure Access. Esto garantiza que el tráfico web omite el proxy de acceso seguro mientras que la seguridad de la capa DNS permanece aplicada y registrada en la búsqueda de actividad.

Paso 2: Identificación y adición de alias de dominio

- Los sitios bancarios a menudo utilizan múltiples alias que también deben agregarse a la lista de desvío. Utilice Cache Check para identificar todos los alias del dominio bancario.
- Para fcbanking.com, estos alias se identificaron y agregaron a la lista de desvío:
    - treasury.fcbanking.com (alias: treasuryvanity.jackhenry.com)
    - my.fcbanking.com (alias: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

Paso 3: Resolución alternativa mediante direcciones IP

- Como alternativa al desvío basado en dominios, las direcciones IP resueltas de los sitios bancarios se pueden agregar a la lista de desvío. Cisco Secure Client traduce los FQDN que se encuentran en la lista de desvío a direcciones IP y enruta el tráfico web directamente a Internet.

Paso 4: Habilitar el registro de depuración para la solución de problemas

- Para capturar registros detallados para análisis adicionales, habilite el registro de depuración máximo:

- Cree un archivo llamado 'SWGConfigOverride.json' con este contenido:

```
{"logLevel": "1"}
```

Coloque el archivo SWGConfigOverride.json en la carpeta SWG:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

Reinicie el servicio SWG o Umbrella, o bien reinicie el sistema para aplicar la configuración de registro de depuración.


Nota: El registro de depuración no afecta al rendimiento del sistema, pero puede aumentar el tamaño del archivo de registro. Elimine el archivo SWGConfigOverride.json después de obtener el paquete DART para volver a los niveles de registro normales.

Paso 5: Verificación

- Después de implementar la configuración de desvío, los usuarios no informaron de más 502 errores al acceder al sitio bancario. El tráfico DNS continúa registrándose en la búsqueda de actividad mientras el tráfico web fluye directamente a Internet.

Causa

Los sitios bancarios suelen implementar medidas de seguridad que detectan y bloquean el tráfico que se origina en los servidores proxy o en los rangos de direcciones IP compartidas. Cisco Secure Access utiliza rangos de IP compartidos (151.186.144.0/20 y 151.186.176.0/20) para el tráfico proxy, que los sitios bancarios pueden detectar y rechazar silenciosamente o responder con errores de HTTP 502.

Cuando los dominios se colocan en la lista de no descifrados, la IP de origen parece seguir originándose en el intervalo de IP compartida de acceso seguro, lo que activa los mecanismos de seguridad del sitio bancario. Además, la inspección de IPS en el tráfico bancario y los alias de dominio que no están exentos correctamente pueden contribuir a fallos de conexión. La naturaleza intermitente de este problema y los 502 errores que aparecen en los archivos HAR

pero no en los registros de búsqueda de actividad indican que los errores fueron generados por el procesamiento de proxy intermedio en lugar de por los servidores bancarios de destino.

Contenido relacionado

- Solución de problemas de acceso al sitio web SWG
- Desactivar el protocolo QUIC para garantizar una inspección adecuada del tráfico web
- Documentación de rangos de IP de Cisco Secure Access
- Soporte técnico y descargas de Cisco

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).