

Falla de intercambio de señales TLS de recursos privados basados en navegador ZTA

Contenido

Problema

Los usuarios no pueden acceder a un recurso privado basado en navegador a través de Cisco Secure Access.

Al intentar conectarse, se producen estos síntomas:

- El protocolo de enlace de tres vías TCP se completa correctamente, pero la negociación TLS falla después del saludo del cliente.
- La conexión a la URL asignada a SSE pública (<https://example-orgid.ztna.sse.cisco.io>) alcanza la autenticación de Cisco pero devuelve el error HTTP 404.
- Después de agregar el FQDN a la configuración de recursos privados, el tráfico se redirige a la solicitud de autenticación, pero se genera una página en blanco después de la autenticación.
- Los archivos HAR muestran respuestas HTTP 200, pero el intercambio de señales TLS no se completa.
- El motivo del bloqueo aparece como: "Acceso privado: los datos de estado obtenidos para el dispositivo son demasiado antiguos o deben actualizarse".

Entorno

- Cisco Secure Access (SSE)
- ID de organización de Secure Access: xxxx
- Acceso a red de confianza cero (ZTNA) basado en navegador

- Recurso privado: example.net
- Recurso privado en funcionamiento para la comparación: abc.net
- Configuración de certificado comodín

Resolución

El problema se resolvió configurando el recurso privado para que utilizara la misma configuración de certificado que un recurso privado en funcionamiento.

Se adoptaron las medidas esbozadas en las secciones siguientes.

Paso 1: Analizar configuración en funcionamiento

Compare el recurso privado que falla (example.net) con un recurso privado en funcionamiento (abc.net) para identificar las diferencias de configuración.

El recurso de trabajo utilizado:

- Usar una URL en la opción de dominio
- Referencia al par clave/certificado comodín existente

Paso 2: Análisis de captura de paquetes

Realice un análisis de captura de paquetes usando Wireshark para confirmar la falla de intercambio de señales TLS:

- Verifique que el protocolo de enlace de tres vías TCP se haya completado correctamente.
- La negociación de confirmación de TLS falla después del saludo del cliente.
- Recopilar artefactos de diagnóstico: archivos HAR, paquete DART y capturas de paquetes.

Paso 3: Verificación de certificados

Acceda a la aplicación a través de la conexión RAVPN para verificar la presentación del certificado:

- Confirme que el sitio web `example.net` presenta un certificado comodín.
- Documentar detalles del certificado para referencia de configuración.

Paso 4: Configurar recurso privado

Aplique el mismo enfoque de configuración utilizado por el recurso privado en funcionamiento:

- Configure el recurso privado para utilizar la opción `Use a URL in your domain`.
- Haga referencia al par clave/certificado comodín existente.
- Asegúrese de que el FQDN esté configurado correctamente en el campo de recurso privado.

Paso 5: Validación

Pruebe el acceso basado en navegador para confirmar la configuración y resolver el problema:

- Verifique que el intercambio de señales TLS se haya completado correctamente.
- Confirme el flujo de autenticación adecuado.
- Validar la accesibilidad de la aplicación después de la autenticación.

Causa

La causa raíz fue una discordancia de configuración en la instalación de recursos privados. El recurso privado con errores no se configuró para hacer referencia correctamente al certificado

comodín que presentaba la aplicación de destino. Error en el intercambio de señales TLS porque la configuración de recursos privados no se alineó con la configuración de certificados utilizada por el servidor de aplicaciones. Si configura el recurso privado para que utilice la opción Use a URL in your domain y hace referencia al par de clave/certificado comodín existente (que coincide con la configuración en funcionamiento), la negociación TLS podría completarse correctamente.

Contenido relacionado

- [Guía de referencia de Cisco para el acceso seguro](#)
- [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).