Comprender los errores comunes de certificados y protocolos TLS

Contenido

Introducción

Este documento describe errores comunes de certificado y protocolo TLS en la Búsqueda de actividad del panel de Umbrella.

Overview

El tráfico HTTP bloqueado debido a errores de certificado y TLS ahora se puede ver en la búsqueda de actividad del panel de Umbrella. En este artículo se proporciona una lista de mensajes de error comunes, así como una breve explicación de cada uno de los errores.

Errores de certificado

El certificado ascendente expiró

Un certificado presentado por el sitio web ha caducado. Póngase en contacto con el webmaster del sitio para informar de este problema.

Certificado ascendente autofirmado

El certificado de servidor presentado por el sitio web no está firmado por una autoridad de certificación y, por lo tanto, Umbrella no puede determinar si el certificado es de confianza.

Los certificados autofirmados se utilizan a veces cuando un servidor aloja un recurso destinado a una audiencia restringida. Por ejemplo, los portales web para los dispositivos de seguridad de TI suelen utilizar de forma predeterminada certificados autofirmados. Umbrella no se puede configurar para confiar en certificados autofirmados.

Falta el certificado intermedio

Umbrella no pudo obtener certificados para todas las autoridades intermedias y, por tanto, no pudo validar toda la cadena de confianza.

Los certificados de servidor web se emiten/firman normalmente como un certificado intermedio de la autoridad certificadora. Estos certificados intermedios también pueden ser emitidos por otros certificados intermedios. El certificado del servidor web (también conocido como "certificado de hoja") y cualquier certificado intermedio forman una cadena de vuelta a un certificado raíz. El sitio web debe agrupar los certificados intermedios con el certificado del servidor para que Umbrella valide toda la cadena de confianza. Póngase en contacto con el webmaster del sitio para informar de este problema.

Alternativamente, si el certificado incluye la extensión "Acceso a la información de la autoridad", Umbrella intenta obtener las CA intermedias automáticamente. Tenga en cuenta que Umbrella sólo admite la extensión AIA cuando están activados el descifrado HTTPS y la inspección de archivos.

Falta el nombre del sujeto del certificado ascendente.

El campo Asunto del certificado no contiene un nombre distinguido (DN) para identificar este certificado. Se trata de un requisito para todos los certificados emitidos por una autoridad de certificación y, por lo tanto, exigido por Cisco Umbrella. Póngase en contacto con el webmaster del sitio para informar de este problema.

Falta el nombre común del certificado ascendente.

El certificado presentado por el sitio web no tiene un nombre común. El campo Nombre común (CN) es obligatorio para Umbrella SWG. Contiene el nombre de host del certificado, que es necesario para validar que el certificado coincide con el recurso solicitado por el usuario (por ejemplo, La dirección introducida en el explorador). Póngase en contacto con el webmaster del sitio para informar de este problema.

Certificado ascendente no fiable

Cisco Umbrella no confía en el certificado. Este error generalmente significa que Cisco no confía en la CA raíz que emitió el certificado.

Umbrella SWG tiene una lista integrada de Autoridades de Certificados Raíz de confianza

conocidas que actualizamos desde una fuente confiable. Si el certificado de los sitios web no está firmado por una CA de esta lista, la validación del certificado no se realizará correctamente. Si cree que a Umbrella le falta una CA raíz de confianza, póngase en contacto con el servicio de asistencia técnica.

El nombre de host en el certificado es diferente del esperado

El recurso solicitado por el usuario (p. ej. la dirección escrita en el explorador) no coincide con el nombre común (CN) o el nombre alternativo del sujeto (SAN) del certificado, por lo que Umbrella no puede confiar en el certificado para esta solicitud. Póngase en contacto con el webmaster del sitio para informar de este problema.

Certificado ascendente revocado

El certificado proporcionado por el sitio web ha sido revocado por la autoridad certificadora emisora.

Umbrella realiza comprobaciones de OCSP (Online Certificate Status Protocol, protocolo de estado de certificados en línea) para determinar si un certificado ha sido revocado posteriormente por una CA. Póngase en contacto con el webmaster del sitio para informar de este problema.

Errores de intercambio de señales TLS

Cifrado ascendente no admitido

No se pudo completar el intercambio de señales TLS. Por lo general, esto significa que el sitio web no admite ninguna de las listas de paquetes Cipher utilizadas por Umbrella SWG. Este error puede ocurrir con servidores web antiguos u obsoletos que sólo admiten cifrados TLS más débiles. Póngase en contacto con el webmaster del sitio para informar de este problema.

Discordancia de versión de TLS ascendente

No se pudo completar el intercambio de señales de TLS porque el sitio web no admite la misma versión de TLS que utiliza Umbrella SWG. Por el momento, Umbrella SWG Proxy soporta TLS 1.2 y TLS 1.3 en las conexiones del lado del cliente a Umbrella SWG y también desde las conexiones proxy de Umbrella SWG a los servidores web de destino.

Clave DH ascendente inferior a 1024 bits

No se pudo completar el intercambio de señales de TLS porque el sitio web usa una clave Diffie-Hellman débil que Umbrella no admite. Póngase en contacto con el webmaster del sitio para informar de este problema.

Soluciones alternativas

Es posible solucionar estos problemas realizando cambios de configuración en Cisco Umbrella.

Esto solo se debe hacer si confía en la autenticidad del servidor y del certificado.

Se pueden aplicar soluciones alternativas utilizando una entrada de "Lista de descifrado selectivo" para desactivar el descifrado o una entrada de "Dominios externos" para omitir el tráfico de Umbrella por completo. Umbrella no realiza la validación de certificados cuando el descifrado está deshabilitado. Tenga en cuenta que, en la mayoría de los casos, el navegador sigue presentando un error o advertencia cuando el tráfico se omite desde Umbrella: los navegadores web realizan una validación de certificado similar.

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).