Solucionar error "517 certificado ascendente revocado"

Contenido

Introducción

Este documento describe cómo resolver el error "517 Upstream Certificate Revoked" (Certificado ascendente revocado) al navegar a una url HTTPS.

Problema

Cuando el proxy web de Umbrella Secure Web Gateway (SWG) se configura para realizar la inspección de HTTPS, un usuario puede recibir una página de error 517 Upstream Certificate Revoked. Este error indica que el sitio web solicitado envió un certificado digital en la negociación TLS que tiene un estado de "revocado" según el emisor de ese certificado, o una autoridad similar. Un certificado revocado ya no es válido.

13351060307092

Causa

Cuando un cliente de Umbrella realiza una solicitud HTTPS a través de Umbrella Secure Web Gateway, SWG realiza comprobaciones de revocación de certificados mediante el protocolo de estado de certificados en línea (OCSP). OCSP proporciona el estado de revocación de un certificado. SWG realiza solicitudes de OCSP para el estado de revocación de certificados en nombre de los clientes de Umbrella.

SWG determina el estado de revocación del certificado del servidor web solicitado y todos los certificados intermedios que emiten en la ruta a un certificado raíz de confianza. Estas comprobaciones aseguran que una cadena de confianza válida no ha dejado de ser válida desde la emisión.

En un certificado digital que utiliza la comprobación de revocación de OCSP, la extensión X.509 "Acceso a la información de autoridad" contiene uno o más campos "OCSP". Un campo contiene una URL HTTP para un "extremo" de OCSP (servidor web) al que se puede consultar el estado de revocación del certificado. SWG realiza solicitudes a cada URL de OCSP en un certificado hasta que se recibe una respuesta que indica uno de:

- el certificado es válido (no revocado) en cuyo momento SWG permite que la solicitud web continúe, O
- cualquier respuesta que no sea un "certificado válido" de OCSP (por ejemplo, si el certificado se revoca, el servidor no puede responder en este momento, un estado de error HTTP, un tiempo de espera de la capa de transporte/red, etc.) en cuyo momento SWG presenta la página/mensaje de error correspondiente y la solicitud web falla

Tenga en cuenta que las respuestas de OCSP suelen almacenarse en caché y utilizarse para responder a comprobaciones futuras. El servidor establece el tiempo de almacenamiento en caché en la respuesta de OCSP.

Diferente comportamiento al navegar directamente

Los clientes Web pueden utilizar diversos mecanismos de comprobación de revocación, dependiendo del cliente. Por ejemplo, el navegador Chrome de Google no utiliza los métodos OCSP o CRL estándar, de forma predeterminada. En su lugar, Chrome utiliza una versión propietaria de una CRL denominada CRLSet, que Secure Web Gateway no utiliza. Como resultado, Chrome puede no producir el mismo resultado que SWG al comprobar el estado de revocación de un certificado.

Sin embargo, tenga en cuenta que, como se indica en la documentación de CRLSet, "en algunos casos, la biblioteca de certificados del sistema subyacente siempre realiza estas comprobaciones independientemente de lo que haga Chromium". Por tanto, en función del entorno local, la comprobación de OCSP o CRL la puede realizar el explorador o las bibliotecas de servicios criptográficos del sistema operativo, como SChannel, Secure Transport o NSS.

Tenga en cuenta también que no se garantiza que las comprobaciones de OCSP y CRL produzcan el mismo resultado.

Consulte la documentación del explorador o del proveedor del sistema operativo para determinar qué comprobaciones de revocación de certificados realizan los clientes al explorar.

Resolución

El uso de certificados válidos es responsabilidad del administrador del servidor web. El administrador del servidor debe realizar la corrección de los certificados revocados en el servidor. Cisco Umbrella no puede ayudar en este proceso.

Cisco Umbrella recomienda encarecidamente no acceder a un sitio web que utilice un certificado revocado. Las soluciones temporales solo se pueden emplear cuando el usuario comprende completamente por qué un sitio utiliza un certificado revocado y acepta totalmente cualquier riesgo.

Para evitar el error, el sitio puede quedar exento de la inspección de HTTPS mediante la creación de una lista de descifrado selectivo que incluya el nombre de dominio del sitio. La lista de descifrado selectivo se aplicaría a la directiva Web que permite el acceso al sitio. Como alternativa, el sitio se puede agregar a la lista de dominios externos para enviar tráfico directamente al sitio, omitiendo SWG.

Additional Information

Los clientes que deseen confirmar si el certificado de un servidor está revocado pueden utilizar herramientas de terceros diseñadas para comprobar el estado de revocación. En particular, la herramienta SSL Server Test de Qualys SSL Labs realiza comprobaciones de OCSP y CRL,

además de proporcionar otra información de validez del certificado. La herramienta está disponible en línea en:

- https://www.ssllabs.com/ssltest/analyze.html

Recomendamos utilizar esta herramienta para verificar el sitio que produce un error 517 Upstream Certificate Revoked, antes de abrir un caso de soporte con Cisco Umbrella.

Vea también: https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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).