

Comprender los errores de protocolo de enlace y certificado SSL en Secure Access

Contenido

Problema

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

Entorno

- Cisco Secure Access: Inspección SSL de gateway web seguro

Resolución

El certificado ascendente ha caducado

El certificado del sitio web ha superado su fecha de caducidad, por lo que Cisco Secure Access no confía en él. Este está en el propietario del sitio web para arreglar, así que llegar al webmaster del sitio y hacerles saber.

Certificado ascendente autofirmado

El sitio web presenta un certificado que firmó él mismo, en lugar de uno emitido por una autoridad

certificadora de confianza. Como ninguna autoridad independiente responde por ello, Cisco Secure Access no tiene forma de confirmar que el certificado sea auténtico.

A menudo se ven certificados autofirmados en recursos destinados a un público interno reducido: los portales de administración de los dispositivos de seguridad de TI son un ejemplo clásico. Tenga en cuenta que Cisco Secure Access no se puede configurar para confiar en los certificados autofirmados.

Falta el certificado intermedio

Cisco Secure Access no pudo reunir todos los certificados intermedios que necesita, por lo que no puede volver a crear la cadena completa de confianza en una raíz.

He aquí por qué esto importa: el certificado de un sitio web (la "hoja") está firmado por un certificado intermedio, que a su vez puede estar firmado por otro intermedio, y así sucesivamente hasta una raíz de confianza. Para que esta cadena pueda comprobarlo, el sitio web tiene que enviar sus certificados intermedios junto con los suyos propios. Cuando faltan, la validación se interrumpe, así que infórmele al webmaster del sitio.

Hay una excepción: si el certificado incluye la extensión "Authority Information Access" (AIA), Cisco Secure Access puede intentar obtener los intermediarios que faltan por sí solo. Tenga en cuenta que esto solo funciona cuando están activados tanto el descifrado HTTPS como la inspección de archivos.

Falta el nombre del sujeto del certificado ascendente

El certificado no incluye un nombre de sujeto (un nombre distinguido) o un nombre alternativo de sujeto, lo que significa que no hay nada que identifique claramente a quién pertenece el certificado. Sin esto, Cisco Secure Access no puede validarlo. Esto es algo que el propietario del sitio web necesita corregir.

Falta el nombre común del certificado ascendente

El certificado no tiene un nombre común (CN): el campo que tradicionalmente contenía el nombre de host del sitio y que ayudó a confirmar que el certificado pertenece realmente al sitio que está

visitando. En la actualidad, esa comprobación depende realmente del nombre alternativo del sujeto (SAN) y CN se considera un campo heredado, pero su ausencia puede activar este error. Dirijase al webmaster para que lo aborde.

Certificado ascendente no confiable

Cisco Secure Access no confía en este certificado, normalmente porque no reconoce la CA raíz que lo emitió.

El SWG de Cisco Secure Access mantiene una lista integrada de autoridades de certificados raíz de confianza, obtenida de un proveedor acreditado y actualizada. Si el certificado de un sitio se remonta a una entidad emisora de certificados que no está en esa lista, se produce un error en la validación. Si está seguro de que la CA raíz es de confianza, póngase en contacto con el soporte técnico y podremos echar un vistazo.

El nombre de host en el certificado es diferente del esperado

La dirección que ha solicitado no coincide con el nombre del certificado, ni con su nombre común (CN) ni con ninguno de sus nombres alternativos de asunto (SAN). Dado que el certificado parece no pertenecer al sitio al que está accediendo, Cisco Secure Access no confía en él para esta solicitud. El webmaster tiene que resolver esto.

Certificado ascendente revocado

La autoridad certificadora que emitió este certificado lo ha revocado desde entonces, es decir, ya no se considera válido.

Cisco Secure Access lo confirma mediante el protocolo de estado de certificados en línea (OSCP), que comprueba en tiempo real si se ha revocado un certificado. Hágale saber al webmaster del sitio para que pueda reemplazarlo.

Errores de intercambio de señales TLS

Cifrado ascendente no admitido

No se pudo completar el intercambio de señales de TLS porque el sitio web no es compatible con ninguno de los conjuntos cifrados que utiliza Cisco Secure Access SWG. Esto tiende a aparecer con servidores antiguos u obsoletos que solo ofrecen cifrados más débiles. La solución está en el lado del servidor, así que pásela al webmaster.

Discordancia de versión de TLS ascendente

Error en el intercambio de señales porque el sitio web no está utilizando una versión de TLS compatible con Cisco Secure Access SWG. En este momento, el proxy SWG de Cisco Secure Access funciona con TLS 1.2 y TLS 1.3, tanto para las conexiones que llegan de los clientes como para las conexiones que realiza a los servidores de destino.

Clave DH ascendente inferior a 1024 bits

No se pudo completar el protocolo de enlace porque el sitio web usa una clave Diffie-Hellman demasiado débil (menos de 1024 bits) para que Cisco Secure Access la acepte. Esta es una limitación del lado del servidor, por lo que el webmaster necesita fortalecerla.

Soluciones alternativas

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

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

Se pueden aplicar soluciones mediante una entrada de la "Lista de descifrado selectivo" para desactivar el descifrado o una entrada de "Dominios externos" para omitir el tráfico de Cisco Secure Access por completo. Cisco Secure access 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 se omite el tráfico de Cisco Secure Access. Los navegadores web realizan una validación de certificado similar.

Causa

El proxy de inspección SSL de Cisco Secure Access no pudo completar el intercambio de señales de TLS, generalmente porque el destino utiliza la fijación de certificados que rechaza el certificado refirmado de CSA.

- Fijación de certificados: client hard-codes expected cert fingerprint
- CA CSA no fiable en el terminal: certificado de CA de inspección no implementado en el almacén raíz de confianza

Contenido relacionado

- [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).