Entender erros comuns de certificado e protocolo TLS

Contents

Introdução

Este documento descreve erros comuns de certificado e protocolo TLS na Pesquisa de atividade do painel Umbrella.

Overview

O tráfego HTTP bloqueado devido a erros de certificado e TLS agora pode ser exibido na Pesquisa de atividades do painel Umbrella. Este artigo fornece uma lista de mensagens de erro comuns, bem como uma breve explicação de cada um dos erros.

Erros de certificado

Certificado upstream expirado

Um certificado apresentado pelo site expirou. Entre em contato com o webmaster do site para relatar esse problema.

Certificado upstream autoassinado

O certificado de servidor apresentado pelo site não está assinado por uma Autoridade de Certificação e, portanto, o Umbrella não pode determinar se o certificado é confiável.

Os certificados autoassinados às vezes são usados quando um servidor hospeda um recurso que se destina a um público restrito. Por exemplo, os portais da Web para dispositivos de segurança de TI geralmente usam como padrão certificados autoassinados. O Umbrella não pode ser configurado para confiar em certificados autoassinados.

Certificado Intermediário Ausente

O Umbrella não pôde obter certificados para todas as Autoridades Intermediárias e, portanto, não pôde validar toda a cadeia de confiança.

Os certificados de servidor Web são tipicamente emitidos/assinados um certificado intermediário de Autoridade de Certificação. Esses certificados intermédios podem também ser emitidos por outros certificados intermédios. O certificado do servidor web (também conhecido como "certificado folha") e qualquer certificado intermediário formam uma cadeia de volta para um certificado raiz. O site deve agrupar o(s) certificado(s) intermediário(is) com o certificado do servidor para que o Umbrella valide toda a cadeia de confiança. Entre em contato com o webmaster do site para relatar esse problema.

Como alternativa, se o certificado incluir a extensão "Acesso às informações da autoridade", o Umbrella tentará buscar as CAs intermediárias automaticamente. Observe que o Umbrella só oferece suporte à extensão AIA quando a Descriptografia HTTPS e a Inspeção de Arquivo estão habilitadas.

Falta o nome da entidade do certificado upstream.

O campo Assunto do certificado não contém um DN (Nome Distinto) para identificar esse certificado. Esse é um requisito para todos os certificados emitidos por uma Autoridade de Certificação e, portanto, exigido pelo Cisco Umbrella. Entre em contato com o webmaster do site para relatar esse problema.

Falta nome comum no certificado upstream.

O certificado apresentado pelo site não tem um Nome Comum. O campo Nome comum (CN) é obrigatório para o Umbrella SWG. Contém o nome de host do certificado, que é necessário para validar se o certificado corresponde ao recurso solicitado pelo usuário (por exemplo, O endereço digitado no navegador). Entre em contato com o webmaster do site para relatar esse problema.

Certificado de upstream não confiável

O certificado não é confiável para o Cisco Umbrella. Normalmente, esse erro significa que a Cisco não confia na CA raiz que emitiu o certificado.

O Umbrella SWG tem uma lista interna de Autoridades de Certificação Raiz conhecidas e confiáveis que atualizamos a partir de uma fonte confiável. Se o certificado dos sites não estiver

assinado por uma CA nesta lista, a validação do certificado falhará. Se você acredita que o Umbrella não possui uma CA raiz confiável, entre em contato com o suporte técnico.

O nome de host no certificado é diferente do esperado

O recurso solicitado pelo usuário (por exemplo, o endereço digitado no navegador) não corresponde ao Nome comum (CN) ou ao Nome alternativo do assunto (SAN) do certificado, portanto, o Umbrella não pode confiar no certificado para esta solicitação. Entre em contato com o webmaster do site para relatar esse problema.

Certificado de upstream revogado

O certificado fornecido pelo site foi revogado pela autoridade de certificação emissora.

O Umbrella executa verificações OCSP (Online Certificate Status Protocol) para determinar se um certificado foi revogado posteriormente por uma CA. Entre em contato com o webmaster do site para relatar esse problema.

Erros de handshake TLS

Cifra de upstream não suportada

Não foi possível concluir o handshake TLS. Isso geralmente significa que o site não suporta nenhuma das listas de Cipher Suites usadas pelo Umbrella SWG. Este erro pode ocorrer com servidores Web antigos ou desatualizados que suportam apenas cifras TLS mais fracas. Entre em contato com o webmaster do site para relatar esse problema.

Incompatibilidade de versão de TLS de upstream

O handshake TLS não pôde ser concluído porque o site não oferece suporte à mesma versão de TLS que o Umbrella SWG usa. No momento, o Umbrella SWG Proxy oferece suporte a TLS 1.2 e TLS 1.3 em ambas as conexões do lado do cliente com o Umbrella SWG e também de conexões proxy do Umbrella SWG para servidores Web de destino.

Chave DH upstream menor que 1024 bits

O handshake TLS não pôde ser concluído porque o site usa uma chave Diffie-Hellman fraca que não é suportada pelo Umbrella. Entre em contato com o webmaster do site para relatar esse problema.

Soluções

É possível solucionar esses problemas fazendo alterações de configuração no Cisco Umbrella. Isso só deverá ser feito se você confiar na autenticidade do servidor e do certificado.

Soluções alternativas podem ser aplicadas usando uma entrada "Lista de descriptografia seletiva"

para desativar a descriptografia ou uma entrada "Domínios externos" para ignorar totalmente o tráfego do Umbrella. O Umbrella não executa validação de certificado quando a descriptografia está desabilitada. Esteja ciente de que, na maioria dos casos, o navegador ainda apresenta um erro ou aviso quando o tráfego é ignorado do Umbrella - os navegadores da Web executam validação de certificado semelhante.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.