Troubleshooting de Erro "517 Certificado de Upstream Revogado"

Contents

Introdução

Este documento descreve como solucionar o erro "517 Upstream Certificate Revoked" ao navegar para uma URL HTTPS.

Problema

Quando o proxy da Web do Umbrella Secure Web Gateway (SWG) é configurado para executar a Inspeção HTTPS, um usuário pode receber uma página de erro 517 Upstream Certificate Revoked. Esse erro indica que o site solicitado enviou um certificado digital na negociação TLS que tem um status de "revogado" de acordo com o emissor desse certificado, ou uma autoridade semelhante. Um certificado revogado não é mais válido.

13351060307092

Causa

Quando um cliente Umbrella faz uma solicitação HTTPS através do Umbrella Secure Web Gateway, o SWG executa verificações de revogação de certificado usando o Online Certificate Status Protocol (OCSP). O OCSP fornece o status de revogação de um certificado. O SWG faz solicitações OCSP para o status de revogação de certificado em nome dos clientes Umbrella.

O SWG determina o status de revogação do certificado do servidor da Web solicitado e todos os certificados intermediários emissores no caminho para um certificado raiz confiável. Essas verificações garantem que uma cadeia de confiança válida não se torne inválida desde a emissão.

Em um certificado digital que usa verificação de revogação OCSP, a extensão X.509 "Authority Information Access" contém um ou mais campos "OCSP". Um campo contém um URL HTTP para um "ponto final" OCSP (servidor web) que pode ser consultado para o status de revogação do certificado. O SWG faz solicitações a cada URL OCSP em um certificado até que uma resposta seja recebida, indicando um dos seguintes itens:

- o certificado é válido (não revogado), momento em que o SWG permite que a solicitação da Web prossiga, OU
- qualquer coisa diferente de uma resposta de "certificado válido" OCSP (por exemplo, o certificado é revogado, o servidor não pode responder no momento, um status de erro HTTP, um timeout de camada de rede/transporte e assim por diante) em que o SWG apresenta a página/mensagem de erro apropriada e a solicitação da Web falha

Observe que as respostas OCSP são normalmente armazenadas em cache e usadas para responder a verificações futuras. O tempo de cache é definido pelo servidor na resposta OCSP.

Comportamento diferente ao navegar diretamente

Os clientes da Web podem usar vários mecanismos de verificação de revogação, dependendo do cliente. Por exemplo, o navegador Chrome do Google não usa os métodos OCSP ou CRL padrão, por padrão. Em vez disso, o Chrome usa uma versão proprietária de uma CRL chamada CRLSet, que o Secure Web Gateway não usa. Como resultado, o Chrome pode não produzir o mesmo resultado que o SWG ao verificar o status de revogação de um certificado.

Observe, no entanto, que, como a documentação do CRLSet afirma, "em alguns casos, a biblioteca de certificados do sistema subjacente sempre executa essas verificações, independentemente do que o Chromium faz." Assim, dependendo do seu ambiente local, uma verificação de OCSP e/ou CRL pode ser executada pelo seu navegador ou pelas bibliotecas de serviços criptográficos do sistema operacional, como SChannel, Secure Transport ou NSS.

Observe também que não há garantia de que as verificações OCSP e CRL produzam o mesmo resultado.

Consulte a documentação do navegador ou do fornecedor do sistema operacional para determinar quais verificações de revogação de certificados são executadas pelos clientes durante a navegação.

Resolução

O uso de certificados válidos é de responsabilidade do administrador do servidor Web. A correção de certificados revogados deve ser executada no servidor pelo administrador do servidor. O Cisco Umbrella não pode auxiliar nesse processo.

O Cisco Umbrella recomenda que você não acesse um site que use um certificado revogado. Soluções alternativas só podem ser empregadas quando o usuário entende totalmente por que um site usa um certificado revogado e aceita totalmente todos os riscos.

Para evitar o erro, o site pode ser isento da Inspeção HTTPS criando uma Lista de Descriptografia Seletiva que inclua o nome de domínio do site. A lista de descriptografia seletiva seria aplicada à política da Web que permite acesso ao site. Como alternativa, o site pode ser adicionado à lista Domínios externos para enviar tráfego diretamente ao site, ignorando o SWG.

Informações adicionais

Os clientes que desejarem confirmar se o certificado de um servidor é revogado podem usar ferramentas de terceiros projetadas para verificar o status de revogação. Mais notavelmente, a ferramenta SSL Server Test da Qualys SSL Labs executa verificações de OCSP e CRL, além de fornecer outras informações de validade de certificado. A ferramenta está disponível online em:

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

Recomendamos o uso dessa ferramenta para verificar o site que produz um erro 517 Upstream Certificate Revoked, antes de abrir um caso de suporte no Cisco Umbrella.

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

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.