Solucionar erros 516 no Umbrella Secure Web Gateway

Contents

Introdução

Este documento descreve como solucionar problemas de um aumento em 516 erros no Umbrella Secure Web Gateway.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Umbrella Secure Web Gateway (SWG).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Os usuários que navegam pelo proxy do Umbrella Secure Web Gateway (SWG) com a Inspeção HTTPS podem receber com mais frequência páginas de erro 516 Upstream Certificate CN Mismatch a partir da segunda metade de outubro de 2023.

A página de erro 516 ocorre quando o certificado de um site não corresponde ao nome de domínio usado pelo cliente para acessar o site.

O aumento nas páginas de erro é devido a uma alteração no tratamento do navegador Chrome das solicitações de URLs que usam o esquema HTTP (não criptografado). O Chrome agora tenta carregar o recurso com o esquema HTTPS (criptografado) primeiro. Quando configurado para Inspeção HTTPS, o SWG inspeciona o certificado de um site e retorna uma página da Web exibindo um código de erro como 516 se o certificado não for aceitável.

Para contornar esse problema, os clientes podem configurar suas políticas da Web para ignorar a Inspeção HTTPS para solicitações que, caso contrário, resultarão em erros 516.

516 Plano de Fundo do Erro

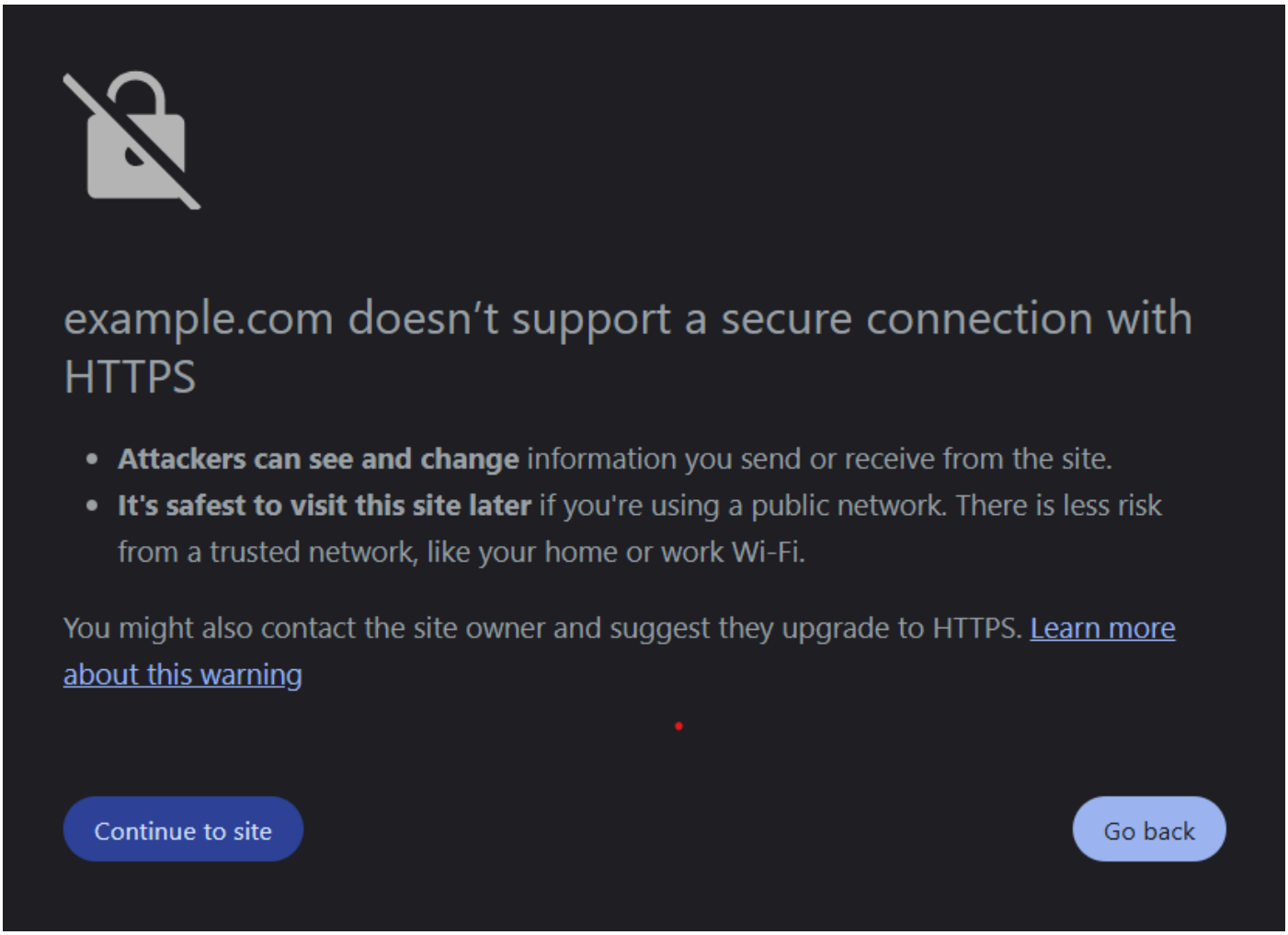
Resumindo, o Umbrella Secure Web Gateway retorna uma página de erro 516 quando o nome de domínio usado para acessar um site via HTTPS não aparece no certificado digital do servidor. Para obter informações adicionais descrevendo o motivo para o Secure Web Gateway retornar uma página de erro 516, consulte o artigo da Base de conhecimento Umbrella "516 Upstream Certificate CN Mismatch".

Por exemplo, considere um site que forneça conteúdo de URLs HTTP no formato: http://www.example.com/path_to_content. Se um usuário solicitar os URLs HTTPS equivalentes, mas o site não tiver um certificado cujas SANs correspondam a www.example.com (talvez a SAN só corresponda a example.com), o usuário receberá um erro 516 se a solicitação for tratada pelo Secure Web Gateway da Umbrella com uma política da Web que use o recurso HTTPS Inspection do SWG.

Mudança de comportamento do Chrome

Na segunda metade de outubro de 2023, o Google concluiu a implantação de um novo recurso para o navegador Chrome. Após essa data, uma solicitação para um URL HTTP é feita automaticamente usando a versão HTTPS desse URL. Por exemplo, quando um usuário faz uma solicitação para http://www.example.com, o Chrome primeiro tenta atender à solicitação usando https://www.example.com.

Se o Chrome receber um erro relacionado a HTTPS ao solicitar o URL HTTPS, ele tentará carregar o mesmo conteúdo por HTTP. Se a solicitação do URL HTTP for bem-sucedida, o Chrome exibe uma página intersticial com texto indicando que o site não é seguro e um link que dá ao usuário a opção de continuar, de acordo com a imagem abaixo.



Esse é o comportamento de retorno na nova funcionalidade do Chrome.

No entanto, ao navegar via SWG com inspeção HTTPS, se a solicitação HTTPS produzir um erro relacionado ao HTTPS, como "ERR_CERT_COMMON_NAME_INVALID" do site, o SWG interceptará o erro e retornará uma página de erro SWG ao Chrome, como a página de erro 516. Esse conteúdo SWG não é considerado um erro relacionado a HTTPS pelo Chrome, portanto, não produz o comportamento de fallback, e a página de erro SWG é exibida, em vez da página na imagem anterior.

Mais informações sobre o novo comportamento do Chrome podem ser encontradas no blog do Chromium e no repositório GitHub do recurso.

Determinando a origem do erro

Agora que o Chrome promove automaticamente URLs HTTP para URLs HTTPS, os sites que geram 516 erros são vistos com mais frequência pelos usuários.

Para confirmar que um site está causando um erro relacionado ao HTTPS, como a resposta 516, navegue pelo site com o Chrome a partir de um sistema de desktop que não use o Umbrella. Certifique-se de inserir manualmente a versão HTTPS do URL explicitamente no Chrome's Omnibox (como a barra de endereços) em vez de clicar em um hiperlink HTTP. Se um hiperlink produziu um erro 516 com o SWG, solicitar manualmente o URL HTTPS no Chrome sem o SWG pode produzir a mensagem de erro "ERR_CERT_COMMON_NAME_INVALID". Essa mensagem

de erro confirma que o problema é um certificado incorreto para o nome de domínio usado para acessar o site.

Como alternativa, use uma ferramenta on-line, como o site Qualys SSL Server Test, para diagnosticar o problema com o site.

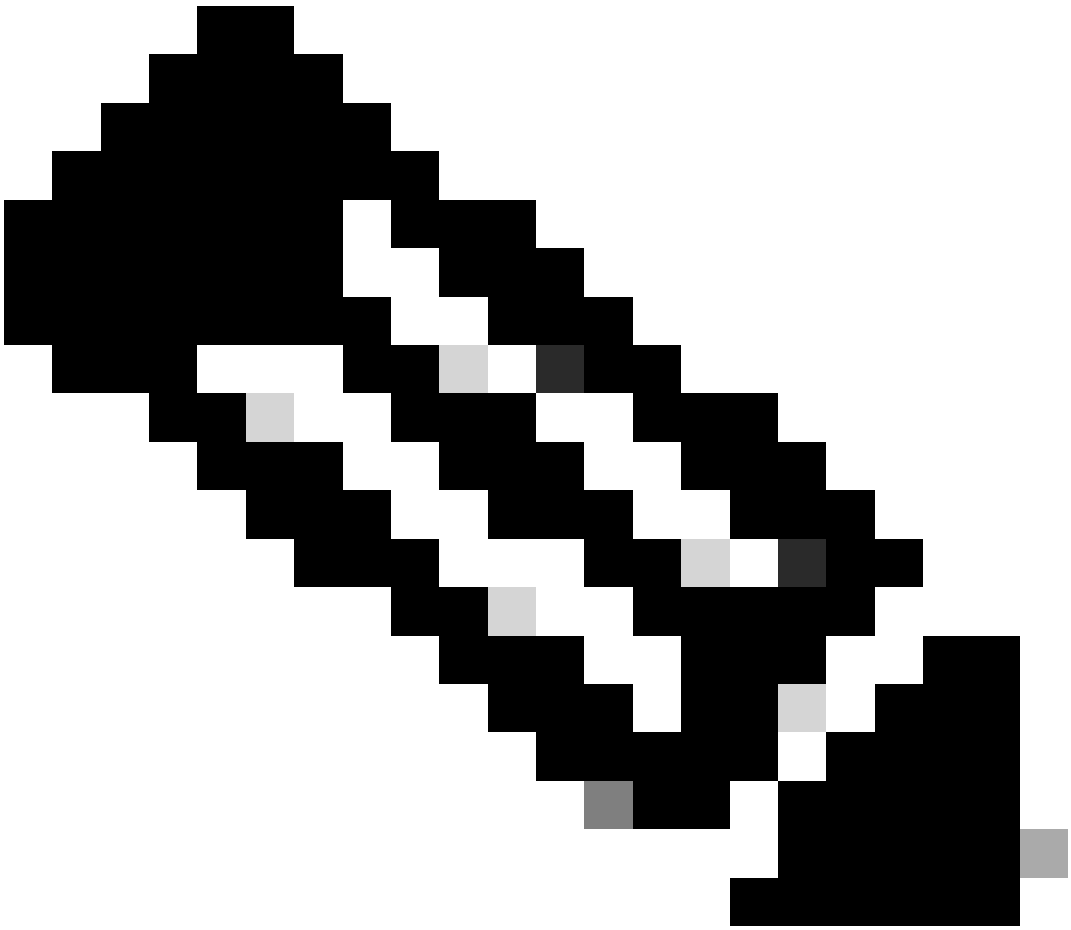
Soluções

Os administradores do Umbrella podem solucionar o problema com uma destas opções:

1. Crie uma Lista de Destinos especificamente para esses sites e adicione a lista a uma política da Web sem Inspeção HTTPS.

2. Crie uma Lista de Descriptografia Seletiva de sites que produzam 516 páginas de erro e adicione a Lista de Descriptografia Seletiva a todas as políticas da Web relevantes

---



Note: Fatores como redirecionamentos HTTP ou sistemas de segurança de e-mail que substituem os URLs HTTPS de seus serviços pelos URLs HTTP originais podem ocultar o nome de domínio necessário. Identificar o nome de domínio correto para uma lista de

---

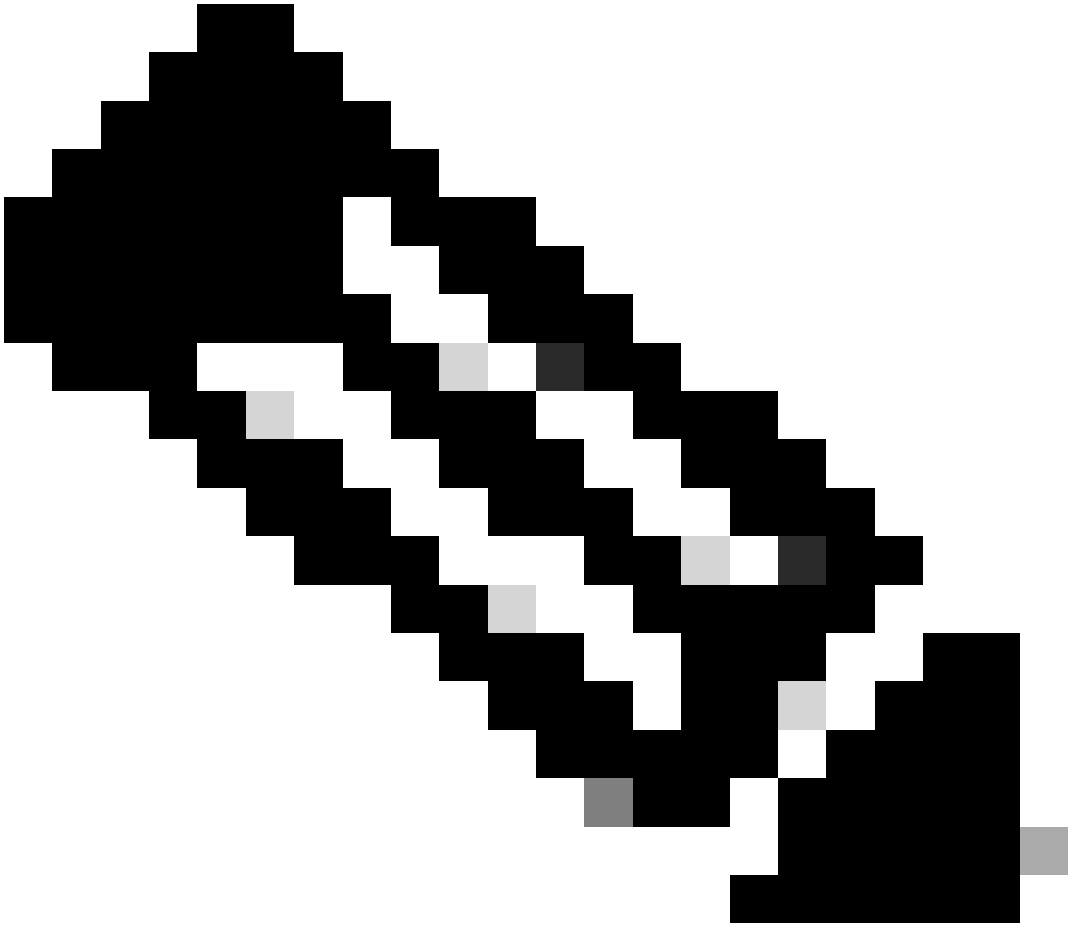
destino ou lista de descriptografia seletiva pode exigir investigação, incluindo o uso de ferramentas específicas (curl, Chrome Developer Tools, um registro do fornecedor de segurança de e-mail, etc.).

516 Erros e sistemas de e-mail

Um aumento na frequência de erros de 516 pode resultar de sistemas de e-mail que exibem e-mails em formato HTML e permitem hiperlinks nos e-mails. Ao redigir um e-mail, se o remetente digitar ou colar um nome de domínio no corpo do e-mail, muitos sistemas de e-mail promovem automaticamente um nome de domínio de texto simples para um hiperlink. Normalmente, quando o link é criado, o esquema é HTTP em vez de HTTPS.

Por exemplo, digitar a string `example.com` em um e-mail pode resultar em um e-mail contendo o código HTML `<a href="http://www.example.com">` que é exibido como o hiperlink www.example.com.

Se um destinatário de tal e-mail clicar no hiperlink HTTP, a solicitação inicialmente usará HTTPS se o clique abrir o Chrome ou se o Chrome já estiver sendo usado para visualizar o e-mail.



Note: Outros navegadores também podem promover HTTP para HTTPS.

Além disso, um hiperlink em um e-mail que use intencionalmente o esquema HTTP é tratado de forma semelhante.

Alguns serviços de nuvem comuns enviam e-mails de seus provedores de serviços de e-mail transacionais de terceiros com hiperlinks HTTP em vez de hiperlinks HTTPS. O site HTTPS que o Chrome tenta carregar automaticamente pode responder com um erro de certificado ao nome de domínio no link de e-mail, como neste exemplo do Seegrid.

Quando esses e-mails têm grandes listas de destinatários, muitos usuários cujos cliques (ou solicitações) são enviados por SWG podem relatar erros como o erro 516. Entre em contato com seu provedor de serviços de e-mail ou com a organização que enviou o e-mail para que o erro de certificado seja solucionado.

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.