Resolver erro de incompatibilidade de CN de certificado de upstream 516

Contents

Introdução

Problema

- Mecânica de identidade do certificado
- Erros de Identidade de Certificado

Resolução

- Nome Comum Preterido

Informações adicionais

Introdução

Este documento descreve como resolver um erro de incompatibilidade de CN de certificado de upstream 516.

Problema

Quando o proxy do Umbrella Secure Web Gateway (SWG) é configurado para executar a Inspeção HTTPS, um usuário pode receber uma página de erro 516 Upstream Certificate CN Mismatch ao navegar para um site usando um URL HTTPS.

Esse erro não indica um problema com o atributo Nome comum (CN) no campo Assunto do certificado do site. Em vez disso, o problema pertence ao atributo Nome DNS na extensão de nomes alternativos do assunto (SAN) de um certificado.

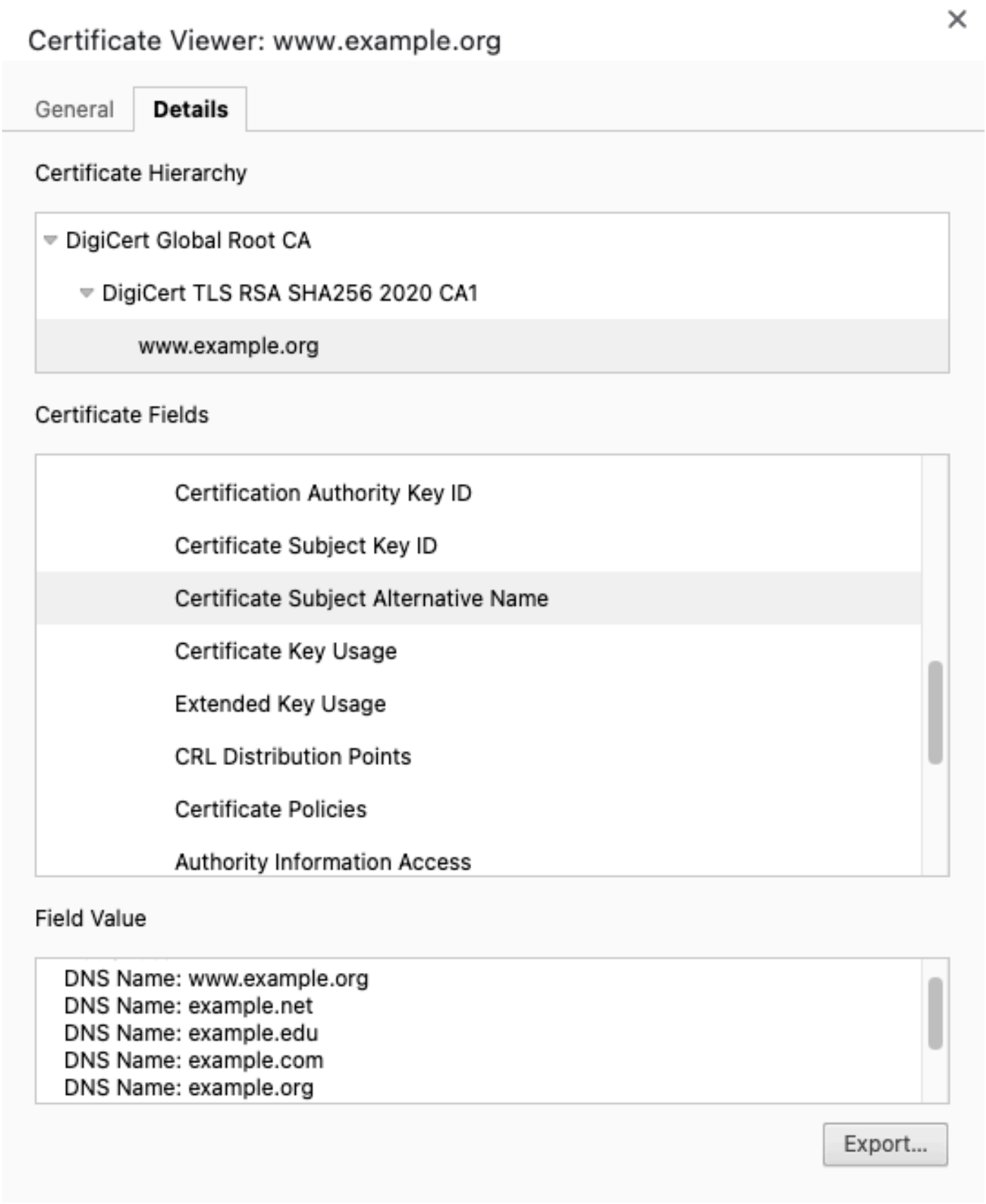
Depois de revisar este artigo, se você não conseguir identificar o motivo da página de erro 516, entre em contato com o suporte técnico da Umbrella e forneça-nos as informações especificadas na seção Erros de Identidade do Certificado neste documento.

Mecânica de identidade do certificado

Ao solicitar um URL HTTPS, um navegador ou outro cliente Web envia o nome de domínio no URL para o servidor Web através da extensão Server Name Indication (SNI) na mensagem de saudação do cliente da negociação TLS. O servidor usa esse valor de SNI para selecionar o certificado do servidor para retornar ao cliente, já que um servidor frequentemente hospeda vários sites e pode ter certificados diferentes para alguns ou todos os sites.

Quando o certificado do servidor é recebido pelo cliente Web, o cliente verifica se o certificado é o correto para a solicitação, comparando o nome de domínio solicitado com o(s) nome(s) de domínio nos atributos DNS Name da extensão Subject Alternative Names do certificado. Esta

imagem mostra essas SANs em um certificado de servidor.



16796247745556

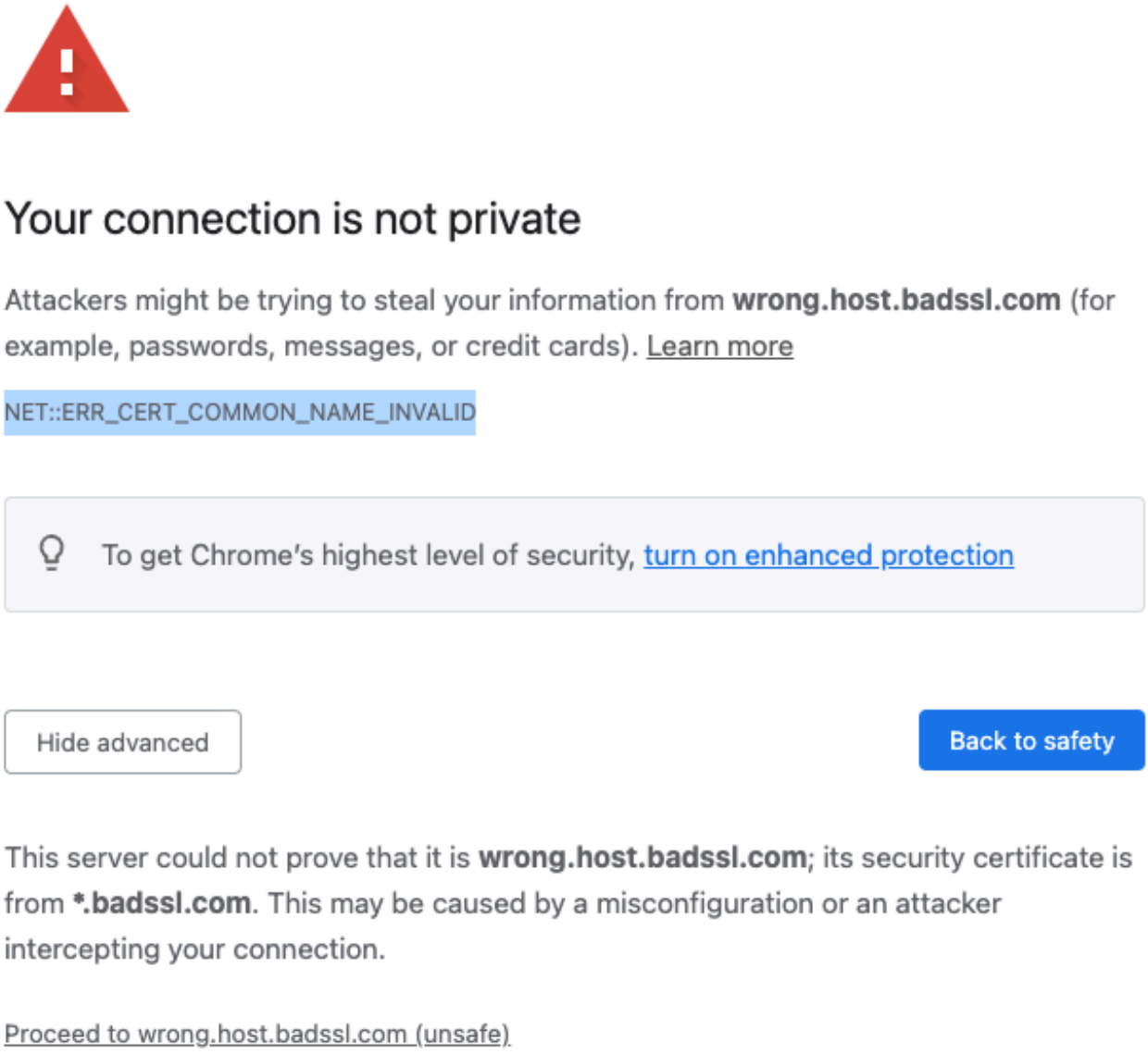
Este servidor Web retorna este certificado em resposta a solicitações com estes valores SNI, bem como outros não visíveis no painel Valor do campo:

- www.example.org
- example.net
- example.edu
- example.com
- example.org

Observe que SAN "example.com" não corresponde a uma SNI de "www.example.com". No entanto, uma SAN curinga de "*.example.com" corresponderia a uma SNI de "www.example.com" ou qualquer outro nome de domínio que contenha um único rótulo (uma string sem "." caractere) precedido de example.com, mas não de vários rótulos. Por exemplo, "www.hr.example.com" não é correspondido por "*.example.com" porque "www.hr" consiste em dois rótulos: "www" e "hr". Um único curinga só pode corresponder a um único rótulo.

Erros de Identidade de Certificado

Quando um cliente Web recebe um certificado de servidor, se nenhum dos Nomes DNS da SAN corresponder ao SNI do nome de domínio na URL solicitada, o cliente Web normalmente exibe um erro para o usuário. Esta imagem mostra o Chrome exibindo uma página intersticial "NET::ERR_CERT_COMMON_NAME_INVALID".



16794294817428

Na imagem, o site solicitado era "https://wrong.host.badssl.com", que não corresponde a nenhuma SAN. O certificado contém um nome DNS SAN curinga, "*.badssl.com" cujo curinga só pode corresponder a um único rótulo, como "host". Além disso, o certificado não tem um nome DNS de SAN com o valor exato "errado.host.badssl.com" ou uma SAN curinga de "*.host.badssl.com", então o erro é apresentado ao usuário.

Para identificar o motivo de uma incompatibilidade de identidade de certificado, inspecione os Nomes DNS SAN do certificado usando a função de exibição de certificado do navegador e compare com o nome de domínio na URL solicitada. Como alternativa, uma ferramenta como o Teste de servidor SSL do Qualys pode ser usada para diagnosticar um problema de identidade de certificado.

Se o motivo para o erro 516 não puder ser identificado depois de empregar as informações nesta

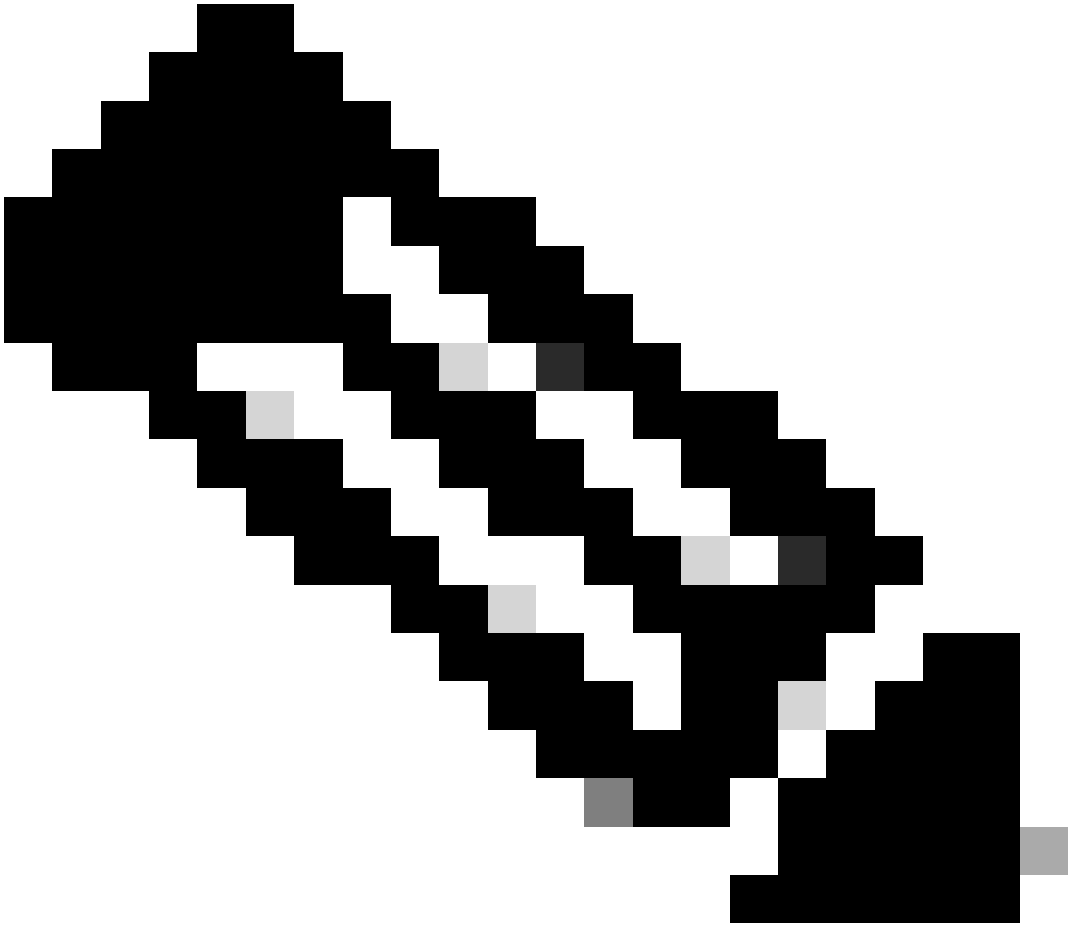
seção, ou se as soluções e soluções alternativas na próxima seção não puderem ser empregadas, abra um caso com o suporte técnico da Umbrella e forneça:

1. uma captura de tela que captura
    - a barra de endereços do navegador mostrando o URL solicitado
    - a página de erro 516 inteira (consulte a imagem na próxima seção)
2. o texto do URL copiado da barra de endereços

Resolução

Para resolver esse problema, acesse o servidor com um nome de domínio que corresponda a um dos Nomes DNS SAN no certificado. Isso pode exigir que o administrador do site adicione um nome de domínio correspondente ao DNS da zona. Como alternativa, o administrador pode emitir novamente o certificado para incluir o nome de domínio do URL em um dos Nomes DNS da SAN.

Como solução alternativa, o nome de domínio da URL pode ser adicionado a uma Lista de Descriptografia Seletiva para o proxy de Gateway da Web Seguro ou a uma Lista de Destino no Proxy Inteligente. Aplique a lista à configuração de conjunto de regras da política da Web apropriada (Gateway da Web seguro) ou à lista de permissões da política DNS (Proxy inteligente). Isso evita que a solicitação para o site seja descriptografada pelo proxy, o que impede que o proxy exiba uma página de erro 516.



Note: O uso do proxy do Secure Web Gateway e do Intelligent Proxy não é suportado. Somente uma tecnologia de proxy pode ser empregada por organização. É recomendável que as organizações que têm assinaturas para o Secure Web Gateway usem o SWG e não o Intelligent Proxy.

Nome Comum Preterido

Os clientes da Web originalmente corresponderam ao nome de domínio na URL solicitada para o atributo Common Name (CN) no campo Subject do certificado. Este mecanismo foi preterido em clientes web modernos; Os domínios agora são comparados com os Nomes DNS da extensão Nome Alternativo do Assunto. No entanto, o texto das mensagens de erro geralmente continua a fazer referência ao mecanismo preterido, como "NET::ERR_CERT_COMMON_NAME_INVALID" no Chrome.

Da mesma forma, o Umbrella SWG exibe uma página de erro 516 com este texto quando o proxy SWG solicita uma URL de um servidor Web e ocorre uma incompatibilidade de Nome DNS da SAN:

16794325789332

O Cisco Umbrella planeja atualizar este texto em uma data futura para refletir melhor o comportamento atual.

Informações adicionais

Consulte RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Seção 4.1.2.6 para obter informações sobre o Assunto do certificado e Seção 4.2.1.6 para obter informações sobre o Nome Alternativo do Assunto.

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.