Solucionar problemas de HSTS e erros de certificado de fixação

Contents

Introdução

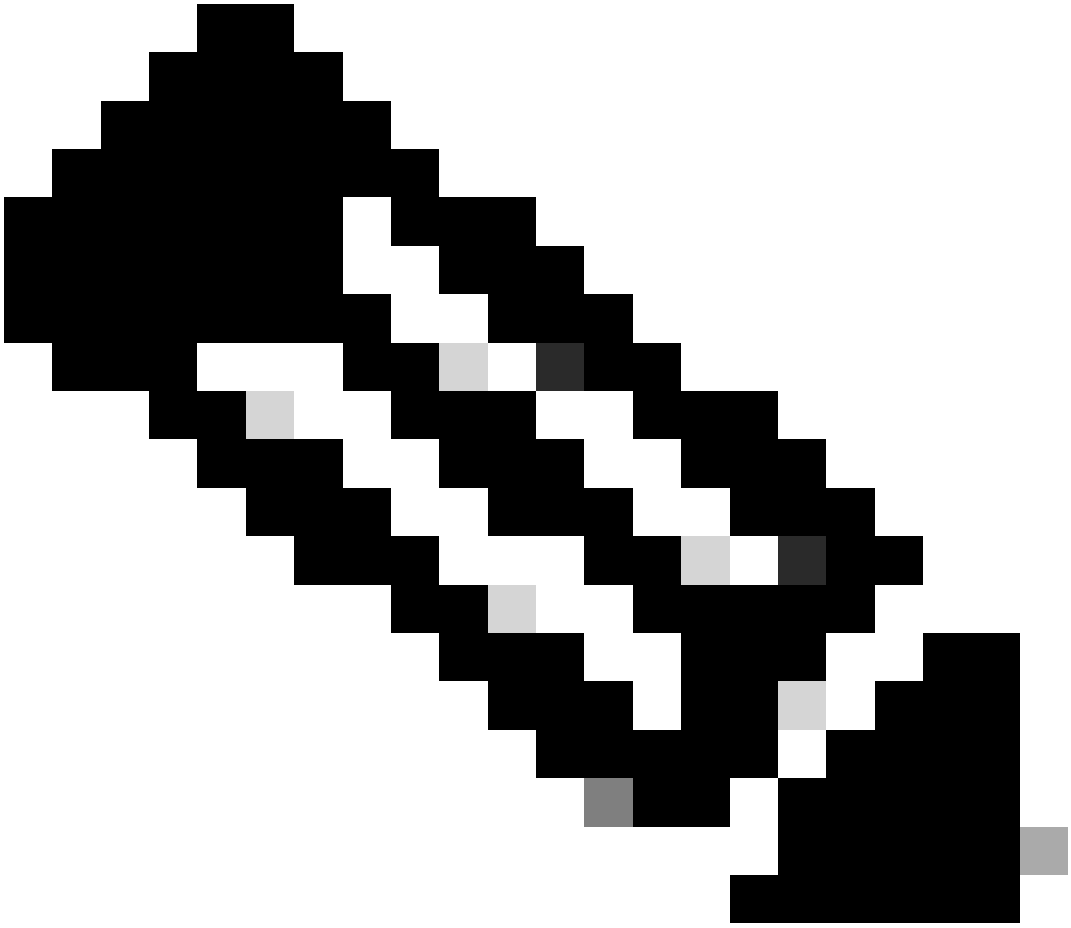
Este documento descreve como limpar um erro de certificado "Sua conexão é não confiável/não privada" que não pode ser ignorado.

Erro de certificado

Quando um erro de certificado para `*.opendns.com` ou `*.cisco.com` for exibido, mas não puder ser ignorado pela adição de uma exceção de certificado, conforme descrito na documentação do Cisco Umbrella Gerenciar o Certificado Raiz do Cisco Umbrella, use estas etapas para permitir que o erro de certificado seja eliminado.

Quando não é possível ignorar o erro de certificado adicionando uma exceção, isso ocorre devido à implementação do HTTP Strict Transport Security (HSTS) ou da Fixação de Certificado pré-carregada em navegadores modernos. A comunicação entre determinados navegadores e determinados sites é feita de uma forma que inclui a exigência de usar HTTPS e não é possível ignorar ou exceções. Essa segurança extra para páginas HTTPS impede que a página de bloqueio Umbrella e o mecanismo de página de bloqueio bypass funcionem quando o HSTS estiver ativo para um site.

Como resultado, a página em questão não pode ser acessada através do Block Page Bypass (BPB) (na verdade, a tela Bypass pode nem aparecer). Esses métodos podem permitir acesso ao login BPB, mas após o login, o erro de certificado reaparece e nega o acesso. Revise o restante deste artigo se você estiver vendo um erro de certificado no Google Chrome, Mozilla Firefox, Safari que não pode ser ignorado e você está tentando acessar o login de desvio.



Note: Uma solução para esse problema que é mais fácil de gerenciar e persistente para todos os sites está disponível agora.

Como resultado, essas informações ainda são aplicáveis, mas agora podem ser contornadas com uma solução permanente. Tente instalar o Cisco Root CA através da documentação do Cisco Umbrella: Gerenciar o certificado raiz do Cisco Umbrella

---

IMPORTANTE: Se o domínio estiver na lista fixa do HSTS, uma exceção não poderá ser adicionada, uma vez que a lista é efetivamente incontornável se você estiver executando o Chrome, Safari ou Firefox (o Internet Explorer (IE) não é afetado). Bloquear desvio de página não funciona para sites como este. Para obter uma lista completa de serviços que usam o HSTS por esses três navegadores, consulte a Pesquisa de Código do Google Chromium. Os serviços notáveis nesta lista incluem:

- Google (e recursos do Google, como Gmail, Youtube ou Google Docs)
- Dropbox
- Twitter

- Facebook

Se isso estiver causando um problema para você ou seus usuários e você quiser ver as alterações no Bloquear desvio de página para ajudar a aliviar esse problema, envie um e-mail para umbrella-support@cisco.com ou seu Gerente de conta para enviar uma solicitação de recurso. Nossas equipes de engenharia e gerenciamento de produtos estão cientes das dificuldades com certificados e desvio de página de bloqueio e estão testando redesigns alternativos deste recurso.

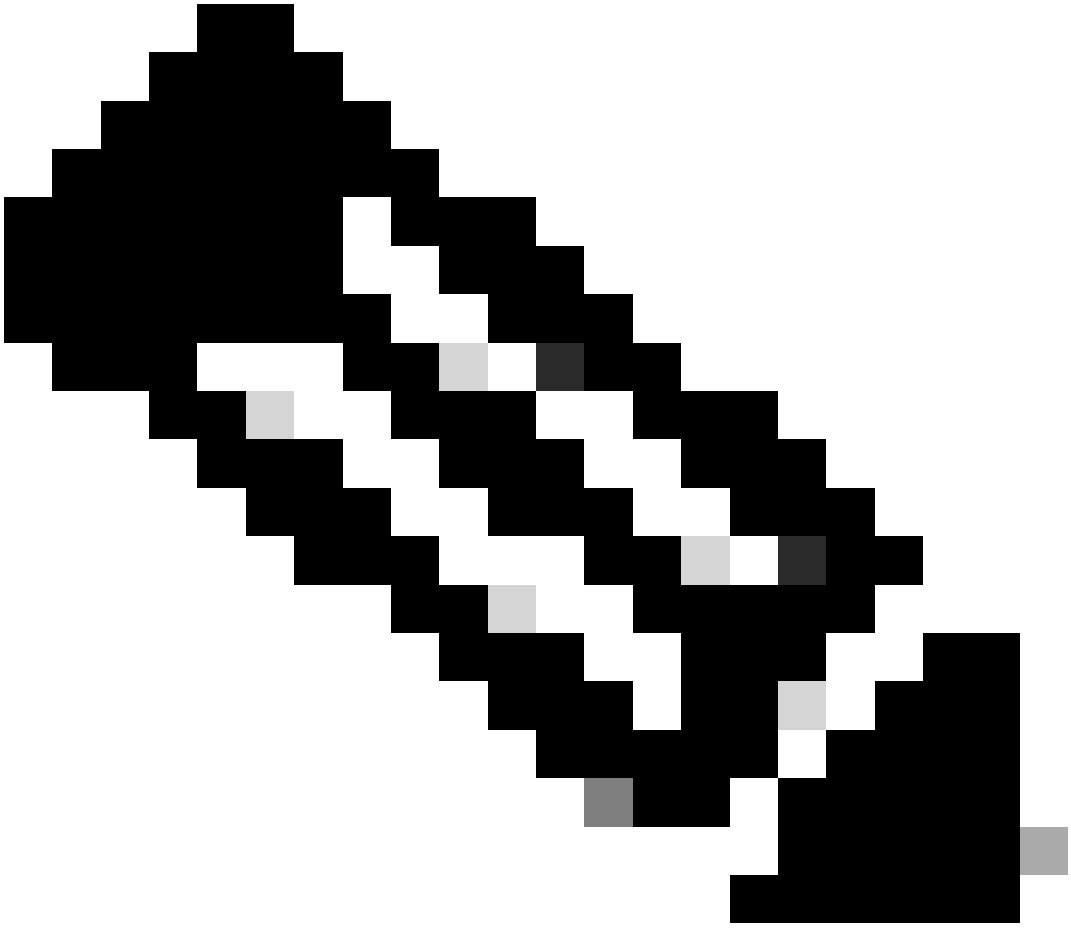
Soluções possíveis

Há algumas maneiras de resolver esses problemas. Primeiro, essas seções demonstram como usar políticas mais granulares para contornar esse problema. Segundo, você pode usar as configurações do navegador, mas elas são isoladas em um subconjunto dos navegadores afetados por esse problema.

Gerenciamento de políticas e cliente de roaming

Pode haver problemas com a configuração da rede ou com a política de uso aceitável (RH) que impeçam essa solução. O gerenciamento de políticas não é uma solução eficaz se os usuários tiverem permissão para visitar esses domínios somente em determinados horários (como durante o horário de almoço). A Umbrella não pode fornecer uma aplicação de política baseada em tempo com nosso serviço, portanto, permitir que um usuário acesse o site o tempo todo pode ser problemático. Em um computador compartilhado, como um terminal público, o cliente de roaming Umbrella não pode diferenciar entre usuários e não pode permitir facilmente os domínios certos para as pessoas certas.

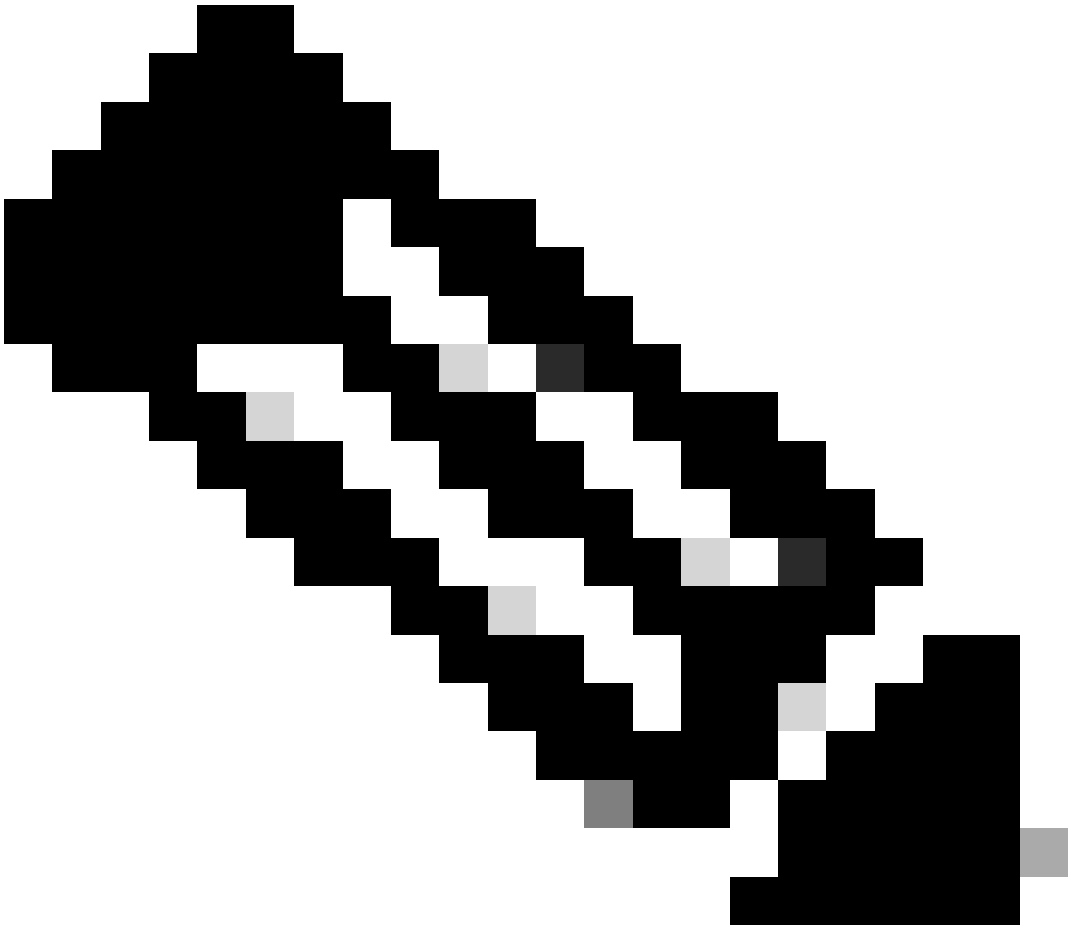
O gerenciamento de políticas não é tão eficaz ao considerar identidades não granulares, como Sites ou Redes, a menos que o administrador se sinta confortável em dar a todos os usuários dessa rede o mesmo acesso. O gerenciamento de políticas funciona melhor quando aplicado a um subconjunto de usuários que têm permissão para acessar sites, enquanto o restante da rede não pode, e isolar esses usuários instalando o cliente de roaming em suas máquinas e aplicando a hierarquia de política apropriada.



Note: A Cisco anunciou o Fim da Vida Útil do Umbrella Roaming Client em 2 de abril de 2024. A última data de suporte para o cliente Umbrella Roaming é 2 de abril de 2025. Todas as funcionalidades do cliente Umbrella Roaming estão disponíveis no Cisco Secure Client. A Cisco está fornecendo inovações futuras apenas no Cisco Secure Client. Recomendamos que os clientes comecem a planejar e programar a migração agora mesmo. Consulte este artigo do KB para obter orientação sobre como migrar do Umbrella Roaming Client para o Cisco Secure Client.

O gerenciamento adequado de políticas é a melhor solução para esse problema, pois o navegador não recebe uma resposta de validação com falha. Se alguns dos seus usuários tiverem permissão para acessar sites que normalmente precisariam usar o Bloquear desvio de página para acessar, você poderá configurar uma política separada para esses usuários e adicionar os domínios que eles podem ter permissão para usar à Lista de permissões. Como as solicitações dos usuários nunca são bloqueadas, o navegador nunca recebe uma solicitação de um domínio com um certificado incompatível. Você pode usar o Umbrella Roaming Client para fornecer essas políticas específicas. Isso significa que você está colocando determinados domínios em uma lista de permissões

para que determinados usuários sempre do dia solucionem esses erros.



Note: O cliente de roaming Umbrella é uma maneira eficaz de distribuir determinadas políticas para vários usuários, mas se você tiver habilitado a integração do Ative Diretory(AD), poderá aplicar essas políticas permitidas a determinados usuários do AD também.

Ignorando erros de exceção de certificado (somente Chrome para Windows)

Somente o Chrome para Windows pode ser configurado para ignorar erros de exceção de certificado, o que atenua esse erro. O navegador é instruído a ignorar o erro e a página de bloqueio normal do Umbrella é vista.

IMPORTANTE: Esse método é mais arriscado do que ajustar o gerenciamento de políticas porque o navegador está configurado para ignorar erros de certificado. É possível que, como

resultado, o navegador possa estar sujeito a ataques de MiTM (man-in-the-middle). Como resultado, não podemos recomendar isso como uma abordagem segura para lidar com esse erro, mas é uma solução alternativa.

Essas alterações de configuração devem ser feitas por computador, o que dificulta ambientes de grande escala, mas funciona.

Firefox, Safari e Chrome para Mac OS X

O Firefox, o Safari e o Chrome para Mac OS X não podem ser configurados para ignorar erros de exceções de certificado para domínios com pin e sempre honram a lista de HSTS. Não há nenhuma solução conhecida para esses erros.

Internet Explorer

O Internet Explorer (IE) não implementa restrições de HSTS. Como resultado, o IE não precisa ser configurado e não exibe esse erro. Isso estará sujeito a alterações em versões futuras do IE se a Microsoft optar por implementar o HSTS no navegador.

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.