Solucionar erros de revogação de certificado do navegador ao usar a filtragem de guarda-chuva

Contents

Introdução

Este documento descreve como resolver erros de revogação de certificados do navegador ao usar a filtragem Umbrella.

Problema

Ao usar o Modo Somente Permitir ou as Configurações de Categoria restritivas, você frequentemente precisa adicionar vários domínios à lista de permissões para que um site seja carregado corretamente.

Um problema específico é que as Listas de Revogação de Certificados (CRLs) para sites HTTPS/SSL podem ser bloqueadas, o que, por sua vez, gera erros em alguns navegadores. Às vezes, o bloqueio dessas CRLs também introduz latência enquanto o navegador tenta fazer sua validação.

Causa

As CRLs (Certificate Revocation Lists - Listas de Certificados Revogados) e o OCSP (Online Certificate Status Protocol - Protocolo de Status de Certificados Online) mais recentes são usados para perguntar a uma autoridade de certificação se um certificado SSL foi revogado por algum motivo. Isso normalmente acontece de forma transparente em segundo plano quando você está se conectando a um site HTTPS.

A ideia é que o navegador pare o usuário de ir para o site se o certificado tiver sido revogado no caso de o certificado / CA ser comprometido. É uma boa ideia permitir o acesso a CRLs.

No Modo Somente Permitir, a maioria das CRLs é bloqueada, a menos que você as tenha desbloqueado especificamente. O impacto disso depende de qual navegador da Web está sendo usado...

- O Internet Explorer 7 mostra um aviso pop-up com um erro como o mostrado abaixo. As informações de revogação do certificado de segurança deste site não estão disponíveis.

- As versões posteriores do Internet Explorer não apresentam nenhum erro a menos que um sinalizador de chave de registro específico tenha sido definido.
- O Google Chrome mostra um aviso ao lado da barra de endereços. Clicar no aviso mostra este erro: Não é possível verificar se o certificado foi revogado
- O Firefox não apresenta nenhum erro a menos que a configuração security.OCSP.require tenha sido definida em about:config

Resolução

1. Localize a CRL do certificado exibindo o certificado no navegador da Web (as etapas variam dependendo do navegador).
2. Use a guia 'Detalhes' e procure estas informações:
    - Pontos de Distribuição de CRL
    - Informações de acesso da autoridade
3. Anote as informações da URL (exemplo abaixo) e adicione-as à lista de permissões no painel do Umbrella:

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.