Problemas de confiança de CA personalizada de acesso seguro com Firefox e Safari no macOS

Contents

Problema

Os usuários experimentaram erros de confiança de certificado em navegadores macOS (Safari e Firefox) ao acessar o tráfego descriptografado da Internet através do Cisco Secure Access. O navegador Chrome funcionou corretamente, mas o Safari e o Firefox exibiram avisos de "certificado não confiável" e bloquearam o acesso a sites e aplicativos.

A cadeia completa de certificados mostrou:

- Site (como cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Os navegadores Firefox e Safari interromperam a validação de certificados nos certificados intermediários da Cisco e não conseguiram se encadear até a CA raiz, enquanto o Chrome validou com êxito toda a cadeia de certificados.

Ambiente

- Implantação do Cisco Secure Access com autoridade de certificação personalizada para descriptografia HTTPS
- dispositivos macOS com navegadores Safari e Firefox
- Infraestrutura de certificado de autoridade de certificação personalizada usando a Autoridade de Certificação da Microsoft
- Políticas de acesso à Internet com descriptografia e prevenção contra invasões ativadas
- ID da organização: xxxxx

Resolução

O problema foi resolvido identificando-se uma incompatibilidade de codificação na cadeia de certificados e alternando-se para a CA raiz do Cisco Secure Access para descriptografia.

Análise da causa raiz

A equipe identificou que a autoridade de certificação personalizada foi criada usando codificação de cadeia de caracteres imprimível, o que causou problemas de incompatibilidade, mesmo quando os certificados folha foram definidos como UTF8STRING. O Firefox e o Safari exigem que todos os certificados em uma cadeia estejam no mesmo formato, enquanto o Chrome não tem esse requisito rigoroso.

Etapas de Resolução

Alternar para CA raiz de acesso seguro da Cisco

Soluções alternativas

Se for necessário usar uma CA personalizada, estas opções serão identificadas:

- Reconstruir toda a infraestrutura de certificado usando codificação UTF8 (alto impacto, não recomendado)
- Usar uma infraestrutura de certificado diferente que suporte a codificação UTF8
- A limitação do Firefox e do Safari não pode funcionar com a configuração atual de CA personalizada

Causa

A causa raiz foi uma incompatibilidade de codificação entre a Microsoft Certificate Authority (que usa a codificação printablestring por padrão) e a cadeia UTF8 usada pelo Cisco Secure Access. O Firefox e o Safari têm requisitos de validação de certificados mais rigorosos e precisam de todos os certificados na cadeia para usar uma codificação consistente. a validação mais tolerante no Chrome permitiu que ele funcionasse com a cadeia de codificação mista, enquanto o Firefox e o Safari rejeitaram os formatos de certificado inconsistentes.

A Microsoft CA criou certificados usando a codificação printablestring, mas os certificados intermediários do Cisco Secure Access usaram a codificação UTF8STRING. Essa incompatibilidade fez com que o Firefox e o Safari falhassem na validação da cadeia de certificados no nível intermediário de certificado da Cisco.

Conteúdo relacionado

- Configurar o acesso à reunião do Webex no SWG
- Suporte técnico e downloads da Cisco

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.