

Tratamento de Erros de Certificado de Descriptografia SSL no Acesso Seguro

Contents

Problema

Os usuários estão experimentando páginas de erro relacionadas ao certificado quando a descriptografia SSL está habilitada no Cisco Secure Access. Várias consultas foram recebidas em relação a três tipos específicos de erros de certificado:

- Erros expirados do certificado do servidor de origem
- Erros de incompatibilidade de CN/SAN de certificado em que o Nome comum ou os Nomes alternativos do assunto listados no certificado não correspondem ao domínio acessado
- Link da Lista de Certificados Revogados (CRL) inserido no certificado do servidor de origem causando problemas de conectividade

Esses erros de certificado são semelhantes a avisos que normalmente seriam exibidos em navegadores da Web. A questão que surge é se o Cisco Secure Access pode lidar com erros relacionados ao certificado exibindo páginas de aviso (semelhantes a navegadores ou filtros de conteúdo) e, em seguida, permitindo acesso após exibir o aviso, ou permitindo acesso em todos os casos. Além disso, é necessário entender o comportamento quando a descriptografia SSL é desativada e se o tráfego passa, independentemente dos problemas de certificado.

Ambiente

- Cisco Secure Access - Acesso à Internet (Módulo de roaming, VA, DNS, SWG, PAC, IPS, Certificados)
- Funcionalidade de descriptografia SSL habilitada
- Vários domínios com problemas de validação de certificado
- Servidores de origem com vários problemas de certificado, incluindo expiração e

Resolução

Limitações de Tratamento de Erros de Certificado

A manipulação de erros relacionados ao certificado não está disponível no Cisco Secure Access. O produto não oferece suporte a:

- Apresentando páginas de aviso semelhantes ao navegador para problemas de certificado
- Configuração de tratamento de erro de certificado específico de domínio
- Tratamento personalizado de erros com base nos domínios de destino
- Páginas de aviso de estilo de filtro de conteúdo com opções de substituição do usuário

Solução alternativa de exclusão decriptografia SSL

A abordagem recomendada é excluir domínios problemáticos da descriptografia SSL usando as configurações de descriptografia de perfil de segurança. Isso pode ser configurado por meio de:

Navegue até a seção Perfil de segurança > Configurações de descriptografia para excluir domínios específicos da inspeção de SSL.

Quando os domínios são excluídos da descriptografia SSL, este comportamento ocorre:

- O tráfego para domínios excluídos ignora a inspeção de SSL completamente
- A validação do certificado não é executada pelo Secure Access
- Os usuários não encontram páginas de erro de certificado geradas pelo Secure Access
- Os erros do certificado original possivelmente ainda estarão visíveis no navegador do usuário se os problemas do certificado persistirem

Comportamento Desabilitado de Descriptografia SSL

Quando a descriptografia SSL é desativada para um domínio ou globalmente, o Cisco Secure Access transmite o tráfego (encaminha), independentemente de qualquer problema de certificado. O produto não inspeciona nem valida certificados quando a descriptografia não está habilitada, permitindo efetivamente que todo o tráfego HTTPS passe de forma transparente.

Causa

Os erros de certificado são causados por problemas legítimos de validação de certificado nos servidores de origem, incluindo certificados expirados, incompatibilidades de CN/SAN e problemas de conectividade de CRL. O Cisco Secure Access executa a validação do certificado como parte de seu processo de descriptografia SSL e, quando essas falhas de validação ocorrem, o produto gera páginas de erro para evitar conexões potencialmente não seguras. Este é o comportamento de segurança pretendido do recurso de inspeção SSL.

Conteúdo relacionado

- [Documentação de Configuração de Descriptografia do Cisco Secure Access](#)
- [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.