

Entender erros de handshake e certificado SSL no acesso seguro

Contents

Problema

O tráfego HTTP bloqueado devido a erros de certificado e TLS agora pode ser exibido na Pesquisa de atividades do painel. Este artigo fornece uma lista de mensagens de erro comuns, bem como uma breve explicação de cada um dos erros.

Ambiente

- Cisco Secure Access — Inspeção SSL do Secure Web Gateway

Resolução

Certificado de upstream expirado

O certificado do site expirou, portanto, o Cisco Secure Access não confia nele. Esta é sobre o proprietário do site para corrigir, então entre em contato com o webmaster do site e avise-os.

Certificado de upstream autoassinado

O site apresenta um certificado que ele próprio assinou, em vez de um certificado emitido por uma Autoridade de Certificação confiável. Como nenhuma autoridade independente está

atestando isso, o Cisco Secure Access não tem como confirmar se o certificado é original.

Você frequentemente vê certificados autoassinados em recursos destinados a um público pequeno e interno — os portais de administração em dispositivos de segurança de TI são um exemplo clássico. Apenas observe que o Cisco Secure Access não pode ser configurado para confiar em certificados autoassinados.

Certificado Intermediário Ausente

O Cisco Secure Access não pôde reunir todos os certificados intermediários de que precisa, portanto, não pode criar a cadeia completa de confiança de volta para uma raiz.

Veja por que isso é importante: um certificado do site (a "folha") é assinado por um certificado intermediário, que por sua vez pode ser assinado por outro intermediário, e assim por diante até uma raiz confiável. Para que esta cadeia faça o check-out, o site tem que enviar seu(s) certificado(s) intermediário(is) junto com o seu próprio. Quando elas estiverem faltando, a validação falha; portanto, avise ao webmaster do site.

Há uma exceção: se o certificado incluir a extensão "Authority Information Access" (AIA), o Cisco Secure Access poderá tentar buscar os intermediários ausentes por conta própria. Lembre-se de que isso só funciona quando a Descriptografia HTTPS e a Inspeção de arquivo estão ativadas.

Certificado de Upstream com Nome de Entidade Ausente

O certificado não inclui um nome da Entidade (um Nome Distinto) ou um Nome Alternativo da Entidade, o que significa que não há nada que identifique claramente a quem o certificado pertence. Sem isso, o Cisco Secure Access não pode validá-lo. Isso é algo que o proprietário do site precisa corrigir.

Certificado de Upstream com Nome Comum Ausente

O certificado não tem um CN (Common Name - Nome comum) — o campo que tradicionalmente continha o nome de host do site e ajudou a confirmar que o certificado realmente pertence ao site que você está visitando. Hoje em dia, essa verificação realmente depende do SAN (Nome alternativo do assunto) e o CN é considerado um campo herdado, mas sua ausência ainda pode

disparar esse erro. Entre em contato com o webmaster para que ele seja tratado.

Certificado de Upstream Não Confiável

O Cisco Secure Access não confia nesse certificado, geralmente porque ele não reconhece a CA raiz que o emitiu.

O Cisco Secure Access SWG mantém uma lista integrada de Autoridades de Certificação Raiz confiáveis, fornecidas por um provedor confiável e atualizadas. Se o certificado de um site for rastreado até uma CA que não esteja na lista, a validação falhará. Se você tiver certeza de que a CA raiz é confiável, entre em contato com o suporte técnico e podemos dar uma olhada.

O nome de host no certificado é diferente do esperado

O endereço solicitado não corresponde ao nome no certificado — nem seu CN (Common Name, nome comum) nem qualquer SAN (Subject Alternative Names, nomes alternativos do assunto). Como o certificado não parece pertencer ao site que você está acessando, o Cisco Secure Access não confia nele para esta solicitação. O webmaster precisa resolver isso.

Certificado de upstream revogado

Desde então, a autoridade de certificação que emitiu o certificado o revogou, ou seja, o certificado deixou de ser considerado válido.

O Cisco Secure Access confirma isso usando o protocolo OSCP, que verifica em tempo real se um certificado foi revogado. Informe ao webmaster do site para que ele possa substituí-lo.

Erros de handshake TLS

Cifra de upstream não suportada

O handshake TLS não pôde ser concluído porque o site não oferece suporte a nenhum dos pacotes de codificação que o Cisco Secure Access SWG usa. Isso tende a aparecer com servidores antigos ou desatualizados que oferecem apenas cifras mais fracas. A correção está no lado do servidor, então passe-a para o webmaster.

Incompatibilidade de versão de TLS de upstream

O handshake falhou porque o site não está usando uma versão TLS que o Cisco Secure Access SWG suporta. No momento, o proxy SWG do Cisco Secure Access funciona com TLS 1.2 e TLS 1.3 — tanto para conexões recebidas dos clientes quanto para conexões estabelecidas com os servidores de destino.

Chave DH upstream menor que 1024 bits

O handshake não pôde ser concluído porque o site está usando uma chave Diffie-Hellman que é muito fraca (abaixo de 1024 bits) para o Cisco Secure Access aceitar. Essa é uma limitação do lado do servidor, portanto, o webmaster precisa fortalecê-la.

Soluções

É possível solucionar esses problemas fazendo alterações de configuração no Cisco Secure Access.

Isso só deverá ser feito se você confiar na autenticidade do servidor e do certificado.

Soluções alternativas podem ser aplicadas usando uma entrada "Selective Decryption List" (Lista de descryptografia seletiva) para desativar a descryptografia ou uma entrada "External Domains" (Domínios externos) para ignorar totalmente o tráfego do Cisco Secure Access. O Cisco Secure Access não executa validação de certificado quando a descryptografia está desabilitada.

Esteja ciente de que, na maioria dos casos, o navegador ainda apresenta um erro ou aviso quando o tráfego é ignorado do Cisco Secure Access - Os navegadores da Web executam validação de certificado semelhante.

Causa

O proxy de inspeção SSL do Cisco Secure Access não pôde concluir o handshake TLS — mais comumente, porque o destino usa a fixação de certificado que rejeita o certificado reassinado CSA.

- Fixação do certificado: impressão digital de certificado esperada de códigos rígidos de cliente
- CA CSA não confiável no endpoint: certificado de autoridade de certificação de inspeção não implantado no repositório raiz confiável

Conteúdo relacionado

- [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.