

Falha de handshake TLS de recurso privado baseado em navegador ZTA

Contents

Problema

Os usuários não podem acessar um recurso privado baseado em navegador por meio do Cisco Secure Access.

Ao tentar se conectar, estes sintomas ocorrem:

- O handshake triplo TCP é concluído com êxito, mas a negociação TLS falha após o Hello do cliente.
- A conexão com a URL pública mapeada para SSE (<https://example-orgid.ztna.sse.cisco.io>) alcança a autenticação Cisco, mas retorna o erro HTTP 404.
- Depois de adicionar o FQDN à configuração de recurso privado, o tráfego é redirecionado para o prompt de autenticação, mas resulta em uma página em branco após a autenticação.
- Os arquivos HAR mostram respostas HTTP 200, mas o handshake TLS não é concluído.
- Motivo do bloqueio aparece como: "Acesso privado: os dados de postura buscados para o dispositivo são muito antigos/precisam ser atualizados".

Ambiente

- Cisco Secure Access (SSE)
- ID da org. do Secure Access: xxxx
- Acesso à rede com confiança zero (ZTNA) baseado em navegador
- Recurso privado: example.net

- Recurso particular de trabalho para comparação: abc.net
- Configuração de certificado curinga

Resolução

O problema foi resolvido com a configuração do recurso privado para usar a mesma configuração de certificado que um recurso privado em funcionamento.

As etapas descritas nas próximas seções foram executadas.

Passo 1: Analisar configuração de trabalho

Compare o recurso privado com falha (example.net) com um recurso privado em funcionamento (abc.net) para identificar as diferenças de configuração.

O recurso de trabalho usado:

- Opção Usar um URL no seu domínio
- Referência ao par de chave/certificado curinga existente

Passo 2: Análise de captura de pacotes

Execute a análise de captura de pacotes usando o Wireshark para confirmar a falha de handshake TLS:

- Verifique se o handshake triplo do TCP foi concluído com êxito.
- Confirme se a negociação TLS falha após o Hello do cliente.
- Coletar artefatos de diagnóstico: Arquivos HAR, pacote DART e capturas de pacotes.

Passo 3: Verificação de certificado

Acesse o aplicativo pela conexão RAVPN para verificar a apresentação do certificado:

- Confirme se o site `example.net` está apresentando um certificado curinga.
- Documente os detalhes do certificado para referência de configuração.

Passo 4: Configurar recurso privado

Aplique a mesma abordagem de configuração usada pelo recurso privado em funcionamento:

- Configure o recurso particular para usar a opção Usar um URL no seu domínio.
- Faça referência ao par de certificado/chave curinga existente.
- Verifique se o FQDN está configurado corretamente no campo de recurso privado.

Passo 5: Validação

Teste o acesso baseado em navegador para confirmar se a configuração resolve o problema:

- Verifique a conclusão bem-sucedida do handshake TLS.
- Confirme o fluxo de autenticação adequado.
- Validar a pós-autenticação de acessibilidade do aplicativo.

Causa

A causa raiz foi uma incompatibilidade de configuração na instalação do recurso particular. O recurso privado com falha não foi configurado para fazer referência adequada ao certificado curinga que o aplicativo de destino estava apresentando. O handshake TLS falhou porque a configuração do recurso privado não estava alinhada com a configuração do certificado usada

pelo servidor de aplicativos. Ao configurar o recurso privado para usar a opção Usar um URL no seu domínio e referenciar o par de chave/certificado curinga existente (correspondendo à configuração de trabalho), a negociação TLS pode ser concluída com êxito.

Conteúdo relacionado

- [Guia de referência da Cisco para acesso seguro](#)
- [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.