Falhas de Autenticação de Verificação de Postura de Inspeção de Certificado de Acesso Seguro

Contents

Problema

Ao tentar implantar o acesso seguro com o perfil de postura de endpoint usando o recurso de inspeção de certificado, todas as tentativas de login falham, apesar do fato de que causas específicas de falha não podem ser identificadas nos logs do pacote DART. Os usuários estão tentando utilizar a autenticação SAML IDP enquanto também desejam aplicar a validação de certificado através do mecanismo de verificação de postura, mas essa configuração resulta em falhas de autenticação consistentes, mesmo quando as correspondências de certificado de back-end são bem-sucedidas.

Ambiente

- Cisco Secure Access - Acesso remoto seguro ao cliente (VPN, postura, recurso privado)
- Integração de autenticação SAML IDP
- Perfil de postura de endpoint com recurso de inspeção de certificado habilitado
- Certificados de usuário com campo UPN na SAN correspondendo a endereços de e-mail
- Configuração de locatário do Secure Access com usuários, grupos e dispositivos de endpoint

Resolução

As verificações de ponto de extremidade de certificado em postura são aplicadas somente ao

usar autenticação multicertificado, que requer validação de certificado do usuário e de certificado do computador. Como o cenário de implantação envolve usuários com apenas certificados de usuário que precisam usar um único perfil de VPN, a solução envolve implementar SAML + Autenticação de certificado único em vez de depender de verificação de certificado de postura.

Etapas de configuração da autenticação

Passo 1: Configurar SAML + Autenticação de Certificado Único

Configure o método de autenticação para usar a autenticação SAML combinada com a autenticação de certificado único, em vez de tentar impor a validação de certificado por meio de verificações de postura.

Passo 2: Configurar Correspondência UPN do Certificado

Certifique-se de que o campo UPN no SAN (nome alternativo do assunto) do certificado contenha o endereço de e-mail do usuário que corresponda à propriedade de autenticação configurada para o usuário no Secure Access em Usuários, Grupos e Dispositivos de ponto final.

Passo 3: Definir Campo de Autenticação Principal

Configure o campo primário para autenticar usando o UPN do certificado, garantindo que ele corresponda ao endereço de email do usuário no banco de dados de usuários do Secure Access.

Requisitos da estrutura do certificado

A estrutura do certificado deve ser configurada de forma que o UPN ou o valor secundário no certificado corresponda à propriedade de autenticação do usuário no Secure Access. Se um usuário apresentar um certificado que tenha um UPN ou um valor secundário que não corresponda à propriedade de autenticação configurada para esse usuário no Secure Access, a autenticação será rejeitada.

Notas importantes sobre configuração

A autenticação de vários certificados (SAML IDP + Autenticação de vários certificados) será necessária se a imposição de verificação de certificado de postura for necessária, mas isso requer certificados de usuário e de computador. Para implantações em que os usuários têm apenas certificados de usuário e precisam usar um único perfil de VPN, a autenticação SAML + Single certificate fornece a solução apropriada, mantendo ainda os controles de segurança baseados em certificado.

Causa

As verificações de ponto de extremidade de certificado em postura são aplicadas somente quando a autenticação multicertificado está configurada. Ao usar a autenticação SAML com verificação de certificado de postura, o sistema espera que os certificados do usuário e da máquina estejam presentes para validação. Como a implantação utilizou somente certificados de usuário com autenticação SAML, o recurso de inspeção de certificado de postura falhou consistentemente nas tentativas de autenticação apesar da correspondência bem-sucedida do certificado de back-end, já que o mecanismo de postura não foi projetado para funcionar com cenários de autenticação de certificado único.

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.