

Comportamento de Autenticação SSO de Acesso Seguro para Tráfego da Web Não Navegador

Contents

Problema

Durante a implementação do Cisco Secure Access (CSA) com conectividade IPsec, houve necessidade de esclarecimentos sobre o comportamento da autenticação SSO nos perfis de segurança. Especificamente, surgiu a questão sobre quais tipos de tráfego de saída da Internet acionam a autenticação SSO quando os sites são conectados por túneis IPsec.

A principal preocupação era entender se a autenticação SSO se aplica somente ao acesso à Web baseado em navegador sobre as portas TCP 80 e 443, ou se também se estende a aplicativos e dispositivos que não são navegadores, como impressoras ou endpoints não Windows que geram tráfego da Web. O comportamento precisava de esclarecimento sobre quando os prompts de autenticação e os redirecionamentos para os Provedores de Identidade (IdP) ocorreriam para diferentes tipos de tráfego da Web provenientes dos sites conectados.

Ambiente

- Implantação do Cisco Secure Access (CSA)
- Conectividade de túnel IPsec entre sites e CSA
- Perfis de Segurança configurados com Autenticação SSO
- Ambiente misto com vários dispositivos, incluindo impressoras e terminais não Windows
- Inspeção HTTPS habilitada
- Integração SAML configurada

Resolução

O comportamento de autenticação SSO no Cisco Secure Access foi projetado especificamente para direcionar apenas o tráfego da Web baseado em navegador. O sistema executa um processo de inspeção sofisticado para determinar se as solicitações da Web devem estar sujeitas à autenticação SSO.

Processo de Autenticação SSO

Antes de redirecionar uma solicitação da Web para um Identity Provider (IdP), o Cisco Secure Access usa a inspeção HTTPS para determinar se uma solicitação se origina de um navegador que suporta cookies. Esse processo de inspeção é o mecanismo principal que diferencia o tráfego da Web baseado em navegador do tráfego da Web que não é baseado em navegador.

Classificação de tráfego

Tráfego baseado em navegador (sujeito à autenticação SSO)

- Solicitações da Web originadas de navegadores que oferecem suporte a cookies
- Tráfego HTTP/HTTPS nas portas TCP 80 e 443 dos aplicativos do navegador
- Tráfego que passa pelo cookie de inspeção HTTPS/detecção de navegador

Tráfego que não é de navegador (não sujeito à autenticação SSO)

- Tráfego da Web de impressoras e outros dispositivos de rede
- Aplicativos que não oferecem suporte a cookies ou não são identificados como navegadores
- Endpoints não Windows que geram tráfego da Web que falham na detecção do navegador

- Qualquer tráfego da Web que não passe na verificação do navegador de inspeção HTTPS

Pré-requisitos para Autenticação SSO

Para que a autenticação SSO funcione corretamente no ambiente, vários pré-requisitos devem ser atendidos:

- A configuração de SAML em funcionamento deve estar em vigor.
- Redes proxy com XFF e/ou túneis sem NAT (o substituto de IP precisa de visibilidade para IPs privados internos).
- A inspeção HTTPS deve ser habilitada.
- As sessões do navegador devem manter cookies (não é recomendável excluir cookies no final da sessão ou navegar de forma anônima).
- Endereços IP não sobrepostos em locais ou separação de site apropriada se houver sobreposição.

Causa

O comportamento é por design no Cisco Secure Access. O mecanismo de autenticação SSO é projetado especificamente para direcionar sessões interativas de usuário através de navegadores da Web, permitindo que sistemas automatizados e dispositivos não interativos acessem recursos da Web sem interrupção da autenticação. Esse design impede a interrupção de processos automatizados, interfaces de gerenciamento de dispositivos e aplicativos que não podem lidar com redirecionamentos de autenticação ou sessões baseadas em cookies.

Conteúdo relacionado

- [Configurar integrações SAML - Ativar substitutos de IP para SAML](#)
- [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.