# Solucionar problema de substituição de cookie de autenticação SAML do SWG para acesso seguro

## Contents

## Problema

Os usuários que acessam aplicativos da Web por meio do Cisco Secure Access apresentam falhas de autenticação quando os aplicativos executam redirecionamentos entre domínios ou buscam recursos de vários domínios relacionados. O problema se manifesta como:

- Falha dos aplicativos Web ao inicializar corretamente após a autenticação SAML.
- As solicitações para recursos entre domínios (erro CORS) que estão sendo bloqueadas por regras de negação padrão.
- Logs de atividades que mostram solicitações atribuídas à identidade da rede ou do túnel em vez da identidade do usuário autenticado.
- Erros de política CORS que aparecem no console do navegador para solicitações redirecionadas.
- Aplicativos funcionando corretamente em máquinas físicas ao usar um substituto de IP, mas falhando em ambientes de desktop virtual Citrix usando um substituto de Cookie.

O problema ocorre especificamente quando a autenticação de substituição de cookie é usada em ambientes virtualizados, onde as solicitações redirecionadas perdem o mapeamento de usuário para cookie durante buscas de recursos entre domínios.

## Ambiente

- Cisco Secure Access com autenticação SAML configurada
- Autenticação Cookie Surrogate habilitada para ambientes de desktop virtual Citrix

- Autenticação IP substituta usada para máquinas físicas
- Aplicativos da Web que executam redirecionamentos entre domínios (erro CORS nos logs do console da ferramenta de desenvolvedor da Web)
- Ambiente misto com infraestrutura de desktop físico e virtual

## Resolução

O problema é resolvido com a implementação do desvio de IP substituto para os intervalos de rede afetados, permitindo a atribuição de identidade de usuário adequada mesmo durante redirecionamentos entre domínios.

### Passo 1: Navegue até IP Surrogate Configuration

Acesse o painel do Cisco Secure Access e navegue para Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate.

### Passo 2: Habilitar desvio de rede interna

Adicione os intervalos de rede afetados à configuração de desvio de Rede Interna. Isso permite que o sistema mantenha a atribuição de identidade de usuário para solicitações originadas dessas redes.

### Passo 3: Testar o acesso do aplicativo

Após implementar o substituto de IP, teste os aplicativos afetados para verificar se:

- As solicitações de recursos entre domínios são atribuídas corretamente à identidade do usuário
- Aplicativos inicializados com êxito sem erros de CORS

- Os logs de atividade mostram a identidade do usuário em vez da identidade baseada na rede ou no túnel para todas as solicitações

### Passo 5: Monitorar relatórios de atividades

Use Monitor > Activity Search para verificar se as solicitações agora são corretamente atribuídas aos usuários autenticados, em vez de mostrar como identidade baseada em rede ou túnel.

## Causa

Esse comportamento é esperado devido à natureza da autenticação SAML combinada com o Cookie Surrogate em ambientes virtualizados. Quando os aplicativos da Web executam redirecionamentos entre domínios ou buscam recursos de vários domínios relacionados, as solicitações redirecionadas possivelmente não carregam o cookie substituto de uma maneira que o Cisco Secure Access possa associar de volta à sessão do usuário autenticado.

A causa raiz ocorre porque:

- O Cookie Surrogate depende da propagação de cookies do navegador através de redirecionamentos.
- As CORS (Políticas de Segurança entre Domínios) podem remover cookies durante cenários de 307/redirecionamento.
- As medidas de segurança do navegador impedem o compartilhamento de cookies em diferentes domínios.
- Os ambientes de desktop virtual lidam com a propagação de cookies de forma diferente das máquinas físicas.

Quando o mapeamento de usuário para cookie é perdido, o Secure Access não pode resolver a solicitação para o usuário autenticado, fazendo com que a solicitação seja atribuída somente à rede registrada/identidade diferente como origem e, subsequentemente, bloqueada por regras de negação padrão.

## 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.