

Autenticação SSO de acesso seguro da Cisco com Duo IdP para tráfego SWG de cliente de roaming

Contents

Problema

Ao tentar usar a autenticação SSO com um Duo IdP para tráfego SWG (Secure Web Gateway) de acesso seguro originado de um cliente de roaming, os usuários não são solicitados a fazer a autenticação SSO Duo e a identidade do usuário não é preenchida no painel de controle de acesso seguro. Embora o tráfego da Web corresponda à regra SWG pretendida com a autenticação habilitada e o tráfego sejacriptografado, o fluxo de autenticação não inicia o tráfego de cliente de roaming, impedindo a identificação da atividade da Web no nível do usuário.

Especificamente, observou-se o seguinte comportamento:

- O registro e a atividade do SWG mostraram que o tráfego correspondia à regra SWG pretendida e que o tráfego de destino eracriptografado
- Os registros e a visualização da atividade de acesso seguro mostraram apenas a identidade do PC e a identidade da rede; nenhum desafio de autenticação Duo/SAML, redirecionamento de SSO ou prompt interativo foi observado
- As entradas de política mostravam apenas informações de roaming e origem; nenhuma identidade de usuário estava presente antes de ingressar no AD
- Quando a VM de teste ingressou no Active Directory durante a solução de problemas, a identidade do usuário se tornou visível na Pesquisa de atividade de acesso seguro, mas o prompt interativo Duo/SAML ainda não ocorreu

Ambiente

- Cisco Secure Access com funcionalidade SWG
- Secure Client versão 5.1.13.177
- IdP Duo configurado para autenticação SSO

- Assinatura da organização: Secure Access Essentials
- Autenticar novamente o intervalo do proxy da Web definido como Diário
- Nenhum arquivo PAC ou VPN em uso durante os testes
- Testar o ambiente usando a configuração do computador em roaming

Resolução

Após uma análise e um teste abrangentes, foi determinado que a autenticação SSO usando SAML não é suportada para tráfego de cliente de roaming de Acesso Seguro devido às limitações do projeto do produto. As seguintes etapas de solução de problemas foram executadas para confirmar essa limitação:

Passo 1: Solução de problemas ao vivo e reprodução de comportamento

O teste confirmou que a correspondência da política SWG e a descryptografia SSL ocorreram corretamente, mas o fluxo de autenticação (redirecionamento e desafio SSO SAML/Duo interativo) não foi iniciado para tráfego de cliente móvel.

Passo 2: Modificações de regra e origem

A origem da regra SWG foi alterada de nome de computador móvel para uma identidade de usuário específica durante tentativas de reparo. Os serviços de Cliente Seguro foram reiniciados e a propagação da política foi observada. Essas modificações não resolveram o problema do fluxo de autenticação.

Passo 3: Teste de Ingresso no Ative Directory

A VM de teste ingressou no Ative Directory para determinar o efeito na visibilidade da identidade do usuário. Embora isso tenha tornado a identidade do usuário visível no Secure Access Activity Search, o prompt interativo Duo/SAML ainda não ocorreu, confirmando que o problema não estava relacionado apenas à visibilidade da identidade do usuário.

Passo 4: Análise do pacote DART

Um pacote DART foi coletado e analisado. A análise confirmou a aplicação da política SWG, mas não mostrou a iniciação do fluxo de autenticação para tráfego de cliente de roaming, suportando a conclusão de que esse comportamento é por design.

Passo 5: Validação de configuração IdP Duo

Testes independentes dos metadados e da configuração do Duo IdP foram realizados e concluídos com êxito, confirmando que a configuração do Duo em si não era a origem do problema.

Passo 6: Validação interna

A autenticação SSO usando SAML não é suportada para tráfego de cliente de roaming de Acesso Seguro como uma limitação de design de produto.

Conclusão: Nenhum erro de configuração foi encontrado na instalação. A falta de prompting SSO interativo foi atribuída a uma limitação explícita de suporte ao produto em vez de um problema de configuração corrigível.

Causa

O problema é causado por uma limitação de design de produto em que a autenticação SSO usando SAML (incluindo integração IdP Duo) não é suportada para tráfego de cliente de roaming de Acesso Seguro. Essa é uma limitação inerente da arquitetura atual da plataforma Secure Access e não está relacionada a problemas de configuração ou bugs de software.

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.