

Desafios de identificação por usuário e aplicação de políticas no Secure Web Gateway (SWG) para ambientes de computador compartilhado com autenticação SAML e encaminhamento de tráfego baseado em PAC

Contents

Problema

Em implantações do Cisco Secure Web Gateway (SWG) que utilizam o Acesso Seguro com autenticação SAML e encaminhamento de tráfego baseado em PAC ou de Ramificação para Internet, apenas o primeiro usuário conectado a um computador compartilhado é identificado corretamente para o tráfego da Web e a aplicação de política. Ao comutar usuários, o tráfego da Web subsequente continua a ser atribuído ao usuário inicial, mesmo quando a opção IP Surrogate está desabilitada e um arquivo PAC é usado. As consultas DNS refletem o usuário ativo correto através do Umbrella Virtual Appliance, mas os logs da Web e de firewall mapeiam a atividade persistentemente para o usuário anterior. A solicitação é determinar se o SWG suporta a identificação por usuário e a aplicação de política em ambientes de computador compartilhado e como garantir mapeamento de usuário correto.

Ambiente

- Virtual Appliance para resolução de DNS.
- Autenticação SAML para identidade do usuário.
- Mistura de encaminhamento de tráfego com PAC e sem arquivos PAC.
- Opção de substituto de IP ativada, com sub-redes específicas e hosts ignorados para substituto de cookie.
- Dispositivos no local; sem endpoints remotos ou usuários.

Resolução

O problema foi resolvido com a instrução do usuário e a orientação para a configuração com estes pontos em mente:

- Use a identificação Cookie Surrogate com arquivos PAC. O tráfego pode rotear para dentro ou para fora de um túnel de rede.
- Use a identificação Cookie Surrogate sem arquivos PAC, mas o tráfego tem que ser roteado

através de um túnel de rede.

- A política de acesso que você deseja aplicar substituto de cookie deve ter a autenticação SAML habilitada no perfil de segurança.
- O tráfego substituto do cookie é somente para tráfego baseado em navegador. Uma regra separada é necessária para identificar o tráfego que não seja de cookie da máquina (por exemplo, o tráfego de Equipes ou Webex) com a identidade de origem como a rede.
- O módulo SWG não deve estar em uso para que o substituto de cookie funcione.
- Quando o substituto de IP também estiver habilitado, você deverá adicionar os endereços IP/sub-redes privados que pretendem usar um substituto de cookie na lista de desvio (Usuários e Grupos - Gerenciamento de Configuração - Configurações Avançadas).
- A lista de desvio para substituto de cookie também corresponde a prefixos mais curtos. Por exemplo, se você adicionar 10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- O substituto de cookie suporta a troca de usuário de uma máquina sem ter que fazer logout para reter várias identidades.

Grande parte da solução de problemas tem sido o teste de políticas e a pesquisa de atividades.

Causa

A causa principal da identificação incorreta do usuário em ambientes de computadores compartilhados é principalmente a educação do usuário.

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.