Desafios de configuração da separação de túneis de acesso seguro

Contents

Problema

Ao configurar o recurso Cisco Secure Access (TIA) para tráfego de túnel dividido, várias complicações foram encontradas durante o processo de configuração que impediram a implantação adequada:

- Desafios de identificação de tráfego: Ao configurar o TIA para tunelamento dividido, todo o tráfego VPN precisa ser excluído da inspeção de segurança da Internet. Identificar os fluxos de tráfego necessários mostrou-se difícil, e alguns URLs de redirecionamento foram particularmente difíceis de rastrear e categorizar.
- Restrições de tráfego de autenticação: Determinados cenários de túnel dividido exigiam que o tráfego de autenticação fosse excluído do proxy. No entanto, com base nas políticas existentes, o tráfego relacionado à autenticação não poderia ser ignorado do proxy, levando a conflitos de política.
- Riscos de segurança na desconexão da VPN: O tráfego de túnel dividido fica exposto à Internet aberta quando a VPN se desconecta, resultando em riscos de segurança adicionais que precisavam ser considerados durante a configuração.

Outros problemas de configuração também foram observados durante o processo, o que exigiu análise e resolução adicionais.

Ambiente

- Linha de produtos: SECACCS (acesso seguro)
- Tecnologia: Cisco Secure Access (TIA) com recurso de separação de túneis
- Configuração: Cenários de tráfego de túnel dividido com políticas existentes

- Autenticação: Tratamento de tráfego de autenticação baseado em proxy
- Segurança de rede: Requisitos de inspeção de segurança da Internet para tráfego VPN

Resolução

Com base nos desafios de configuração identificados com o split-tunneling do Cisco Secure Access, uma solicitação de recurso abrangente foi enviada para resolver as limitações identificadas e os conflitos de política.

Envio de solicitação de recurso

Uma solicitação de recurso (CSE-I-5636) foi aberta e enviada para análise pela equipe de engenharia relevante para lidar com estes desafios de configuração:

- Recursos avançados de identificação de tráfego para exclusão de tráfego VPN da inspeção de segurança da Internet
- Melhor tratamento de URLs de redirecionamento que são difíceis de rastrear e categorizar
- Resolução de limitações de desvio de tráfego de autenticação com políticas existentes
- Redução do risco de segurança para exposição do tráfego de túnel dividido durante a desconexão da VPN

Causa

Os desafios de configuração se originam das limitações atuais na implementação do split-tunneling do Cisco Secure Access (TIA) que não abordam adequadamente cenários de implantação empresarial complexos. Especificamente, o sistema não tem controle granular suficiente para identificação e categorização de tráfego, tem restrições para ignorar o tráfego de autenticação quando as políticas estão em vigor e não fornece proteções de segurança adequadas para o tráfego de túnel dividido quando as conexões VPN são interrompidas.

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.