Problemas de visibilidade de identidade de cliente segura com o túnel de rede MX75 no acesso seguro

Contents

Problema

Quando os endpoints com o Secure Client são implantados por trás de um túnel de rede MX75 que se conecta ao Secure Access, as identidades de cliente e usuário móveis não são visíveis corretamente no sistema. Os seguintes comportamentos específicos são observados:

- As configurações de recuo configuradas para priorizar o Secure Client em conexões de túnel de rede não funcionam como esperado quando os pontos de extremidade estão atrás do MX75
- As regras de orientação de tráfego baseadas em domínios não se aplicam porque o tráfego é atribuído apenas à identidade do túnel de rede, em vez do cliente de roaming
- A pesquisa de atividades exibe informações incompletas sobre o local de origem, mostrando apenas a identidade do túnel de rede, ao mesmo tempo em que omite as identidades de usuário e cliente móvel
- As regras de direcionamento de tráfego com base em identidade (como aquelas baseadas em usuários do Ative Diretory ou identidade de cliente de roaming) não se aplicam ao tráfego que atravessa o túnel MX75

Esse comportamento impede a segregação de identidade e a aplicação de políticas adequadas para terminais que se conectam através da infraestrutura de túnel de rede.

Ambiente

- Implantação do Cisco Secure Access
- Dispositivo MX75 com configuração de túnel de rede para acesso seguro
- Agentes do Secure Client instalados em todos os endpoints
- Configurações de recuo desabilitadas em clientes móveis para priorizar o Cliente Seguro em

conexões de túnel de rede
- Regras de direcionamento de tráfego configuradas para roteamento baseado em domínio
- Políticas baseadas em identidade configuradas para usuários do Ative Diretory e clientes móveis

Resolução

O problema foi resolvido com a implementação de uma configuração alternativa usando uma abordagem de rede registrada, em vez de depender da visibilidade de identidade de roaming através do túnel de rede MX75.

Implementação alternativa

Passo 1: Configurar o RSM (Roaming Security Module, Módulo de segurança de roaming) com a rede registrada

Substitua a configuração de túnel de rede existente por uma implantação de RSM combinada com uma configuração de rede registrada. Essa configuração permite a atribuição de identidade e a aplicação de políticas adequadas.

Passo 2: Validar Visibilidade da Identidade

Após implementar a configuração da Rede Registrada, verifique se:

- As identidades dos usuários são exibidas corretamente na Pesquisa de atividades
- As identidades de clientes móveis estão visíveis e atribuídas corretamente
- Regras de orientação de tráfego baseadas na função de identidade do usuário e do cliente conforme esperado

Passo 3: Testar a funcionalidade de direcionamento de tráfego

Confirme se as regras de direcionamento de tráfego baseadas em domínio e as políticas baseadas em identidade se aplicam corretamente à nova configuração.

Abordagem alternativa

Para ambientes onde a segregação de identidade em redes privadas não é necessária, considere implementar a configuração de RSM - Internet. Essa abordagem envia o tráfego RSM diretamente para a Internet, e não através do túnel de rede privada, que pode fornecer visibilidade de identidade adequada, mantendo os controles de segurança.

Análise técnica

Durante a solução de problemas, a saída de diagnóstico foi coletada usando policy.test.sse.cisco.com para demonstrar o comportamento de atribuição de identidade quando os pontos finais estavam por trás do túnel MX75. A análise confirmou que, embora o roteamento de identidades de roaming por meio de um túnel de rede seja tecnicamente possível, não é um fluxo operacional recomendado ou suportado para esse cenário de implantação específico.

Causa

A causa raiz está relacionada ao modo como o Secure Access lida com a atribuição de identidade quando o tráfego atravessa a infraestrutura de túnel de rede. Quando os endpoints se conectam através do túnel de rede MX75, o sistema atribui todo o tráfego à identidade do túnel, em vez de preservar as identidades individuais do cliente e do usuário de roaming. Esse comportamento é projetado para conexões de túnel de rede, mas conflita com o requisito de visibilidade de identidade individual e aplicação de política.

Embora seja tecnicamente viável rotear identidades de roaming através de túneis de rede, essa configuração não é recomendada ou suportada como um fluxo operacional padrão devido às limitações de atribuição de identidade descritas acima.

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.