Pop-up de Autenticação de Túnel de Máquina de Cliente Seguro Causa Desconexões em Redes Não Confiáveis

Contents

Problema

O Cisco Secure Client (AnyConnect) solicita repetidamente o nome de usuário e a senha enquanto um túnel de máquina está conectado, particularmente quando os usuários se conectam de redes não confiáveis. A janela pop-up de autenticação interrompe a conectividade do túnel da máquina e causa desconexões, afetando a capacidade dos usuários de manter o acesso remoto estável. Esse problema ocorre apesar de o túnel da máquina estar corretamente estabelecido e autenticado, com o pop-up aparecendo inesperadamente e interrompendo a continuidade da sessão VPN.

Ambiente

- Cisco Secure Client (AnyConnect) com configuração de túnel de máquina
- Perfil de VPN de Acesso Remoto com o recurso Detecção de Rede Confiável (TND) habilitado
- Máquina do usuário conectada ao Túnel da Máquina
- Objetos de Diretiva de Grupo (GPO) usados para a distribuição do perfil do cliente
- Perfis de túnel de usuário e de túnel de máquina configurados com configurações TND

Resolução

O problema foi resolvido com a modificação das definições de configuração do Trust Network

Detection (TND) para perfis de túnel de máquina e de túnel de usuário. A solução envolve a configuração do comportamento da ação TND para evitar prompts de autenticação desnecessários em redes não confiáveis.

Passo 1: Definir Configurações TND para Redes Não Confiáveis

Defina a ação Detecção de rede confiável como Não fazer nada para redes não confiáveis nos perfis de túnel de máquina e de túnel de usuário. Essa configuração impede que o cliente solicite credenciais adicionais quando conectado a redes não confiáveis.

Passo 2: Definir Configurações TND para Redes Confiáveis

Defina a ação de Detecção de Rede Confiável como Desconectar para redes confiáveis, mantendo o comportamento de segurança pretendido para ambientes de rede seguros conhecidos.

Passo 3: Implantar Alterações de Configuração

Implante as configurações TND atualizadas por meio do push GPO (Objeto de Política de Grupo) para distribuir as alterações de configuração em todas as máquinas clientes afetadas.

Passo 4: Reiniciar Máquinas Cliente

Reinicialize as máquinas cliente após a atualização do perfil para garantir que as novas configurações TND entrem em vigor corretamente.

Passo 5: Teste de validação

Teste a conectividade do túnel da máquina em várias redes não confiáveis para verificar se:

- A janela pop-up de autenticação não é mais exibida
- O túnel da máquina permanece conectado consistentemente
- Nenhum prompt de credencial interrompe a sessão VPN
- Os usuários podem manter o acesso remoto estável sem desconexões

O usuário confirmou a resolução bem-sucedida após implementar essas alterações, com vários testes de usuário validando a continuidade estável da sessão VPN em várias condições de rede.

Causa

A causa raiz foi a configuração incorreta da Detecção de Rede Confiável (TND) nos perfis do Cisco Secure Client. O recurso TND estava disparando avisos de autenticação quando os usuários se conectavam de redes não confiáveis, mesmo que o túnel da máquina já estivesse autenticado e estabelecido corretamente. As ações TND para perfis de túnel de usuário e de túnel de máquina não foram configuradas de forma ideal para o ambiente de rede, fazendo com que o cliente solicite credenciais adicionais desnecessariamente e interrompendo a conectividade do túnel de máquina.

Conteúdo relacionado

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.