Considerações sobre o comportamento de conexão VPN manual do Secure Client TND e bloqueio de URL

Contents

Problema

Ao usar um perfil de VPN com o recurso Trusted Network Detection (TND) configurado com a configuração Trusted Network definida como Disconnect, os endpoints localizados dentro da Trusted Network ainda poderão estabelecer com êxito uma conexão de VPN quando os usuários iniciarem manualmente conexões usando o Cisco Secure Client.

Esse comportamento ocorre apesar da configuração TND estar definida para desconectar sessões VPN quando o ponto final é detectado em uma rede confiável.

As preocupações específicas identificadas incluem:

- As conexões VPN manuais de pontos de extremidade de Rede Confiável não podem ser controladas ou bloqueadas por meio da configuração TND padrão
- Incerteza sobre se as configurações do Cisco Secure Access (CSA) podem bloquear conexões VPN manuais de endpoints de rede confiável
- Dúvidas sobre a estabilidade da URL de conexão do perfil VPN (xxxx.vpn.sse.cisco.com) e se ela muda periodicamente, o que pode afetar as estratégias de bloqueio baseadas em firewall

Ambiente

- Implantação do Cisco Secure Access (CSA)
- Cisco Secure Client com configuração de perfil VPN

- Recurso de Detecção de Rede Confiável (TND) habilitado
- Configuração de Rede Confiável TND configurada como Desconectar
- Endpoints localizados dentro da rede confiável configurada
- Infraestrutura de firewall para controle de acesso à rede

Resolução

Entender o comportamento do TND com conexões VPN manuais

O comportamento observado é consistente com a funcionalidade documentada do Cisco Secure Client. De acordo com a documentação da Cisco, o TND não desconecta nem impede uma sessão VPN iniciada manualmente por um usuário em uma rede confiável. Esse é o comportamento esperado, independentemente das configurações de TND.

Os principais fatos técnicos são:

- A funcionalidade de desconexão automática de TND aplica-se somente a conexões VPN estabelecidas automaticamente.
- As conexões VPN manuais iniciadas pelos usuários ignoram o comportamento de desconexão TND.
- Não existe nenhuma definição de configuração de CSA para bloquear conexões VPN manuais de pontos de extremidade de Rede Confiável.

Estratégia de mitigação operacional

O principal método para controlar conexões VPN manuais de endpoints de rede confiável é através de controles em nível de rede:

Passo 1: Implemente o bloqueio de URLs do firewall: Configure o firewall da Rede Confiável para bloquear o acesso à URL de conexão do perfil VPN (xxxx.vpn.sse.cisco.com). Isso impede que os pontos de extremidade na Rede Confiável acessem o ponto de extremidade do serviço VPN.

Passo 2: Verifique a estabilidade da URL: O identificador da URL do perfil de VPN (a parte xxxx) é específica do locatário e não deve ser alterado periodicamente. Isso fornece um destino estável para regras de bloqueio de firewall.

Validação e teste

Os testes confirmaram que o bloqueio da URL de conexão do perfil VPN no firewall de Rede Confiável impede com êxito que os endpoints estabeleçam conexões VPN, mesmo quando os usuários tentam conexões manuais através do Cisco Secure Client.

Causa

Esse comportamento ocorre por projeto na implementação da TND do Cisco Secure Client. O recurso TND foi projetado especificamente para gerenciar conexões VPN automáticas com base no status de confiança da rede, mas intencionalmente não interfere em conexões VPN manuais iniciadas pelo usuário. Esse design permite que os usuários substituam o comportamento automático quando necessário, fornecendo detecção de rede automatizada e gerenciamento de conexão para casos de uso típicos.

Conteúdo relacionado

- Guia do administrador do Cisco Secure Client - Configuração TND
- 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.