Comportamento do protocolo Cisco Secure Access RAVPN com configuração dupla TLS/DTLS e IPsec(IKEv2)

Contents

Problema

Quando os protocolos TLS/DTLS e IPsec(IKEv2) estão habilitados no Cisco Secure Access RAVPN com o protocolo primário definido como IPsec(IKEv2), ocorrem falhas de conexão durante a tentativa de estabelecer conectividade VPN de redes onde o tráfego IPsec (portas UDP 500/4500) é bloqueado. O Cliente Seguro assume como padrão a opção IPsec no menu suspenso de interface do usuário do cliente e não executa automaticamente failover para TLS/DTLS quando a conectividade IPsec falha, resultando em erros de conexão e incapacidade de estabelecer conectividade de RAVPN a partir de ambientes de rede restritos.

Ambiente

- Cisco Secure Access RAVPN com configuração de protocolo duplo
- Os protocolos TLS/DTLS e IPsec(IKEv2) estão habilitados
- Configuração de protocolo primário configurada como IPsec(IKEv2)
- Cliente seguro com menu suspenso de seleção de protocolo contendo opções separadas de IPsec e TLS
- Ambiente de rede que bloqueia o tráfego IPsec nas portas UDP 500 e 4500

Resolução

O comportamento observado é esperado e por projeto. O Cisco Secure Access RAVPN não executa failover automático de protocolo de IPsec(IKEv2) para TLS/DTLS quando ambos os protocolos estão habilitados e o protocolo primário encontra problemas de conectividade.

Seleção Manual de Protocolo Necessária

Ao conectar-se de redes que bloqueiam o tráfego IPsec, os usuários devem selecionar manualmente o protocolo apropriado no Secure Client:

Passo 1: Abra o aplicativo Secure Client

Passo 2: Localize o menu suspenso de seleção de protocolo na interface do cliente

Passo 3: Alterar manualmente a seleção da opção IPsec para a opção TLS

Passo 4: Inicie a conexão VPN usando o protocolo TLS/DTLS

Clarificação do comportamento do protocolo

A configuração do protocolo Primário no Cisco Secure Access RAVPN determina o protocolo padrão apresentado no Cliente Seguro, mas não ativa a funcionalidade de failover automático. Quando TLS/DTLS e IPsec(IKEv2) estão habilitados:

- O Secure Client exibe opções de protocolo separadas no menu suspenso
- O padrão do cliente é a configuração do protocolo primário (IPsec nesse caso)
- Não ocorre comutação automática entre protocolos com base nas condições de conectividade da rede
- Os usuários devem selecionar manualmente o protocolo apropriado com base em seu ambiente de rede

Causa

O Cisco Secure Access RAVPN foi projetado sem a funcionalidade de failover automático de protocolo. Quando os protocolos TLS/DTLS e IPsec(IKEv2) estão habilitados, o sistema requer a seleção manual do protocolo através da interface do cliente seguro. A configuração de protocolo primário determina apenas a seleção padrão no menu suspenso do cliente e não implementa a lógica de comutação automática quando problemas de conectividade são encontrados com o protocolo primário.

Conteúdo relacionado

- Documentação do Cisco Secure Access
- 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.