

Túnel VTI para acesso seguro com problemas de negociação IKEv2 no CAT8500

Contents

Problema

Um túnel VTI (Virtual Tunnel Interface) configurado para Secure Access em um roteador CAT8500 mostra IPsec SA como estabelecido ao verificar com `show crypto ipsec sa`, mas o IKEv2 SA permanece no estado de negociação quando visualizado com `show crypto ikev2 sa`. O protocolo de linha da interface do túnel está inoperante e o lado do acesso seguro mostra a conexão como desconectada, impedindo que o túnel se estabeleça corretamente.

Ambiente

- Linha de produtos: CAT8500
- Versão de software: 17.15.4c
- Tecnologia: Túneis de rede de acesso seguro (IPsec, site a site)
- Tipo de túnel: VTI (Virtual Tunnel Interface, interface de túnel virtual)
- Versão do IKE: IKEv2

Resolução

De acordo com nossos parâmetros de IPSec suportados,

Os valores recomendados são 19,20 para o grupo DH.

crypto ikev2 proposal csse-G256

encryption aes-gcm-256

prf sha256

[illegible]

Toque de Tecla -

crypto ikev2 keyring csse_useast

peer csse_virginia1

address x.x.x.x <<<<<<<<<<< Acesso seguro DC

pre-shared-key local <removed>

pre-shared-key remote <removed>

!

Perfil - identidade local de correspondência ausente, que seria tunnelID da interface do usuário do CSA quando criamos um grupo de túneis de rede.

crypto ikev2 profile csse_virginia1

match identity remote address x.x.x.x 255.255.255.255

pré-compartilhamento remoto de autenticação

pré-compartilhamento local de autenticação

keyring local csse_useast

!

Depois de alterar o grupo DH, o problema de identidade local de correspondência adicionado é corrigido.

Causa

A principal causa desse problema é geralmente a configuração de identidade local incorreta ou ausente no perfil IKEv2. O acesso seguro requer parâmetros de identidade específicos para estabelecer corretamente a negociação IKEv2. Além disso, o uso de grupos Diffie-Hellman não suportados (grupos diferentes de 19 e 20) pode impedir a negociação IKEv2 bem-sucedida com o Secure Access.

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.