A autenticação de túnel IPSec falha entre o acesso seguro e o firewall FortiGate

Problema

O estabelecimento de túnel IPSec está falhando entre o Cisco Secure Access e um firewall FortiGate com erros de autenticação. Os registros de depuração do firewall FortiGate mostram mensagens de "falha de autenticação", apesar da verificação de que as chaves pré-compartilhadas (PSKs) correspondem em ambos os lados. A negociação da Fase 1 está falhando com um erro INVALID_KE_PAYLOAD, impedindo que o túnel seja ativado. As propostas para a conexão parecem corresponder entre os dois pontos finais, mas o processo de estabelecimento do túnel não está sendo concluído com êxito.

Ambiente

- Acesso seguro da Cisco
- Firewall FortiGate (gerenciado por terceiros)
- Configuração de túnel IPSec com endpoints redundantes primários e de backup

Resolução

O problema de conectividade de túnel IPSec foi resolvido com ajustes específicos de configuração para resolver os problemas de erro e autenticação de INVALID_KE_PAYLOAD.

Configuração do grupo DH da fase 1

Configure apenas um grupo DH (Diffie-Hellman) para a negociação da Fase 1. Defina o grupo DH 20 na Fase 1 em vez de usar vários grupos DH ou o grupo DH 14 configurado anteriormente.

Correção de configuração

```
config vpn ipsec phase1-interface
    edit "sse-tunnel"
        set dhgrp 20
    next
end
```

Configuração transversal de NAT

Ative o NAT Traversal (NAT-T) na configuração do túnel IPSec. Isso foi desabilitado anteriormente, mas precisa ser habilitado para o estabelecimento de túnel apropriado.

Configuração de segredo de encaminhamento perfeito

Desative o Perfect Forward Secrecy (PFS) na configuração da Fase 2 para eliminar possíveis conflitos de negociação.

Causa

A falha de túnel IPSec foi causada por várias incompatibilidades e incompatibilidades de configuração:

- Erro INVALID_KE_PAYLOAD: Este erro de Fase 1 ocorreu devido a conflitos de negociação de grupo Diffie-Hellman entre os pontos finais do Cisco Secure Access e do FortiGate
- Incompatibilidade do Grupo DH: Vários grupos DH configurados e o uso do grupo DH 14 na configuração original não era compatível com os requisitos do Cisco Secure Access
- Configurações de passagem NAT: O NAT Traversal foi desabilitado, o que impediu o estabelecimento de túnel apropriado no ambiente de rede

Conteúdo relacionado

- Configure o acesso seguro com o firewall FortiGate
- 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.