Échec de l'authentification du tunnel IPSec entre Secure Access et FortiGate Firewall

Problème

L'établissement du tunnel IPSec échoue entre Cisco Secure Access et un pare-feu FortiGate avec des erreurs d'authentification. Les journaux de débogage du pare-feu FortiGate affichent les messages « authentication failed », malgré la vérification de la correspondance des clés prépartagées (PSK) des deux côtés. La négociation de phase 1 échoue avec une erreur INVALID_KE_PAYLOAD, empêchant le tunnel de s'activer. Les propositions pour la connexion semblent correspondre entre les deux points d'extrémité, mais le processus d'établissement du tunnel ne se termine pas correctement.

Environnement

- Accès sécurisé Cisco
- Pare-feu FortiGate (géré par un tiers)
- Configuration de tunnel IPSec avec terminaux principaux et de secours redondants

Résolution

Le problème de connectivité du tunnel IPSec a été résolu en effectuant des ajustements de configuration spécifiques pour résoudre les problèmes d'authentification et d'erreur INVALID_KE_PAYLOAD.

Phase 1 Configuration du groupe DH

Configurez un seul groupe Diffie-Hellman (DH) pour la négociation de phase 1. Définissez le groupe DH 20 sur Phase 1 au lieu d'utiliser plusieurs groupes DH ou le groupe DH 14

précédemment configuré.

Correctif de configuration

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

Configuration de traversée NAT

Activez NAT Traversal (NAT-T) sur la configuration du tunnel IPSec. Cette option était précédemment désactivée, mais doit être activée pour permettre l'établissement correct du tunnel.

Configuration parfaite de Forward Secrecy

Désactivez le protocole PFS (Perfect Forward Secrecy) dans la configuration de phase 2 pour éliminer les conflits de négociation potentiels.

Motif

La défaillance du tunnel IPSec a été causée par plusieurs incompatibilités et incohérences de configuration :

- Erreur INVALID_KE_PAYLOAD : Cette erreur de phase 1 s'est produite en raison de conflits de négociation de groupe Diffie-Hellman entre les terminaux Cisco Secure Access et FortiGate
- Incompatibilité de groupe DH : Plusieurs groupes DH configurés et l'utilisation du groupe DH 14 dans la configuration d'origine n'était pas compatible avec les exigences d'accès sécurisé Cisco
- Paramètres de traversée NAT : La traversée NAT a été désactivée, ce qui a empêché l'établissement correct du tunnel dans l'environnement réseau

Autres informations utiles

- Configurer un accès sécurisé avec le pare-feu FortiGate
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.