IPSec-tunnelverificatie mislukt tussen beveiligde toegang en FortiGate-firewall

uitgeven

IPSec-tunnelinstallatie faalt tussen Cisco Secure Access en een FortiGate-firewall met verificatiefouten. De foutopsporingslogboeken van FortiGate firewall tonen "authenticatie mislukt" berichten, ondanks verificatie dat de Pre-Shared Keys (PSK's) aan beide zijden overeenkomen. De fase 1-onderhandeling faalt met een INVALID_KE_PAYLOAD-fout, waardoor de tunnel niet naar boven komt. De voorstellen voor de verbinding lijken overeen te komen tussen beide eindpunten, maar het tunneloprichtingsproces wordt niet met succes afgerond.

milieu

- Cisco Secure Access
- FortiGate-firewall (beheerd door derden)
- IPSec-tunnelconfiguratie met redundante primaire en back-upeindpunten

resolutie

Het probleem met de IPSec-tunnelconnectiviteit werd opgelost door specifieke configuratieaanpassingen aan te brengen om de INVALID_KE_PAYLOAD-fout en authenticatieproblemen aan te pakken.

Fase 1 DH-groepsconfiguratie

Configureer slechts één Diffie-Hellman-groep (DH) voor fase 1-onderhandelingen. Stel DH-groep 20 in op fase 1 in plaats van meerdere DH-groepen of de eerder geconfigureerde DH-groep 14 te gebruiken.

Configuratiefix

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

NAT-transversale configuratie

NAT Traversal (NAT-T) inschakelen in de IPSec-tunnelconfiguratie. Dit was eerder uitgeschakeld, maar moet worden ingeschakeld voor de juiste tunnelinstelling.

Perfect Forward Secrecy Configuration

Schakel Perfect Forward Secrecy (PFS) uit in de fase 2-configuratie om potentiële onderhandelingsconflicten te elimineren.

Oorzaak

De IPSec-tunnelfout werd veroorzaakt door meerdere configuratiefouten en incompatibiliteiten:

- ONGELDIG_KE_PAYLOAD Fout: Deze Fase 1-fout is opgetreden als gevolg van Diffie-Hellman-groepsonderhandelingsconflicten tussen de Cisco Secure Access- en FortiGate-eindpunten
- DH Group Mismatch: Meerdere DH-groepen geconfigureerd en het gebruik van DH-groep 14 in de oorspronkelijke configuratie was niet compatibel met de Cisco Secure Access-vereisten
- NAT Traversal-instellingen: NAT Traversal is uitgeschakeld, waardoor de juiste tunnelinstelling in de netwerkomgeving is voorkomen

Verwante inhoud

- Beveiligde toegang configureren met FortiGate Firewall
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.