

VTI-tunnel voor veilige toegang met IKEv2-onderhandelingsproblemen op CAT8500

Inhoud

uitgeven

Een VTI-tunnel (Virtual Tunnel Interface) die is geconfigureerd voor Secure Access op een CAT8500-router, toont IPsec SA zoals vastgesteld bij het controleren met `show crypto ipsec sa`, maar de IKEv2 SA blijft in onderhandelingsstoestand wanneer deze wordt bekeken met `show crypto ikev2 sa`. Het lijnprotocol van de tunnelinterface is uitgeschakeld en aan de kant van de beveiligde toegang wordt de verbinding als losgekoppeld weergegeven, waardoor de tunnel niet goed tot stand kan worden gebracht.

milieu

- Productfamilie: CAT8500
- Softwareversie: 17.15.4c
- Technologie: Netwerktunnels voor beveiligde toegang (IPsec, site-to-site)
- Type tunnel: VTI (Virtual Tunnel Interface)
- IKE-versie: IKEv2

resolutie

Volgens onze ondersteunde ipsec-parameters -

Aanbevolen waarden zijn 19,20 voor de DH-groep.

crypto ikev2 voorstel csse-G256

Codering AES-GCM-256

PRF SHA256

groep 19.21. <<<<<<<<<<<<<<<<<<<<<<<<< Hiervoor is een verandering naar
19.20 nodig

Sleutelhanger -

Crypto IKEV2 sleutelhanger csse_useast

peer csse_virginia1

adres x.x.x.x <<<<<<<<<<<<<<< Veilige toegang DC

Vooraf gedeelde lokale sleutel <verwijderd>

Remote met gedeelde sleutel <verwijderd>

Ja!

Profiel - ontbrekende match-identiteit lokaal die tunnelID van CSA UI zou zijn wanneer we een netwerktunnelgroep maken.

Crypto IKEV2 profiel csse_virginia1

Overeenkomen Identificatie Extern adres x.x.x.x 255.255.255.255

Verificatie op afstand vooraf delen

Verificatie lokaal voordelen

keyring local csse_useast

Ja!

Zodra u de DH-groep hebt gewijzigd, is het toegevoegde probleem met de lokale identiteit van de match opgelost.

Oorzaak

De primaire oorzaak van dit probleem is meestal ontbrekende of onjuiste lokale identiteitsconfiguratie in het IKEv2-profiel. Secure Access vereist specifieke identiteitsparameters om de IKEv2-onderhandeling goed vast te stellen. Bovendien kan het gebruik van niet-ondersteunde Diffie-Hellman-groepen (andere groepen dan 19 en 20) succesvolle IKEv2-onderhandeling met Secure Access voorkomen.

Verwante inhoud

- [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.