Cisco Secure Access RAVPN-protocolgedrag met TLS/DTLS en dubbele configuratie van IPsec(IKEv2)

Inhoud

uitgeven

Wanneer zowel TLS/DTLS- als IPsec(IKEv2)-protocollen zijn ingeschakeld in Cisco Secure Access RAVPN met het primaire protocol ingesteld op IPsec(IKEv2), treden verbindingsfouten op bij pogingen om VPN-connectiviteit tot stand te brengen vanaf netwerken waar IPsec-verkeer (UDP-poorten 500/4500) is geblokkeerd. De Secure Client maakt standaard gebruik van de IPsec-optie in de keuzelijst Client UI en zorgt niet automatisch voor failover naar TLS/DTLS wanneer de IPsec-connectiviteit mislukt, wat leidt tot verbindingsfouten en het niet kunnen vaststellen van RAVPN-connectiviteit vanuit beperkte netwerkomgevingen.

milieu

- Cisco Secure Access RAVPN met dubbele protocolconfiguratie
- TLS/DTLS- en IPsec(IKEv2)-protocollen beide ingeschakeld
- Primaire protocolinstelling geconfigureerd als IPsec(IKEv2)
- Beveiligde client met keuzelijst voor protocolselectie met afzonderlijke IPsec- en TLS-opties
- Netwerkomgeving blokkeert IPsec-verkeer op UDP-poorten 500 en 4500

resolutie

Het waargenomen gedrag wordt verwacht en door ontwerp. Cisco Secure Access RAVPN voert geen automatische protocolfailover uit van IPsec (IKEv2) naar TLS/DTLS wanneer beide protocollen zijn ingeschakeld en het primaire protocol verbindingsproblemen ondervindt.

Handmatige protocolselectie vereist

Wanneer gebruikers verbinding maken met netwerken die IPsec-verkeer blokkeren, moeten ze handmatig het juiste protocol selecteren in de beveiligde client:

Stap 1: Open de Secure Client-toepassing

Stap 2: Zoek het vervolgkeuzemenu Protocolselectie in de clientinterface

Stap 3: Wijzig handmatig de selectie van de IPsec-optie in de TLS-optie

Stap 4: Start de VPN-verbinding met behulp van het TLS/DTLS-protocol

Verduidelijking van protocolgedrag

De instelling Primair protocol in Cisco Secure Access RAVPN bepaalt het standaardprotocol dat wordt weergegeven in de Secure Client, maar maakt automatische failover-functionaliteit niet mogelijk. Wanneer zowel TLS/DTLS als IPsec(IKEv2) zijn ingeschakeld:

- De Secure Client geeft afzonderlijke protocolopties weer in het vervolgkeuzemenu
- De client is standaard ingesteld op de primaire protocolinstelling (in dit geval IPsec)
- Er vindt geen automatische schakeling plaats tussen protocollen op basis van netwerkconnectiviteitsvoorwaarden
- Gebruikers moeten handmatig het juiste protocol selecteren op basis van hun netwerkomgeving

Oorzaak

Cisco Secure Access RAVPN is ontworpen zonder automatische protocol failover functionaliteit. Wanneer zowel TLS/DTLS- als IPsec(IKEv2)-protocollen zijn ingeschakeld, moet het systeem handmatig worden geselecteerd via de beveiligde clientinterface. De instelling Primair protocol bepaalt alleen de standaardselectie in het vervolgkeuzemenu voor de client en implementeert geen automatische schakellogica wanneer er verbindingsproblemen met het primaire protocol optreden.

Verwante inhoud

- Cisco Secure Access-documentatie
- 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.