

IPsec-tunnelconnectiviteitsprobleem met Versa Networks Router vanwege ESN-onderhandelingen

Inhoud

uitgifte

Tijdens de implementatie van Cisco Secure Access in een filiaal met Versa-Network Router als randapparaat, werden connectiviteitsproblemen ondervonden ondanks het feit dat beide IPsec-tunnels operationeel leken.

De specifieke symptomen omvatten:

- Geen connectiviteit van de vestiging naar Cisco Secure Access
- Internettoegang via statische routes werkt niet
- Unidirectioneel gecodeerd verkeer waargenomen (alleen uitgaand naar Secure Access)
- Routerstatistieken met uitgaande pakketten die worden verzonden, maar geen inkomende pakketten die worden ontvangen
- Dead peer-detectie werkt bidirectioneel tussen SD-WAN-router en Secure Access
- Security Parameter Index (SPI)-waarden voor correct overeenkomen van uitgaand verkeer
- Tunnelflappen (opnieuw instellen) heeft het verbindingsprobleem niet opgelost
- Packet-opnames en screenshots bevestigden het gebrek aan inkomende verkeer
- Het veranderen van tunnelversleuteling van CBC naar GCM heeft het probleem niet opgelost

Onderzoek wees uit dat het verkeer niet kon worden ontsleuteld aan de Cisco-kant vanwege checksum-fouten, die werden herleid tot de Versa-router die onderhandelde over ESN (Extended Sequence Number) -functionaliteit.

milieu

- Implementatie van Cisco Secure Access
- Versa-Networks Router als randapparaat
- IP-Identity Tunnel-configuratie
- IPsec-tunnelconfiguratie met zowel CBC- als GCM-coderpogingen

resolutie

De resolutie betrof het uitschakelen van Extended Sequence Number (ESN) onderhandelingen op de Versa router om checksum fouten die decryptie fouten op de Cisco Secure Access head-end veroorzaken voorkomen.

Stappen voor het oplossen

Stap 1: Identificeer de oorzaak

Uit het onderzoek bleek dat de Versa-router onderhandelde over ESN (Extended Sequence Number), waardoor de Cisco Secure Access-kop controlesomfouten ontving en de door ESN gebouwde pakketten niet kon ontcijferen.

Stap 2: Schakel ESN uit op Versa Router

Neem contact op met de ondersteuning van Versa Networks of de routerbeheerder om de ESN-controles en onderhandelingen over de configuratie van de Versa-router uit te schakelen. Dit adresseert de bekende Versa-bug die ervoor zorgt dat ESN onjuist wordt onderhandeld.

Stap 3: Controleer de connectiviteit

Nadat ESN-onderhandelingen zijn uitgeschakeld, moet u bevestigen dat de bidirectionele verkeersstroom tot stand is gebracht en dat de volledige connectiviteit van het filiaal naar Secure Access en Internet is hersteld.

Stap 4: Bewaak de verkeersstroom

Controleer of de statistieken van zowel inkomende als uitgaande pakketten op de router een goede verkeersstroom in beide richtingen laten zien, wat een succesvolle oplossing van het unidirectionele verkeersprobleem bevestigt.

Oorzaak

De hoofdoorzaak werd geïdentificeerd als een bekende Versa Networks-bug (Versa-ondersteuningsbug-ID: 122437 - ESN mag niet door VOS worden onderhandeld) waarbij de Versa-router ten onrechte onderhandelt over de Extended Sequence Number (ESN) - functionaliteit tijdens het instellen van de IPsec-tunnel. Deze ESN-onderhandeling zorgt ervoor dat de Cisco Secure Access head-end pakketten ontvangt met checksum-fouten, waardoor een goede decryptie wordt voorkomen en unidirectionele verkeersstroom wordt veroorzaakt. De Versa-router verzendt uitgaande pakketten met succes, maar het retourverkeer kan niet goed worden verwerkt vanwege de ESN-gerelateerde decoderingsfouten.

Gerelateerde 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.