Overmatige DNS-verzoeken op poort 53 tijdens AnyConnect VPN-sessies

Inhoud

uitgeven

Na de implementatie van Remote Access VPN (RA-VPN) genereren gebruikers die verbinding maken via Cisco AnyConnect tientallen DNS-verzoeken op poort 53 naar de secundaire DNS-server. Dit gedrag wordt waargenomen in de Activiteitenmonitor voor alle gebruikers die zijn aangesloten op de VPN-tunnel en resulteert in tal van toegestane verzoeken die de tunnel overstromen. Deze overmatige DNS-activiteit treedt niet op wanneer gebruikers verbinding maken via Zero Trust Access (ZTA), wat aangeeft dat het probleem specifiek verband houdt met de AnyConnect VPN-verbindingsmethode.

milieu

- Productfamilie: veilige toegang
- Implementatie: VPN-implementatie voor externe toegang
- Vergelijkingsomgeving: Zero Trust Access (ZTA) - niet hetzelfde DNS-overstromingsgedrag ervaren

resolutie

Het onderzoeken van de buitensporige DNS-verzoeken vereist logboekverzameling en -analyse om de hoofdoorzaak van het DNS-overstromingsgedrag te identificeren. De logboekverzameling omvat het verzamelen van pakketvastlegging met PID voor elk pakket om te bepalen welke toepassing op een eindpunt de uitvoer voor verkeer en procesbewaking genereert.

Oorzaak

Uit de analyse bleek dat deze hoeveelheid DNS-verkeer wordt verwacht.

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.