VPN-client kan IP-wijzigingstabel voor doorsturen niet verifiëren op Secure Client RAVPN Split-Tunnel/Default DNS

Inhoud

uitgeven

Mac-gebruikers ervaren intermitterende fouten bij het proberen van CLI-verificatie voor interne toepassingen terwijl ze zijn verbonden met Cisco Secure Client VPN. De fouten worden weergegeven als "host not found"-fouten tijdens CLI-verificatie en bij het gebruik van opdrachten zoals `curl`. DNS-resolutiecommando's zoals `nslookup` en `dig` slagen echter. Het probleem treedt willekeurig op en kan tijdelijk worden opgelost door de VPN opnieuw te verbinden, waarna de connectiviteit een korte periode werkt voordat het probleem opnieuw optreedt. Split-tunnel VPN wordt gebruikt en Cisco Umbrella is actief. Het probleem doet zich niet voor bij het gebruik van Palo Alto GlobalProtect VPN.

- Foutbericht: "host niet gevonden" op CLI-verificatie en `curl`-opdrachten.
- Foutbericht: VPN-client kan wijzigingen in de IP-doorstuurtabel niet verifiëren. Probleem met DNS-oplossing (Domain Name Server) bij verbinding maken met privébronnen
- `NSLOOKUP` en `DIG` commando's slagen
- Intermitterende connectiviteit na opnieuw verbinden met VPN
- Split-tunnel remote access VPN en Umbrella module ingeschakeld
- Probleem alleen reproduceerbaar met Cisco Secure Client VPN op MacOS-apparaten

milieu

- Product: Cisco Secure Client (CSC) met meerdere modules
- Platform: zakelijke Mac-apparaten
- VPN-profielconfiguratie: VPN-profiel voor externe toegang - Beveiligde toegang omzeilen - Split-tunnel-modus en DNS-modus geselecteerd als "Standaard DNS"
- DNS-filtering: Cisco Umbrella ingeschakeld
- Moduleversies:
    - Cloud Management v1.0.0.23
    - AnyConnect VPN v5.1.13.177
    - Paraplu v5.1.13.177
    - DART v5.1.13.177
    - Secure Firewall Posture v5.1.13.177
    - Network Visibility Module v5.1.13.177
- Diagnostische gegevens: DART-bundels verzameld voor analyse

- Alleen waargenomen op Cisco Secure Client VPN (niet op Palo Alto GlobalProtect)

resolutie

- Tijdens het debuggen van de VPN-profielconfiguratie (`naic.org`) en de AnyConnect VPN-routeringstabel aan de clientzijde werd dit gedrag waargenomen:
  - Werkscenario - Bij het uitvoeren van een `nslookup` voor de niet-prod lokale domeinen van de Vault worden DNS-verzoeken die worden afgehandeld door de DNS-servers die in het VPN-profiel zijn geconfigureerd, correct opgelost tot 10.x-adressen. Dienovereenkomstig werd de routeringstabel bijgewerkt met het opgeloste IP (bijvoorbeeld 10.59.130.193) op niet-beveiligde routes.
  - Niet-werkend scenario - Wanneer dezelfde DNS-verzoeken echter werden afgehandeld door de lokale DNS (192.168.x.x) van het macOS-systeem die is geconfigureerd op de untun4- en en en0-adapter in plaats van de DNS-servers die zijn gedefinieerd in het VPN-profiel, is dit gedrag duidelijk waargenomen bij het vastleggen van pakketten terwijl het probleem werd opgemerkt.
  - de privédomeinen zijn opgelost tot een IP-bereik van 34.x.x.x, wat heeft geleid tot het connectiviteitsprobleem. Wireshark capture hielp om deze onderliggende oorzaak van het probleem te identificeren.
- Vanuit het oogpunt van ontwerp en configuratie, met een gesplitste VPN-profielconfiguratie, wordt het aanbevolen om gesplitste DNS te gebruiken in plaats van te vertrouwen op lokale DNS / standaard DNS van het systeem.
- Bovendien is de vermelding `us-east-eks-amazonaws.com` toegevoegd om ervoor te zorgen dat het verkeer voor dit EKS-cluster correct door de externe tunnelinterface wordt geleid.
- Ook werd besproken dat de RAVPN-interface voorrang moet hebben op de Umbrella-module en niet in strijd mag zijn met het `OrgInfo.json`-bestand met de Umbrella Organization ID.
- Tijdens ons probleemoplossingsproces hebben we een nieuwe installatie van CSC-client zonder paraplu-module uitgevoerd, met dat scenario konden we het probleem niet zien. Ik was in staat om te bekijken vanuit Umbrella perspectief ook, root domein naic.org geconfigureerd in de interne domeinen lijst te omzeilen Umbrella wat betekent dat de lokale domein resoluties wordt doorgestuurd naar macOS geconfigureerd systeem DNS niet onderschept door Umbrella DNS module op kernel level loopback interface.

Dit sluit aan bij het oplossen van problemen als er geen paraplu-module is geïnstalleerd. Met de juiste VPN-profielconfiguratie, inclusief de juiste domeinen in de verkeersregel en gesplitste DNS-configuratie, zouden we het probleem niet moeten zien, zelfs als het Umbrella-model is ingeschakeld.

De gebruiker heeft bevestigd dat het probleem is opgelost nadat de DNS-modus is gewijzigd in Split Tunnel en de VPN-profielconfiguratie is bewerkt.

Oorzaak

VPN-profiel - Bypass Secure Access - DNS-modus zou moeten worden ingesteld op Split Tunnel (meest voorkomende opties uit een use case scenario's) en alle privé / interne

toepassingsdomeinen onder gesplitste DNS-configuratie bevatten om het probleem op te lossen.

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.