DNS-registratie en apparaatregistratiegedrag met Cisco Secure Client op iOS voor VPN voor externe toegang

Inhoud

uitgeven

Wanneer u Cisco Secure Client op iOS (iPad) gebruikt om externe VPN-toegang met Cisco Secure Access tot stand te brengen met behulp van SAML-verificatie via Microsoft Entra ID, worden DNS-logs niet weergegeven in Secure Access na een succesvolle VPN-verbinding, ook al worden firewall- en weblogs correct gegenereerd. Bovendien wordt de iPad niet weergegeven onder Zwervende apparaten > Mobiele apparaten in het dashboard voor beveiligde toegang nadat de VPN-verbinding tot stand is gebracht.

De specifieke waargenomen symptomen omvatten:

- Logboeken voor externe toegang tonen succesvolle "connect"-gebeurtenissen in Secure Access
- Firewall- en weblogs worden gegenereerd en geven de door SAML geverifieerde gebruikersidentiteit weer
- DNS-logs zijn volledig afwezig in de logboekregistratie voor beveiligde toegang
- De iPad-apparaatgegevens worden niet ingevuld in het gedeelte Zwervende apparaten met beveiligde toegang
- Alle verkeer stroomt door de VPN-tunnel (geen gesplitste tunneling geconfigureerd)

milieu

- iPad met iOS 26.2
- Cisco Secure Client

- Identiteitsprovider: Microsoft Entra ID
- Beveiligingsconnector: niet geïnstalleerd
- Cisco Secure Access met SSO-verificatie geconfigureerd
- Implementatie van SAML-verificatie
- VPN-profiel geconfigureerd met DNS-modus ingesteld op standaard
- Geen gesplitste tunneling geconfigureerd (alle verkeer wordt via VPN gerouteerd)
- Mobile Device Management (MDM) gebruikt voor profieldistributie

resolutie

Het waargenomen gedrag wordt verwacht voor de gedocumenteerde configuratie. Cisco Secure Client op iOS functioneert als een VPN-client (AnyConnect-equivalent) en bevat standaard geen RSM-equivalente functionaliteit. Security Connector is de RSM-equivalente component op iOS die nodig is voor endpoint identity population en Umbrella-style DNS control.

Inzicht in de architectuur

De afwezigheid van DNS-logs en apparaatregistratie treedt op omdat:

- Alleen Cisco Secure Client biedt VPN-connectiviteit, maar mist de functionaliteit van de endpoint agent die nodig is voor DNS-zichtbaarheid
- Beveiligingsconnector (gelijk aan RSM op Windows) is vereist voor DNS-besturing en apparaatregistratie in Secure Access
- Zonder Security Connector worden DNS-query's afgehandeld door de VPN-verkregen DNS-servers zonder zichtbaarheid voor Umbrella / Secure Access

DNS-logboekoplossing via verkeerssturing

Als u DNS-logboekregistratie wilt inschakelen zonder Security Connector te installeren,

configureert u de verkeersbesturing om DNS-query's naar Umbrella DNS-servers te sturen:

Stap 1: verkeerssturing configureren in beveiligde toegang

Navigeer naar Traffic Steering > Add > Add a source en specificeer de DNS-server IP als bron.

Stap 2: Direct DNS-verkeer naar paraplu-servers

Configureer het VPN-profiel om Umbrella DNS-servers (208.67.222.222 en 208.67.220.220) te gebruiken om ervoor te zorgen dat DNS-query's zichtbaar zijn voor beveiligde toegang.

Stap 3: DNS-registratie valideren

Na het implementeren van de verkeerssturingsconfiguratie moeten DNS-logs zichtbaar worden in het Secure Access-dashboard voor VPN-sessies.

VPN-profiel DNS-modus instellen

De instelling "DNS-modus" in het VPN-profiel is niet gerelateerd aan de afwezigheid van DNS-logs in deze configuratie. RAVPN-sessies (Remote Access VPN) maken gebruik van de VPN-verkregen DNS-servers, ongeacht deze instelling, en de zichtbaarheid van de registratie hangt af van de vraag of het DNS-verkeer naar de bewaakte DNS-infrastructuur wordt geleid.

Installatie van beveiligingsconnector, optie

Het installeren van Security Connector op iOS zal het volgende mogelijk maken:

- Zichtbaarheid van DNS-registratie in Secure Access
- Verbeterde mogelijkheden voor identificatie van eindpunten en apparaatregistratie
- DNS-besturing en -beveiliging in paraplustijl

Beveiligingsconnector kan worden gebruikt in combinatie met Secure Client, maar om conflicten tussen de twee componenten te voorkomen, zijn passende verkeersuitsluiting en ontwerpoverwegingen vereist.

Oorzaak

De hoofdoorzaak is architecturaal: Cisco Secure Client op iOS biedt VPN-connectiviteit, maar bevat niet de functionaliteit van de endpoint agent die vereist is voor DNS-zichtbaarheid en apparaatregistratie in Secure Access. Voor deze functionaliteit is de installatie van de Security Connector of de configuratie van de verkeersbesturing nodig om DNS-query's door de bewaakte infrastructuur te leiden. Zonder deze componenten omzeilen DNS-query's de bewaking van beveiligde toegang en wordt de apparaatidentiteitsinformatie niet ingevuld in het gedeelte met roamingapparaten.

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.