

Beveiligde client TND Handmatig VPN-verbindingsgedrag en overwegingen voor URL-blokkering

Inhoud

uitgifte

Wanneer een VPN-profiel met de functie Trusted Network Detection (TND) wordt gebruikt dat is geconfigureerd met de instelling Trusted Network (Vertrouwd netwerk) die is ingesteld op Verbinding verbreken, kunnen eindpunten in het vertrouwde netwerk nog steeds met succes een VPN-verbinding tot stand brengen wanneer gebruikers handmatig verbindingen starten met behulp van Cisco Secure Client.

Dit gedrag treedt op ondanks dat de TND-configuratie is ingesteld om VPN-sessies te verbreken wanneer het eindpunt wordt gedetecteerd op een vertrouwd netwerk.

De specifieke punten van zorg zijn onder meer:

- Handmatige VPN-verbindingen van Trusted Network-eindpunten kunnen niet worden beheerd of geblokkeerd via de standaard TND-configuratie
- Onzekerheid over de vraag of Cisco Secure Access (CSA)-instellingen handmatige VPN-verbindingen van Trusted Network-eindpunten kunnen blokkeren
- Vragen over de stabiliteit van de URL van de VPN-profielverbinding (xxxx.vpn.sse.cisco.com) en of deze periodiek verandert, wat van invloed kan zijn op op firewall gebaseerde blokkeringsstrategieën

milieu

- Cisco Secure Access (CSA)-implementatie
- Cisco Secure Client met VPN-profielconfiguratie

- Trusted Network Detection (TND)-functie ingeschakeld
- Instelling TND Trusted Network geconfigureerd als Verbinding verbreken
- Eindpunten binnen geconfigureerd Trusted Network
- Firewallinfrastructuur voor netwerktoegangscontrole

resolutie

TND-gedrag begrijpen met handmatige VPN-verbindingen

Het waargenomen gedrag is consistent met de gedocumenteerde Cisco Secure Client-functionaliteit. Volgens Cisco-documentatie verbreekt of voorkomt TND geen VPN-sessie die een gebruiker handmatig start terwijl hij zich op een vertrouwd netwerk bevindt. Dit is het verwachte gedrag, ongeacht de instellingen voor de TND-configuratie.

De belangrijkste technische feiten zijn:

- De TND-functionaliteit voor automatische ontkoppeling is alleen van toepassing op automatisch ingestelde VPN-verbindingen.
- Handmatige VPN-verbindingen die door gebruikers worden geïnitieerd, omzeilen het TND-ontkoppelingsgedrag.
- Er bestaat geen CSA-configuratie-instelling om handmatige VPN-verbindingen te blokkeren van Trusted Network-eindpunten.

operationele mitigatiestrategie

De primaire methode voor het besturen van handmatige VPN-verbindingen vanaf Trusted Network-eindpunten is via besturingselementen op netwerkniveau:

Stap 1: Implementeer Firewall URL Blocking: Configureer de Trusted Network firewall om de toegang tot de VPN-profielverbinding URL (xxxx.vpn.sse.cisco.com) te blokkeren. Dit voorkomt dat eindpunten op het vertrouwde netwerk het VPN-service-eindpunt bereiken.

Stap 2: Controleer de stabiliteit van de URL: de VPN-profiel-URL-ID (het xxxx-gedeelte) is huurderspecifiek en zal naar verwachting niet periodiek worden gewijzigd. Dit biedt een stabiel doel voor firewallblokkeringsregels.

Validatie en testen

Testen heeft bevestigd dat het blokkeren van de VPN-profielverbinding-URL bij de Trusted Network-firewall met succes voorkomt dat endpoints VPN-verbindingen tot stand brengen, zelfs wanneer gebruikers handmatige verbindingen proberen via Cisco Secure Client.

Oorzaak

Dit gedrag is door ontwerp in Cisco Secure Client TND-implementatie. De TND-functie is specifiek ontworpen om automatische VPN-verbindingen te beheren op basis van de vertrouwensstatus van het netwerk, maar het interfereert opzettelijk niet met handmatige VPN-verbindingen die door de gebruiker worden geïnitieerd. Dit ontwerp stelt gebruikers in staat om automatisch gedrag te negeren wanneer dat nodig is, terwijl ze toch geautomatiseerde netwerkdetectie en verbindingsbeheer bieden voor typische gebruikgevallen.

Gerelateerde inhoud

- [Cisco Secure Client Administrator Guide - TND-configuratie](#)
- [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.