

Beveiligde netwerken uitschakelen voor overkoepelende roamingclients op bedrijfsnetwerken

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Wat is de functie Vertrouwd netwerkdomein?](#)

[IPv6-gedrag, Windows versus MacOS](#)

[Hoe schakel ik de functie in?](#)

[Hoe test ik de functie voor één machine?](#)

Inleiding

In dit document wordt beschreven hoe u de Umbrella-roamingclients (standalone en AnyConnect) op een bedrijfsnetwerk kunt uitschakelen en kunt uitschakelen.

Achtergrondinformatie

Dit artikel is bedoeld voor beheerders. Als u de roamingclient op het netwerk niet wilt uitschakelen, stopt u hier.

De functie Umbrella Protected Networks is bedoeld voor één toegangsnetwerk. Voor netwerken met meer dan één uitgang is een alternatieve functie vereist.

Tegenwoordig bestaat deze functie in productie als de vertrouwde netwerkdomeinfunctie. Lees verder om te leren hoe u de functie kunt aanvragen en wat er nodig is op uw netwerk.

Wat is de functie Vertrouwd netwerkdomein?

De functie Vertrouwd netwerk per domein is een manier om de zwervende client in uw bedrijfsnetwerk uit te schakelen, maar deze ingeschakeld te houden van het netwerk. Wanneer geactiveerd, de functie:

- Hiermee schakelt u de DNS-beveiliging uit die door de roamingclient wordt geboden
 - Het beleid wordt uitgesteld tot het netwerkbeleid
- Stopt alle netwerkprobes behalve de controle van het vertrouwde netwerkdomein
 - Ideaal voor drukke netwerken!
 - Geweldig alternatief voor de VA-backoff
 - Gebruik in combinatie met VA's voor minder netwerkgesprekken

IPv6-gedrag, Windows versus MacOS

- In Windows wordt het domein opgevraagd op IPv4 en IPv6. Het afsluitgedrag wordt op elke netwerkstapel afzonderlijk afgehandeld. Als het domein bijvoorbeeld wordt opgelost op IPv4 maar niet op IPv6, wordt de roamingclient alleen afgesloten op IPv4 en blijft deze actief op IPv6. Als u de client volledig wilt uitschakelen, moeten IPv4- en IPv6-query's worden opgelost.
- Op MacOS wordt het domein opgevraagd op IPv4 en IPv6. In tegenstelling tot Windows wordt de roamingclient afgesloten voor zowel IPv4 als IPv6 als het domein wordt opgelost op beide netwerkstapels.

Hoe schakel ik de functie in?

Deze functie wordt nu bestuurd in het dashboard. Zie Instellingen voor zwervende computers.

- Het gewenste subdomein Umbrella uitschakelen. Dit domein moet:
 - Een A-record hebben dat oplost naar een RFC-1918 intern IP-adres (voor IPv4)
 - Heb een AAAA-record dat oplost naar een RFC-4193 IP op IPv6 (als IPv6 wordt gebruikt)
 - RFC-1918 IP's zien er meestal uit als 10.x.x.x, 172.x.x.x of 192.168.x.x
 - RFC-4193: IPv6-adressen beginnen met 'FD'
 - IP-adressen hoeven niet bereikbaar te zijn
 - Moet een subdomein zijn
 - sub.domain.com - goed!
 - subdomain.com - niet goed.
 - Los het netwerk op naar NXDOMAIN, NODATA of openbaar IP-adres (zodat de client in deze scenario's ingeschakeld blijft)
 - Geen service alstublieft
 - Wees een domein in een zone die u beheert om ervoor te zorgen dat u de openbare en lokale ruimte beheert
- Ondersteunt:
 - Umbrella Roaming-client
 - Alleen AnyConnect Umbrella Roaming Security Module 4.5 MR4+

Hoe test ik de functie voor één machine?

Als u lokaal wilt testen voordat het Umbrella-team de instelling globaal toepast, past u deze overschrijving toe.

1. Maak een bestand "customer_network_probe.flag"
 1. Controleer of het bestand geen .flag.txt is
2. Zet het gewenste domein in de inhoud van het bestand
3. Plaats het bestand in:
 1. Zwervende client
 1. Windows: %ProgramData\OpenDNS\ERC\

2. AnyConnect

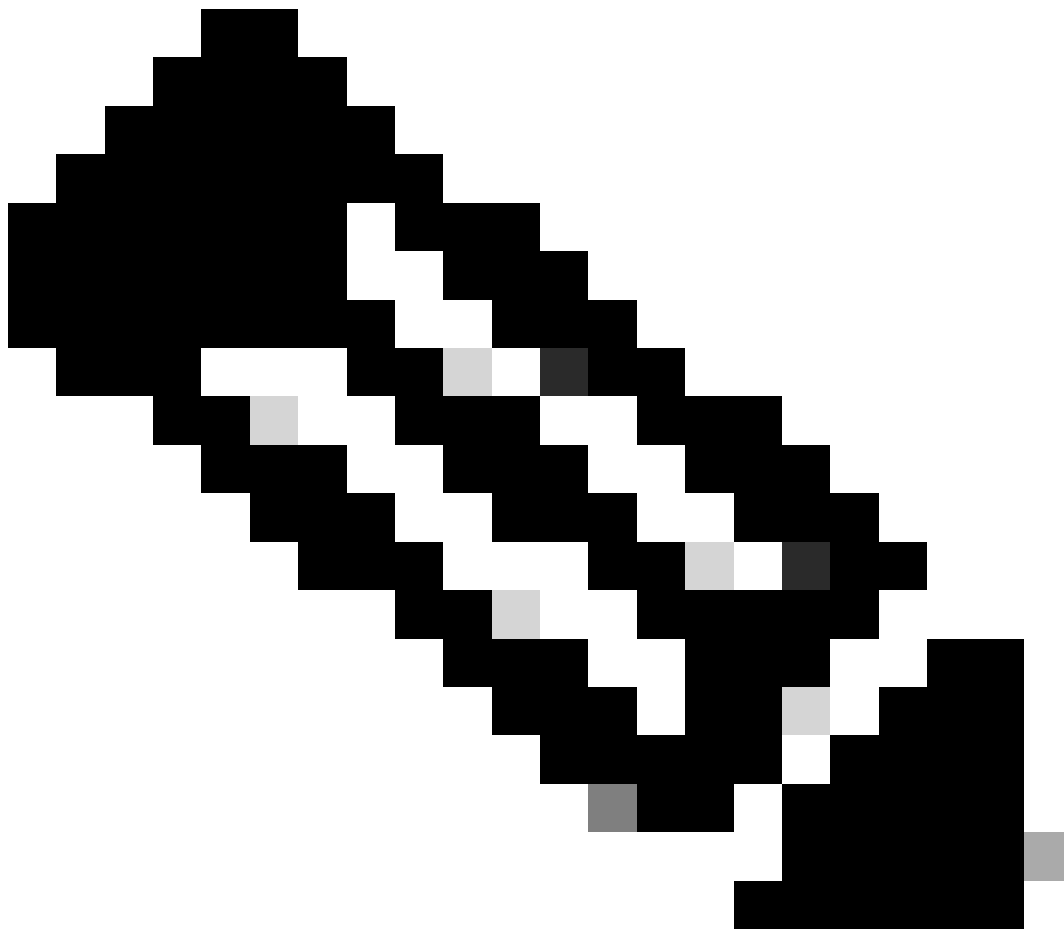
1. Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\

3. Cisco Secure Client

1. Windows: C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\
2. macOS: /opt/cisco/secureclient/umbrella/data/

4. Start de zwervende client opnieuw op

1. Zwervende client: Umbrella Roaming Client: handmatig uitschakelen of opnieuw opstarten.
2. AnyConnect: de bovenliggende AnyConnect-service opnieuw starten



Opmerking: voor MacOS Roaming-client wordt deze vlag niet ondersteund in AnyConnect-versies.

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.