

Umbrella Roaming Client- en VPN-compatibiliteit beheren

Inhoud

[Inleiding](#)

[Overzicht](#)

[Hoe de Umbrella Roaming Client werkt met VPN-clients](#)

[Incompatibiliteiten met Umbrella Roaming Client](#)

[Incompatibiliteitsredenen voor VPN-clients](#)

[Virtuele apparaten en beveiligde netwerken](#)

[Speciale overwegingen voor de beveiligingsmodule Standalone en Cisco Secure Client + Roaming](#)

[DNS Binding Order VPN Compatibility Mode voor Windows 10 en 11](#)

[Voorbeeld resolv.conf output](#)

[Speciale overwegingen voor VPN's van derden](#)

[Always-on VPN](#)

[Oplossingen](#)

[Viscosity VPN](#)

[Viscositeit configureren](#)

[Tunnelblick](#)

[Problemen met Tunnelblick VPN-verbinding verbreken](#)

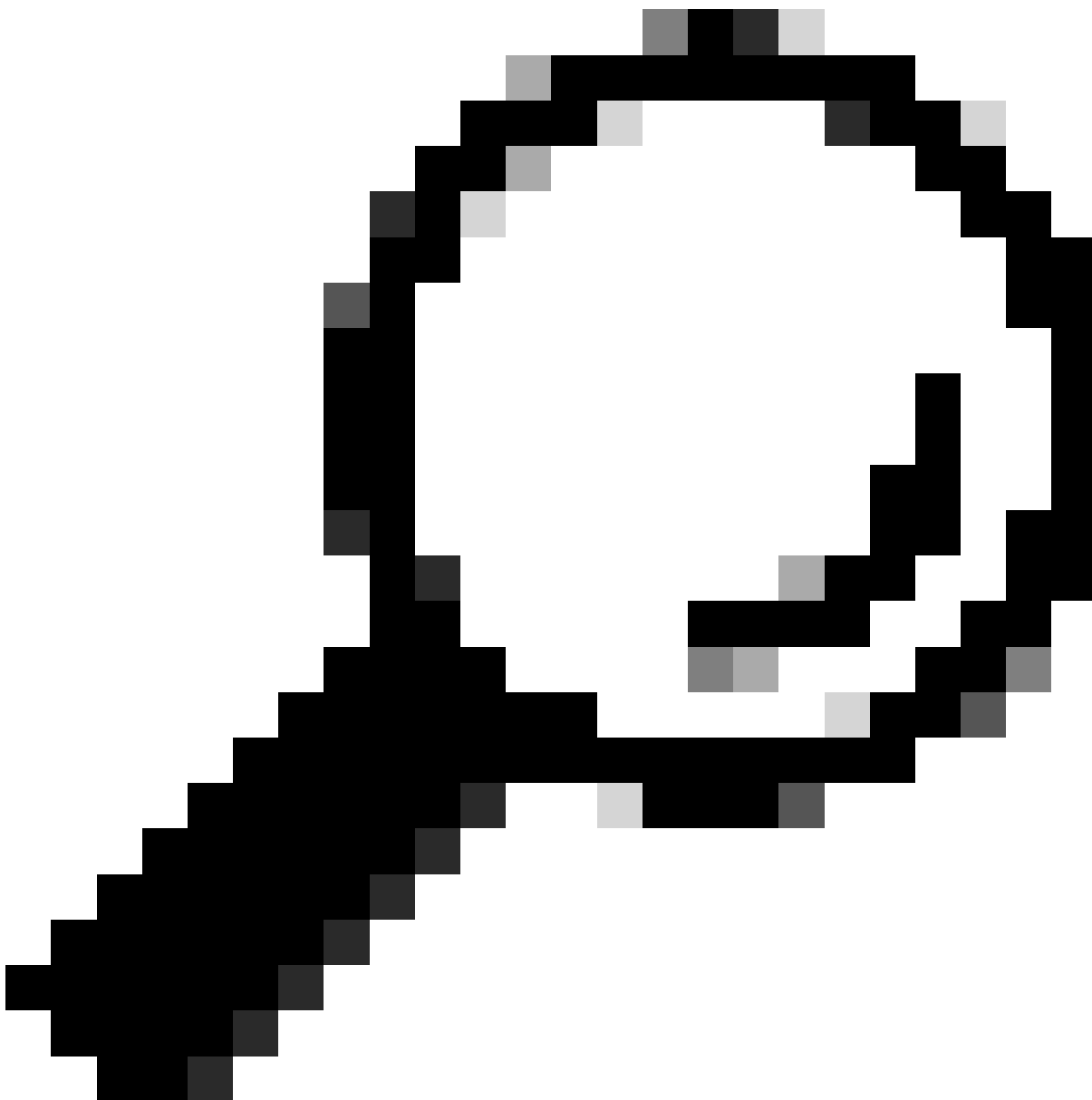
[raket met lichtsnelheid](#)

Inleiding

Dit document beschrijft de interactie en compatibiliteit van de Cisco Umbrella Roaming Client met verschillende VPN-software.

Overzicht

De Cisco Umbrella Roaming Client werkt met de meeste VPN-software, maar voor de verwachte werking kunnen extra stappen nodig zijn. Cisco Umbrella raadt u aan de Cisco Secure Client- en Roaming Security-module te implementeren voor maximale compatibiliteit. Deze module kan worden geïmplementeerd zonder de VPN-componenten.



Tip: Dit document dient als algemene leidraad en dient niet als een officiële lijst met ondersteunde software. Cisco Umbrella test, valideert of certificeert geen functionaliteit met software of VPN-clients van derden.

Dit document biedt technische informatie en aanvullende context voor specifieke VPN-clients die verdere configuraties kunnen vereisen. Voor een lijst met bekende incompatibele VPN-software raadpleegt u de sectie Incompatibiliteiten van Umbrella Roaming Client. DNS-incompatibiliteit met de zwervende client kan ook leiden tot het falen van de Cisco Secure Client + Roaming Security-module met SWG, omdat de SWG-client ook afhankelijk is van het succesvol tot stand brengen van een DNS-verbinding.

Hoe de Umbrella Roaming Client werkt met VPN-clients

De Umbrella Roaming Client bindt zich aan alle netwerkadapters en wijzigt de DNS-instellingen op de computer in 127.0.0.1 (localhost). Hierdoor kan de Umbrella Roaming Client alle DNS-query's rechtstreeks doorsturen naar Umbrella, terwijl de oplossing van lokale domeinen via de functie Interne domeinen mogelijk wordt. Bij het maken van een verbinding met een VPN-server detecteert de Umbrella Roaming Client een nieuwe netwerkverbinding in het systeem en wijzigt de DNS-instellingen van de verbinding om naar de Umbrella Roaming Client te wijzen. De Umbrella Roaming Client is afhankelijk van het uitvoeren van DNS-opzoeken naar de IP-adressen van Umbrella AnyCast DNS (208.67.222.222/208.67.220.220).

Als een gebruiker verbinding maakt met een VPN, moet de firewall die aan de VPN is gekoppeld toegang tot Umbrella toestaan.

Incompatibiliteiten met Umbrella Roaming Client

De Umbrella Roaming Client levert momenteel DNS-laaghandhaving. De DNS-laag is de primaire functie van de roamingclient en past op DNS gebaseerd beveiligingsbeleid toe op elk netwerk. Deze functie van de roamingclient kan bekende software-incompatibiliteiten ervaren. De DNS-laag van de Umbrella Roaming Client is niet compatibel met de hieronder vermelde clients, op basis van tests door het supportteam. Cisco Umbrella Engineering verifieert of test deze clients niet en alle inzendingen kunnen worden beoordeeld. In dit artikel wordt verwezen naar de zelfstandige Umbrella Roaming Client. Voor een begeleidend artikel over de Umbrella Roaming Security Module voor Cisco Secure Client (en legacy), raadpleegt u de relevante documentatie.

VPN-client	Probleem/incompatibiliteit	resolutie
impulsbestendig	Bij het verbreken van de verbinding kunnen opgeslagen lokale DNS VPN-waarden blijven in plaats van WiFi/Ethernet-waarden als gevolg van Pulse-wijzigingen tijdens de VPN-verbinding.	Opgelost met de Umbrella-module - inbegrepen in de meeste licenties.
Avaya VPN	Incompatibel.	Opgelost met de Umbrella-module - inbegrepen in de meeste licenties.
Windows VPN (met name Always On VPN)	Dit kan ertoe leiden dat lokale DNS het interne antwoord niet oplost, ondanks dat de DNS-hostnamen in de lijst met interne domeinen staan.	Opgelost met de Umbrella-module - inbegrepen in de meeste licenties.
VPN-apps gebouwd bovenop het Windows Universal Platform	Deze apps moeten een Microsoft-API voor verbindingen gebruiken waarvoor DNS naar de lokale NIC moet worden verzonden, niet naar 127.0.0.1. Daarom geeft de app een	Opgelost met de Umbrella-module - inbegrepen in de meeste licenties.

VPN-client	Probleem/incompatibiliteit	resolutie
	fout weer die aangeeft dat er geen verbinding kan worden gemaakt.	
OpenVPN	Incompatibel.	Geen oplossing beschikbaar.
Palo Alto GlobalProtect VPN	Werkt niet met een standalone roamingclientversie na 3.0.110.	Opgelost met behulp van de Umbrella-module - inbegrepen in de meeste licenties.
F5 VPN	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.
Checkpoint VPN	Alleen macOS, alleen Split-tunnelmodus.	Schakel split-tunnel uit op macOS.
SonicWall NetExtender	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.
Zscaler VPN	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.
Akamai endpoint protection (ETPclient)	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.
NordVPN	Gebruik een tijdelijke oplossing.	Er zijn twee opties voor het toevoegen van compatibiliteit: 1. Gebruik de methode OpenVPN-verbinding zoals beschreven in Een handmatige verbinding instellen op Windows met OpenVPN 2. Aangepaste DNS toestaan onder

VPN-client	Probleem/incompatibiliteit	resolutie
		Geavanceerde instellingen. Stel DNS in op 208.67.220.220 en 208.67.222.222.
Azure VPN	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.
AWS VPN	Gebruik een tijdelijke oplossing.	Bewerk het configuratiebestand (handmatig gedownload van AWS) om een tweede regelpull-filter ignore "block-outside-dns" te krijgen.
Pritunl VPN	Incompatibel.	Opgelost door de Umbrella-module - inbegrepen in de meeste licenties.

Incompatibiliteitsredenen voor VPN-clients

Sommige VPN-clients hebben DNS-gedrag dat vergelijkbaar is met de Umbrella Roaming Client. Als de DNS-server van de VPN-verbinding verandert in een onverwachte waarde, wijzigt de VPN-software de DNS-instellingen van het systeem terug naar de waarde die de VPN heeft ingesteld bij de eerste verbinding. De Umbrella Roaming Client voert ook dezelfde bewerking uit en verandert alle DNS-servers terug naar 127.0.0.1. Dit heen-en-weer gedrag zorgt voor een conflict tussen de VPN en de Umbrella Roaming Client. Dit conflict veroorzaakt een eindeloze cyclus van de DNS-servers voor het resetten van de VPN-verbinding. De Roaming Client detecteert dit en schakelt zichzelf uit om de VPN-verbinding te onderhouden indien mogelijk.

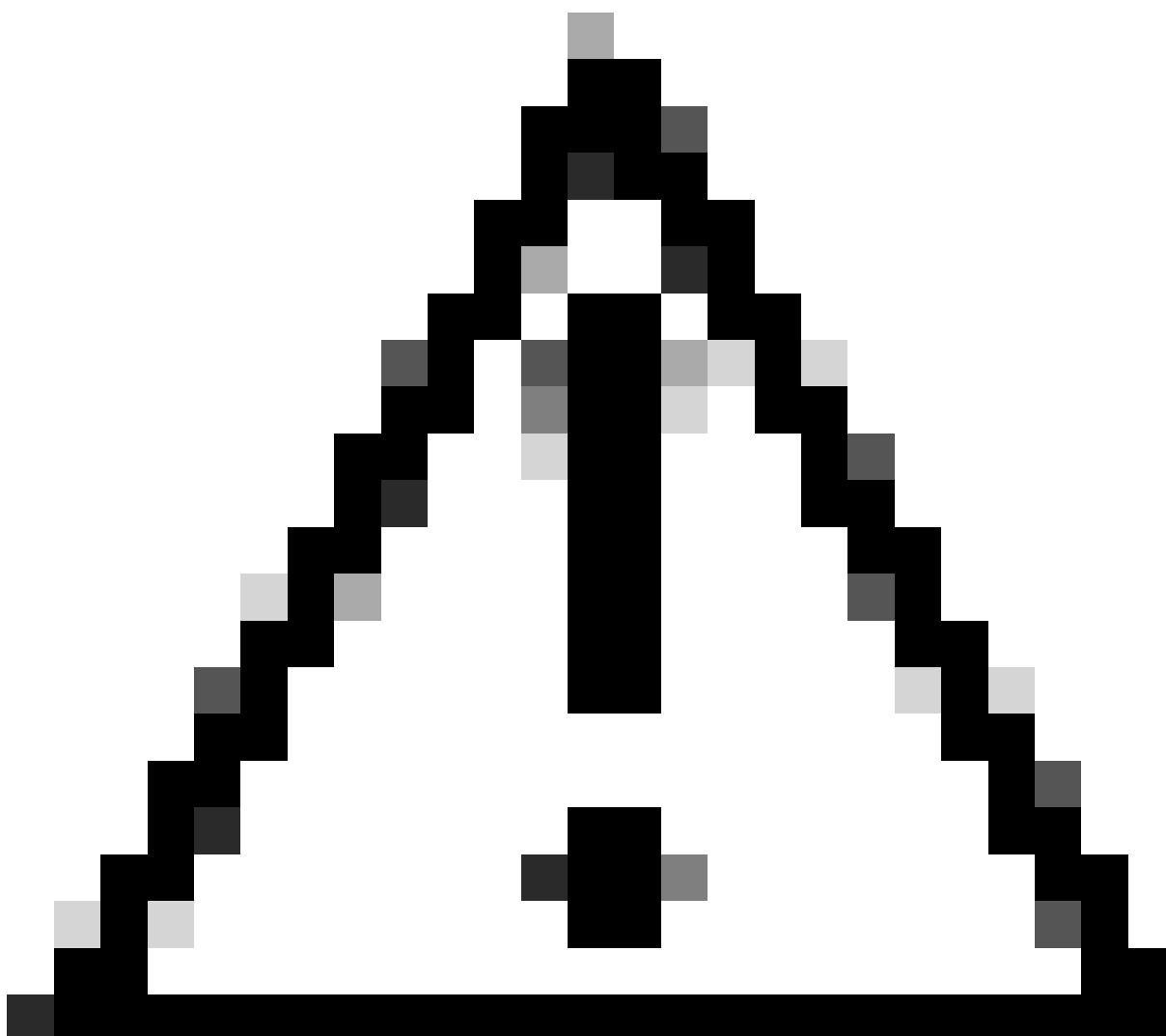
Virtuele apparaten en beveiligde netwerken

De Umbrella-roamingclient gedraagt zich anders wanneer deze is verbonden met een netwerk dat gebruikmaakt van de functie Umbrella Virtual Appliances (VA) of Protected Networks. Dit geldt ongeacht of een gebruiker lokaal of via een VPN verbinding maakt met het netwerk. Raadpleeg voor meer informatie de documentatie bij Roaming Client en Virtual Appliances of Protected Networks.

Speciale overwegingen voor de beveiligingsmodule Standalone en Cisco Secure Client + Roaming

De informatie die hier wordt verstrekt, is specifiek voor de zelfstandige Umbrella Roaming Client en is niet van toepassing op de Cisco Secure Client (CSC) + Roaming Security Module. Gebruikers die op zoek zijn naar een eenvoudige plug-in-installatie kunnen Umbrella Roaming gebruiken die is geïntegreerd in CSC. Cisco Secure Client VPN-gebruikers moeten migreren naar de CSC + Roaming Security Module als zich een functioneel probleem met de VPN voordoet. Cisco Umbrella vereist validatie op de CSC + Roaming Security Module en beveelt een volledige migratie aan.

De Cisco Secure Client VPN-software biedt opties voor de manier waarop het systeem met DNS omgaat wanneer een VPN-verbinding tot stand wordt gebracht. Zie het artikel [Gedragsverschillen met betrekking tot DNS-query's en domeinnaamresolutie in verschillende besturingssystemen](#) voor meer informatie. Deze informatie is gebaseerd op ervaring met Cisco Secure Client en de Umbrella Roaming Client. Het testen van de Umbrella-roamingclient met Cisco Secure Client VPN ingeschakeld wordt aanbevolen om interne en externe DNS-resolutiefuncties te garanderen zoals verwacht.



Let op: Cisco vereist dat u de CSC + Roaming Security Module gebruikt als u ook Cisco Secure Client voor DNS-servicecompatibiliteit gebruikt. De geboden stappen gelden alleen voor de niet-geïntegreerde roamingclient als dat nodig is. Deze stappen zijn niet vereist voor de CSC + Roaming Security Module.

In zowel de volledige als de gesplitste tunnelmodus zijn speciale instructies vereist om de roamingclient te laten werken terwijl de Cisco Secure Client is verbonden. Dit is nodig om DNS naar de roamingclient te laten stromen in plaats van te worden overschreven door de kerneldriver. Voor een volledige tunnel is het symptoom dat de klant gedwongen wordt uit te schakelen. Voor split tunneling is het symptoom een verlies van interne DNS tijdens verbinding met de VPN.

DNS Binding Order VPN Compatibility Mode voor Windows 10 en 11

Een beperkte set Windows 10-gebruikers ondervindt een specifiek probleem waarbij het lokale LAN prioriteit krijgt in plaats van de VPN-NIC voor DNS. In dit geval lost het lokale DNS in de lijst met interne domeinen voor de roamende client niet op terwijl het openbare DNS zonder problemen functioneert. Dit heeft invloed op versies 2.0.338 en 2.0.341 (standaard) en alle latere versies. Het probleem deed zich niet voor op versie 2.0.255.

De eerder getroffen VPN-clients zijn onder meer:

- AnyConnect 3.x
- AnyConnect 4.x (de AnyConnect-paraplu of CSC +-roamingmodule wordt niet beïnvloed)
- Sophos VPN
- Sommige Palo Alto GlobalProtect-configuraties op oudere versies
- WatchGuard Mobile VPN
- Shrew Soft VPN
- Barracuda VPN

resolutie

Schakel de instelling Zwervende client in Schakel de compatibiliteitsmodus voor bestaande VPN in.

Roaming Computers Settings

Umbrella Roaming Client

- ☐ Disable DNS redirection while on an Umbrella Protected Network. 
- ☒ Enable Active Directory user and group policy enforcement and internal IP address visibility.
- ☒ Enable legacy VPN compatibility mode. [Learn More](#)

360027547111

Om te bevestigen of dit het probleem is, voert u de diagnostische test uit en klikt u op de resultaten voor `resolv.conf`s. Als de VPN-adapter als eerste wordt vermeld, heeft het probleem geen invloed op de gebruiker. Als de VPN-adapter als tweede wordt vermeld, kan het probleem gevolgen hebben voor de gebruiker.

Voorbeeld `resolv.conf`s output

```
Results for: resolv.conf
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Local Area Connection
nameserver 192.168.2.1
```

```
C:\ProgramData\OpenDNS\ERC\Resolver1-76F52CE47B124D9FB05591D162777829-resolv.conf
# resolvers for Cisco AnyConnect Secure Mobility
nameserver 10.1.1.27
nameserver 10.1.1.28
```

Speciale overwegingen voor VPN's van derden

Always-on VPN

De zelfstandige roamingclient is niet compatibel met de Cisco Secure Client Always On VPN-instelling wanneer vertrouwde DNS-servers zijn gedefinieerd. Wanneer de zelfstandige roamingclient actief is, wordt DNS altijd ingesteld op 127.0.0.1, waardoor alle vertrouwde DNS-servers niet meer in de NIC-instellingen worden opgenomen. De Zwervende client kan op het

netwerk worden uitgeschakeld om de DHCP-instellingen te herstellen. Alle Zwervende client-gerelateerde beveiligingen worden echter stopgezet wanneer ze worden geconfigureerd. Neem contact op met Umbrella Support voor meer informatie over het uitschakelen van de client op een vertrouwd netwerk.

Oplossingen

- De CSC + Roaming Security Module (Roaming Client for Cisco Secure Client) wordt niet beïnvloed en werkt effectief met een automatisch VPN-beleid.
- Voeg 127.0.0.1 toe aan de lijst met vertrouwde DNS-servers.
- Zorg ervoor dat alternatieve methoden voor betrouwbare detectie zijn gedefinieerd (DNS-namen en -servers) om te voorkomen dat alle netwerken als vertrouwd worden aangemerkt.

The screenshot shows the configuration interface for the Cisco Secure Client. It includes sections for 'Automatic VPN Policy', 'Trusted Network Policy', 'Untrusted Network Policy', 'Trusted DNS Domains', 'Trusted DNS Servers', and 'Trusted Servers'. The 'Automatic VPN Policy' checkbox is checked. The 'Trusted Network Policy' dropdown is set to 'Disconnect'. The 'Untrusted Network Policy' dropdown is set to 'Connect'. The 'Trusted DNS Domains' field contains 'mydomain.local'. The 'Trusted DNS Servers' field contains '172.16.191.1'. A note states: 'Note: adding all DNS servers in use is recommended with Trusted Network Detection'. The 'Trusted Servers @ https://<server>[:<port>]' section shows a list with 'https://mysite.mydomain.local:443' selected, and buttons for 'Add' and 'Delete'.

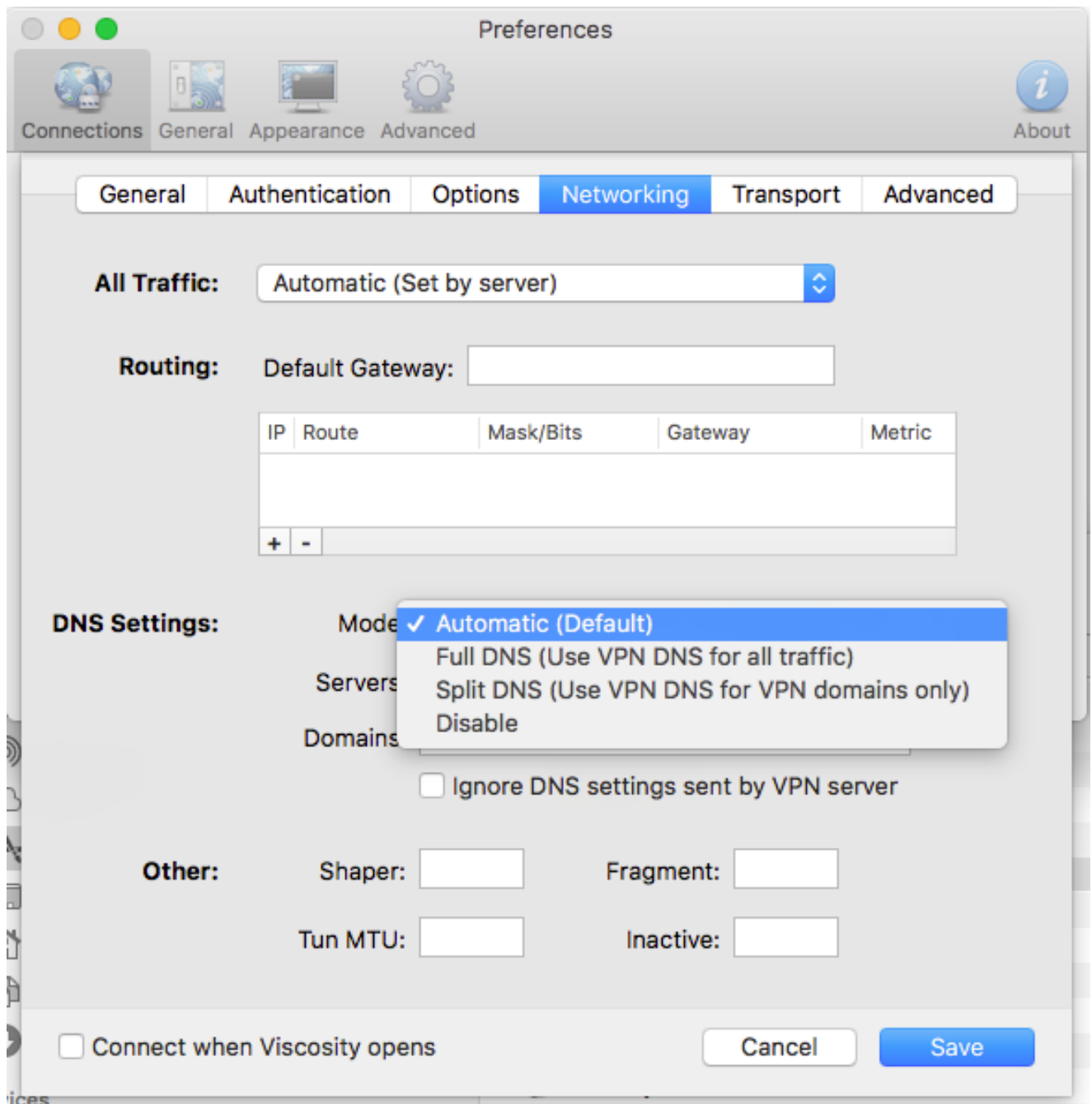
360031250911

Viscosity VPN

Viscosity VPN vereist een wijziging in de instellingen om te werken met de Umbrella-roamingclient. Als deze wijziging niet wordt doorgevoerd, bootst het standaardgedrag van Viscosity dat van andere incompatibele VPN's na. Deze wijziging geeft Viscosity de instructie om de DNS-instellingen te gebruiken die via de Umbrella-server zijn gepusht voor alle domeinen in het zoekdomein, en 127.0.0.1 blijft worden gebruikt voor andere verzoeken.

Viscositeit configureren

1. Navigeer in Viscosity naar Voorkeuren > Verbindingen > <uw verbinding> (sitespecifiek) > Netwerken > DNS-instellingen.
2. Selecteer Automatisch (standaard).



115013433283

Wanneer u een OpenVPN-server gebruikt, moet u ervoor zorgen dat persistent-tun niet aan de serverzijde is ingeschakeld om ervoor te zorgen dat netwerkwijzigingen worden geactiveerd bij het verbreken of opnieuw verbinden.

Tunnelblick

Tunnelblick heeft twee wijzigingen nodig:

- Sta het wijzigen van de DNS-servers voor de adapter toe.
- Pas DNS-instellingen toe nadat de tunnel tot stand is gebracht.

Door de instellingen in het menu Geavanceerd te garanderen, werkt Tunnelblick samen met de Umbrella Roaming Client:

Schakel op het tabblad Verbinden en verbreken de volgende twee instellingen in:

- DNS-cache doorspoelen na verbinding maken of verbreken (standaard)
- DNS instellen nadat routes zijn ingesteld in plaats van voordat routes zijn ingesteld

Wijzig op het tabblad Verbonden deze instelling in Negeren:

- DNS: Servers > Wanneer wijzigingen worden aangebracht in de pre-VPN-waarde, wanneer wijzigingen worden aangebracht in iets anders.

Wanneer u een OpenVPN-server gebruikt, moet u ervoor zorgen dat persistent-tun niet aan de serverzijde is ingeschakeld om ervoor te zorgen dat netwerkwijzigingen worden geactiveerd bij het verbreken of opnieuw verbinden.

Problemen met Tunnelblick VPN-verbinding verbreken

Bij sommige Tunnelblick-versies kan de roamingclient de juiste interne DNS-servers niet goed identificeren nadat de VPN-verbinding is verbroken. Als er problemen met Internal Domains optreden na het verbreken van de VPN-verbinding, raadt Umbrella de volgende stappen aan:

Deze wijziging zorgt ervoor dat Tunnelblick de primaire netwerkinterface naar beneden en omhoog brengt nadat de VPN-verbinding is verbroken. Dit wordt beheerd op het tabblad Instellingen van het configuratiescherm Tunnelblick:

- Gebruik in oudere versies van Tunnelblick (vóór 3.7.5beta03) het selectievakje Reset the primary interface after disconnecting (De primaire interface herstellen na het loskoppelen).
- Op nieuwere versies van Tunnelblick (3.7.5beta03 en hoger), stelt u zowel de On verwachte ontkoppeling en de On onverwachte ontkoppeling instellingen te Reset primaire interface.

raket met lichtsnelheid

Lightspeed Rocket heeft bepaalde functies die niet compatibel zijn met de roamingclient. Specifiek, de DNS-wijziging voor Geen SSL-zoekopdracht en SafeSearch CNAME-omleiding van www.google.com naar nosslsearch.google.com en forcesafesearch.com respectievelijk zorgt ervoor dat alle www.google.com DNS-resolutie mislukt zolang Lightspeed Rocket DNS-omleiding is ingeschakeld.



Opmerking: Dit artikel verwijst naar de zelfstandige Umbrella Roaming-client. Raadpleeg de relevante documentatie voor een begeleidend artikel over de Umbrella Roaming Security Module voor Cisco Secure Client en oudere software.

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.