Management der Umbrella Roaming Client- und VPN-Kompatibilität

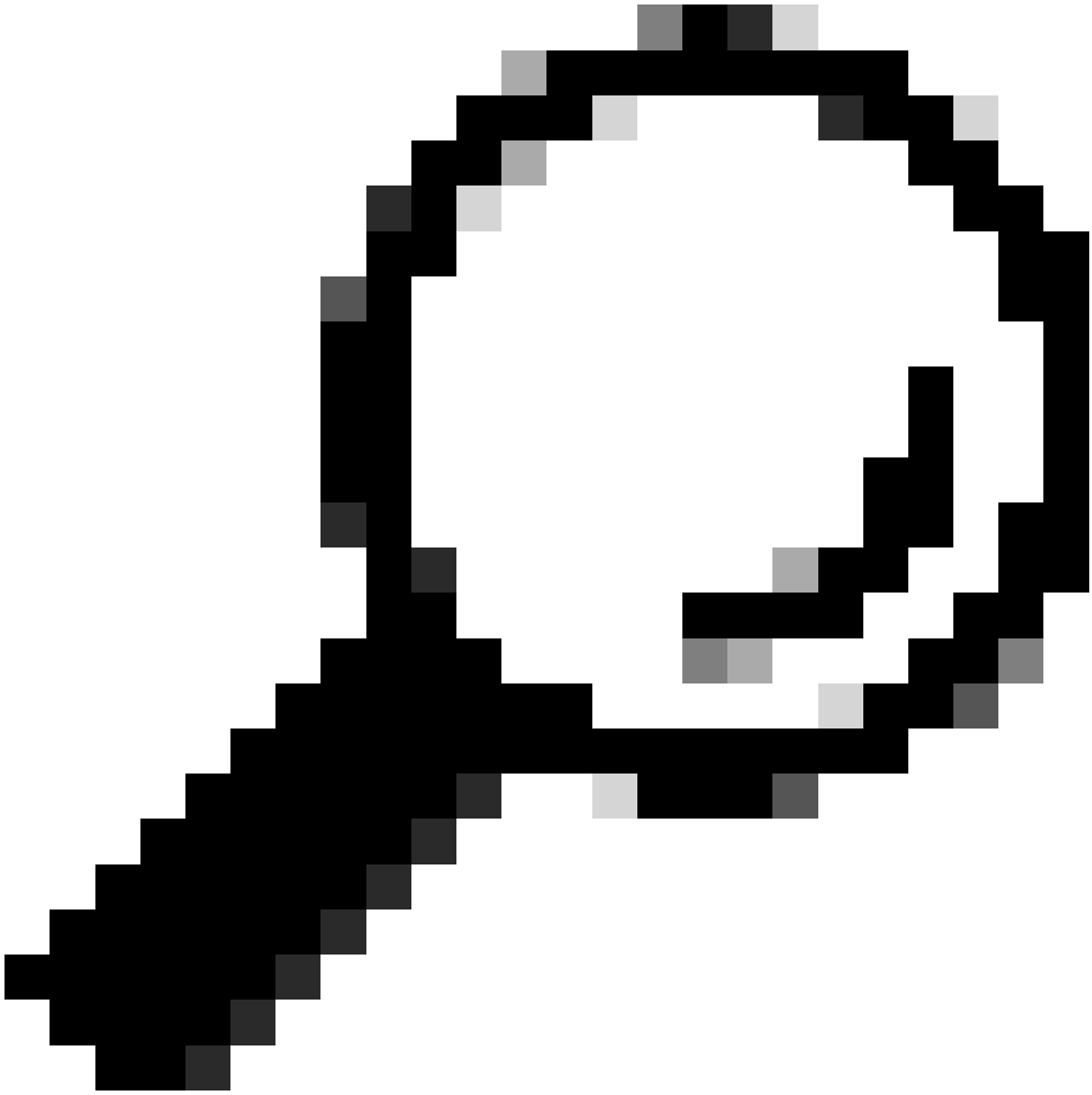
Inhalt

Einleitung

In diesem Dokument werden die Interaktion und Kompatibilität des Cisco Umbrella Roaming Client mit verschiedenen VPN-Software beschrieben.

Überblick

Der Cisco Umbrella Roaming Client kann mit den meisten VPN-Software verwendet werden, es können jedoch zusätzliche Schritte für den erwarteten Betrieb erforderlich sein. Cisco Umbrella empfiehlt für maximale Kompatibilität die Bereitstellung des Cisco Secure Client und Roaming Security-Moduls. Dieses Modul kann ohne die VPN-Komponenten bereitgestellt werden.



Tipp: Dieses Dokument dient als allgemeine Anleitung und nicht als offizielle Liste unterstützter Software. Cisco Umbrella testet, validiert oder zertifiziert keine Funktionalität mit Software oder VPN-Clients von Drittanbietern.

Dieses Dokument enthält technische Informationen und zusätzlichen Kontext für spezifische VPN-Clients, die weitere Konfigurationen erfordern können. Eine Liste der bekannten inkompatiblen VPN-Software finden Sie im Abschnitt Inkompatibilitäten des Umbrella Roaming Client. Die DNS-Inkompatibilität mit dem Roaming-Client kann auch dazu führen, dass das Cisco Secure Client + Roaming Security-Modul mit der SWG ausfällt, da der SWG-Client ebenfalls vom erfolgreichen Aufbau einer DNS-Verbindung abhängt.

Wie der Umbrella Roaming Client mit VPN Clients funktioniert

Der Umbrella Roaming Client wird an alle Netzwerkadapter gebunden und ändert die DNS-Einstellungen auf dem Computer in 127.0.0.1 (localhost). Auf diese Weise kann der Umbrella Roaming Client alle DNS-Anfragen direkt an Umbrella weiterleiten und gleichzeitig die Auflösung lokaler Domänen über die Funktion Interne Domänen ermöglichen. Beim Herstellen einer Verbindung mit einem VPN-Server erkennt der Umbrella Roaming Client eine neue Netzwerkverbindung im System und ändert die DNS-Einstellungen der Verbindung so, dass sie auf den Umbrella Roaming Client zeigen. Der Umbrella Roaming Client benötigt DNS-Abfragen von Umbrella AnyCast DNS-IP-Adressen (208.67.222.222/208.67.220.220).

Wenn ein Benutzer eine Verbindung zu einem VPN herstellt, muss die mit dem VPN verknüpfte Firewall den Zugriff auf Umbrella zulassen.

Inkompatibilitäten des Umbrella Roaming Client

Der Umbrella Roaming Client stellt derzeit die Durchsetzung auf DNS-Ebene bereit. Die DNS-Schicht ist die Hauptfunktion des Roaming-Clients und wendet DNS-basierte Sicherheitsrichtlinien auf alle Netzwerke an. Bei dieser Funktion des Roaming-Clients können bekannte Software-Inkompatibilitäten auftreten. Die DNS-Ebene des Umbrella Roaming Client ist mit den unten aufgeführten Clients aufgrund von Support-Team-Tests nicht kompatibel. Cisco Umbrella Engineering überprüft oder testet diese Clients nicht, und alle Einträge werden überprüft. Dieser Artikel bezieht sich auf den eigenständigen Umbrella Roaming Client. Einen Begleitartikel zum Umbrella Roaming Security Module für Cisco Secure Client (und zu älteren Versionen) finden Sie in der entsprechenden Dokumentation.

VPN-Client	Problem/Inkompatibilität	Auflösung
Pulssicherheit	Wenn die Verbindung getrennt wird, kann der gespeicherte lokale DNS aufgrund der Pulsänderung während der VPN-Verbindung VPN-Werte anstelle von WiFi-/Ethernet-Werten beibehalten.	Auflösbar mit dem Umbrella-Modul - enthalten in den meisten Lizenzen.
Avaya VPN	Inkompatibel.	Auflösbar mit dem Umbrella-Modul - enthalten in den meisten Lizenzen.
Windows VPN (insbesondere Always On VPN)	Dies kann dazu führen, dass der lokale DNS nicht in die interne Antwort aufgelöst werden kann, obwohl die DNS-Hostnamen in der Liste der internen Domänen aufgeführt sind.	Auflösbar mit dem Umbrella-Modul - enthalten in den meisten Lizenzen.
VPN-"Apps", die auf der universellen	Diese Apps müssen eine Microsoft-Verbindungs-API verwenden, für die DNS an die lokale Netzwerkkarte und	Auflösbar mit dem Umbrella-Modul - enthalten in den meisten Lizenzen.

VPN-Client	Problem/Inkompatibilität	Auflösung
Windows-Plattform aufbauen	nicht an 127.0.0.1 gesendet werden muss. Daher zeigt die App einen Fehler an, der darauf hinweist, dass sie keine Verbindung herstellen kann.	
OffenVPN	Inkompatibel.	Kein Fix verfügbar.
Palo Alto GlobalProtect VPN	Funktioniert nicht mit einer Standalone-Version des Roaming-Clients nach 3.0.110.	Behoben durch Verwendung des Umbrella-Moduls - enthalten in den meisten Lizenzen.
F5-VPN	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.
Checkpoint-VPN	macOS Only, Split-tunnel mode only.	Split-Tunnel unter macOS deaktivieren.
SonicWall NetExtender	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.
Zscaler-VPN	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.
Akamai-Endpunktschutz (ETP-Client)	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.
NordVPN	Problemumgehung verwenden.	Es gibt zwei Optionen zum Hinzufügen der Kompatibilität: 1. Verwenden Sie die OpenVPN-Verbindungsmethode, wie unter So richten Sie eine manuelle Verbindung unter Windows mithilfe von OpenVPN ein 2. Benutzerdefinierten DNS unter den erweiterten Einstellungen zulassen. Legen Sie DNS auf

VPN-Client	Problem/Inkompatibilität	Auflösung
		208.67.220.220 und 208.67.222.222 fest.
Azure-VPN	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.
AWS-VPN	Problemumgehung verwenden.	Bearbeiten Sie die Konfigurationsdatei (manuell von AWS heruntergeladen), um eine zweite Zeile mit`pull-filter ignore "block-outside-dns"`zu erhalten.
Pritunl VPN	Inkompatibel.	Behoben durch das Umbrella-Modul - in den meisten Lizenzen enthalten.

Gründe für die Inkompatibilität von VPN-Clients

Einige VPN-Clients verhalten sich ähnlich wie der Umbrella Roaming Client. Wenn der DNS-Server für die VPN-Verbindung zu einem unerwarteten Wert wechselt, ändert die VPN-Software die DNS-Einstellungen des Systems wieder auf den Wert, den das VPN bei der ersten Verbindung festgelegt hat. Der Umbrella Roaming Client führt ebenfalls den gleichen Vorgang aus und ändert alle DNS-Server auf 127.0.0.1 zurück. Dieses Hin- und Herschalten führt zu einem Konflikt zwischen dem VPN und dem Umbrella Roaming Client. Dieser Konflikt verursacht einen endlosen Zyklus der DNS-Server für das Zurücksetzen der VPN-Verbindung. Der Roaming-Client erkennt dies und schaltet sich aus, um die VPN-Verbindung nach Möglichkeit aufrechtzuerhalten.

Virtuelle Appliances und geschützte Netzwerke

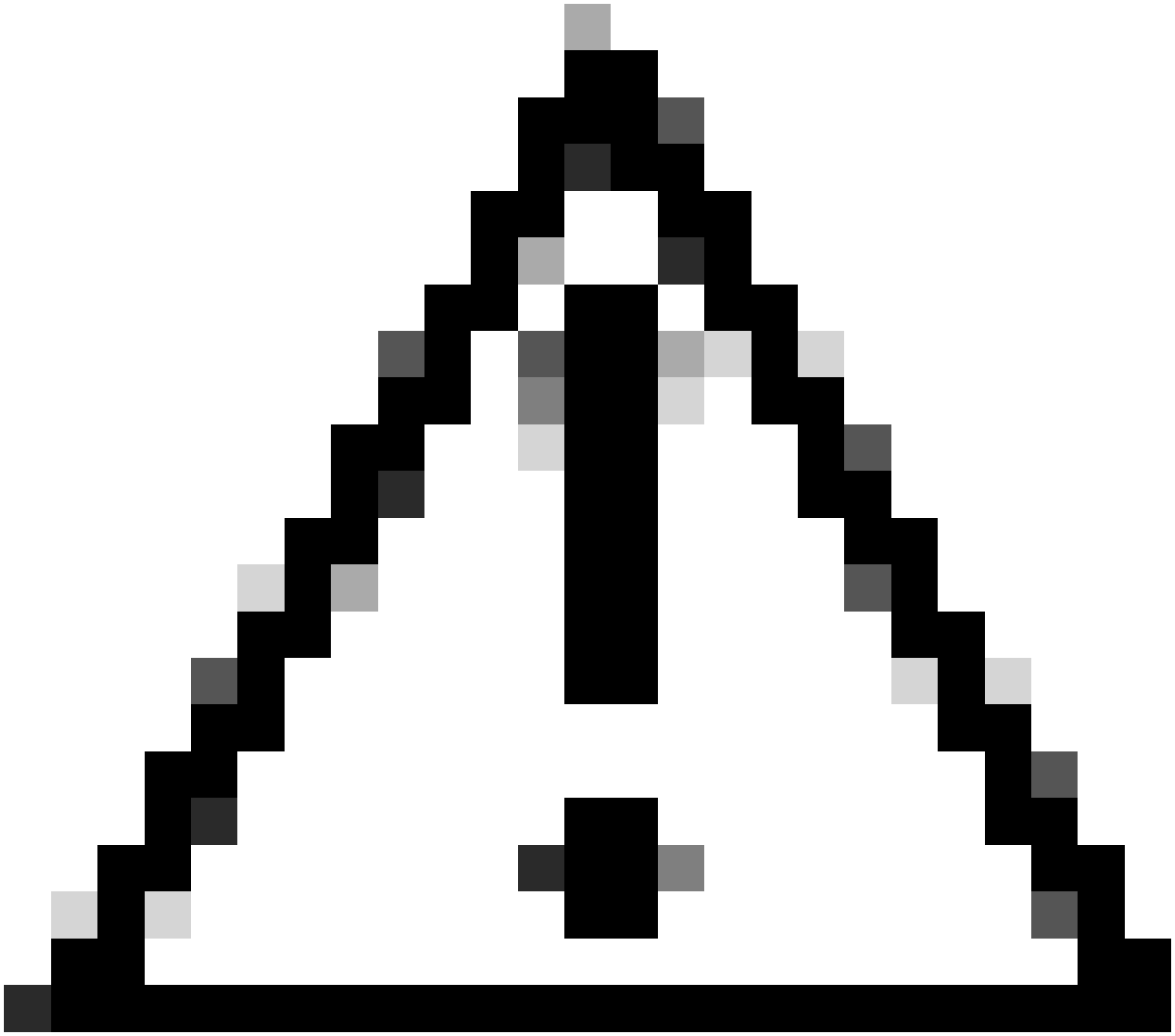
Der Umbrella-Roaming-Client verhält sich anders, wenn er mit einem Netzwerk verbunden ist, das die Umbrella Virtual Appliances (VA) oder die Funktion "Protected Networks" verwendet. Dies gilt unabhängig davon, ob ein Benutzer sich lokal oder über ein VPN mit dem Netzwerk verbindet. Weitere Informationen finden Sie in der Dokumentation zu Roaming-Client und virtuellen Appliances oder geschützten Netzwerken.

Besondere Überlegungen für ein eigenständiges und ein Cisco Secure Client + Roaming-Sicherheitsmodul

Die hier bereitgestellten Informationen beziehen sich auf den eigenständigen Umbrella Roaming Client und gelten nicht für den Cisco Secure Client (CSC) + das Roaming Security Module. Benutzer, die eine einfache Plugin-Installation wünschen, können Umbrella Roaming in CSC

integriert verwenden. Cisco Secure Client VPN-Benutzer müssen zum CSC + Roaming Security Module migrieren, wenn ein funktionelles Problem mit dem VPN auftritt. Cisco Umbrella muss auf dem CSC- und Roaming-Sicherheitsmodul validiert werden und empfiehlt eine vollständige Migration.

Die Cisco Secure Client VPN-Software bietet Optionen für den Umgang des Systems mit DNS, wenn eine VPN-Verbindung hergestellt wird. Weitere Informationen finden Sie im Artikel Verhaltensunterschiede bei DNS-Abfragen und Domänennamenauflösung in verschiedenen Betriebssystemen. Diese Informationen basieren auf Erfahrungen mit dem Cisco Secure Client und dem Umbrella Roaming Client. Es wird empfohlen, den Umbrella-Roaming-Client mit aktiviertem Cisco Secure Client VPN zu testen, um die erwarteten internen und externen DNS-Auflösungsfunktionen sicherzustellen.



Vorsicht: Wenn Sie den Cisco Secure Client aus Gründen der DNS-Servicekompatibilität ebenfalls verwenden, müssen Sie das CSC + Roaming Security Module verwenden. Die angegebenen Schritte gelten nur für den nicht integrierten Roaming-Client, wenn dies

---

erforderlich ist. Diese Schritte sind für das CSC + Roaming Security Module nicht erforderlich.

Sowohl im Voll- als auch im Split-Tunnelmodus sind spezielle Anweisungen erforderlich, damit der Roaming-Client während der Verbindung mit dem Cisco Secure Client funktionieren kann. Dies ist erforderlich, damit DNS zum Roaming-Client fließen kann, anstatt vom Kernel-Treiber überschrieben zu werden. Bei einem vollen Tunnel besteht das Symptom darin, dass der Client deaktiviert werden muss. Beim Split-Tunneling tritt ein Symptom auf, dass der interne DNS-Dienst verloren geht, während eine Verbindung zum VPN besteht.

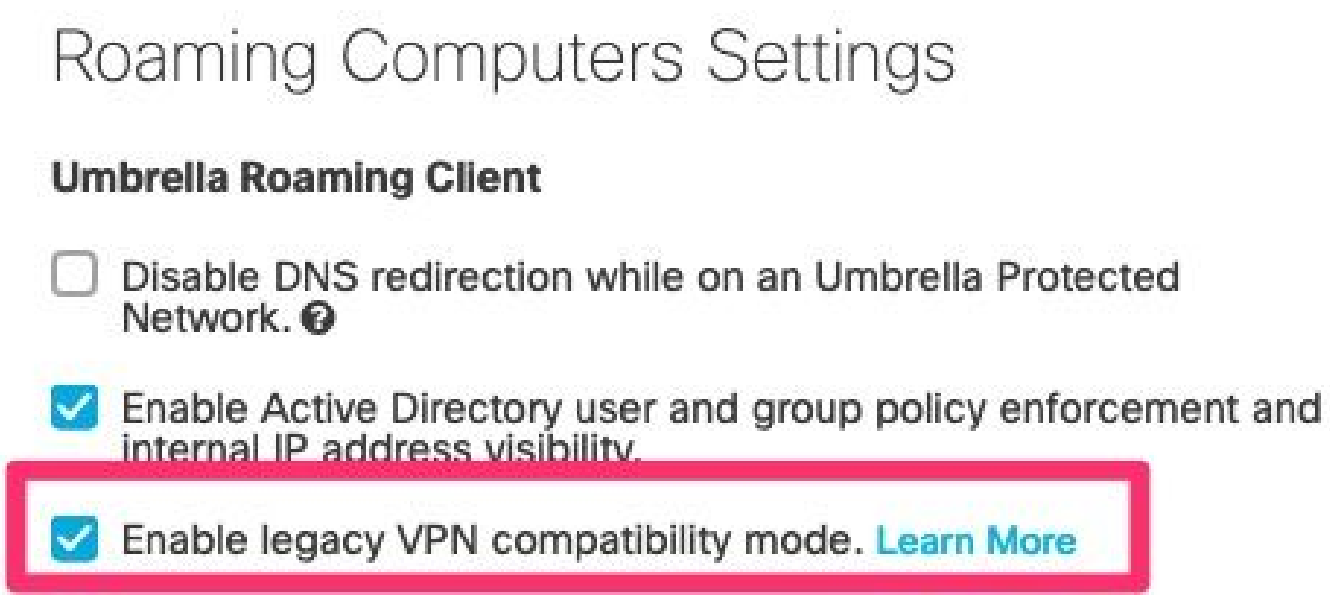
DNS Binding Order VPN-Kompatibilitätsmodus für Windows 10 und 11

Bei einer begrenzten Anzahl von Windows 10-Benutzern tritt ein spezielles Problem auf, bei dem das lokale LAN anstelle der VPN-NIC für DNS priorisiert wird. In diesem Fall kann der lokale DNS in der Liste der internen Domänen für den Roaming-Client nicht aufgelöst werden, während der öffentliche DNS problemlos funktioniert. Dies betrifft standardmäßig die Versionen 2.0.338 und 2.0.341 sowie alle späteren Versionen. Das Problem trat in Version 2.0.255 nicht auf.

Zu den zuvor betroffenen VPN-Clients gehören:

- AnyConnect 3.x
- AnyConnect 4.x (keine Auswirkungen auf AnyConnect Umbrella oder CSC + Roaming-Modul)
- Sophos-VPN
- Einige Palo Alto GlobalProtect Konfigurationen auf älteren Versionen
- WatchGuard Mobile VPN
- Shrew Soft VPN
- Barracuda VPN

Auflösung
Schalten Sie die Einstellung für den Roaming-Client Enable legacy VPN compatibility mode to enabled um.



360027547111

Führen Sie den Diagnosetest aus, und klicken Sie auf die Ergebnisse fürresolv.confs, um zu bestätigen, ob das Problem aufgetreten ist. Wenn der VPN-Adapter zuerst aufgeführt wird, hat das Problem keine Auswirkungen auf den Benutzer. Wenn der VPN-Adapter an zweiter Stelle aufgeführt wird, kann sich das Problem auf den Benutzer auswirken.

Beispiel einer Ausgabe von resolv.config

```
Results for: resolv.confs
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
```

Besondere Überlegungen für VPNs von Drittanbietern

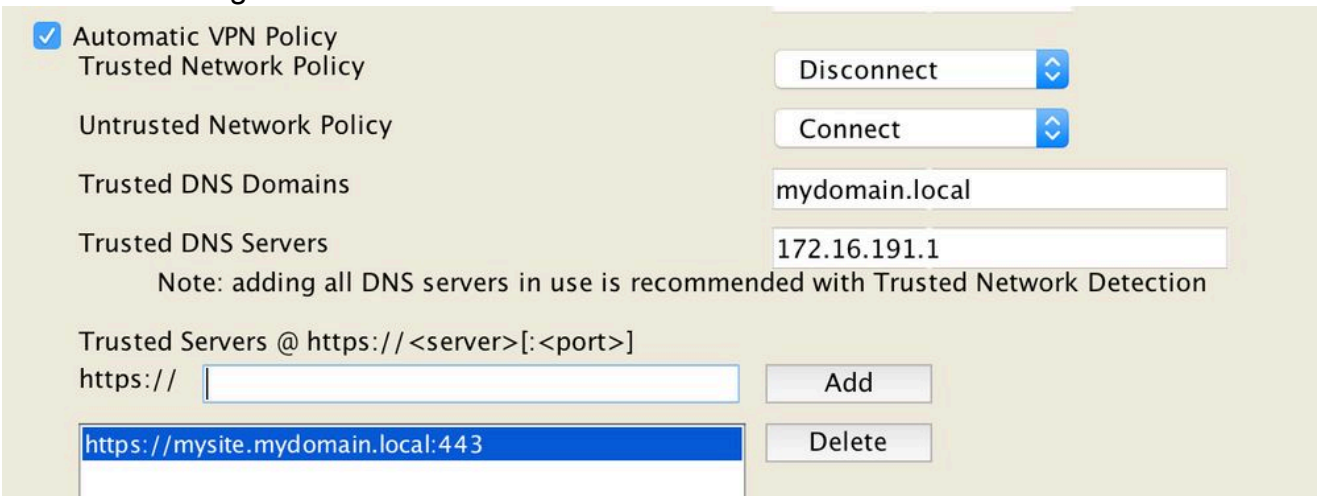
Stets verfügbares VPN

Der Standalone-Roaming-Client ist nicht mit der Cisco Secure Client Always On VPN-Einstellung kompatibel, wenn vertrauenswürdige DNS-Server definiert sind. Wenn der Standalone-Roaming-Client aktiv ist, setzt er DNS immer auf 127.0.0.1, sodass alle vertrauenswürdigen DNS-Server aus den Netzwerkkarteneinstellungen entfernt werden. Der Roaming-Client kann im Netzwerk

deaktiviert werden, um die DHCP-Einstellungen wiederherzustellen. Alle mit dem Roaming-Client zusammenhängenden Schutzmaßnahmen werden jedoch nach der Konfiguration aufgehoben. Wenden Sie sich an den Umbrella Support, um mehr über die Deaktivierung des Clients in einem vertrauenswürdigen Netzwerk zu erfahren.

Lösungen

- Das CSC + Roaming Security Module (Roaming Client für Cisco Secure Client) ist nicht betroffen und funktioniert mit einer automatischen VPN-Richtlinie effektiv.
- Fügen Sie 127.0.0.1 zur Liste der vertrauenswürdigen DNS-Server hinzu.
- Stellen Sie sicher, dass alternative Methoden der vertrauenswürdigen Erkennung definiert werden (DNS-Namen und Server), um zu verhindern, dass alle Netzwerke als vertrauenswürdig deklariert werden.



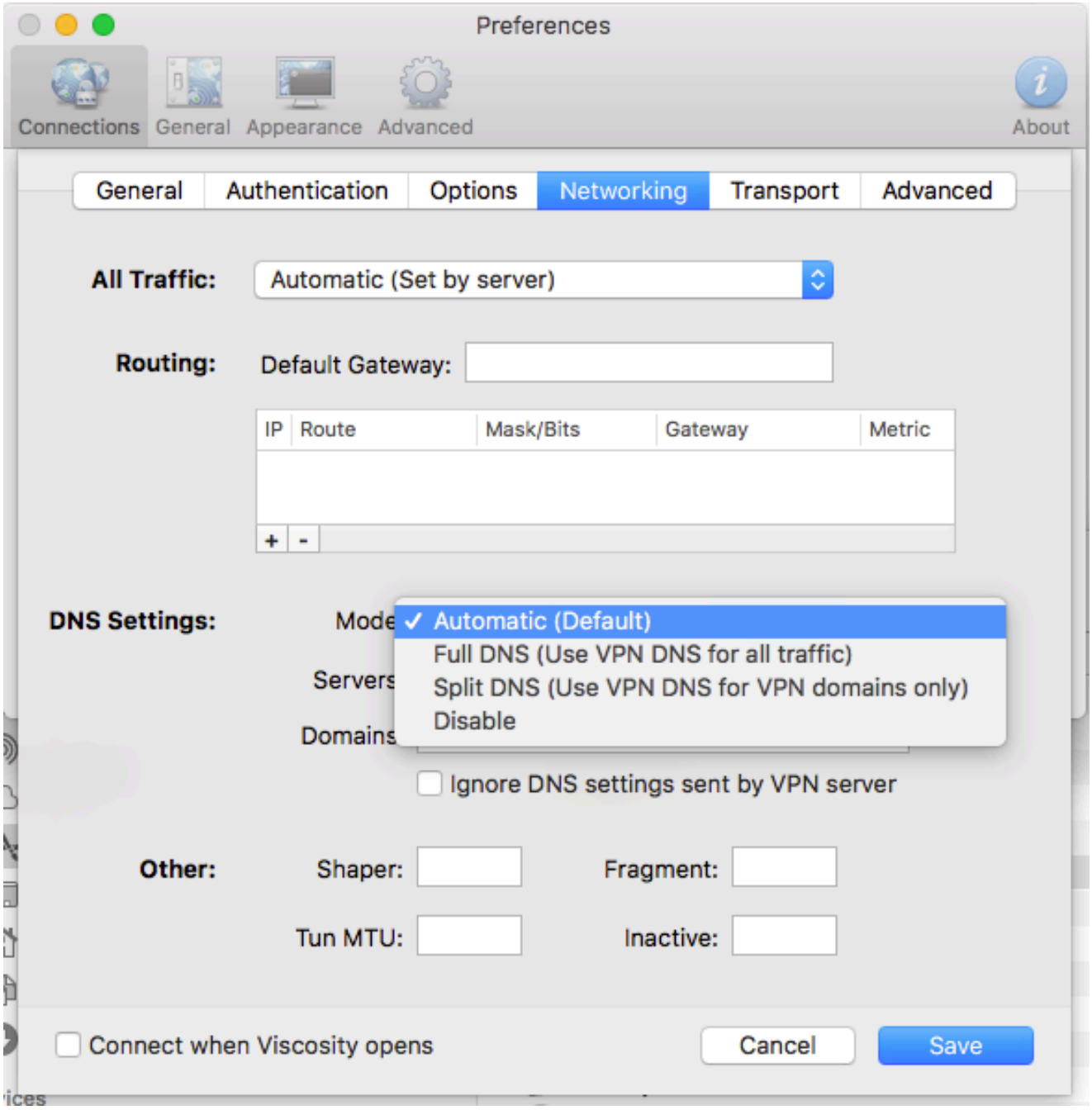
360031250911

Viskosität VPN

Viscosity-VPN erfordert eine Änderung der Einstellungen, um mit dem Umbrella-Roaming-Client zu funktionieren. Wenn diese Änderung nicht vorgenommen wird, entspricht das Standardverhalten der Viskosität dem anderer inkompatibler VPNs. Mit dieser Änderung wird "Viskosität" angewiesen, die DNS-Einstellungen, die über den Umbrella-Server übertragen werden, für alle Domänen in der Suchdomäne zu verwenden. 127.0.0.1 wird weiterhin für alle anderen Anforderungen verwendet.

Konfigurieren der Viskosität

1. Navigieren Sie unter Viskosität zu Einstellungen > Verbindungen > <Ihre Verbindung> (standortspezifisch) > Netzwerk > DNS-Einstellungen.
2. Wählen Sie Automatisch (Standard) aus.



115013433283

Wenn Sie einen OpenVPN-Server verwenden, stellen Sie sicher, dass persist-tun nicht serverseitig aktiviert ist, um sicherzustellen, dass Netzwerkänderungen beim Trennen oder erneuten Herstellen der Verbindung ausgelöst werden.

Tunnelblick

Tunnelblick erfordert zwei Änderungen:

- Ändern der DNS-Server für den Adapter zulassen.
- Wenden Sie die DNS-Einstellungen an, nachdem der Tunnel eingerichtet wurde.

Tunnelblick funktioniert mit dem Umbrella Roaming Client, indem Sie die im Menü Advanced (Erweitert) angegebenen Einstellungen festlegen:

Aktivieren Sie auf der Registerkarte Verbindung und Trennung die folgenden beiden Einstellungen:

- DNS-Cache nach Verbindungsherstellung oder Verbindungstrennung leeren (Standard)
- DNS wird nach dem Festlegen von Routen und nicht vor dem Festlegen von Routen festgelegt

Ändern Sie auf der Registerkarte "Während verbunden" diese Einstellung zu Ignorieren:

- DNS: Server > Wenn sich der Wert vor dem VPN ändert, Wenn sich etwas Anderes ändert.

Wenn Sie einen OpenVPN-Server verwenden, stellen Sie sicher, dass persist-tun nicht serverseitig aktiviert ist, um sicherzustellen, dass Netzwerkänderungen beim Trennen oder erneuten Herstellen der Verbindung ausgelöst werden.

VPN-Verbindungsprobleme bei Tunnelblick

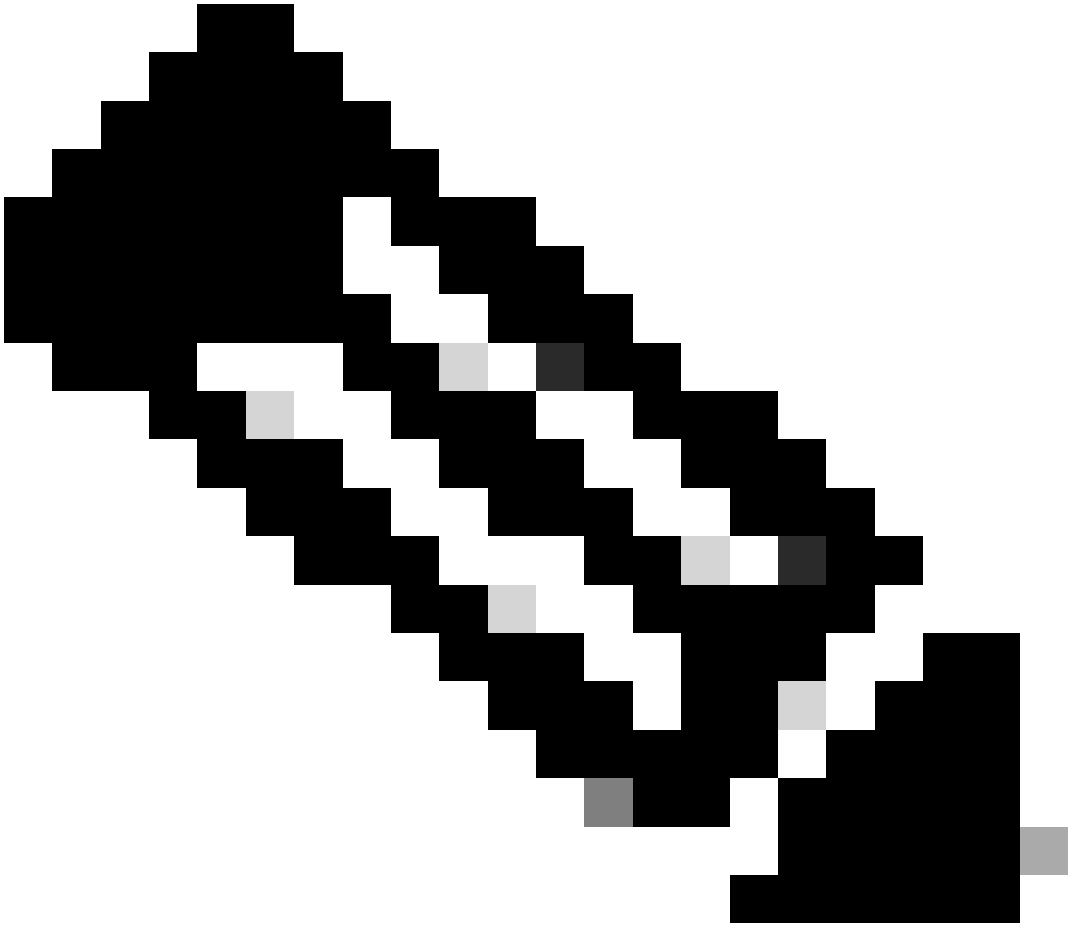
Bei einigen Tunnelblick-Versionen kann der Roaming-Client die richtigen internen DNS-Server nach einer VPN-Trennung nicht richtig identifizieren. Wenn nach einer VPN-Trennung Probleme mit internen Domänen auftreten, empfiehlt Umbrella die folgenden Schritte:

Diese Änderung bewirkt, dass Tunnelblick die primäre Netzwerkschnittstelle nach der VPN-Trennung ein- und ausschaltet. Dies wird auf der Registerkarte Einstellungen des Tunnelblick-Konfigurationspanels verwaltet:

- In älteren Versionen von Tunnelblick (vor 3.7.5beta03) verwenden Sie das Kontrollkästchen Primärschnittstelle nach Trennung zurücksetzen.
- Setzen Sie bei neueren Versionen von Tunnelblick (3.7.5beta03 und höher) sowohl die Einstellungen Bei erwartetem Verbindungsabbruch als auch Bei unerwartetem Verbindungsabbruch auf Primäre Schnittstelle zurücksetzen.

Leichtlaufrakete

Lightspeed Rocket verfügt über ausgewählte Funktionen, die nicht mit dem Roaming-Client kompatibel sind. Die DNS-Änderung für No SSL Search und die SafeSearch CNAME-Umleitung von `www.google.com` an nosslsearch.google.com bzw. führt forcesafesearch.com dazu, dass alle `www.google.com` DNS-Auflösung fehlschlägt, solange die Lightspeed Rocket DNS-Umleitung aktiviert ist.



Anmerkung: Dieser Artikel bezieht sich auf den eigenständigen Umbrella Roaming Client. Einen Begleitartikel zum Umbrella Roaming Security Module für Cisco Secure Client und zu Legacy-Software finden Sie in der entsprechenden Dokumentation.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.