# Umbrella Roaming 클라이언트 및 VPN 호환성 관리

## 목차

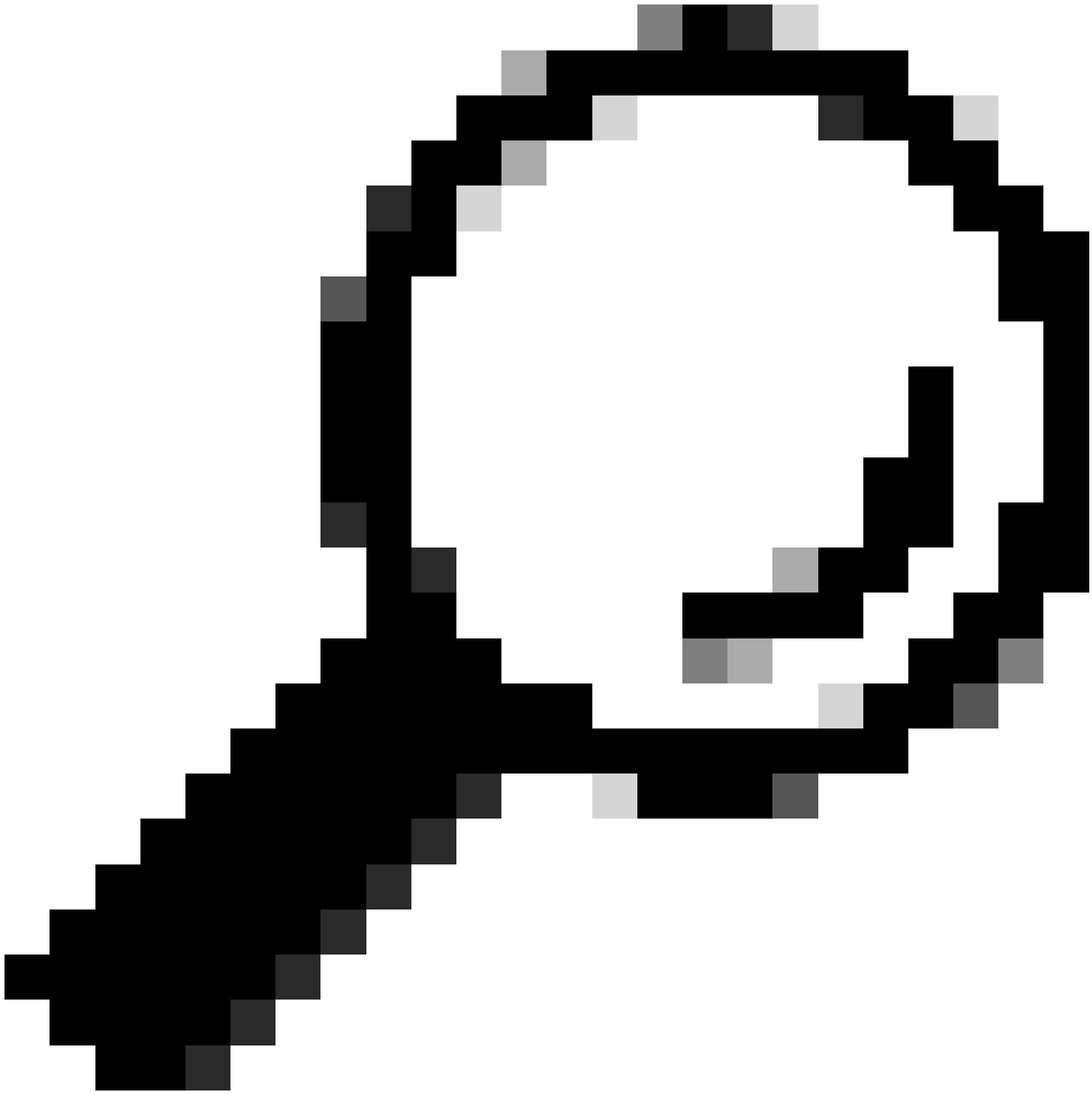


## 소개

이 문서에서는 Cisco Umbrella Roaming Client와 다양한 VPN 소프트웨어의 상호 작용 및 호환성에 대해 설명합니다.

## 개요

Cisco Umbrella Roaming Client는 대부분의 VPN 소프트웨어에서 작동하지만, 추가 단계는 예상된 작동에 필요할 수 있습니다. Cisco Umbrella는 호환성을 극대화하기 위해 Cisco Secure Client 및 Roaming Security 모듈을 구축할 것을 권장합니다. 이 모듈은 VPN 구성 요소 없이 구축할 수 있습니다.



팁: 이 문서는 일반적인 지침 역할을 하며 지원되는 소프트웨어의 공식적인 목록으로는 사용되지 않습니다. Cisco Umbrella는 서드파티 소프트웨어 또는 VPN 클라이언트에서 기능을 테스트, 검증 또는 인증하지 않습니다.

---

이 문서에서는 추가 컨피그레이션이 필요할 수 있는 특정 VPN 클라이언트에 대한 추가 컨텍스트 및 기술 정보를 제공합니다. 알려진 호환되지 않는 VPN 소프트웨어 목록은 Umbrella Roaming Client Incompatibility(Umbrella 로밍 클라이언트 비호환성) 섹션을 참조하십시오. 로밍 클라이언트와의 DNS 비호환성은 SWG를 사용하는 Cisco Secure Client + Roaming Security 모듈에 오류가 발생할 수도 있습니다. SWG 클라이언트도 DNS 연결을 성공적으로 설정해야 하기 때문입니다.

## Umbrella Roaming Client가 VPN 클라이언트에서 작동하는 방식

Umbrella Roaming Client는 모든 네트워크 어댑터에 바인딩하고 컴퓨터의 DNS 설정을

127.0.0.1(localhost)로 변경합니다. 이렇게 하면 Umbrella Roaming Client가 모든 DNS 쿼리를 Umbrella로 직접 전달하는 동시에 Internal Domains(내부 도메인) 기능을 통해 로컬 도메인을 확인할 수 있습니다. VPN 서버에 연결되면 Umbrella Roaming Client는 시스템에서 새 네트워크 연결을 탐지하고 Umbrella Roaming Client를 가리키도록 연결 DNS 설정을 변경합니다. Umbrella Roaming Client는 Umbrella AnyCast DNS IP 주소(208.67.222.222/208.67.220.220)에 대한 DNS 조회를 수행합니다.

사용자가 VPN에 연결하는 경우 VPN과 연결된 방화벽에서 Umbrella에 대한 액세스를 허용해야 합니다.

## Umbrella Roaming 클라이언트 비호환성

Umbrella Roaming Client는 현재 DNS 레이어 적용을 제공합니다. DNS 레이어는 로밍 클라이언트의 기본 기능으로, 모든 네트워크에 DNS 기반 보안 정책을 적용합니다. 로밍 클라이언트의 이 기능은 알려진 소프트웨어 비호환성을 경험할 수 있습니다. 지원 팀 테스트에 따르면 Umbrella Roaming Client의 DNS 레이어가 아래 나열된 클라이언트와 호환되지 않습니다. Cisco Umbrella Engineering에서는 이러한 클라이언트를 검증하거나 테스트하지 않으며, 모든 항목은 검토 대상이 됩니다. 이 문서에서는 독립형 Umbrella Roaming 클라이언트를 참조합니다. Umbrella Roaming Security Module for Cisco Secure Client(및 레거시)에 대한 관련 문서는 관련 문서를 참조하십시오.

| VPN 클라이언트 | 문제/비호환성 | 해결 |
|---|---|---|
| 펄스 보안 | 연결 해제 시 저장된 로컬 DNS는 VPN 연결 중 펄스 수정으로 인해 WiFi/이더넷 값이 아닌 VPN 값으로 유지될 수 있습니다. | Umbrella 모듈로 해결됨 - 대부분의 라이센스에 포함됨. |
| Avaya VPN | 호환되지 않습니다. | Umbrella 모듈로 해결됨 - 대부분의 라이센스에 포함됨. |
| Windows VPN(특히 Always On VPN) | DNS 호스트 이름이 내부 도메인 목록에 있음에도 불구하고 로컬 DNS가 내부 응답으로 확인되지 않을 수 있습니다. | Umbrella 모듈로 해결됨 - 대부분의 라이센스에 포함됨. |
| Windows 유니버설 플랫폼을 기반으로 구축된 VPN "앱" | 이러한 앱은 DNS를 127.0.0.1이 아니라 로컬 NIC로 보내야 하는 Microsoft 연결 API를 사용해야 합니다. 따라서 이 앱은 연결할 수 없음을 나타내는 오류를 표시합니다. | Umbrella 모듈로 해결됨 - 대부분의 라이센스에 포함됨. |
| OpenVPN | 호환되지 않습니다. | 사용할 수 있는 해결 방법이 없습니다. |

| VPN 클라이언트 | 문제/비호환성 | 해결 |
| --- | --- | --- |
| Palo Alto GlobalProtect VPN | 3.0.110 이후의 독립형 로밍 클라이언트 버전에서는 작동하지 않습니다. | 대부분의 라이센스에 포함된 Umbrella 모듈을 사용하여 수정되었습니다. |
| F5 VPN | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 라이센스에 포함됨. |
| 체크포인트 VPN | macOS만, 스플릿 터널 모드만 | macOS에서 스플릿 터널을 비활성화합니다. |
| SonicWall NetExtender | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 라이센스에 포함됨. |
| Zscaler VPN | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 라이센스에 포함됨. |
| Akamai 엔드포인트 보호(ETPclient) | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 라이센스에 포함됨. |
| NordVPN | 해결 방법을 사용합니다. | 호환성을 추가하기 위한 두 가지 옵션이 있습니다.<br>1. OpenVPN을 사용하여 Windows에서 수동 연결을 설정하는 방법에 설명된 대로 OpenVPN 연결 방법 사용<br>2. 고급 설정에서 사용자 지정 DNS를 허용합니다. DNS를 208.67.220.220 및 208.67.222.222로 설정합니다. |
| Azure VPN | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 라이센스에 포함됨. |
| AWS VPN | 해결 방법을 사용합니다. | 구성 파일(AWS에서 수동으로 다운로드)을 수정하여 두 번째 행을 pull-filter ignore "block-outside-dns"갖도록 합니다. |
| Pritunl VPN | 호환되지 않습니다. | Umbrella 모듈에서 수정됨 - 대부분의 |

| VPN 클라이언트 | 문제/비호환성 | 해결 |
| --- | --- | --- |
| | | 라이센스에 포함됨. |

## VPN 클라이언트의 비호환성 이유

일부 VPN 클라이언트에는 Umbrella Roaming Client와 유사한 DNS 동작이 있습니다. VPN 연결 DNS 서버가 예기치 않은 값으로 변경되면 VPN 소프트웨어는 시스템 DNS 설정을 처음 연결할 때 VPN이 설정한 값으로 다시 변경합니다. 또한 Umbrella Roaming Client는 동일한 작업을 수행하여 모든 DNS 서버를 127.0.0.1로 변경합니다. 이러한 왕복 동작은 VPN과 Umbrella Roaming Client 간에 충돌을 일으킵니다. 이러한 충돌로 인해 VPN 연결 재설정을 위한 DNS 서버가 끊임없이 순환합니다. 로밍 클라이언트는 이를 감지하고 가능한 경우 VPN 연결을 유지하기 위해 자신을 비활성화합니다.

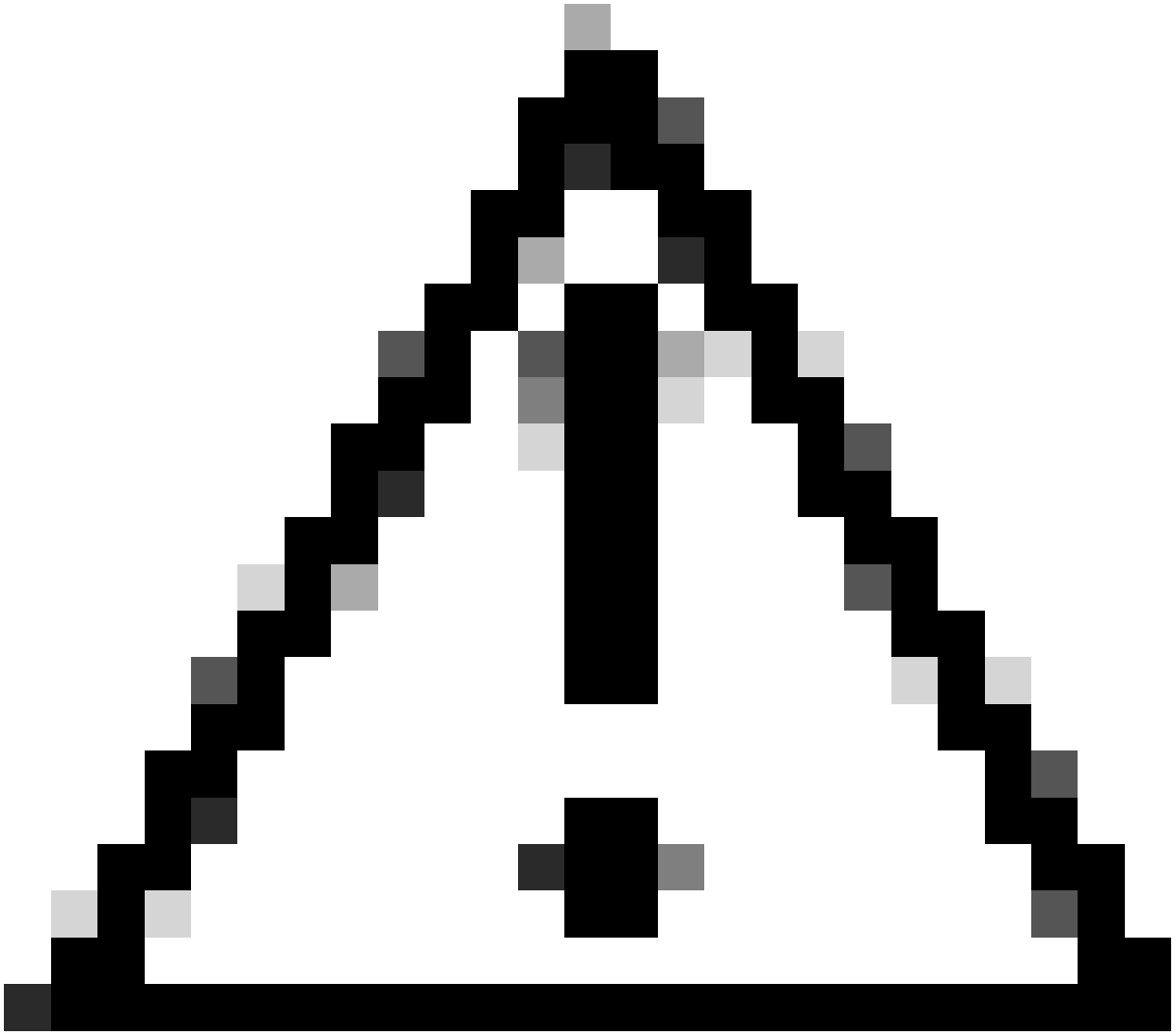
## 가상 어플라이언스 및 보호된 네트워크

Umbrella 로밍 클라이언트는 Umbrella VA(Virtual Appliance) 또는 Protected Networks 기능을 사용하는 네트워크에 연결될 때 다르게 작동합니다. 이는 사용자가 네트워크에 로컬로 연결하거나 VPN을 통해 연결하는지 여부에 따라 적용됩니다. 자세한 내용은 Roaming Client and Virtual Appliances 또는 Protected Networks 설명서를 참조하십시오.

## 독립형 및 Cisco Secure Client + Roaming Security Module의 특별 고려 사항

여기서 제공하는 정보는 독립형 Umbrella Roaming Client에 대한 것이며 Cisco Secure Client(CSC) + Roaming Security Module로 확장되지 않습니다. 쉬운 플러그인 설치를 원하는 사용자는 CSC에 통합된 Umbrella Roaming을 사용할 수 있습니다. VPN에 기능 문제가 발생하는 경우 Cisco Secure Client VPN 사용자는 CSC + Roaming Security Module로 마이그레이션해야 합니다. Cisco Umbrella는 CSC + Roaming Security Module에 대한 검증을 필요로 하며 완전한 마이그레이션을 권장합니다.

Cisco Secure Client VPN 소프트웨어는 VPN 연결이 설정될 때 시스템이 DNS를 처리하는 방법에 대한 옵션을 제공합니다. 자세한 내용은 다른 OS의 DNS 쿼리 및 도메인 이름 확인과 관련된 동작 차이 문서를 참조하십시오. 이 정보는 Cisco Secure Client 및 Umbrella Roaming Client를 사용한 경험을 기반으로 합니다. 내부 및 외부 DNS 확인이 예상대로 작동하도록 하려면 Cisco Secure Client VPN이 활성화된 Umbrella 로밍 클라이언트를 테스트하는 것이 좋습니다.



주의: DNS 서비스 호환성을 위해 Cisco Secure Client를 사용하는 경우에도 CSC + Roaming Security Module을 사용해야 합니다. 제공된 단계는 필요한 경우에만 비통합 로밍 클라이언트에 대한 것입니다. CSC + Roaming Security Module에는 이러한 단계가 필요하지 않습니다.

---

전체 및 스플릿 터널 모드 모두에서 Cisco Secure Client가 연결된 동안 로밍 클라이언트가 작동하도록 허용하는 특수 지침이 필요합니다. 이는 DNS가 커널 드라이버에 의해 재정의되지 않고 로밍 클라이언트로 이동할 수 있도록 하기 위해 필요합니다. 전체 터널의 경우 클라이언트가 강제로 비활성화되는 현상이 발생합니다. 스플릿 터널링의 경우 VPN에 연결된 상태에서 내부 DNS가 손실되는 현상이 발생합니다.

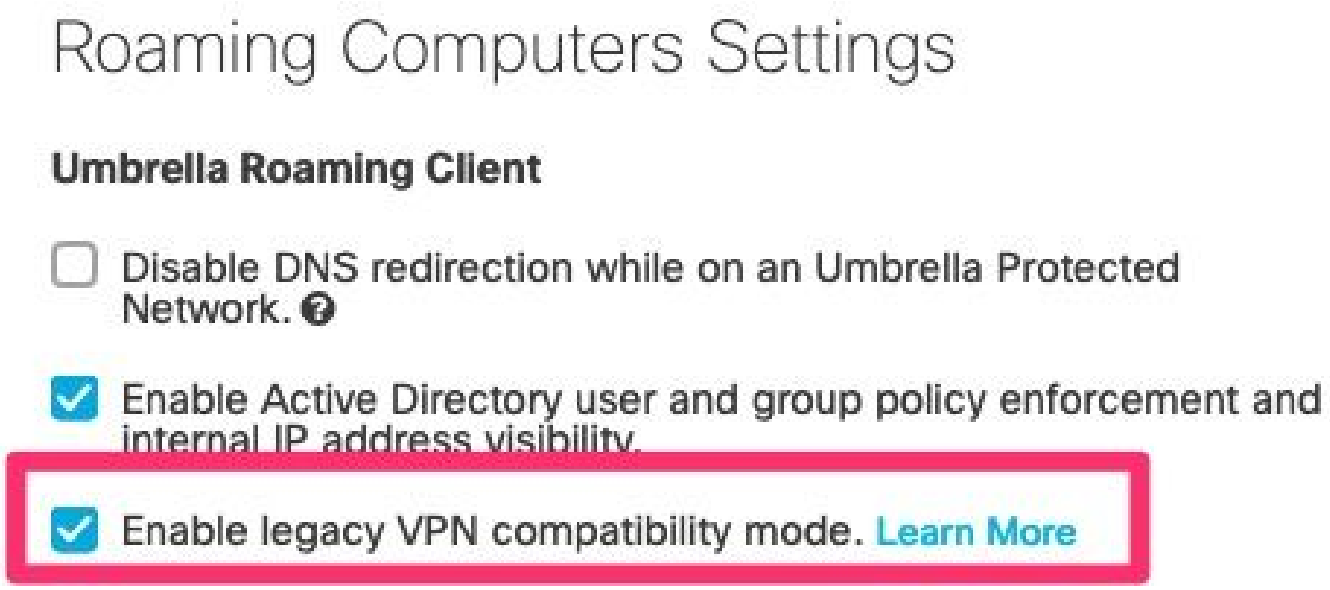
## Windows 10 및 11용 DNS 바인딩 순서 VPN 호환성 모드

제한된 Windows 10 사용자 집합에서 DNS용 VPN NIC 대신 로컬 LAN에 우선 순위를 지정하는 특정 문제가 발생합니다. 이 경우 공용 DNS가 문제 없이 작동하는 동안 로밍 클라이언트의 내부 도메인 목록에 있는 로컬 DNS를 확인할 수 없습니다. 이는 버전 2.0.338 및 2.0.341(기본값) 및 모든 이후 버전에 영향을 줍니다. 버전 2.0.255에서 문제가 발생하지 않았습니다.

이전에 영향을 받은 VPN 클라이언트는 다음과 같습니다.

- AnyConnect 3.x
- AnyConnect 4.x(AnyConnect Umbrella 또는 CSC + 로밍 모듈은 영향을 받지 않음)
- Sophos VPN
- 일부 Palo Alto Global이전 버전의 컨피그레이션 보호
- WatchGuard Mobile VPN
- Shrew 소프트 VPN
- 바라쿠다 VPN

해결
Roaming Client(로밍 클라이언트) 설정 Enable legacy VPN compatibility mode(레거시 VPN 호환성 모드 활성화)를 enabled(활성화됨)로 전환합니다.




360027547111

이 문제가 있는지 확인하려면 진단 테스트를 실행하고 의 결과를 클릭하십시오resolv.confs. VPN 어댑터가 먼저 나열되면 사용자에게 영향을 주지 않습니다. VPN 어댑터가 두 번째로 나열되면 사용자에게 영향을 줄 수 있습니다.

resolv.confs 출력 예

```
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
```

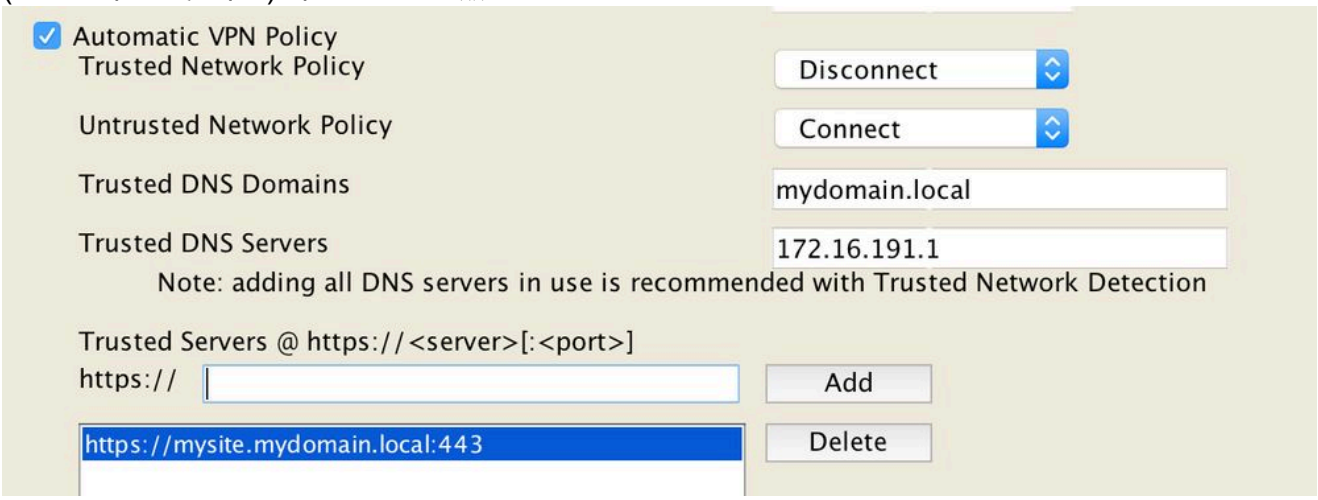
# 서드파티 VPN에 대한 특별 고려 사항

## Always-On VPN

신뢰할 수 있는 DNS 서버가 정의된 경우 독립형 로밍 클라이언트는 Cisco Secure Client Always On VPN 설정과 호환되지 않습니다. 활성 상태인 경우 독립형 로밍 클라이언트는 항상 DNS를 127.0.0.1로 설정하므로 NIC 설정에서 신뢰할 수 있는 DNS 서버가 모두 제거됩니다. DHCP 설정을 복원하기 위해 네트워크에서 로밍 클라이언트를 비활성화할 수 있습니다. 그러나 모든 로밍 클라이언트 관련 보호는 구성 시 중단됩니다. 신뢰할 수 있는 네트워크에서 클라이언트를 비활성화하는 방법에 대한 자세한 내용은 Umbrella 지원에 문의하십시오.

### 솔루션

- CSC + Roaming Security Module(Roaming Client for Cisco Secure Client)은 영향을 받지 않으며 자동 VPN 정책을 통해 효과적으로 작동합니다.
- 127.0.0.1을 신뢰할 수 있는 DNS 서버 목록에 추가합니다.
- 모든 네트워크가 신뢰할 수 있는 것으로 선언되지 않도록 신뢰할 수 있는 탐지의 대체 방법(DNS 이름 및 서버)이 정의되어 있는지 확인합니다.



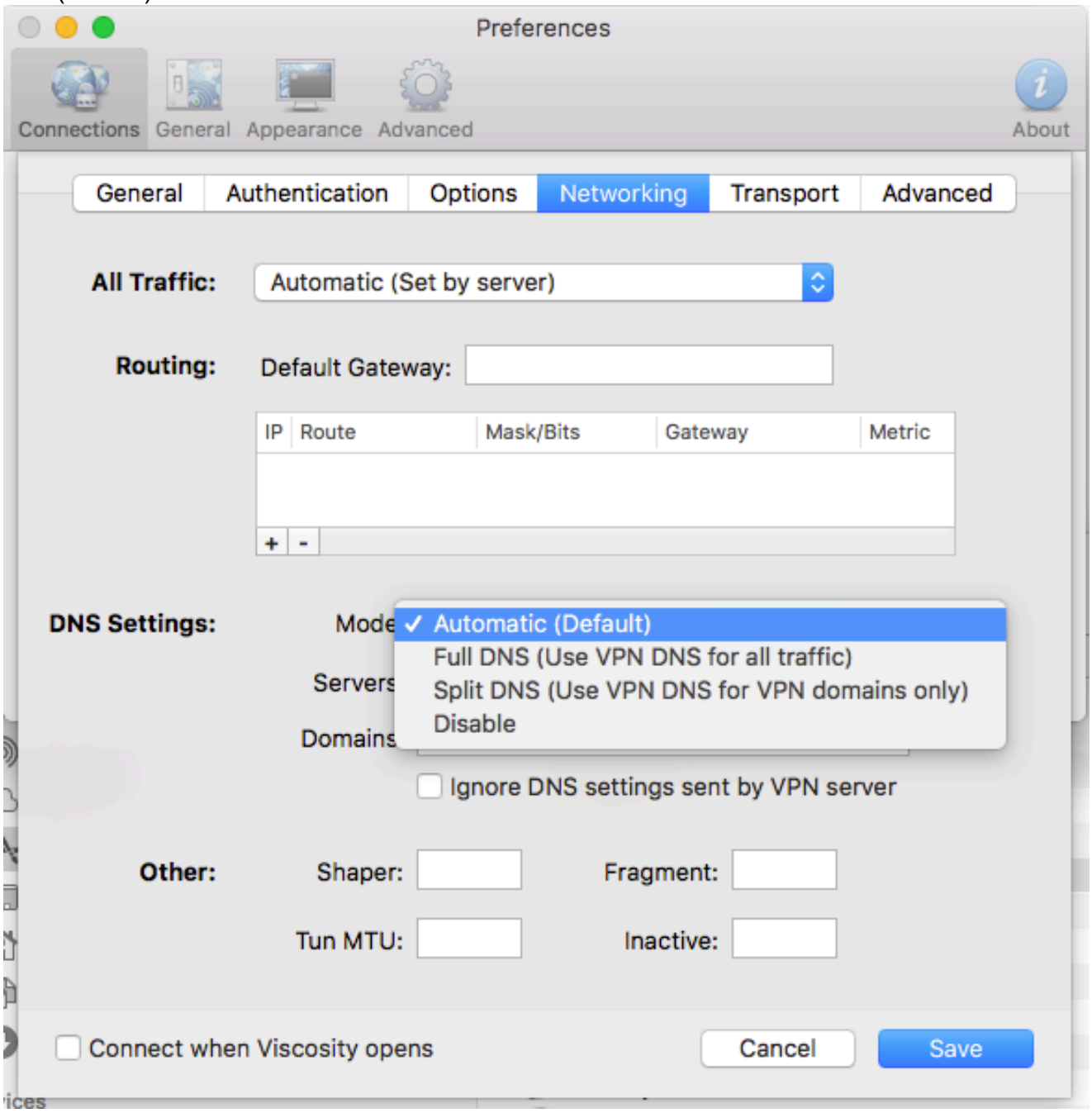

360031250911

## 점도 VPN

Viscosity VPN이 Umbrella 로밍 클라이언트와 작동하려면 설정을 변경해야 합니다. 이러한 변경이 이루어지지 않으면 Viscosity 기본 동작은 호환되지 않는 다른 VPN과 유사한 동작입니다. 이 변경 사항은 Viscosity가 검색 도메인의 모든 도메인에 대해 Umbrella 서버를 통해 푸시된 DNS 설정을 사용하도록 지시하며, 127.0.0.1은 다른 요청에도 계속 사용됩니다.

점도 구성

1. Viscosity(점도)에서 Preferences(환경 설정) > Connections(연결) > <your connection> (site specific) > Networking(네트워킹) > DNS Settings(DNS 설정)로 이동합니다.
2. 자동(기본값)을 선택합니다.




115013433283

OpenVPN 서버를 사용할 때 연결 끊기 또는 재연결 시 네트워크 변경이 트리거되도록 서버 측에서 persist-tun이 활성화되지 않았는지 확인합니다.

## 튠넬블리크

Tunnelblick을 사용하려면 다음 두 가지 사항을 변경해야 합니다.

- 어댑터의 DNS 서버 변경을 허용합니다.

- 터널이 설정된 후 DNS 설정을 적용합니다.

Tunnelblick은 Advanced(고급) 메뉴에서 제공된 설정을 확인하면 Umbrella Roaming Client(Umbrella 로밍 클라이언트)와 함께 작동합니다.

연결 및 연결 끊기 탭에서 다음 두 설정을 활성화합니다.

- 연결 또는 연결 해제 후 DNS 캐시 플러시(기본값)
- 경로를 설정하기 전 대신 경로를 설정한 후 DNS 설정

While Connected(연결된 동안) 탭에서 이 설정을 Ignore(무시)로 변경합니다.

- DNS: Servers(서버) > When changes to the pre-VPN value(VPN 이전 값으로 변경할 경우), When changes to anything(다른 값으로 변경할 경우).

OpenVPN 서버를 사용할 때 네트워크 변경 사항이 연결 끊기 또는 재연결 시 트리거되도록 서버 측에서 persist-tun이 활성화되지 않았는지 확인합니다.

## Tunnelblick VPN 연결 끊기 문제

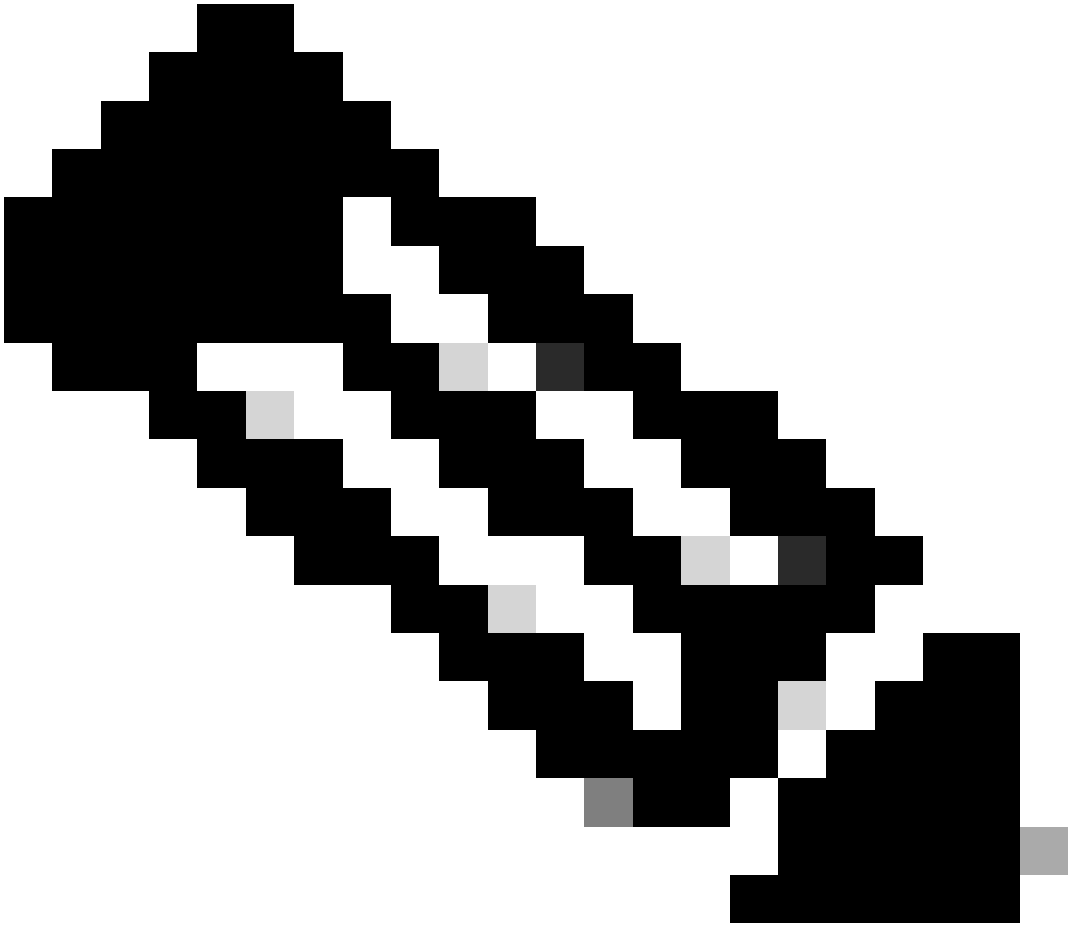
일부 Tunnelblick 버전에서는 VPN 연결 끊기 후 로밍 클라이언트가 올바른 내부 DNS 서버를 제대로 식별할 수 없습니다. VPN 연결 끊기 후 내부 도메인에 문제가 발생하면 Umbrella는 다음 단계를 권장합니다.

이 변경으로 인해 Tunnelblick은 VPN 연결이 끊어진 후 기본 네트워크 인터페이스를 중단하거나 가동합니다. Tunnelblick 컨피그레이션 패널의 Settings 탭에서 관리합니다.

- 이전 버전의 Tunnelblick(3.7.5beta03 이전)에서는 Reset the primary interface after disconnecting(연결을 끊은 후 기본 인터페이스 재설정) 확인란을 사용합니다.
- 최신 버전의 Tunnelblick(3.7.5beta03 이상)에서는 On expected disconnect와 On expected disconnect 설정을 모두 Reset Primary Interface(기본 인터페이스 재설정)로 설정합니다.

## 광속 로켓

Lightspeed Rocket에는 로밍 클라이언트와 호환되지 않는 일부 기능이 있습니다. nosslsearch.google.com 특히, www.google.com의 No SSL Search 및 SafeSearch CNAME 리디렉션에 대한 DNS 수정은 Lightspeed Rocket DNS 리디렉션이 활성화된 경우 모든 `www.google.com` DNS 확인이 forcesafesearch.com 실패하게 합니다.



참고: 이 문서에서는 독립형 Umbrella Roaming 클라이언트를 참조합니다. Umbrella Roaming Security Module for Cisco Secure Client and legacy software에 대한 관련 문서는 관련 문서를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.