Gerenciar compatibilidade de cliente de roaming Umbrella e VPN

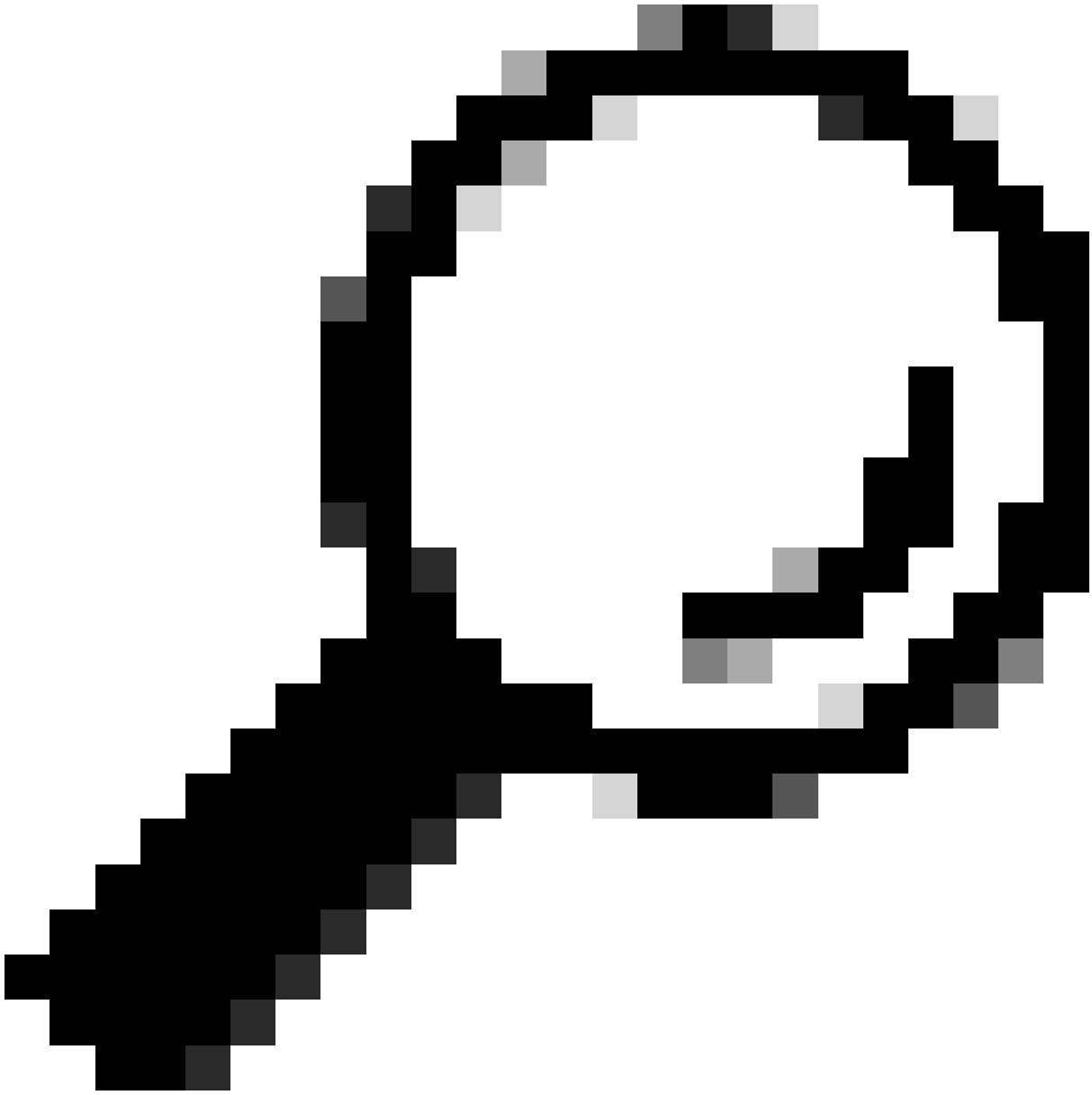
Contents

Introdução

Este documento descreve a interação e a compatibilidade do Cisco Umbrella Roaming Client com vários softwares de VPN.

Overview

O Cisco Umbrella Roaming Client funciona com a maioria dos softwares de VPN, mas etapas adicionais podem ser necessárias para a operação esperada. O Cisco Umbrella recomenda a implantação do módulo Cisco Secure Client and Roaming Security para máxima compatibilidade. Este módulo pode ser implantado sem os componentes VPN.



Tip: Este documento serve como orientação geral e não serve como uma lista oficial de softwares suportados. O Cisco Umbrella não testa, valida ou certifica a funcionalidade com nenhum software de terceiros ou cliente VPN.

Este documento fornece informações técnicas e contexto adicional para clientes VPN específicos que podem exigir configurações adicionais. Para obter uma lista de softwares de VPN incompatíveis conhecidos, consulte a seção Incompatibilidades do cliente de roaming Umbrella. A incompatibilidade de DNS com o cliente de roaming também pode fazer com que o Cisco Secure Client + módulo de segurança de roaming com SWG falhe, pois o cliente SWG também depende do estabelecimento bem-sucedido de uma conexão DNS.

Como o cliente Umbrella Roaming opera com clientes VPN

O Umbrella Roaming Client vincula-se a todos os adaptadores de rede e altera as configurações DNS no computador para 127.0.0.1 (localhost). Isso permite que o cliente de roaming Umbrella encaminhe todas as consultas DNS diretamente para o Umbrella enquanto permite a resolução de domínios locais através do recurso Domínios internos. Ao estabelecer uma conexão com um servidor VPN, o cliente de roaming Umbrella detecta uma nova conexão de rede no sistema e altera as configurações DNS da conexão para apontar para o cliente de roaming Umbrella. O cliente de roaming Umbrella depende da realização de pesquisas de DNS nos endereços IP DNS do AnyCast Umbrella (208.67.222.222/208.67.220.220).

Se um usuário se conectar a uma VPN, o firewall associado à VPN deverá permitir acesso ao Umbrella.

Incompatibilidades de cliente de roaming Umbrella

O cliente Umbrella Roaming atualmente aplica a camada DNS. A camada DNS é a função principal do cliente de roaming, aplicando políticas de segurança baseadas em DNS em qualquer rede. Essa função do cliente de roaming pode ter incompatibilidades de software conhecidas. A camada DNS do cliente Umbrella Roaming é incompatível com os clientes listados abaixo, com base no teste da equipe de suporte. A Cisco Umbrella Engineering não verifica ou testa esses clientes, e todas as entradas estão sujeitas a revisão. Este artigo refere-se ao Umbrella Roaming Client autônomo. Para obter um artigo complementar sobre o Umbrella Roaming Security Module for Cisco Secure Client (e seu legado), consulte a documentação relevante.

Cliente de VPN	Problema/Incompatibilidade	Resolução
Pulso seguro	Na desconexão, o DNS local salvo pode permanecer como valores de VPN em vez de valores de WiFi/Ethernet devido à modificação de pulso durante a conexão VPN.	Resolvido com o módulo Umbrella - incluído na maioria das licenças.
VPN Avaya	Incompatível.	Resolvido com o módulo Umbrella - incluído na maioria das licenças.
VPN Windows (notavelmente a VPN Always On)	O DNS local pode falhar ao resolver para a resposta interna apesar dos nomes de host DNS estarem na lista de domínios internos.	Resolvido com o módulo Umbrella - incluído na maioria das licenças.
"aplicativos" de VPN criados sobre a plataforma universal do Windows	Esses aplicativos devem utilizar uma API de conexão da Microsoft que exige o envio de DNS para a NIC local, não 127.0.0.1. Portanto, o aplicativo exibe um erro indicando que não pode se conectar.	Resolvido com o módulo Umbrella - incluído na maioria das licenças.

Cliente de VPN	Problema/Incompatibilidade	Resolução
OpenVPN	Incompatível.	Nenhuma correção disponível.
Palo Alto GlobalProteger VPN	Não funciona com nenhuma versão de cliente de roaming autônomo posterior à 3.0.110.	Corrigido usando o módulo Umbrella - incluído na maioria das licenças.
VPN F5	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.
VPN de ponto de verificação	Somente macOS, somente modo de túnel dividido.	Desative o túnel dividido no MacOS.
SonicWall NetExtender	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.
VPN Zscaler	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.
Proteção de endpoint Akamai (ETPclient)	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.
NordVPN	Use uma solução alternativa.	Existem duas opções para adicionar compatibilidade: 1. Use o método de conexão OpenVPN conforme descrito em Como configurar uma conexão manual no Windows usando o OpenVPN 2. Permitir DNS personalizado nas configurações avançadas. Defina o DNS como 208.67.220.220 e 208.67.222.222.

Cliente de VPN	Problema/Incompatibilidade	Resolução
VPN do Azure	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.
AWS VPN	Use uma solução alternativa.	Edite o arquivo de configuração (baixado do AWS manualmente) para ter uma segunda linha depull-filter ignore "block-outside-dns".
VPN Pritunl	Incompatível.	Corrigido pelo módulo Umbrella - incluído na maioria das licenças.

Motivos de incompatibilidade para clientes VPN

Alguns clientes VPN têm comportamento de DNS semelhante ao cliente de roaming Umbrella. Se o servidor DNS da conexão VPN mudar para um valor inesperado, o software VPN mudará as configurações DNS do sistema de volta para o valor que a VPN definiu quando conectada inicialmente. O cliente de roaming Umbrella também executa a mesma operação, alterando qualquer servidor DNS de volta para 127.0.0.1. Esse comportamento de ida e volta cria um conflito entre a VPN e o cliente de roaming Umbrella. Esse conflito causa um ciclo infinito dos servidores DNS para a redefinição da conexão VPN. O cliente de roaming detecta isso e se desabilita para manter a conexão VPN, se possível.

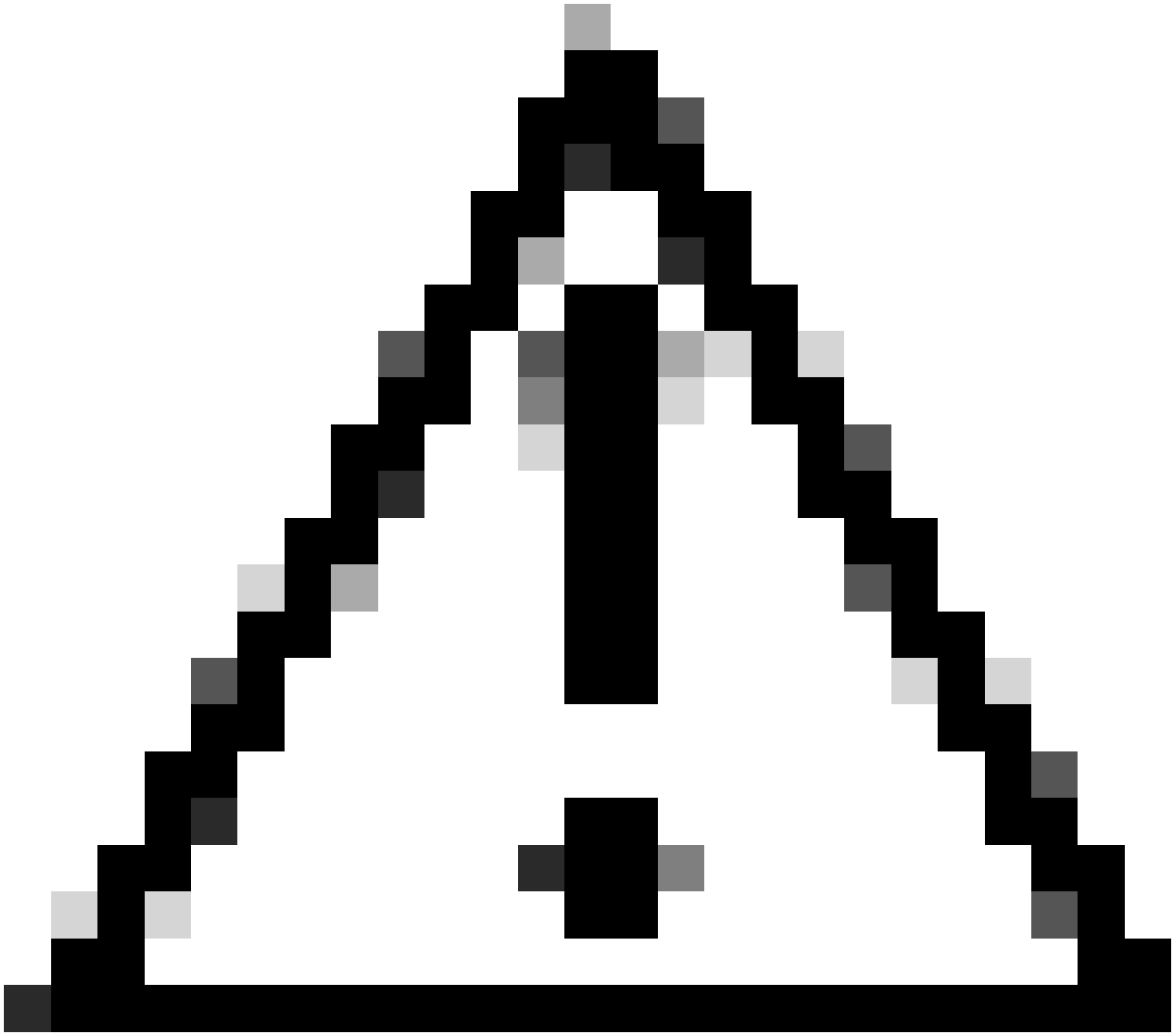
Dispositivos virtuais e redes protegidas

O cliente de roaming Umbrella se comporta de forma diferente quando conectado a uma rede que utiliza o recurso Umbrella Virtual Appliances (VA) ou Redes Protegidas. Isso se aplica se um usuário se conecta à rede localmente ou por meio de uma VPN. Para obter mais informações, consulte a documentação Roaming Client and Virtual Appliances ou Protected Networks.

Considerações especiais sobre o Cisco Secure Client + Módulo de segurança de roaming independente

As informações fornecidas aqui são específicas ao cliente de roaming Umbrella independente e não se estendem ao Cisco Secure Client (CSC) + Módulo de segurança de roaming. Os usuários que buscam uma instalação de plug-in fácil podem usar o Umbrella Roaming integrado ao CSC. Os usuários do Cisco Secure Client VPN devem migrar para o CSC + Módulo de segurança de roaming se ocorrer um problema funcional com a VPN. O Cisco Umbrella requer validação no CSC + Módulo de segurança de roaming e recomenda uma migração completa.

O software Cisco Secure Client VPN fornece opções para como o sistema lida com o DNS quando uma conexão VPN é estabelecida. Consulte o artigo Diferenças comportamentais sobre consultas DNS e resolução de nomes de domínio em sistemas operacionais diferentes para obter detalhes adicionais. Essas informações são baseadas na experiência de uso do Cisco Secure Client e do Umbrella Roaming Client. É recomendável testar o cliente de roaming Umbrella com o Cisco Secure Client VPN habilitado para garantir que a resolução de DNS interno e externo funcione conforme esperado.



Caution: A Cisco exige que você use o CSC + Módulo de segurança de roaming se também estiver usando o Cisco Secure Client para compatibilidade de serviço DNS. As etapas fornecidas são para o cliente de roaming não integrado somente se necessário. Essas etapas não são necessárias para o CSC + Módulo de segurança de roaming.

Nos modos de túnel completo e dividido, são necessárias instruções especiais para permitir que o cliente de roaming funcione enquanto o Cisco Secure Client estiver conectado. Isso é necessário para permitir que o DNS flua para o cliente de roaming em vez de ser substituído pelo driver do

kernel. Para o túnel completo, o sintoma é que o cliente é forçado a desativar. Para o tunelamento dividido, o sintoma é uma perda de DNS interno quando conectado à VPN.

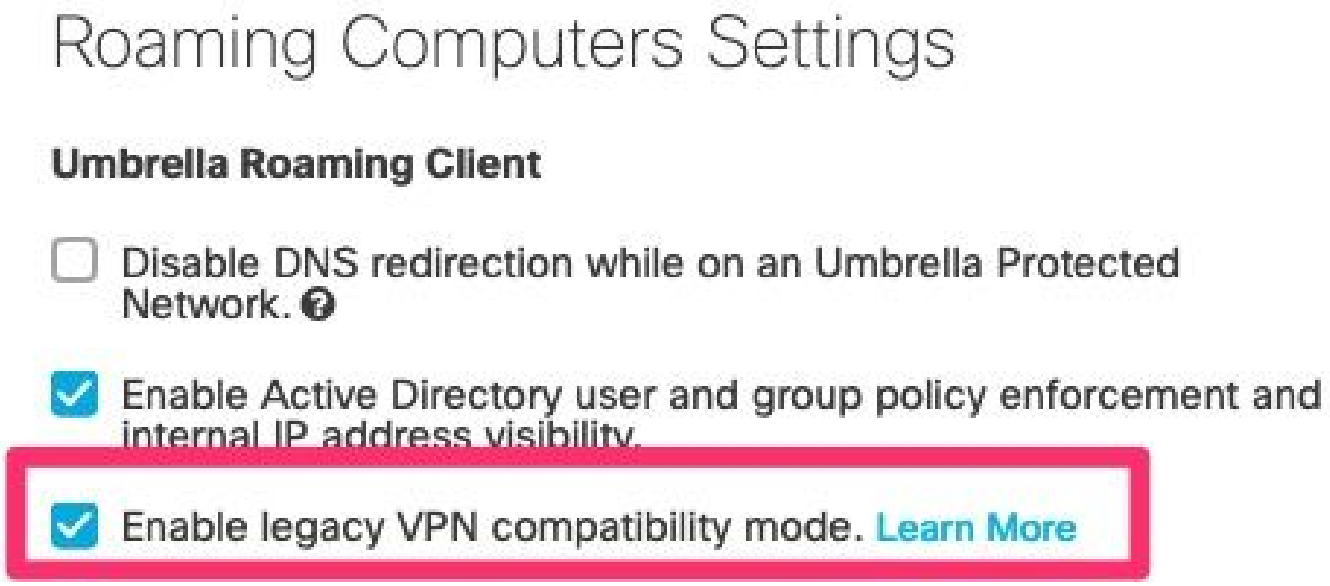
Modo de Compatibilidade VPN de Ordem de Associação DNS para Windows 10 e 11

Um conjunto limitado de usuários do Windows 10 encontra um problema específico em que a LAN local é priorizada em vez da NIC VPN para DNS. Nesse caso, o DNS local na lista de domínios internos do cliente de roaming não será resolvido, enquanto o DNS público funciona sem problemas. Isso afeta as versões 2.0.338 e 2.0.341 (por padrão) e todas as versões posteriores. O problema não ocorreu na versão 2.0.255.

Os clientes VPN impactados anteriormente incluem:

- AnyConnect 3.x
- AnyConnect 4.x (O AnyConnect Umbrella ou CSC + módulo de roaming não é afetado)
- VPN Sophos
- Algumas configurações da Palo Alto GlobalProtect em versões mais antigas
- VPN móvel WatchGuard
- Shrew Soft VPN
- VPN Barracuda

Resolução
Alterne a configuração do Roaming Client (Cliente de roaming) para Enable legacy VPN compatibility mode (Habilitar modo de compatibilidade de VPN herdado) para enabled (habilitado).



360027547111

Para confirmar se esse é o problema, execute o teste de diagnóstico e clique nos resultados para`resolv.confs`. Se o adaptador VPN for listado primeiro, o problema não afeta o usuário. Se o

adaptador VPN estiver listado em segundo lugar, o problema pode afetar o usuário.

Exemplo de saída resolv.confs

```
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
```

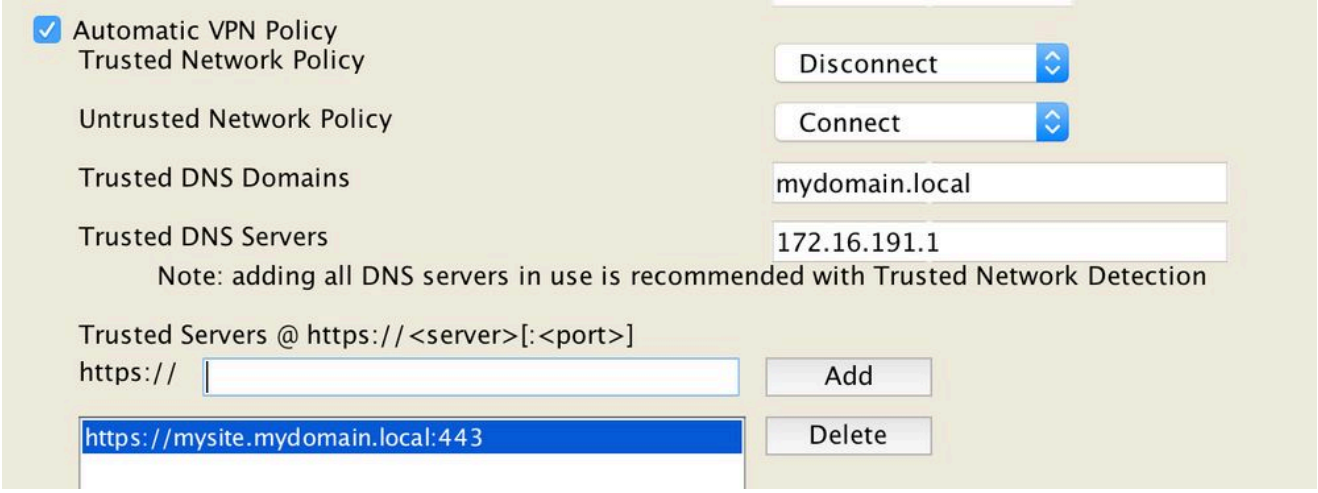
Considerações especiais para VPNs de terceiros

VPN sempre ativa

O cliente de roaming autônomo é incompatível com a configuração do Cisco Secure Client Always On VPN quando servidores DNS confiáveis são definidos. Quando ativo, o cliente de roaming autônomo sempre define o DNS como 127.0.0.1, eliminando todos os servidores DNS confiáveis das configurações de NIC. O cliente de roaming pode ser desativado na rede para restaurar as configurações de DHCP; no entanto, todas as proteções relacionadas ao cliente de roaming cessam quando configuradas. Entre em contato com o suporte do Umbrella para saber mais sobre como desativar o cliente em uma rede confiável.

Soluções

- O CSC + Módulo de segurança de roaming (cliente de roaming para o Cisco Secure Client) não é afetado e funciona efetivamente com uma política de VPN automática.
- Adicione 127.0.0.1 à lista de servidores DNS confiáveis.
- Certifique-se de que métodos alternativos de detecção confiável estejam definidos (nomes DNS e servidores) para evitar que todas as redes sejam declaradas confiáveis.



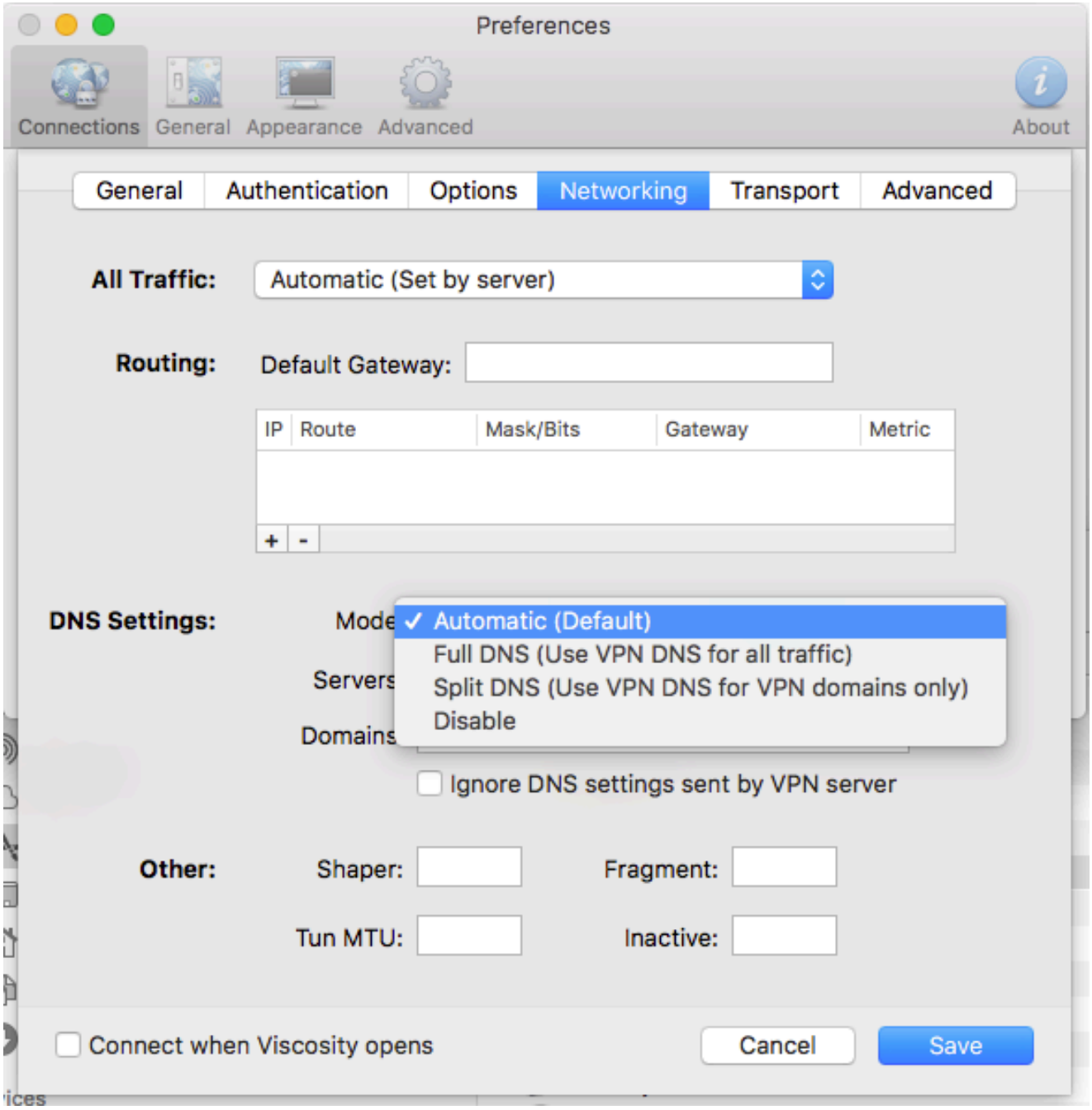
360031250911

VPN de viscosidade

A VPN Viscosidade requer uma alteração nas configurações para funcionar com o cliente de roaming Umbrella. Se essa alteração não for feita, o comportamento padrão de Viscosidade imitará o de outras VPNs incompatíveis. Essa alteração instrui o Viscoity a usar as configurações DNS enviadas por push através do servidor Umbrella para todos os domínios no domínio de pesquisa, e 127.0.0.1 continua a ser usado para quaisquer outras solicitações.

Configurar viscosidade

1. Em Viscosidade, navegue para Preferências > Conexões > <sua conexão> (específico do site) > Rede > Configurações DNS.
2. Selecione Automático (Padrão).



115013433283

Ao usar um servidor OpenVPN, certifique-se de que persist-tun não esteja habilitado no lado do servidor para garantir que as alterações na rede sejam disparadas na desconexão ou reconexão.

Túnel em movimento

A opção Tunnelblick requer duas alterações para:

- Permitir a alteração dos servidores DNS do adaptador.
- Aplique as configurações de DNS depois que o túnel for estabelecido.

Garantindo as configurações fornecidas no menu Advanced, o botão de túnel funciona com o Umbrella Roaming Client:

Na guia Conectando e desconectando, habilite estas duas configurações:

- Liberar cache DNS após conectar ou desconectar (padrão)
- Definir DNS após a definição das rotas, em vez de antes da definição das rotas

Na guia Enquanto conectado, altere essa configuração para Ignorar:

- DNS: Servers > Quando muda para o valor pré-VPN, Quando muda para qualquer outra coisa.

Ao usar um servidor OpenVPN, certifique-se de que persist-tun não esteja habilitado no lado do servidor para garantir que as alterações na rede sejam disparadas na desconexão ou reconexão.

Problemas de desconexão de VPN em clique de túnel

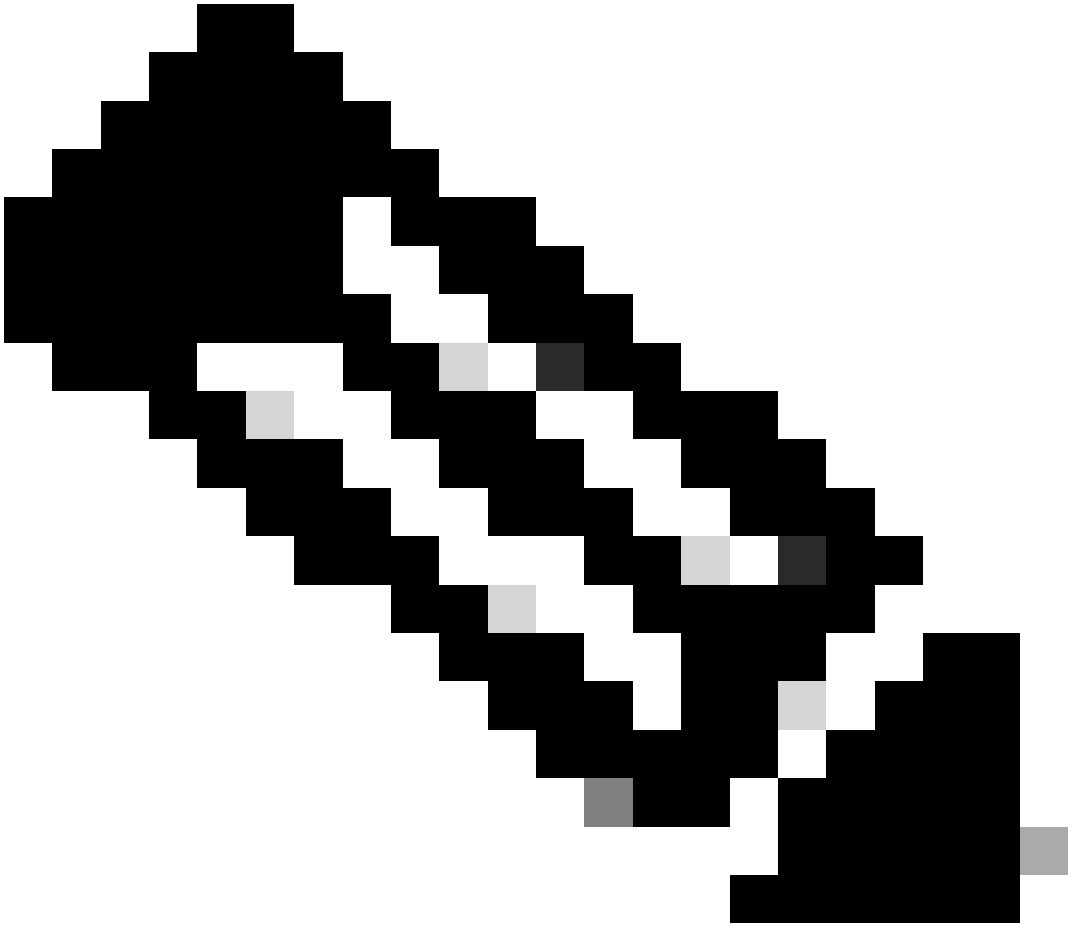
Com algumas versões de Túneis Blicados, o cliente de roaming não pode identificar corretamente os servidores DNS internos corretos após uma desconexão de VPN. Se ocorrerem problemas com Domínios internos após uma desconexão de VPN, a Umbrella recomenda estas etapas:

Essa alteração faz com que Tunnelblick ative e desative a interface de rede primária após a desconexão da VPN. Isso é gerenciado na guia Settings do painel de configuração Tunnelblick:

- Em versões mais antigas do Tunnelblick (anterior à 3.7.5beta03), use a caixa de verificação Redefinir a interface primária após desconectar.
- Em versões mais recentes do Tunnelblick (3.7.5beta03 e posterior), defina as configurações On expected disconnect e On expected disconnect como Reset Primary Interface.

Foguete Lightspeed

O Lightspeed Rocket possui recursos selecionados que não são compatíveis com o cliente de roaming. Especificamente, a modificação de DNS para No SSL Search e SafeSearch redirecionamento de CNAME de www.google.com para nosslsearch.google.com e forcesafesearch.com respectivamente faz com que toda a resolução de DNS de www.google.com falhe, desde que o redirecionamento de DNS do Lightspeed Rocket esteja habilitado.



Note: Este artigo refere-se ao Umbrella Roaming Client autônomo. Para obter um artigo complementar sobre o Umbrella Roaming Security Module for Cisco Secure Client e o software herdado, consulte a documentação relevante.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.