Gestisci compatibilità VPN e client mobili Umbrella

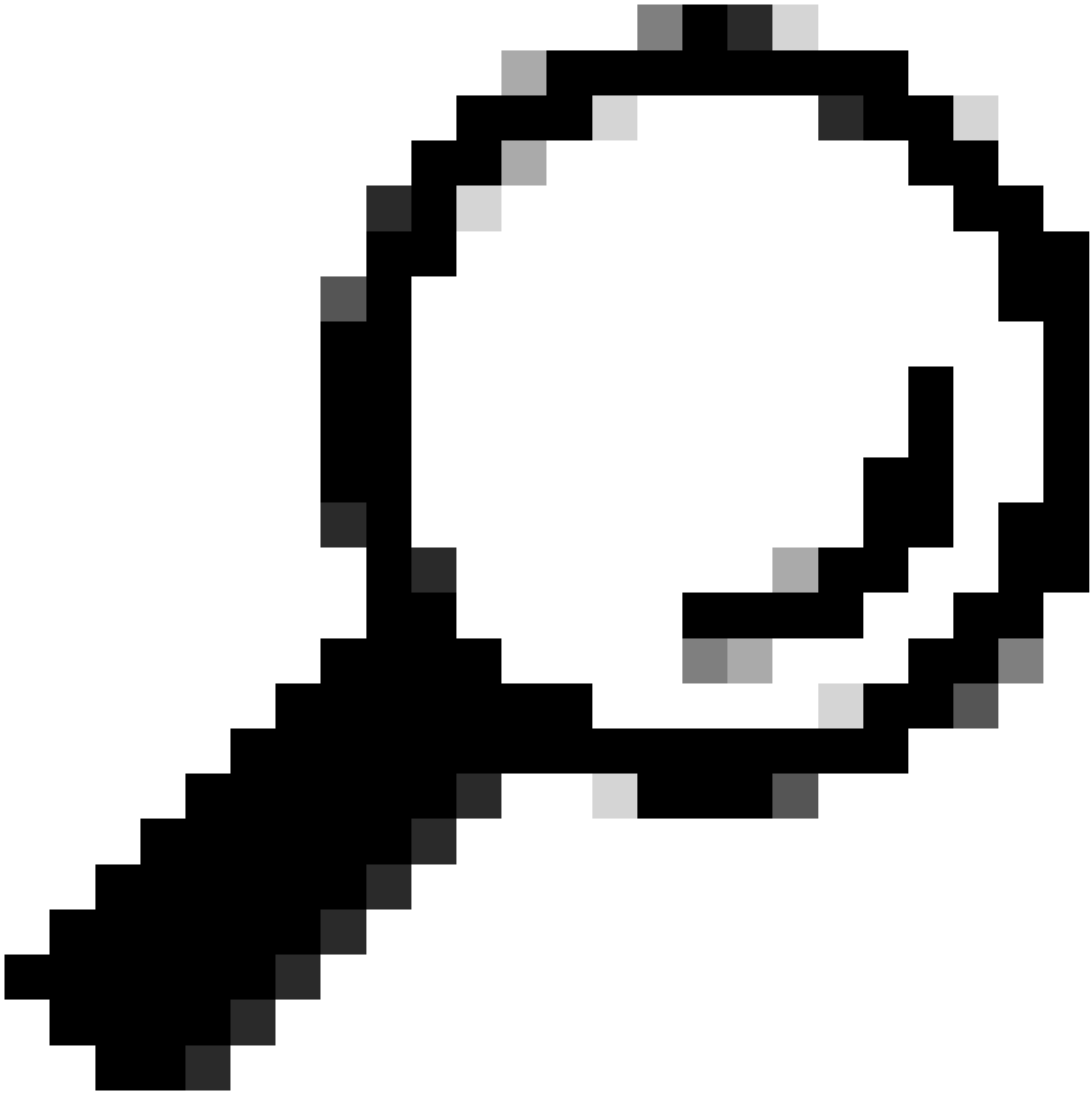
Sommario

Introduzione

Questo documento descrive l'interazione e la compatibilità di Cisco Umbrella Roaming Client con vari software VPN.

Panoramica

Il Cisco Umbrella Roaming Client funziona con la maggior parte dei software VPN, ma per il funzionamento previsto possono essere necessari passaggi aggiuntivi. Cisco Umbrella consiglia di installare il modulo Cisco Secure Client and Roaming Security per la massima compatibilità. Questo modulo può essere distribuito senza i componenti VPN.



Suggerimento: Il presente documento costituisce una guida generale e non costituisce un elenco ufficiale del software supportato. Cisco Umbrella non testa, convalida o certifica le funzionalità con software di terze parti o client VPN.

Questo documento fornisce informazioni tecniche e contesto aggiuntivo per client VPN specifici che possono richiedere ulteriori configurazioni. Per un elenco dei software VPN noti e incompatibili, fare riferimento alla sezione Incompatibilità con i client mobili Umbrella. L'incompatibilità DNS con il client di roaming può inoltre causare il malfunzionamento del modulo Cisco Secure Client + Roaming Security con SWG, in quanto il client SWG dipende anche dalla corretta connessione DNS.

Come funziona il client Umbrella Roaming con i client VPN

Il client Umbrella Roaming si associa a tutte le schede di rete e modifica le impostazioni DNS del computer in 127.0.0.1 (localhost). In questo modo il client Umbrella Roaming può inoltrare tutte le query DNS direttamente a Umbrella, consentendo al contempo la risoluzione dei domini locali tramite la funzionalità Domini interni. Quando stabilisce una connessione a un server VPN, il client Umbrella Roaming rileva una nuova connessione di rete nel sistema e modifica le impostazioni DNS della connessione in modo che puntino verso il client Umbrella Roaming. Il client Umbrella Roaming si basa sull'esecuzione di ricerche DNS negli indirizzi IP DNS di Umbrella AnyCast (208.67.222.222/208.67.220.220).

Se un utente si connette a una VPN, il firewall associato alla VPN deve consentire l'accesso a Umbrella.

Incompatibilità con i client di roaming Umbrella

Attualmente il client Umbrella Roaming fornisce l'imposizione del livello DNS. Il livello DNS è la funzione principale del client di roaming, che applica i criteri di sicurezza basati su DNS in qualsiasi rete. Questa funzione del client di roaming può sperimentare incompatibilità software note. Il livello DNS del client Umbrella Roaming non è compatibile con i client elencati di seguito, in base ai test eseguiti dal team di supporto. Cisco Umbrella Engineering non verifica né testa questi client e tutte le voci sono soggette a revisione. Questo articolo fa riferimento al client di roaming Umbrella autonomo. Per un articolo complementare sul modulo Umbrella Roaming Security per Cisco Secure Client (e versioni precedenti), fare riferimento alla documentazione pertinente.

Client VPN	Problema/Incompatibilità	Risoluzione
Pulse Secure	Alla disconnessione, il DNS locale salvato può rimanere un valore VPN anziché un valore WiFi/Ethernet a causa della modifica Pulse durante la connessione VPN.	Risolto con il modulo Umbrella - incluso nella maggior parte delle licenze.
Avaya VPN	Incompatibile.	Risolto con il modulo Umbrella - incluso nella maggior parte delle licenze.
VPN per Windows (in particolare, VPN Sempre attiva)	È possibile che il DNS locale non riesca a risolvere la risposta interna nonostante i nomi host DNS siano presenti nell'elenco dei domini interni.	Risolto con il modulo Umbrella - incluso nella maggior parte delle licenze.
App VPN basate sulla piattaforma universale Windows	Queste app devono utilizzare un'API di connessione Microsoft che richiede l'invio di DNS alla scheda NIC locale, non 127.0.0.1. Pertanto, l'app visualizza un	Risolto con il modulo Umbrella - incluso nella maggior parte delle licenze.

Client VPN	Problema/Incompatibilità	Risoluzione
	errore che indica che non è possibile connettersi.	
OpenVPN	Incompatibile.	Nessuna correzione disponibile.
Palo Alto GlobalProtect VPN	Non funziona con le versioni dei client mobili autonomi successive alla 3.0.110.	Fisso utilizzando il modulo Umbrella - incluso nella maggior parte delle licenze.
VPN F5	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.
Checkpoint VPN	Solo macOS, solo modalità split-tunnel.	Disabilitare lo split-tunnel su macOS.
SonicWall NetExtender	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.
Zscaler VPN	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.
Endpoint Protection Akamai (ETPclient)	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.
NordVPN	Utilizzare la soluzione alternativa.	Sono disponibili due opzioni per l'aggiunta della compatibilità: 1. Utilizzare il metodo di connessione OpenVPN come descritto in Come configurare una connessione manuale in Windows utilizzando OpenVPN 2. Consenti DNS personalizzato

Client VPN	Problema/Incompatibilità	Risoluzione
		in Impostazioni avanzate. Impostare DNS su 208.67.220.220 e 208.67.222.222.
VPN di Azure	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.
VPN AWS	Utilizzare la soluzione alternativa.	Modificare il file di configurazione (scaricato manualmente da AWS) in modo che abbia una seconda riga di`pull-filter ignore "block-outside-dns"`.
Pritunl VPN	Incompatibile.	Fissato dal modulo Umbrella - incluso nella maggior parte delle licenze.

Motivi di incompatibilità per i client VPN

Alcuni client VPN hanno un comportamento DNS simile al client di roaming Umbrella. Se il server DNS della connessione VPN assume un valore imprevisto, il software VPN ripristina le impostazioni DNS del sistema sul valore impostato dalla VPN alla connessione iniziale. Anche il client Umbrella Roaming esegue la stessa operazione, riportando tutti i server DNS a 127.0.0.1. Questo comportamento di tipo "back-and-forward" crea un conflitto tra la VPN e il client Umbrella Roaming. Questo conflitto causa un ciclo infinito dei server DNS per la reimpostazione della connessione VPN. Il client in roaming rileva questa condizione e, se possibile, si disattiva per mantenere la connessione VPN.

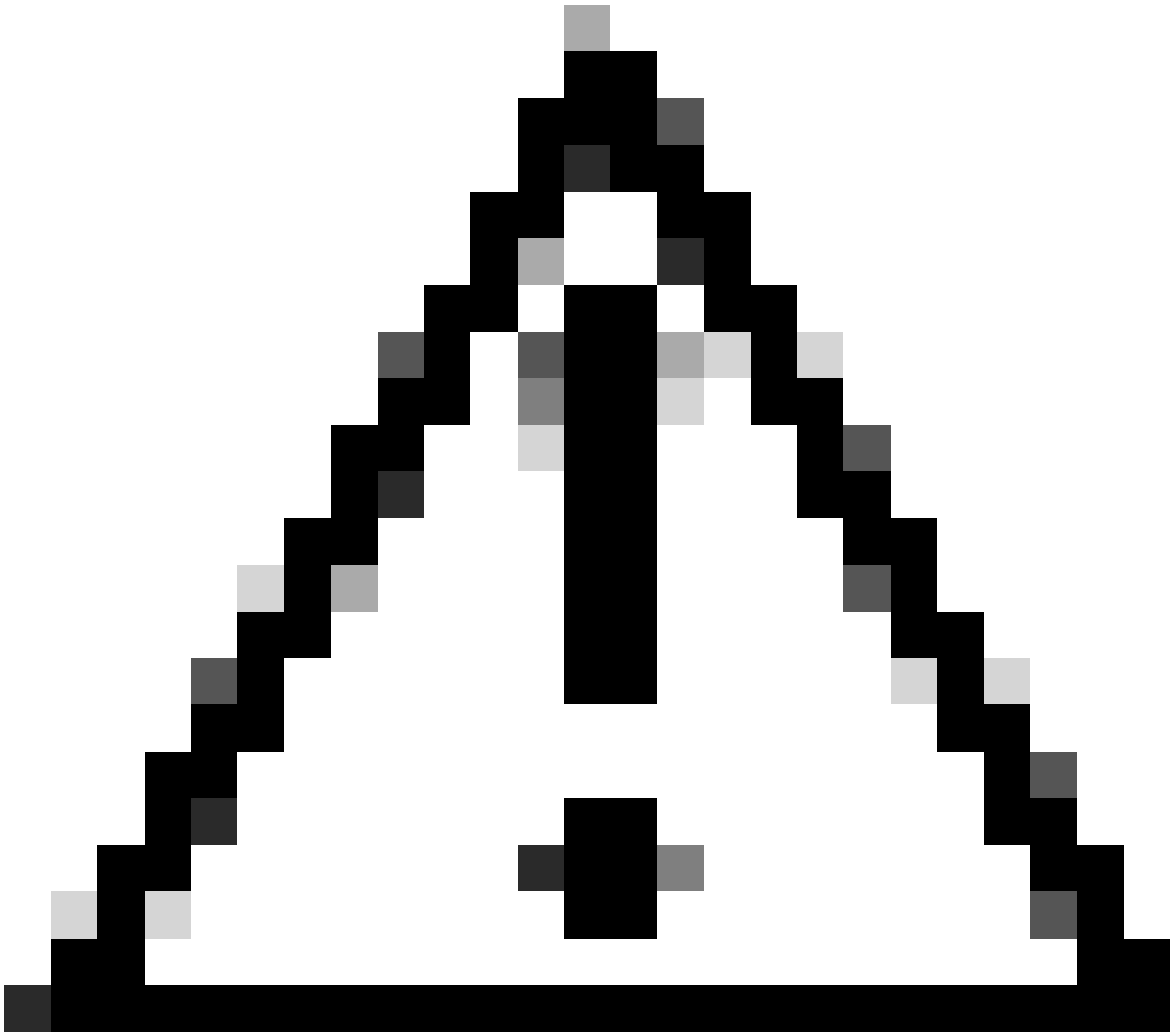
Appliance virtuali e reti protette

Il comportamento del client di roaming Umbrella è diverso se collegato a una rete che utilizza la funzionalità Umbrella Virtual Appliance (VA) o le reti protette. Ciò vale sia che un utente si connetta alla rete localmente sia che si connetta tramite una VPN. Per ulteriori informazioni, consultare la documentazione relativa ai client e alle appliance virtuali in roaming o alle reti protette.

Considerazioni speciali per standalone e Cisco Secure Client + modulo di sicurezza in roaming

Le informazioni fornite sono specifiche per il client di roaming Umbrella standalone e non si estendono al Cisco Secure Client (CSC) + modulo di sicurezza di roaming. Gli utenti che desiderano installare facilmente un plugin possono utilizzare Umbrella Roaming integrato in CSC. Gli utenti di Cisco Secure Client VPN devono migrare a CSC + modulo di sicurezza in roaming se si verifica un problema funzionale con la VPN. Cisco Umbrella richiede la convalida sul modulo CSC + Roaming Security e consiglia una migrazione completa.

Il software Cisco Secure Client VPN offre opzioni per la gestione del DNS da parte del sistema quando viene stabilita una connessione VPN. Per ulteriori informazioni, vedere l'articolo Differenze comportamentali relative alle query DNS e alla risoluzione dei nomi di dominio in sistemi operativi diversi. Queste informazioni si basano sull'esperienza acquisita utilizzando Cisco Secure Client e Umbrella Roaming Client. Si consiglia di testare il client di roaming Umbrella con Cisco Secure Client VPN abilitata per garantire le funzioni di risoluzione DNS interne ed esterne come previsto.



Attenzione: Cisco richiede l'utilizzo di CSC + modulo di sicurezza roaming se si utilizza anche Cisco Secure Client per la compatibilità con i servizi DNS. I passaggi forniti sono

---

per il client mobile non integrato solo se necessario. questi passaggi non sono richiesti per CSC + modulo di sicurezza roaming.

In modalità tunnel completo e split, sono necessarie istruzioni speciali per consentire al client in roaming di funzionare mentre Cisco Secure Client è connesso. Ciò è necessario per consentire il flusso del DNS nel client mobile anziché essere ignorato dal driver del kernel. Per il tunnel completo, il sintomo è che il client è costretto a disabilitare. Per il tunneling ripartito, il sintomo è una perdita di DNS interno mentre è connesso alla VPN.

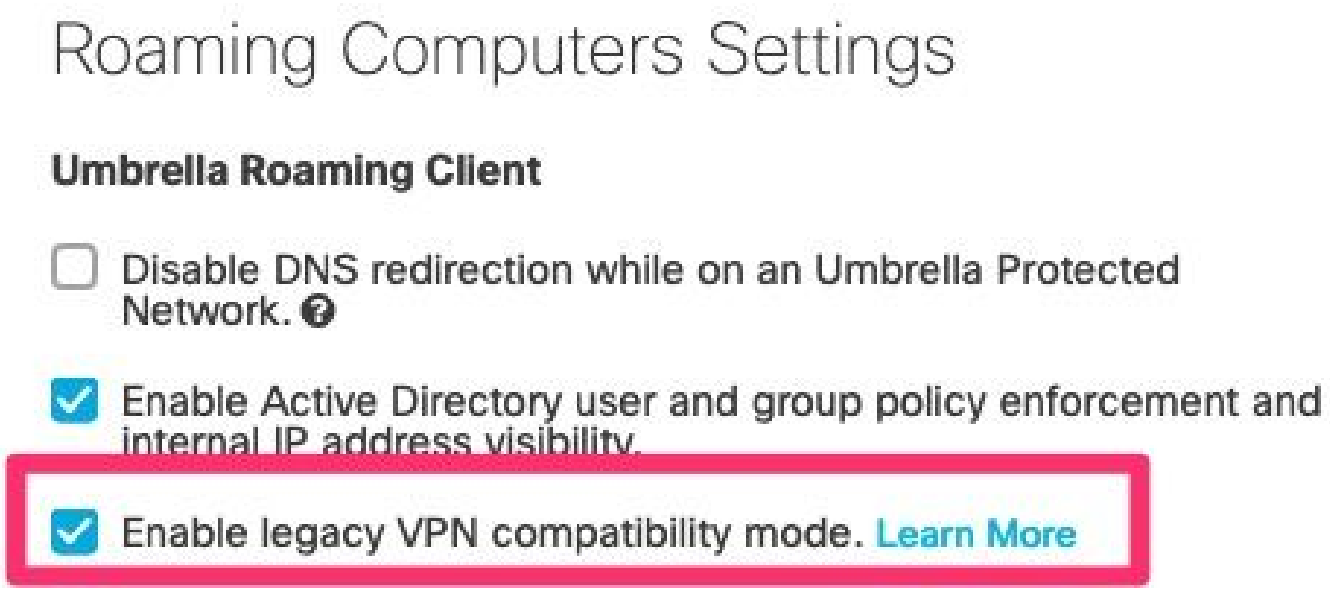
Modalità di compatibilità VPN ordine di binding DNS per Windows 10 e 11

Un gruppo limitato di utenti di Windows 10 incontra un problema specifico in cui la LAN locale ha la priorità rispetto alla NIC VPN per DNS. In questo caso, il DNS locale nell'elenco dei domini interni per il client di roaming non viene risolto mentre il DNS pubblico funziona senza problemi. Questa impostazione influisce sulle versioni 2.0.338 e 2.0.341 (per impostazione predefinita) e su tutte le versioni successive. Il problema non si è verificato nella versione 2.0.255.

I client VPN interessati in precedenza includono:

- AnyConnect 3.x
- AnyConnect 4.x (AnyConnect Umbrella o CSC + modulo roaming)
- Sophos VPN
- Alcune configurazioni di Palo Alto GlobalProtect su versioni precedenti
- WatchGuard Mobile VPN
- Mostra VPN soft
- Barracuda VPN

Risoluzione
Attiva/disattiva l'impostazione Client di roaming Attiva modalità di compatibilità VPN legacy su Attiva.



Per verificare se questo è il problema, eseguire il test di diagnostica e fare clic sui risultati per`resolv.confs`. Se la scheda VPN è elencata per prima, il problema non influirà sull'utente. Se la scheda VPN è elencata per seconda, il problema può influire sull'utente.

Esempio di output 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
```

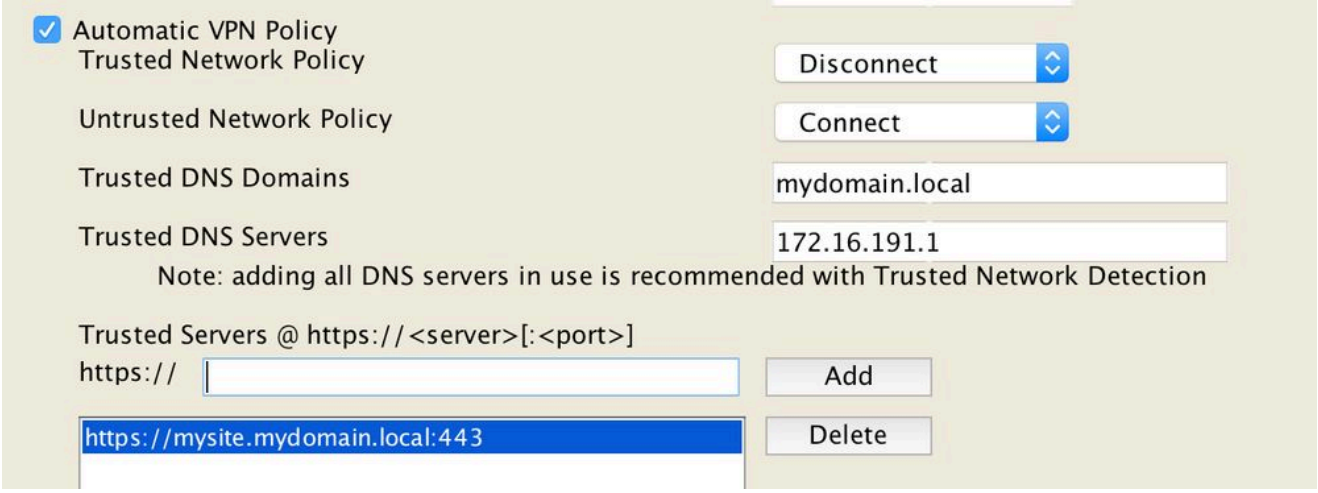
Considerazioni speciali per VPN di terze parti

VPN sempre attiva

Il client in roaming autonomo non è compatibile con l'impostazione VPN Cisco Secure Client Always On quando sono definiti server DNS trusted. Quando è attivo, il client in roaming autonomo imposta sempre DNS su 127.0.0.1, eliminando tutti i server DNS trusted dalle impostazioni NIC. Il client di roaming può essere disattivato sulla rete per ripristinare le impostazioni DHCP; tuttavia, tutte le protezioni relative ai client mobili cessano quando vengono configurate. Contatta il supporto Umbrella per ulteriori informazioni sulla disabilitazione del client su una rete attendibile.

Soluzioni

- CSC + Roaming Security Module (Roaming Client per Cisco Secure Client) non è interessato e funziona in modo efficace con una policy VPN automatica.
- Aggiungere 127.0.0.1 all'elenco dei server DNS trusted.
- Verificare che siano definiti metodi alternativi di rilevamento attendibili (nomi DNS e server) per impedire che tutte le reti vengano dichiarate attendibili.



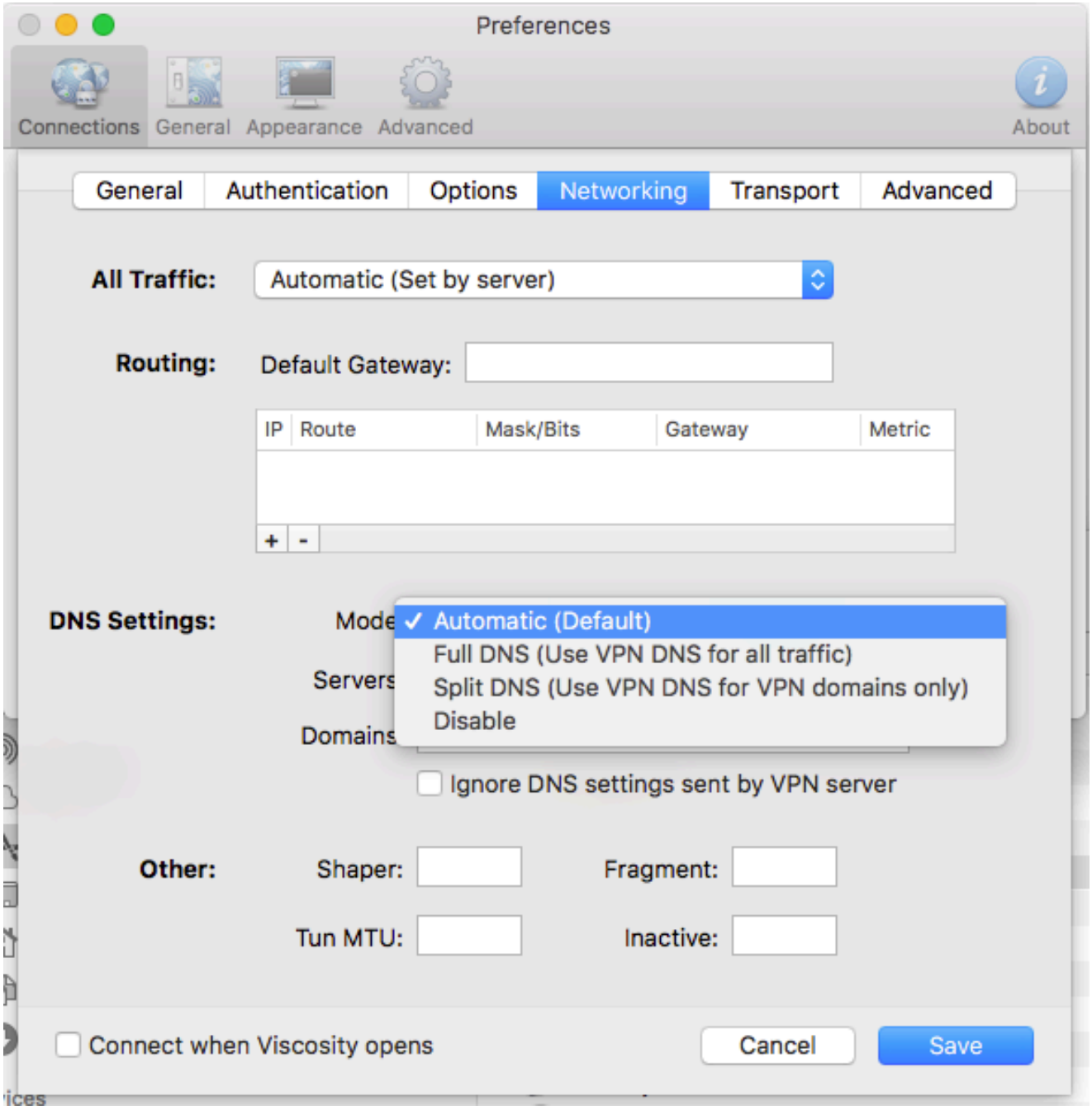
360031250911

Viscosity VPN

Per utilizzare il client di roaming Umbrella, è necessario modificare le impostazioni di Viscosity VPN. Se questa modifica non viene apportata, il comportamento predefinito di Viscosity simula quello di altre VPN incompatibili. Questa modifica indica a Viscosity di utilizzare le impostazioni DNS sottoposte a push tramite il server Umbrella per tutti i domini nel dominio di ricerca e 127.0.0.1 continua ad essere utilizzato per qualsiasi altra richiesta.

Configura viscosità

1. In Viscosity, selezionare Preferenze > Connessioni > <connessione> (specifica del sito) > Rete > Impostazioni DNS.
2. Selezionate Automatico (Automatic) (Default).



115013433283

Quando si utilizza un server OpenVPN, verificare che persist-tun non sia abilitato sul lato server per assicurare che le modifiche alla rete vengano attivate alla disconnessione o alla riconnessione.

Tunnelblick

Tunnelblick richiede due modifiche a:

- Consente la modifica dei server DNS per la scheda.
- Applicare le impostazioni DNS dopo che il tunnel è stato stabilito.

Accertandosi che le impostazioni fornite nel menu Avanzate, Tunnelblick funziona con Umbrella Roaming Client:

Nella scheda Connessione e disconnessione, attivare le due impostazioni seguenti:

- Svuota la cache DNS dopo la connessione o la disconnessione (impostazione predefinita)
- Imposta DNS dopo l'impostazione delle route anziché prima dell'impostazione delle route

Nella scheda While Connected, modificare questa impostazione in Ignore:

- DNS: Server > Quando viene modificato il valore pre-VPN, Quando viene modificato in qualsiasi altro valore.

Quando si utilizza un server OpenVPN, verificare che persist-tun non sia abilitato sul lato server per assicurarsi che le modifiche alla rete vengano attivate alla disconnessione o alla riconnessione.

Problemi di disconnessione VPN tunnel

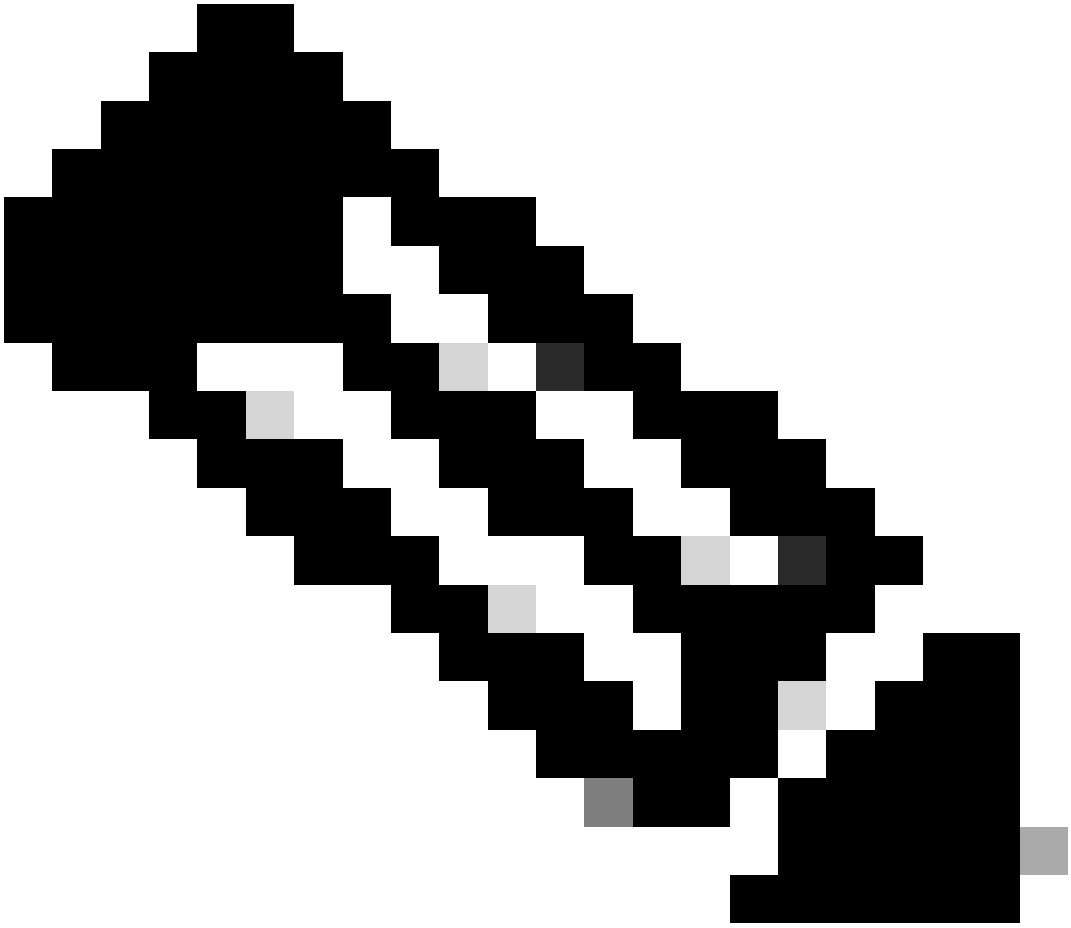
Con alcune versioni di Tunnelblick, il client mobile non è in grado di identificare correttamente i server DNS interni corretti dopo una disconnessione VPN. Se si verificano problemi con i domini interni dopo una disconnessione VPN, Umbrella consiglia i seguenti passaggi:

Questa modifica determina la disconnessione della VPN tramite Tunnelblick, che disattiva e attiva l'interfaccia di rete primaria. Questa operazione viene gestita nella scheda Impostazioni del pannello di configurazione Tunnelblick:

- Nelle versioni precedenti di Tunnelblick (prima della versione 3.7.5beta03), usare la casella di controllo Ripristina l'interfaccia primaria dopo la disconnessione.
- Nelle versioni più recenti di Tunnelblick (3.7.5beta03 e versioni successive), impostare le impostazioni On previsto disconnect e On imprevisto disconnect su Reset Primary Interface.

Razzo a velocità ridotta

Lightspeed Rocket dispone di funzionalità selezionate non compatibili con il client in roaming. In particolare, la modifica DNS per No SSL Search e il reindirizzamento SafeSearch CNAME di `www.google.com` a nosslsearch.google.com e forcesafesearch.com provoca rispettivamente l'esito negativo di tutte le risoluzioni `www.google.com` DNS finché è abilitato il reindirizzamento DNS di Lightspeed Rocket.



Nota: Questo articolo fa riferimento al client di roaming Umbrella autonomo. Per un articolo complementare sul modulo Umbrella Roaming Security per Cisco Secure Client e il software legacy, consultare la documentazione pertinente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).