

Comprendere la compatibilità tra Umbrella Roaming Client e VPN F5

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Compatibilità VPN F5](#)

[BigIP F5 VPN Client](#)

[Proxy di inoltro DNS F5](#)

[Trova l'impostazione del tunneling suddiviso in DNS o basato su DNS](#)

[Nuovo client F5](#)

Introduzione

In questo documento viene descritta la compatibilità tra Cisco Umbrella Roaming Client e VPN F5.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sul client di roaming Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Introduzione

Il client di roaming Umbrella può essere utilizzato in un'ampia varietà di configurazioni di rete e software. In questo articolo vengono illustrati tutti gli argomenti noti relativi alla compatibilità con il client VPN F5. In questo articolo vengono illustrati i comportamenti di rilevamento correnti previsti e quindi le note sulla compatibilità specifiche per la VPN F5.

Il client Umbrella ha implementato meccanismi di rilevamento automatico per reagire alle modifiche VPN per garantire il mantenimento della funzionalità DNS. In questo modo il client potrebbe rimanere temporaneamente non protetto mentre la VPN è connessa. Fare riferimento all'articolo Euristiche di rilevamento VPN di terze parti con il client di roaming Umbrella per ulteriori dettagli.

Compatibilità VPN F5

In molte configurazioni, la VPN F5 funziona inserendo gli indirizzi DNS della VPN nelle NIC non VPN anticipando i server VPN al DNS della NIC. Pertanto, per una configurazione DNS locale di x.x.x.x e una configurazione VPN di y.y.y, il risultato è y.y.y, x.x.x.x.

Con il client di roaming Umbrella, questa impostazione sostituisce la versione 127.0.0.1 inserita. Per garantire che la VPN F5 non sia compromessa da un ciclo di cambiamento continuo, Umbrella interrompe il reindirizzamento se 127.0.0.1 viene posizionato alla fine dell'elenco DNS o viene rapidamente modificato di nuovo da 127.0.0.1.

Nella maggior parte dei casi, Umbrella consiglia di utilizzare il modulo di sicurezza roaming Umbrella che fa parte del client di sicurezza roaming AnyConnect. La VPN non deve essere distribuita (può essere rimossa dalla visualizzazione per l'utente al momento dell'installazione).

La compatibilità con F5 in questo momento è definita come una connessione VPN F5 riuscita con DNS locali e pubblici completamente funzionanti. Questa situazione può essere il risultato di un backoff regolare del client in roaming in uno stato non protetto. Verificare che la copertura di rete sia attiva durante l'utilizzo di F5 configurando la rete per Cisco Umbrella.

BigIP F5 VPN Client

Il BigIP F5 edge client è il client VPN F5 più comune in questo momento. Tuttavia, in molte implementazioni viene sostituito con il nuovo client F5. In questo articolo vengono illustrati tutti i problemi di interoperabilità noti con il client F5 BigIP.

Proxy di inoltro DNS F5

Il client mobile non è compatibile con il client VPN 2.2+ nelle configurazioni che attivano il servizio proxy di inoltro DNS F5. Questo proxy di inoltro viene attivato in modalità split-dns e in modalità split-tunneling basata su DNS. Impossibile utilizzare F5 con nomi DNS definiti con il client in roaming. Per utilizzare il tunneling suddiviso con F5 e il client in roaming in questo momento, utilizzare il tunneling suddiviso basato su IP anziché il tunneling suddiviso basato su DNS. Inoltre, alcune configurazioni e versioni possono causare l'override di Umbrella nonostante venga visualizzato in verde quando il proxy di inoltro DNS è attivato.

Trova l'impostazione del tunneling suddiviso in DNS o basato su DNS

Il tunneling ripartito della VPN F5 con split-dns viene visualizzato sotto forma di impostazione "Spazio indirizzi DNS". Quando è attivo, il proxy DNS di F5 viene ruotato e ciò è in conflitto con il

client mobile. Il sintomo è un errore nella risoluzione dei record A mentre sia il client mobile che la VPN sono attivi. Per una configurazione di lavoro, vedere questa schermata:

Client Settings: Advanced ▾

Traffic Options

- Force all traffic through tunnel
- Use split tunneling for traffic

IPV4 LAN Address Space

IP Address

Mask

0.0.0.0/0.0.0.0

Ensure this is empty!

DNS Address Space

DNS

IPV4 Exclude Address Space

IP Address

Mask

DNS Exclude Address Space

DNS

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).