Begrijp Umbrella Roaming Client- en F5 VPN-compatibiliteit

Inhoud

Inleiding

Dit document beschrijft de compatibiliteit tussen de Cisco Umbrella Roaming Client en F5 VPN.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella Roaming Client.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Inleiding

De Umbrella-roamingclient kan worden gebruikt in een breed scala aan netwerk- en softwareconfiguraties. Dit artikel documenteert alle bekende compatibiliteitsonderwerpen met de F5 VPN-client. Dit artikel begint met het huidige verwachte detectiegedrag en bespreekt vervolgens F5 VPN-specifieke compatibiliteitsnotities.

De Umbrella-client heeft geautomatiseerde detectiemechanismen geïmplementeerd om te reageren op VPN-wijzigingen om ervoor te zorgen dat de DNS-functionaliteit wordt gehandhaafd. Dit kan ertoe leiden dat de client tijdelijk onbeschermd blijft terwijl de VPN is verbonden. Raadpleeg het artikel VPN-detectieheuristiek van derden met de Umbrella Roaming Client voor meer informatie.

F5 VPN-compatibiliteit

In veel configuraties functioneert F5 VPN door de VPN-DNS-adressen in te voegen in niet-VPN-NIC's door de VPN-servers vooraf in te dienen bij de DNS van de NIC. Dus, voor een lokale DNS-configuratie van x.x.x.x en een VPN-configuratie van y.y.y.y, is het resultaat y.y.y, x.x.x.x.x.

Bij de Umbrella roaming client heeft dit voorrang op de geplaatste 127.0.0.1. Om ervoor te zorgen dat F5 VPN niet wordt aangetast door een eindeloze wijzigingslus, stopt Umbrella met omleiden als 127.0.0.1 aan het einde van de DNS-lijst wordt geplaatst of snel wordt teruggezet van 127.0.0.1.

In de meeste gevallen raadt Umbrella het gebruik aan van de Umbrella-beveiligingsmodule voor roaming die deel uitmaakt van de AnyConnect-client voor roamingbeveiliging. VPN hoeft niet te worden geïmplementeerd (het kan op het moment van installatie worden verwijderd van weergave aan de gebruiker).

F5-compatibiliteit wordt op dit moment gedefinieerd als een succesvolle F5 VPN-verbinding met volledig functionele lokale en openbare DNS. Dit kan het gevolg zijn van een gracieuze back-off door de roamende client in een onbeschermde staat. Zorg ervoor dat uw netwerkdekking aanwezig is tijdens het gebruik van F5 door uw netwerk te configureren voor Cisco Umbrella.

BigIP F5 VPN-client

De BigIP F5 edge client is op dit moment de meest voorkomende F5 VPN client. Het wordt echter in veel implementaties vervangen door de nieuwe F5-client. In dit artikel worden alle bekende problemen met de interoperabiliteit van de F5 BigIP-client besproken.

F5 DNS Relay Proxy

De zwervende client is niet compatibel met VPN-client 2.2+ in configuraties die de F5 DNS Relay Proxy-service activeren. Het is bekend dat deze relay-proxy wordt geactiveerd in de split-dns-modus en op DNS gebaseerde split-tunneling-modi. F5 kan niet worden gebruikt met DNS-namen die zijn gedefinieerd met de roamingclient Als u op dit moment split tunneling wilt gebruiken met F5 en de roamingclient, gebruikt u op IP gebaseerde split tunneling in plaats van op DNS gebaseerde split tunneling. Bovendien kunnen sommige configuraties en versies ertoe leiden dat Umbrella wordt overschreven, ondanks het feit dat groen wordt weergegeven wanneer de DNS Relay Proxy is geactiveerd.

Zoek de split-dns- of DNS-gebaseerde Split Tunneling-instelling

F5 VPN Split Tunneling met split-dns verschijnt in de vorm van de instelling "DNS Address Space". Als deze optie actief is, wordt de eigen DNS-proxy van F5 gecentrifugeerd, wat in strijd is met de zwervende client. Het symptoom is een falen om A-records op te lossen terwijl zowel de roamingclient als de VPN actief is. Zie deze screenshot voor een werkende configuratie:

Client Settings: Advanced ▼

Traffic Options	○ Force all traffic through tunnel ◉ Use split tunneling for traffic
IPV4 LAN Address Space	IP Address Mask Add 0.0.0.0/0.0.0.0 Edit Delete
DNS Address Space	DNS Add Edit Delete
IPV4 Exclude Address Space	IP Address Mask Add Edit Delete
DNS Exclude Address Space	DNS Add

Ensure this is empty!

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.