Verständnis der Kompatibilität von Umbrella Roaming Client und F5 VPN

Inhalt

Einleitung

In diesem Dokument wird die Kompatibilität zwischen dem Cisco Umbrella Roaming Client und F5 VPN beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Umbrella Roaming Client.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Einleitung

Der Umbrella Roaming Client kann in einer Vielzahl von Netzwerk- und Softwarekonfigurationen eingesetzt werden. In diesem Artikel werden alle bekannten Kompatibilitätsthemen mit dem F5-VPN-Client beschrieben. Dieser Artikel beginnt mit dem aktuell erwarteten Erkennungsverhalten und behandelt dann F5 VPN-spezifische Kompatibilitätshinweise.

Der Umbrella-Client hat automatisierte Erkennungsmechanismen implementiert, um auf VPN-Änderungen zu reagieren und so sicherzustellen, dass die DNS-Funktionalität erhalten bleibt. Dies kann dazu führen, dass der Client vorübergehend ungeschützt bleibt, während das VPN verbunden ist. Weitere Informationen finden Sie im Artikel Heuristik zur VPN-Erkennung durch Drittanbieter mit dem Umbrella Roaming Client.

F5 VPN-Kompatibilität

In vielen Konfigurationen funktioniert F5 VPN, indem die VPN-DNS-Adressen in Nicht-VPN-NICs eingefügt werden, indem die VPN-Server dem DNS der NIC vorgeschaltet werden. Für eine lokale DNS-Konfiguration von x.x.x.x und eine VPN-Konfiguration von y.y.y.y lautet das Ergebnis y.y.y.y, x.x.x.x.

Beim Umbrella-Roaming-Client wird dadurch die 127.0.0.1-Datei überschrieben. Um sicherzustellen, dass das F5-VPN nicht durch eine endlose Änderungsschleife beeinträchtigt wird, unterbricht Umbrella die Umleitung, wenn 127.0.0.1 am Ende der DNS-Liste platziert oder schnell von 127.0.0.1 zurückgeändert wird.

In den meisten Fällen empfiehlt Umbrella die Verwendung des Umbrella Roaming Security-Moduls, das Teil des AnyConnect Roaming Security Clients ist. VPN muss nicht bereitgestellt werden (es kann bei der Installation vom Display für den Benutzer entfernt werden).

Die F5-Kompatibilität ist zu diesem Zeitpunkt definiert als eine erfolgreiche F5-VPN-Verbindung mit einem voll funktionsfähigen lokalen und öffentlichen DNS. Dies kann das Ergebnis eines ordnungsgemäßen Backoffs durch den Roaming-Client in einen ungeschützten Zustand sein. Bitte stellen Sie sicher, dass Ihre Netzwerkabdeckung während der Verwendung von F5 gewährleistet ist, indem Sie Ihr Netzwerk für Cisco Umbrella konfigurieren.

BigIP F5 VPN-Client

Der BigIP F5 Edge-Client ist derzeit der gebräuchlichste F5-VPN-Client. In vielen Bereitstellungen wird er jedoch durch den neuen F5-Client ersetzt. In diesem Artikel werden alle bekannten Interoperabilitätsprobleme mit dem F5-BigIP-Client behandelt.

F5 DNS-Relay-Proxy

Der Roaming-Client ist in Konfigurationen, die den F5-DNS-Relay-Proxy-Dienst aktivieren, nicht mit VPN-Client 2.2+ kompatibel. Dieser Relay-Proxy wird bekanntermaßen im Split-DNS-Modus und im DNS-basierten Split-Tunneling-Modus aktiviert. F5 kann nicht mit DNS-Namen verwendet werden, die mit dem Roaming-Client definiert wurden. Um Split-Tunneling mit F5 und dem Roaming-Client zu verwenden, verwenden Sie IP-basiertes Split-Tunneling anstelle von DNS-basiertem Split-Tunneling. Darüber hinaus können einige Konfigurationen und Versionen dazu führen, dass Umbrella überschrieben wird, obwohl Umbrella grün angezeigt wird, wenn der DNS-Relay-Proxy aktiviert ist.

Suche nach der Split-DNS- oder DNS-basierten Split Tunneling-Einstellung

F5 VPN Split Tunneling mit Split-DNS wird in der Form der Einstellung "DNS Address Space" (DNS-Adressraum) angezeigt. Wenn diese Funktion aktiv ist, wird der DNS-Proxy von F5 aktiviert, der mit dem Roaming-Client in Konflikt steht. Das Symptom ist ein Fehler beim Auflösen von A-Datensätzen, während sowohl der Roaming-Client als auch das VPN aktiv sind. Eine funktionierende Konfiguration finden Sie in diesem Screenshot:

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!

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.