Comprendre la compatibilité entre Umbrella Roaming Client et F5 VPN

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Introduction

Compatibilité VPN F5

Client VPN F5 BigIP

- Proxy de relais DNS F5
  - Recherche du paramètre de fractionnement en canaux ou DNS (Split Tunneling Setting)

Nouveau client F5

Introduction

Ce document décrit la compatibilité entre Cisco Umbrella Roaming Client et F5 VPN.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella Roaming Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Introduction

Le client d'itinérance Umbrella peut être utilisé dans une grande variété de configurations réseau et logicielles. Cet article présente tous les sujets de compatibilité connus avec le client VPN F5. Cet article commence par les comportements de détection attendus actuels, puis traite des notes de compatibilité spécifiques à F5 VPN.

Le client Umbrella a mis en oeuvre des mécanismes de détection automatisés pour réagir aux

changements de VPN afin de garantir le maintien de la fonctionnalité DNS. Cela peut entraîner le client à rester temporairement non protégé pendant que le VPN est connecté. Pour plus d'informations, reportez-vous à l'article Third-Party VPN Detection Heuristics with the Umbrella Roaming Client.

Compatibilité VPN F5

Dans de nombreuses configurations, le VPN F5 fonctionne en insérant les adresses DNS VPN dans les cartes réseau non VPN en pré-mettant les serveurs VPN en attente dans le DNS de la carte réseau. Ainsi, pour une configuration DNS locale x.x.x.x et une configuration VPN y.y.y.y, le résultat est y.y.y.y, x.x.x.x.

Avec le client d'itinérance Umbrella, cela remplace l'adresse 127.0.0.1 placée. Pour s'assurer que le VPN F5 n'est pas altéré par une boucle de modification sans fin, Umbrella arrête la redirection si 127.0.0.1 est placé à la fin de la liste DNS ou est rapidement modifié en s'éloignant de 127.0.0.1.

Dans la plupart des cas, Umbrella recommande l'utilisation du module de sécurité d'itinérance Umbrella qui fait partie du client de sécurité d'itinérance AnyConnect. Le déploiement du VPN n'est pas obligatoire (il peut être supprimé de l'affichage pour l'utilisateur au moment de l'installation).

La compatibilité F5 à ce stade est définie comme une connexion VPN F5 réussie avec des DNS locaux et publics entièrement fonctionnels. Cela peut être dû à un retour arrière en douceur du client itinérant vers un état non protégé. Assurez-vous que votre couverture réseau est en place lorsque vous utilisez F5 en configurant votre réseau pour Cisco Umbrella.

Client VPN F5 BigIP

Le client de périphérie F5 BigIP est le client VPN F5 le plus courant à l'heure actuelle. Cependant, il est remplacé par le nouveau client F5 dans de nombreux déploiements. Cet article traite de tous les problèmes d'interopérabilité connus avec le client F5 BigIP.

Proxy de relais DNS F5

Le client d'itinérance n'est pas compatible avec le client VPN 2.2+ dans les configurations qui activent le service proxy relais DNS F5. Ce proxy de relais est connu pour être activé en mode split-dns et en mode split tunneling basé sur DNS. F5 ne peut pas être utilisé avec les noms DNS définis avec le client en itinérance Pour utiliser la transmission tunnel partagée avec F5 et le client en itinérance à ce stade, utilisez la transmission tunnel partagée basée sur IP plutôt que la transmission tunnel partagée basée sur DNS. En outre, certaines configurations et versions peuvent entraîner le remplacement d'Umbrella, même si le voyant vert s'affiche lorsque le proxy de relais DNS est activé.

Recherche du paramètre de fractionnement en canaux ou DNS (Split Tunneling Setting)

La tunnellisation partagée VPN F5 avec split-dns apparaît sous la forme du paramètre « Espace d'adressage DNS ». Lorsqu'elle est active, cette option fait tourner vers le haut le propre proxy DNS de F5 qui est en conflit avec le client d'itinérance. Le symptôme est un échec de résolution des enregistrements A alors que le client d'itinérance et le VPN sont actifs. Reportez-vous à cette capture d'écran pour une configuration opérationnelle :

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!

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.