Umbrella口ーミングクライアントとF5 VPNの互換性について

内容

はじめに

このドキュメントでは、Cisco Umbrella口ーミングクライアントとF5 VPNの間の互換性について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrella口ーミングクライアントに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

はじめに

Umbrella口ーミングクライアントは、さまざまなネットワークおよびソフトウェア設定で使用できます。この記事では、F5 VPNクライアントとの既知の互換性に関するトピックをすべて取り上げています。この記事では、最初に現在予想されている検出動作について説明し、次にF5 VPN固有の互換性に関する注意事項について説明します。

Umbrellaクライアントには、VPNの変更に対応してDNS機能を維持するための自動検出メカニズムが実装されています。これにより、VPNが接続されている間、クライアントが一時的に保護されないままになる可能性があります。詳細については、「Umbrella Roaming Clientを使用したサードパーティ製VPN検出ヒューリスティック」を参照してください。

F5 VPN互換性

多くの設定では、F5 VPNは、VPNサーバをNICのDNSに事前に保留することによって、非VPN NICにVPN DNSアドレスを挿入することによって機能します。したがって、x.x.x.xのローカルDNS設定とy.y.y.yのVPN設定の場合、結果はy.y.y.y、x.x.x.xになります。

Umbrellaローミングクライアントでは、これは配置された127.0.0.1を上書きします。F5 VPNが無限の変更ループで損なわれないようにするため、127.0.0.1がDNSリストの最後に配置されているか、127.0.0.1から急速に戻された場合、Umbrellaはリダイレクトを停止します。

ほとんどの場合、Umbrellaでは、AnyConnectローミングセキュリティクライアントの一部であるUmbrellaローミングセキュリティモジュールを使用することをお勧めします。VPNを導入する必要はありません（インストール時にユーザに対して表示から削除できます）。

この時点でのF5互換性は、完全に機能するローカルおよびパブリックDNSを使用したF5 VPN接続の成功と定義されます。これは、ローミングクライアントによる保護されていない状態への正常なバックオフの結果である可能性があります。F5キーを押しながら、Cisco Umbrellaのネットワークを設定して、ネットワーク上のカバレッジが適切であることを確認してください。

BigIP F5 VPNクライアント

BigIP F5エッジクライアントは、現時点で最も一般的なF5 VPNクライアントです。ただし、多くの導入では、新しいF5クライアントに置き換えられています。 この記事では、F5 BigIPクライアントとの相互運用性に関する既知の問題について説明します。

F5 DNSリレープロキシ

F5 DNSリレープロキシサービスをアクティブにする設定では、ローミングクライアントはVPN Client 2.2+と互換性がありません。このリレープロキシは、split-dnsモードおよびDNSベースのスプリットトンネリングモードでアクティブ化されることが確認されています。F5は、ローミングクライアントで定義されたDNS名では使用できません。現時点でF5とローミングクライアントでスプリットトンネリングを使用するには、DNSベースのスプリットトンネリングではなく、IPベースのスプリットトンネリングを使用します。また、一部の設定とバージョンでは、DNSリレープロキシがアクティブ化されると緑色で表示されているにもかかわらず、Umbrellaが上書きされる可能性があります。

split-dnsまたはDNSベースのスプリットトンネリング設定の検索

split-dnsを使用したF5 VPNスプリットトンネリングは、「DNS Address Space」設定の形式で表示されます。アクティブな場合、ローミングクライアントと競合するF5独自のDNSプロキシがスピンアップします。症状は、ローミングクライアントとVPNの両方がアクティブである間にAレ

コードを解決できないことです。有効な設定については、次のスクリーンショットを参照してください。

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!

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。