Entender a compatibilidade do Umbrella Roaming Client e da VPN F5

Contents

Introdução

Este documento descreve a compatibilidade entre o Cisco Umbrella Roaming Client e o F5 VPN.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella Roaming Client.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Introdução

O cliente de roaming Umbrella pode ser usado em uma grande variedade de configurações de rede e software. Este artigo documenta todos os tópicos de compatibilidade conhecidos com o cliente VPN F5. Este artigo começa com os comportamentos de detecção esperados no momento e discute as notas de compatibilidade específicas da VPN F5.

O cliente Umbrella implementou mecanismos de detecção automatizados para reagir a alterações de VPN para garantir que a funcionalidade de DNS seja mantida. Isso pode fazer com que o cliente permaneça temporariamente desprotegido enquanto a VPN está conectada. Consulte o artigo Heurística de detecção de VPN de terceiros com o cliente Umbrella Roaming para obter mais detalhes.

Compatibilidade de VPN F5

Em muitas configurações, a VPN F5 funciona inserindo os endereços DNS da VPN em NICs não-VPN ao pré-aguardar os servidores VPN para o DNS da NIC. Portanto, para uma configuração de DNS local de x.x.x.x e uma configuração de VPN de y.y.y.y, o resultado é y.y.y.y, x.x.x.x.

Com o cliente de roaming Umbrella, isso substitui o 127.0.0.1 colocado. Para garantir que a VPN F5 não seja prejudicada por um loop de alteração sem fim, o Umbrella pára de redirecionar se 127.0.0.1 for colocado no final da lista DNS ou for rapidamente alterado de volta para 127.0.0.1.

Na maioria dos casos, a Umbrella recomenda o uso do módulo de segurança de roaming Umbrella que faz parte do cliente de segurança de roaming AnyConnect. A VPN não precisa ser implantada (ela pode ser removida da exibição para o usuário no momento da instalação).

A compatibilidade F5 neste momento é definida como uma conexão VPN F5 bem-sucedida com DNS local e público totalmente funcionais. Isso pode ser resultado de um backoff gracioso do cliente de roaming para um estado desprotegido. Certifique-se de que sua cobertura na rede esteja em vigor ao usar F5 configurando sua rede para o Cisco Umbrella.

Cliente VPN F5 BigIP

O cliente de borda F5 BigIP é o cliente VPN F5 mais comum no momento. No entanto, ele está sendo substituído pelo novo cliente F5 em muitas implantações. Este artigo discute todas as preocupações de interoperabilidade conhecidas com o cliente F5 BigIP.

Proxy de Retransmissão DNS F5

O cliente de roaming não é compatível com o cliente VPN 2.2+ em configurações que ativam o serviço Proxy de Retransmissão DNS F5. Esse proxy de retransmissão é conhecido por ser ativado no modo split-dns e nos modos de tunelamento dividido baseados em DNS. F5 não pode ser usado com nomes DNS definidos com o cliente de roaming. Para usar o tunelamento dividido com F5 e o cliente de roaming no momento, use o tunelamento dividido baseado em IP em vez do tunelamento dividido baseado em DNS. Além disso, algumas configurações e versões podem fazer com que o Umbrella seja substituído, apesar de mostrar verde quando o Proxy de Retransmissão DNS é ativado.

Localizar a Configuração de Túnel Dividido Baseada em DNS ou split-dns

O F5 VPN Split Tunneling com split-dns aparece na forma da configuração "DNS Address Space". Quando ativo, ele ativa o próprio proxy DNS de F5 que entra em conflito com o cliente de

roaming. O sintoma é uma falha ao resolver registros A enquanto o cliente de roaming e a VPN estão ativos. Veja esta captura de tela para uma configuração de trabalho:

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!

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.