

Umbrella and F5 BIG-IP Edge Client VPN Interoperability Issue

Contents

Issue

Users experience complete loss of internet access when both Cisco Umbrella (Secure Client) and F5 BIG-IP Edge Client VPN are enabled simultaneously.

The issue manifests as follows:

- Internet connectivity is completely unavailable after connecting to the BIG-IP Edge Client VPN when Cisco Umbrella is active.
- The problem affects all internet resources and websites, not just specific URLs
- VPN connectivity to internal project-related applications works as expected
- Internet access functions normally when Cisco Umbrella is disabled
- The issue occurs exclusively when both services are running concurrently

Environment

- Cisco Secure Client with Umbrella module enabled
- F5 BIG-IP Edge Client VPN configured for split tunneling
- F5 DNS Relay Proxy Service enabled
- Windows endpoint environment

Resolution

This interoperability issue requires implementing one of two supported workarounds to resolve the DNS

traffic conflict between Cisco Umbrella and F5 BIG-IP Edge Client VPN.

Option 1: Disable F5 DNS Relay Proxy Service

The first resolution approach involves disabling the F5 DNS Relay Proxy Service on the BIG-IP Edge Client configuration:

Step 1: Access the F5 BIG-IP Edge Client configuration interface

Step 2: Navigate to the DNS Relay Proxy Service settings

Step 3: Disable the DNS Relay Proxy Service



Note: This approach restores normal Umbrella DNS functionality but can impact the current split-tunnel design depending on your F5 configuration requirements.

Option 2: Configure F5 VPN Split-Tunneling Exclusions

The recommended resolution involves configuring the F5 BIG-IP Edge Client to exclude Umbrella traffic from VPN tunneling:

Step 1: Contact your F5 Administrator to modify the BIG-IP Edge Client configuration

Step 2: Configure the split-tunneling list to explicitly exclude all network traffic destined for Umbrella DNS and Proxy IP ranges

Step 3: Apply the configuration changes to ensure Umbrella security traffic functions alongside the VPN connection



Tip: This configuration change must be implemented by the F5 Administrator and requires specific knowledge of the Umbrella DNS and proxy IP ranges to ensure proper exclusion from the VPN tunnel.

Cause

This issue results from a known interoperability limitation between Cisco Secure Client (Umbrella module) and F5 BIG-IP Edge Client VPN when the VPN is configured for split tunneling with the F5 DNS Relay Proxy Service enabled.

The root cause occurs because both the Umbrella client and the F5 VPN client attempt to intercept and proxy DNS traffic at the endpoint level. When both services are active simultaneously, this creates a conflict where DNS requests are not forwarded correctly, resulting in complete loss of internet connectivity. The F5 DNS Relay Proxy Service interferes with the Umbrella DNS interception mechanism, preventing proper DNS resolution for internet resources.

This behavior is documented by both Cisco and F5 as a known limitation and is not related to a specific software defect in either product.

Related Content

- [DNS issues with BIG-IP Edge Client and Cisco Umbrella Client](#)
- [Understand Umbrella Roaming Client and F5 VPN Compatibility](#)
- [Cisco Technical Support & Downloads](#)