

Umbrella- und F5 BIG-IP Edge Client VPN Interoperabilitätsproblem

Inhalt

Problem

Wenn Cisco Umbrella (Secure Client) und F5 BIG-IP Edge Client VPN gleichzeitig aktiviert sind, geht der Internetzugriff vollständig verloren.

Das Problem manifestiert sich wie folgt:

- Wenn Cisco Umbrella aktiv ist, ist nach dem Herstellen einer Verbindung mit dem BIG-IP Edge Client VPN die Internetverbindung komplett unterbrochen.
- Das Problem betrifft alle Internetressourcen und Websites, nicht nur bestimmte URLs
- VPN-Verbindung zu internen projektbezogenen Anwendungen funktioniert wie erwartet
- Internetzugang funktioniert normal, wenn Cisco Umbrella deaktiviert ist
- Das Problem tritt ausschließlich dann auf, wenn beide Dienste gleichzeitig ausgeführt werden

Umwelt

- Cisco Secure Client mit aktiviertem Umbrella-Modul
- F5 BIG-IP Edge Client VPN für Split-Tunneling konfiguriert
- F5 DNS-Relay-Proxydienst aktiviert
- Windows-Endgeräteumgebung

Auflösung

Dieses Interoperabilitätsproblem erfordert die Implementierung einer von zwei unterstützten Problemumgehungen, um den DNS-Datenverkehrskonflikt zwischen Cisco Umbrella und F5 BIG-IP Edge Client VPN zu lösen.

Option 1: F5 DNS-Relay-Proxydienst deaktivieren

Der erste Lösungsansatz beinhaltet die Deaktivierung des F5 DNS-Relay-Proxy-Service in der Konfiguration des BIG-IP-Edge-Clients:

Schritt 1: Zugriff auf die Konfigurationsschnittstelle des BIG-IP Edge-Clients

Phase 2: Navigieren zu den Einstellungen des DNS-Relay-Proxydiensts

Schritt 3: Deaktivieren des DNS-Relay-Proxydiensts



Anmerkung: Dieser Ansatz stellt die normale Umbrella DNS-Funktionalität wieder her, kann sich jedoch je nach Ihren F5-Konfigurationsanforderungen auf das aktuelle Split-Tunnel-Design auswirken.

Option 2: Ausschlüsse für F5-VPN-Split-Tunneling konfigurieren

Die empfohlene Lösung umfasst die Konfiguration des F5 BIG-IP Edge-Clients, um Umbrella-Datenverkehr vom VPN-Tunneling auszuschließen:

Schritt 1: Wenden Sie sich an Ihren F5-Administrator, um die Konfiguration des BIG-IP Edge-Clients zu ändern.

Phase 2: Konfigurieren Sie die Split-Tunneling-Liste so, dass der gesamte Netzwerkverkehr für Umbrella DNS- und Proxy-IP-Bereiche explizit ausgeschlossen wird.

Schritt 3: Übernehmen Sie die Konfigurationsänderungen, um sicherzustellen, dass Umbrella neben der VPN-Verbindung auch die Sicherheitsfunktionen übernimmt.



Tipp: Diese Konfigurationsänderung muss vom F5-Administrator implementiert werden und erfordert spezielle Kenntnisse der Umbrella DNS- und Proxy-IP-Bereiche, um einen ordnungsgemäßen Ausschluss aus dem VPN-Tunnel sicherzustellen.

Ursache

Dieses Problem resultiert aus einer bekannten Interoperabilitätsbeschränkung zwischen dem Cisco Secure Client (Umbrella-Modul) und dem F5 BIG-IP Edge Client VPN, wenn das VPN für Split-Tunneling mit aktiviertem F5 DNS-Relay-Proxy-Service konfiguriert ist.

Die Ursache liegt darin, dass sowohl der Umbrella Client als auch der F5 VPN Client versuchen, den DNS-Datenverkehr auf Endpunktebene abzufangen und als Proxy zu verwenden. Wenn beide Dienste gleichzeitig aktiv sind, führt dies zu einem Konflikt, bei dem DNS-Anfragen nicht richtig weitergeleitet werden, was zu einem vollständigen Verlust der Internetverbindung führt. Der F5 DNS Relay Proxy Service stört den Umbrella DNS Interception Mechanismus und verhindert eine korrekte DNS Auflösung für Internetressourcen.

Dieses Verhalten wird sowohl von Cisco als auch von F5 als bekannte Einschränkung dokumentiert und steht in keinem Zusammenhang mit einem bestimmten Softwarefehler in einem der beiden Produkte.

Verwandte Inhalte

- [DNS-Probleme mit BIG-IP Edge-Client und Cisco Umbrella Client](#)
- [Verständnis der Kompatibilität von Umbrella Roaming Client und F5 VPN](#)
- [Technischer Support und Downloads von Cisco](#)

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.