OpenVPN Profil erstellen

20.04.2024 16:46:15

FAQ-Artikel-Ausdruck

Kategorie:	Datennetz::VPN-Zugang	**Bewertungen:**	8
Status:	öffentlich (Alle)	**Ergebnis:**	25.00 %
Sprache:	de	**Letzte Aktualisierung:**	08:31:20 - 15.11.2023

Schlüsselwörter

VPN OpenVPN ProfilGenerator

Lösung (öffentlich)

Im Self-Service-Portal erhalten Nutzer:innen die Möglichkeit, sich auf ihr System und Anforderungen abgestimmte OpenVPN-Profile zu generieren. Die OpenVPN-Programme erlauben den Import mehrerer Profile. Sie können das Profil hier herunterladen und konfigurieren:
[1]https://selfservice.tu-dresden.de/services/vpn/openvpn

Nutzer:innen wird ein empfohlenes Profil angeboten, das sie anpassen können. Bei der Anpassung gehen sie in vier Schritten vor.

Schritt 1: Betriebssystem auswählen

Sie können zwischen fünf Betriebssystemen wählen:

-

Windows

-

Linux

-

macOS

-

iOS

-

Android

Mit dieser Auswahl sind die gängigsten Betriebssysteme abgedeckt. Sollte Ihr Betriebssystem hier nicht aufgeführt sein, probieren Sie eines der aufgeführten. In den meisten Fällen, sind die Profile für unterschiedliche Betriebssysteme gleich.

Schritt 2: Tunneling-Modus auswählen

Beim Tunneling werden zwei Arten unterschieden:

-

Full Tunneling

-

Split Tunneling

Mit dieser Auswahl entscheiden Sie, welche Daten über den sicheren "Tunnel" übertragen werden.

Full Tunneling

Beim Full Tunneling wird der gesamte Internet-Verkehr durch einen verschlüsselten Tunnel übertragen, um Ihre Daten vor Hackern und Schnüfflern zu schützen. Sie bauen also eine Verbindung zum Campus-Netz der TU Dresden auf und gehen aus diesem sicheren Netz ins Internet.

Aus Sicht von Zielen im Internet (wie z.B. Online-Journalen) haben Sie eine Adresse der TU Dresden.

Full Tunneling Split Tunneling

Beim Split-Tunneling erfolgen nur Verbindungen zu Zielen im Campus-Netz der TU Dresden über den verschlüsselten VPN-Tunnel. Verbindungen zu Zielen außerhalb der TU Dresden erfolgen direkt ohne Umweg über die TU Dresden. Dadurch wird die Geschwindigkeit und Latenz für Verbindungen außerhalb der TU Dresden verbessert. Schutzmaßnahmen vor bösartigen Servern im Internet, die durch das ZIH bzw. das CERT im Campusnetz umgesetzt werden, sind auf Ihrem System nicht oder nur eingeschränkt wirksam.

Aus Sicht von Zielen im Internet (wie z.B. Online-Journalen) haben Sie jedoch keine Adresse der TU Dresden.

Split Tunneling Schritt 3: Transportprotokoll und Port setzen

Die OpenVPN-Verbindung kann über verschiedene Transportprotokolle und Port-Nummern aufgebaut werden. Im Allgemeinen ist immer die Standard-Variante UDP 1194 zu wählen. Es kann jedoch sein, dass in manchen Netzwerken (z.B. in manchen öffentlichen WLANs) besonders restriktive Zugangsregeln herrschen, welche Verbindung mittels UDP 1194 aktiv limitieren/benachteiligen oder sogar komplett blockieren.

Für diese Fällen ermöglichen wir Ihnen alternativ den Zugang über andere Port-Nummern oder das Transportprotokoll TCP. Probieren Sie bei Problemen die Alternativen in der folgenden Reihenfolge:

UDP 1194 (Empfohlen)

UDP 53

TCP 1194

TCP 443

VPN-Verbindungen über TCP empfehlen wir nur in absoluten Ausnahmefällen in denen überhaupt keine oder keine stabile Verbindung per UDP erreicht werden kann. VPN über TCP kann zu erheblichen Geschwindigkeitseinbußen und Latenzproblemen (TCP Meltdown) führen.

Schritt 4: Zusammenfassung und Download der Datei

Abschließend werden die gewählten Einstellungen zusammengefasst dargestellt und die Profil-Datei zum Herunterladen angeboten.

[1] https://selfservice.tu-dresden.de/services/vpn/openvpn