FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
52425 Jülich, ☎ (02461) 61-6402

JuNet-Helpdesk, ☎ (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0387
W.Anrath,S.Werner,M.Meier

19.02.2024

L2TP over IPSEC

Built-in VPN für
Microsoft Windows, macOS und Linux

1. Einleitung

Virtual Private Networks, kurz VPNs, minimieren die Gefährdungspotentiale einer Datenübertragung durch unsichere öffentliche Netze. Diese Technologie nutzt kryptografische Verfahren zum Aufbau eines sicheren Zugangs zu einem Firmennetz. Diese Anleitung beschreibt die Konfiguration und den Einsatz der in den Betriebssystemen Windows 10, Linux und macOS integrierten L2TP over IPSEC Implementierungen (Built-in VPN); Ziel ist die Nutzung interner Dienste im JuNet (Intranet).

Zur Technologie - Hintergrundinformation: Als Baustein für Virtual Private Networks (VPN) favorisiert Microsoft das Layer 2 Tunneling Protocol (L2TP), wobei zur Sicherstellung der VPN-Eigenschaften Vertraulichkeit, Integrität und Authentizität das Standardprotokoll IPSEC (Internet Protocol Security) verwendet wird. Die Kombination dieser beiden Protokolle wird L2TP over IPSEC genannt und von der Internet Engineering Task Force (IETF) standardisiert – die RFCs 2661 (LT2P) und RFC 3193 (Securing L2TP over IPSEC) beschreiben den Protokollstandard.

Beim Zugang aus dem Internet kann dieses VPN-Protokoll genutzt werden. Alternativ kann die Cisco Secure Client/AnyConnect VPN Lösung (FZJ-JSC-TKI-0410, vgl. FAQ ‚IPv6 Support') zum Einsatz kommen. Ein wesentlicher Vorteil dabei ist, dass die L2TP-Lösung bereits Bestandteil diverser Betriebssysteme ist. **Falls Sie im HomeOffice einen DS-Lite Anschluss (UnityMedia/Vodafone/DN-CONNECT) haben, beachten Sie bitte den Hinweis ‚DS-Lite und L2TP' im FAQ zur Gatewayauswahl.**

Zulassungen/Accounts (Mitarbeiter) zur VPN-Benutzung können beim Dispatch im JSC beantragt werden:

https://intranet.fz-juelich.de/de/organisation/it-portal/software_services/infrastruktur/vpn

Sollten Zugänge für Kooperationspartner erforderlich sein, ist eine individuelle Konfiguration nötig. Für Beratung und Fragen dazu stehen die Ansprechpartner im JSC zur Verfügung (EMAIL: vpn@fz-juelich.de).

2. Unterstützte Plattformen

Microsoft unterstützt seit der Einführung von Windows XP das Protokoll L2TP over IPSEC. L2TP over IPSEC gehört seitdem zum Standardlieferumfang aller Windows Betriebssysteme. Die Betriebssysteme Linux sowie macOS unterstützen ebenfalls L2TP over IPSEC Implementierung.

3. Konfiguration - Windows 10

Zuerst in der Systemsteuerung das Netzwerk- und Freigabecenter öffnen:

Systemsteuerung - Alle Systemsteuerungselemente - Netzwerk- und Freigabecenter

Danach unter 'Netzwerkeinstellungen ändern' die Option

Neue Verbindung oder neues Netzwerk einrichten

auswählen.

Im nächsten Schritt wird die Verbindungsoption

Verbindung mit dem Arbeitsplatz herstellen

gewählt.

Weiter geht es mit der Auswahl

eine neue Verbindung erstellen

Im folgenden Menu wird die Option

Die Internetverbindung (VPN) verwenden

ausgewählt.

Im Feld Internetadresse wird der vollqualifizierte Namen des VPN-Gateways eingetragen

l2tpgate.zam.kfa-juelich.de

und ein Name für die Verbindung festgelegt - z.B.:

FZJ-L2TP-A

Nach dem Erstellen der Verbindung sind noch einzelne Parameter anzupassen - im Menu

Systemsteuerung - Alle Systemsteuerungselemente - Netzwerk- und Freigabecenter

wird die die Option

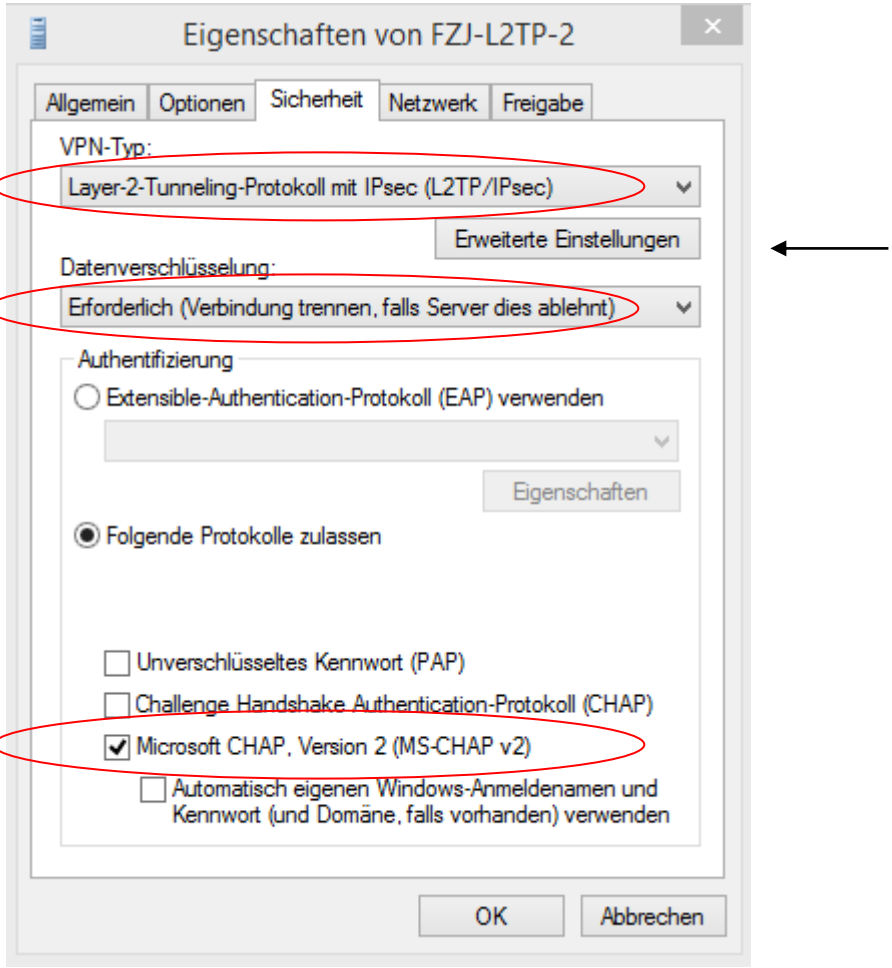
Adaptereinstellungen ändern

geöffnet.

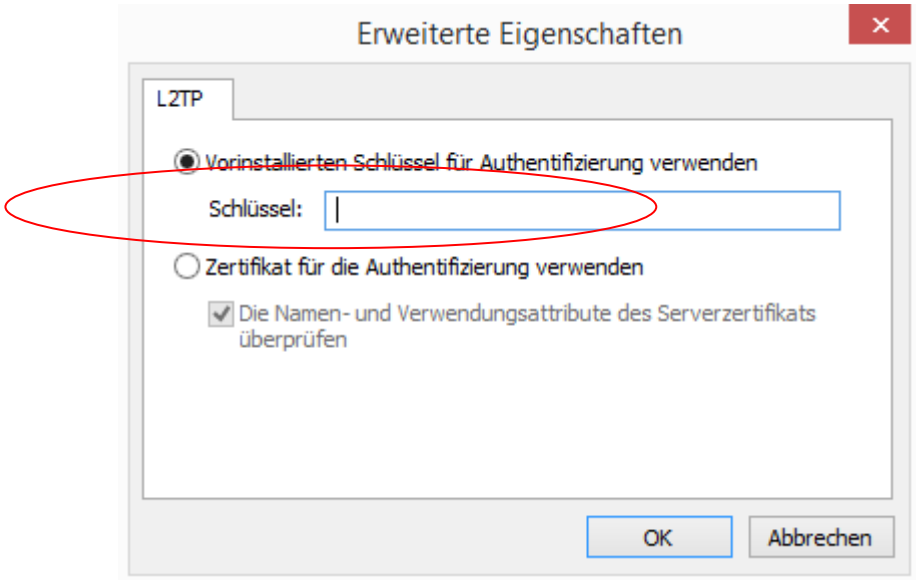
Die 'Eigenschaften' der neuen Verbindung 'FZJ-L2TP-A' werden geöffnet und in der Registerkarte

Sicherheit

können die nötigen Anpassungen vorgenommen werden



Klicken Sie auf den Button ‚Erweiterte Einstellungen'. Sie haben dann Zugriff auf die folgende Registerkarte.



Der sogenannte PresharedKey aus der "JSC Office for User Services" Anmeldebestätigung (vorinstallierter Schlüssel/Shared Secret) ist einzutragen.

Die VPN-Verbindung ist fertiggestellt und funktionsfähig.

Wichtiger Hinweis: Als Backup kann diese Verbindung kopiert werden und als VPN-Server l2tpgateb.zam.kfa-juelich.de eingetragen werden und die Verbindung FZJ-L2TP-B genannt werden. Damit steht eine zweite unabhängige VPN-Verbindung zur Verfügung (bei Störungen, Problemen, Wartungsarbeiten usw.).

Häufige Fehlermeldungen – Windows 10:

(I)

‚Verbindung mit FZJ-L2TP-A' nicht möglich – Die Remoteverbindung wurde nicht hergestellt, da der Name des RAS-Servers nicht aufgelöst wurde.

Ursache u. Lösung: der VPN-Gatewayname ist nicht korrekt; erster Buchstabe ist ein kleines L (wie lustig)

(II)

‚***Verbindung mit FZJ-L2TP-A' nicht möglich – Der L2TP-Verbindungsversuch ist fehlgeschlagen, da ein Verarbeitungsfehler während der ersten Sicherheitsaushandlung mit dem Remotecomputer aufgetreten ist.***

Ursache u. Lösung: (a) meist wurde der vorinstallierte Schlüssel nicht korrekt eingegeben (b) eine Firewall-Regel blockiert den VPN-Verkehr (c) die Windows-Dienste IKE und AuthIP IPsec-Schlüsselerstellungsmodule sind abgeschaltet (oftmals liegt ein Installationskonflikt mit einer anderen IPSEC-Software z.B. AVM vor); reaktivieren Sie den automatischen Start in Systemsteuerung -> Verwaltung -> Dienste

(III)

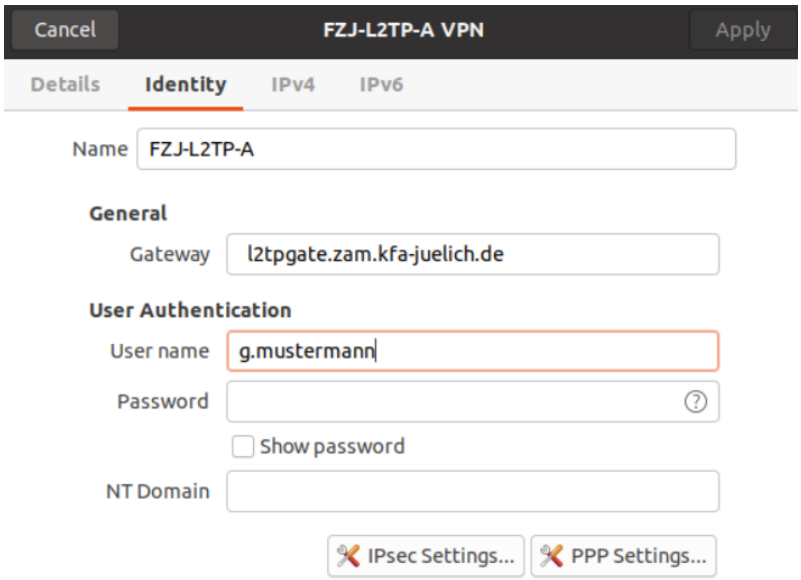
‚Der Nutzername bzw. das Kennwort ist falsch'

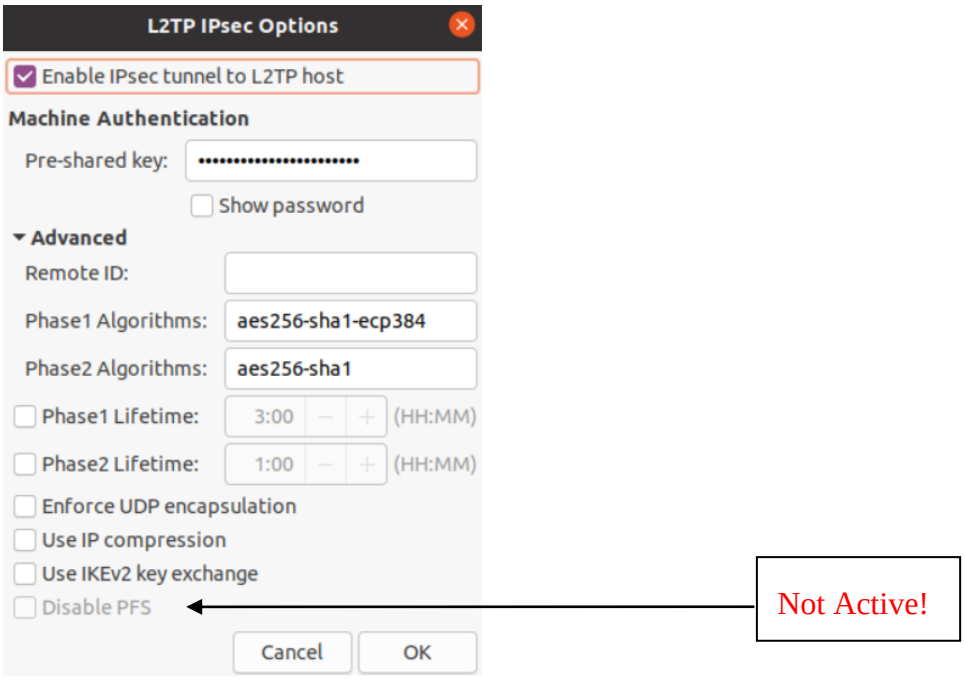
Ursache u. Lösung: die VPN-Anmeldeinformationen sind nicht korrekt. Bitte prüfen Sie die Eingabe.

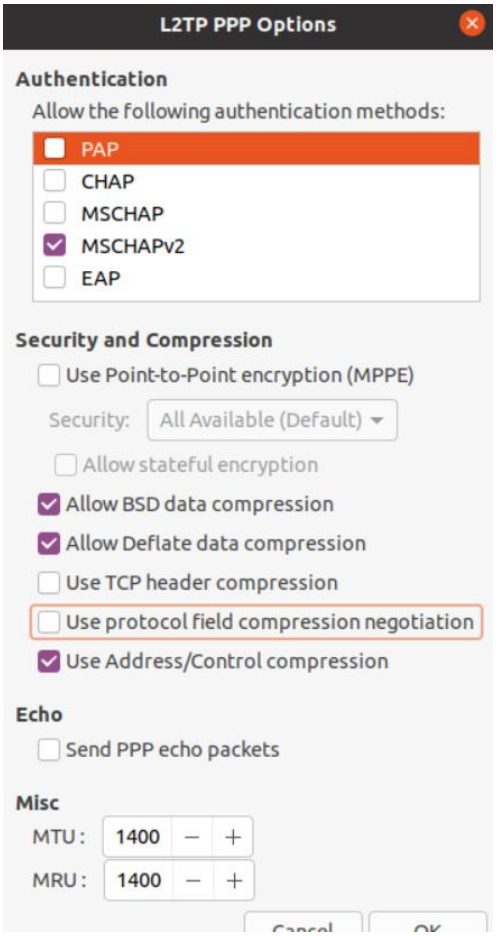
4. Konfiguration – Linux/Ubuntu 22.04 LTS

Auch Linux-Anwender (hier: Ubuntu mit strongSwan IPSEC) können eine VPN-Verbindung mittels L2TP over IPSEC nutzen.

Nach Installation der nötigen Plugins für den Network-Manager (network-manager-l2tp) und Gnome (network-manager-l2tp-gnome) kann die Konfiguration (Gnome-Desktop GUI) erfolgen:







Fehleranalyse – SYSLOG:

Der NetworkManager schreibt LOGGING- und DEBUG-Informationen in Abhängigkeit von der jeweiligen Systemkonfiguration; die konfigurierten Einstellungen können mittels

$ nmcli general logging

geprüft und dann mittels

$ nmcli general logging level <level> domain <domain>

geändert werden.

Explizit kann zur Nachbesserung oder zum Erstellen neuer Verbindungen die grafische Oberfläche ‚nm-connection-editor' aufgerufen werden. Die Bearbeitung erfolgt in den beschriebenen Schaltflächen ‚IPSEC settings' bzw. ‚PPP settings'.

5. Konfiguration - macOS

L2TP over IPSEC kann auf macOS ohne zusätzlichen Installationsaufwand konfiguriert werden. Die folgenden Bilder zeigen die nötigen Konfigurationseinstellungen, die folgende Schritte umfasst:

Systemeinstellung/Netzwerk

Schloss öffnen

+ klicken zum Hinzufügen einer Verbindung

VPN & L2TP auswählen

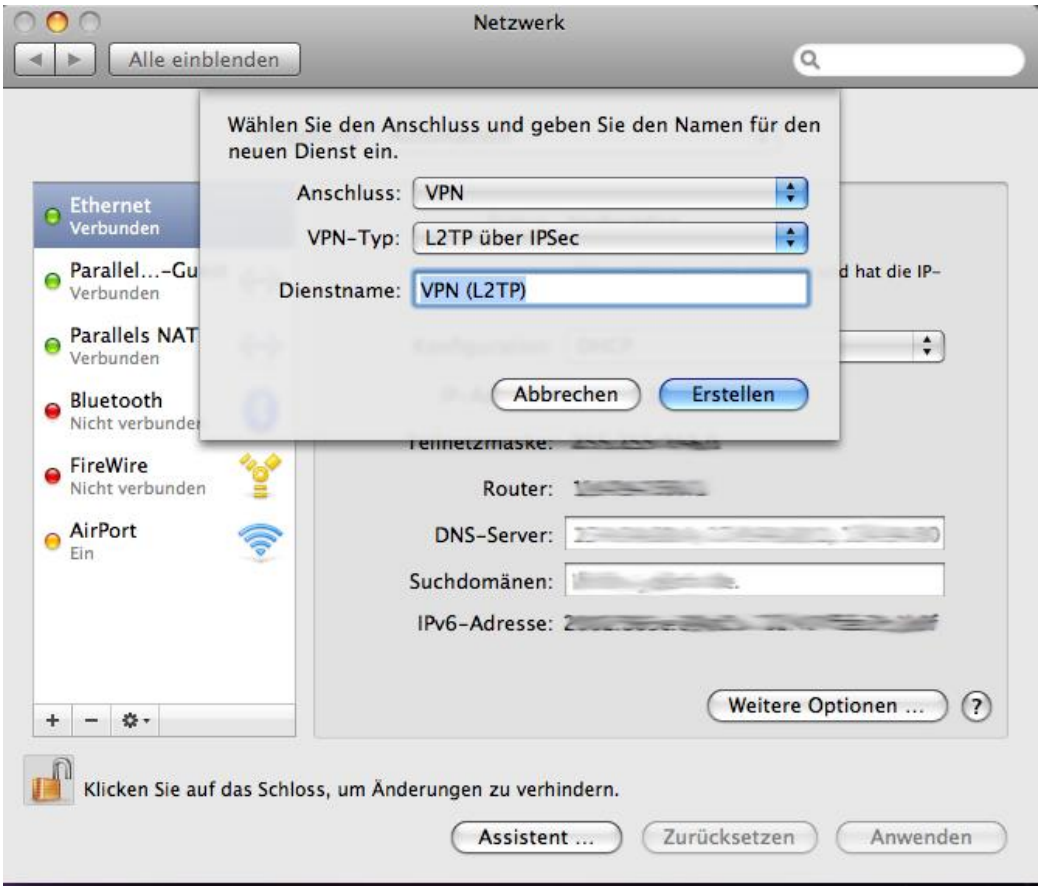
VPN Gateway (vollqualifizierter Name) und Benutzername eingeben

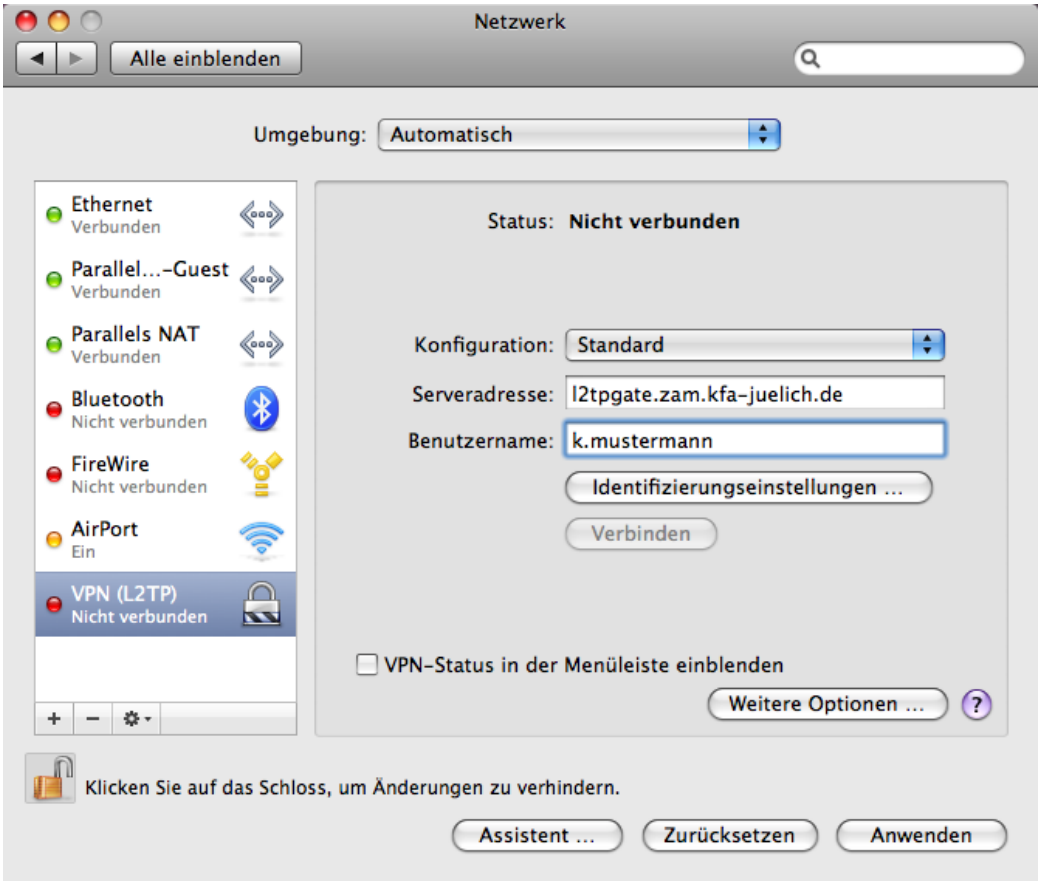
Identifizierungseinstellungen eingeben (Shared Secret=vorinstallierter Schlüssel)

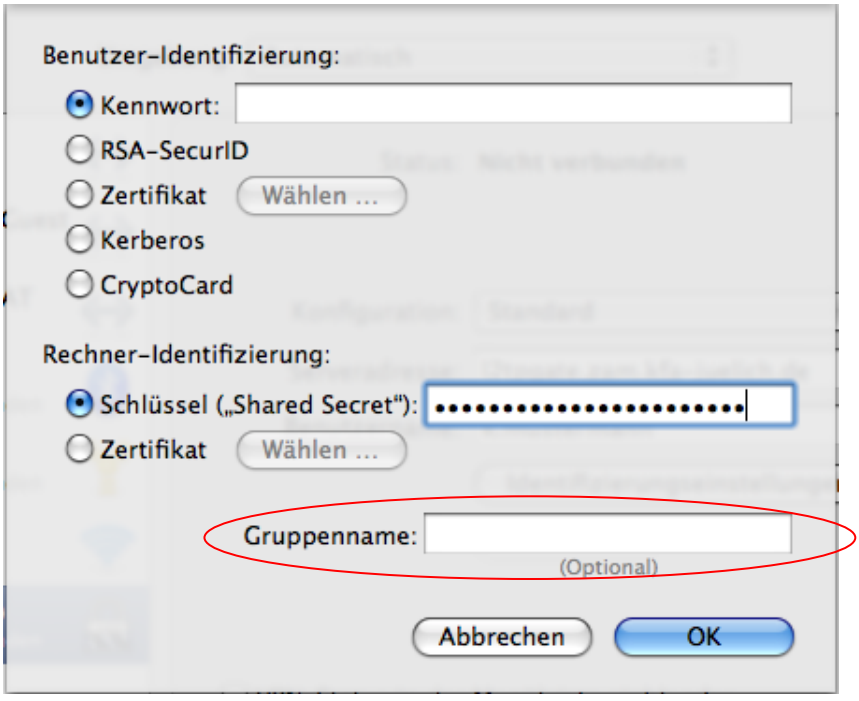
"Anwenden" klicken

"Verbinden" klicken

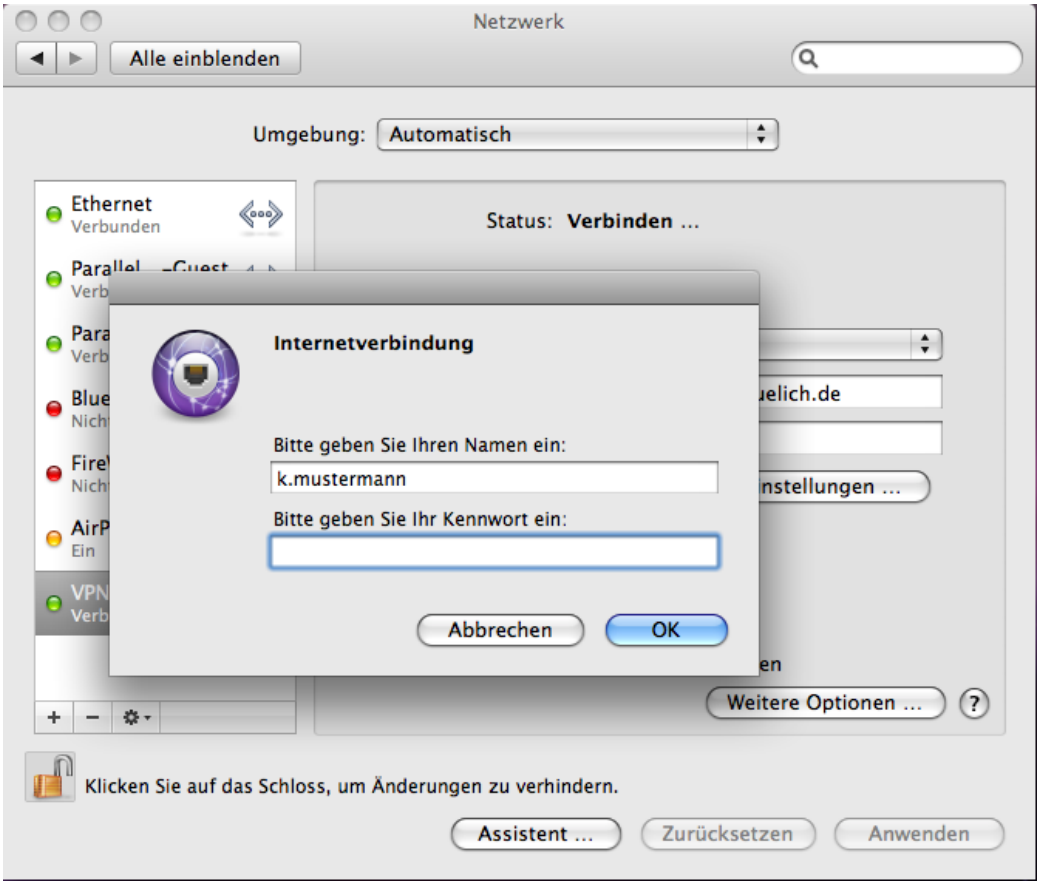
VPN-User Passwort beim Verbindungsaufbau eingeben







Das Eingabefeld ‚Gruppenname' muss leer bleiben!



Im Anwendungsfenster sind während der Verbindungsdauer Anzeigen zur Verbindungsdauer, der erhaltenen IP-Adresse und zum Verkehr (Gesendet bzw. Empfangen (metrisch)) dargestellt.

Besondere Hinweise:

Voreinstellungen: Nur Traffic zu 134.94.0.0/16 wird durch den VPN-Tunnel geleitet; diese Einstellung entspricht der Gruppen-Policy „fzj“ bei den Cisco VPN-Policies. Eine Änderung kann über den Button „Optionen“ erfolgen. Falls also **ZB Online-Services (Zeitschriften)** genutzt werden sollen, kann der gesamte Traffic (Internet Upstream) durch den Tunnel laufen. (weitere Detailinfo mit Bild im FAQ)

Aktivierung von Logging:
„Optionen“-Button → unter „weitere VPN-Optionen“
„Ausführliches Protokoll“ aktivieren
Unter /var/log werden dann Details über den Verbindungsaufbau in die Datei racoon.log und ppp.log geschrieben (nur für root bzw. Administratorrechten lesbar)

Im Anwendungsfenster sind während der Verbindungsdauer Anzeigen zur Verbindungsdauer, der erhaltenen IP-Adresse und zum Verkehr (Gesendet bzw. Empfangen (metrisch)) enthalten.

Fehlerfälle:

- Falscher Schlüssel (Shared Secret / PreSharedKey):

Erneuter Prompt auf Passwort, dann Fehlermeldung: „Der L2tp-VPN-Server antwortet nicht. Versuchen Sie erneut, eine Verbindung herzustellen. Wenn das Problem weiterhin besteht, überprüfen Sie die Einstellungen und wenden Sie sich an Ihren Administrator.“

- Falsches Passwort:
  Im Prompt auf Passwort Fehlermeldung: Ihr Benutzername oder Kennwort sind falsch. Nach dem zweiten falschen Passwort kommt Fehlermeldung: „Ihr Kommunikationsgerät hat die Verbindung getrennt. Versuchen Sie erneut, eine Verbindung herzustellen. Wenn das Problem weiterhin besteht, überprüfen Sie die Einstellungen und wenden Sie sich an Ihren Administrator.“

6. Ausblick

Die L2TP over IPSEC Unterstützung wird von Microsoft in allen aktuellen Betriebssystemversionen angeboten. Zum Verbindungsaufbau mit PreSharedKeys (Schlüssel) können die VN-Gateways

l2tpgate.zam.kfa-juelich.de bzw. l2tpgateb.zam.kfa-juelich.de (Backup)

genutzt werden. Tablets und Smartphones (Apple/Android < 13) unterstützen in der Regel auch diese VPN-Variante.

Falls IPv6 Unterstützung benötigt wird, ist die TKI-0410 (Cisco Secure Client/AnyConnect VPN) anzuwenden. beachten Sie bitte in diesem Zusammenhang die Information der ZB

Zugriff über VPN auf die elektronischen Lizenzen und Services der Zentralbibliothek (fz-juelich.de)

7. FAQ

Wer sind die richtigen Ansprechpartner bei weiteren Fragen?

Bei Fragen zum VPN-Antrag und Password-Reset

Ansprechpartner: "JSC Office for User Services" Telefon: 02461 61- 5642

E-Mail: user-services.jsc@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit:

Name und Organisationseinheit, VPN-Benutzername (z.B. m.mustermann)

Datum und Uhrzeit der Antragsstellung bzw. des Passwort-Resets

Bei Verbindungsproblemen und techn. Problemen

Ansprechpartner: Abteilung Kommunikationssysteme im JSC

Telefon: 02461 61 – 6440 E-Mail: vpn@fz-juelich.de

Halten Sie bitte die folgenden Informationen bereit oder teilen Sie diese mit:

Name und Organisationseinheit, VPN-Benutzername

Betriebssystem, Internet Provider zu Hause (Telekom, Vodafone, etc.)

IP-Adressen, die vom Provider zugewiesen wurden

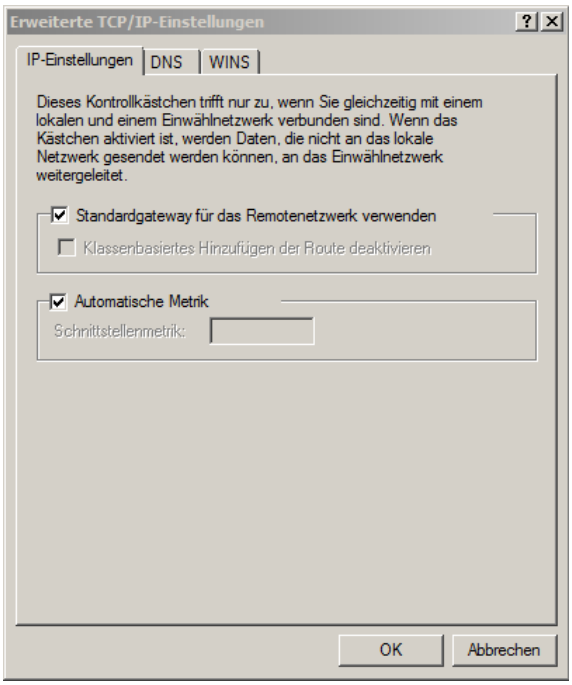
Datum und Uhrzeit, wann Ihr Problem auftrat.

Welche Vorteile hat L2TP over IPSEC auf Windows-Systemen gegenüber den CISCO VPN Lösungen?

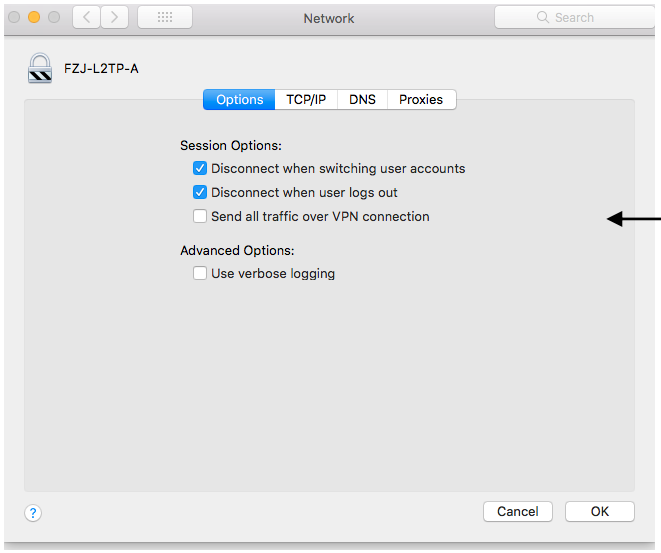
Es muss keine zusätzliche Software installiert werden.

Kann L2TP over IPSEC eine Split-Tunnel-Verbindung aufbauen?

Ja. Wenn beispielsweise wie hier für Windows im Bild zu sehen, das Kontrollkästchen für das Standardgateway im Remotenetzwerk deaktiviert wird; danach wird nur der für das JuNet bestimmte Traffic im Tunnel übertragen.



macOS – Traffic Options (Send All traffic …)



Falls dieses Kontrollkästchen aktiviert wird, geht der gesamte Traffic durch den Tunnel *(entspricht fzj-nosplit)*

Da mehrere L2TP VPNs (Windows / Linux / macOS) eingerichtet werden können, kann die Split-Tunnel Variante auch zusätzlich eingerichtet werden, was eine einfache Auswahl des jeweils gewünschten Verbindungstyps ermöglicht.

Welche VPN-Pool-Adressen müssen im JuNet bei der Firewall-Konfiguration beachtet werden?

Bei der VPN-Einwahl (Verbindungsaufbau) werden IP-Adressen aus vordefinierten Bereichen (s.o.) vergeben. Die Bereiche sind

134.94.48.0/20 (IPv4) /
2001:638:404:3000::/52 (IPv6)

Je nach Sicherheitsanforderungen kann ein System im JuNet die Kommunikation durch entsprechende Einträge im Firewall Regelwerk blockieren oder erlauben.
Eine aktuelle Gesamtliste für alle VPN-Varianten (inkl. Cisco Secure Client/ AnyConnect) finden Sie unter https://junet-portal.fz-juelich.de/cgi-bin/public/junet_server.cgi

(weitere Dokumentation - Linux: TKI-0402 Linux Personal Firewall)

Wo gibt es Anleitungen für andere Betriebssysteme (Versionen)?

\\pcsrv.zam.kfa-juelich.de\public\VPN-Software\L2TPoverIPSEC

Diese MINI-HOWTOs sind in englischer Sprache.

DS-Lite und L2TP

Ungünstige Parameter-Aushandlungen (MTU, Fragmentierung, Keepalive-Options...) zwischen Client und Server für die lokale Internet-Anbindung oder generelle Probleme im IPSEC-Passthrough können in dieser Kombination Probleme verursachen. Bitte konfigurieren Sie testweise die Gatewayadresse (FQDN)

l2tpgatef.zam.kfa-juelich.de („f“ -> Fortinet-FW)

und prüfen dann, ob die Kommunikation im gewünschten Umgang funktioniert. Falls es dann weiterhin nicht geht, bleibt nur der Wechsel zur VPN-Variante mit Cisco Secure Client /Anyconnect VPN und IPv6 Transport (Weitere Information: TKI 410).

IPv6 Support?

Nein – IPv6 Support kann aus diversen techn. Gründen nicht angeboten werden. Anwender (z.B. DS-Lite UnityMedia Kunden), die IPv6-Unterstützung benötigen, müssen derzeit die in FZJ-JSC-TKI-0410 beschriebene VPN-Software Cisco Secure Client/AnyConnect VPN einsetzen. Ebenso kann der Zugriff auf bestimmte Angebote der ZB IPv6-Fähigkeit voraussetzen.

Zugriff über VPN auf die elektronischen Lizenzen und Services der Zentralbibliothek (fz-juelich.de)

(Stand: 19.02.2024 / Letzte Kontrolle: 19.02.2024)