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

JuNet-Helpdesk, ☎ (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0371
W.Anrath, S.Werner, E.Grünter
09.10.2018

Virtual Private Networks – Cisco IPSEC kompatible VPN Clients Microsoft Windows / Linux / Mac OS X

Inhaltsverzeichnis

1. Einführung
2. Cisco IPSEC VPN - Kompatible Client Software
3. Hinweis Microsoft Windows Betriebssysteme
4. Installation u. Konfiguration - Linux
5. Konfiguration - Mac OS X
6. FAQ

1. Einführung

Virtual **P**rivate **N**etworks, kurz **VPN**s, minimieren die Gefährdungspotentiale einer Datenübertragung durch unsichere öffentliche Netze. Diese Technologie nutzt kryptografische Verfahren zum Aufbau eines sicheren Zugangs zu einem Firmennetz.

Zur Realisierung eines VPNs werden die ursprünglichen IP-Pakete verschlüsselt und in einem neuen IP-Paket durch das INTERNET zu einem Security Gateway übertragen; diese Art der Übertragung ist eine spezielle Variante von sogenannten IP-Tunneln. Das Security Gateway ist im Forschungszentrum Jülich eine Cisco ASA Appliance. Benötigt wird dazu eine CISCO IPSEC VPN kompatible Client-Software. Viele LINUX-Distributionen, Android und MAC OS X ab 10.6.x enthalten bereits eine kompatible Software als Bestandteil des Betriebssystems.

Eine weitere VPN-Eigenschaft ist die Zuordnung einer offiziellen Klasse B-Internet-Adresse des Forschungszentrums in dem geschützten IP-Tunnel. Damit sind VPN-Benutzer beim Zugriff auf Intranet-Dienste internen JuNet-Benutzern gleichgestellt. Insbesondere bei Nutzung von

- DSL
- EDUROAM
- Anschluß von Laptops in Fremdfirmen / Tagungshotels

wird durch die VPN-Software eine hohe Sicherheit beim Zugriff auf JuNet-Dienste erreicht.

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

http://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/JSCOnline/jsconline_node.html

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. Cisco IPSEC VPN – Kompatible Client Software

Für Linux (x86) und MacOS X werden keine Distributionen zum Download angeboten, da bereits eine kompatible Implementierung Bestandteil dieser Betriebssysteme ist.

Die von Cisco bereitgestellte Windows Software wird nicht mehr unterstützt; die noch im Umlauf befindlichen Distributionen sind nicht mit neueren Windows 8 / 10 Betriebssystemen kompatibel.

3. Hinweis - Microsoft Windows Betriebssysteme

Windows 7 / 8 / 10 Benutzer können die in TKI-0387 beschriebene VPN-Lösung verwenden oder in Kombination mit DFN-Zertifikaten bevorzugt die Cisco AnyConnect-Software (TKI-410) einsetzen.

4. Installation u. Konfiguration - Linux

An dieser Stelle wird die Konfiguration der CISCO VPN kompatiblen LINUX Software VPNC erläutert. Diese Lösung ist in der grafischen Benutzeroberfläche GNOME integriert. Paketinstallation: network-manager-vpnc / network-manager-vpnc-gnome

(Alternativ kann auf Kommandozeilenebene direkt mit dem Programm *vpnc* gearbeitet werden; Frage 5 im FAQ erläutert dazu die Details.)

Zum Erstellen der Konfiguration öffnet der Benutzer/Admin die Netzwerkeinstellungen.
Als Connection Type wird

Cisco Compatible VPN (vpnc)

ausgewählt und angelegt. Der Connection Name kann beliebig festgelegt werden. Gateway ist

wingate.zam.kfa-juelich.de

wobei später eine zweite Verbindung für den Backup-Fall mit wingateb.zam.kfa-juelich.de optional eingerichtet werden kann.

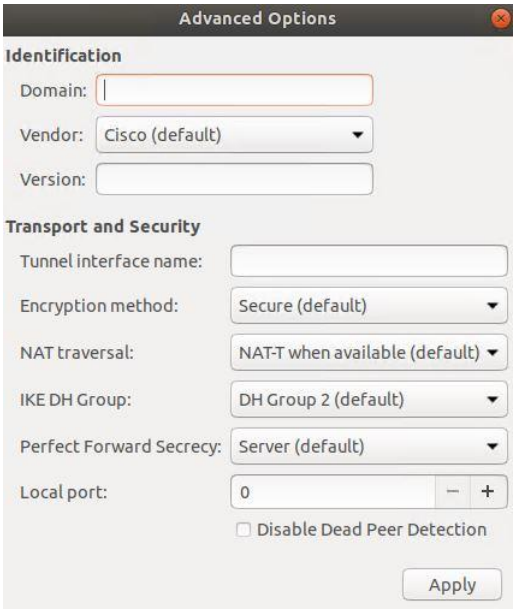
Als Group Name wird

fzj oder fzj-nosplit

eingetragen. Der Eintrag fzj bewirkt, dass sämtlicher Datenverkehr zu Zielen im JuNet (134.94.0.0/16) im VPN-Tunnel übertragen wird. Der alternative Eintrag fzj-nosplit an dieser

Stelle bewirkt, dass der gesamte Internet-Datenverkehr im VPN-Tunnel übertragen wird (z.B. nötig für ZB Zeitschriften).

Den Wert für das Feld Group Password erhalten Sie bei der Bestätigung der Anmeldung durch das JSC-Dispatch.

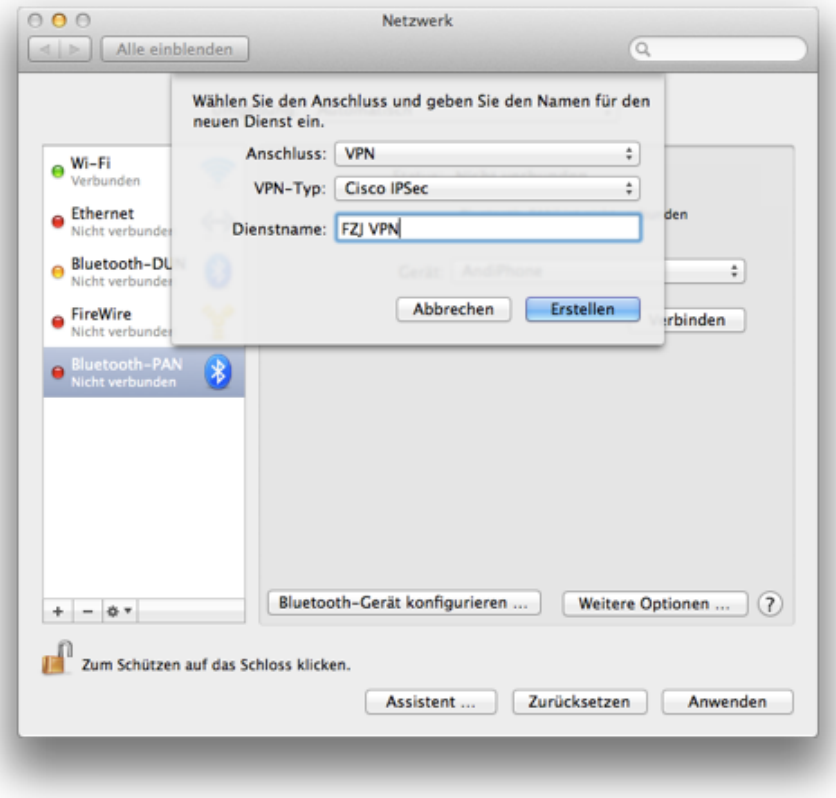


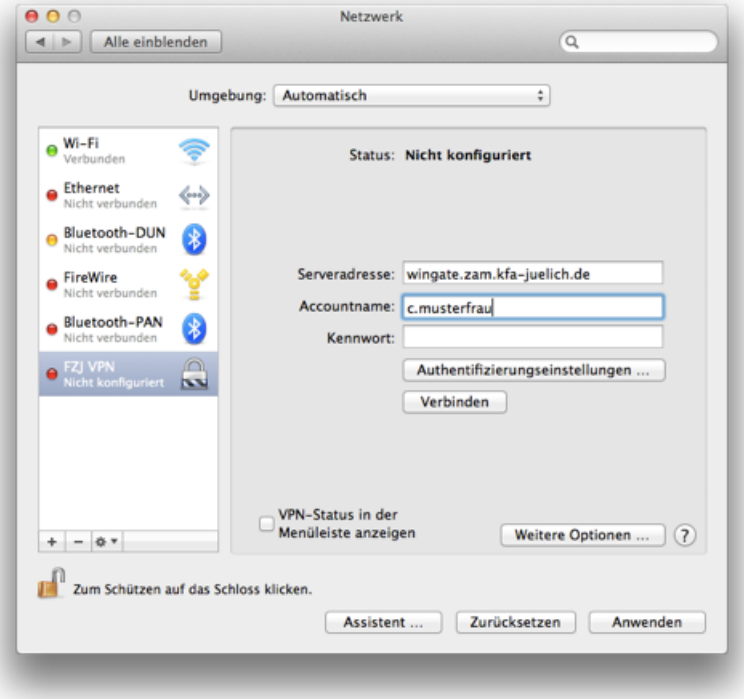
Optional: Wie bereits erwähnt, kann zur Absicherung gegen Ausfälle eine zweite Ersatzverbindung eingerichtet werden. Die VPN-Appliance wingateb.zam.kfa-juelich.de ist als Gateway einzutragen.

5. Konfiguration - Mac OS X

Hinweis: MacOS X können alternativ die in TKI-0387 beschriebene VPN-Lösung konfigurieren.
Soll die Auswahlmöglichkeit zwischen den VPN-Policies fzj und fzj-nopslit bestehen, kann wie folgt die Cisco kompatible Konfiguration vorgenommen werden.

Zur Konfiguration werden Administratorrechte benötigt.
MENÜ öffnen Systemeinstellungen / Netzwerk / +
(ggf. vorher das Schloß öffnen)

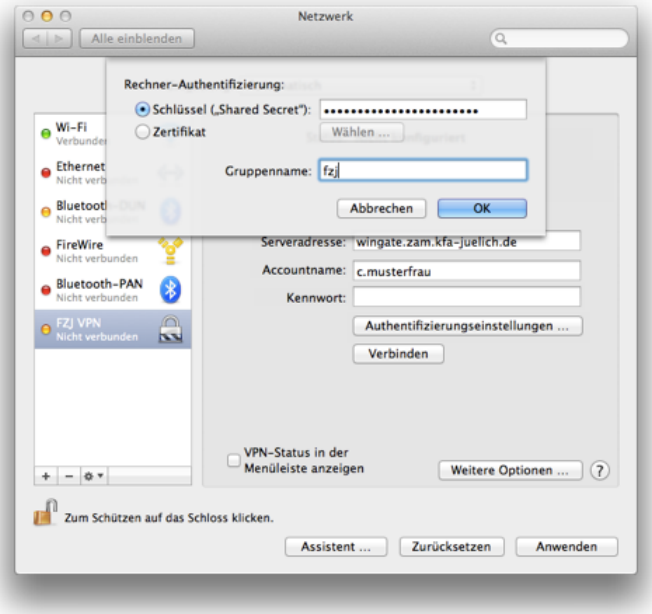




Kennwort bitte frei lassen und bei jedem Verbindungsaufbau eingeben.

MENÜ öffnen Authentifizierungseinstellungen ...

Schlüssel („Shared Secret“): *Gruppen-Password aus der Anmeldebestätigung*
Gruppenname: fzj



Alternativ kann, falls der gesamte Internet-Verkehr über den VPN-Tunnel geführt werden soll,

der Gruppenname fzj-nosplit eingetragen werden. Im anderen Fall (Gruppenname fzj) wird der für das JuNet bestimmte Datenverkehr im Tunnel übertragen.
Über ‘Anwenden’ werden die Eingaben aktiviert. Über ‘Verbinden’ wird der Aufbau des VPN-Tunnels gestartet.

Im Anwendungsfenster sind während der Verbindungsdauer Anzeigen zur Verbindungsdauer und der erhaltenen IP-Adresse.

Fehlerfälle:

- Falscher Schlüssel (Shared Secret / PreSharedKey):
  Fehlermeldung: „Der VPN-Schlüssel (Shared Secret) ist nicht korrekt.“
- Falsches Passwort:
  Erneuter Prompt auf Passwort ohne Fehlermeldung.
  Nach dem dritten falschen Passwort Fehlermeldung: „Benutzer-Authentifizierung fehlgeschlagen

6. FAQ:

1. **Der Zugriff auf elektronische Zeitschriften der ZB funktioniert nicht / ist nicht erlaubt**.

   Wegen der Split-Tunnel-Einstellung wird nur der IP-Traffic zu Rechnern im JuNet (134.94.0.0/16) in den VPN-Tunnel geleitet. Die Kommunikation zum Internet erfolgt direkt über den jeweiligen Service-Provider (z.B. T-Online) mit deren IP-Adressen. Durch Änderung der VPN-Gruppe auf fzj-nosplit wird der gesamte IP-Traffic in den VPN-Tunnel geleitet und der Zugriff auf die Zeitschriften erfolgt mit einer gültigen JuNet-IP-Adresse.

2. **Welche Tunnelendpunkte können im Wireless LAN (FZJ) genutzt werden?**
   Grundsätzlich sind die Tunnelendpunkte wingate.zam.kfa-juelich.de bzw. im Backup-Fall wingateb.zam.kfa-juelich.de zu verwenden.

3. **Microsoft Windows - Gibt es eine Alternative/Nachfolger zum Cisco VPN Client?**
   Derzeit unterstützt das JSC als weitere VPN-Variante L2TP over IPSEC. Die Konfiguration ist in TKI-0387 beschrieben. Windows 7 / 8 / 10 und MacOS X Benutzer sollten diese Lösung bevorzugt einsetzen. Ebenso ist der Cisco AnyConnect Client verfügbar – siehe dazu TKI-0410; dieser ersetzt den bisherigen Client.

4. **Der Verbindungsaufbau von einer externen Firma oder Universität aus funktioniert nicht – die Fehlermeldung ist:**

   Secure VPN Connection terminated locally by the Client.
   Reason 412: The remote peer is no longer responding.

Um die Verbindung aufbauen zu können, muss IKE UDP Port 500, ESP, UDP Port 4500 und UDP Port 10000 in der Firewall-Konfiguration der jeweiligen Firma freigeschaltet sein.
Versuchsweise kann noch IPSEC over TCP (Transport Registerkarte) ausprobiert werden - es gibt dann nur eine TCP-Verbindung Richtung FZJ mit Zielport 10000 - da es sich um eine ausgehende TCP-Verbindung handelt, ist es nicht unwahrscheinlich, damit Erfolg zu haben (vgl. Bild FAQ Frage 3).

5. Wie können LINUX-Benutzer die zu CISCO kompatible VPNC Implementierung auf der Kommandozeilenebene nutzen?

Die Konfigurationsdatei /etc/vpnc.conf muss folgende Einträge haben:

IPSec gateway wingate.zam.kfa-juelich.de
IPSec ID fzj
IKE Authmode psk
IPSec secret *Pre-shared-Key*
NAT Traversal Mode cisco-udp

Datei-Zugriffsrechte: chmod 755 /etc/vpnc.conf && chown root /etc/vpnc.conf

Verbindungsaufbau und Verbindungsbau setzen Superuser-Rechte voraus und werden wie folgt genutzt (Aufruf für Benutzer mittels SUDO möglich):

Verbindungsaufbau:

/usr/sbin/vpnc

Verbindungsabbau:

/usr/sbin/vpnc-disconnect

6. Welche VPN-Pool-Adressen müssen Systeme im JuNet bei der Firewall-Konfiguration beachten?

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

134.94.7.0/24
134.94.79.0/24
134.94.112.0/24

Je nach Sicherheitsanforderungen kann ein System im JuNet die Kommunikation durch entsprechende Einträge im Firewall-Regelwerk blockieren oder zulassen. (Linux: TKI-0402 Linux Personal Firewall)