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,E.Grünter

16.01.2018

L2TP over IPSEC

Built-in VPN für Microsoft Windows und MacOS X

1. Einleitung 1
2. Unterstützte Plattformen 2
3. Konfiguration - Windows 8 / 8.1 / 10 2
4. Konfiguration - Windows 7 Professional 4
5. Konfiguration - Mac OS X Leopard - Yosemite 5
6. Ausblick 8
7. FAQ 9

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 / 8 / 7 und Mac OS X 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. Der Einsatz von L2TP over IPSEC ist die favorisierte Lösung. Alternativ können CISCO IPSEC VPN kompatible Clients (FZJ-JSC-TKI-0371) oder die Cisco Anyconnect Variante (FZJ-JSC-TKI-0410) zum Einsatz kommen. Ein wesentlicher Vorteil dabei ist, dass die L2TP-Lösung bereits Bestandteil diverser Betriebssysteme ist.

Zulassungen/Accounts (Mitarbeiter) zur VPN-Benutzung können beim Dispatch im JSC 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. 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. Das Betriebssystem Mac OS X bietet ebenfalls eine L2TP over IPSEC Implementierung.

3. Konfiguration - Windows 8 / 8.1 / 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-1

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

Systemsteuerung - Alle Systemsteuerungselemente - Netzwerk- und Freigabecenter

wird die die Option

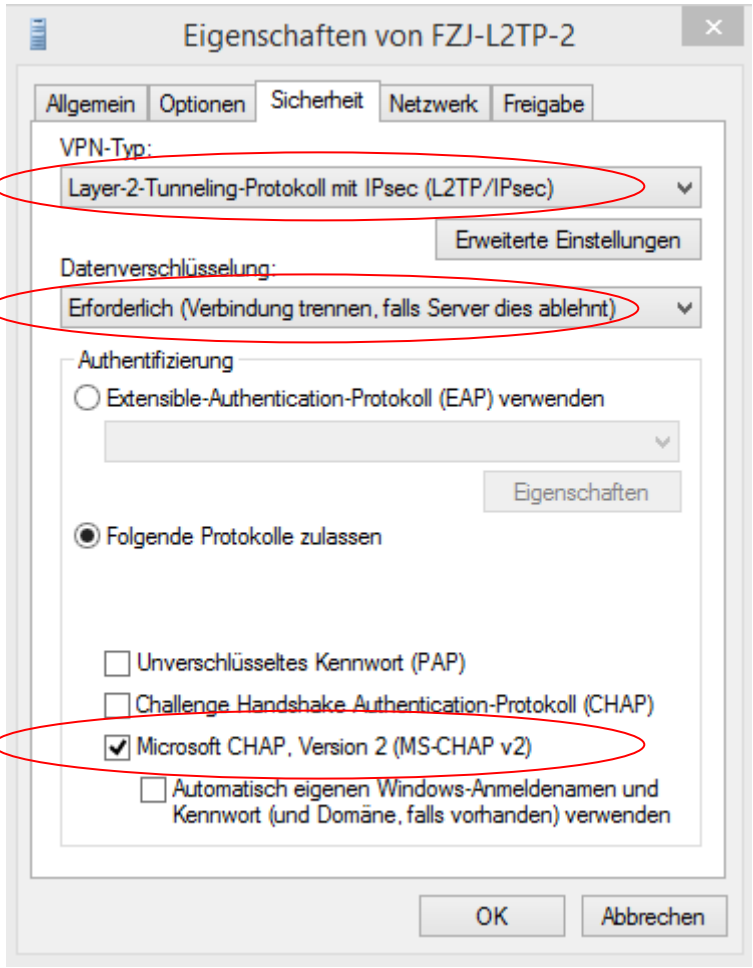
Adaptereinstellungen ändern

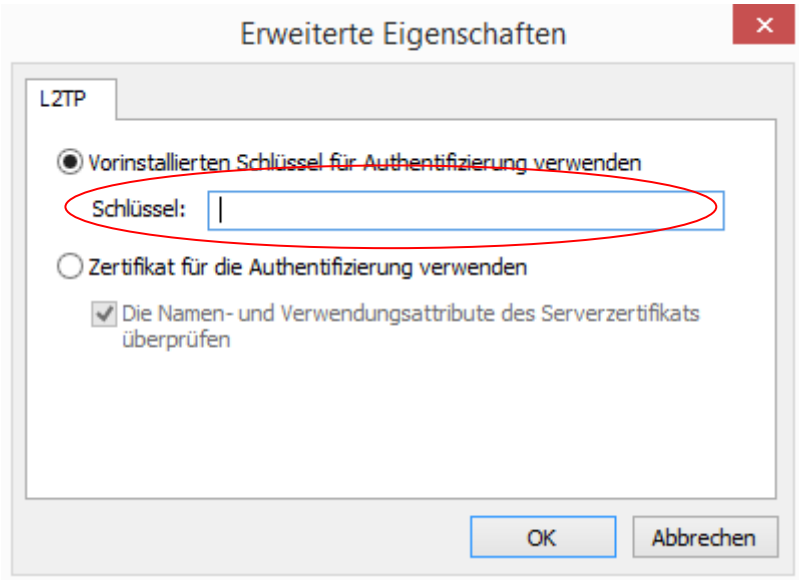
geöffnet.

Die 'Eigenschaften' der neuen Verbindung 'FZJ-L2TP-1' werden geöffnet und in der Registerkarte

Sicherheit

können die nötigen Anpassungen vorgenommen werden





Der sogenannte PresharedKey aus der JSC-Dispatch-Anmeldebestätigung (vorinstallierter Schlüssel/Shared Secret) ist einzutragen.

Die VPN-Verbindung ist fertiggestellt und funktionsfähig.

Hinweis: Als Backup kann diese Verbindung kopiert werden und als VPN-Server l2tpgateb.zam.kfa-juelich.de eingetragen werden.

4. Konfiguration - Windows 7 Professional

Hier die nötigen Konfigurationsschritte zum Einrichten einer VPN-Verbindung:

Systemsteuerung - Netzwerk und Internet - Netzwerk und Freigabecenter öffnen.

Unter *Netzwerkeinstellungen ändern*, die Möglichkeit

Neue Verbindung oder neues Netzwerk einrichten aufrufen.

Danach wird die Verbindungsoption

Verbindung mit dem Arbeitsplatz herstellen gewählt.

Es soll eine neue Verbindung erstellt werden und in der nächsten Auswahl wird

Die Internetverbindung (VPN) verwenden festlegt.

VPN-Gateway IP-Adresse eingeben

Internet-Adresse: ***l2tpgate.zam.kfa-juelich.de***

Zielname – z.B.: ***FZJ-VPN***

und das Kontrollkästchen

‚**Jetzt nicht verbinden, nur für spätere Verwendung einrichten**‘ markieren

Optional kann im folgenden Dialog noch der Benutzername eingetragen werden.

Vor der ersten Nutzung der Verbindung müssen im **Netzwerk und Freigabecenter** die Eigenschaften der neuen VPN-Verbindung bearbeitet werden. Dazu die Auswahl **Verbindung mit einem Netzwerk herstellen** aufrufen und in der nachfolgenden Liste die Eigenschaften (rechte Maustaste) bearbeiten:

Registerkarte Sicherheit öffnen und explizit in der Auswahlliste den **VPN-Typ**

Layer-2-Tunneling-Protokoll mit IPSEC (L2TP/IPSEC) wählen.

Button **Erweiterte-Einstellungen** öffnen und das Eingabefeld (vgl. Bilder zu Win8/10)

Vorinstallierter Schlüssel ausfüllen.

Jetzt kann die neue VPN-Verbindung verwendet werden.

Hinweis: Als Backup kann diese Verbindung kopiert werden und als VPN-Server l2tpgateb.zam.kfa-juelich.de eingetragen werden.

5. Konfiguration - Mac OS X Leopard - Yosemite

L2TP over IPSEC kann auf Mac OS X ohne zusätzlichen Installationsaufwand konfiguriert werden und bevorzugt zum Einsatz kommen. Die folgenden Bilder zeigen die nötigen Konfigurationseinstellungen, die folgende Schritte umfasst:

Systemeinstellung/Netzwerk

Schloss öffnen

\+ klicken zum Hinzufügen einer Verbindung

VPN & L2TP auswählen

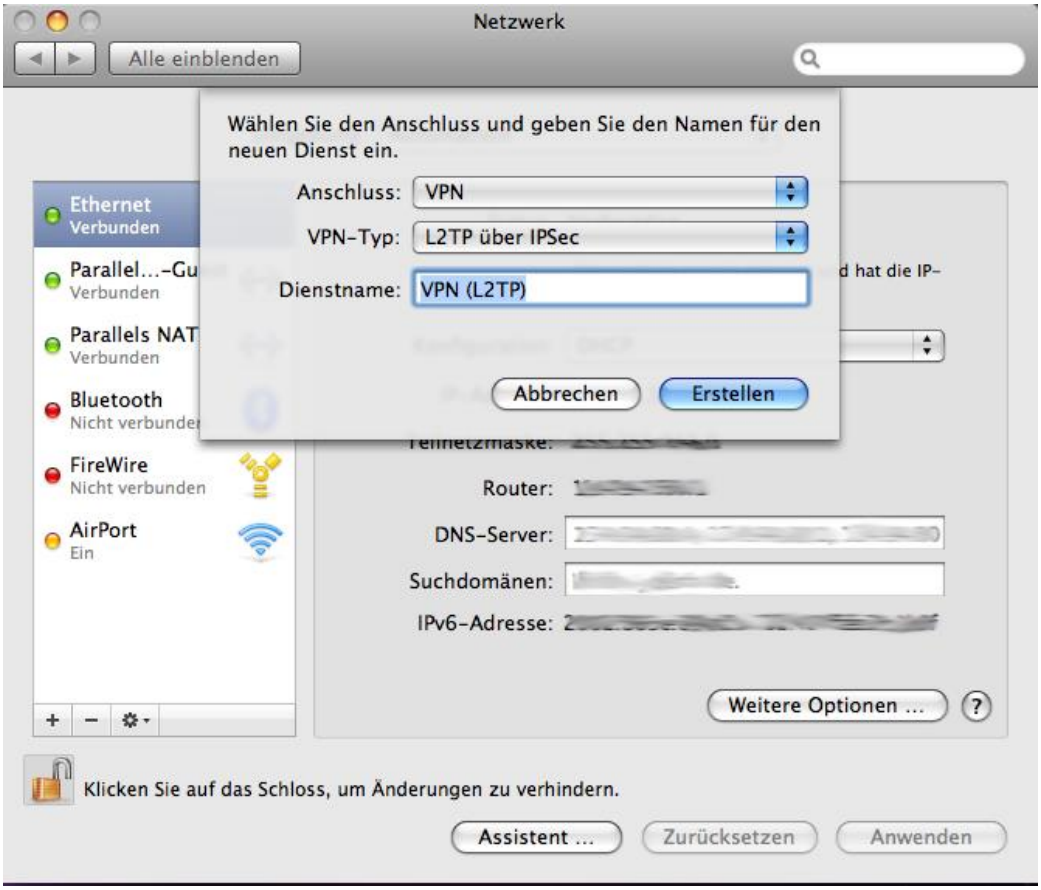
VPN Gateway (vollqualifizierter Name) und Benutzername eingeben

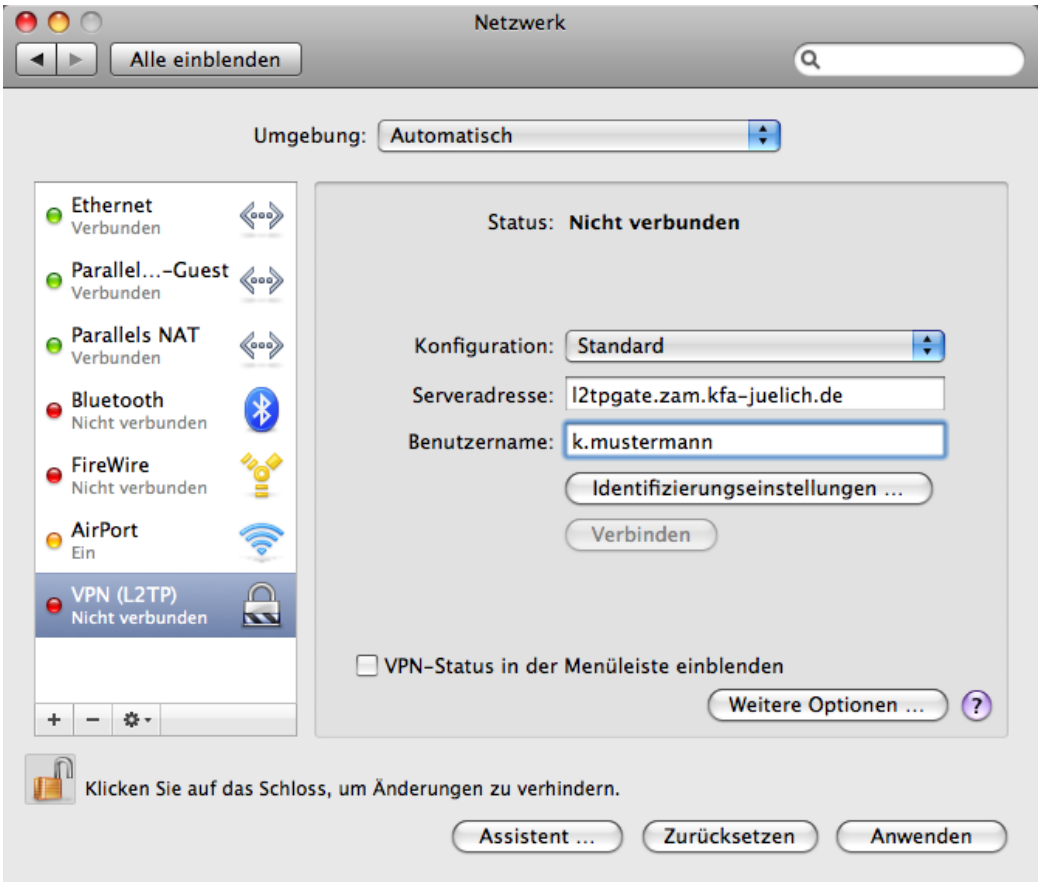
Identifizierungseinstellungen eingeben (Shared Secret=vorinstallierter Schlüssel)

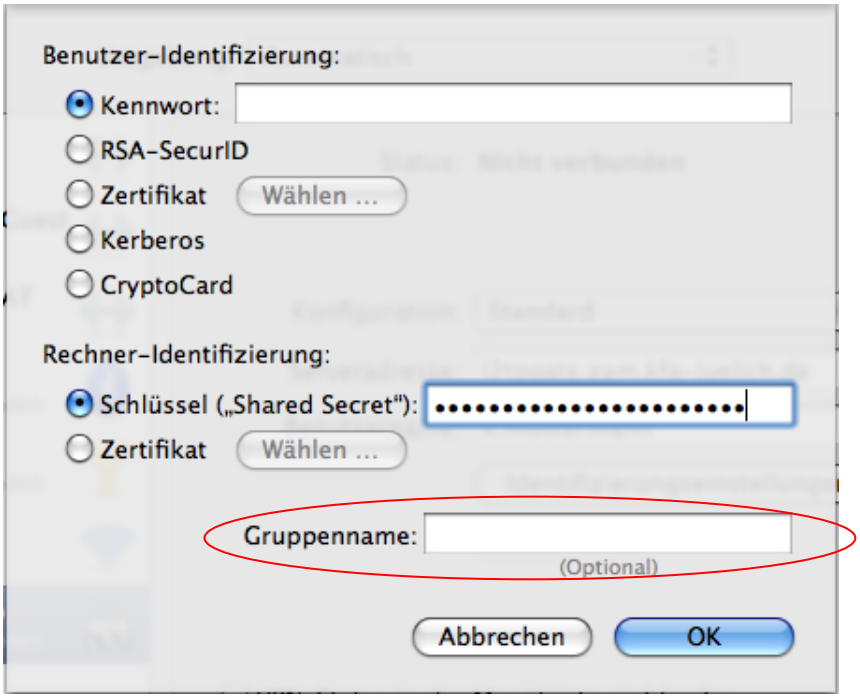
"Anwenden" klicken

"Verbinden" klicken

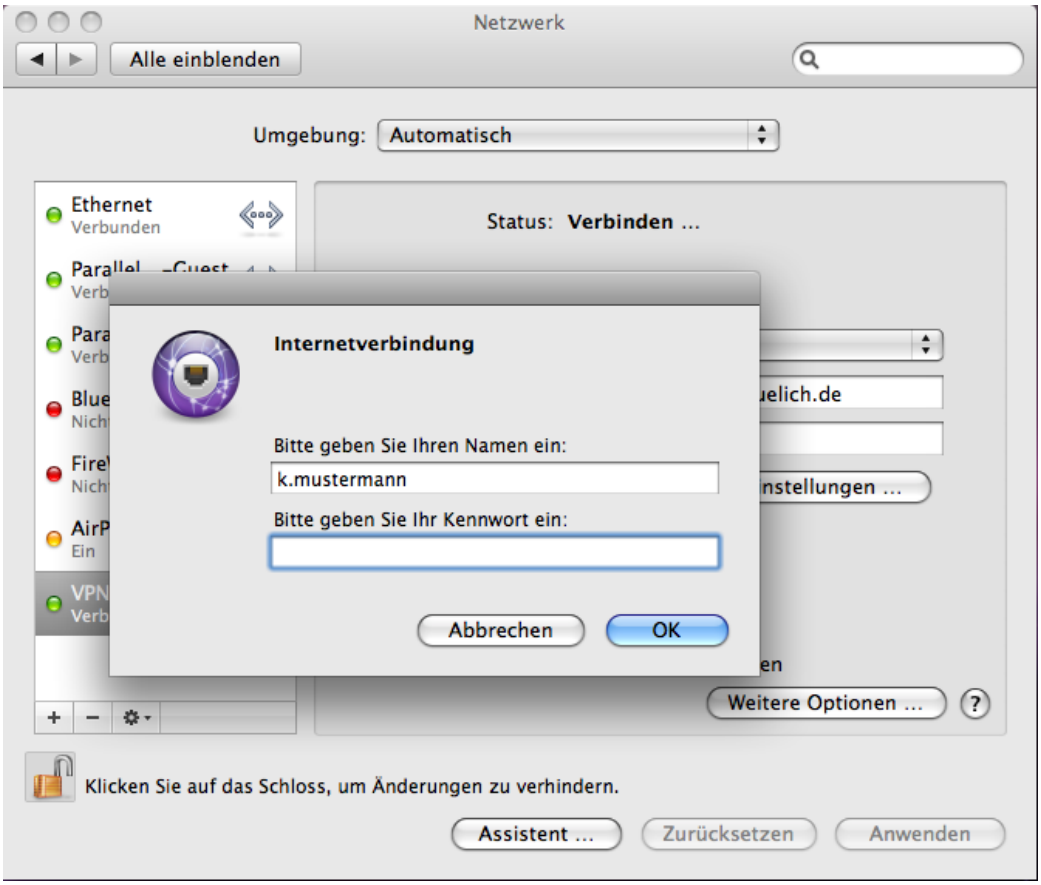
VPN-User Passwort beim Verbindungsaufbau eingeben


Netzwerk
Alle einblenden
Wählen Sie den Anschluss und geben Sie den Namen für den neuen Dienst ein.
Anschluss: VPN
VPN-Typ: L2TP über IPSec
Dienstname: VPN (L2TP)
Abbrechen
Erstellen
Ethernet
Verbunden
Parallel...-Gu
Verbunden
Parallels NAT
Verbunden
Bluetooth
Nicht verbunden
FireWire
Nicht verbunden
AirPort
Ein
Router:
DNS-Server:
Suchdomänen:
IPv6-Adresse:
Weitere Optionen ...
Klicken Sie auf das Schloss, um Änderungen zu verhindern.
Assistent ...
Zurücksetzen
Anwenden


Netzwerk
Alle einblenden
Umgebung: Automatisch
Ethernet
Verbunden
Parallel...-Guest
Verbunden
Parallels NAT
Verbunden
Bluetooth
Nicht verbunden
FireWire
Nicht verbunden
AirPort
Ein
VPN (L2TP)
Nicht verbunden
Status: Nicht verbunden
Konfiguration: Standard
Serveradresse: l2tpgate.zam.kfa-juelich.de
Benutzername: k.mustermann
Identifizierungseinstellungen ...
Verbinden
VPN-Status in der Menüleiste einblenden
Weitere Optionen ...
Klicken Sie auf das Schloss, um Änderungen zu verhindern.
Assistent ...
Zurücksetzen
Anwenden



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 in den VPN-Tunnel geroutet (entspricht Gruppen-Policy „fzj“ bei Cisco VPN-Lösungen), Ändern über „Optionen“-Button

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)).

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 Die 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 Die 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 PresSharedKeys (Schlüssel) können die VN-Gateways

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

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

Die IPv6-Unterstützung befindet sich derzeit im Aufbau.

7. FAQ

Kann L2TP over IPSEC in Verbindung mit NAT/PAT-Routern eingesetzt werden?

Ja. Die VPN-Gateways unterstützen den NAT-Transparency Standard (kurz NAT-T).

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

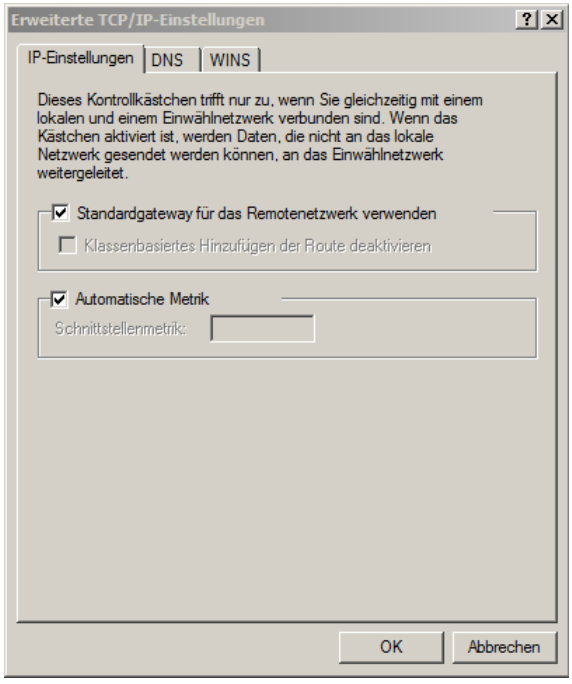
Es muss keine zusätzliche Software installiert werden.

Welche der von den angebotenen Varianten – CISCO VPN Client oder L2TP over IPSEC – ist die sicherste?

Beide Implementierung stellen die in der Einleitung geforderten VPN-Features durch die gleichen kryptografischen Verfahren sicher. Der Konfigurationsaufwand ist in beiden Fällen gleich. Von Vorteil: L2TP over IPSEC ist in Windows schon integriert – Zusatzsoftware ist nicht erforderlich.

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

Ja. Wenn die beispielsweise wie hier für Windows 7 im Bild zu sehen in den Einstellungen, das Kontrollkästchen für das Standardgateway im Remotenetzwerk entfernt wird; danach wird nur der für das JuNet bestimmte Traffic im Tunnel übertragen.



Kann L2TP over IPSEC im Wireless LAN (W-JuNet) genutzt werden?

Ja.

Welche IP-Adresse erhält ein VPN-Client?

Für den L2TP-Tunnel werden dynamisch IP-Adressen verwendet – Bereich:

134.94.79.0/24

134.94.7.0/24

134.94.112.0/24

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

Bei der VPN-Einwahl (Verbindungsaufbau) werden IP-Adressen aus vordefinierten Bereichen (s.o.) 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 erlauben.

(Linux: TKI-0402 Linux Personal Firewall)

(Stand: 16.01.2018 / Letzte Kontrolle: 16.01.2018)