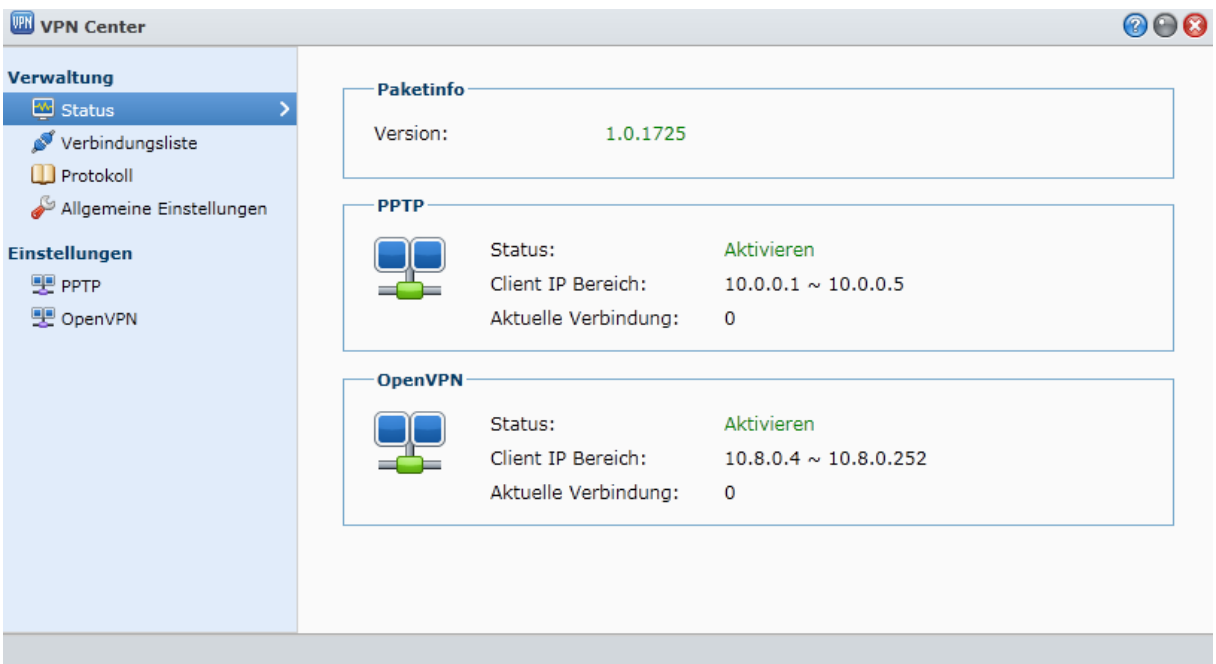
13.5.2011

COMMUNITY-ÜBERSETZUNG
SYNOLOGY-FORUM.DE

SYNOLOGY VPN CENTER - BENUTZERANLEITUNG

Ergänzte, leicht veränderte Übersetzung der offiziellen englischen Benutzeranleitung von Synology Inc.



Zu VPN Center Version 1.0.1725 | Matthieu von synology-forum.de

INHALT

I. AUS DER COMMUNITY

Bevor die Übersetzung der Benutzeranleitung von Synology beginnt, ein wenig Hintergrundwissen. Wer mit VPN einfach starten möchte ohne sich Gedanken über die Hintergründe zu machen, der sollte dieses Kapitel überspringen.

Portfreigaben sind immer eine Möglichkeit um an der so oft als lästig empfundenen Firewall des Routers vorbei zu kommen. Ein Port hier, einer dort. Ohne es jedoch zu bemerken öffnen viele Internetnutzer ihr lokales Netzwerk bereitwillig für nicht so friedliche Zeitgenossen. Dass das auch unangenehme Folgen haben kann, führen Datenpannen bei Firmen oft genug vor. Grund für diese Freizügigkeit ist der Wille, von überall auf die eigenen Daten zugreifen zu können. In Zeiten von Cloud und Breitbandinternet selbst per Funk ist dies kein technisches Problem. Doch in ihrem Eifer werden schnell Ports etwa für SMB geöffnet, die jedoch nie für Internetnutzung ausgelegt waren.

Der saubere und vor allem sichere Weg für alle Beteiligten ist daher ein anderer. Sogenannte virtuelle, private Netze binden einen Laptop oder ein ganzes Netzwerk in ein anderes ein. Anwendungen dafür gibt es viele, etwa Niederlassungen mit VPN-Verbindungen in die Firmenzentrale oder Außendienstmitarbeiter mit Vollzugriff unabhängig von ihrem geografischen Standort - da mittlerweile selbst Smartphones Anwendungen für VPN-Verbindungen bereitstellen, ist auch dies kein Hindernis. Mit einem VPN ist jedoch nur noch eine Portfreigabe nötig, denn der Netzwerkverkehr wird vom VPN-Server in das Netzwerk verteilt als würde sich der Laptop oder das Smartphone direkt dort befinden. Ist die VPN-Verbindung daher erst einmal hergestellt, reduziert sich der Aufwand für die Absicherung der Firmendaten auf die Server Firmenzentrale. Die Speicherung der Daten in den Niederlassungen wird überflüssig.

In der Gegenwart konnten sich zwei VPN-Technologien gegen Standleitung und Einwahl durchsetzen: OpenVPN und PPTP. Letzteres wurde von mehreren Herstellern gemeinsam entwickelt und ist daher in mehreren Betriebssystemen ab Werk enthalten. Dies macht es zu einer sehr benutzerfreundlichen und einfachen Lösung. Bei OpenVPN handelt es sich hingegen um OpenSource, was häufig ein Garant für mehr Sicherheit und bessere Verschlüsselung ist.

PPTP VS. OPENVPN

Hier eine Übersicht über die wichtigsten Unterschiede für Benutzer der beiden Technologien.

Einrichtung im VPN Center – Durch die etwas geringere Anzahl von Einstellungen ist OpenVPN für Einsteiger etwas leichter in Betrieb zu nehmen. PPTP erfordert zwei weitere Einstellungen welche bei falscher Wahl für Probleme sorgen können. Doch insgesamt sind beide sehr einfach einzurichten, verglichen mit einer manuellen Installation der Software auf der DiskStation.

Installation und Einrichtung – PPTP ist in Windows Mac und auf den meisten Linux-Distributionen bereits vorinstalliert und kann über einfache und übersichtliche Dialoge eingerichtet werden. In wenigen Minuten ist somit eine Verbindung aufgebaut. Nur die beiden bereits angesprochenen Einstellungen erfordern etwas zusätzliche Aufmerksamkeit. OpenVPN hingegen muss meist zunächst installiert werden. Die Software ist OpenSource und somit vollkommen kostenfrei verfügbar. Nach der Installation muss eine der Zertifikate kurz angepasst und anschließend kopiert werden. Dann ist auch OpenVPN bereit für eine Verbindung.

Sicherheit – Hier ist OpenVPN ungeschlagen. Durch seine offene Struktur kann jeder den Programmcode auf Schwachstellen oder gar Hintertüren überprüfen. Bei PPTP hilft nur Vertrauen. Die auf Zertifikaten basierende Verschlüsselung von OpenVPN ist außerdem deutlich sicherer als die verschiedenen PPTP-Algorithmen. Besonders bei kurzen, unsicheren Passwörtern zeigt PPTP deutliche Schwächen, doch durch die Voreinstellungen von Synology verwendet auch OpenVPN das Passwort zur Verschlüsselung, was bei kurzen Passwörtern auch hier ein Sicherheitsproblem darstellen kann.

Smartphones – PPTP wird von den meisten Geräten mit aktuellen Betriebssystemen unterstützt. OpenVPN hingegen deutlich seltener (aus verschiedenen Gründen), für einige wie Android sind jedoch entsprechende Apps verfügbar[1].

Geschwindigkeit – Nur OpenVPN bietet zusätzlich eine Komprimierung an um Daten schneller zu übertragen.

LINKSAMMLUNG

Mehr Informationen zu den Themen dieser Anleitung gibt es auch im Internet:

- http://wiki.freifunk.net/OpenVPN_Howto
- http://openvpn.net/
- http://de.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol
- http://de.wikipedia.org/wiki/Openvpn
- http://wiki.ubuntuusers.de/Network-Manager/VPN_Plugins
- http://compnetworking.about.com/gi/o.htm?zi=1/XJ&zTi=1&sdn=compnetworking&cdn=compute&tm=4838&f=11&tt=14&bt=1&bts=1&zu=http%3A//tldp.org/HOWTO/VPN-HOWTO/
- http://www.apfelmagazin.de/unter-mac-osx-eine-vpn-verbindung-einrichten/
- http://www.elektronik-kompendium.de/sites/net/0906141.htm

DANKSAGUNG

Vielen Dank an:

- „amarthius“ aus der deutschen Community für die Bereitstellung der Mac-Screenshots
- die Community für ihre Mithilfe und konstruktive Kritik
- Synology für die Erlaubnis und aktive Mithilfe zur Übersetzung

[1] Nicht jedoch für iOS-Geräte.

II. OFFIZIELLES HANDBUCH - ÜBERSETZUNG

EINLEITUNG

Um eine sichere Fernverbindung aufzubauen nutzten Unternehmen wie Privatpersonen lange Zeit Standleitungen, Einwahlverbindungen und andere Technologien. Aber mit den wachsenden Anforderungen und Bedürfnissen an Netzwerke stiegen die Kosten für solche Systeme mit Wartung und Support exponentiell.

WAS IST VPN

Ein VPN, oder Virtual Private Network, ist eine Lösung um verschlüsselten Zugriff auf das Private Netzwerk durch das Internet hindurch zu erreichen. Mit Verschlüsselung und anderen Mechanismen erlaubt VPN es Mitarbeitern von Unternehmen auf Ressourcen des lokalen Netzwerks wie gewohnt zuzugreifen.

Privatpersonen können ebenso Zugang zu ihrem Heimnetzwerk erhalten, obwohl sie sich weit entfernt davon befinden. Dennoch ist VPN für die meisten Nutzer nur schwer einzurichten. Die Kosten eines VPN-Server können zusätzlich abschrecken.

SYNOLOGY VPN CENTER

Mit dem Synology VPN Center wird diese Technologie einfacher als je zuvor. Das VPN Center ist ein Zusatzpaket das eine DiskStation mit den Fähigkeiten eines VPN-Servers ausstattet. DSM-Benutzer sind somit in der Lage, lokale Ressourcen im Netzwerk ihrer DiskStation zu verwenden. Die benutzerfreundliche Oberfläche und einfache Einrichtung machen VPN einfach und durchschaubar. Die am meisten verbreiteten Protokolle für VPN – PPTP und OpenVPN – sind im Synology VPN Center enthalten und machen es somit zum idealen Tool um VPN Verbindungen zu erstellen und zu verwalten.

Diese Anleitung beschreibt den Aufbau eines eigenen VPN mit dem Synology VPN Center und zeigt, wie Geräte verschiedener Plattformen darauf zugreifen können.

VOR DEM BEGINN

Bevor das Synology VPN Center Paket auf der DiskStation installiert wird, stellen Sie bitte folgendes sicher:

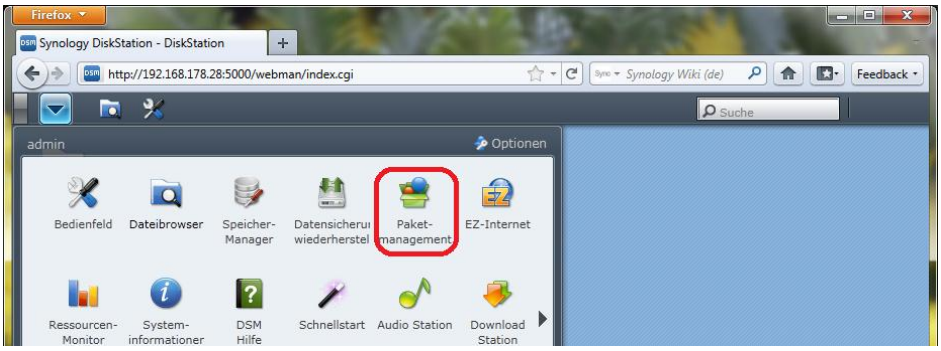
- Die Internetverbindung arbeitet wie normal.
- Das Volumen auf der DiskStation arbeitet wie normal.
- Der DiskStation Manager (DSM) der DiskStation ist aktuell. Nur DSM-Versionen höher als 3.1-1725 unterstützen VPN Center
- Um VPN Center einzurichten ist ein Zugang mit dem Benutzerkonto „admin“ oder einem anderen Nutzer der Gruppe „administrators“ zum DSM notwendig.

INSTALLIEREN UND AUSFÜHREN VON VPN CENTER

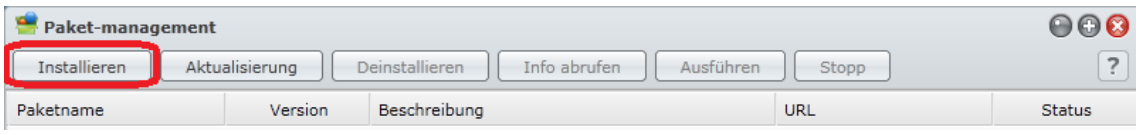
Mit den folgenden Schritten können Sie VPN Center in Betrieb nehmen:

(1) Nach dem Download des Pakets (bitte auf korrekte Version achten, es gibt verschiedene Pakete für verschiedene DiskStation-Modelle), melden Sie sich im DSM mit den Zugangsdaten von „admin“ oder einem anderen Benutzer der Gruppe „administrators“ an.

(2) Gehen Sie im Hauptmenü auf „Paket-Management“



(3) Klicken Sie auf „Installieren“ und wählen Sie die heruntergeladene Datei um sie zu installieren. Sie trägt die Dateiendung „.spk“. Folgen Sie anschließend den einzelnen Schritten.



(4) Nach der Installation wählen Sie das VPN Center aus und klicken auf „Ausführen“ um das Paket zu starten. Nachdem Sie die Aktion bestätigt haben, wechselt der Status in der Zeile von VPN Center zu „Läuft“.

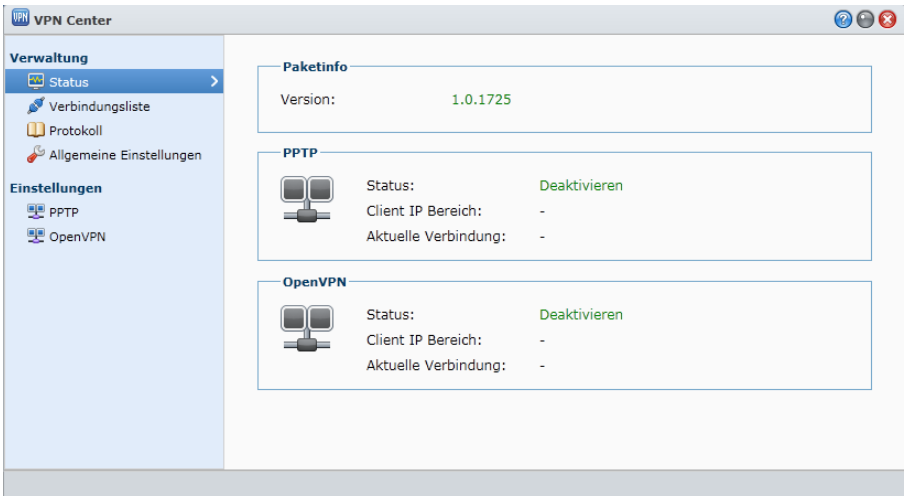
VPN Center	1.0.1725	Synology VPN center	Läuft

VPN CENTER VERWENDEN

Diese Anleitung erläutert die Bedienoberfläche von VPN Center:

(1) Gehen Sie im Hauptmenü auf „VPN Center“ um die Anwendung zu starten.

(2) Die Seite „Status“ wird wie hier zu sehen ist geöffnet. Unter „Verwaltung“ auf der linken Seite werden 4 weitere Punkte um den VPN Dienst der DiskStation zu administrieren. Diese sind „Status“, „Verbindungsliste“, „Protokoll“ und „Allgemeine Einstellungen“. Es wird nun beschrieben was jede dieser Seiten beinhaltet



- Status
  - Paketinfo zeigt die verwendete Version von VPN Center. Sollten Sie Probleme haben, geben Sie bitte bei Support oder Forum stets diese Versionsnummer an.
  - Die Felder für PPTP und OpenVPN zeigen jeweils den aktuellen Status, die verwendeten IP-Adressen für Clients (wie in den dortigen Einstellungen angegeben) und die Aktuelle Verbindung (die Netzwerkschnittstelle, ebenfalls wie in den entsprechenden Einstellungen definiert).
- Verbindungsliste
  - Hier werden alle aktuellen Verbindungen aufgeführt. Eine bestehende Verbindung kann über den Schalter „Trennen“ unterbrochen werden. Über „Aktualisieren“ wird die Liste auf Veränderungen überprüft.
- Protokoll
  - Diese Übersicht zeigt alle Aktivitäten von VPN Center mit allen eingegangenen Verbindungen. Sie kann gelöscht, exportiert oder aktualisiert werden.
- Allgemeine Einstellungen
  - Gegenwärtig lässt sich hier nur die zu verwendende Netzwerkschnittstelle konfigurieren. Dies ist nur relevant für größere Geräte mit zwei oder mehr Anschlüssen.

DIE VPN-SERVER AKTIVIEREN

VPN Center bietet 2 Arten von Servern: PPTP und OpenVPN. Es handelt sich dabei um die beiden am häufigsten verwendeten Technologien für VPN. Windows unterstützt ohne zusätzliche Software PPTP, Anwender von anderen Plattformen sollten in der Regel zu OpenVPN greifen.

PPTP SERVER

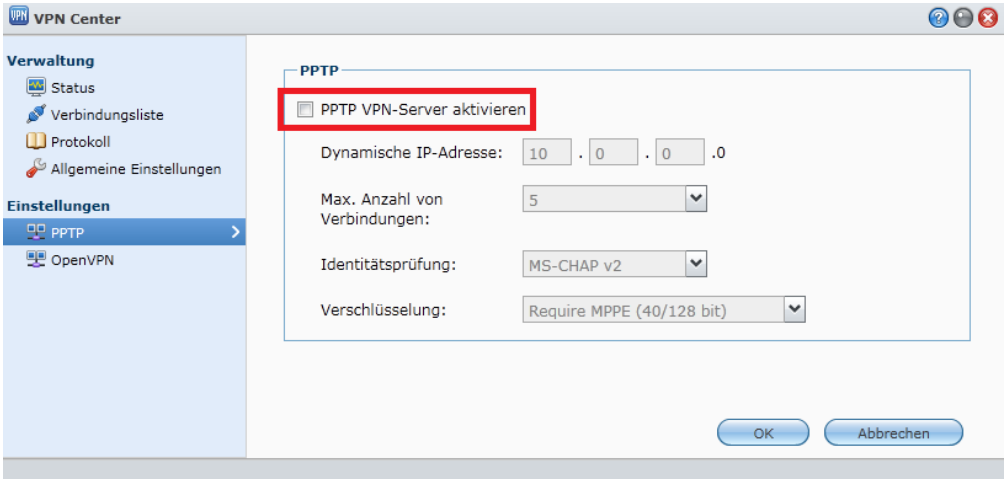
PPTP (Point-to-Point Tunneling Protocol) ist eine häufig verwendete VPN Technologie, die durch die meisten Plattformen unterstützt wird. Für mehr Informationen zu PPTP, lesen Sie bitte hier[2].

Aktivieren des PPTP VPN-Server:

(3) Öffnen Sie wie bereits beschrieben VPN Center

[2] http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

(4) Klicken Sie unter „Einstellungen“ auf „PPTP“.
(5) Setzen Sie einen Haken in das Feld vor „PPTP VPN-Server aktivieren“.



(6) Geben Sie eine virtuelle IP-Adresse für den VPN-Server im Feld „Dynamische IP-Adresse“. Lesen Sie den folgenden Text „Über Dynamische IP-Adressen“ für mehr Informationen.
(7) Setzen Sie eine maximale Anzahl für gleichzeitige Verbindungen.[3]
(8) Wählen Sie eine der folgenden Methoden zur „Identitätsprüfung“ (Authentifizierung) aus der Auswahlliste:
   - PAP: Die Passwörter der Clients werden während der Übertragung nicht verschlüsselt.
   - MS-CHAP v2: Die Passwörter der Clients werden während der Übertragung mit Microsofts CHAP-Algorithmus in Version 2 verschlüsselt.
(9) Wenn Sie „MS-CHAP v2“ zur Identitätsprüfung/Authentifizierung nutzen, wählen Sie unter Verschlüsselung die Stärke dieser:
   - No MPPE: VPN-Verbindungen werden nicht verschlüsselt.
   - Require MPPE (40/128 bit): VPN-Verbindungen werden mit 40- oder 128-bit[4] verschlüsselt, abhängig von den Einstellungen des Client.
   - Maximum MPPE (128 bit): VPN-Verbindungen werden mit 128-bit verschlüsselt, was die größtmögliche Sicherheit bietet.
(10) Bestätigen Sie mit „OK“.

> *Anmerkung: Die Identitätsprüfung/Authentifizierung und Verschlüsselung muss identisch sein mit den Einstellungen des Clients.*

OPENVPN SERVER

OpenVPN ist eine OpenSource-Lösung für VPN. Es schützt Verbindungen mit SSL/TLS-Verschlüsselung. Für mehr Informationen über OpenVPN, lesen Sie bitte hier[5].

Aktivieren des OpenVPN VPN-Server:

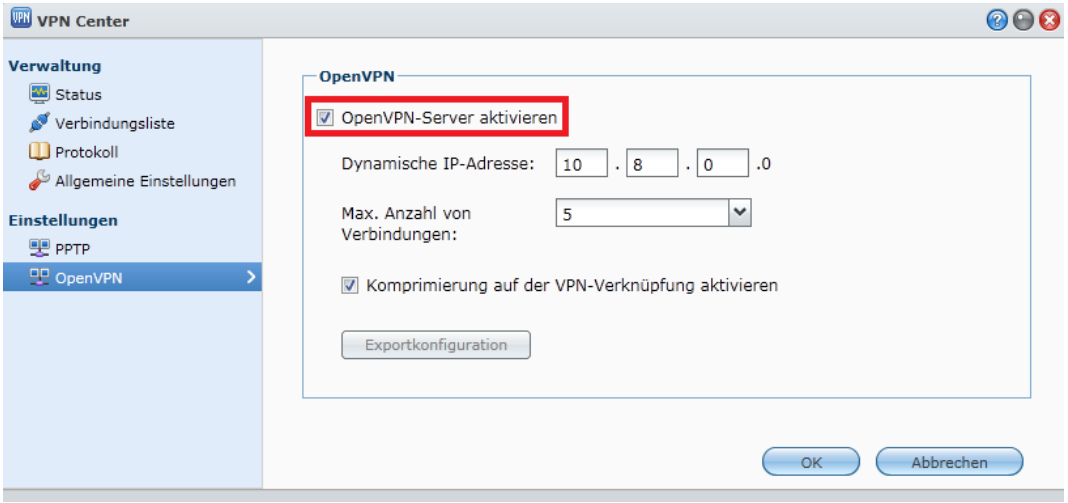
(1) Öffnen Sie wie bereits beschrieben VPN Center.

[3] Der höchste Wert wird von der DiskStation limitiert. Leistungsstärkere Geräte haben eine höhere Anzahl an möglichen Verbindungen. Besuchen Sie den Support-Bereich der Synology-Homepage für weitere Informationen.

[4] Diese „bit“ spezifizieren die Länge des Schlüssels welcher zur Verschlüsselung eingesetzt wird. Ein längerer Schlüssel bedeutet stets mehr Rechenaufwand für beide Seiten, bietet jedoch auch mehr Sicherheit.

[5] http://openvpn.net/

(2) Klicken Sie unter „Einstellungen“ auf „OpenVPN“.
(3) Setzen Sie einen Haken in das Feld vor „OpenVPN-Server aktivieren“.



(4) Geben Sie eine virtuelle IP-Adresse für den VPN-Server im Feld „Dynamische IP-Adresse“. Lesen Sie den folgenden Text „Über Dynamische IP-Adressen“ für mehr Informationen.
(5) Setzen Sie eine maximale Anzahl für gleichzeitige Verbindungen.
(6) Setzen Sie einen Haken vor „Komprimierung auf der VPN-Verknüpfung aktivieren“ wenn Sie dies möchten um die Übertragungsgeschwindigkeit zu erhöhen.
(7) Bestätigen Sie mit „OK“.

Konfiguration von OpenVPN exportieren

Ein OpenVPN-Server muss ein Zertifikat ausgeben über das sich Clients identifizieren. Über die Schaltfläche „Exportkonfiguration“ kann dieses heruntergeladen werden.

Die heruntergeladene Datei ist eine zip-Datei[6] welche 3 Dateien enthält:

- ca.crt: Dies ist das eigentliche Zertifikat welches zur Authentifizierung verwendet wird.
- openvpn.ovpn: Konfigurationsdatei für den Client.
- README.txt: Einfache Anleitung über das Einrichten einer Verbindung mit OpenVPN.

> *Über Dynamische IP-Adressen*
>
> *Abhängig von den Angaben zur Dynamischen IP-Adresse wählt VPN Center aus einem Bereich von Adressen die virtuelle IP-Adresse welche dem VPN-Client zugewiesen wird.*
>
> *Beispiel: Wenn die dynamische IP-Adresse mit „10.0.0.0“ gesetzt ist, werden die IP-Adressen der Clients von „10.0.0.1“ bis „10.0.0.[maximale Anzahl von Verbindungen]“ für PPTP und von „10.0.0.2“ bis „10.0.0.255“ für OpenVPN.*
>
> *Bevor Sie eine Dynamische IP-Adresse für den VPN-Server vergeben, beachten Sie dass die IP-Adresse aus einem der folgenden Bereiche stammen sollte:*
>
> - *Von „10.0.0.0“ bis „10.255.255.0“*

[6] Es gibt viele Programme um diese komprimierten Dateien zu öffnen. Eines der beliebtesten kostenfreien ist 7zip: http://www.7-zip.org/

- *Von „172.16.0.0“ bis „172.31.255.0”*
- *Von “192.168.0.0” bis “192.168.255.0”*

Die spezifizierte dynamische IP-Adresse des VPN-Servers und der daraus resultierende Bereich für Client-IPs sollten nicht mit den Adressen des lokalen Netzwerks in Konflikt stehen.

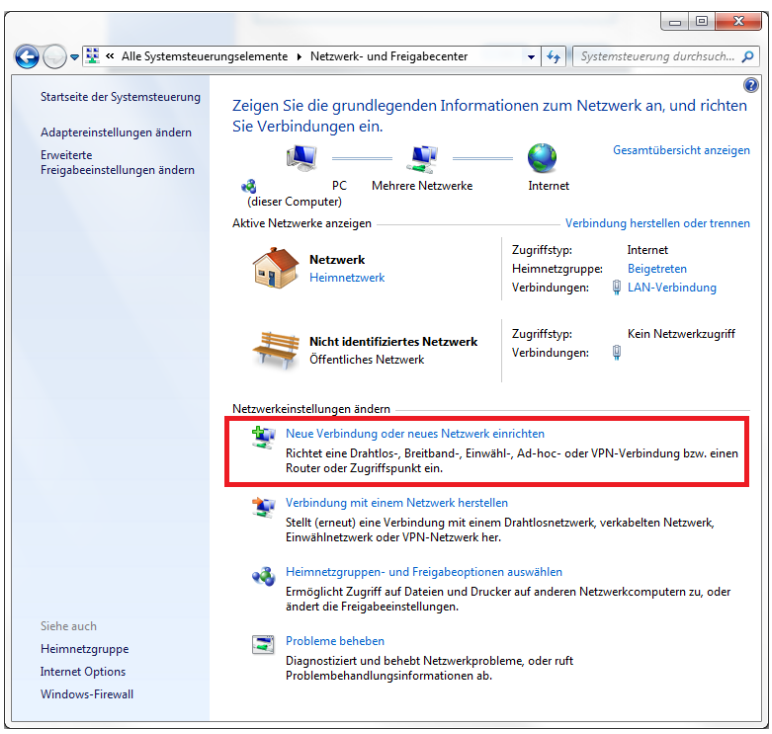
VERBINDEN MIT PPTP

In diesem Abschnitt wird gezeigt, wie eine PPTP VPN-Verbindung mit Windows- und Mac-Systemen aufgebaut werden kann. Eine eingerichtete Portfreigabe bzw. Portweiterleitung in Router und/oder DiskStation wird vorausgesetzt.

WINDOWS

PPTP ist das in Windows integrierte Protokoll ab Windows Vista. Es müssen keine zusätzlichen Anwendungen installiert werden. Um eine solche Verbindung (hier gezeigt an Windows 7) aufzubauen, wird wie folgt vorgegangen:

(1) Öffnen Sie die „Systemsteuerung“ aus dem Startmenü heraus. Klicken Sie anschließend auf „Netzwerk- und Freigabecenter“ und dort auf „Neue Verbindung oder neues Netzwerk einrichten“.



(2) Wählen Sie nun „Verbindung mit dem Arbeitsplatz herstellen“ und anschließend „Die Internetverbindung (VPN) verwenden“.

(3) Bei „Internetadresse“ muss die externe Adresse (statische IP oder DDNS) der DiskStation eingegeben werden. Der „Zielname“ ist nur für Sie und Windows um das Netzwerk später zu identifizieren.

(4) Die Benutzerdaten im folgenden Dialog sind mit denen des DSM identisch. Ein letzter Klick auf „Verbinden“ schließt den Vorgang ab und das VPN ist bereit zur Verwendung.

(5) Um die Verbindung zu trennen, klicken Sie auf das Netzwerk-Symbol von Windows und wählen Sie die VPN-Verbindung mittels Rechtsklick aus der Übersicht.

(6) Wenn die Verbindung nicht erfolgreich aufgebaut werden kann, überprüfen Sie die Einstellungen der Verbindung. Wählen Sie dazu wieder die Netzwerkübersicht und klicken Sie statt auf „Trennen“ auf „Eigenschaften“. Prüfen Sie hier die Einstellungen unter „Sicherheit“. Diese müssen identisch mit den Einstellungen aus VPN Center sein. Im nächsten Reiter müssen die Protokolle *IPv4* und *Client für Microsoft-Netzwerke* aktiviert sein.

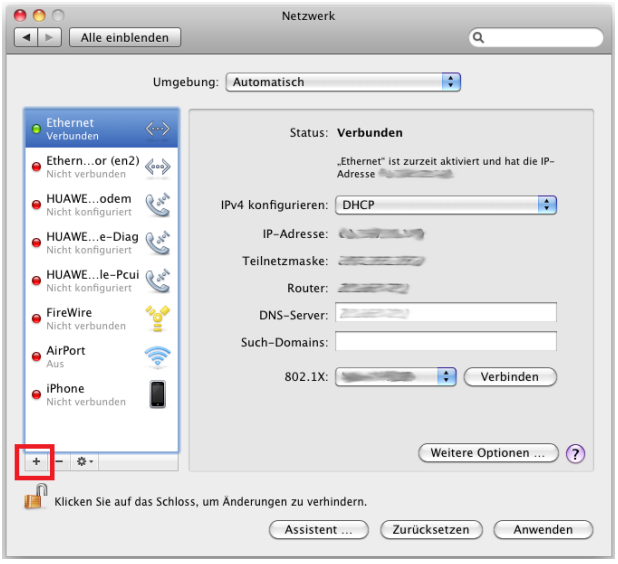
(7) Sollten weiterhin Probleme auftreten, lesen Sie bitte das Kapitel über die Gateway Konfiguration in diesem Dokument.

MAC

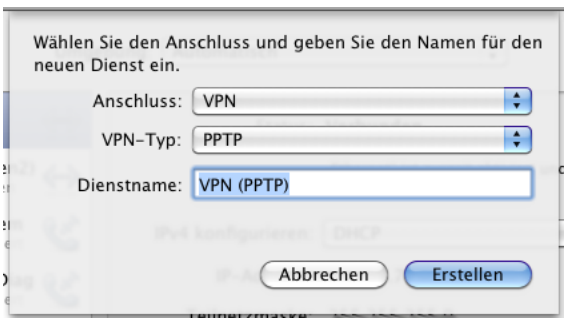
PPTP ist das in Mac OS integrierte Protokoll. Es müssen keine zusätzlichen Anwendungen installiert werden. Um eine solche Verbindung aufzubauen, wird wie folgt vorgegangen:

(1) Im Apple Menü, klicken Sie auf „Systemeinstellungen“ und anschließend dort auf „Netzwerk“.

(2) Erstellen Sie über einen Klick auf das „+“-Symbol am linken unteren Rand eine neue Verbindung.

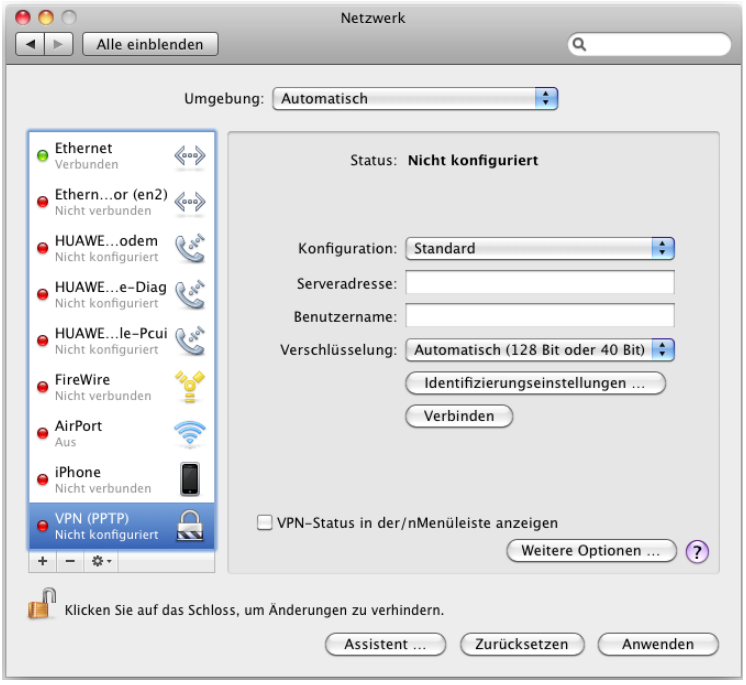


(3) Wählen unter „Anschluss“ „VPN“, unter „VPN-Typ“ „PPTP“ und geben Sie der Verbindung anschließend einen Namen um Sie später identifizieren zu können.



(4) Geben Sie unter „Serveradresse“ die Adresse ein, unter der Ihr Netzwerk via Internet erreichbar ist (statische IP oder DDNS-Namen).

(5) Geben Sie einen gültigen Benutzer des DSM in „Benutzername“ an.



(6) Wählen Sie die „Verschlüsselung“. Diese Einstellung muss identisch mit der in VPN Center unter PPTP sein! Je höher die Verschlüsselung, desto sicherer ist die Verbindung.

(7) Klicken Sie auf „Identifizierungseinstellungen“ und geben Sie dort das Passwort des in (5) angegebenen DSM-Benutzers ein. Bestätigen Sie mit „OK“.

(8) Schließen Sie die Konfiguration mit einem Klick auf „Verbinden“ ab um das Gerät mit dem VPN Center zu verbinden. Anschließend können Sie an selbiger Stelle die Verbindung wieder trennen.

(9) Sollten weiterhin Probleme auftreten, lesen Sie bitte das Kapitel über die Gateway Konfiguration in diesem Dokument.

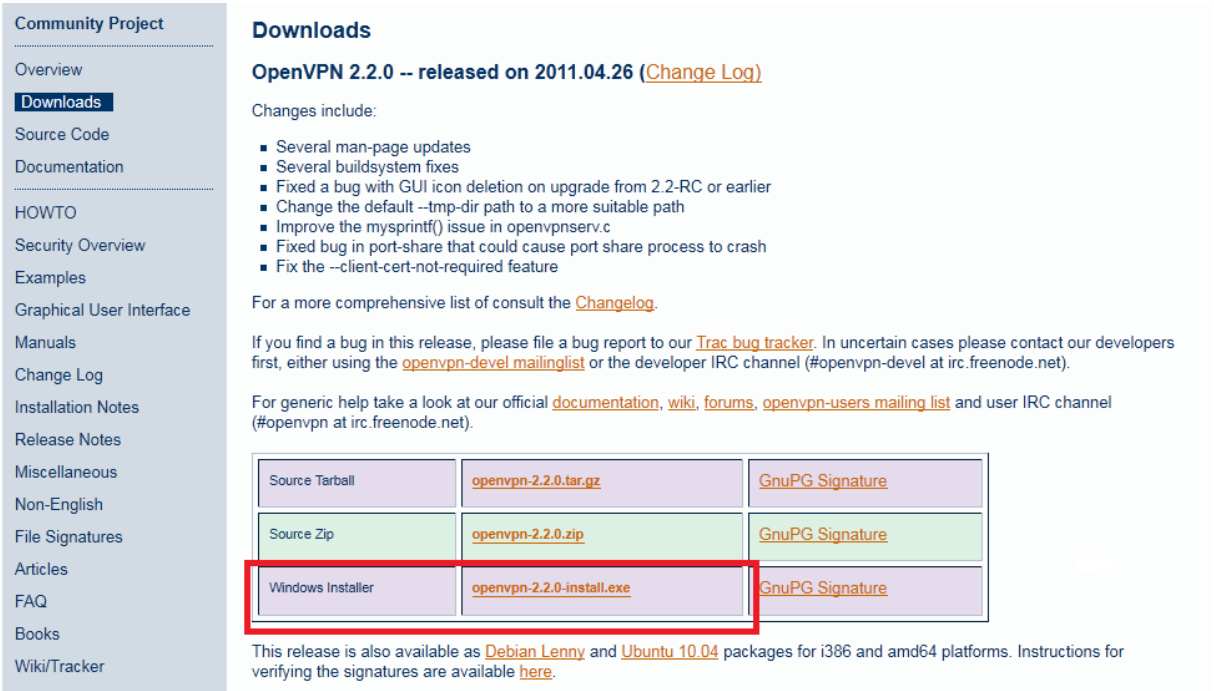
VERBINDEN MIT OPENVPN

In diesem Abschnitt wird gezeigt, wie eine OpenVPN-Verbindung mit Windows- und Mac-Systemen aufgebaut werden kann. Eine eingerichtete Portfreigabe bzw. Portweiterleitung in Router und/oder DiskStation, sowie ein Export der Konfiguration des VPN Center wird vorausgesetzt.

WINDOWS

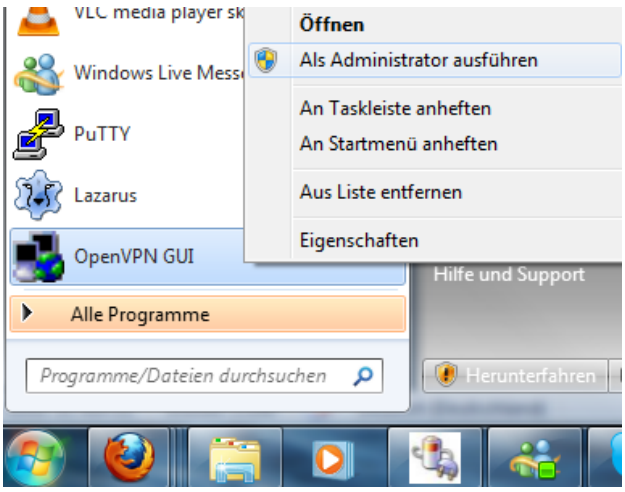
OpenVPN ist ein OpenSource-Projekt um VPN-Verbindungen aufzubauen. Sie benötigen dazu die OpenVPN-Software von der Internetseite des Projekts: http://openvpn.net/index.php/open-source/downloads.html

Wählen Sie dort die aktuellste Version des „Windows Installer“, nicht jedoch eine Beta- oder Entwicklerversion. Überprüfen Sie aus Sicherheits- und Stabilitätsgründen bitte OpenVPN regelmäßig auf Aktualisierungen.



Nach erfolgter Installation der OpenVPN-Software folgen Sie bitte diesen Schritten um eine Verbindung aufzubauen:

(1) Öffnen Sie das Startmenü und klicken Sie mit der rechten Maustaste auf den Eintrag „OpenVPN GUI“. Klicken Sie nun auf „Als Administrator ausführen“ und bestätigen Sie die Sicherheitsabfrage.



(2) Öffnen Sie die zip-Datei welche Sie aus VPN Center exportiert haben. Diese sollte 3 Dateien beinhalten: ca.crt,openvpn.ovpn und README.txt.

(3) Öffnen Sie die Datei openvpn.ovpn mit einem Texteditor und ersetzen Sie die Zeichenkette „YOUR_SERVER_IP“ mit der externen Adresse Ihres Netzwerks (statische IP-Adresse oder DDNS-Adresse). Speichern Sie anschließend die Datei

(4) Verschieben Sie die Dateien ca.crt und openvpn.ovpn in den Ordner „config“ im Installationsverzeichnis von OpenVPN. Standardmäßig ist dieses Verzeichnis „C:\Program Files\OpenVPN“ bzw. „C:\Program Files (x86)\OpenVPN“ für 64-bit Windows-Systeme.

(5) Doppelklicken Sie auf das OpenVPN-Symbol in der Taskleiste.

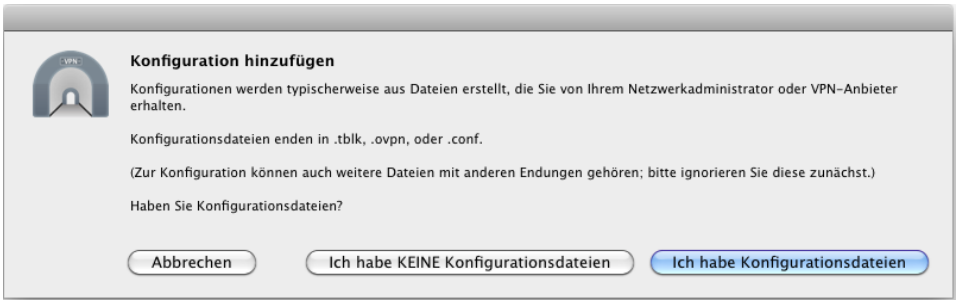
(6) Verbinden Sie sich mit Benutzer und Passwort des DSM mit VPN Center.

MAC

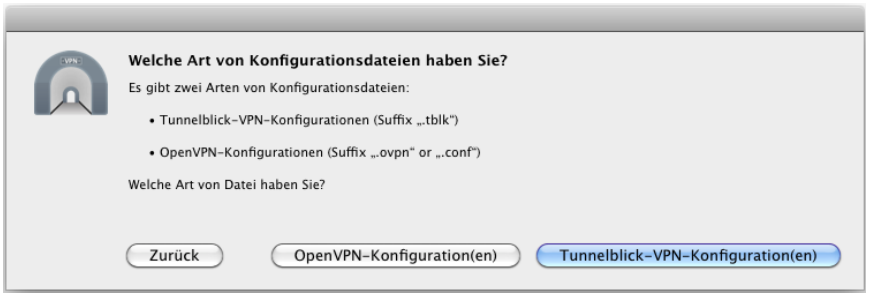
Um OpenVPN mit Mac zu nutzen wird die Software „Tunnelblick“ benötigt:
http://code.google.com/p/tunnelblick/

Diese muss installiert und anschließend als Administrator gestartet werden. Die finale Konfiguration erfolgt in diesen Schritten:

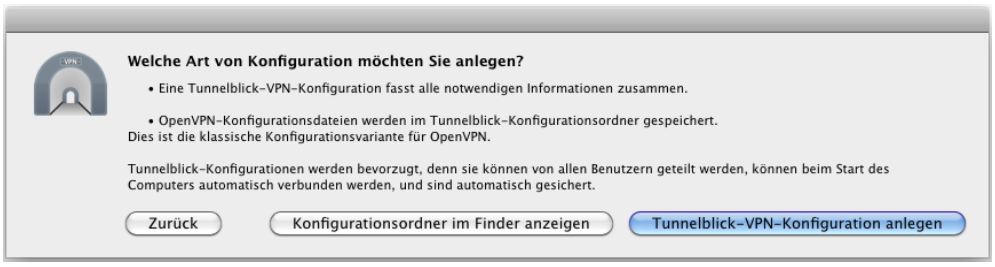
(1) Der Willkommensbildschirm von Tunnelblick fragt, ob Sie Konfigurationsdateien für die gewünschte Verbindung besitzen. Wählen Sie hier „Ich habe Konfigurationsdateien“.



(2) Wählen Sie nun „OpenVPN-Konfiguration(en)“.

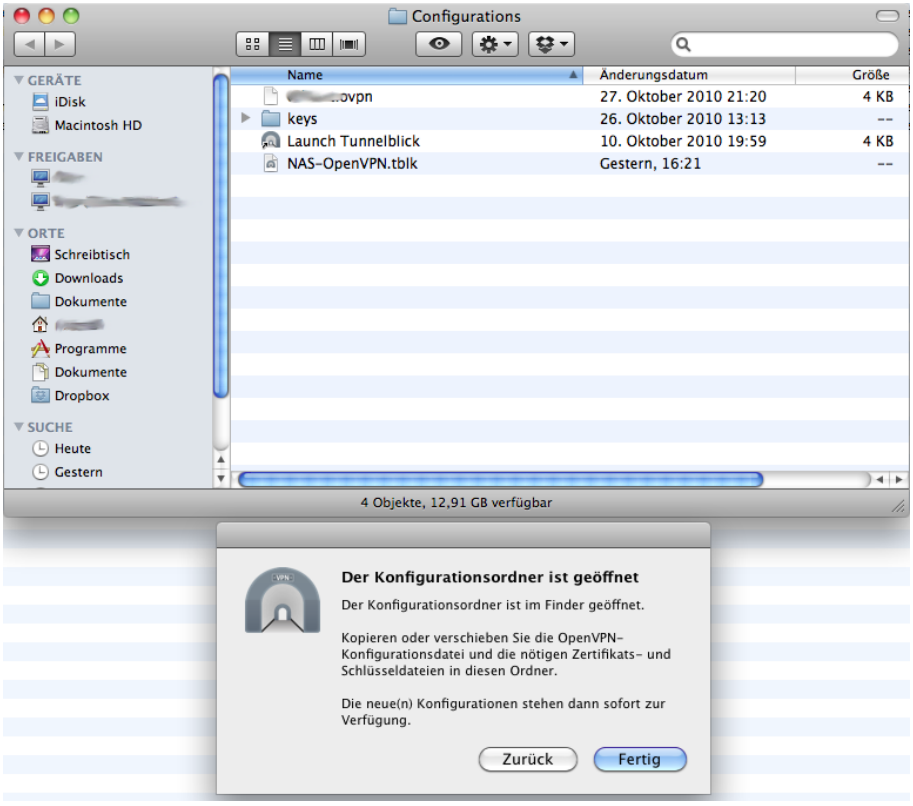


(3) Nachdem Sie Tunnelblick nun bestätigt haben, dass Sie im Besitz der Dateien sind („Konfigurationsordner im Finder anzeigen“) wird der entsprechende Ordner angezeigt.



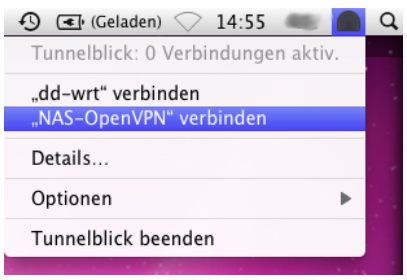
(4) Öffnen Sie nun die exportierte zip-Datei und bearbeiten Sie die „openvpn.ovpn“. Ersetzen Sie in dieser Datei die Zeichenkette „YOUR_SERVER_IP“ mit der externen Adresse ihres Netzwerks (statische, externe IP oder DDNS-Adresse).

(5) Kopieren Sie nun die Dateien „openvpn.ovpn“ und „ca.crt“ in den geöffneten Ordner.

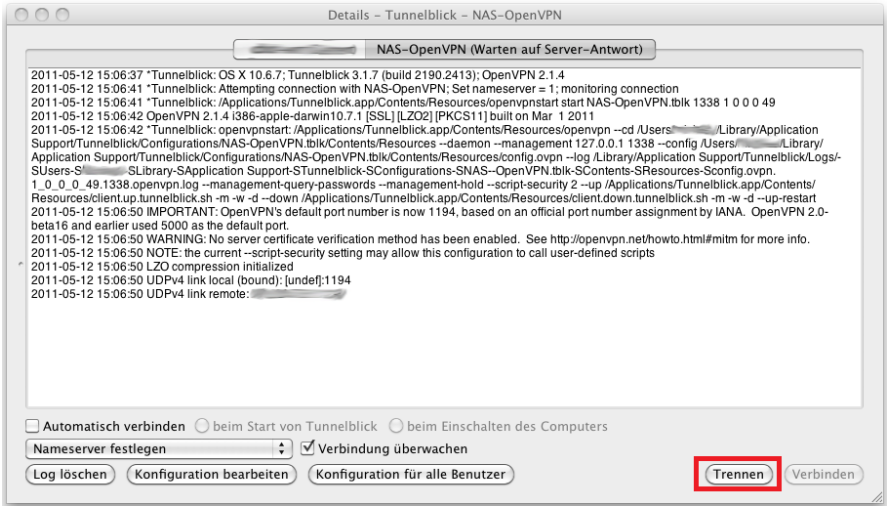


(6) Bestätigen Sie die Vollständigkeit der Konfiguration gegenüber Tunnelblick, indem Sie auf „Fertig“ klicken.

(7) Sie können die neue Verbindung nun in Tunnelblick auswählen. Klicken Sie auf das Symbol in der oberen rechten Ecke und wählen Sie „[Name] verbinden“.



(8) Weitere Informationen über die Verbindung erhalten Sie, wenn Sie auf „Details“ klicken. Dort können Sie die Verbindung auch „Trennen“.



GATEWAY-EINSTELLUNGEN FÜR VPN-VERBINDUNGEN

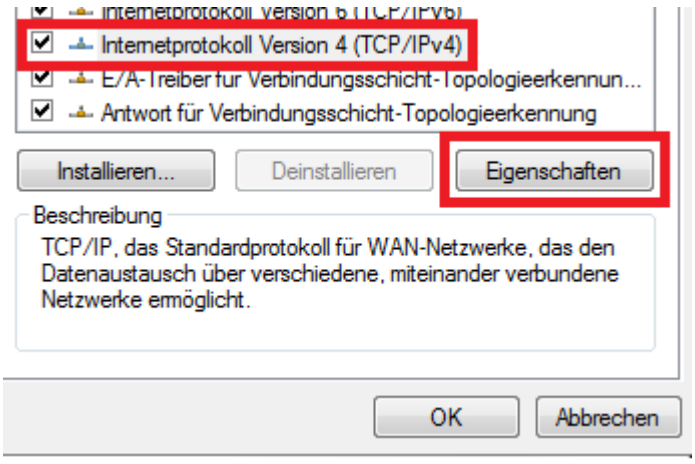
WINDOWS

Wenn eine VPN-Verbindung unter Windows aktiv ist, verwendet das System auch das dort konfigurierte Gateway für Internetverbindungen. Jedes Datenpaket wandert somit zunächst durch das VPN, tritt an der DiskStation wieder aus und verlässt erst dort das sichere Netzwerk in Richtung Internet. Dieser längere Weg kann sich auch durch die häufig geringere Bandbreite im Upload negativ auf die Interneterfahrung auswirken. Verbindungen können deutlich länger laden oder gar abbrechen.

Um dies zu umgehen und das Gateway zu verändern, folgen Sie den folgenden Schritten:

(1) Klicken Sie in der Windows-Taskleiste auf das Netzwerksymbol und klicken Sie mit der rechten Maustaste auf die aktive VPN-Verbindung. Wählen Sie nun „Einstellungen“.

(2) Wechseln Sie zum Reiter „Netzwerk“ und wählen Sie dort IPv4. Nach einem Klick auf „Eigenschaften“ öffnet sich ein neues Fenster.



(3) Klicken Sie nun zuerst auf „Erweitert“ und dann auf den Reiter „Allgemein“.

(4) Setzen Sie einen Haken vor „Standardgateway für das Remotenetzwerk verwenden“.

Verbindungen für das Internet werden nun nicht durch das VPN geleitet, sondern verlassen direkt das lokale Netzwerk.

MAC

Im Gegensatz zu Windows, leitet Mac OS den Netzwerkverkehr nicht zwangsweise über das VPN. Häufig ist dies aus Sicherheitsgründen jedoch erwünscht. In diesem Fall muss die Konfiguration geändert werden:

(1) Öffnen Sie „Terminal“ und führen Sie den folgenden Befehl aus:

> ifconfig –a

(2) Sie sehen nun die Netzwerkverbindungen. Unter „pppX“ wird u.a. das VPN aufgeführt, inklusive den dort definierten Gateway-Einstellungen um eine Verbindung durch das VPN zu leiten. Um nun auch die normalen Netzwerkschnittstellen auf das VPN-Gateway zu leiten, geben Sie folgenden Befehl ein:

> sudo route add –net 192.168.X.X/16 10.10.0.50

Oder

> sudo route add –net 192.168.X.X/16 10.10.0.1

Ändern Sie unbedingt „10.10.0.50“ bzw. „10.10.0.1“ auf die Adressen wie von „ifconfig“ unter „pppX“ ausgegeben. Der Internetverkehr wird nun über Ihr VPN geleitet.

III. COMMUNITY-ADDITUM

TUNNELBLICK-KONFIGURATION FÜR MAC ERSTELLEN

Um den Weg der Tunnelblick-Konfiguration etwas abzukürzen kann man auch eine spezielle Konfiguration für dieses Programm erstellen. Zur Weitergabe an Kunden, Mitarbeiter oder Freunde ist diese Datei sehr viel besser geeignet als der lange Einrichtungsvorgang. Bitte folgen Sie dieser kurzen Anleitung:

(1) Das zip-Archiv muss extrahiert werden. Eine Änderung der Endung des zip-Archivs führt nicht zum gewünschten Ziel!
(2) Die Datei „openvpn.ovpn“ muss dann wie oben beschrieben angepasst werden („YOUR_SERVER_IP“ ersetzen).
(3) Nun alle Dateien in einen neuen Ordner verschieben. Dieser Ordner sollte möglichst eindeutig benannt werden, etwa „NAS-OpenVPN“.
(4) Zuletzt muss die Endung des Ordners geändert werden in „.tblk“. Im genannten Beispiel würde der Ordner somit „NAS-OpenVPN.tblk“ heißen. Dies macht den Ordner zu einer Tunnelblick-Konfigurationsdatei die ähnlichem selbigem Weg in ihre Bestandteile zerlegt werden kann.
(5) Diese Datei kann nun beliebig an Personen verschickt werden. Bei installiertem Tunnelblick wird der Benutzer bei Doppelklick auf die Datei nach Bestätigung und Administrationspasswort gefragt. Nach diesen beiden Schritten ist die Konfiguration in Tunnelblick vorhanden und die Verbindung kann über das Menü eingegangen werden.

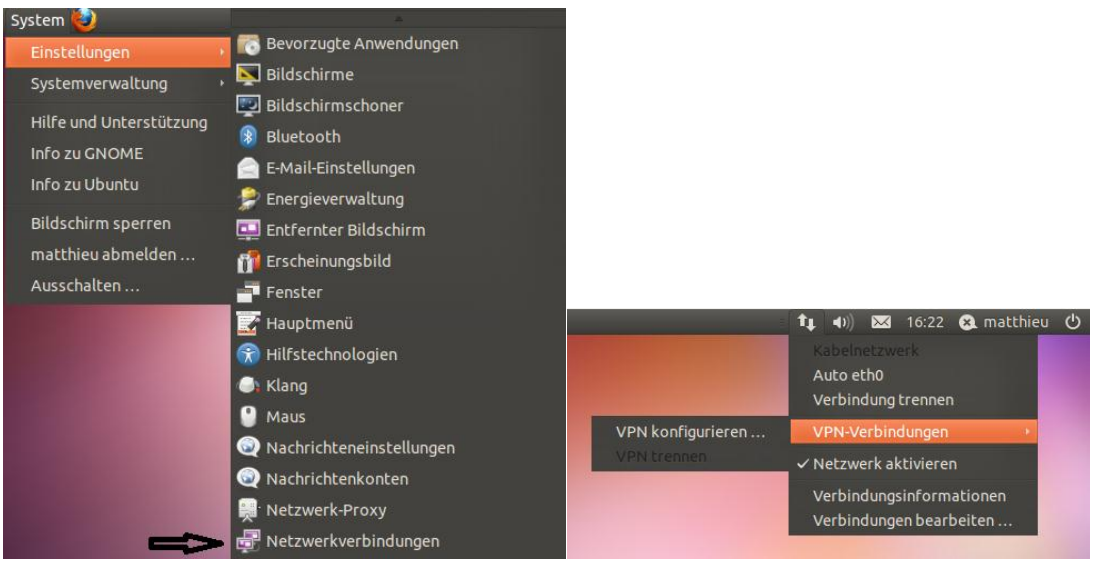
VPN UNTER LINUX (UBUNTU/MINT)

Da Linux im offiziellen Teil der Anleitung nicht, bzw. im Original nur durch Links berücksichtigt wird, hier zusätzlich eine Anleitung zur Verwendung von OpenVPN unter Linux. Exemplarisch für die verschiedenen Linux-Distributionen werden hier die weit verbreiteten Systeme Ubuntu und Linux Mint behandelt.

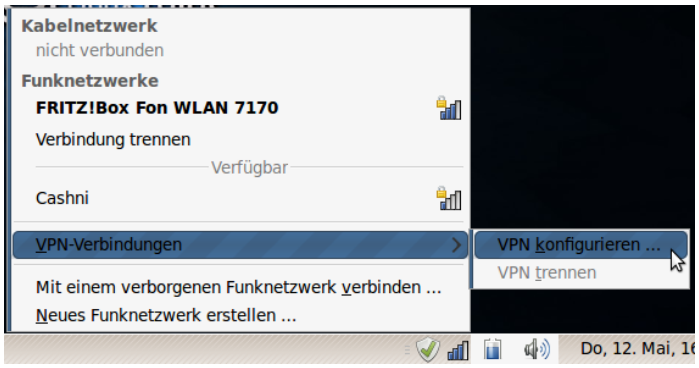
PPTP

(1) Der einfachste Zugang zur VPN-Konfiguration führt über die Taskleiste und das dortige Netzwerksymbol. Alternativ kann man das Fenster Netzwerkverbindungen auch über die Einstellungen öffnen

Ubuntu:

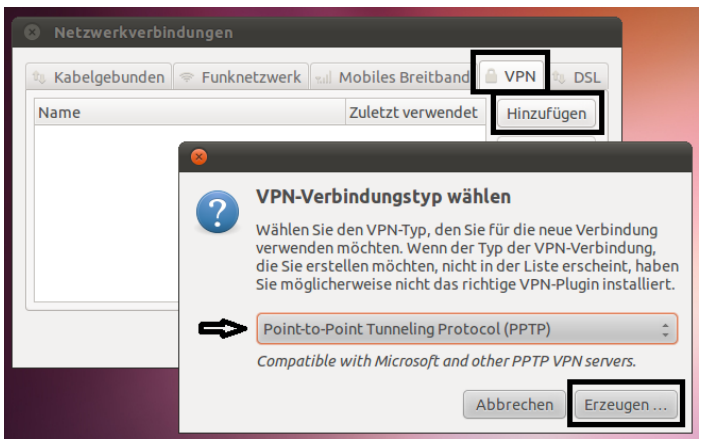


Linux Mint:

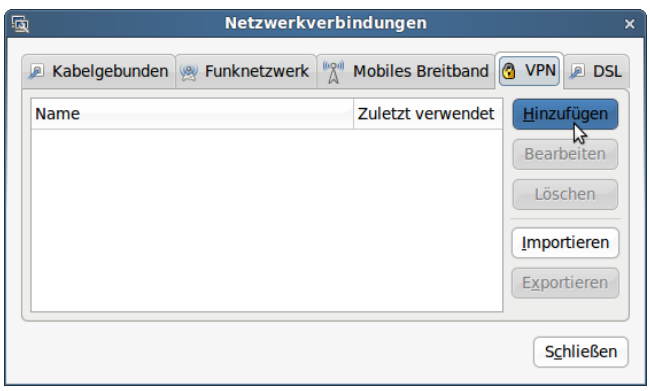


(2) Der Reiter VPN führt alle bereits konfigurierten Verbindungen auf. Über die Schaltfläche „Hinzufügen“ lässt sich eine weitere Verbindung erstellen. Standardmäßig können sowohl Ubuntu als auch Linux Mint nur mit PPTP umgehen. Auf OpenVPN wird im nächsten Kapitel eingegangen.

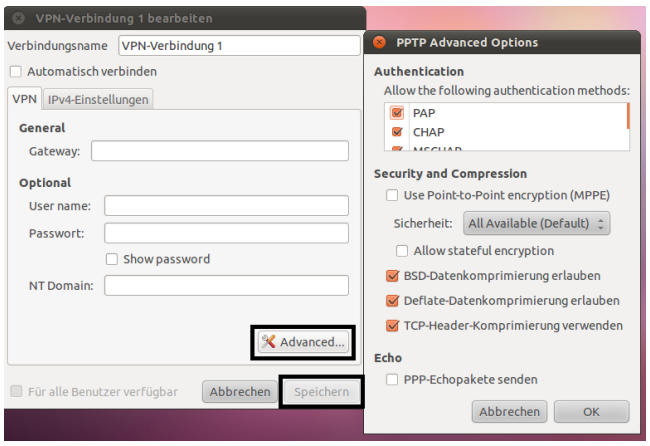
Ubuntu:



Linux Mint:



(3) Die Einstellungen sind vergleichbar mit denen unter Windows und Mac. Auch hier gilt: Alle Einstellungen bezüglich Authentifikation und Verschlüsselung müssen mit denen des VPN Center identisch oder kompatibel sein. Gateway ist wiederum die externe Adresse, Benutzername und Passwort sind mit denen des DSM identisch.

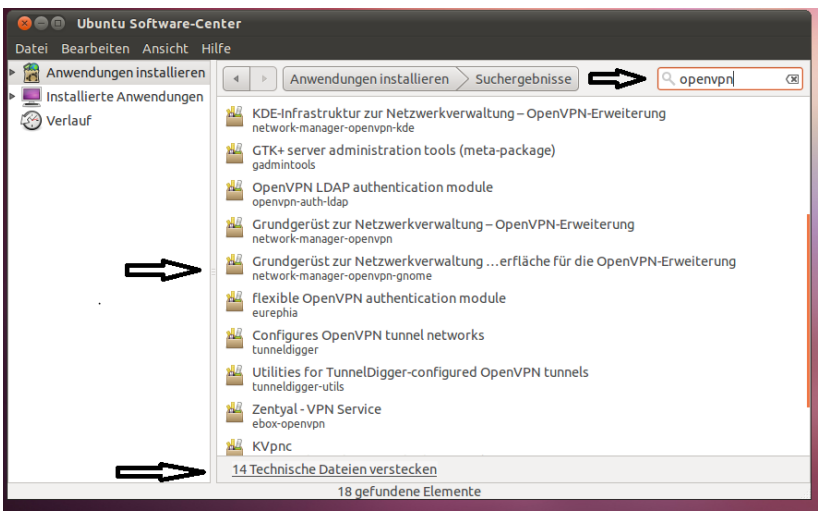


(4) Mit einem Klick auf „Speichern“ werden die Zugangsdaten dauerhaft im System gespeichert und die Verbindung kann sowohl über das Symbol in der Taskleiste als auch über das Menü „Netzwerkverbindungen“ aktiviert werden.

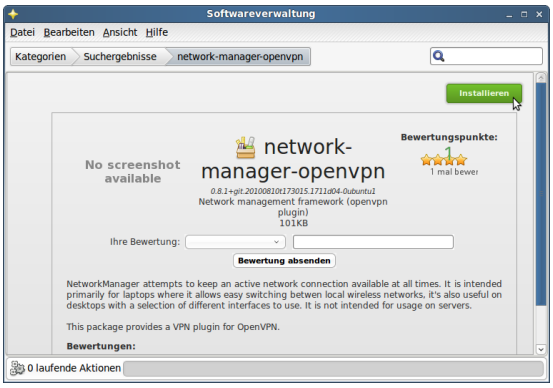
OPENVPN

Um im oben beschriebenen Einrichtungsvorgang auch OpenVPN zur Auswahl zu haben, muss ein Plugin für den Netzwerkmanager installiert werden. Sowohl Ubuntu als auch Linux Mint haben eine Paketverwaltung (Ubuntu Software-Center bzw. Softwareverwaltung). Beide Distributionen bieten darin das Paket „network-manager-openvpn“ an. Ubuntu versteckt dieses jedoch als „Technische Datei“. Erst ein Klick auf die Option am unteren Bildrand zeigt es auch an.

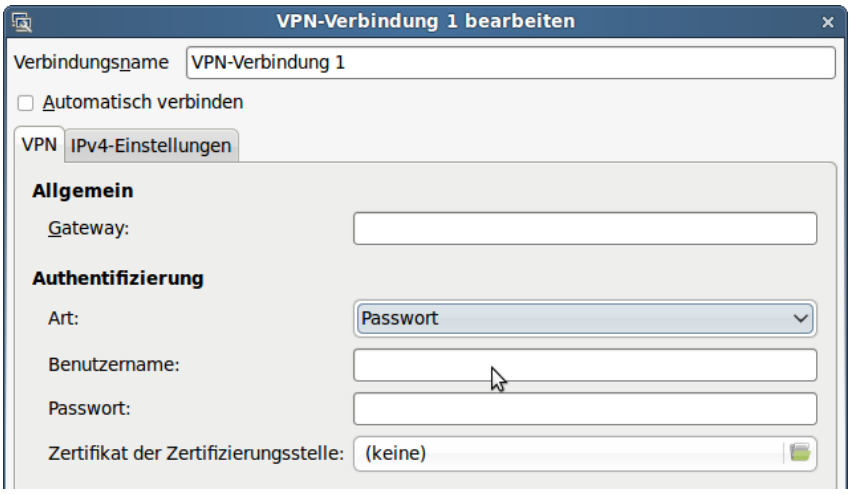
Ubuntu:



Linux Mint:



Hat man im Einstellungsdialog nun OpenVPN ausgewählt, so bieten sich folgende Möglichkeiten:



Wichtig sind hier die Einstellungen zur Authentifizierung. Um mit VPN Center zu arbeiten muss „Passwort“ gewählt werden. Das „Zertifikat der Zertifizierungsstelle“ ist in der zip-Datei der Exportfunktion enthalten. Benutzername und Passwort sind wiederum mit denen des DSM identisch.