Zugriff auf ownCloud per VPN

Teil I – Einrichtung des VPN-Servers auf Synology Diskstation

Nachdem ich bereits dargestellt habe, wie in meiner Umgebung der Zugriff auf die ownCloud-Instanz per https realisiert werden könnte, nun die Alternative zu https – Zugriff über ein VPN. Warum greife ich zu VPN und bleibe nicht bei https? Dafür gibt es einen ganz einfachen Grund: die Verbindung zu ownCloud ist nicht die einzige Anwendung, die ich auf meiner Diskstation nutzen möchte. Ich möchte auch Audiostation, Photostation und diverse andere Anwendungen nutzen bis hin zum direkten Browserzugriff auf die Diskstation. Das Problem besteht nun darin, das all diese Anwendungen eigene Ports verwenden, am Router also für all diese Anwendungen Ports geöffnet werden müssen. Jeder geöffnete Port aber stellt ein gewisses Sicherheitsrisiko dar …

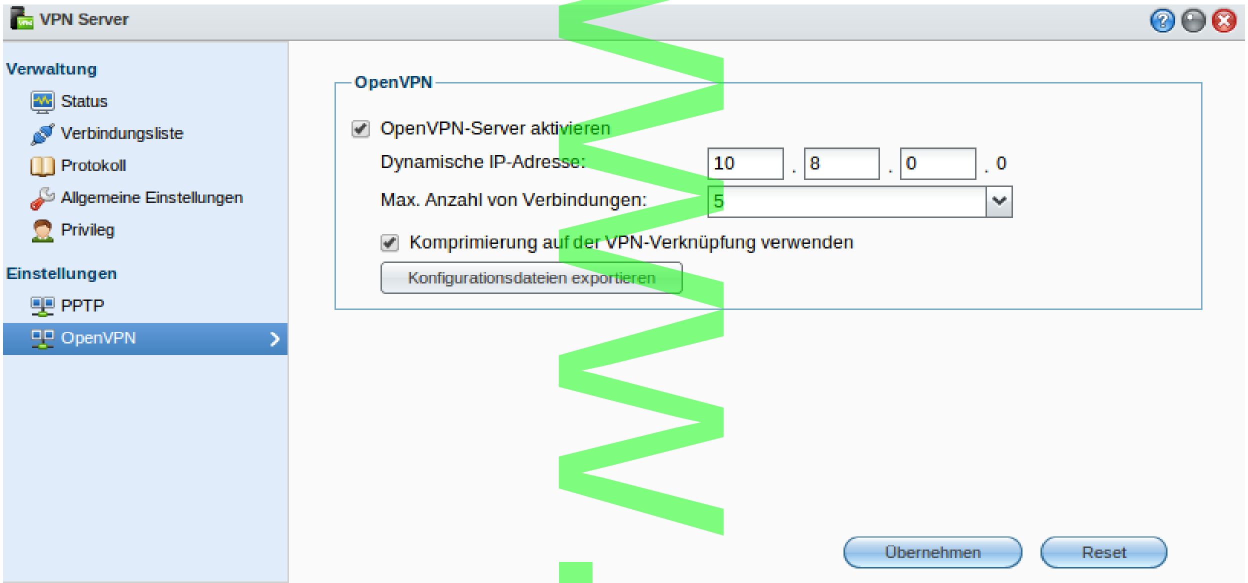
Bei einer Verbindung per VPN wird dagegen nur ein einziger Port geöffnet, denn der Datenverkehr wird über den VPN-Server geleitet und so verteilt, als wenn der anmeldende Client sich direkt im Lokalen Netzwerk befindet. VPN wird von allen PC-Betriebssystemen und auch Android-Smartphones können derartige Verbindungen aufbauen. Ich nehme an, das auch iPhones das können, weiss es allerdings nicht genau …

Der VPN-Server der Diskstation unterstützt im Moment 2 Protokolle: PPTP und OpenVPN. Mit der DSM 4.3, derzeit in der Betaphase, kommt ein drittes Protokoll hinzu: IPsec/L2TP. Über die Unterschiede der Protokolle könnt ihr euch im Netz informieren (Wikipedia oder Faqs der Firma Synology). Eine umfassende Erläuterung würde in diesem Rahmen zu weit führen …

Ich selbst nutze OpenVPN. Gründe OpenVPN statt PPTP zu verwenden sind u.a.:

- höhere Sicherheit, da digitale Zertifikate verwendet werden
- höhere Geschwindigkeit durch mögliche Kompression der zu übertragenden Daten
- hohe Zuverlässigkeit
- Verschlüsselung mit bis 160 oder 256 bit.

Die Einrichtung von OpenVPN am Synology VPNServer ist relativ einfach: Nach der Installation des Paketes steht im Hauptmenu auch ein Icon zum Start des VPN-Servers zur Verfügung über das die Konfigurationsroutine gestartet wird. Unter Einstellungen OpenVPN-Server aktivieren, Komprimierung aktivieren – übernehmen (siehe Bild 1).



Jetzt bleibt nur noch die Schaltfläche “Konfigurationsdateien exportieren” zu drücken. Eine “openvpn.zip” wird in euer Standard-Downloadverzeichnis heruntergeladen. Entpackt ihr diese Datei, stehen folgende 3 Dateien zur Verfügung:

1. Readme.txt. Hier steht die Beschreibung der nächsten Schritte – lesen hilft. 😉
2. Openvpn.ovpn. Konfigurationsdatei für den Client. Diese Datei muss mit einem Texteditor bearbeite werden, der Eintrag “Your_Server_IP” muss mit der Internet-IP des Routers oder dem DynDNS-Namen ersetzt werden.
3. ca.crt. Zertifikatsdatei des Servers.

Datei 2 und 3 braucht ihr für die Konfiguration der Clients. Nun muss am Router nur noch der entsprechende Port für OpenVPN weitergeleitet werden. OpenVPN verwendet standardmäßige Port 1194 und UDP. Der Eintrag in Freigabeliste der Fritz!Box wird in Bild 2 dargestellt.

Damit ist der VPN-Server eurer Diskstation fertig konfiguriert. Einrichtung der Clients unter einem KDE-Linux bzw. einem Windows-PC folgt in einem weiteren Artikel.

Teil 2 – OpenVPN-Client unter Linux (KDE) einrichten

Nachdem wir unseren VPN-Server auf der Synology Diskstation konfiguriert haben und serverseitig alles bereit ist für den Verbindungsufbau, geht es nun an die Einrichtung der Clients. Ich werde auf 3 verschieden Clients eingehen: Linux mit KDE (in meinem Fall ZevenOS-Neptune 3.1), Windows (ein Windows 7 -Notebook) und Android (Galaxy Note II Smartphone und Galaxy Note 2 Tab 10.1) – ganz einfach weil ich eben solche Clients mit ownCloud verbinde. Mit diesen Geräten synchronisiere ich zum einen Dateien (im Moment ca.

900 MB), zum anderen werden meine Kalender- und Kontaktdaten synchron gehalten. Dieser Artikel widmet sich erst einmal ausschließlich der Implementation von OpenVPN im KDE-Linux.

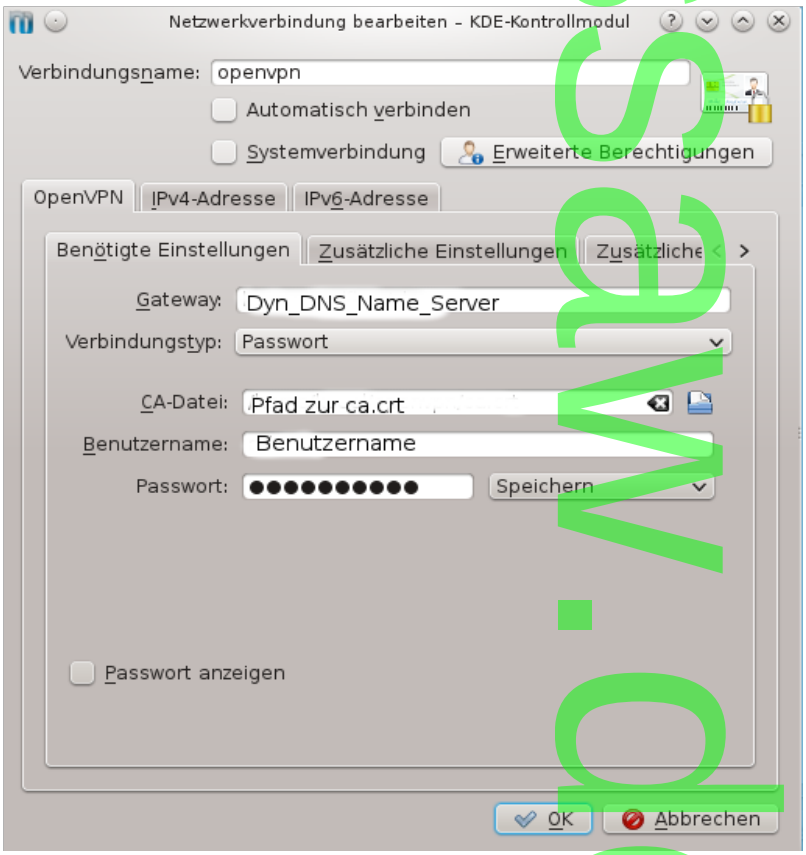
Wie bereits geschrieben setze ich auf meinen Rechnern im Moment ZevenOS-Neptune 3.1 ein, eine debianbasierte Distribution.

1. Voraussetzungen

Ich verwende zur Verwaltung der Netzwerkverbindungen den in KDE integrierten Networkmanager. Nach meinem Wissen unterscheidet er sich bei der Handhabung nicht von seinem Pendanten aus der Gnomewelt. Da diese Komponente Standard in der KDE-Welt ist, sollte sie auf euren Rechnern bereits installiert sein. Desweiteren benötigen wir unsere auf dem Server erzeugten Dateien OpenVPN.vpn und CA.crt. Ich habe dazu in Home ein Verzeichnis OpenVPN angelegt und die Dateien dorthin kopiert.

2. OpenVpn einrichten

Networkmanager öffnen und “Verbindungen verwalten” aufrufen, bei “Netzwerkverbindungen” den Reiter VPN auswählen. Durch die Erstellung der Konfigurationsdatei OpenVPN.vpn haben wir es an dieser Stelle sehr leicht: statt nun jede Einstellung manuell vorzunehmen, können wir die Einstellungen inklusive des Verweises auf unsere Zertifikatsdatei einfach importieren. Dazu die Schaltfläche “importieren” anklicken, Pfad zu unserer OpenVPN.vpn auswählen und OK. Das Ergebnis sollte dann etwa so aussehen:



OK und an sich ist schon nicht mehr zu tun. Ein Hinweis noch: der hier gewählte Verbindungstyp ist die einfachste Form der Authentifizierung, es können auch zertifikatsbasierte Methoden ausgewählt werden. Halte ich im privaten Umfeld in dem wir uns ja hier bewegen nicht unbedingt für notwendig. Es besteht auch die Möglichkeit, dass erforderliche Passwort nicht zu speichern, sondern jedes Mal abfragen zu lassen – eine Entscheidung, die jedem selbst überlassen ist …

Im Networkmanager ist nun ein weiteres Symbol zu sehen, welches den oben vergebenen Namen trägt. Anklicken und die Verbindung zu unserem Netz zu Hause wird aufgebaut. Jetzt ist es möglich, im Browser ownCloud aufzurufen, per

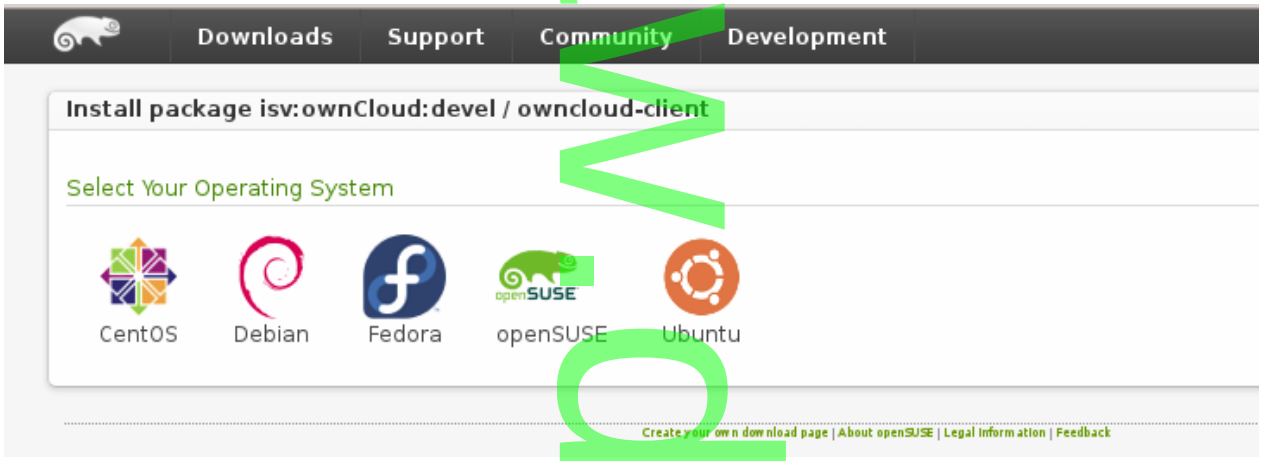
http://interne_IP_Adresse/owncloud bzw.
https://interne_IP_Adresse/owncloud

wird der Anmeldebildschirm der ownCloud-Instanz aufgerufen und man kann damit arbeiten, als würde man sich zu Hause, im eigenen Netzwerk befinden.

3. Installation des Synchronisationsclients

Durch ownCloud.org werden diverse Clients für verschiedene Betriebssystem bereit gestellt. Für Linux hat man die Möglichkeit sich entweder den Client aus den Quellen selbst zu kompilieren oder sich den fertigen Client per Repository in das System einzubinden. Diesen Service stellt dankenswerte openSuse zu Verfügung, inklusive einer ausführlichen Anleitung, wie die Repositories in das System eingebunden werden können …

Opensuse stellt fertige Clients für CentOS, Debian, openSuse, Fedora und Ubuntu zur Verfügung. Die Debianpakete können auch für die “Tochterdistributionen” Kanotix und ZevenOS-Neptune sowie weitere debianbasierte OS verwendet werden. Aktuelle Version des Clients ist 1.3 .



4. Abschluss

Nach der Installation des Clients können die gewünschten Datei-Synchronisationen eingerichtet werden. Die Installation ist selbsterklärend.
Um Kontakt- und Kalenderdaten zwischen KDE und ownCloud zu synchronisieren, empfehle ich die Verwendung der KDE-PIM. Hier ist es relativ einfach möglich, ownCloud als Quelle einzubinden. Voraussetzung hierfür ist KDE in Version 4.8.4 oder höher, allerdings unterstützen nicht alle Distributionen dieses Feature, z.B. ist die Einbindung per KDE-PIM in Kanotix nicht möglich.
Nächster Artikel: Open-VPN in Windowssystemen einbinden.

Teil III - OpenVPN-Client unter Windows einrichten

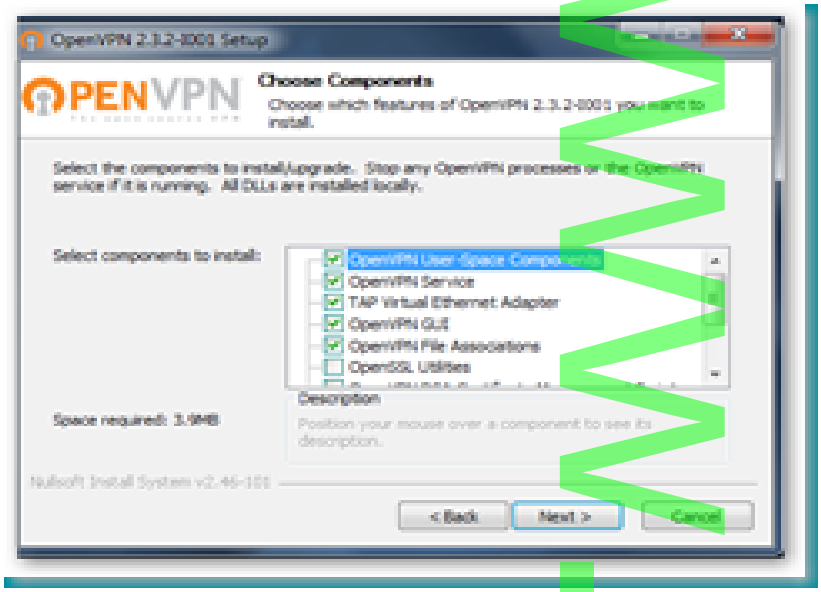
Nachdem nun der VPN-Server auf der Diskstation konfiguriert ist und seinen Job macht und die Linux-Clients per VPN eingebunden sind, geht es nun darum, Windows-Rechner den Zugriff ebenfalls per VPN zu ermöglichen. Im Gegensatz zu den Linuxen unterstützt Windows das bisher verwendete Protokoll OpenVPN nicht – jedenfalls nicht “von Hause” aus. Der einfachste Weg ein Windows per VPN mit einer Gegenstelle zu verbinden heisst PPTP – “Point to Point Tunneling Protocol”. Da Microsoft einer der Initiatoren für die Entwicklung dieses Protokolls ist, unterstützen Windows-Betriebssyteme PPTP “out of the Box”. Eine eher schwache Verschlüsselung ist der große Minuspunkt des inzwischen in der RFC 2637 spezifizierten PPTP. 2012 machte ein Sicherheitsexperte das Angebot, jedes mit PPTP aufgebaute VPN oder WLAN innerhalb eines Tages zu knacken. Die Zeitschrift “CT” machte Tests mit dem vorgestellten Verfahren und hatte mit diesen Tests Erfolg. Fazit: wer tatsächlich Wert auf sichere Verbindungen legt, sollte zu anderen Verfahren greifen.

Deshalb verwende ich in meinem Beispiel auch für Windows OpenVPN, obwohl die Implementierung in dieses OS etwas mehr Aufwand verursacht.

1. Client installieren

Die Community von OpenVPN stellt Clients sowohl für Windows als auch für Linux zur Verfügung. Auf OpenVPN Community kann der Client heruntergeladen werden. Für Windows gibt es den entsprechenden Client in einer 32bit- und einer 64bit-Version. Bitte darauf achten, welche Version des OS aus Redmond ihr verwendet …

Das Installationspaket ist ca. 1,7 MB groß. Nach dem Start der Installation und der obligatorischen Zustimmung zu den Bedingungen erscheint ein Auswahlfenster, in dem die zu installierenden Komponenten “angehakt” werden können. Für die Standardinstallation kann die Auswahl wie vorgegeben übernommen werden (Bild 1).

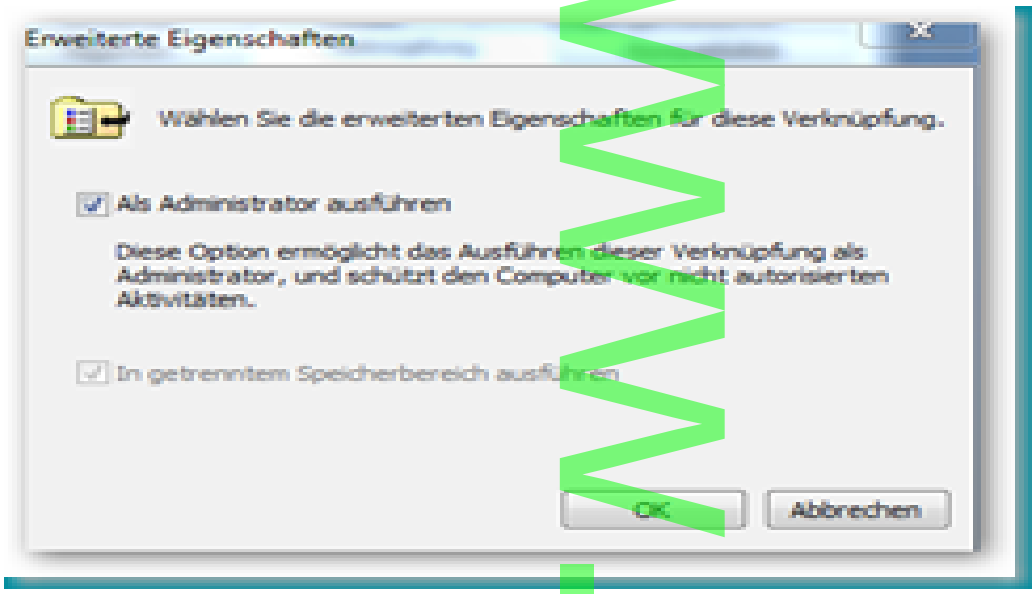


Nach der folgenden Bestätigung des Installationspfades (C:\Programme\OpenVPN) läuft die Installation ohne weiteren Benutzereingriff durch. Nach der Beendigung wird standardmäßig eine readme-Datei angezeigt – jedenfalls, wenn der Haken im Beendigungsfenster von euch nicht entfernt wurde. Lest euch diese Readme durch, e´s werden einige Hinweise für die Konfiguration gegeben, die zumindest zum Teil für den geplanten Zugriff auf ownCloud per openVPN beachtet werden müssen.

2. Konfiguration

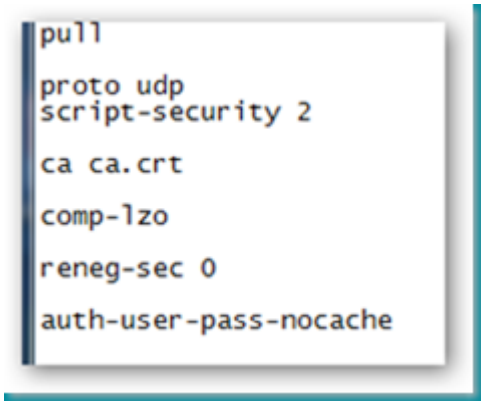
Als erstes müssen wir unsere vom VPN-Server erstellten Dateien Openvpn.vpn und ca.crt in das Konfigurationsverzeichnis unserer Installation (C:\Programme\OpenVPN\config) kopieren. Einen weiteren Hinweis der Readme gilt es noch umzusetzen: unter Vista und Windows 7/8 muss das Programm als Administrator ausgeführt werden., dass gilt nach den unergründlichen Rechtesystem der entsprechenden Windows-Versionen auch, wenn ihr bereits Mitglied der Gruppe Administratoren seid …

Auf das Icon unseres VPN-Clients mit der rechten Maustaste klicken, Eigenschaften, Reiter Verknüpfung, Erweitert und den Haken bei “als Administrator ausführen” setzen (Bild 2), ok und wir können unseren OpenVPN-Client das erste Mal starten …



Nach dem Start des Clients, findet man ein Symbol in Taskleiste, mit der rechten Maustaste auswählen und verbinden. In der Eingabemaske den am VPN-Server definierten Benutzer und Passwort eingeben, ok und die Verbindung wird aufgebaut. Der Aufruf unserer ownCloud-Instanz über die interne IP-Adresse als Test sollte genügen …

Eine Kleinigkeit bleibt noch: in der Konfiguration sollte noch ein kleiner Zusatz erfolgen. Um das Cachen des Benutzernamens und dem entsprechenden Passwortes zu verhindern, sollte der Konfiguration der Zusatz "-nocache" hinzugefügt werden (rechte Maustaste auf das Symbol in der Taskleiste, "Konfiguration anpassen" und den Zusatz in der entsprechenden Zeile hinzufügen – Bild 3).



Konfiguration abgeschlossen!

Im Teil IV werde ich mich mit der Einbindung von Android-Mobilgeräten per OpenVPN beschäftigen.

Teil IV -OpenVPN-Client unter Android einrichten

Server läuft, Linux- und Windows-Desktops sind eingerichtet – was fehlt jetzt noch? Natürlich soll auch per mobilem Gerät zugegriffen werden …

In meiner Umgebung kommen für diesen Zweck ausschließlich Androiden zum Einsatz, aktuell ein Samsung Galaxy Note II (Smartphone) und ein Samsung Galaxy Note 2 (Tablet). Ja ich finde diesen feinen Unterschied bei der Benennung auch sehr interessant , Aus diesem Grund werde ich mich hier auch auf die Einrichtung unter Android beschränken …

Hier gibt es eigentlich nicht viel zu beachten. Zuerst müssen unsere beiden Dateien OpenVPN.vpn und ca.crt auf die SD-Card des entsprechenden Gerätes kopiert werden. Im zweiten Schritt im playstore eine OpenVPN-App herunterladen. Ich verwende die kostenlose App “OpenVPN for Android” von Arne Schwabe. Eine kleine aber feine Anwendung die ihre Aufgabe sehr gut erfüllt und durch Stabilität glänzt. In der App kann ein Profil entweder manuell (sind nur einige wenige Schritte) oder per Import der Konfigurationsdatei OpenVpn.vpn angelegt werden. Verbindung herstellen und fertig! Zugriff auf owncloud ist jetzt einfach über den Browser per

http://interne_IP_DS/owncloud möglich.

Zum Zugriff auf die abgelegten Daten gibt es eine owncloud-App. Synchronisation von Kontakten und Kalendern gibt es verschiedene Synchronisations-Applikationen. Ich selbst verwende CardDAV-Sync und CalDAV-Sync von Marten Gajda – in der Vollversion kostenpflichtig.

Eine Bemerkung noch zum gesamten Thema VPN. Sinn macht die ganze Sache natürlich nur, wenn ihr von unterwegs, aus dem Büro usw. auf euer Heimnetzwerk zugreifen wollt. Durch den Einsatz erreicht ihr eine höhere Sicherheit beim Zugriff auf eure Daten als per reinem HTTP oder auch HTTPS, u.a. (aber nicht nur) weil an eurem Router nur noch ein einziger Port geöffnet sein muss, der den Zugang in das eigene Netz zudem nur verschlüsselt, per Zertifikat gesichert und mit Authentifizierung zulässt.
Nach der Anmeldung befindet ihr euch sozusagen in eurem eigenen Netzwerk zu Hause, als wenn ihr euch z.B. mit eurem mobilen Gerät per WLAN im Heimnetzwerk angemeldet habt …