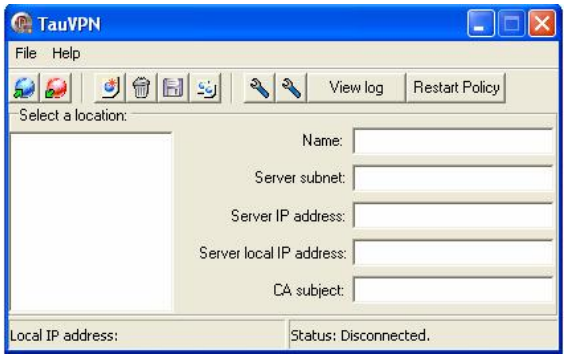
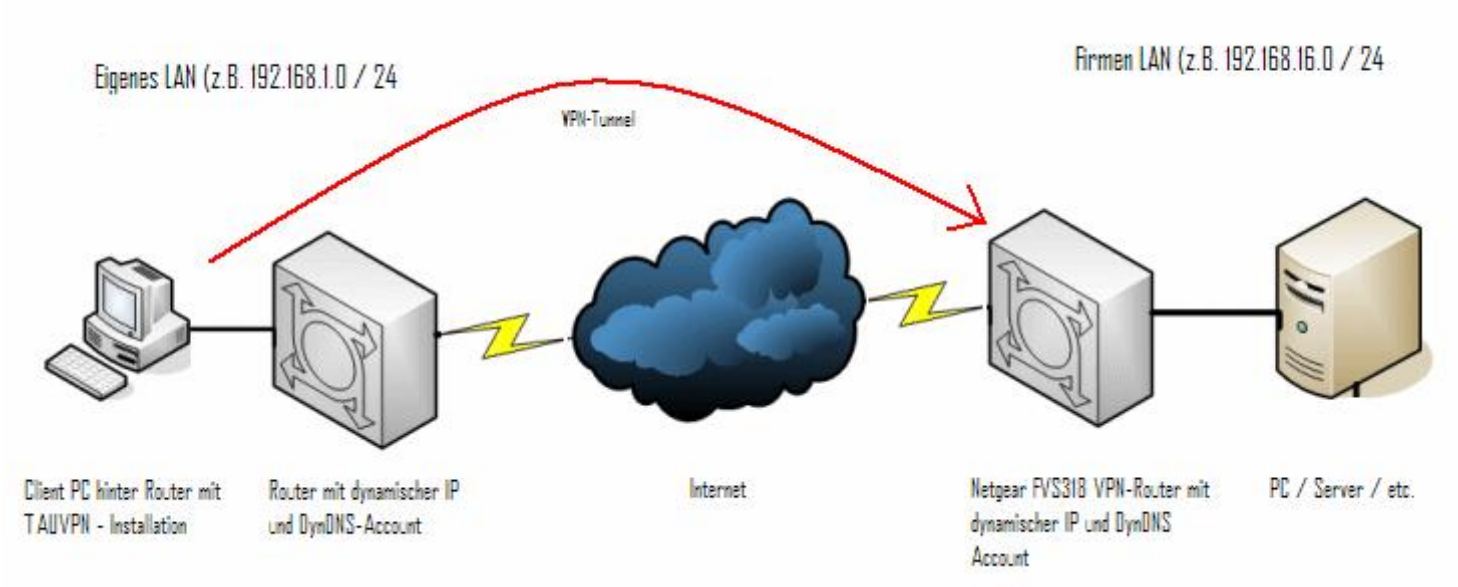
# IPSec-VPN Verbindung zwischen Netgear FVS318 Router und TauVPN Client mittels Preshared Key einrichten

**Netzwerkschema:**




**Das Eigene LAN hat in diesem Beispiel das Subnetz 192.168.1.0 / 24, das FirmenLAN hat das Subnetz 192.168.16.0 / 24!**
**In den gezeigten Dialogfeldern weiter unten ggf. die eigenen Subnetze eintragen!**

# Einstellungen im Netgear FVS318 - Router:

1. Der Netgear-VPN-Router sollte vorab korrekt für den Internetzugang inkl. Dyndns-Account konfiguriert sein.

2. Im Router Web-Interface einloggen und VPN-Settings anklicken.
   Dort eine Verbindung mit folgenden Einstellungen anlegen:

## VPN Settings - Main Mode

| | |
|---|---|
| Connection Name: Beliebiger Name | Verbindungsname beliebig |
| Local IPSec Identifier: 0.0.0.0 | IPSec Identifier beliebig(?) |
| Remote IPSec Identifier: 0.0.0.0 | IPSec Identifier beliebig(?) |
| Tunnel can be accessed from: any local address | Tunnelzugriff vom Remote- |
| Local LAN start IP Address: 0.0.0.0 | Netzwerk aus bei Bedarf |
| Local LAN finish IP Address: 0.0.0.0 | auf eine IP beschränken! |
| Local LAN IP Subnetmask: 0.0.0.0 | |
| Tunnel can access: a subnet of remote address | Tunnelzugriff vom eigenen |
| Remote LAN start IP Address: 192.168.1.0 | Netzwerk aus ggf. |
| Remote LAN finish IP Address: 0.0.0.0 | beschränken! |
| Remote LAN IP Subnetmask: 255.255.255.0 | |
| Remote WAN IP or FQDN: | Hier KANN der Dyndns-Account des eigenen LANs eingetragen werden. |
| Secure Association: Main Mode | Main Mode auswählen |
| Perfect Forward Secrecy: (•) Enabled ( ) Disabled | PFS aktivieren |
| Encryption Protocol: 3DES | 3DES Verschlüsselung |
| PreShared Key: Keyblabla | Beliebigen Key eintragen |
| Key Life: 3600 | Standard belassen |
| Seconds IKE Life Time: 28800 Seconds | Standard belassen |
| [x] NETBIOS Enable | Falls Netbios gewünscht |

## Einstellungen auf der Clientseite:
## (in diesem Fall TauVPN auf Windows XP SP2)

3. Zunächst UNBEDINGT die **Windows XP SP2 – Support Tools** von Microsoft herunterladen und VOLLSTÄNDIG in C:\Programme\Support Tools installieren! Ohne die Support-Tools funktioniert TauVPN nicht!
   http://www.microsoft.com/downloads/details.aspx?displaylang=de&familyid=49ae8576-9bb9-4126-9761-ba8011fabf38

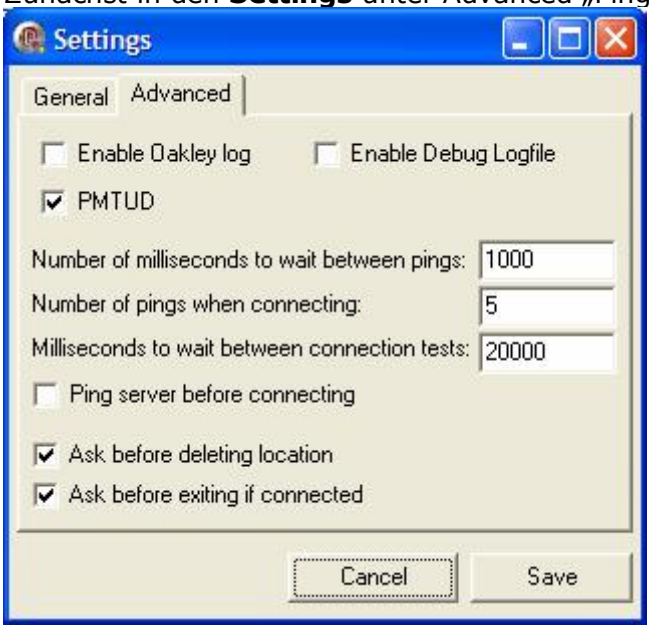
4. **TauVPN** von Sourceforge herunterladen (hier Version 0.43) und installieren und neu starten(!) http://sourceforge.net/project/showfiles.php?group_id=81232

5. Zunächst ggf. **Desktop – Firewall deaktivieren** um Fehlerquelle auszuschließen.

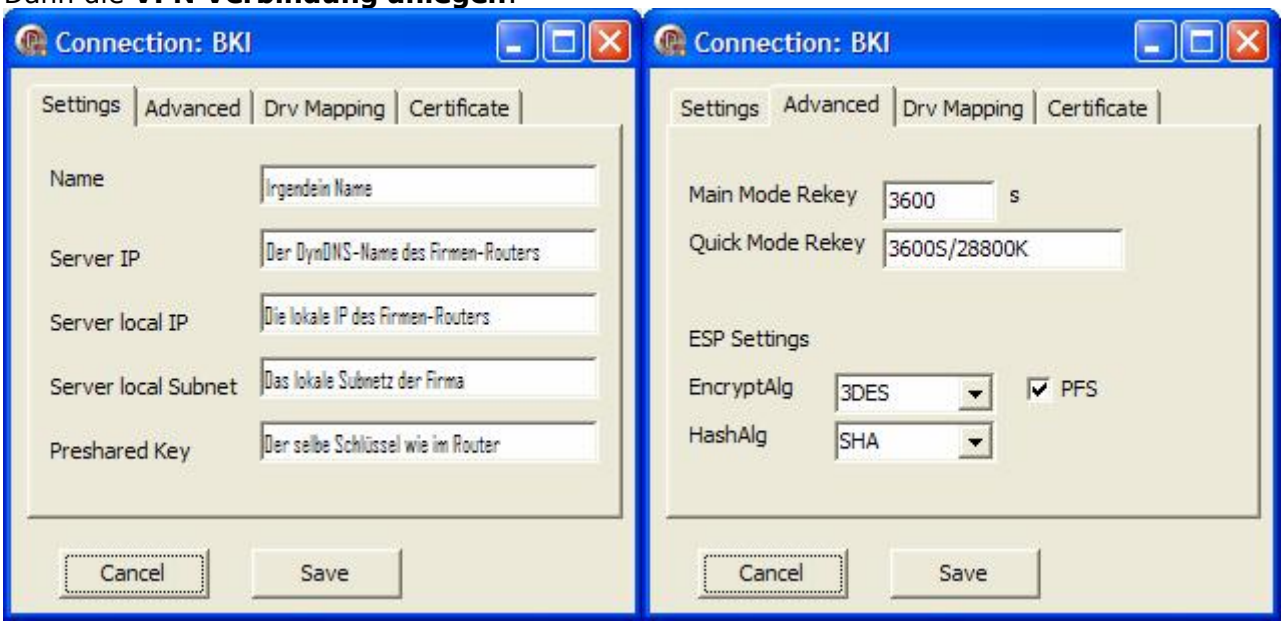
6. Im eigenen Router der Außenstelle / Heimnetzwerk EVENTUELL folgende Ports auf den eigenen Rechner weiterleiten:
   **500 UDP und 4500 UDP** (ging bei mir auch ohne Weiterleitung)

7. **TauVPN** einrichten:

Zunächst in den **Settings** unter Advanced „Ping Server before connecting" deaktivieren.



Dann die **VPN Verbindung anlegen**:




Hinweise:
Die Server IP lautet z.B.: meineFirma.dyndns.org
Die Server local IP lautet z.B.: 192.168.16.1
Das Server local Subnet ist z.B. 192.168.16.0/255.255.255.0

8. Verbindung herstellen, nach einigen Sekunden sollte TauVPN „Connected" melden! Falls dies nicht der Fall ist, obige Einstellungen noch einmal überprüfen und ggf. die genannten Ports UDP 500 und UDP 4500 im eigenen Router auf den eigenen PC weiterleiten. Wurde der Client nach der TauVPN-Installation neu gestartet?

9. Wenn gewünscht, Desktop – Firewall wieder aktivieren und bei der Verbindungsherstellung alle beteiligten Programme erlauben.
   Bei manchen Desktop-Firewalls ist noch eine Regel notwendig, das IP-Protokoll Nr. 50 ausgehend zuzulassen!