

## Securepoint Security Systems

Version 2007nx Release 3



•• **SECUREPOINT**

## Inhalt

1	Einstellungen an der Appliance vornehmen .....	4
1.1	Netzwerkobjekte anlegen.....	4
1.2	Regeln für die OpenVPN-Verbindung anlegen.....	5
1.3	OpenVPN-Zertifikate für die Firewall und den Roadwarrior erstellen.....	6
1.4	Roadwarrior-Zertifikat und Stammzertifikat exportieren.....	8
1.4.1	Private Key aus der zu exportierenden Datei löschen .....	9
1.5	Allgemeine OpenVPN-Einstellungen für die Appliance .....	11
1.6	OpenVPN-Benutzer anlegen.....	12
1.7	Dienststatus prüfen.....	13
2	OpenVPN-Client für Windows .....	14
2.1	Installieren von OpenVPN.....	14
2.2	Einbinden der OpenVPN-GUI (graphical user interface) .....	16
2.3	OpenVPN-Client Konfiguration erstellen .....	17
2.4	Verbindung mit der Firewall herstellen .....	19
2.5	Punkte des Kontextmenüs .....	20

## **VPN mit OpenVPN und Roadwarrior**

Ein VPN verbindet einen oder mehrere Rechner oder Netzwerke miteinander, indem es ein anderes Netzwerk, z. B. das Internet, als Transportweg nutzt. Das kann z. B. der Rechner eines Mitarbeiters zu Hause oder einer Filiale sein, der mit dem Netzwerk der Zentrale über das Internet verbunden ist.

Für den Benutzer sieht das VPN wie eine normale Netzwerkverbindung zum Zielrechner aus. Den tatsächlichen Übertragungsweg sieht er nicht. Das VPN stellt dem Benutzer eine virtuelle IP-Verbindung zur Verfügung, die durch eine tatsächliche getunnelt wird. Die über diese Verbindung übertragenen Datenpakete werden am Client verschlüsselt und vom Secu-repoint Server wieder entschlüsselt und umgekehrt.

# 1 Einstellungen an der Appliance vornehmen

## 1.1 Netzwerkbjekte anlegen

Für OpenVPN-Benutzer muss ein Netzwerkbjekt angelegt werden.

- Soweit noch nicht vorhanden, erstellen Sie Netzwerkbjekte für das *externe Interface*, das *interne Netzwerk* und für die *OpenVPN-Benutzer*.



Abb. 1 externes Interface anlegen



Abb. 2 Gruppensymbol auswählen



Abb. 3 internes Netzwerk anlegen



Abb. 4 Gruppensymbol auswählen



Abb. 5 OpenVPN Roadwarrior anlegen



Abb. 6 Gruppensymbol auswählen

So sollte das Ergebnis aussehen:

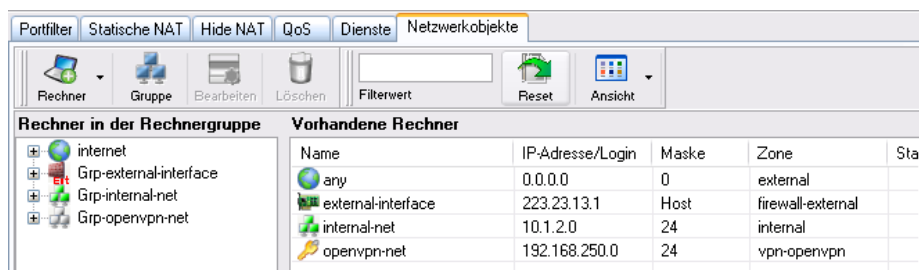


Abb. 7 angelegte Netzwerkobjekte

## 1.2 Regeln für die OpenVPN-Verbindung anlegen

Sie benötigen nun zwei Regeln. Die erste erlaubt den externen Rechnern, eine OpenVPN Verbindung zu dem externen Interface der Appliance aufzubauen.

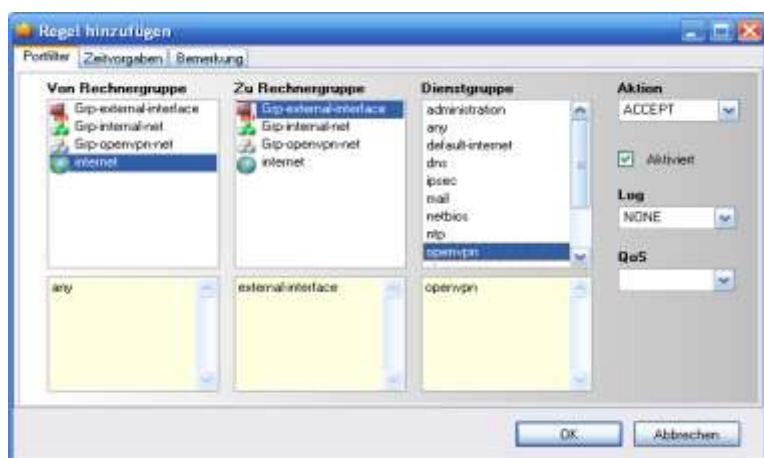


Abb. 8 Regel any → Grp-external-interface → openvpn

Die zweite Regel ermöglicht dem OpenVPN-Benutzer den vollen Zugriff auf das interne Netzwerk.



Abb. 9 Regel Grp-openvpn-net → Grp-internal-net → any

### 1.3 OpenVPN-Zertifikate für die Firewall und den Roadwarrior erstellen

Mit VPN Verbindungen über OpenVPN können Sie Roadwarrior mit der Securepoint Appliance verbinden. OpenVPN benutzt zur Verschlüsselung das Secure Sockets Layer Protokoll (SSL).

Um eine Verbindung anzulegen, müssen Sie zunächst ein OpenVPN Serverzertifikat und für jeden Roadwarrior ein OpenVPN Clientzertifikat erzeugen.

**Hinweis:** Sie benötigen ein Stammzertifikat (CA), um die Zertifikate signieren zu können. Erstellen Sie ggf. zuerst eine CA, indem Sie im Dialog *Zertifikate* den Punkt *Stammzertifikat* auswählen.

- Wählen Sie in der VPN Ansicht die Registerkarte *Zertifikate*.
- Wählen Sie die Firewall aus und klicken Sie auf das Icon *Neu*.

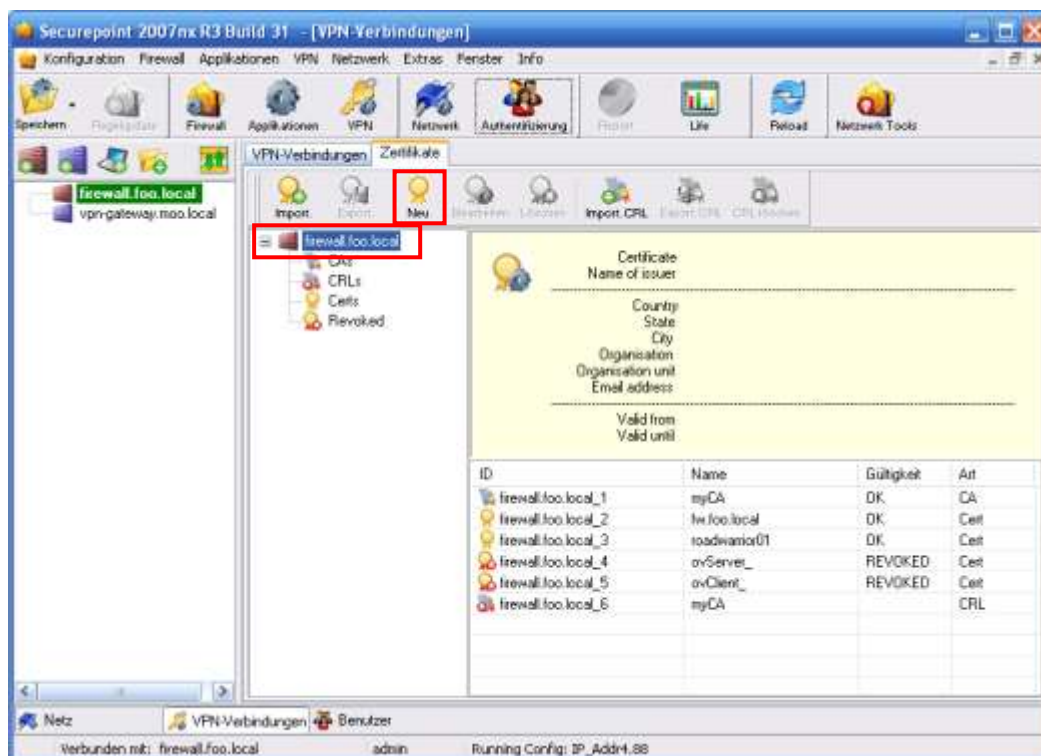
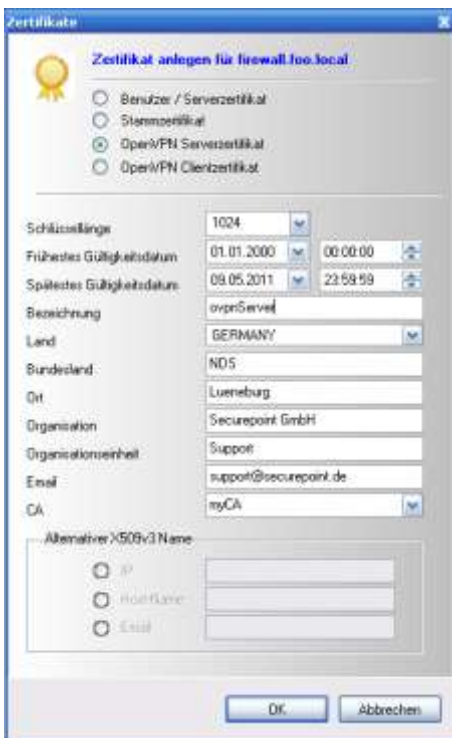


Abb. 10 VPN - Registerkarte Zertifikate

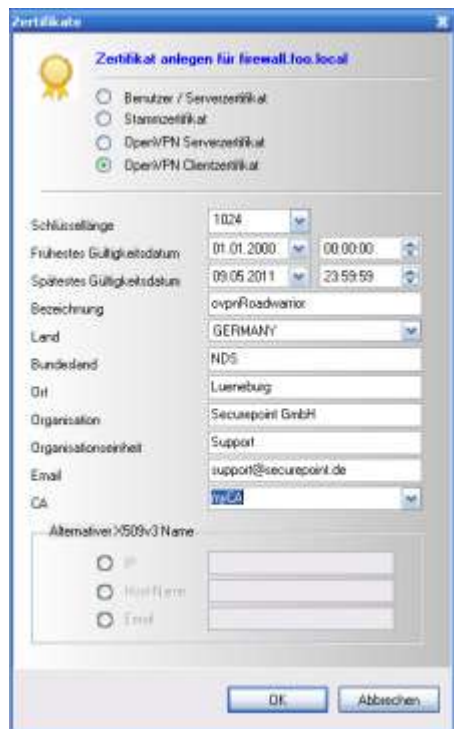
Es öffnet sich der Dialog *Zertifikate*.

- Wählen Sie die Option *OpenVPN-Serverzertifikat*.
- Füllen Sie die Felder mit den entsprechenden Daten.
- Bestätigen Sie Ihre Eingabe mit *OK*.
- Erstellen Sie anschließend ein *Roadwarrior-Zertifikat*. Wählen Sie hierfür die Option *OpenVPN-Clientzertifikat*.



The screenshot shows the 'Zertifikate' dialog box titled 'Zertifikat anlegen für firewall.foo.local'. The 'OpenVPN Serverzertifikat' option is selected. The fields are filled with: Schlüsselgröße: 1024; Frühestes Gültigkeitsdatum: 01.01.2000 00:00:00; Spätestes Gültigkeitsdatum: 09.05.2011 23:59:59; Bezeichnung: ovpnServer; Land: GERMANY; Bundesland: NDS; Ort: Lueneburg; Organisation: Securepoint GmbH; Organisationseinheit: Support; Email: support@securepoint.de; CA: myCA. The 'Alternativer X509v3 Name' section has 'IP' selected.

Abb. 11 OpenVPN - Serverzertifikat erstellen



The screenshot shows the 'Zertifikate' dialog box titled 'Zertifikat anlegen für firewall.foo.local'. The 'OpenVPN Clientzertifikat' option is selected. The fields are filled with: Schlüsselgröße: 1024; Frühestes Gültigkeitsdatum: 01.01.2000 00:00:00; Spätestes Gültigkeitsdatum: 09.05.2011 23:59:59; Bezeichnung: ovpnRoadwarrior; Land: GERMANY; Bundesland: NDS; Ort: Lueneburg; Organisation: Securepoint GmbH; Organisationseinheit: Support; Email: support@securepoint.de; CA: myCA. The 'Alternativer X509v3 Name' section has 'Host Name' selected.

Abb. 12 OpenVPN - Clientzertifikat erstellen

- Beenden Sie die Zertifikaterstellung, indem Sie die Schaltfläche *Abbrechen* betätigen.

## 1.4 Roadwarrior-Zertifikat und Stammzertifikat exportieren

- Exportieren Sie das Roadwarrior-Zertifikat und das Stammzertifikat und geben Sie beide an den Roadwarrior weiter. Gewöhnlich wird das Standard Format (PEM-Datei) gewählt. Wenn Sie das pkcs#12 Format wählen, brauchen Sie nur das Roadwarrior-Zertifikat zu exportieren, weil in diesem Format das Stammzertifikat mit enthalten ist. Außerdem ist der Private Key des Stammzertifikats in diesem Format verschlüsselt und muss nicht vor der Weitergabe entfernt werden (siehe 1.4.1).



Abb. 13 Roadwarrior-Zertifikat exportieren

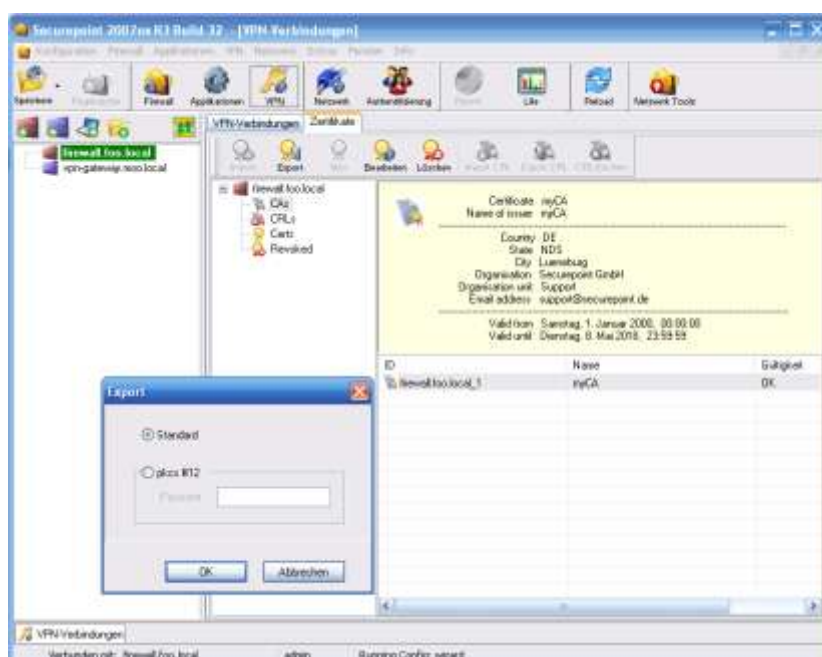


Abb. 14 Stammzertifikat exportieren

**Beachten Sie:** Wenn Sie das Stammzertifikat im Standardformat exportieren, wird auch der Private Key des Stammzertifikats mit in der PEM-Datei gespeichert. Den Private Key der CA sollten Sie nie an Clients weitergeben, um Missbrauch vorzubeugen. Löschen Sie daher den Private Key aus der zu exportierenden Datei.

### 1.4.1 Private Key aus der zu exportierenden Datei löschen

Wenn Sie den Private Key nicht aus der PEM-Datei löschen und so an den Client weitergeben, kann der Client neue Zertifikate erstellen und diese mit der CA signieren. Sie könnten die so erstellten Zertifikate nicht von originalen von Ihnen erstellten Zertifikaten unterscheiden.

- Suchen Sie die exportierte Datei heraus und klicken Sie mit der rechten Maustaste auf die Datei. Es öffnet sich ein Kontextmenü.

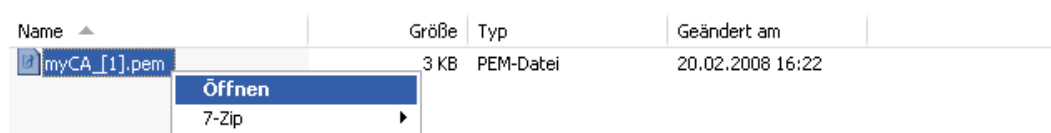


Abb. 15 exportiertes Stammzertifikat öffnen

- Klicken Sie auf *Öffnen*.
- Geben Sie im nächsten Dialog an *Programm aus der Liste wählen* und bestätigen mit *OK*.
- Wählen Sie aus der Liste einen Editor z.B. den Microsoft Editor.
- Entfernen Sie ggf. den Haken bei *Dateityp immer mit dem ausgewählten Programm öffnen*.
- Bestätigen Sie mit *OK*.

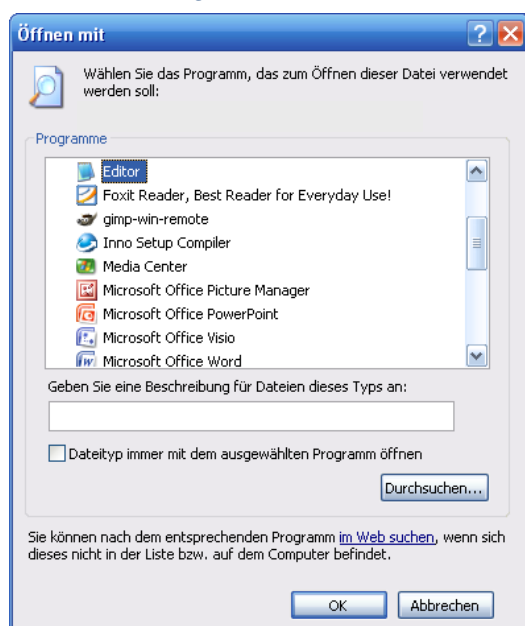


Abb. 16 Programm zum Öffnen wählen



## 1.5 Allgemeine OpenVPN-Einstellungen für die Appliance

Nun müssen Sie die Einstellungen für die Appliance vornehmen.

- Wählen Sie über das Menü *VPN* und hier den Unterpunkt *VPN OpenVPN*.



Abb. 19 Menüpunkt VPN - VPN OpenVPN

Es öffnet sich der Dialog *OpenVPN*.

- Im Standardfall können Sie die Einstellungen über *Port* und *Protokoll* beibehalten.
- Wählen Sie als *Serverzertifikat* das eben erstellte Zertifikat *ovpnServer*.
- Wenn Sie OpenVPN im Multipathbetrieb betreiben, müssen Sie den Dienst an ein externes Interface binden, um einen korrekten Betrieb zu gewährleisten.
- Bestätigen Sie Ihre Angaben mit *OK*.

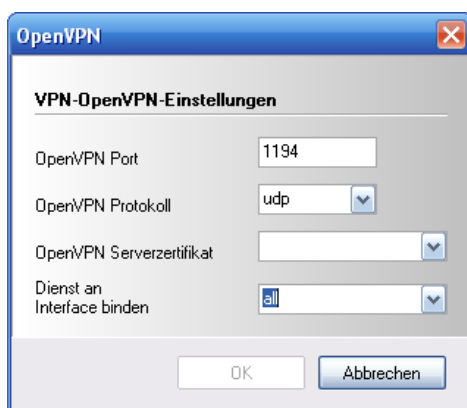


Abb. 20 Dialog OpenVPN

## 1.6 OpenVPN-Benutzer anlegen

Sie müssen noch einen OpenVPN-Benutzer auf der Appliance anlegen.

- Geben Sie als Gruppenmitgliedschaft *VPN-OpenVPN-Benutzer* an.

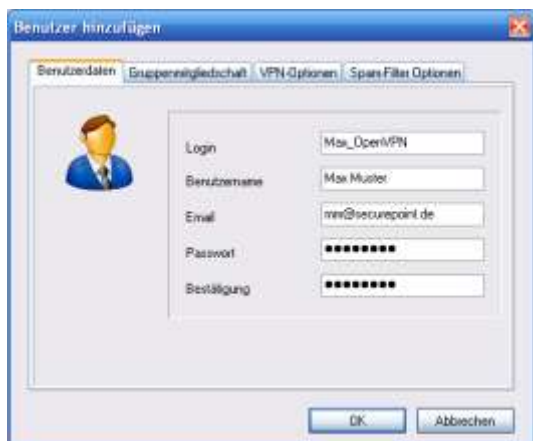


Abb. 21 Benutzerdaten eingeben



Abb. 22 Gruppenmitgliedschaft festlegen

Auf der Registerkarte VPN-Optionen können Sie dem Benutzer eine feste IP-Adresse im lokalen Netzwerk zuweisen.

**Beachten Sie:** Für das vorinstallierte tun-Interface ist der IP-Adresspool 192.168.250.1/24 eingestellt. Der letzte Teil der IP-Adresse (192.168.250.xxx) muss folgendes Kriterium erfüllen: Die Zahl ist ein Vielfaches von 4 minus 2. Entspricht der Rechenvorschrift:  $(y * 4) - 2 = x$   
 z.B.  $(5 * 4) - 2 = 18$   
 Folgende Werte sind also möglich: {2, 6, 10, 14, ... 246, 250, 254}



Abb. 23 feste IP-Adresse zuweisen

## 1.7 Dienststatus prüfen

- Speichern Sie Ihre Konfiguration und führen Sie dann ein Regelupdate aus.



Abb. 24 Konfiguration speichern und Regelupdate durchführen

Damit sich OpenVPN Roadwarrior mit der Firewall verbinden können, muss der Dienst `SERVICE_OPENVPN` aktiviert sein.

- Klicken Sie auf das Icon *Applikation* und wechseln Sie in die Registerkarte *Dienste Status* oder wählen Sie aus der Menüleiste den Punkt *Applikationen* und dort den Punkt *Dienste Status*.
- Wenn der Dienst `SERVICE_OPENVPN` nicht aktiviert ist, klicken Sie doppelt auf das rote X in der Status Spalte. Klicken Sie dann auf *Einstellungen übernehmen*.

Dienstname	Status	Cluster
SERVICE_OPENSSH	✓	✗
SERVICE_SENDMAIL	✓	✗
SERVICE_DNS	✓	✗
SERVICE_POP3_PROXY	✗	✗
SERVICE_HTTP_PROXY	✓	✗
SERVICE_VOIP_PROXY	✗	
SERVICE_VNC_PROXY	✗	
SERVICE_DYNDNS	✗	
SERVICE_NTP	✓	✗
SERVICE_IDS	✓	✗
SERVICE_L2TP	✗	
SERVICE_PPTP	✗	
SERVICE_SPUVA	✓	✗
SERVICE_WEBSEVER	✗	
SERVICE_DHCPD	✗	
SERVICE_IPSEC	✓	✗
SERVICE_OPENVPN	✓	✗

Abb. 25 Dienste Status

Nun können sich OpenVPN-Benutzer zu Ihrer Appliance verbinden.

## 2 OpenVPN-Client für Windows

Um sich von einem externen Rechner mit der Firewall über OpenVPN zu verbinden, müssen Sie OpenVPN auf Ihr System installieren.

Auf der Internetadresse <http://openvpn.net/download.html#stable> können Sie die aktuelle Version von OpenVPN herunterladen. In dem Paket ist auch ein virtuelles Interface enthalten, was zum Aufbau von OpenVPN-Verbindungen benötigt wird.

Von Mathias Sundman ist ein Windows Client für OpenVPN entwickelt worden, der unter der Adresse <http://openvpn.se/download.html> heruntergeladen werden kann. Auf der Seite finden Sie auch eine deutsche Übersetzung des Clienten.

### 2.1 Installieren von OpenVPN

- Laden Sie sich den Windows Installer von der OpenVPN Internetseite herunter und führen die Installationsroutine mit einem Doppelklick auf die heruntergeladene Datei aus.



Abb. 26 Startdialog des OpenVPN Installers

- Folgen Sie den Anweisungen der Installationsroutine.
- Bestätigen Sie die Frage, ob der *TAP-Win32 Adapter V8* installiert werden soll, obwohl er den Windows-Logo-Test nicht bestanden hat, mit einem Klick auf den Button *Installation fortsetzen*.



Abb. 27 Installieren des virtuellen Interfaces bestätigen

- Beenden Sie die Installation mit einem Klick auf *Finish*.



Abb. 28 Installation beenden

Unter Ihren Netzwerkverbindungen sollte jetzt ein Eintrag für den TAP-Win32Adapter V8 zu finden sein.

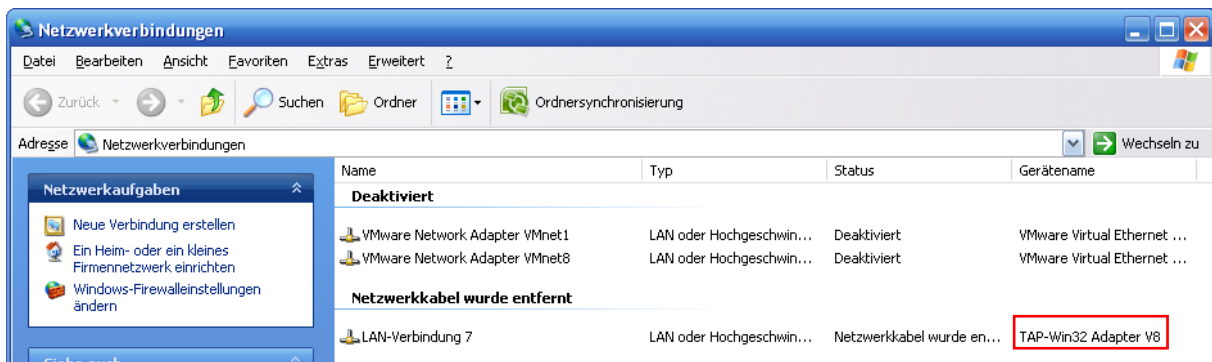


Abb. 29 Liste der Netzwerkverbindungen

## 2.2 Einbinden der OpenVPN-GUI (graphical user interface)

- Kopieren Sie die Datei *openvpn-gui-versionsnummer-de.exe* in das *bin* Verzeichnis des OpenVPN Programms (z.B. *C:\Programme\OpenVPN\bin*).
- Anschließend können Sie noch eine Verknüpfung der GUI auf dem Desktop bzw. im Startmenü erstellen.
- Starten Sie die OpenVPN GUI über das Startmenü oder eine Verknüpfung auf dem Desktop oder über die Kopie im *bin* Verzeichnis von OpenVPN.

In der Windows System Tray Leiste wird ein neues Icon angezeigt.



Abb. 30 Icon im System Tray

Das zweite Icon zeigt, dass das virtuelle Interface nicht aktiv ist. Diese Icon wird nur angezeigt, wenn dies in den Optionen des Interfaces angegeben ist.

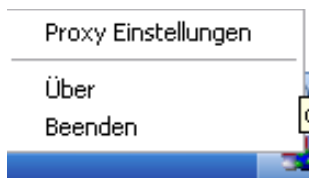


Abb. 31 Icon PopUp-Menü

Mit einem Rechtsklick auf das Icon wird ein Menü angezeigt, über das bislang nur Proxy-Einstellungen vorgenommen werden können.

Es fehlt eine Konfiguration über die dann eine Verbindung zur Firewall hergestellt werden kann.

## 2.3 OpenVPN-Client Konfiguration erstellen

- Öffnen Sie einen Editor zum Beispiel *Notepad* und fügen Sie folgenden Text ein.

```
#####
#   Client Konfiguration
#####
# OpenVPN Standard Client Konfiguration
# Kommentare werden mit vorangestellter
# Raute(#) oder Semikolon(;) gekennzeichnet.

client

dev tun

# Diese Direktiven werden normalerweise nicht benötigt.
;tun-mtu 1500
;fragment 1300
;mssfix

proto udp

float

# Verbindungsdaten des Servers
# Geben Sie nach „remote“ die IP-Adresse
# des Servers ein sowie den Port (default: 1194)
# z.B.: remote 192.168.4.253 1194
remote IP_des_Servers 1194

nobind

persist-key
persist-tun

# Pfad zum Stammzertifikat und zum Client-Zertifikat
# z.B.:
#   ca C:/Programme/OpenVPN/config/keys/myCA.pem
#   cert C:/Programme/OpenVPN/config/keys/roadwarrior01.pem
#   key C:/Programme/OpenVPN/config/keys/roadwarrior01.pem
# Beachten Sie: Sind im Pfad Leerzeichen enthalten, muss
# der Pfad in Anführungszeichen („Pfad zum Zertifikat“) angegeben werden.
ca Pfad/zum/Zertifikat/der/CA.pem
cert Pfad/zum/Zertifikat/des/Clients.pem
key Pfad/zum/Zertifikat/des/Clients.pem

# Pfad zu den Zertifikaten im pkcs#12 Format
# Wenn Sie die Zertifiakte als pkcs#12 Datei benutzen,
# dann kommentieren Sie die 3 Zeilen ca, cert und key aus
# und benutzen stattdessen die folgende (ohne Semikolon).
# z.B.:
#   pkcs12 C:/Programme/OpenVPN/config/keys/roadwarrior01.p12
# Es gilt wieder: Bei Leerzeichen im Pfad, muss der Pfad in Anführungszeichen
# („Pfad zur pkcs#12 Datei.p12“) angegeben werden.
;pkcs12 Pfad/zur/pkcs#12/Datei.p12

# Mit dieser Option akzeptiert der Client nur Zertifikate vom Server,
# die mit dem Zusatz „server“ versehen sind. Dies erschwert einen
# „Man-in-the-middle“ Angriff.
ns-cert-type server

comp-lzo

verb 3

mute 20
```

```
auth-nocache
auth-user-pass

# Wenn Sie einen Proxy benutzen, kommentieren Sie die
# folgenden Zeilen aus und geben Sie die Server IP und Port ein.
# Oder Sie nutzen die Einstellungen der OpenVPN-GUI.
#http-proxy server_IP port
#http-proxy-retry
```

- Speichern Sie diese Datei in den *config* Ordner von OpenVPN. Die Datei muss die Endung *ovpn* haben.

Bsp: C:\Programme\OpenVPN\config\client.ovpn

- Legen Sie in dem *config* Ordner einen weiteren Ordner *keys* an, soweit dieser noch nicht existiert und kopieren Sie in diesen Ordner die Zertifikate des Zertifizierungsstelle und des Clients oder die pkcs#12 Datei.

Dies ist der Standardordner für die Zertifikate, diesen Pfad müssen Sie in der Konfigurationsdatei angeben. Sie können natürlich auch einen anderen Speicherort wählen, sie müssen dann die Konfigurationsdatei entsprechend anpassen.

Außerdem müssen Sie die Zeile *remote IP\_des\_Servers 1194* anpassen. Geben Sie hier zwischen *remote* und der Portangabe die IP des Servers ein, mit dem Sie sich verbinden wollen. z.B. *remote 192.168.175.1 1194*

## 2.4 Verbindung mit der Firewall herstellen

Wenn Sie jetzt mit einem Rechtsklick auf das Icon im System Tray klicken, wurde das Menü erweitert.

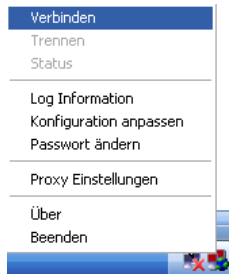


Abb. 32 vollständiges Icon PopUp-Menü

- Drücken Sie die Schaltfläche *Verbinden*.

Es öffnen sich das Logging-Fenster sowie die Login-Maske.



Abb. 33 Logging Fenster und Login-Dialog

- Tragen Sie in der Login-Maske den *Benutzernamen* und das *Kennwort* des OpenVPN-Benutzers ein.
- Wenn Sie Zertifikate im pkcs#12 Format benutzen, werden Sie auch zur Eingabe des Kennwortes der Datei aufgefordert.

Eine erfolgreiche Anmeldung am System wird Ihnen mit folgender Meldung bestätigt.

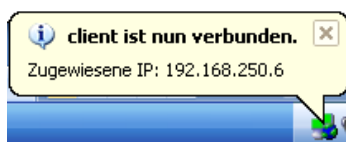


Abb. 34 Verbindung wird bestätigt

Solange das Icon zwei grüne Monitore anzeigt, ist die Verbindung aktiv.  
Zeigt das Icon zwei gelbe Monitore, wird die Verbindung aufgebaut.  
Zwei rote Monitore stellen dar, dass keine Verbindung besteht.

Beim Überfahren des Icons mit der Maus gibt ein PopUp Fenster nochmal die Verbindungsdaten an.

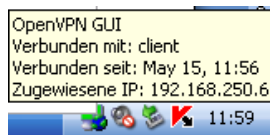


Abb. 35 PopUp Tooltip

## 2.5 Punkte des Kontextmenüs

Menüpunkt	Beschreibung
Verbinden	Startet den Verbindungsaufbau.
Trennen	Beendet die Verbindung.
Status	Zeigt die Logging Meldungen der aktuellen Verbindung.
Log Information	Zeigt das gesamte Logging Protokoll der letzten Verbindung bzw. der aktuellen Verbindung, wenn eine Verbindung aktiv ist.
Konfiguration anpassen	Öffnet die Konfigurationsdatei in einem Editor, in dem Optionen direkt angepasst werden können. Änderungen werden erst bei einem neuen Verbindungsaufbau übernommen.
Passwort ändern	Verschlüsselt den Privaten Schlüssel im Zertifikat. <b>Achtung:</b> Unterstützt nicht das PEM-Format. Die Verschlüsselung löscht das Zertifikat aus der pem-Datei.
Proxy Einstellungen	Hier können Einstellungen für eine Verbindung über einen Proxy vorgenommen werden. Einstellungen müssen so nicht in der Konfigurationsdatei geschrieben werden.
Über	Info-Fenster
Beenden	Beendet die OpenVPN Applikation.

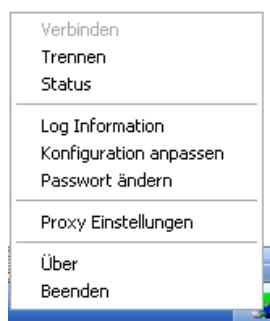


Abb. 36 Kontextmenü