

1) Mit Hilfe des Assistenten VPN in der Digitalisierungsbox eine Client-Verbindung erstellen:

Ausgewähltes Szenario: Einwahl eines einzelnen Clients

The screenshot shows two panels of a configuration assistant. The left panel, titled 'Verbindungsdetails', contains the following fields:

- Beschreibung: IPsecTest
- Lokale IPsec ID: IPsecLokal
- Entfernte IPsec ID: IPsecEntfernt
- Preshared Key: [Redacted]

The right panel, titled 'Entferntes Netzwerk', shows a table of local networks:

IP-Adresse	Netzmaske
192.168.0.254	255.255.255.0
192.168.3.5	255.255.255.0
192.168.1.5	255.255.255.0
0.0.0.0	255.255.255.255
192.168.2.5	255.255.255.0

Below the table, there are two dropdown menus:

- IP-Adresspool auswählen: DHCP Adressbereich intern
- IP-Adresspool für Einwahl-Clients: 192.168.1.100-192.168.1.199

2) Shrewsoft VPN Access Manager starten und neue Verbindung anlegen.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'General' tab selected. The 'Remote Host' section contains:

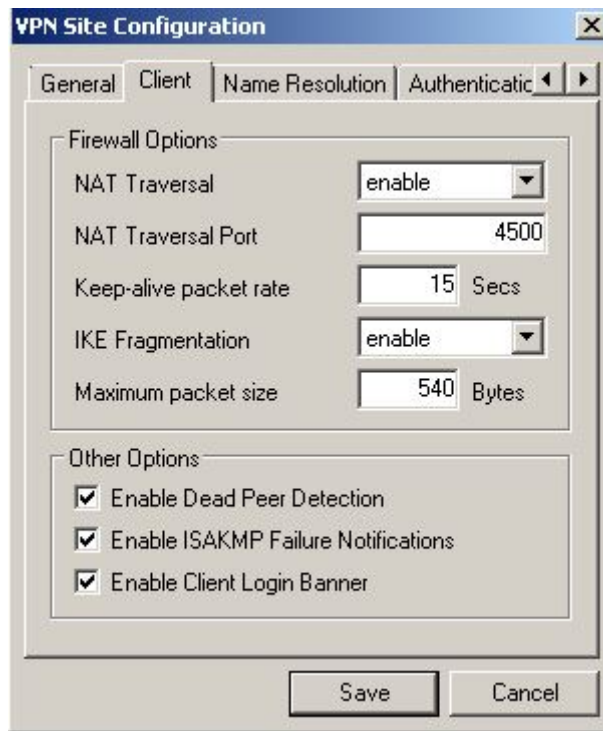
- Host Name or IP Address: öffentliche IPv4/Name der Digibox
- Port: 500
- Auto Configuration: ike config pull

The 'Local Host' section contains:

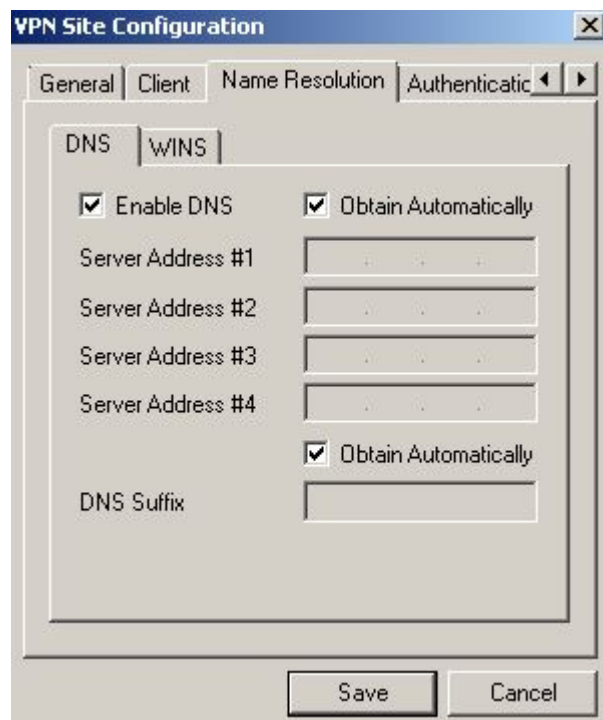
- Adapter Mode: Use a virtual adapter and assigned address
- MTU: 1380
- Obtain Automatically:
- Address: [Empty field]
- Netmask: [Empty field]

Buttons for 'Save' and 'Cancel' are at the bottom.

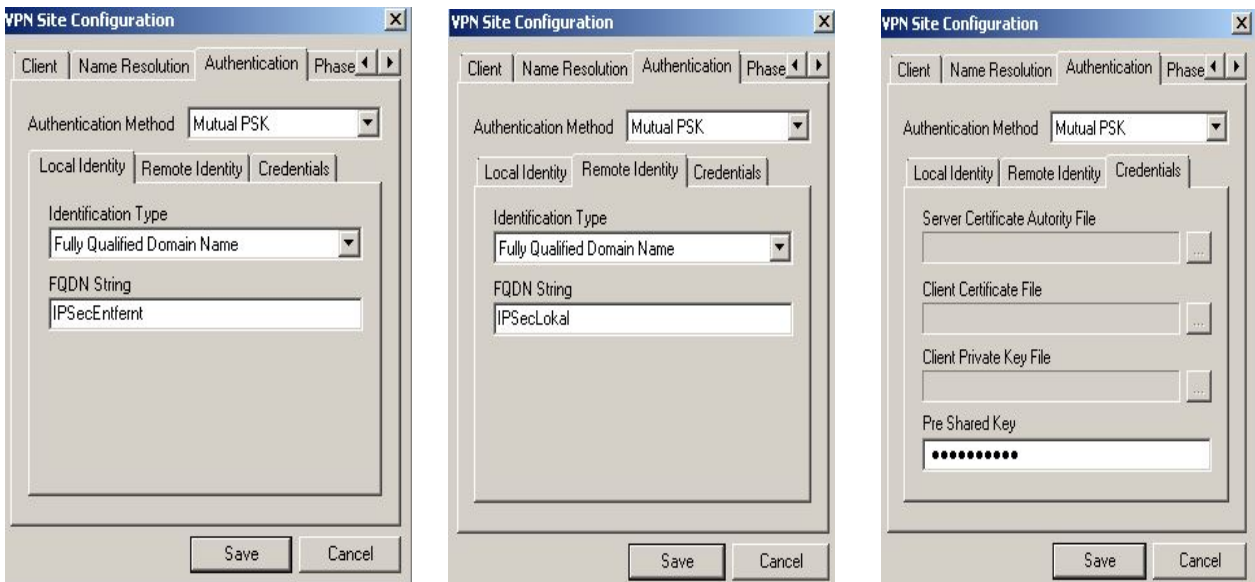
Im Reiter **General** reicht es das Feld **Host Name or IP Address** auszufüllen.



Im Reiter **Client** werden die Default-Einstellungen benutzt.



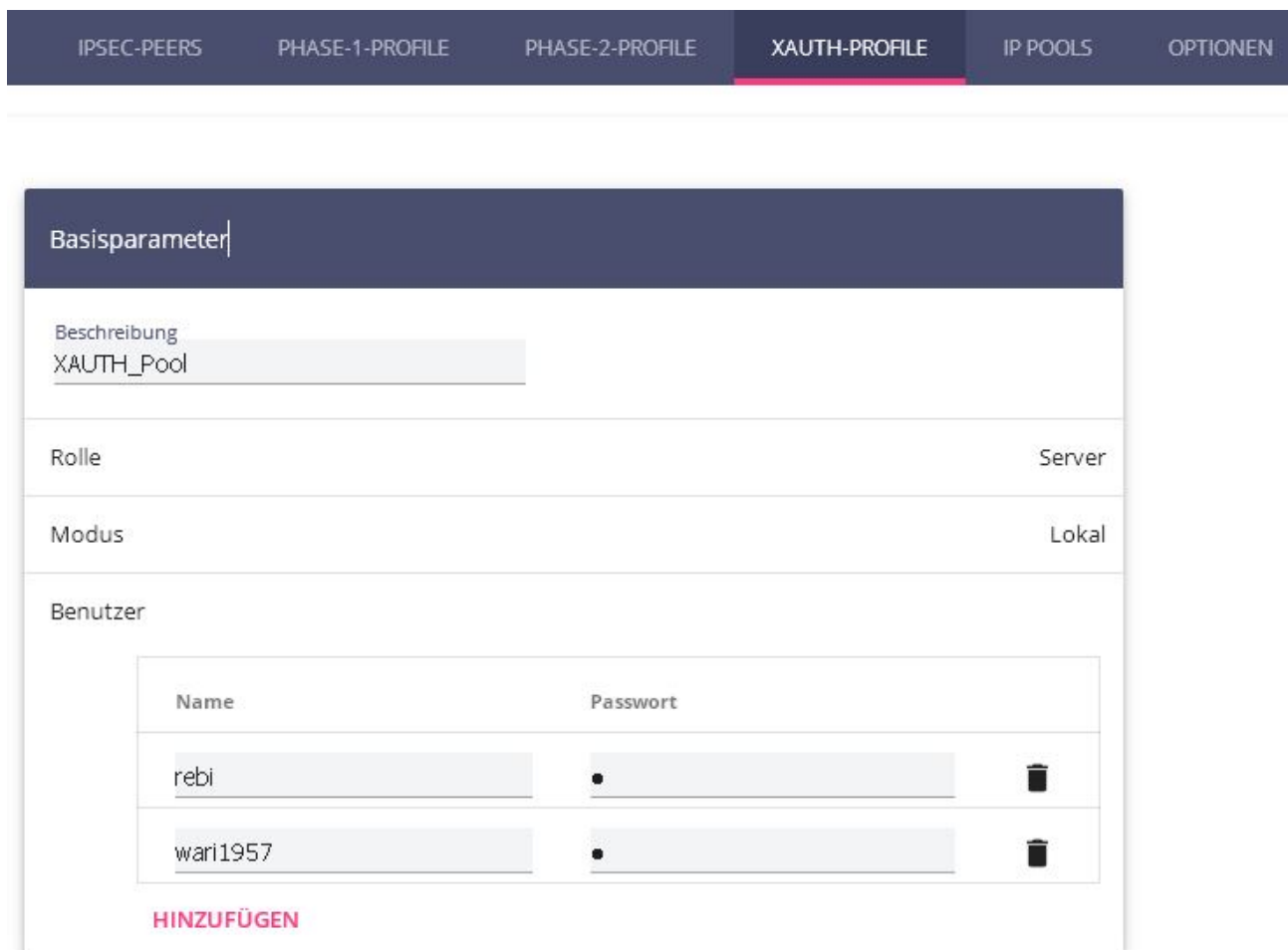
Im Reiter **Name Resolution** werden die Default-Einstellungen benutzt.



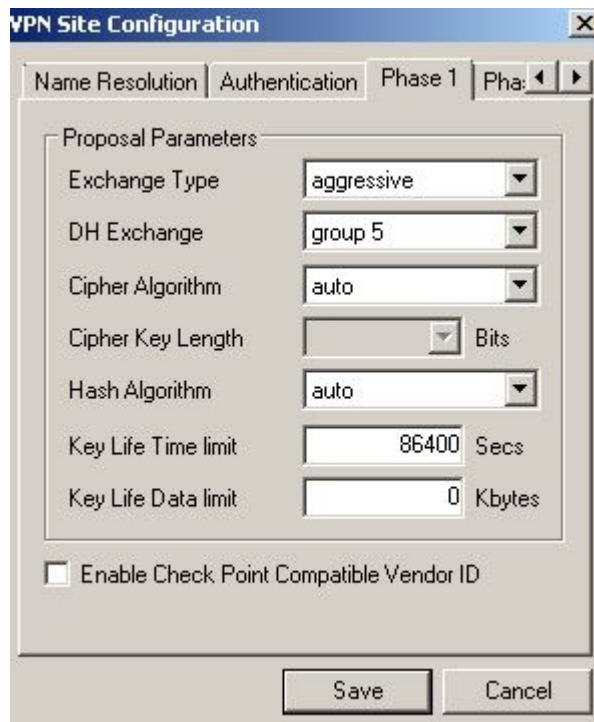
Im Reiter **Authentication** werden die in der Digitalisierungsbox angegebenen Identitäten und der Pre Shared Key eingetragen.
 Als **Authentication Method** Mutual PSK auswählen.

Wenn eine Anmeldung mit Benutzername und Passwort gefordert ist, dann als **Authentication Method** Mutual PSK + XAuth auswählen.

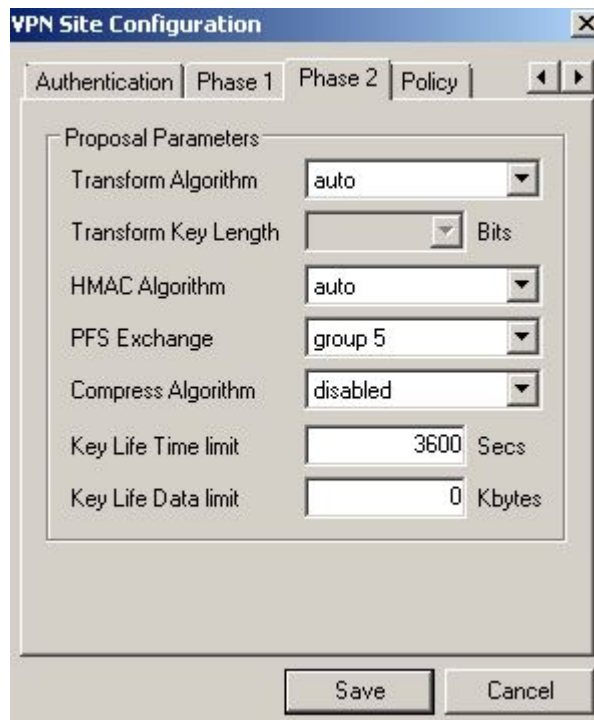
In der Digitalisierungsbox muß dann ein XAuth-Pool unter VPN->IPSec->XAUTH-PROFILE angelegt werden wie z.B.



Danach unter VPN->IPSec->IPSEC-PEERS-> IPsecTest bearbeiten, Erweiterte Einstellungen unter XAUTH-Profil, das angelegt auswählen und mit OK speichern.



Beim Reiter **Phase 1** im Eingabefeld DH Exchange group 5 auswählen.



Beim Reiter **Phase 2** im Eingabefeld PFS Exchange group 5 auswählen.

Das wars dann auch schon.

Mit Save das Ganze speichern und von einem **anderen** Internetanschluß aus testen.

