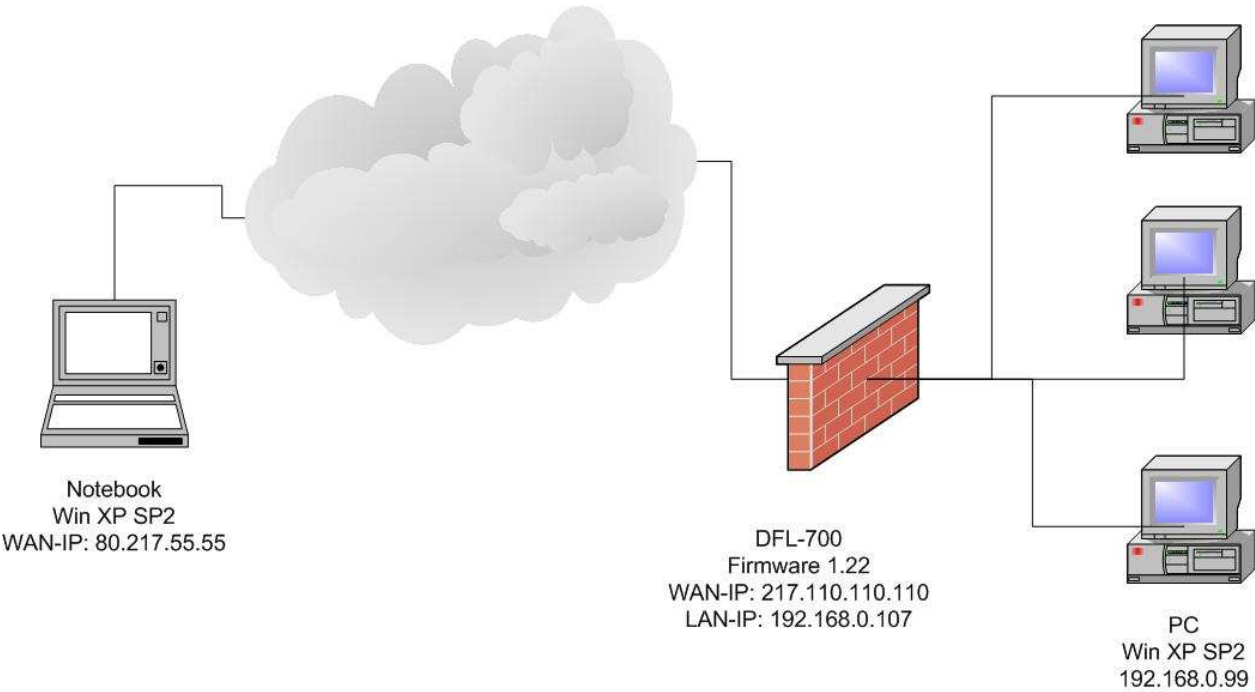


VPN-Einwahl des  
D-Link VPN Client  
über die DFL-700

VPN Umgebung:



## Konfiguration der DFL-700

1. Bevor Sie mit der Konfiguration der DFL-700 beginnen, richten Sie die DFL-700 zuvor komplett ein.

2. Klicken Sie auf „Firewall / VPN“ und „Add new“. Füllen Sie die Felder wie angezeigt aus. Unter „Local Net“ tragen Sie das Subnet der gewünschten DFL-700-Schnittstelle ein. Wählen Sie „PSK – Pre-Shared Key“ aus und tragen Sie das Kennwort für den VPN-Sitzungsaufbau ein.

The screenshot shows the configuration interface for a VPN tunnel. At the top, there is a navigation bar with tabs for System, Firewall, Servers, Tools, Status, and Help. The 'Firewall' tab is selected. Below the navigation bar, the page title is 'VPN Tunnels'. The main content area is titled 'Edit VPN tunnel DLink-Test:'. There are two input fields: 'Name:' with the value 'DLink-Test' and 'Local Net:' with the value '192.168.0.0/24'. Below these fields, there is a section for 'Authentication:'. There are two radio button options: 'PSK - Pre-Shared Key' (which is selected) and 'Certificate-based'. Under 'PSK - Pre-Shared Key', there are two input fields for 'PSK:' and 'Retype PSK:', both containing masked characters. Under 'Certificate-based', there is a dropdown menu for 'Local Identity:' with the value 'Admin - CN=000F3D10D929'. Below this is a large empty box for 'Certificates:'. Below the 'Certificates:' box, there is a note: 'Use ctrl/shift click to select multiple certificates. To use ID lists below, you must select a CA certificate.' At the bottom, there is a dropdown menu for 'Identity List:' with the value '(no list)'.

3. Wählen Sie „Roaming Users“ und „IKE XAuth“ aus.  
Klicken Sie danach auf „Advanced“.

Tunnel type:

**Roaming Users** - single-host VPN clients

IKE XAuth:  Require user authentication via IKE XAuth to open tunnel.

**LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Proxy ARP:  Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client:  Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

**Delete this VPN tunnel**

     
**Advanced   Apply   Cancel   Help**

4. Füllen Sie die Felder (wie in der Abbildung beschrieben) aus.

Sollten Sie an diesen Einstellungen Änderungen vornehmen, so müssen diese auch im D-Link VPN Client abgeändert werden.

The image shows a web-based configuration interface for a D-Link device. At the top, there is a navigation bar with tabs for 'System', 'Firewall', 'Servers', 'Tools', 'Status', and 'Help'. The 'Firewall' tab is currently selected. Below the navigation bar, the page title is 'VPN Tunnels'. The main content area is titled 'Edit advanced settings of VPN tunnel DLink-Test:'. The settings are as follows:

- Limit MTU:
- IKE Mode:  Main mode IKE  
 Aggressive mode IKE
- IKE DH Group:
- PFS:  Enable Perfect Forward Secrecy
- PFS DH Group:
- NAT Traversal:  Disabled  
 On if supported and needed (NAT detected between gateways)  
 On if supported
- Keepalives:  No keepalives.  
 Automatic keepalives (works with other DFL-200/700/1100 units)  
 Manually configured keepalives:
  - Source IP:
  - Destination IP:

### IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	AES-256 Allowed:256-256	SHA-1	0	28800
#2:	AES-128 Allowed:128-256	MD5	0	28800
#3:	3DES	SHA-1	0	28800
#4:	3DES	MD5	0	28800
#5:	DES	SHA-1	0	28800
#6:	DES	MD5	0	28800
#7:	-	MD5	0	0
#8:	-	MD5	0	0

### IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	AES-256 Allowed:256-256	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600
#3:	3DES	SHA-1	0	3600
#4:	3DES	MD5	0	3600
#5:	DES	SHA-1	0	3600
#6:	DES	MD5	0	3600
#7:	-	MD5	0	0
#8:	-	MD5	0	0



Apply



Cancel



Help

Klicken Sie auf „Apply“.

5. Danach sollten Sie diese Anzeige erhalten.

The screenshot shows the 'Firewall' tab in a configuration interface. The 'VPN Tunnels' section is active, displaying a table with one entry: 'DLink-Test' with local network '192.168.0.0/24', remote network 'Any', and remote gateway '(No gateway)'. There are links for '[Add new]' and '[Edit]'. A red plus icon and 'Help' text are also visible.

Name	Local Net	Remote Net	Remote Gateway
DLink-Test	192.168.0.0/24	Any	(No gateway)

6. Wählen Sie „Firewall/Users“ aus und legen Sie einen lokalen User an.

The screenshot shows the 'User Management' section in the 'Firewall' tab. It includes a form to 'Add new user' with fields for 'User name' (testuser), 'Group membership' (test), 'Password', and 'Retype password'. Below the form are 'Apply', 'Cancel', and 'Help' buttons. A list of users is shown, including 'Administrative users' (admin, Read-only) and 'Users in local database' (testuser).

User name:

Group membership:

Password:

Retype password:

Apply Cancel Help

User name	Groups
admin	
Read-only	
testuser	testuser

7. Um einen „Ping“ auszuführen oder die Konfiguration auf der DFL-700 über VPN ändern zu dürfen, müssen Sie weiterhin unter „System/Administration“ die Freigabe über den VPN Tunnel einrichten.

Administrative access via **DLink-Test** vpn tunnel [\[Edit\]](#)

<b>Ping:</b>	Any address
<b>Admin:</b>	Any address (HTTP + HTTPS)

Speichern Sie die Einstellungen über den Punkt „Activate“.

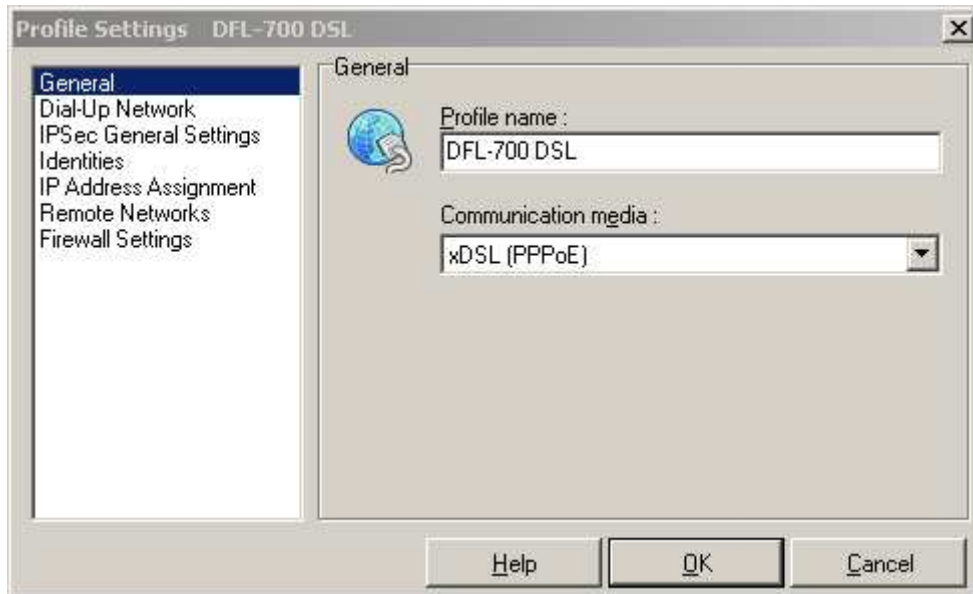


## Konfiguration des D-Link VPN Client

1. Starten Sie den D-Link VPN Client und wählen Sie „Configuration / Profile Settings“. Wählen Sie den Eintrag DFL-700 und den Menüpunkt „Duplicate“.

Danach erhalten Sie folgende Anzeige:

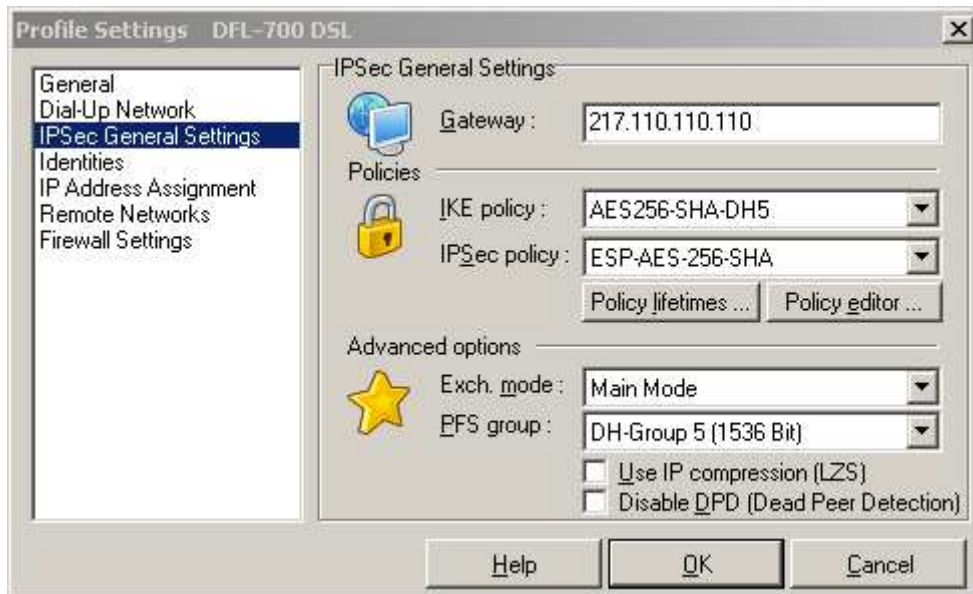
Tragen Sie den Profilnamen ein und wählen Sie die Übertragungsart aus.



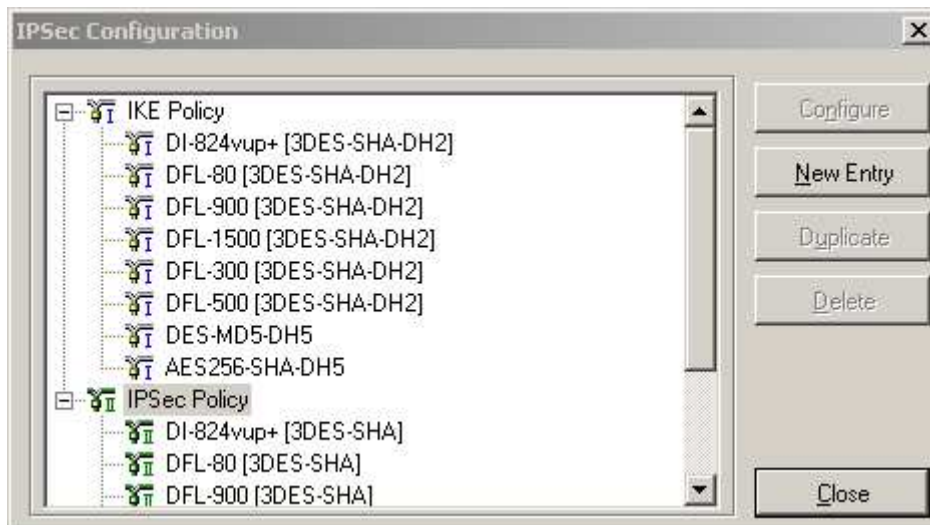
2. Klicken Sie auf „Dial-Up Network“ und tragen Sie Ihre Zugangsdaten zum Provider ein.

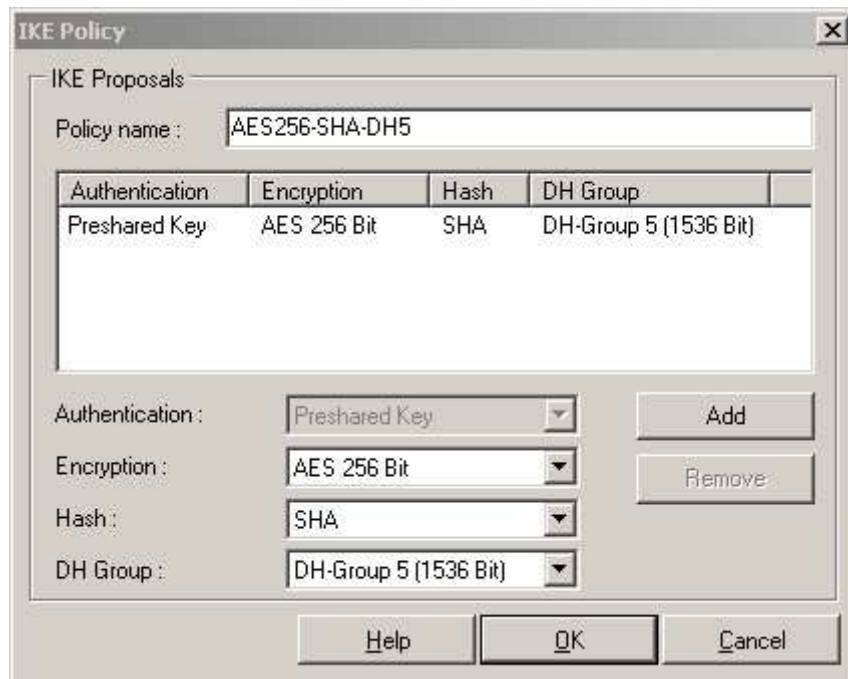


3. Tragen Sie unter „Gateway“ die IP-Adresse des DFL-700 WAN-Interfaces ein.  
Durch Auswahl von „Policy editor“ können Sie die Verschlüsselungstiefe einstellen.



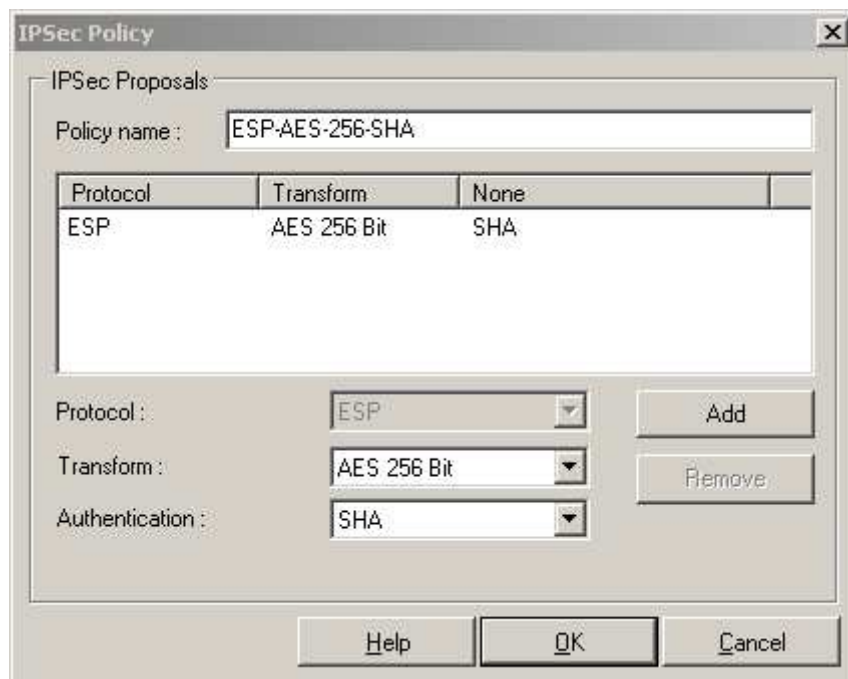
4. Klicken Sie unter „IKE Policy“ auf „New Entry“ und wählen Sie die Verschlüsselungstiefe für IKE aus.



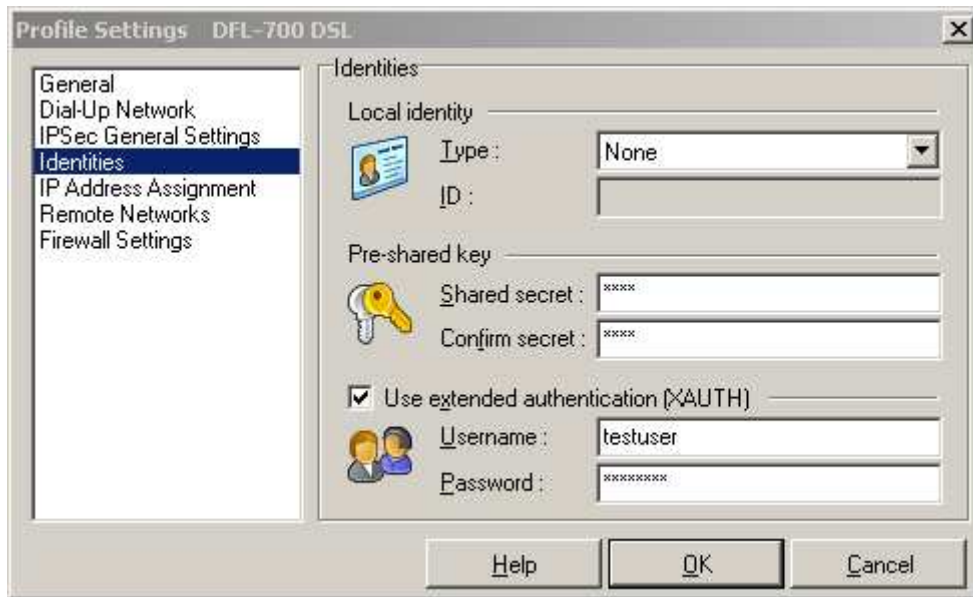


Bestätigen Sie durch „OK“

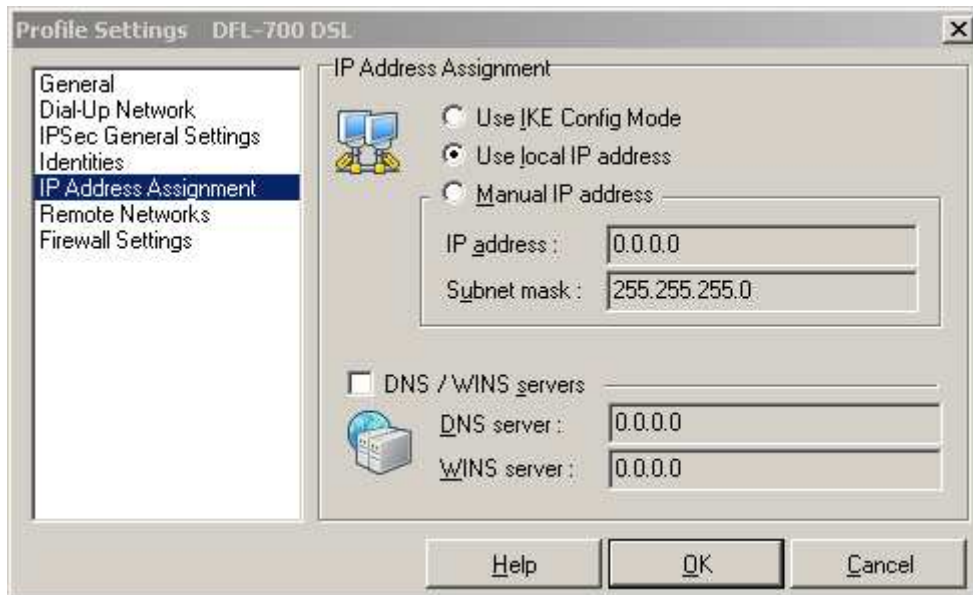
5. Klicken Sie unter „IPSec Policy“ auf „New Entry“ und wählen Sie die Verschlüsselungstiefe für IPSec aus.



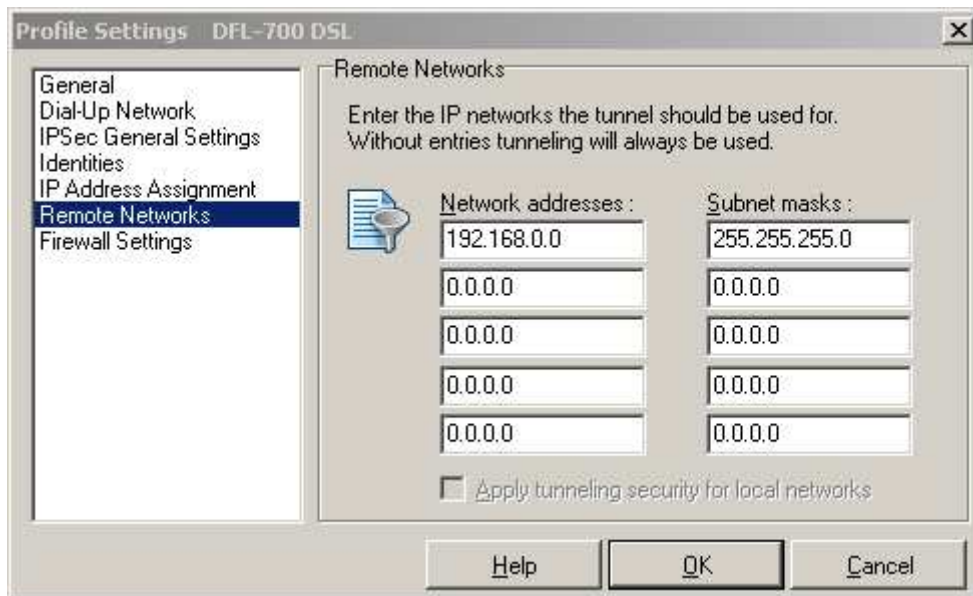
6. Tragen Sie unter dem Menüpunkt „Identities“ den „Pre-shared key“ und den in der DFL-700 zuvor angelegten User inkl. Passwort ein.



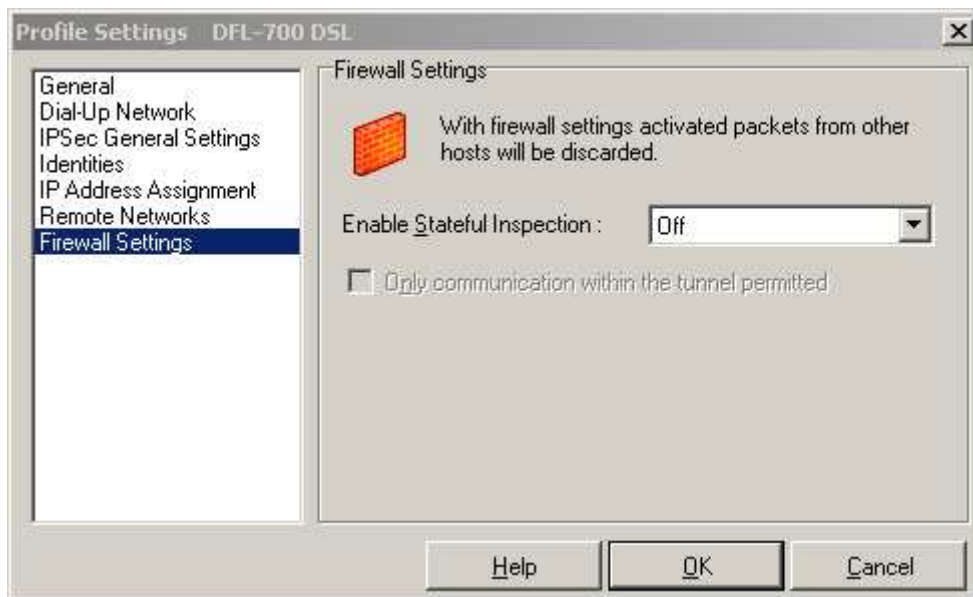
7. Tragen Sie unter „IP Address Assignment“ folgende Einstellungen ein.



8. Tragen Sie unter „Remote Networks“ das Subnetz des LAN ein.



9. In diesem Beispiel ist die integrierte Firewall ausgeschaltet, diese sollten Sie nach erfolgreichem Test bei Bedarf aktivieren.



10. Nach „Bestätigung“ mit „OK“ wählen Sie im Hauptmenü das eben angelegte Profil aus.



11. Durch klicken auf den „Connect“ Knopf sollte der Verbindungsaufbau ohne weitere Probleme stattfinden.

