

Verbindungsaufbau von

**Windows XP**

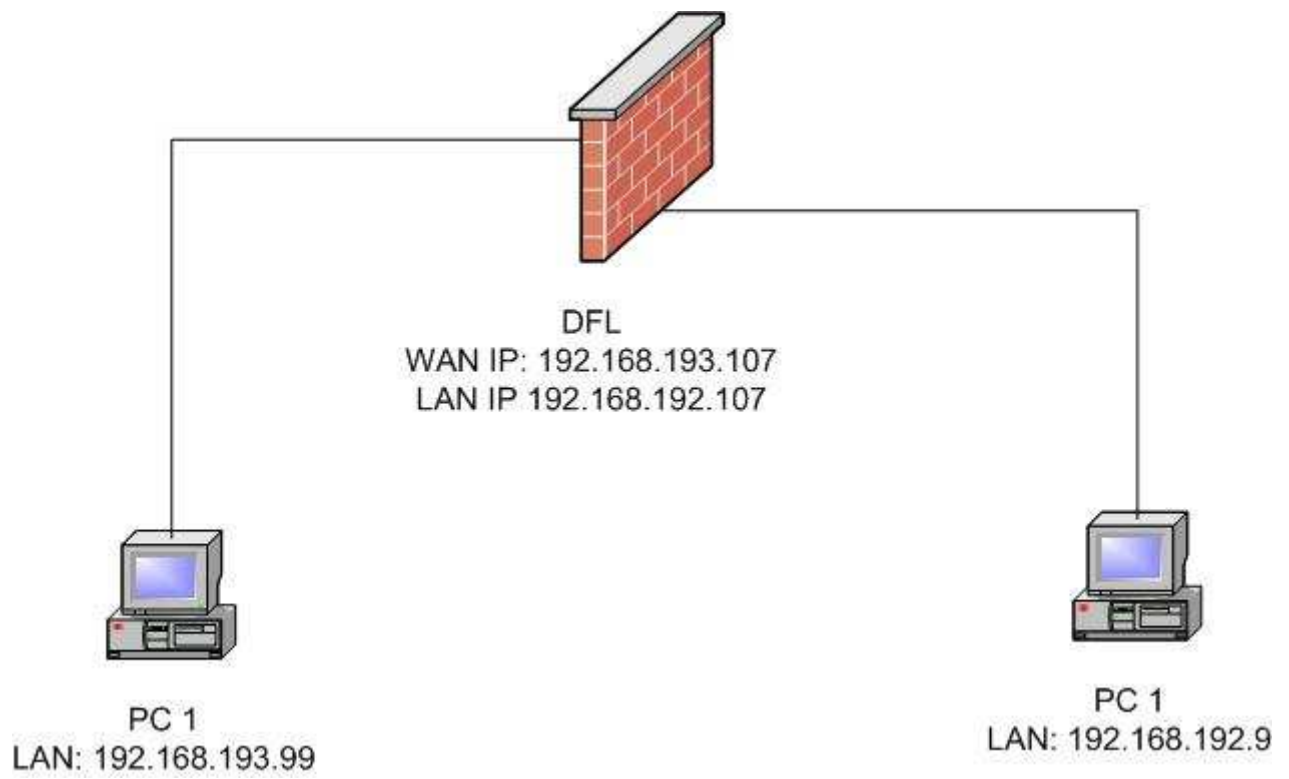
zur

DFL-200, DFL-700 und DFL-1100

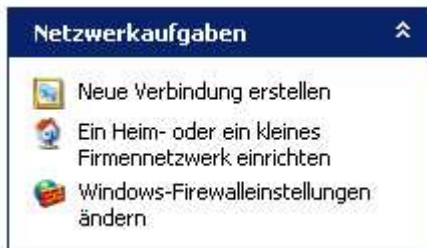
über

**L2TP/IPSEC**

Testumgebung:



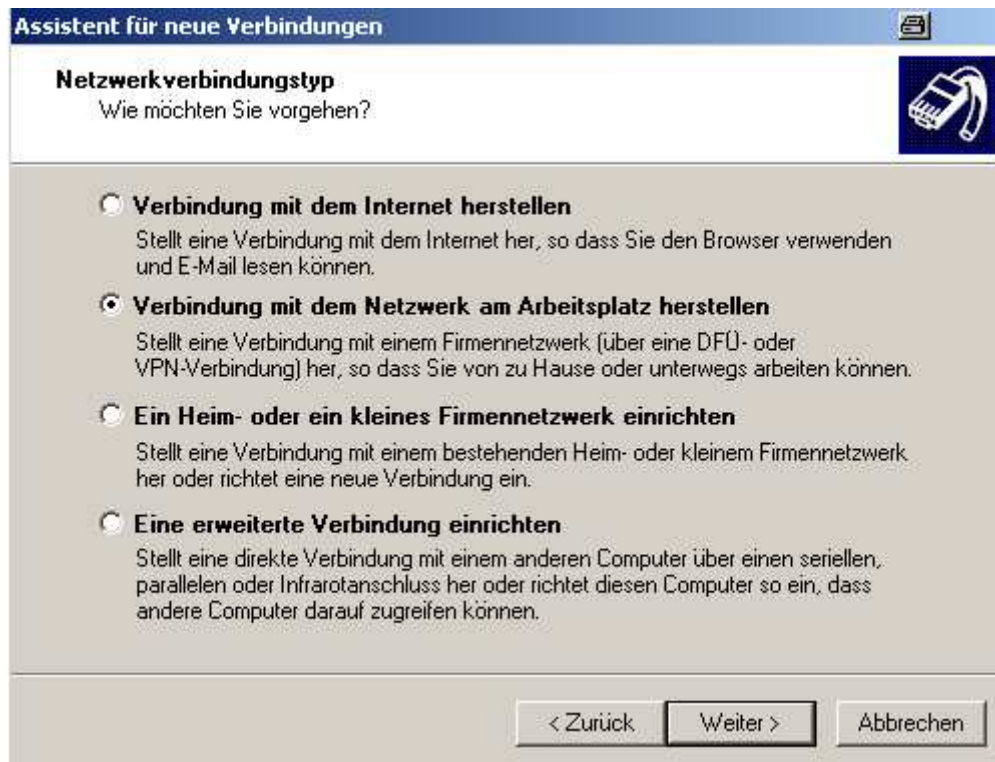
Klicken Sie in der Netzwerkkumgebung auf „Neue Verbindung erstellen“



Klicken Sie auf „Weiter“



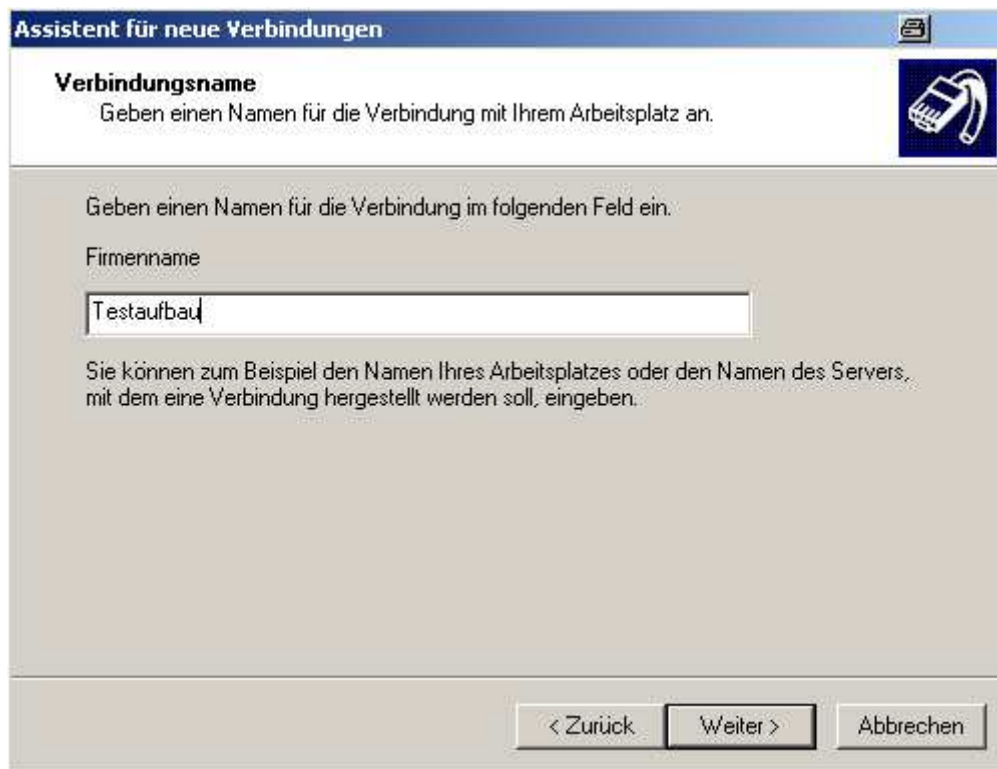
Klicken Sie auf „Verbindung mit dem Netzwerk am Arbeitsplatz herstellen“. Danach auf „Weiter“.



Klicken Sie auf „VPN-Verbindung“. Danach auf „Weiter“



Tragen Sie hier einen Namen ein und klicken auf „Weiter“.



**Assistent für neue Verbindungen**

**Verbindungsname**  
Geben einen Namen für die Verbindung mit Ihrem Arbeitsplatz an.

Geben einen Namen für die Verbindung im folgenden Feld ein.

Firmenname

Testaufbau

Sie können zum Beispiel den Namen Ihres Arbeitsplatzes oder den Namen des Servers, mit dem eine Verbindung hergestellt werden soll, eingeben.

< Zurück   Weiter >   Abbrechen

In diesem Test wird eine direkte Anbindung gezeigt, somit wird keine DFÜ-Verbindung benötigt. Sollten Sie vorher eine DFÜ-Verbindung aufbauen müssen, so können Sie diese unter „Automatisch diese Anfangsverbindung wählen:“ auswählen.



**Assistent für neue Verbindungen**

**Öffentliches Netzwerk**  
Windows kann gewährleisten, dass die Verbindung mit dem öffentlichen Netzwerk zuerst hergestellt wird.

Windows kann eine Anfangsverbindung mit dem Internet oder einem anderen öffentlichen Netzwerk automatisch wählen, bevor die virtuelle Verbindung hergestellt wird.

Keine Anfangsverbindung automatisch wählen

Automatisch diese Anfangsverbindung wählen:

< Zurück   Weiter >   Abbrechen

Geben Sie hier die IP Adresse des L2TP/IPSEC Servers ein.  
In diesem Fall: 192.168.193.107.



**Assistent für neue Verbindungen**

**VPN-Serverauswahl**  
Wie lautet der Name bzw. die Adresse des VPN-Servers?

Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, zu dem eine Verbindung hergestellt werden soll.

Hostname oder IP-Adresse (z.B. microsoft.com oder 157.54.0.1):

192.168.193.107

< Zurück    Weiter >    Abbrechen

Hier kann der Benutzername eingegeben werden. Vorher sollten Sie jedoch die Konfiguration über „Eigenschaften“ abändern.



**Verbindung mit "Testaufbau" herstellen**

Benutzername:

Kennwort:

Benutzernamen und Kennwort speichern für:

- Nur für eigene Verwendung
- Alle Benutzer dieses Computers

Verbinden    Abbrechen    Eigenschaften    Hilfe

Klicken Sie auf „Sicherheit“ und danach auf „IPSec-Einstellungen“



Hier tragen Sie Ihren PSK-Key ein. In diesem Fall „1234567890“



Unter „Netzwerk“ und „VPN-Typ“ wählen Sie bitte „L2TP-IPSec-VPN“ aus.



Geben Sie bitte hier den Benutzernamen und das Kennwort ein. In diesem Beispiel ist dies Benutzer „HomeUser“ und das Kennwort „1234567890“. Dieses wird im weiteren Verlauf auf der DFL konfiguriert.





Starten Sie die Firewall und führen Sie die Grundkonfiguration durch.  
(Wizard, LAN und WAN Interface etc).

Danach klicken Sie auf „Firewall/VPN“ und „Add new L2TP Server“

- Tragen Sie einen Namen ein
  - Unter Client IP Pool tragen Sie die Range ein, aus der die IP Adresse vom L2TP-IPSEC Server die IP-Adressen vergibt.
  - Aktivieren Sie „Proxy ARP dynamically added routes“
  - Aktivieren Sie „Use unit’s own DNS relay addresses“
  - Aktivieren Sie unter „Authentication protocol“ „MSCHAPv2“
  - MPPE encryption stellen Sie bitte auf „None“
  - Unter „Enquire IPsec encryption“ tragen Sie bitte den PSK ein  
In diesem Fall „1234567890“.
- Aktivieren Sie die Einstellungen mit „Apply“

### L2TP/PPTP Servers

Edit L2TP tunnel L2TPserver:

Name:

Outer IP:  Blank = WAN IP  
Must be WAN IP if IPsec encryption is required

Inner IP:  Blank = LAN IP

### IP Pool and settings:

Client IP Pool:

Proxy ARP dynamically added routes

Primary DNS:  (Optional)

Secondary DNS:  (Optional)

Use unit's own DNS relay addresses

Primary WINS:  (Optional)

Secondary WINS:  (Optional)

**Authentication protocol:**

- No authentication
  - PAP
  - CHAP
  - MSCHAP (MPPE encryption possible)
  - MSCHAPv2 (MPPE encryption possible)
- 

**MPPE encryption:**

- None - unencrypted
- 40 bit
- 56 bit
- 128 bit (best security)

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol.

**Require IPsec encryption**

**PSK - Pre-Shared Key**

Key:

Retype key:

**Certificate based**

Local Identity:

Certificates:

Use ctrl/shift click to select multiple certificates.  
To use ID lists below, you must select a CA certificate.

Identity List:

---

**Delete this VPN tunnel**

    
**Apply** **Cancel** **Help**

In der Übersicht sollte nun folgendes angezeigt werden.

L2TP / PPTP Server					
Name	Type	Outer IP	Inner IP	IPsec	
L2TPserver	L2TP	WAN IP	LAN IP	PSK	<a href="#">[Edit]</a>
<a href="#">[Add new PPTP server]</a>					
<a href="#">[Add new L2TP server]</a>					

Legen Sie einen neuen User unter „Firewall / Users / Users in local database / add new“ an. In diesem Beispiel ist dies „HomeUser“ mit dem Passwort „1234567890“

### User Management

Add new user:

User name:

Group membership:

Password:

Retype password:

### L2TP/PPTP settings:

Static client IP:   
If empty, the IP address will be taken from the server's IP pool

Networks behind user:

Nun kann die Verbindung über den Win XP Client aufgebaut werden.

Ein Ping kann Ihnen die Funktionalität bestätigen.

```
Ping wird ausgeführt für 192.168.192.9 mit 32 Bytes Daten:
Antwort von 192.168.192.9: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.192.9: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.192.9: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.192.9: Bytes=32 Zeit=2ms TTL=63
Ping-Statistik für 192.168.192.9:
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
  Ca. Zeitangaben in Millisek.:
  Minimum = 2ms, Maximum = 2ms, Mittelwert = 2ms
```