

Beispielkonfiguration eines IPSec VPN Servers mit dem NCP Client

(Für DFL-160)

Zur Konfiguration eines IPSec VPN Servers gehen bitte folgendermaßen vor.

Konfiguration des IPSec VPN Servers in der DFL-160:

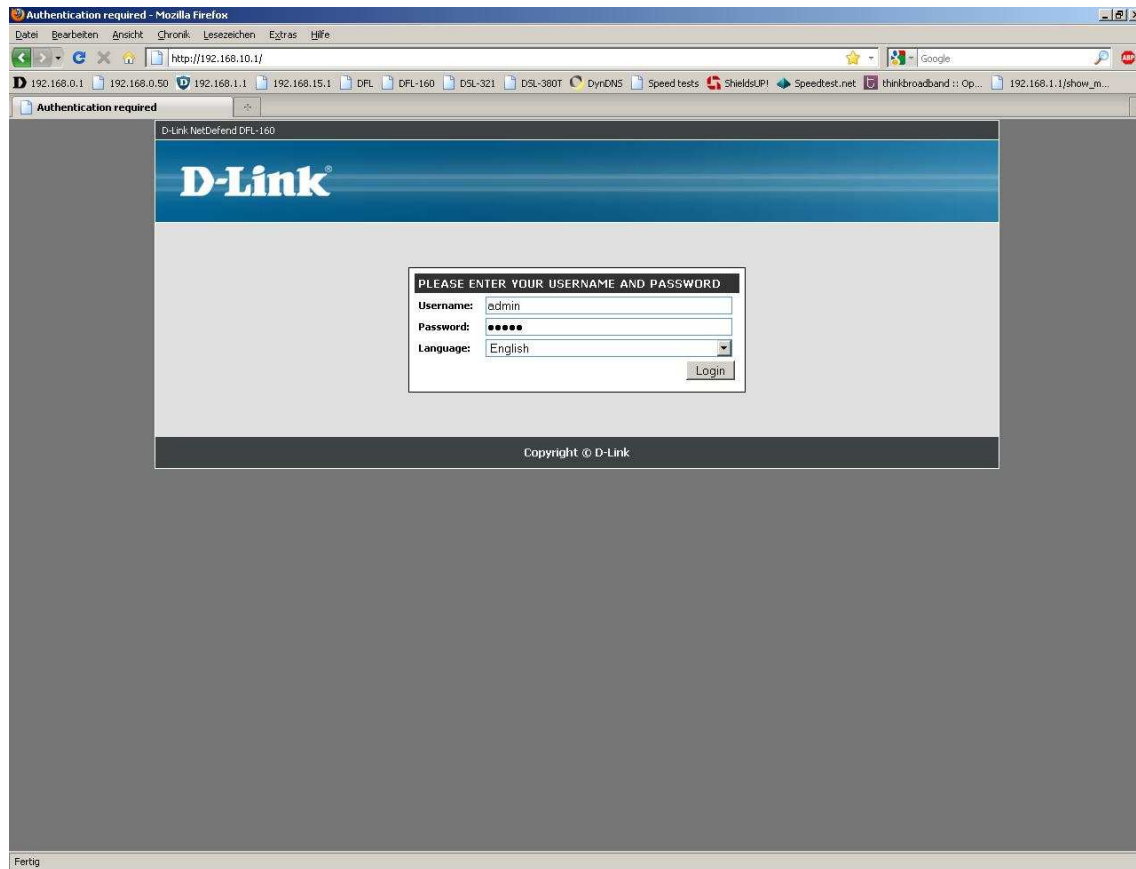
1. Loggen Sie sich auf die Konfiguration der DFL-160 ein.

Die Standard Adresse ist <http://192.168.10.1>

Username = admin

Password = admin

Klicken Sie auf **Login**.



2. Unter Firewall – VPN klicken Sie **Add** und wählen **IPSec Tunnel** aus.

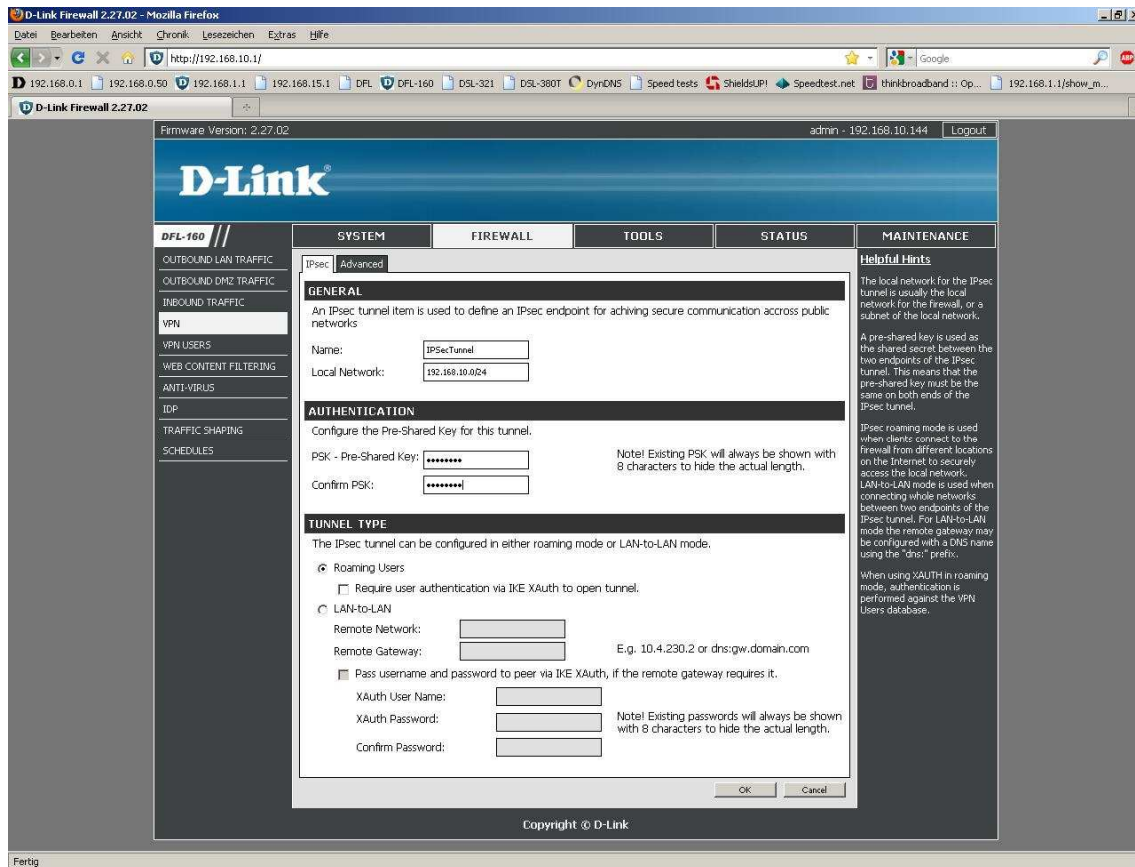
The screenshot shows the D-Link Firewall 2.27.02 web interface. The browser address bar shows the URL `http://192.168.10.1/`. The interface has a top navigation bar with tabs for SYSTEM, FIREWALL, TOOLS, STATUS, and MAINTENANCE. The FIREWALL tab is active, and the VPN section is selected. On the left, there is a sidebar menu with options like OUTBOUND LAN TRAFFIC, INBOUND TRAFFIC, VPN, VPN USERS, WEB CONTENT FILTERING, ANTI-VIRUS, IDP, TRAFFIC SHAPING, and SCHEDULES. The main content area shows a table with the following columns: Add, Name, RemoteGateway, and Action. The 'Add' button is highlighted, and the 'IPSec Tunnel' option is selected from the dropdown menu. The table contains one entry: 'emoteNetwork' with 'RemoteGateway' in the Action column. Below the table, there is a note: 'Right-click on a row for additional options.' On the right side, there is a 'Helpful Hints' section with text explaining that VPN (Virtual Private Network) can be used to securely connect over the public Internet to a protected network. The footer of the page shows the URL `http://192.168.10.1/?Page=Node0CEJ=/Firewall/VPN&Action=AddNew&NodeClass=SimpleDFLVPNIPsec`.

3.
Vergeben Sie dem Tunnel einen Namen.

Belassen Sie den Eintrag bei Local Network.

Bei **PSK – Pre-Shared Key** tragen Sie Ihren Pre-Shared Key ein und wiederholen ihn im darunter liegenden Feld.

Unter **Tunnel Type** muss **Roaming User** ausgewählt sein.



Möchten Sie den IPSec VPN Tunnel zusätzlich mittels XAUTH absichern, setzen Sie bei **Require user authentication via IKE XAuth to open tunnel.**

The screenshot shows the D-Link Firewall 2.27.02 web interface in Mozilla Firefox. The page title is "D-Link Firewall 2.27.02" and the URL is "http://192.168.10.1/". The interface is in German and shows the "IPsec" configuration page under the "FIREWALL" tab. The "TUNNEL TYPE" section is expanded, and the option "Require user authentication via IKE XAuth to open tunnel" is checked. Other options include "Roaming Users" and "LAN-to-LAN". The "XAuth" section has fields for "XAuth User Name", "XAuth Password", and "Confirm Password". The "PSK" section has fields for "PSK - Pre-Shared Key" and "Confirm PSK". The "GENERAL" section has fields for "Name" (IPsecTunnel) and "Local Network" (192.168.10.0/24). The "Helpful Hints" section on the right provides additional information about IPsec tunneling and XAuth.

D-Link Firewall 2.27.02 admin - 192.168.10.144 Logout

D-Link

DFL-160 // SYSTEM FIREWALL TOOLS STATUS MAINTENANCE

OUTBOUND LAN TRAFFIC
OUTBOUND DMZ TRAFFIC
INBOUND TRAFFIC
VPN
VPN USERS
WEB CONTENT FILTERING
ANTI-VIRUS
IDP
TRAFFIC SHAPING
SCHEDULES

IPsec: Advanced

GENERAL
An IPsec tunnel item is used to define an IPsec endpoint for achieving secure communication across public networks.

Name: IPsecTunnel
Local Network: 192.168.10.0/24

AUTHENTICATION
Configure the Pre-Shared Key for this tunnel.

PSK - Pre-Shared Key: ***** Note! Existing PSK will always be shown with 8 characters to hide the actual length.
Confirm PSK: *****

TUNNEL TYPE
The IPsec tunnel can be configured in either roaming mode or LAN-to-LAN mode.

Roaming Users
 Require user authentication via IKE XAuth to open tunnel.
 LAN-to-LAN

Remote Network: []
Remote Gateway: [] E.g. 10.4.230.2 or dns:gw.domain.com

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

XAuth User Name: []
XAuth Password: [] Note! Existing passwords will always be shown with 8 characters to hide the actual length.
Confirm Password: []

OK Cancel

Copyright © D-Link

Helpful Hints
The local network for the IPsec tunnel is usually the local network for the firewall, or a subnet of the local network.
A pre-shared key is used as the shared secret between the two endpoints of the IPsec tunnel. This means that the pre-shared key must be the same on both ends of the IPsec tunnel.
IPsec roaming mode is used when clients connect to the firewall from different locations on the Internet to securely access the local network.
LAN-to-LAN mode is used when connecting whole networks between two endpoints of the IPsec tunnel. For LAN-to-LAN mode the remote gateway may be configured with a DNS name using the "dns:" prefix.
When using XAUTH in roaming mode, authentication is performed against the VPN Users database.

Fertig

4.
Wählen Sie oben den Reiter **Advanced** aus.

Belassen Sie den **IKE Mode** auf **Main Mode**.

Setzen Sie die **DH Group** auf **5**.

Setzen Sie **PFS** auf **PFS**.

Setzen Sie die **PFS Group** auf **5**.

Klicken Sie unten auf **OK**.

The screenshot shows the D-Link Firewall 2.27.02 web interface in Mozilla Firefox. The browser address bar shows 'http://192.168.10.1/'. The page title is 'D-Link Firewall 2.27.02'. The interface includes a navigation menu on the left with options like 'OUTBOUND LAN TRAFFIC', 'VPN', and 'SCHEDULES'. The main content area is titled 'IPsec Advanced' and contains several sections: 'LIFETIMES' with input fields for 'IKE lifetime: 28800 seconds' and 'IPsec lifetime: 3600 seconds'; 'IKE SETTINGS' with 'IKE Mode' set to 'Main mode' and 'DH Group' set to '5'; 'PERFECT FORWARD SECRECY' with 'PFS' set to 'PFS' and 'PFS DH Group' set to '5'; 'DEAD PEER DETECTION' with 'Enable Dead Peer Detection' checked; and 'KEEP-ALIVE' with 'Auto' selected and 'Keep-alive destination IP' set to an empty field. A 'Helpful Hints' sidebar on the right provides additional information about IPsec settings. The bottom of the page shows the word 'Fertig'.

5.

Möchten Sie XAUTH nutzen und haben **Require user authentication via IKE Xauth to open tunnel** aktiviert (siehe Seite 4), wählen Sie links das Menü **VPN Users** aus.

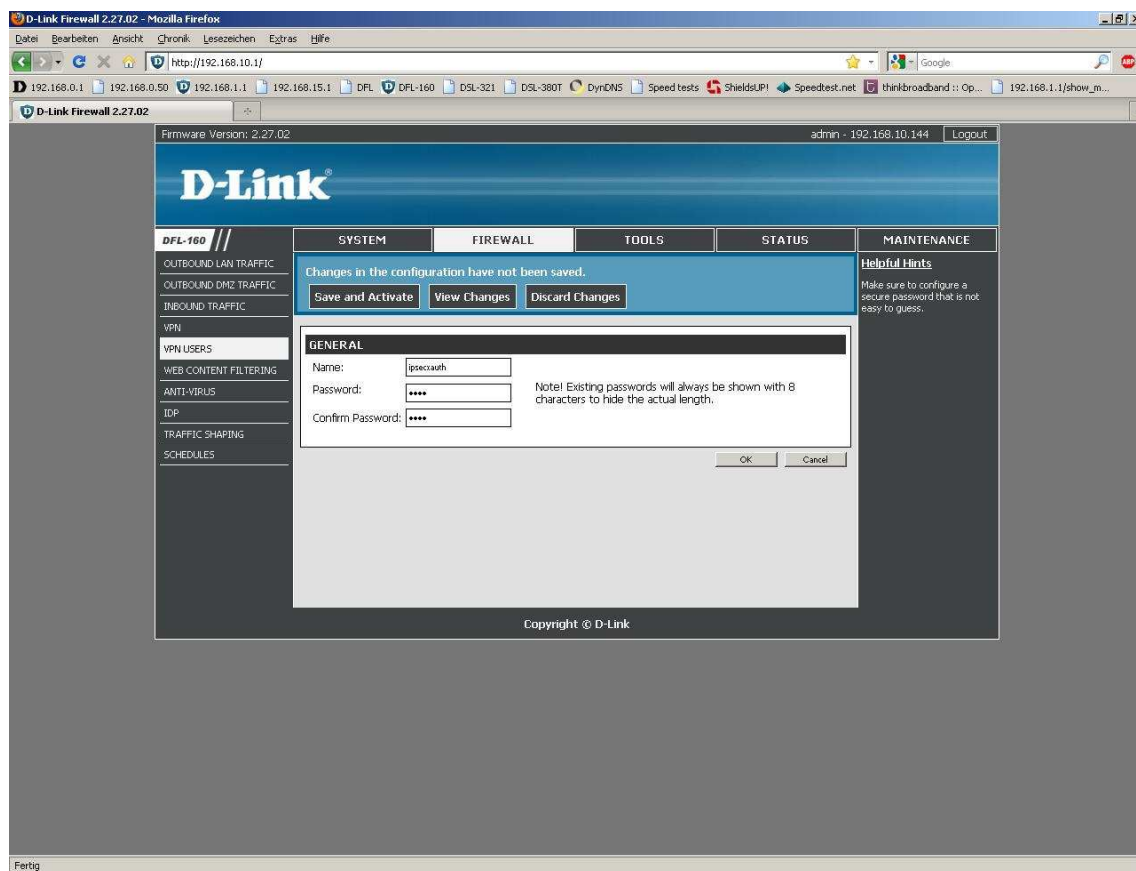
Klicken Sie auf **Add** und wählen **User** aus.

Tragen Sie nun die Zugangsdaten für das XAUTH ein:

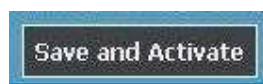
Vergeben Sie bei **Name** einen Benutzernamen.

Bei **Password** tragen Sie ein Passwort ein und wiederholen es im Feld darunter.

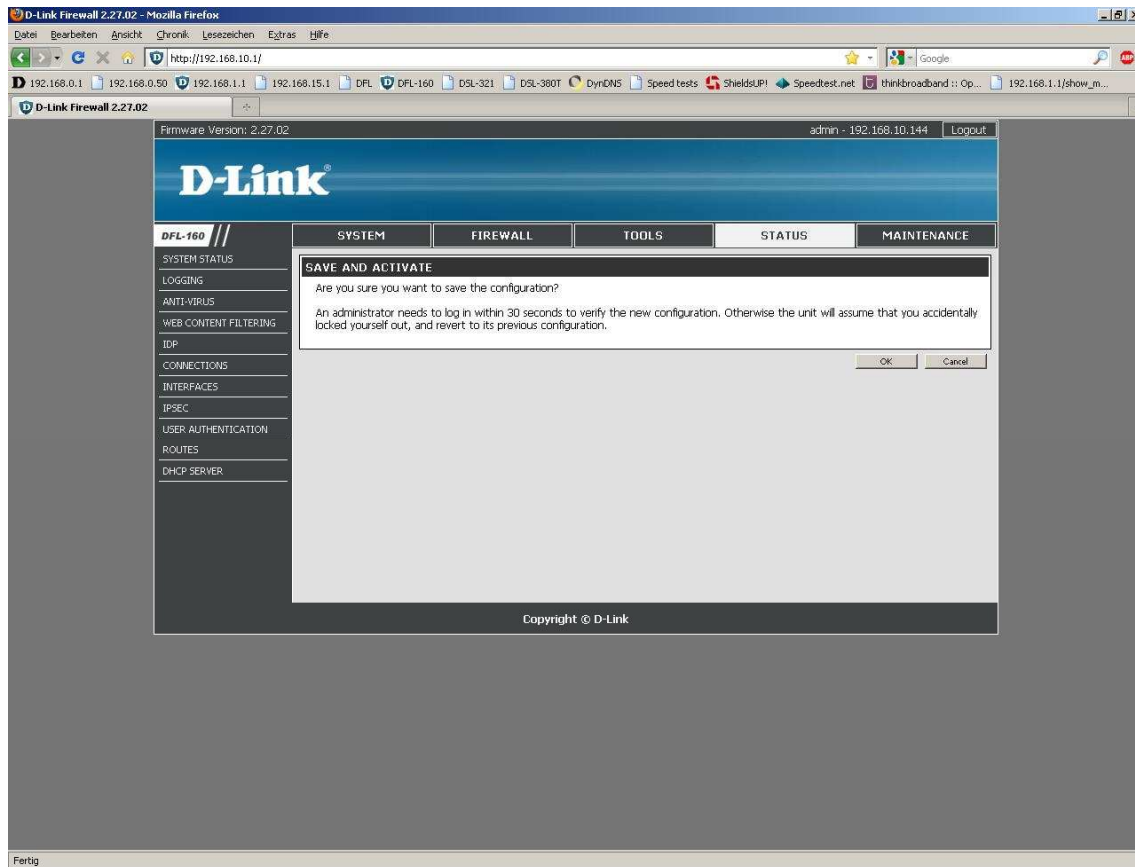
Klicken Sie unten auf **OK**.



6. Klicken Sie abschließend auf **Save and Activate**.



7. Die DFL-160 übernimmt nun die Einstellungen.



Die Einrichtung des IPSec Servers in der DFL-160 ist damit abgeschlossen.

Einrichtung des NCP Clients

1. Rufen Sie den NCP Client auf.
2. Wählen Sie unter **Konfiguration** den Punkt **Profile** aus.



3. Klicken Sie auf **Hinzufügen / Import**.



4. **Verbindung zum Firmennetz über IPsec** muss ausgewählt sein.
Klicken Sie auf **Weiter**.



5. Vergeben Sie einen Profil-Namen.
Klicken Sie auf **Weiter**.



6. Wählen Sie das **Verbindungsmedium** aus.

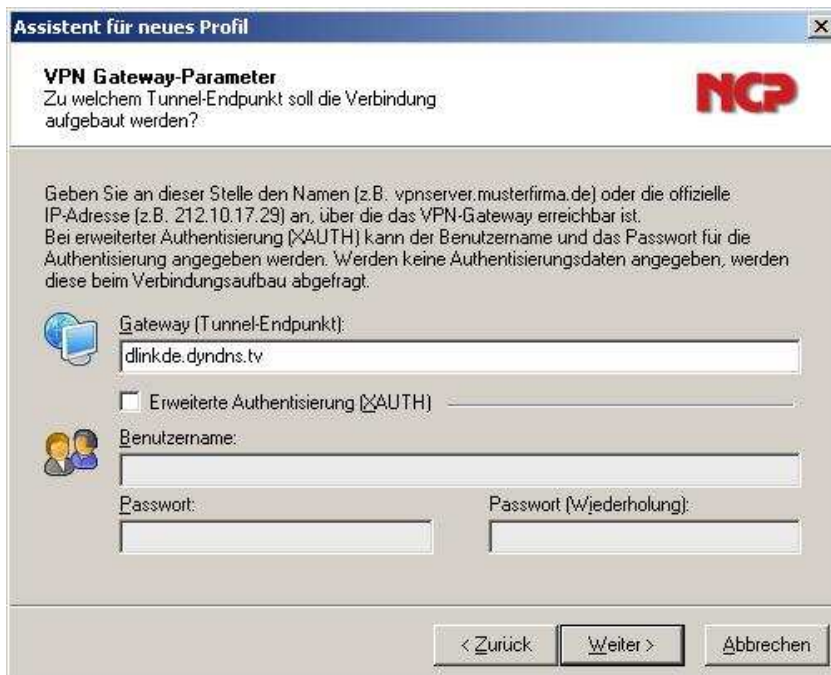
Geht der Client-Rechner über einen Router online oder stellt die Internetverbindung über eine eigene Breitbandverbindung her, belassen Sie die Einstellung auf **LAN (over IP)**.

Klicken Sie auf **Weiter**.



The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main heading is "Verbindungsmedium" with a sub-heading "Auswahl des Mediums, über das die Verbindung hergestellt werden soll." and the NCP logo. Below this is a paragraph of instructions: "Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Das Verbindungsmedium wird für jedes Profil eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert. Soll z. B. das Internet über Modem genutzt werden, stellen Sie unter Verbindungsmedium 'Modem' ein und wählen anschließend das gewünschte Modem aus." There is a globe icon to the left of the label "Verbindungsmedium:" and a dropdown menu currently set to "LAN (over IP)". At the bottom are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

7. Tragen Sie bei **Gateway (Tunnel-Endpunkt)** die WAN IP Adresse bzw. DynDNS Adresse der DFL-160 ein.



The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main heading is "VPN Gateway-Parameter" with a sub-heading "Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?" and the NCP logo. Below this is a paragraph of instructions: "Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist. Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt." There is a globe icon to the left of the label "Gateway (Tunnel-Endpunkt):" and a text input field containing "dlinkde.dyndns.tv". Below this is a checkbox labeled "Erweiterte Authentisierung (XAUTH)" which is unchecked. There is a user icon to the left of the label "Benutzername:" and a text input field. Below that are two text input fields labeled "Passwort:" and "Passwort (Wiederholung):". At the bottom are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Möchten Sie XAUTH nutzen und haben in der DFL-160 **Require user authentication via IKE Xauth to open tunnel** aktiviert (siehe Seite 4), setzen Sie hier bei **Erweiterte Authentisierung (XAUTH)** einen Haken und tragen darunter die XAUTH Zugangsdaten ein.

Klicken Sie auf **Weiter**.

The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main heading is "VPN Gateway-Parameter" with the NGP logo to the right. Below the heading is the question: "Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?". A detailed instruction follows: "Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist. Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt." The form contains three input fields: "Gateway (Tunnel-Endpunkt):" with the value "dlinkde.dyndns.tv", "Benutzername:" with the value "ipsecxauth", and "Passwort:" with masked characters. A "Passwort (Wiederholung):" field also contains masked characters. A checkbox labeled "Erweiterte Authentisierung (XAUTH)" is checked. At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

8. Wählen Sie bei **PFS-Gruppe** die **DH-Gruppe 5** aus.
Klicken Sie auf **Weiter**.

The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main heading is "IPsec-Konfiguration" with the NGP logo to the right. Below the heading is the question: "Konfiguration der grundlegenden Parameter für IPsec". A detailed instruction follows: "Hier können sie grundlegende Parameter für IPsec angeben. Für die Richtlinien der IPsec-Verhandlung wird die Einstellung 'Automatischer Modus' verwendet. Sollen bestimmte IKE / IPsec-Richtlinien verwendet werden, müssen diese anschließend in den Profil-Einstellungen definiert und zugewiesen werden." The form contains two dropdown menus: "Austausch-Modus:" with "Main Mode" selected, and "PFS-Gruppe:" with "DH-Gruppe 5 (1536 Bit)" selected. A checkbox labeled "Benutze IPsec-Kompression" is unchecked. At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

9. Tragen Sie in beiden Shared Secret Feldern den Pre-Shared Key ein, den Sie in der DFL-160 konfiguriert hatten.
Klicken Sie auf **Weiter**.

The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main title is "IPsec-Konfiguration - Pre-shared Key" and the subtitle is "Gemeinsamer Schlüssel für die IPsec". The NCP logo is in the top right. The text explains that a shared key is needed for authentication and encryption. It contains a "Pre-shared Key" label, a "Shared Secret" field with a masked input, and a "Shared Secret (Wiederholung)" field with a masked input. Below that is a "Lokale Identität (IKE)" section with a "Typ" dropdown menu set to "IP-Adresse" and an empty "ID" field. At the bottom are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

10. Nehmen Sie hier keine Änderungen vor.
Klicken Sie auf **Weiter**.

The screenshot shows a window titled "Assistent für neues Profil" with a close button (X) in the top right corner. The main title is "IPsec-Konfiguration - IP-Adressen" and the subtitle is "Welche IP-Adressen sollen verwendet werden?". The NCP logo is in the top right. The text asks for the IP address to be assigned to the client. It contains an "IP-Adressen-Zuweisung" dropdown menu set to "Lokale IP-Adresse verwenden", an "IP-Adresse" field with "0.0.0.0", and a "DNS / WINS Server" section with "DNS Server" and "WINS Server" fields, both containing "0.0.0.0". At the bottom are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

11. Sie können das Stateful Inspection nach Belieben ändern.

Klicken Sie auf **Fertigstellen**.



12. Wählen Sie Ihr Profil aus und klicken auf **Bearbeiten**.



13. Wählen Sie links das Menü **IPSec-Einstellungen** aus.

Klicken Sie auf den Knopf **Editor**.



14. Markieren Sie **IKE-Richtlinie** und klicken dann auf den Knopf **Hinzufügen**.



15.

Vergeben Sie der Richtlinie einen Namen.

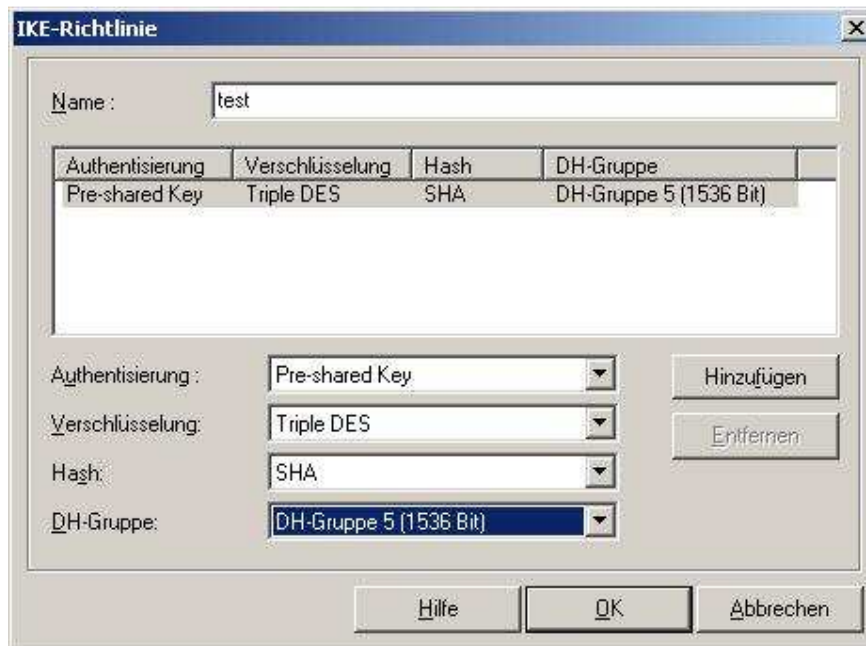
Bei **Authentisierung** muss **Pre-Shared Key** ausgewählt sein.

Wählen Sie bei **Verschlüsselung** **Triple DES** aus.

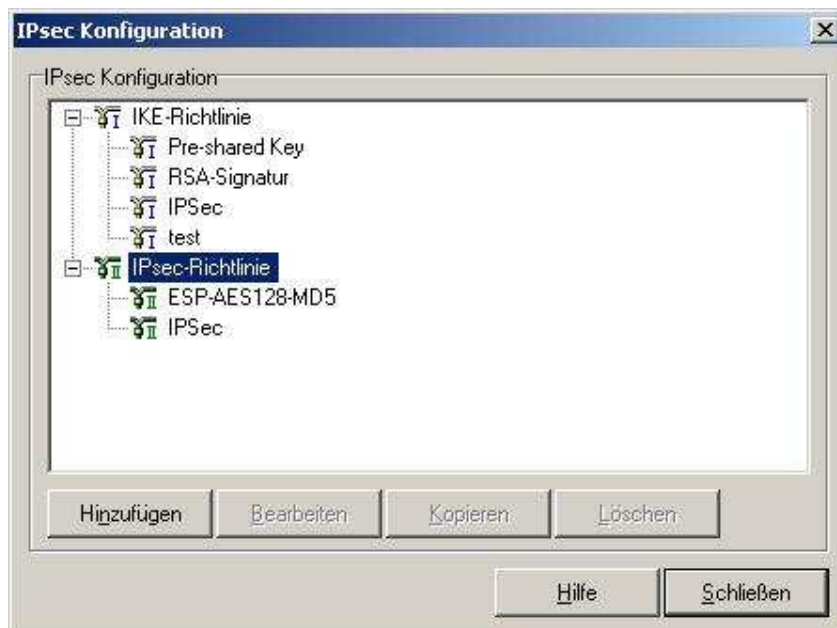
Wählen Sie bei **HASH** **SHA** aus.

Wählen Sie bei **DH-Gruppe** die **DH-Gruppe 5** aus.

Klicken Sie auf **OK**.



16. Markieren Sie **IPSec-Richtlinie** und klicken dann auf den Knopf **Hinzufügen**.



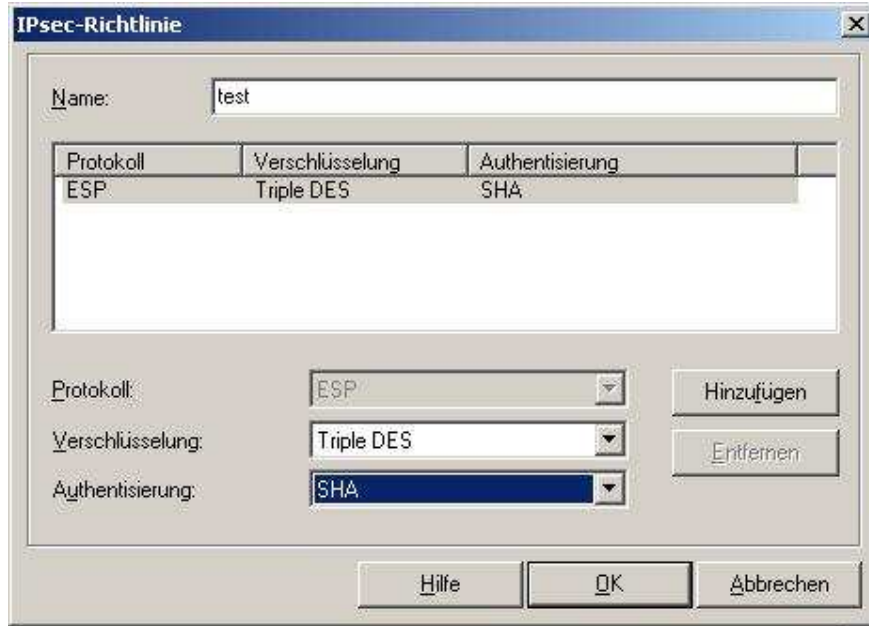
17.

Vergeben Sie der Richtlinie einen Namen.

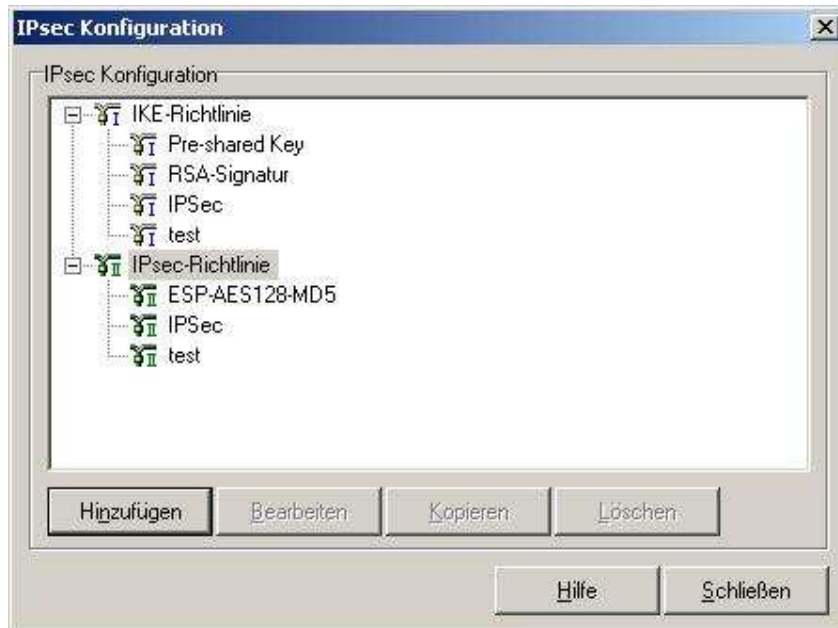
Wählen Sie bei **Verschlüsselung Triple DES** aus.

Wählen Sie bei **Authentisierung SHA** aus.

Klicken Sie auf **OK**.



18. Klicken Sie auf **Schließen**.



19. Wählen Sie nun bei **IKE-Richtlinie** und **IPsec-Richtlinie** die eben hinzugefügten aus.



20. Wählen Sie ggf. bei **PFS-Gruppe** die **DH-Gruppe 5** aus.



21. Wählen Sie links das Menü **Split Tunneling** aus und klicken auf den Knopf **Hinzufügen**.

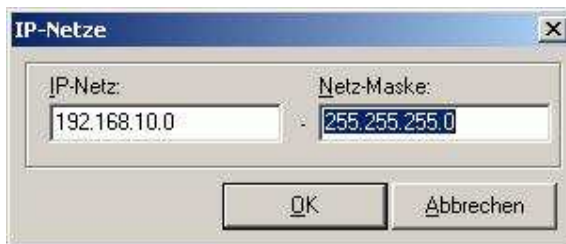


22. Teilen Sie dem NCP Client mit, welches IP Netz er über den Tunnel anzusprechen hat. So kann der NCP Client dann im Rechner die entsprechende Route setzen.

Tragen Sie die IP Netz Adresse der LAN Seite der DFL-160 ein.
Die DFL-160 hat standardmäßig die IP Adresse 192.168.10.1 mit der Subnetmaske 255.255.255.0

Bei **IP-Netz** tragen Sie dann 192.168.10.0 ein.
Bei **Netz-Maske** tragen Sie 255.255.255.0 ein.

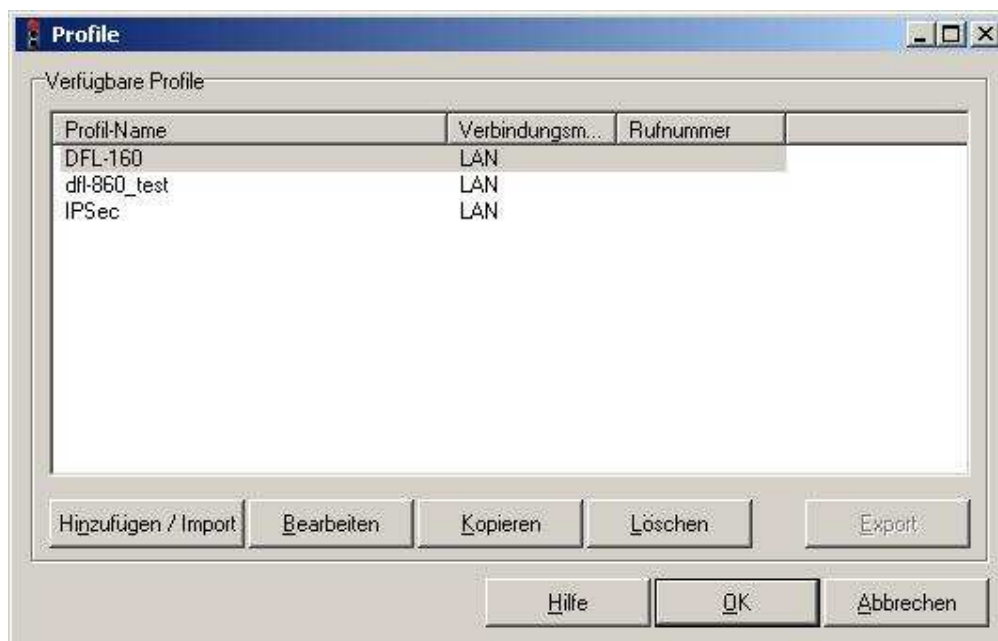
Klicken Sie auf **OK**.



23. Klicken Sie auf **OK**.



24. Klicken Sie auf **OK**.



25. Sie können nun den IPSec VPN Tunnel aufbauen.



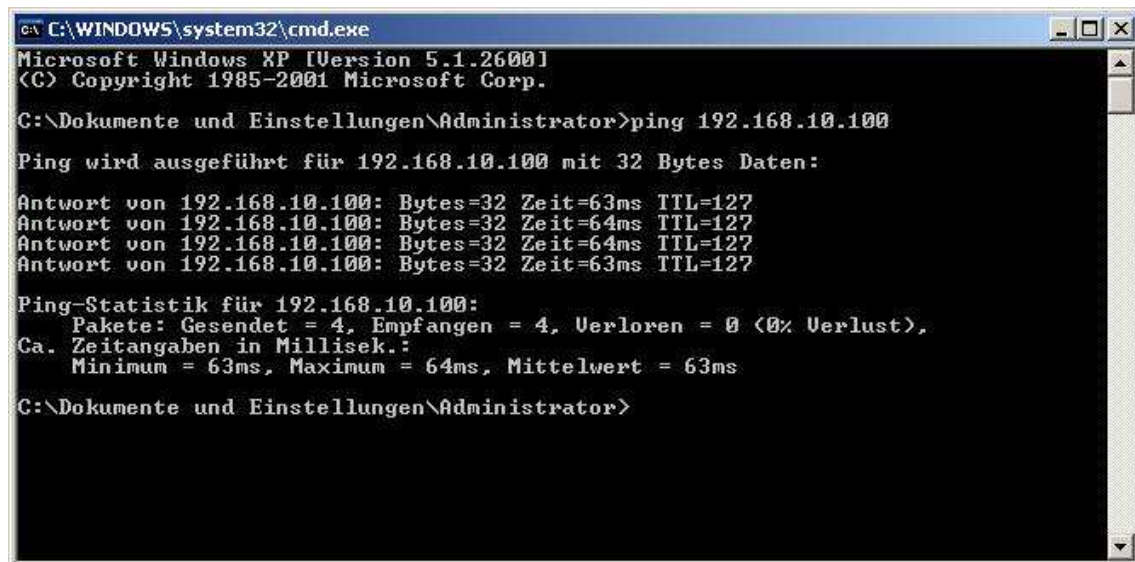
... Verbindungsaufbau ...



... Verbindung ist hergestellt.



Um den VPN Tunnel zu testen, schicken Sie vom Client-Rechner aus einen PING auf die IP Adresse eines Rechners im LAN der DFL-160.
(! Der PING könnte von einer auf dem Zielrechner aktiven Firewall geblockt werden !)



Sehr wichtig: Der Client-Rechner darf sich mit seiner eigenen Lanverbindung nicht im gleichen IP Netz wie das Ziel IP Netz befinden, das er über den VPN tunnel ansprechen soll. In dem Fall würde der Client-Rechner das Ziel nicht über den VPN Tunnel sondern im eigenen LAN versuchen anzusprechen, wo er das eigentliche Ziel aber nicht finden wird. Der Rechner würde dabei nicht versuchen das Ziel über den Tunnel anzusprechen.