

Anleitung zur Einrichtung eines Lan-to-Lan Tunnels zwischen einem DI-804HV und einer DSR

(Für DI-804HV ab Firmware 1.44b06 und DSR-250N/500N/1000N)

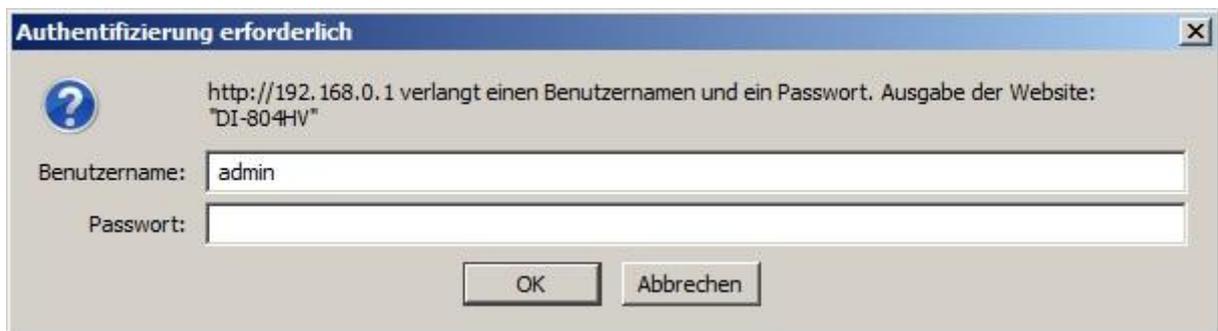
Einrichtung des DI-804HV

(Einrichtung des DSR ab Seite 8)

1. Greifen Sie per Webbrowser auf die Konfiguration Ihres DI-804HV zu und loggen Sie sich ein. Die Standard Adresse ist <http://192.168.0.1>

Der Benutzername ist **admin**.

Ein Passwort ist standardmäßig nicht gesetzt.



The image shows a screenshot of a web browser's authentication dialog box. The title bar reads "Authentifizierung erforderlich" (Authentication required). The main text says "http://192.168.0.1 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: 'DI-804HV'" (http://192.168.0.1 requires a username and a password. Website output: 'DI-804HV'). There are two input fields: "Benutzername:" (Username) with the value "admin" and "Passwort:" (Password) which is empty. At the bottom, there are two buttons: "OK" and "Abbrechen" (Cancel).

2. Wählen Sie oben das Menü **Home** und links **VPN** aus.

- Setzen Sie bei **VPN** und **NetBIOS broadcast** einen Haken und geben Sie bei **Max. numbers of Tunnels** die Anzahl der maximal gleichzeitig herstellbaren VPN Tunnel an.

- Unter der **ID 1** geben die dem Tunnel einen Namen.

Klicken Sie auf **Apply** um die Angaben zu übernehmen.

The screenshot shows the web configuration interface for a D-Link DI-804HV Broadband VPN Router. The browser window title is "D-Link DI-804HV Web Configuration - Mozilla Firefox" and the address bar shows "192.168.0.1". The interface has a blue header with the D-Link logo and the router model name. Below the header are navigation tabs: Home, Advanced, Tools, Status, and Help. The "Home" tab is selected. On the left side, there are buttons for Wizard, WAN, LAN, DHCP, and VPN. The main content area is titled "VPN Settings" and contains a table with the following data:

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	5

ID	Tunnel Name	Method
1	Tunnel	IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

At the bottom of the settings area, there are buttons for "Previous page", "Next page", "Dynamic VPN Settings", "L2TP Server Setting...", "PPTP Server Setting...", and "View VPN Status...". Below these are three icons: a green checkmark, a red X, and a red plus sign, with the labels "Apply", "Cancel", and "Help" respectively.

3. Der DI-804HV startet neu.

Klicken Sie dann auf **Continue**.

The screenshot shows the D-Link DI-804HV Broadband VPN Router web configuration interface. The header is the same as in the previous screenshot. The main content area is a simple grey box with the text "The device is restarting..." centered. Below the text is a single button labeled "Continue".

4. Gehen Sie ggf. wieder in das VPN-Menü und klicken dann rechts bei Ihrem Tunnel auf den **More**-Knopf.

- Tragen Sie bei **Local Subnet** die an LAN des DI-804HV anliegende Netz-IP-Adresse und bei **Local Netmask** die Subnetmaske ein.

Hat der DI-804HV die IP Adresse 192.168.0.1 mit der Subnetmaske 255.255.255.0, also Standardeinstellung, ist die anzugebende **Local Subnet** (Netz-IP-Adresse) die 192.168.0.0 und die **Local Netmask** (Subnetmaske) die 255.255.255.0

- Tragen Sie bei **Remote Subnet** die an LAN der DSR anliegende Netz-IP-Adresse und bei **Remote Netmask** die Subnetmaske ein.

Hat die DSR die IP Adresse 192.168.10.1 mit der Subnetmaske 255.255.255.0, also Standardeinstellung, ist die anzugebende **Local Subnet** (Netz-IP-Adresse) die 192.168.10.0 und die **Local Netmask** (Subnetmaske) die 255.255.255.0

- Bei **Remote Gateway** geben Sie entweder die WAN-IP-Adresse der DRS an, oder wenn die DSR DynDNS nutzt, können Sie deren DynDNS-Adresse angeben.

- Setzen Sie bei **Auto-reconnect** einen Haken, wenn der Tunnel sich automatisch aufbauen soll.

Klicken Sie auf **Apply** um die Angaben zu übernehmen.

The screenshot shows the D-Link DI-804HV Web Configuration interface in Mozilla Firefox. The page title is "D-Link DI-804HV Web Configuration - Mozilla Firefox". The browser address bar shows "192.168.0.1". The page content includes a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". The "Advanced" tab is selected, and the "VPN Settings - Tunnel 1" page is displayed. The settings are as follows:

Item	Setting
Tunnel Name	Tunnel
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.10.0
Remote Netmask	255.255.255.0
Remote Gateway	dlinkde.dyndns.tv
IKE Keep Alive (Ping IP Address)	
Preshare Key	*****
Extended Authentication (xAUTH)	<input type="checkbox"/> Enable <input type="checkbox"/> Server mode Set Local user... <input type="checkbox"/> Client mode
User Name	
Password	
IPSec NAT Traversal	<input type="checkbox"/> Enable
Auto-reconnect	<input checked="" type="checkbox"/> Enable
Remote ID	Type: IP Address Value:
Local ID	Type: IP Address Value:
IKE Proposal Index	Select IKE Proposal...
IPSec Proposal Index	Select IPSec Proposal...

At the bottom of the page, there are four buttons: "Back", "Apply", "Cancel", and "Help".

5. Der DI-804HV startet neu.
Klicken Sie dann auf **Continue**.



6. Klicken Sie unten auf **Select IKE Proposal**.

Editieren Sie die Proposal **ID 1**:

- Vergeben Sie einen **Proposal Name**.
- Wählen Sie unter **DH Group** die **Group 5** aus.
- Wählen Sie bei **Encrypt algorithm** das **3DES** aus.
- Wählen Sie bei **Auth algorithm** das **SHA1** aus.
- Tragen Sie bei **Life Time** **28800** (Sekunden) ein.

Wählen Sie unten die **Proposal ID 1** aus und klicken auf **Add to**, um die Proposal zu übernehmen.

Klicken Sie auf **Apply** um die Angaben zu übernehmen.

The screenshot shows the D-Link DI-804HV web configuration page in Mozilla Firefox. The browser address bar shows "192.168.0.1". The page title is "D-Link DI-804HV Web Configuration - Mozilla Firefox". The main content area is titled "DI-804HV Broadband VPN Router" and "VPN Settings - Tunnel 1 - Set IKE Proposal".

On the left side, there are navigation buttons: Wizard, WAN, LAN, DHCP, and VPN (highlighted in yellow). The main configuration area has tabs for Home, Advanced, Tools, Status, and Help. The "Advanced" tab is selected.

The configuration area shows a table for IKE Proposals:

Item	Setting
IKE Proposal index	1

Below this is a table for the IKE Proposals:

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1		Group 5	3DES	SHA1	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

At the bottom, there is a "Proposal ID" dropdown menu with a list of options (1-10) and an "Add to" button. Below the dropdown are buttons for Back, Apply, Cancel, and Help.

7. Der DI-804HV startet neu.
Klicken Sie dann auf **Continue**.



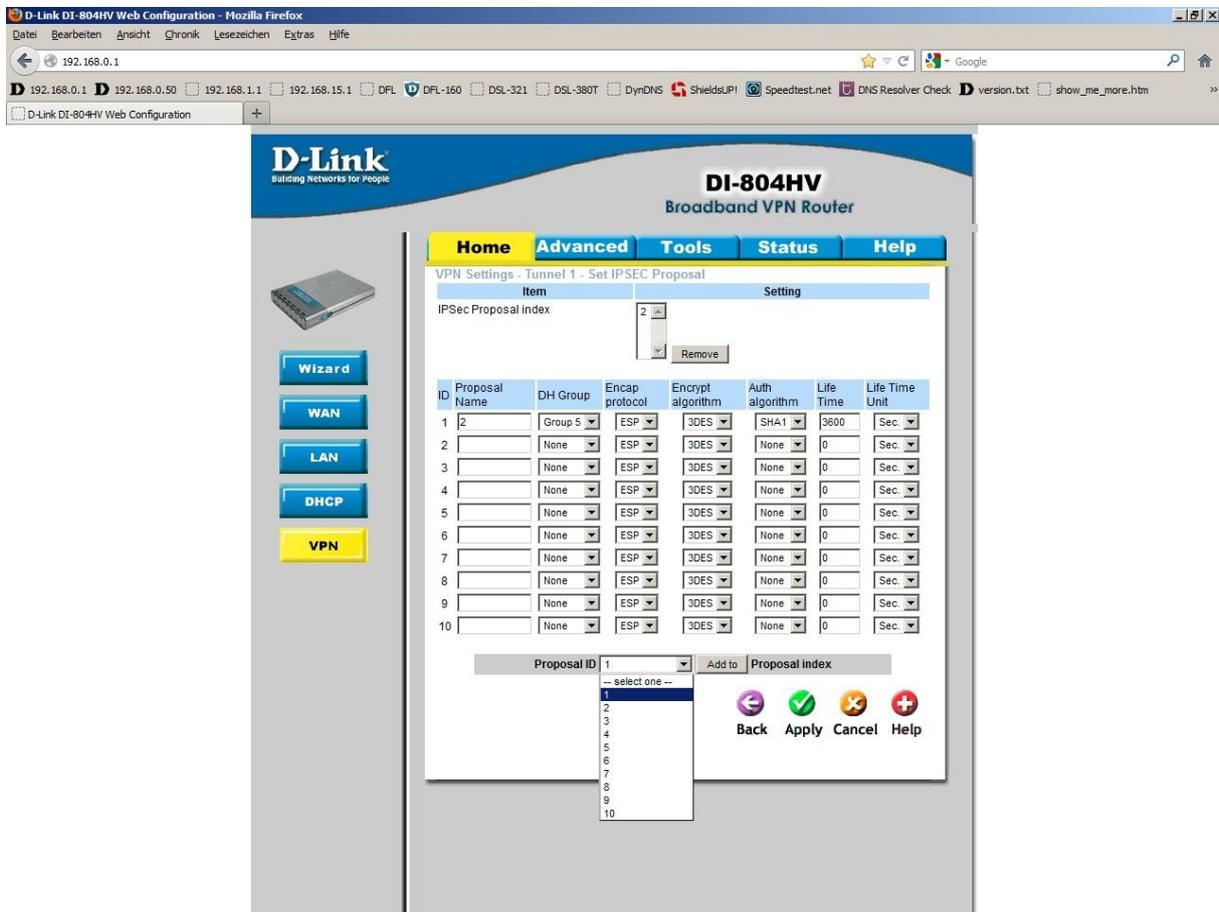
8. Klicken Sie unten auf **Back** und dann unten auf **Select IPsec Proposal**.

Editieren Sie die Proposal **ID 1**:

- Vergeben Sie einen **Proposal Name**.
- Wählen Sie unter **DH Group** die **Group 5** aus.
- Wählen Sie bei Encrypt Protocol das **ESP** aus.
- Wählen Sie bei **Encrypt algorithm** das **3DES** aus.
- Wählen Sie bei **Auth algorithm** das **SHA1** aus.
- Tragen Sie bei **Life Time** **3600** (Sekunden) ein.

Wählen Sie unten die **Proposal ID 1** aus und klicken auf **Add to**, um die Proposal zu übernehmen.

Klicken Sie auf **Apply** um die Angaben zu übernehmen.



9. Der DI-804HV startet neu.
Klicken Sie dann auf **Continue**.

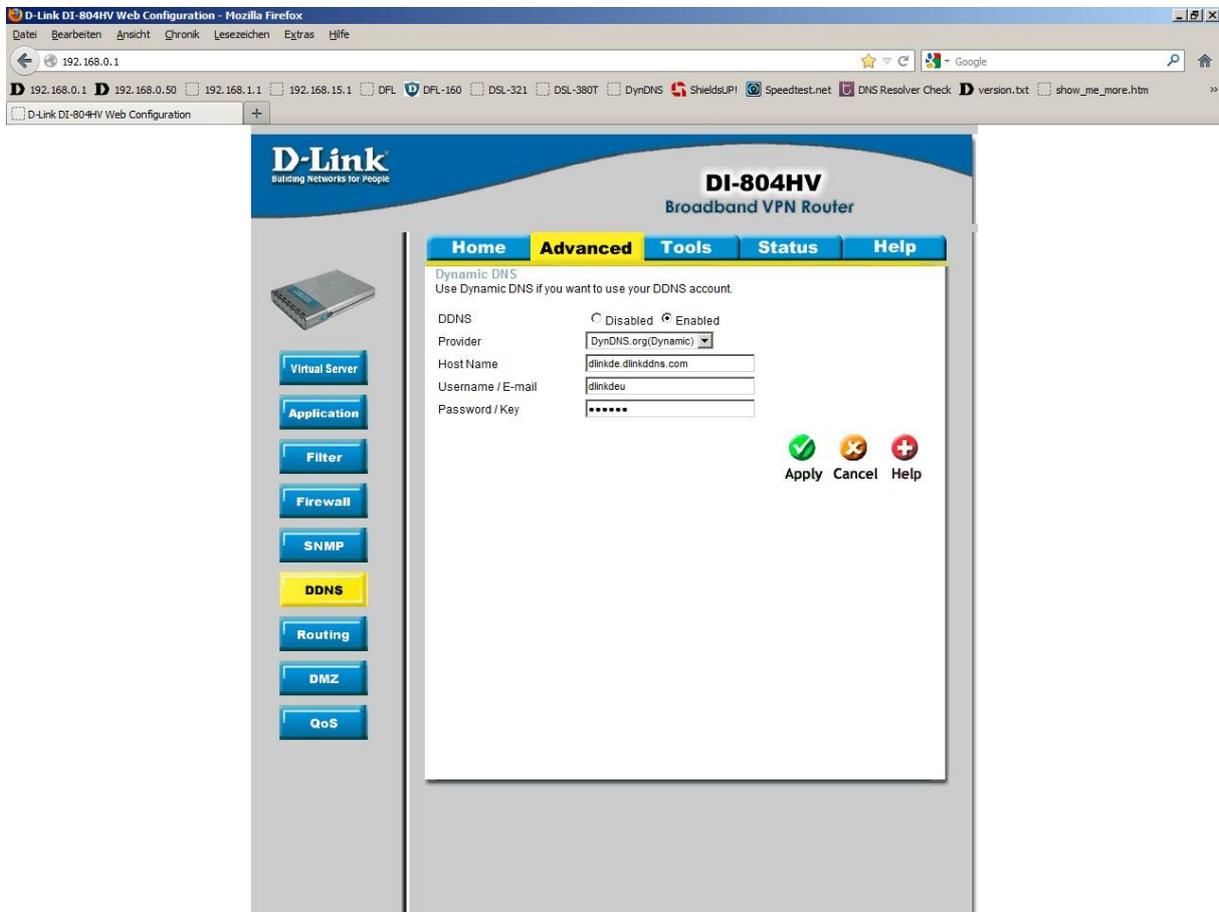


10. Soll der DI-804HV selbst DynDNS Client sein, wählen Sie oben das Menü **Advanced** und links **DDNS** aus.

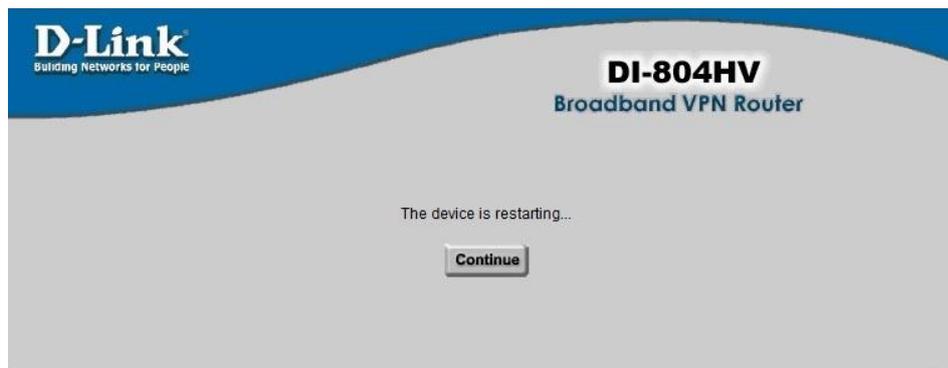
Beachten Sie bitte die Anleitungen <ftp://ftp.dlink.de/anleitungen/ddns/dyndns.pdf> und <ftp://ftp.dlink.de/anleitungen/ddns/dlinkddns.pdf> bezüglich DynDNS.

- Markieren Sie bei **DDNS Enabled**.
- Wählen Sie bei **Provider** den Eintrag **DynDNS.org (Dynamic)** aus.
- Tragen Sie bei **Host Name** Ihren bei dyndns.com oder dlinkddns.com erstellte Host Adresse ein.
- Tragen Sie bei **Username** und **Password** Ihre Zugangsdaten ein, mit denen Sie sich auf der Webseite von dyndns.com oder dlinkddns.com anmelden.

Klicken Sie auf **Apply** um die Angaben zu übernehmen.



11. Der DI-804HV startet neu.
Klicken Sie dann auf **Continue**.



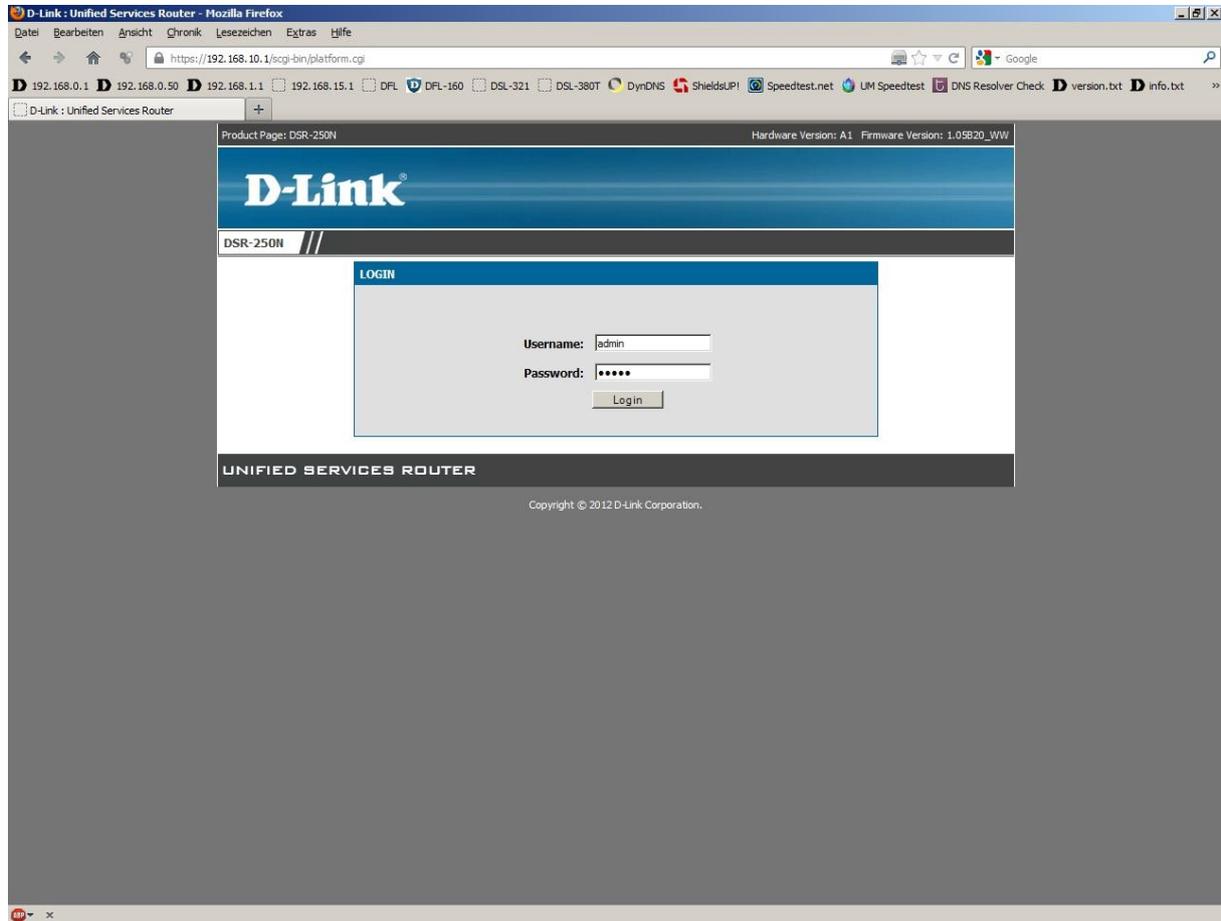
Stellen sie bitte sicher, dass Sie den Internetzugang im DI-804HV ebenfalls eingerichtet haben und er online ist.

Der DI-804HV ist damit für den Lan-to-Lan Internetzugang eingerichtet.

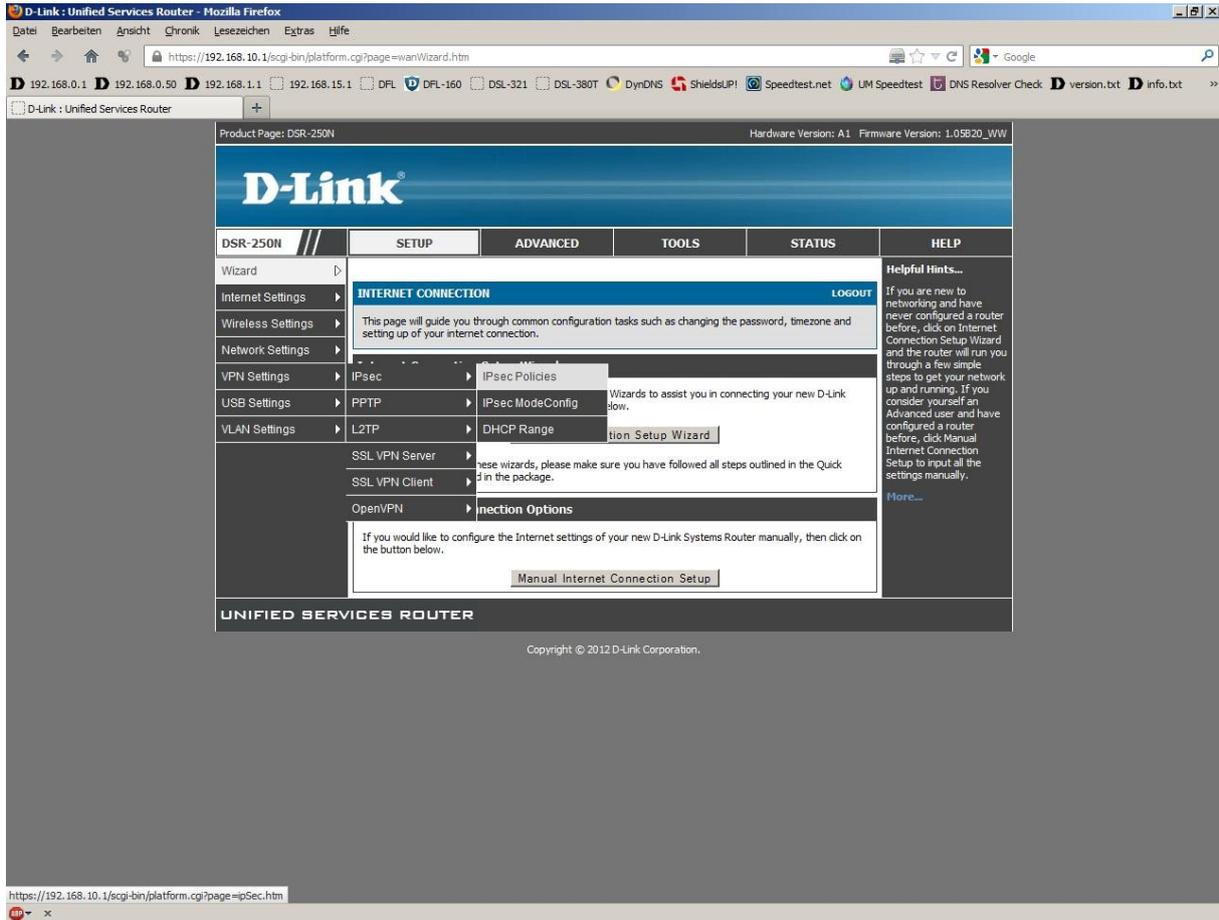
Einrichtung des DSR

1. Greifen Sie per Webbrowser auf die Konfiguration Ihres DSR zu und loggen Sie sich ein. Die Standard Adresse ist <http://192.168.10.1>

Der **Username** und das **Password** ist **admin**.



2. Wählen Sie oben das Menü **Setup** und links das Menü **VPN Settings -> IPSec -> IPSec Policies** aus.



3. Klicken Sie auf **Add** um eine neue IPsec Policy (einen neue VPN Tunnel-Konfiguration) zu erstellen.

The screenshot shows the web interface of a D-Link Unified Services Router (DSR-250N) accessed via a Mozilla Firefox browser. The browser's address bar shows the URL `https://192.168.10.1/scg-bin/platform.cgi?page=ipSec.htm`. The interface includes a navigation menu on the left with options like Wizard, Internet Settings, Wireless Settings, Network Settings, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled "IPSEC POLICIES" and contains a "List of VPN Policies" table. The table has columns for Status, Name, Type, IPsec Mode, Local, Remote, Auth, and Encr. Below the table are buttons for Edit, Enable, Disable, Delete, Add, and Export. A "Helpful Hints..." section on the right explains that IPsec VPN can be established over the internet by configuring the appropriate policy. The footer of the interface displays "UNIFIED SERVICES ROUTER" and "Copyright © 2012 D-Link Corporation."

Status	Name	Type	IPsec Mode	Local	Remote	Auth	Encr
<input type="checkbox"/>							

4. Konfigurieren Sie die folgenden Felder. Alle anderen belassen Sie bitte auf Standardeinstellung.

Unter **General**:

- Vergeben Sie bei **Policy Name** der Tunnel-Konfiguration einen Namen.

- Bei **Remote Endpoint** können Sie festlegen, ob die DSR den DI-804HV mit dessen WAN-IP-Adresse oder DynDNS-Adresse ansprechen soll.

Soll es die WAN-IP-Adresse sein, wählen Sie **IP Address** aus und tragen darunter die WAN-IP-Adresse des DI-804HV ein.

Soll es die DynDNS-Adresse sein, wählen Sie **FQDN** aus und tragen darunter die DynDNS-Adresse des DI-804HV ein.

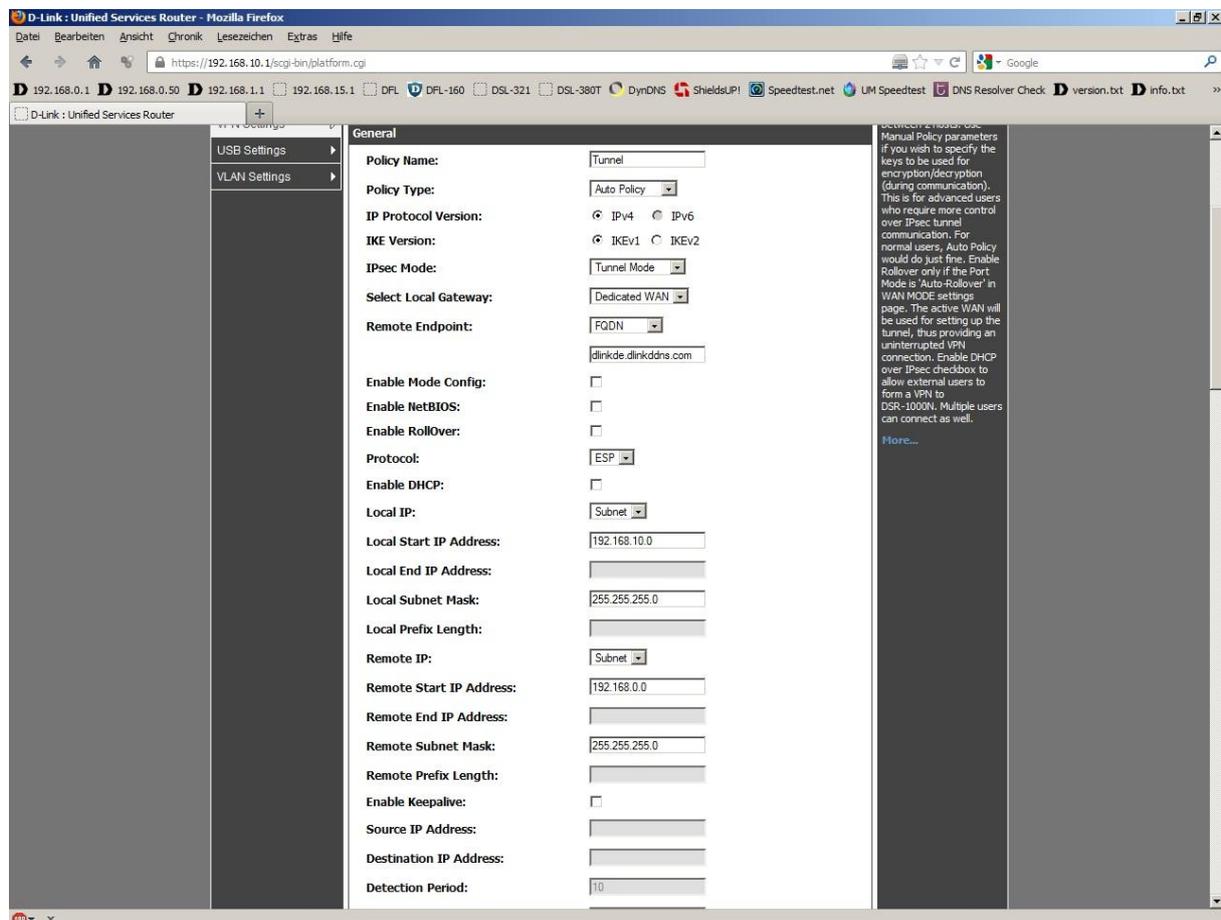
- Tragen Sie bei **Local Start IP Address** die an LAN der DSR anliegende Netz-IP-Adresse und bei **Local Subnet Mask** die Subnetmaske ein.

Hat der DSR die IP Adresse 192.168.10.1 mit der Subnetmaske 255.255.255.0, also Standardeinstellung, ist die anzugebende **Local Start IP Address** (Netz-IP-Adresse) die 192.168.0.0 und die **Local Subnet Mask** (Subnetmaske) die 255.255.255.0

- Tragen Sie bei **Remote Start IP Address** die an LAN des DI-804HV anliegende Netz-IP-Adresse und bei **Remote Subnet Mask** die Subnetmaske ein.

Hat der DI-804HV die IP Adresse 192.168.0.1 mit der Subnetmaske 255.255.255.0, also Standardeinstellung, ist die anzugebende **Remote Start IP Address** (Netz-IP-Adresse) die 192.168.0.0 und die **Local Netmask** (Subnetmaske) die 255.255.255.0

Schieben Sie das Fenster ggf. weiter nach unten ...



...

Unter **Phase1 (IKE SA Parameters)**:

- Schalten Sie **Nat Traversal** auf **Off**.

- Wählen Sie bei **Encrypt Algorithm 3DES** aus und deaktivieren die anderen.

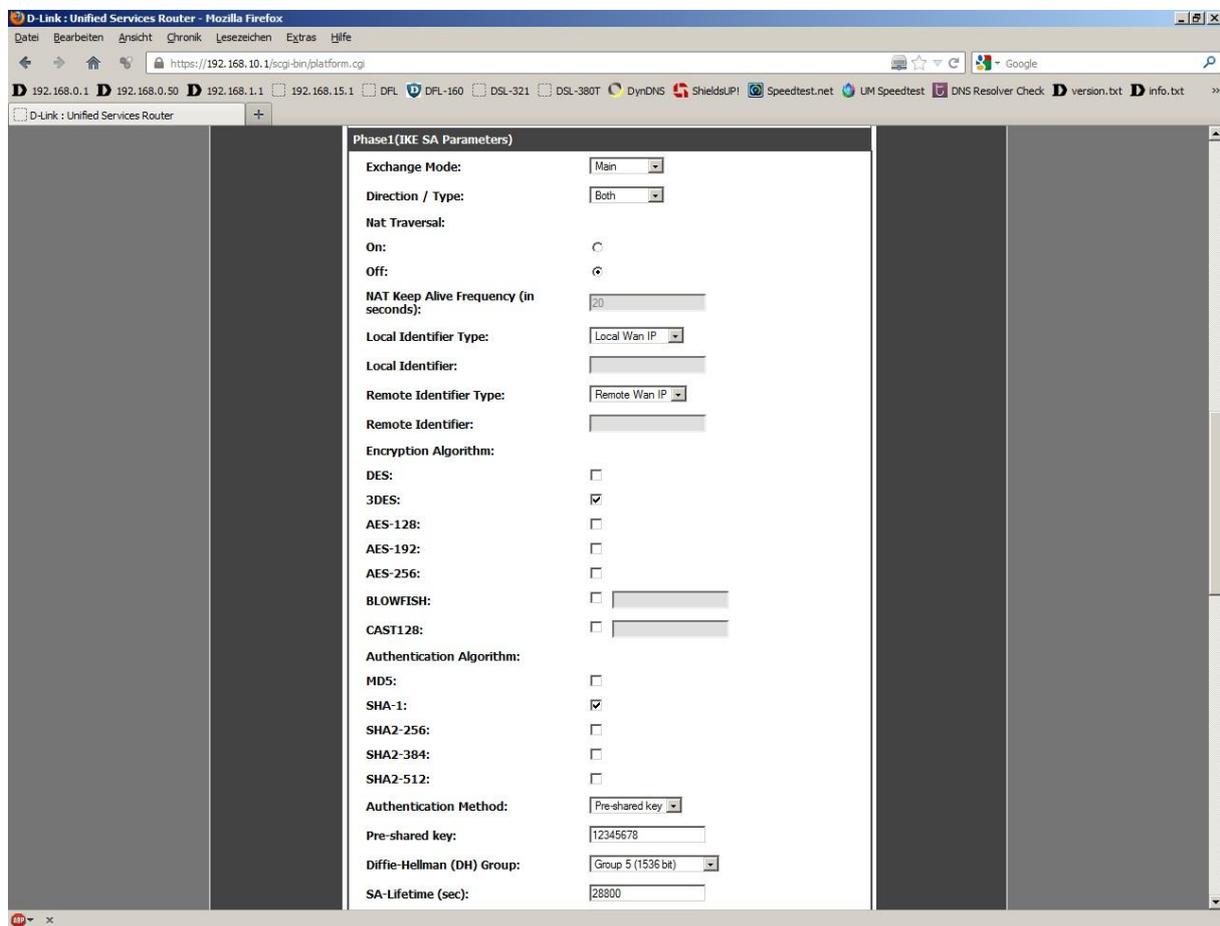
- Wählen Sie bei **Authentication Algorithm SHA-1** aus und deaktivieren die anderen.

- Tragen Sie bei **Pre-shared key** den gleichen ein, wie auch im DI-804HV.

- Wählen Sie bei **Diffie-Hellman (DH) Group** die **Group 5** aus.

- Tragen Sie bei **SA-Lifetime (sec)** **28800** ein.

Schieben Sie das Fenster ggf. weiter nach unten ...



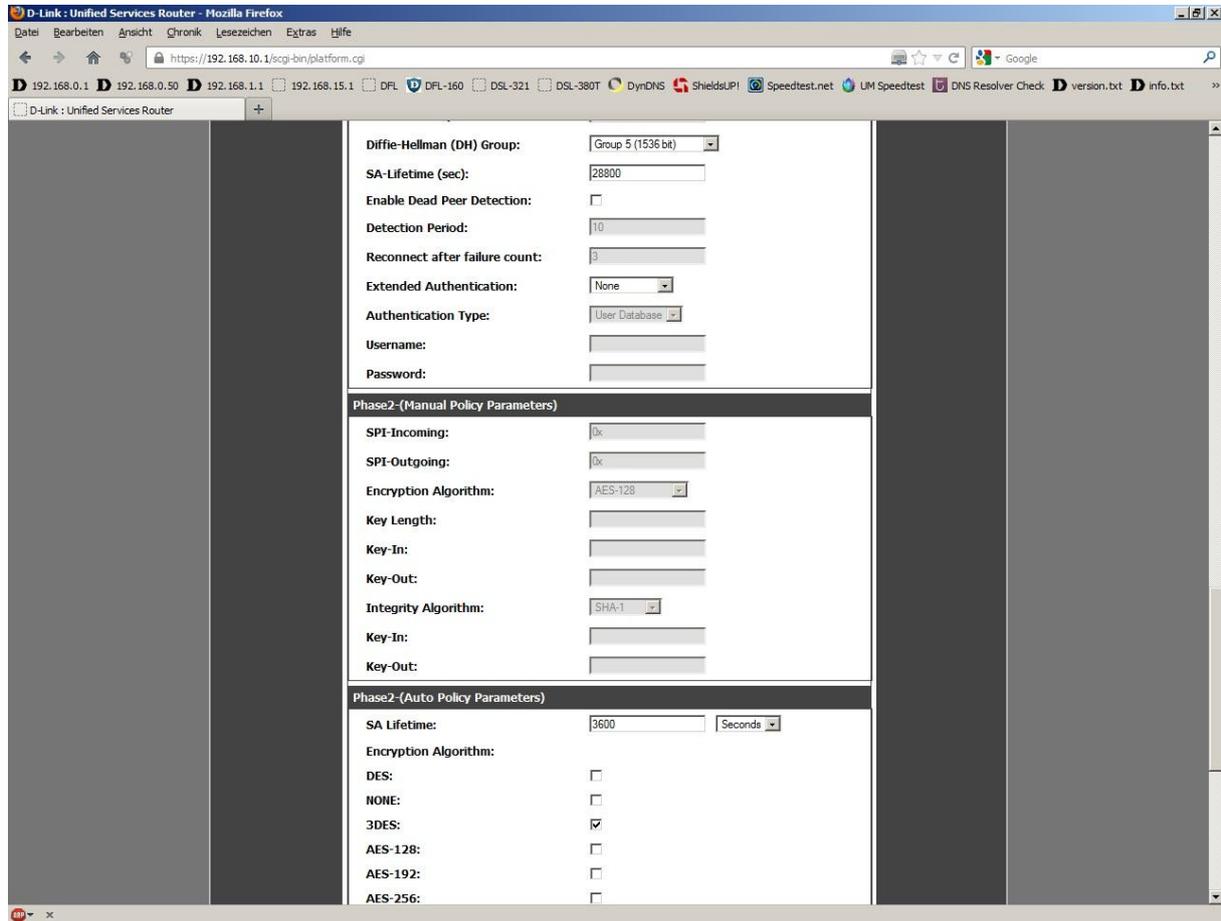
...

Unter **Phase2 (Auto Policy Parameters)**:

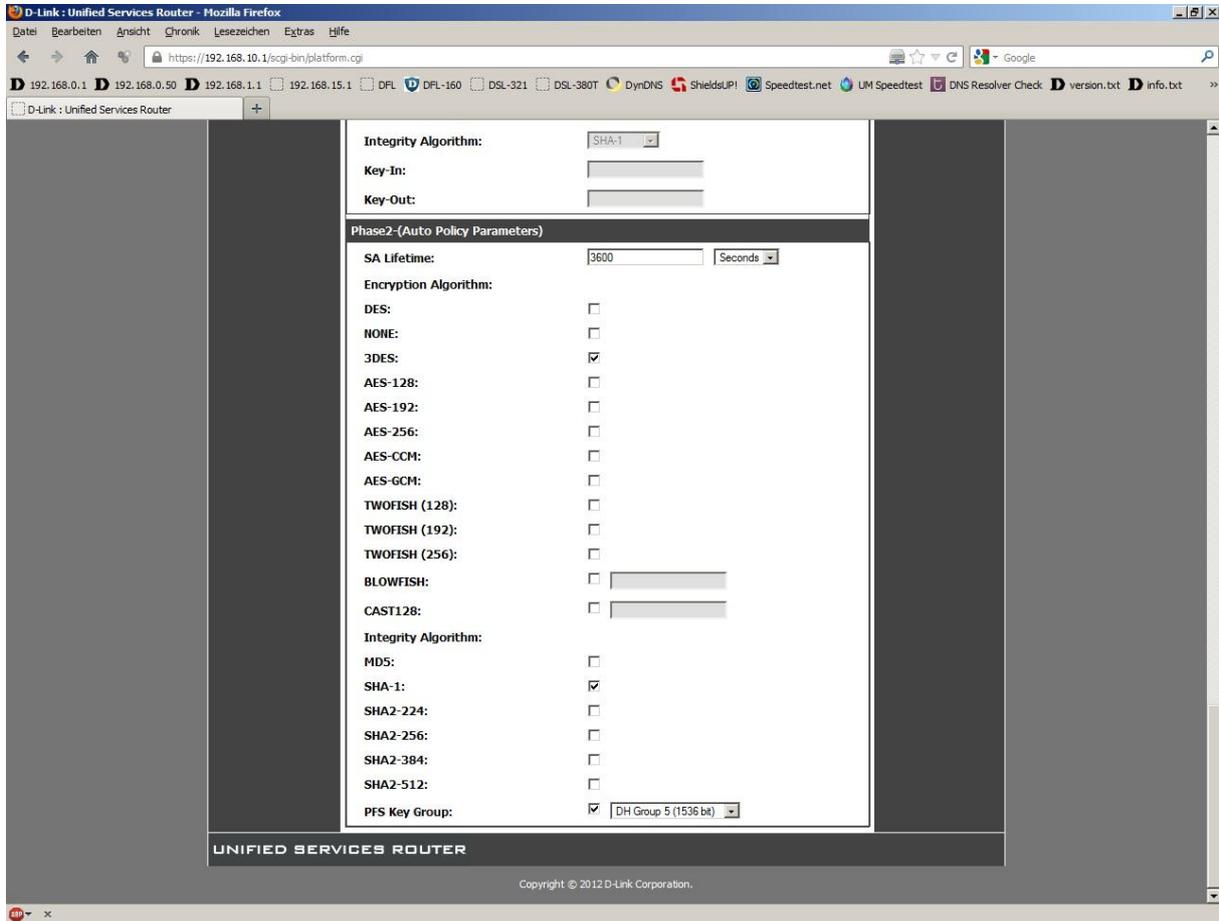
- Tragen Sie bei **SA Lifetime 3600** (Seconds) ein.

- Wählen Sie bei **Encrypt Algorithm 3DES** aus und deaktivieren die anderen.

Schieben Sie das Fenster ggf. weiter nach unten ...



- ...
- Wählen Sie bei **Integrity Algorithm SHA-1** aus und deaktivieren die anderen.
 - Setzen Sie ganz unten bei **PFS Key Group** eine Haken und wählen die **DH Group 5** aus.



Schieben Sie das Fenster wieder ganz nach oben und klicken Sie auf **Save Settings**, um die vorgenommenen Einstellungen zu übernehmen.

The screenshot shows the D-Link Unified Services Router (DSR-250N) web interface in Mozilla Firefox. The browser address bar shows the URL `https://192.168.10.1/scg-bin/platform.cgi`. The interface includes a navigation menu with options like Wizard, Internet Settings, Wireless Settings, Network Settings, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled "IPSEC CONFIGURATION" and includes a "LOGOUT" link. Below this, there is a "Save Settings" button and a "Don't Save Settings" button. The configuration is divided into a "General" section with the following fields:

- Policy Name:** Tunnel
- Policy Type:** Auto Policy
- IP Protocol Version:** IPv4 IPv6
- IKE Version:** IKEV1 IKEV2
- IPsec Mode:** Tunnel Mode
- Select Local Gateway:** Dedicated WAN
- Remote Endpoint:** FQDN
- Remote Endpoint:** dlinkde.dlinkdns.com
- Enable Mode Config:**
- Enable NetBIOS:**
- Enable RollOver:**
- Protocol:** ESP
- Enable DHCP:**
- Local IP:** Subnet
- Local Start IP Address:** 192.168.10.0
- Local End IP Address:** [Empty field]
- Local Subnet Mask:** 255.255.255.0
- Local Prefix Length:** [Empty field]

On the right side, there is a "Helpful Hints..." section with text explaining Tunnel mode and Auto Policy. A "More..." link is also present.

5. Die vorgenommene Tunnel-Konfiguration ist nun als IPSec Policy eingetragen.

The screenshot shows the D-Link Unified Services Router web interface. The main content area is titled "IPSEC POLICIES" and includes a "LOGOUT" link. Below this, there is a section for "List of VPN Policies" with an "Auto Policy" section. A table lists the configured policies:

<input type="checkbox"/>	Status	Name	Type	IPsec Mode	Local	Remote	Auth	Encr
<input type="checkbox"/>	Enabled	Tunnel	Auto Policy	Tunnel Mode	192.168.10.0 / 255.255.255.0	192.168.0.0 / 255.255.255.0	SHA1	3DES

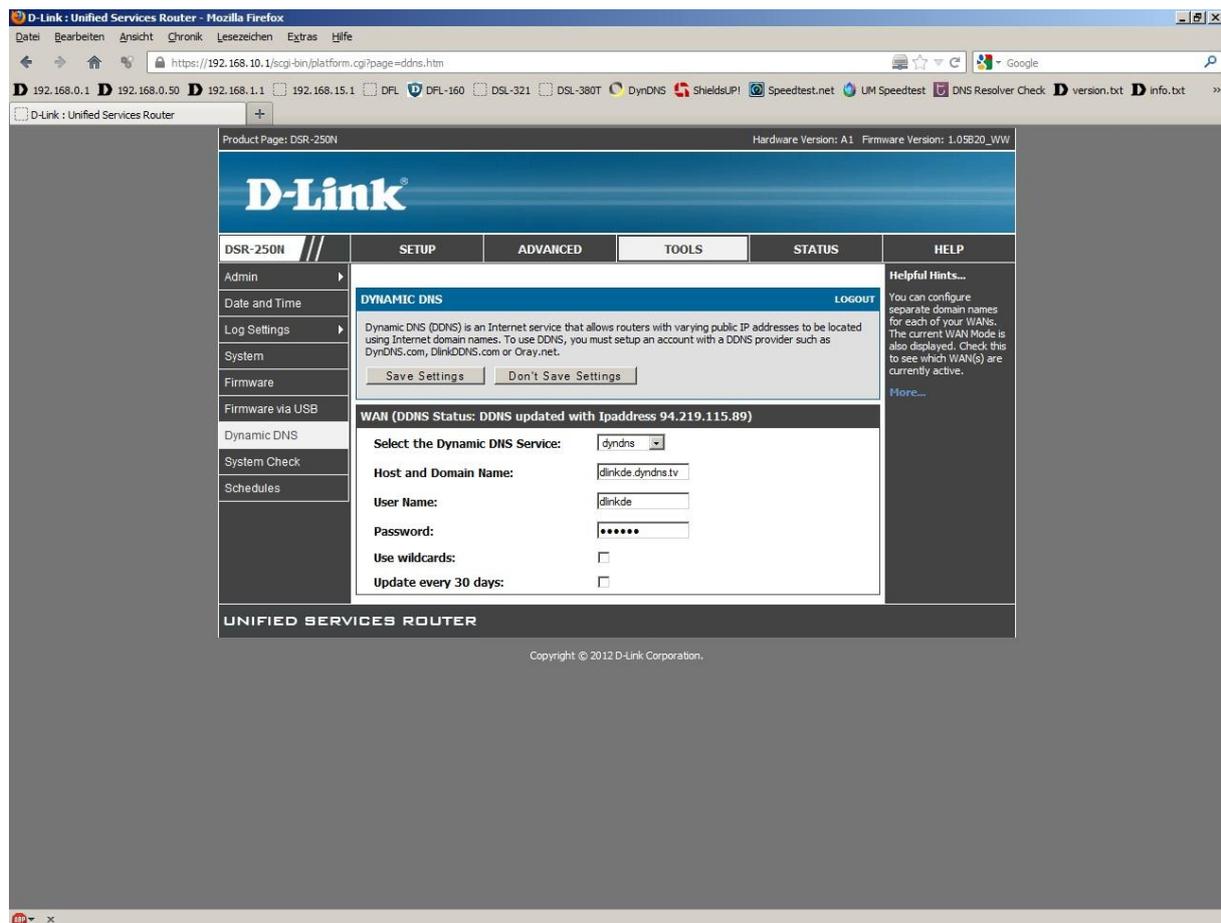
Below the table is a "Manual Policy" section with buttons for "Edit", "Enable", "Disable", "Delete", "Add", and "Export".

6. Soll der DSR selbst DynDNS Client sein, wählen Sie oben das Menü **Tools** und links **Dynamic DNS** aus.

Beachten Sie bitte die Anleitungen <ftp://ftp.dlink.de/anleitungen/ddns/dyndns.pdf> und <ftp://ftp.dlink.de/anleitungen/ddns/dlinkddns.pdf> bezüglich DynDNS.

- Wählen Sie bei Select **the Dynamic DNS Service** das **dyndns** aus.
- Tragen Sie bei **Host and Domain Name** Ihren bei dyndns.com oder dlinkddns.com erstellte Host Adresse ein.
- Tragen Sie bei **User Name** und **Password** Ihre Zugangsdaten ein, mit denen Sie sich auf der Webseite von dyndns.com oder dlinkddns.com anmelden.

Klicken Sie oben auf **Save Settings** um die Angaben zu übernehmen.



Stellen sie bitte sicher, dass Sie den Internetzugang im DSR ebenfalls eingerichtet haben und er online ist.

Der DSR ist damit für den Lan-to-Lan Internetzugang eingerichtet.

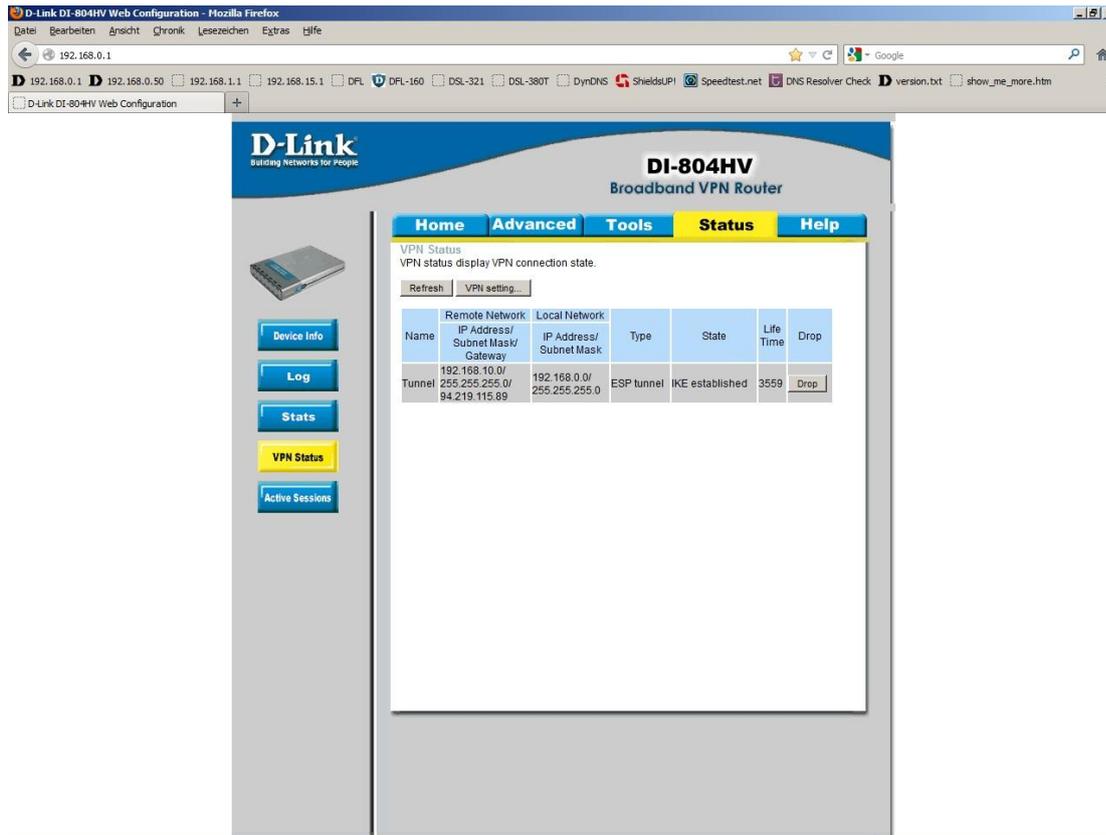
Überprüfung des Lan-to-Lan VPN-Tunnels zwischen dem DI-804HV und der DSR

In der Konfiguration des **DI-804HV** unter **Status – VPN Status** können Sie den Status (**State**) des Tunnels auslesen.

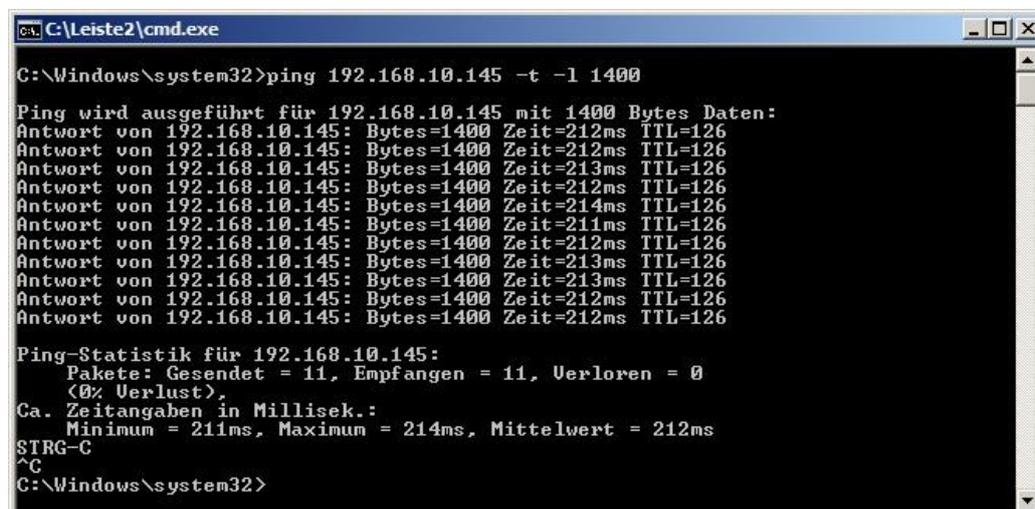
IKE established = der Tunnel ist verbunden

Idle = der Tunnel ist nicht aufgebaut und „wartet“ auf Aufbau.

Establishing = der Tunnel wird gerade versucht aufzubauen – Ist das ein Dauerzustand, stimmt in einen der beiden Geräten etwas mit den Einstellungen nicht – bitte entsprechend dieser Anleitung überprüfen!

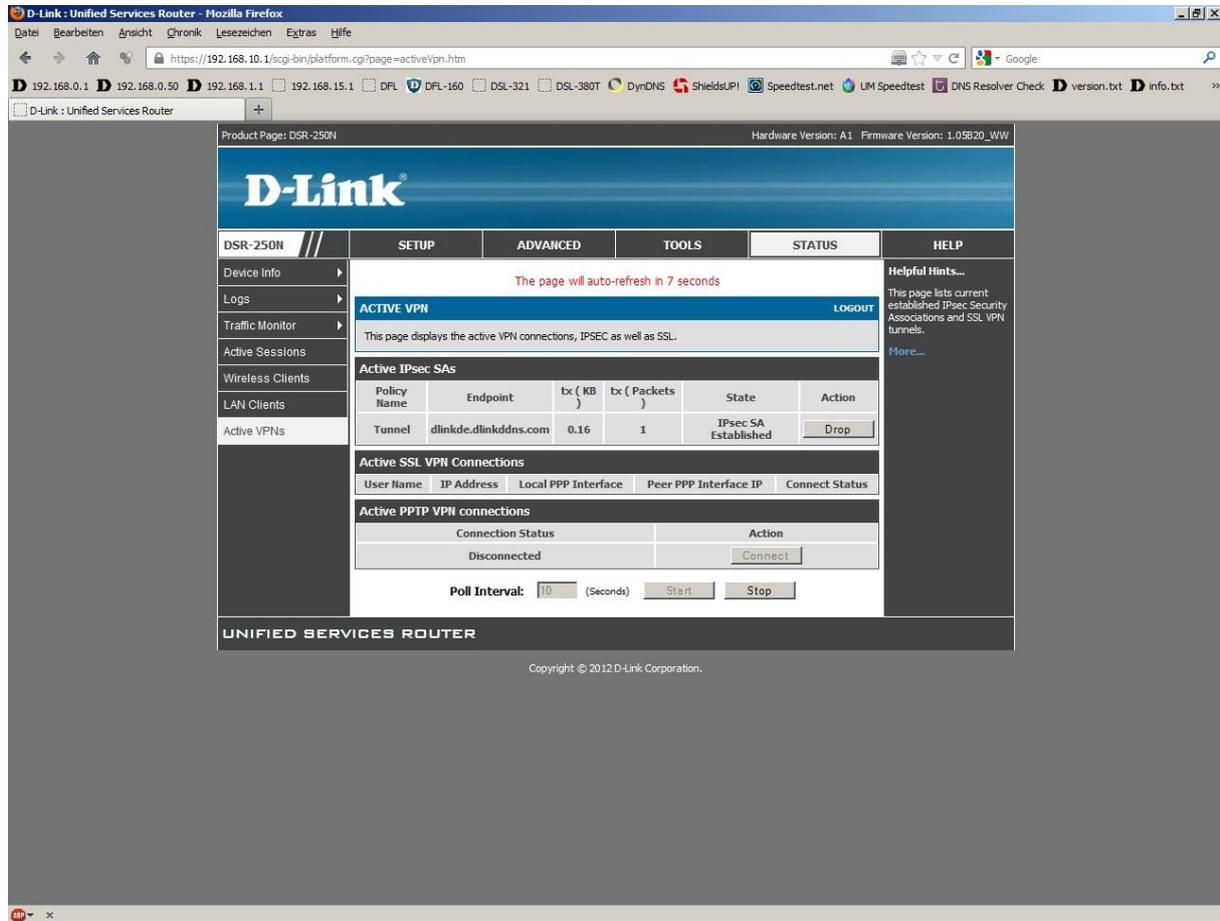


Steht der Tunnel (IKE established), können Sie einen Rechner auf der anderen Seite des Tunnels testweise anpingen.



In der Konfiguration der **DSR** unter **Status – Active VPNs** können Sie den Status (**State**) des Tunnels auslesen.

IPSec SA Established = der Tunnel ist verbunden



Steht der Tunnel, können Sie einen Rechner auf der anderen Seite des Tunnels testweise anpingen.

