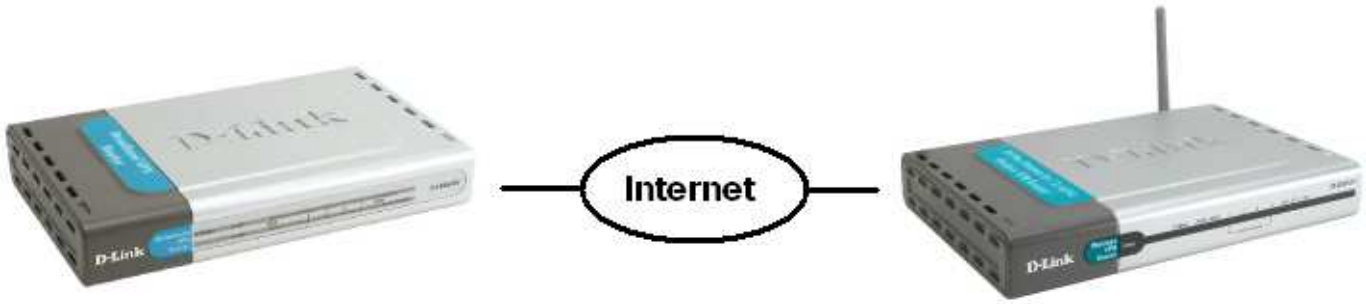
VPN IPSec Tunnel zwischen zwei DI-804HV / DI-824VUP+

Schritt für Schritt Anleitung

DI-804HV Firmwarestand 1.41b03
DI-824VUP+ Firmwarestand 1.04b02



Seite 1: Netz 192.168.0.0 / 24

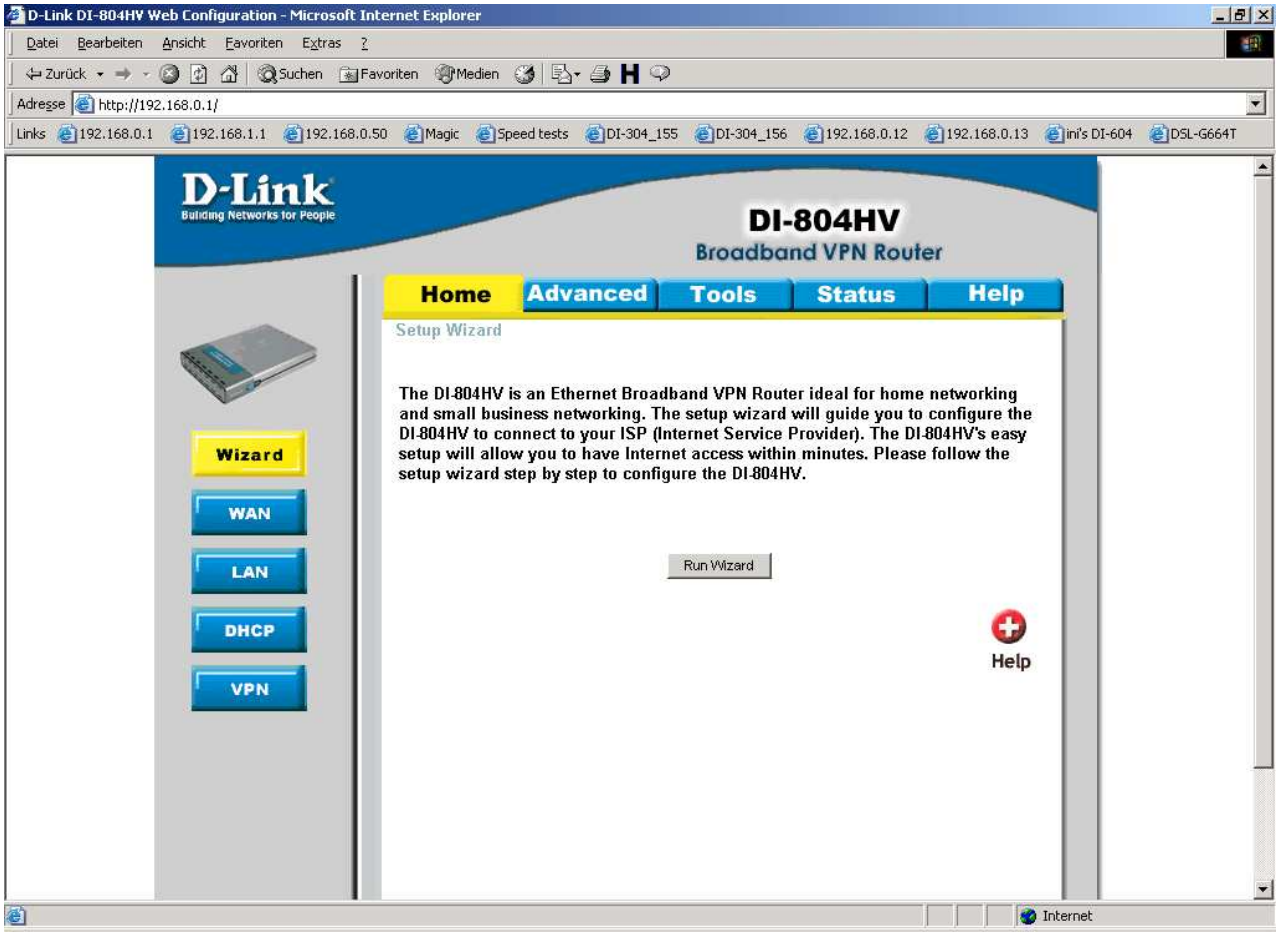
Seite 2: Netz 192.168.1.0 / 24

Wichtiger Hinweis: Die IP Netze beider Seiten müssen verschieden sein da sonst keine Kommunikation über den Tunnel erfolgen kann !

Eine Grundregel bei der Konfiguration eines „Lan to Lan“ Tunnels ist, dass die Sicherheitseinstellungen auf beiden Seiten identisch sein müssen. Entsprechende Hinweise finden Sie in dieser Anleitung.

Voraussetzung für diese Beispielkonfiguration ist eine bereits vollendete Einrichtung des Internetzugangs.

1. Greifen Sie auf die Konfiguration des Routers zu. Wählen Sie oben Home und links VPN aus.



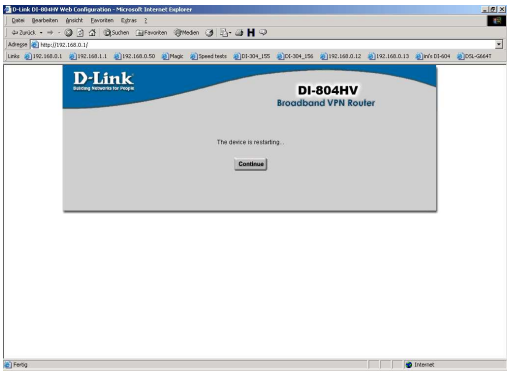
2. Setzen Sie rechts neben VPN und NetBIOS Broadcast bei Enable einen Haken.

3. Bei Max. numbers of tunnels lassen Sie 1 oder tragen eine höhere Zahl ein.

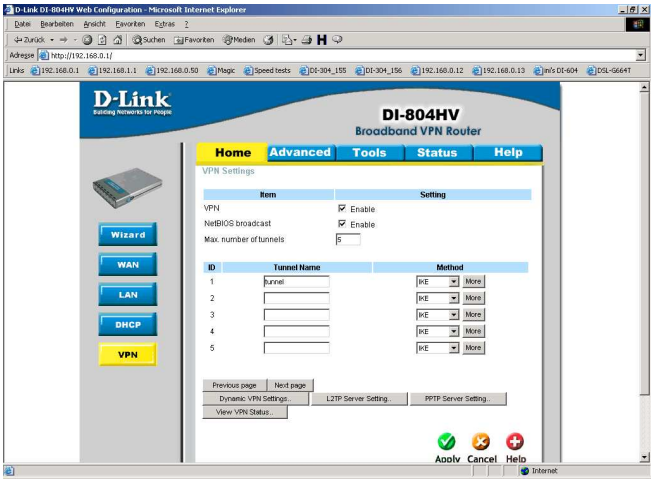
4. Unter Tunnel Name geben Sie dem Tunnel einen Namen.

5. Klicken Sie auf Apply

6. Klicken Sie auf Continue.



7. Wieder in diesem Fenster klicken Sie rechts bei ID1 und dem eingetragene Tunnel Namen auf More.

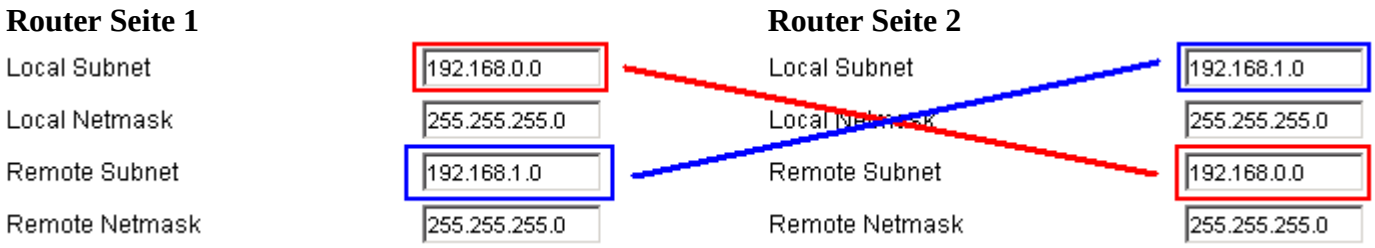


8. Der Aggressive Mode ist optional. Soll dieser verwendet werde, aktivieren Sie dies dann in beiden Routern.

9. Bei Local Subnet geben Sie das IP Netz auf der eigenen LAN-Seite des Routers ein, ebenso bei Local Netmask tragen Sie die zugehörige Subnet Maske ein.

10. Bei Remote Subnet tragen Sie das IP Netz auf der Seite des gegenüberliegenden Routers ein, ebenfalls bei Remote Netmask die zugehörige Subnet Maske.

Achtung: Die Angaben zum Local und Remote Subnet der Punkte 8. und 9. sind in beiden Routern „vertauscht“ einzugeben.



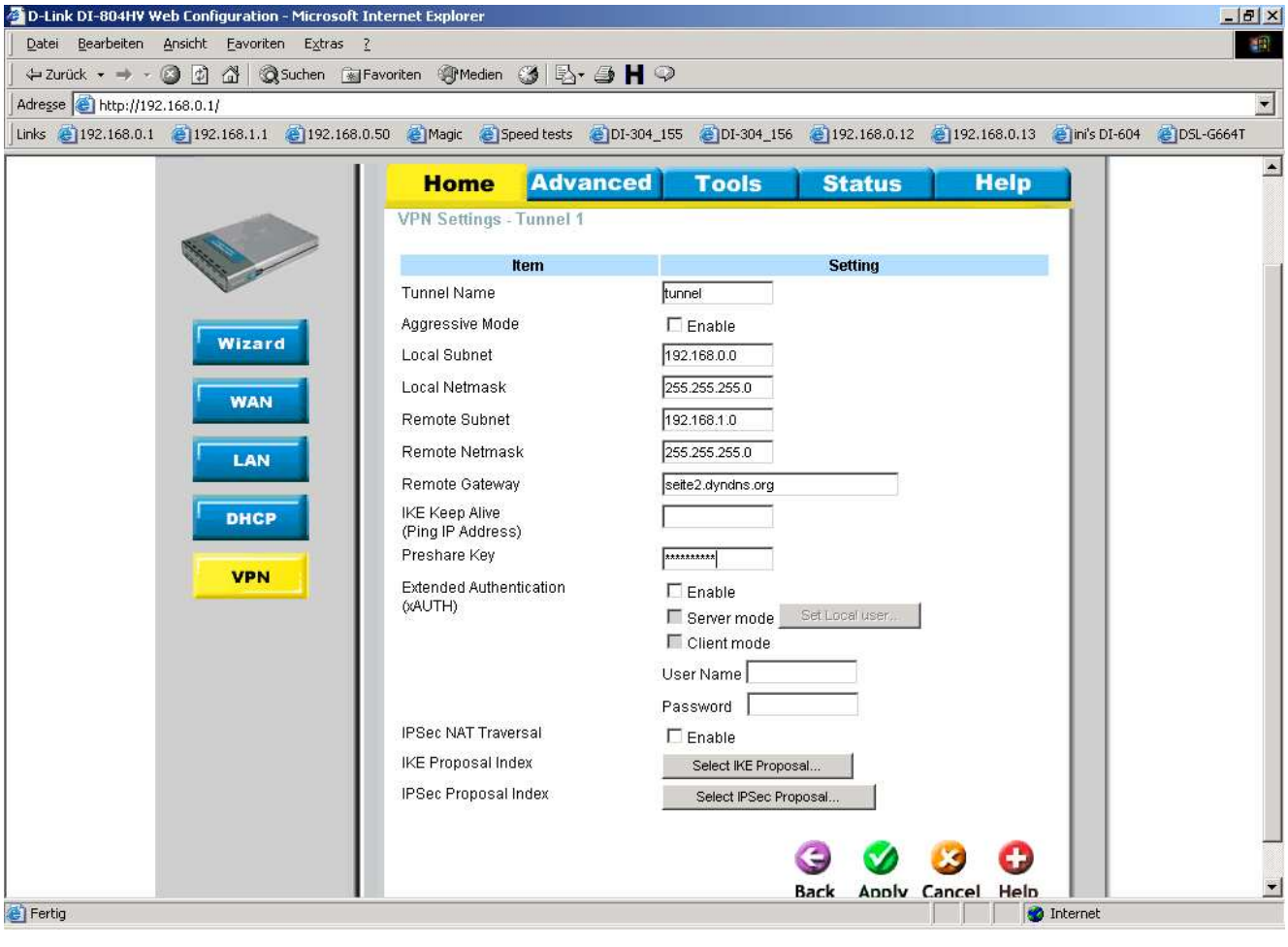
11. Bei Remote Gateway geben Sie die WAN IP Adresse des gegenüberliegenden Routers ein. Dies kann auch eine DynDNS Adresse sein. Mehr dazu unter Konfigurationspunkt 36.

12. Bei Preshare Key tragen Sie einen max. 63 Stellen langen ASCII Schlüssel ein.
Dieser muss in beiden Routeren identisch eingegeben werden !!!

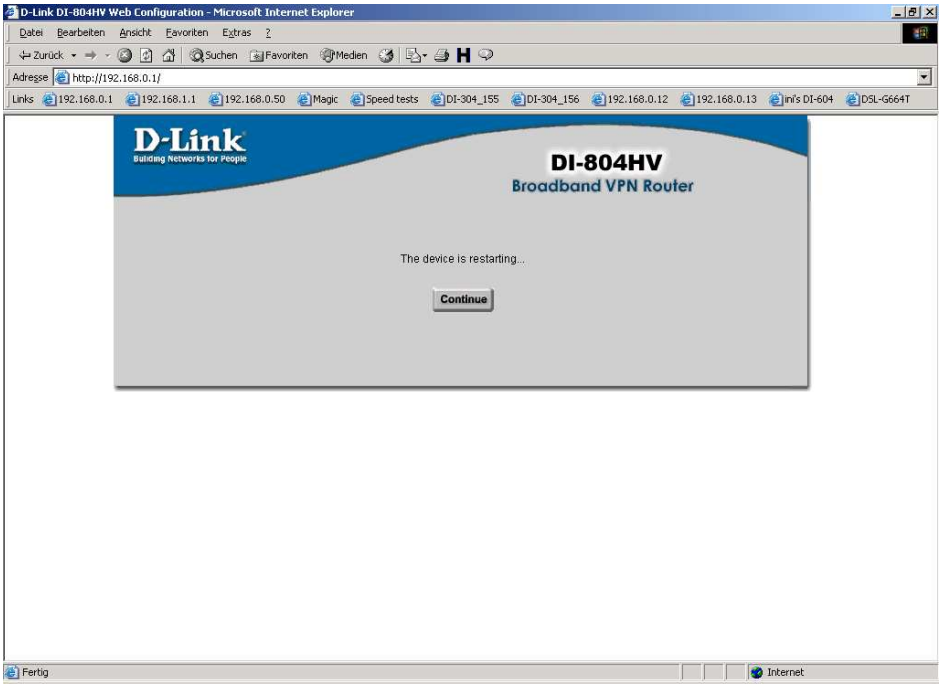
13. Die Extended Authentication (xAUTH) ist optional. Mehr dazu unter 17. (a.-h.). Sonst weiter bei 18.

14. IPSec Nat Traversal ist optional.

15. Klicken Sie auf Apply.



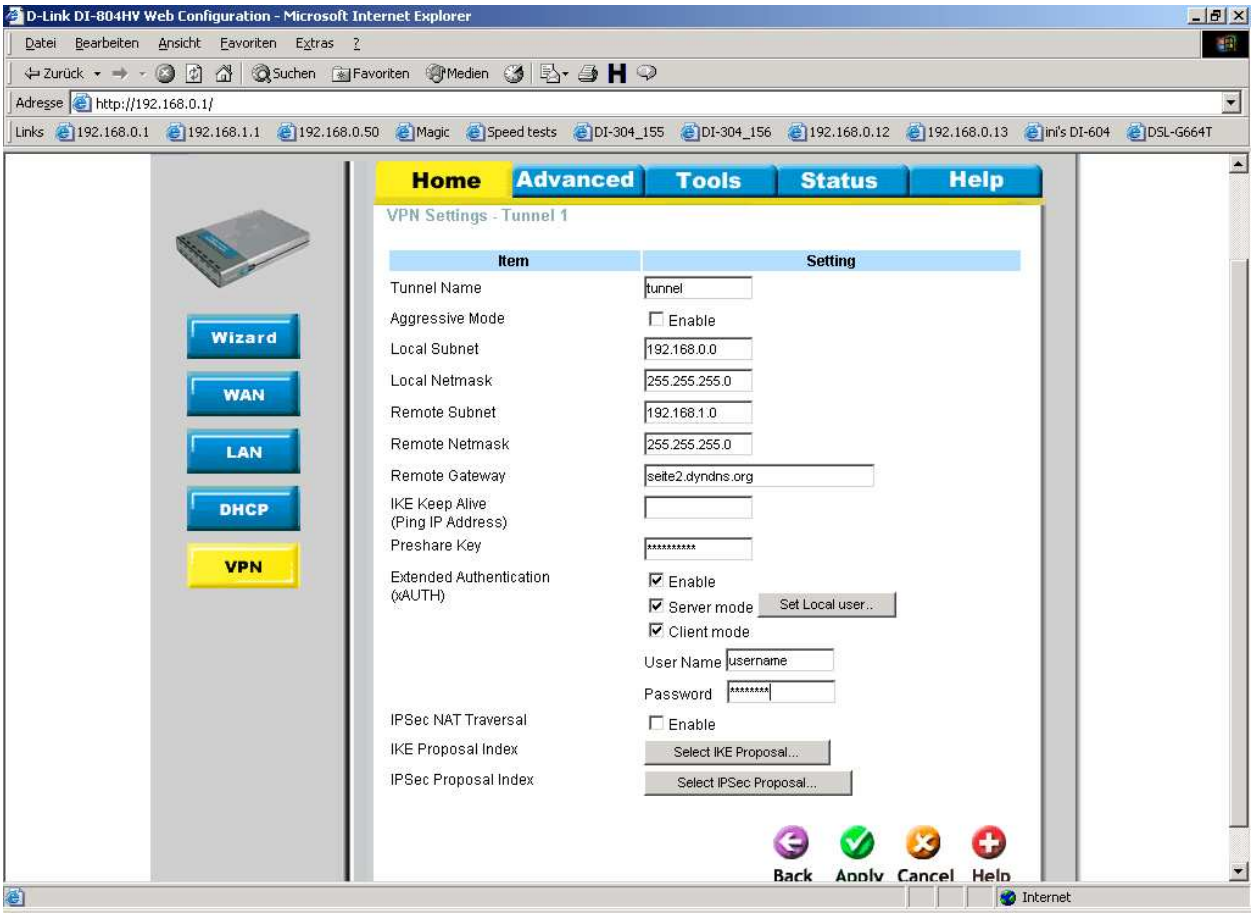
16. Klicken Sie auf Continue.



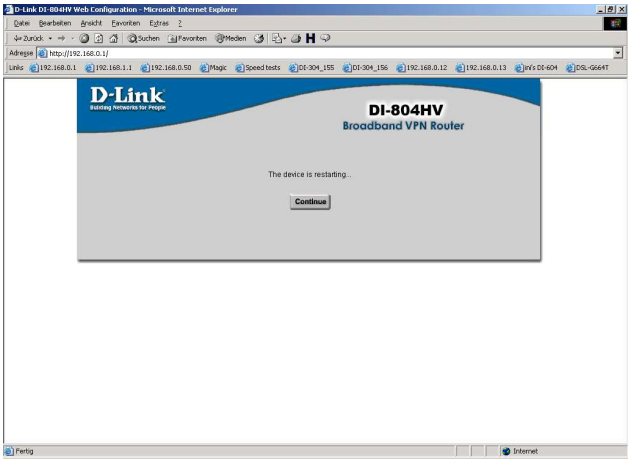
17. **Hinweise zum xAUTH:**
Die Extended Authentication ist eine weitere Möglichkeit für mehr Sicherheit beim Tunnelaufbau.
Dabei wird ein Username und Passwort übertragen und von der Gegenseite überprüft.

Wenn Sie dies Nutzen möchten muss dies in beiden Routern konfiguriert werden. Gehen Sie wie folgt vor:

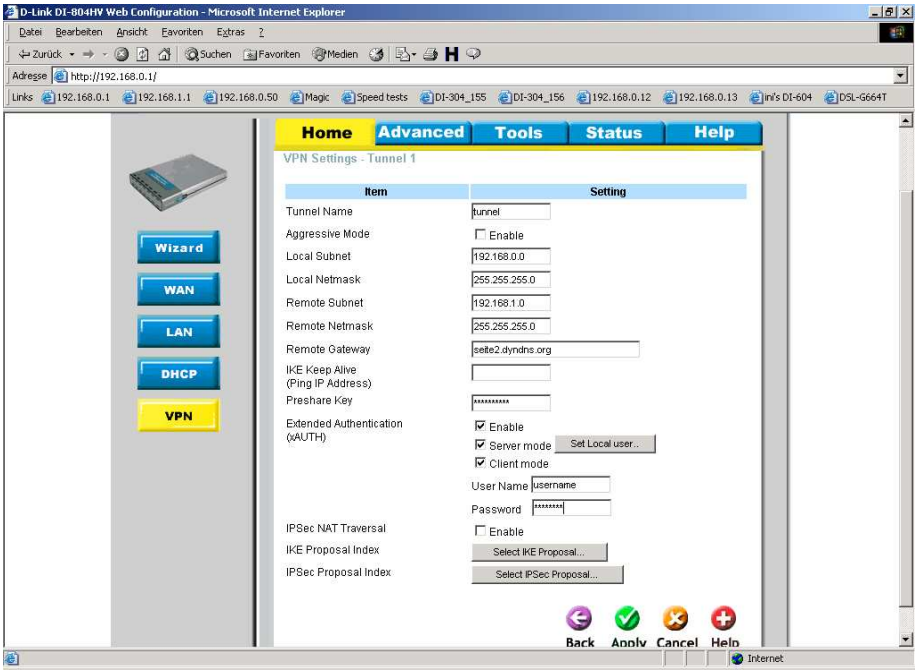
a. Setzen Sie bei Enable, Server Mode und Client Mode einen Haken.
b. Geben Sie bei Username und Password die Zugangsdaten ein die an die Gegenseite gesendet werden sollen.
c. Klicken Sie auf Apply



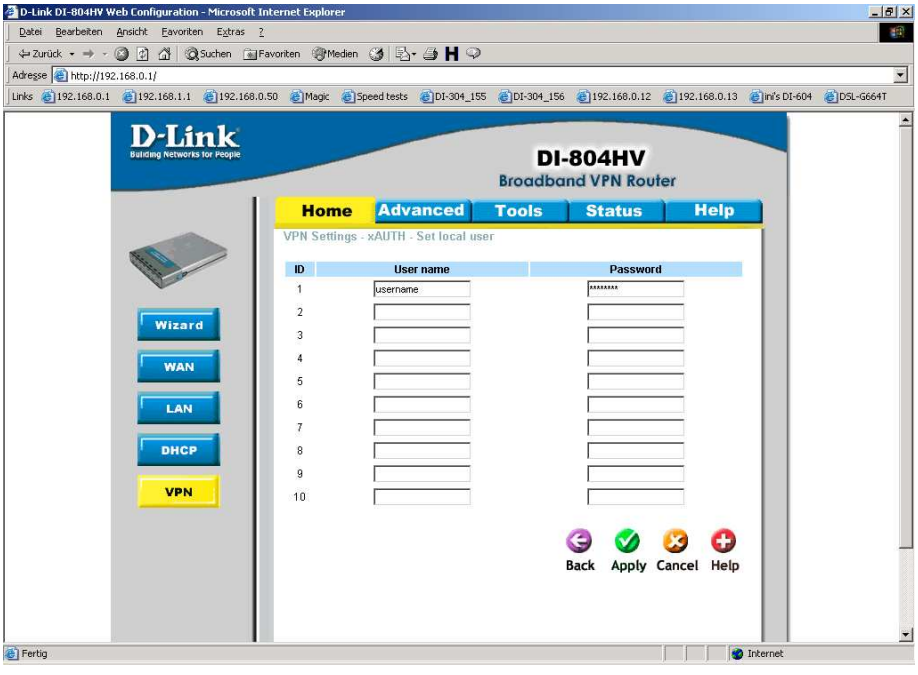
d. klicken Sie auf Continue.



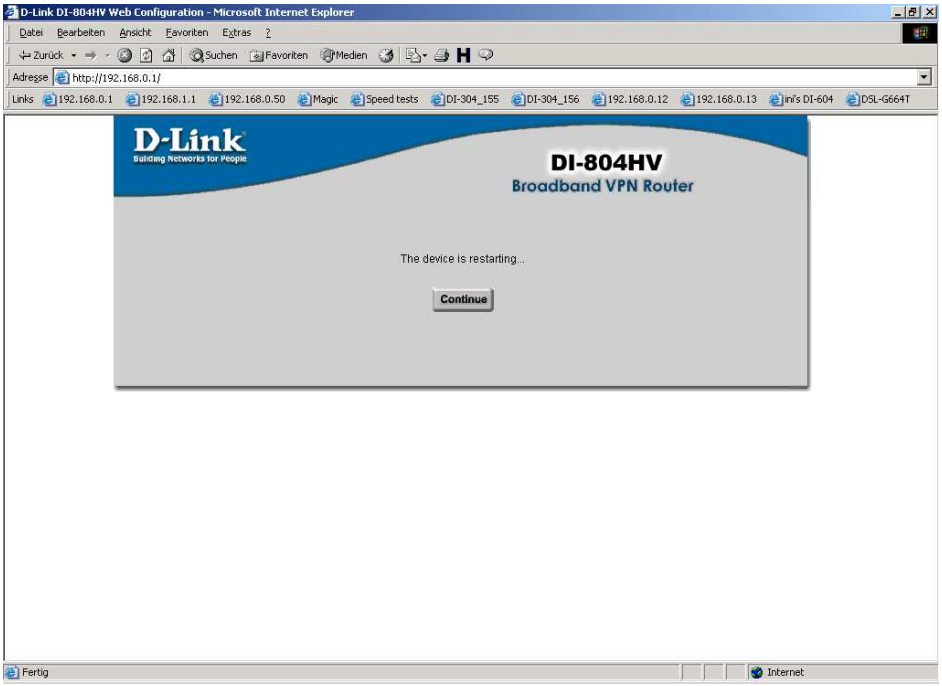
e. Wieder zurück in dem Fenster klicken Sie auf Set Local user.



f. Geben Sie Bei Username und Password die Zugangsdaten ein mit dem sich die Gegenseite authentifizieren muss.
g. Klicken Sie auf Apply.

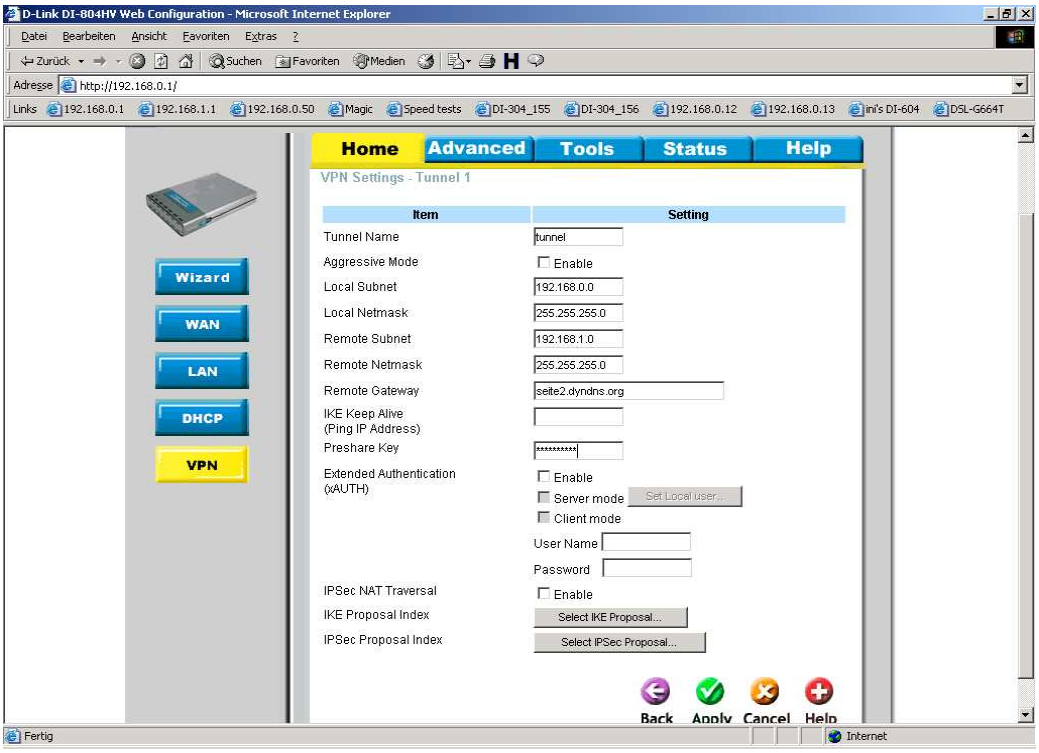


h. Klicken Sie auf Continue **und dann auf Back.**



Die folgenden Konfigurationspunkte 18. – 35. müssen auf beiden Seiten absolut identisch vorgenommen werden !!!

18. Klicken Sie unten auf Select IKE Proposal.



18. Vergeben Sie unter Proposal Name einen Namen.

19. Bei DH Group wählen Sie eine Diffi Hellman Gruppe aus, z.B. Group 2 .

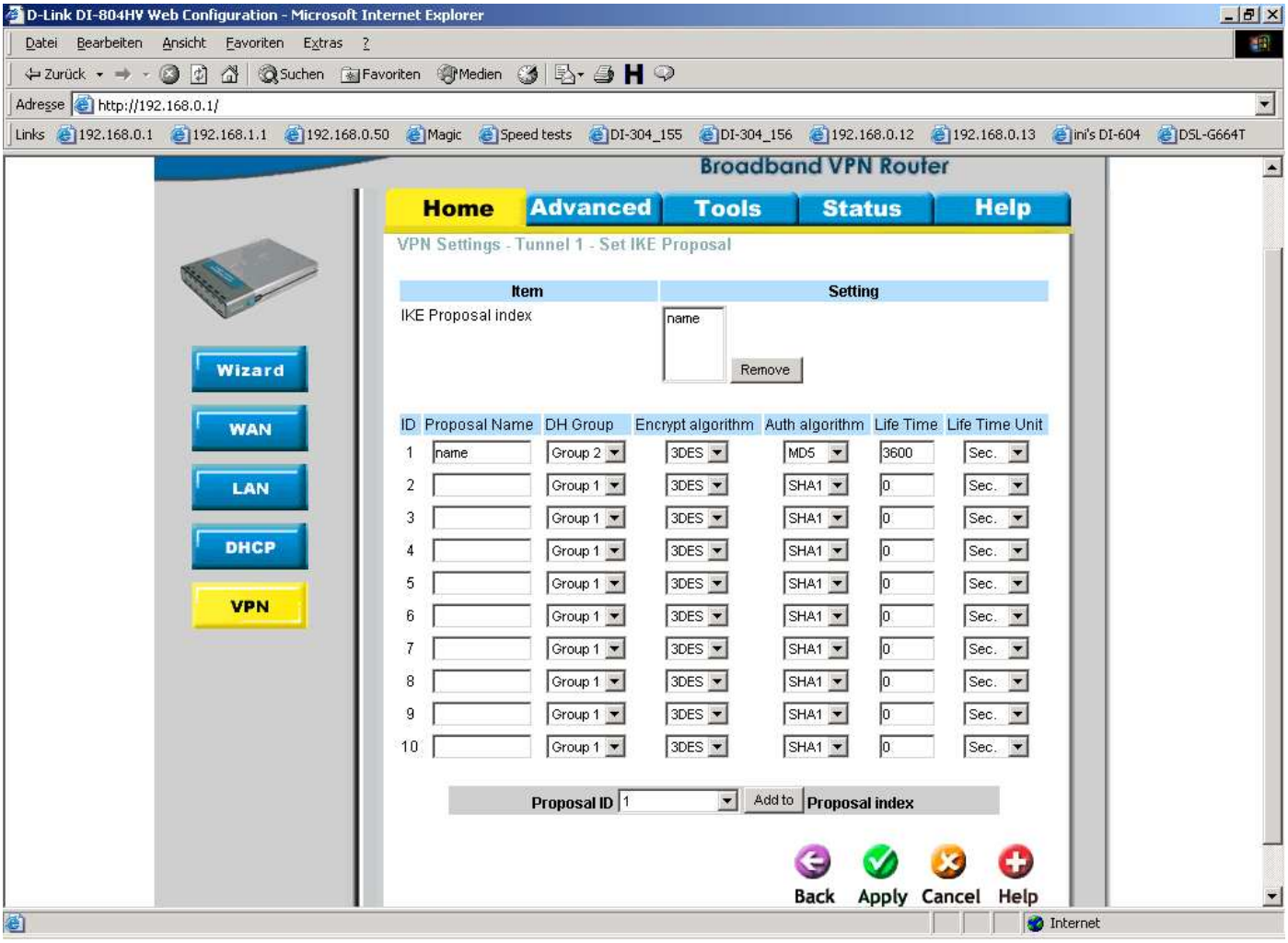
20. Wählen Sie einen Encrypt algorithm aus, z.B. 3DES .

21. Wählen Sie einen Auth. algorithm aus, z.B. MD5 .

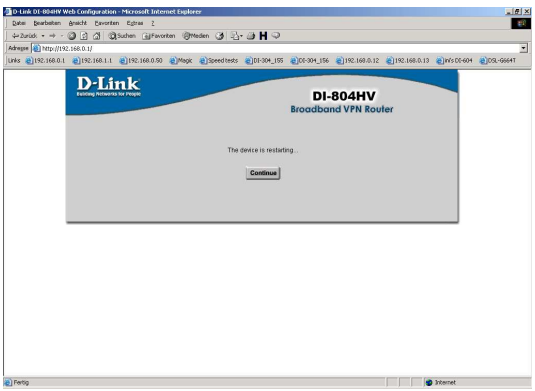
22. Geben Sie eine Life Time für die IKE Proposal ein, z.B. 3600 Sec.

23. Unten Wählen Sie bei Proposal ID die 1 aus und klicken auf Add to um die Einstellungen in den IKE Proposal index (oben) zu übernehmen.
Dieser Schritt ist wichtig und wird leider nicht selten übersehen !

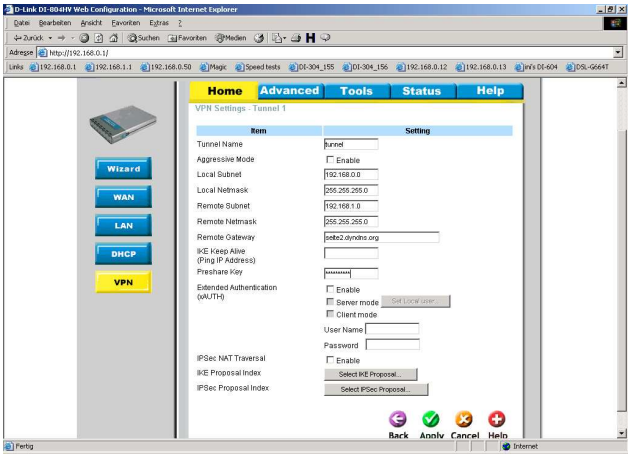
24. Klicken Sie auf Apply



25. Klicken Sie auf Continue **und dann auf Back.**



26. Klicken Sie unten auf Select IPSec Proposal.



27. Vergeben Sie unter Proposal Name einen Namen.

28. Bei DH Group wählen Sie eine Diffi Hellman Gruppe aus, z.B. Group 2 .

29. Wählen Sie ein Encap protocol aus, z.B. ESP .

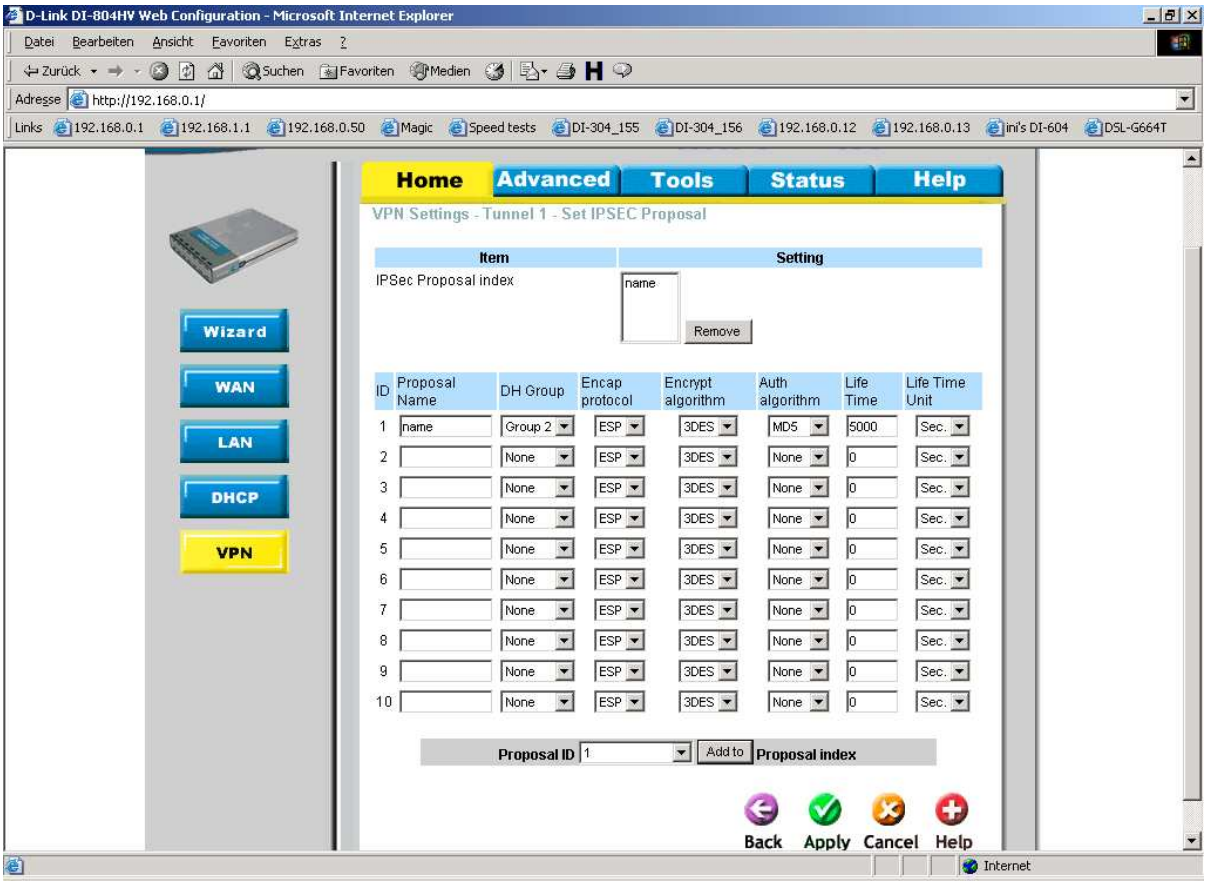
30. Wählen Sie einen Encrypt algorithm aus, z.B. 3DES .

31. Wählen Sie einen Auth. algorithm aus, z.B. MD5 .

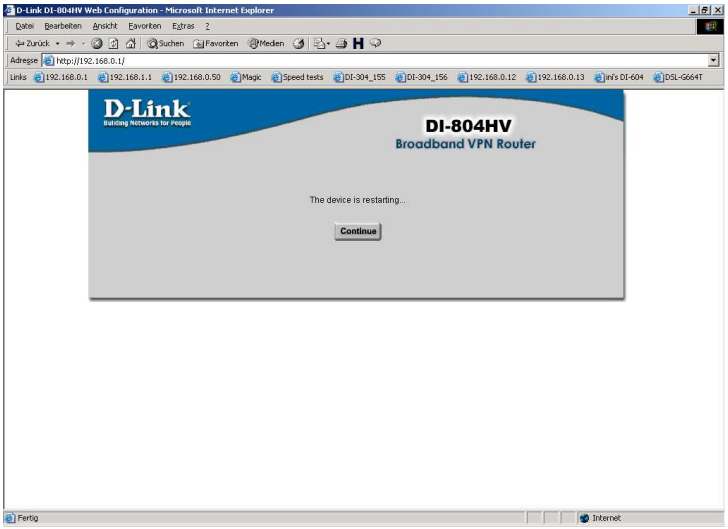
32. Geben Sie eine Life Time für die IPSec Proposal ein, z.B. 5000 Sec.

33. Unten Wählen Sie bei Proposal ID die 1 aus und klicken auf Add to um die Einstellungen in den IPSec Proposal index (oben) zu übernehmen.
Dieser Schritt ist wichtig und wird leider nicht selten übersehen !

34. Klicken Sie auf Apply

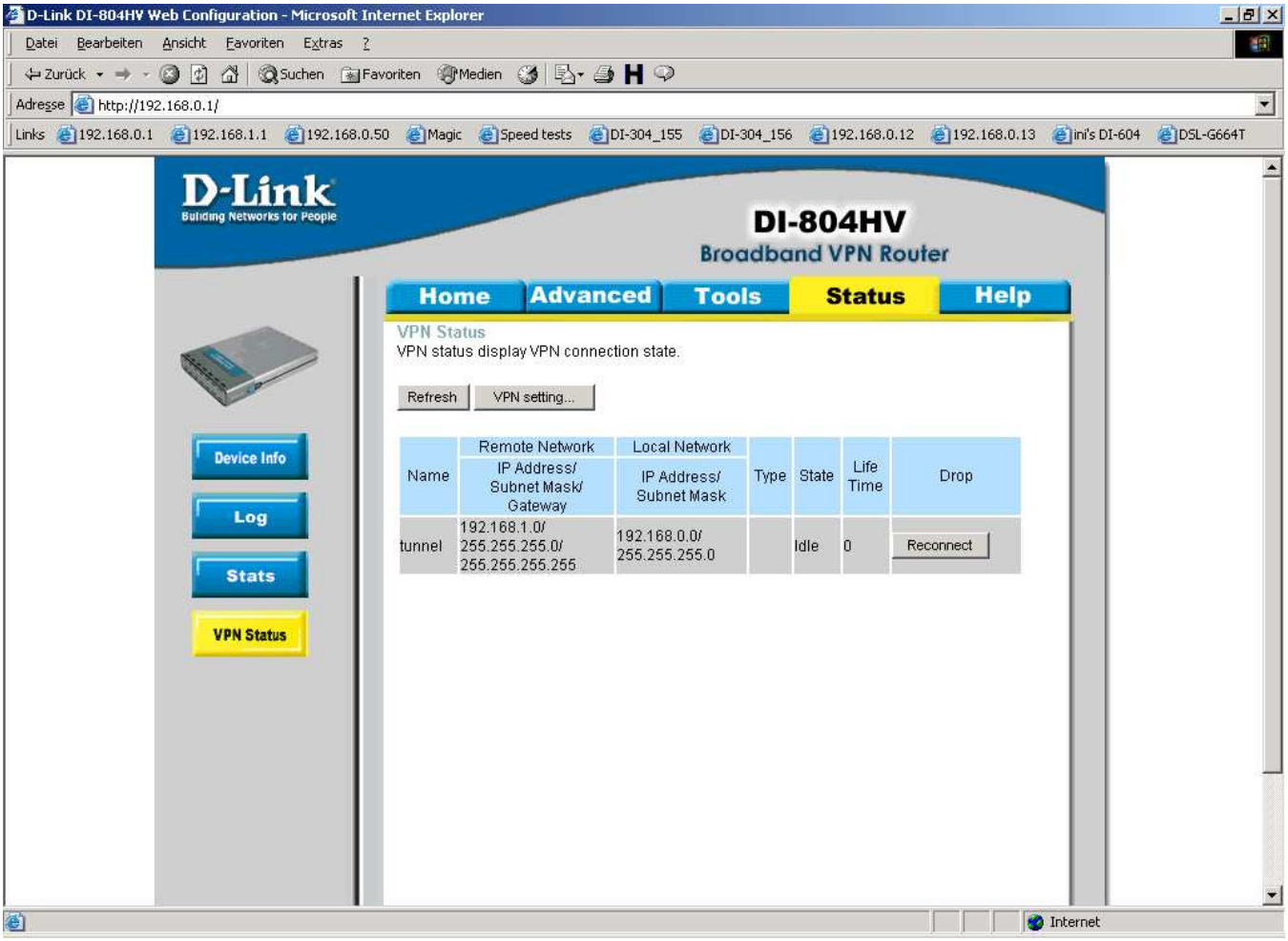


35. Klicken Sie auf Continue.



Damit ist die Konfiguration des Tunnels abgeschlossen.

Unter Staus – VPN Status bekommen Sie den Zustand des Tunnels angezeigt.

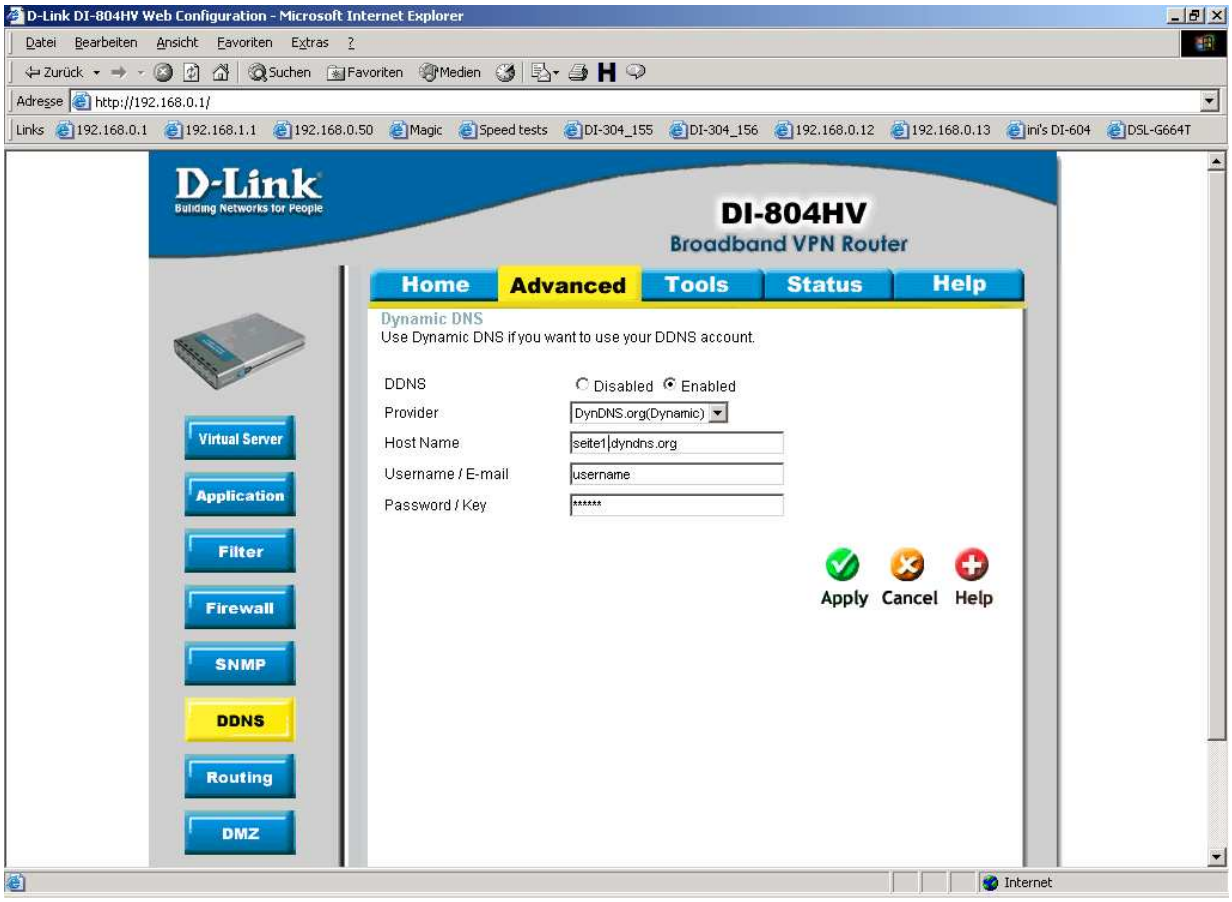


36. **DynDNS**

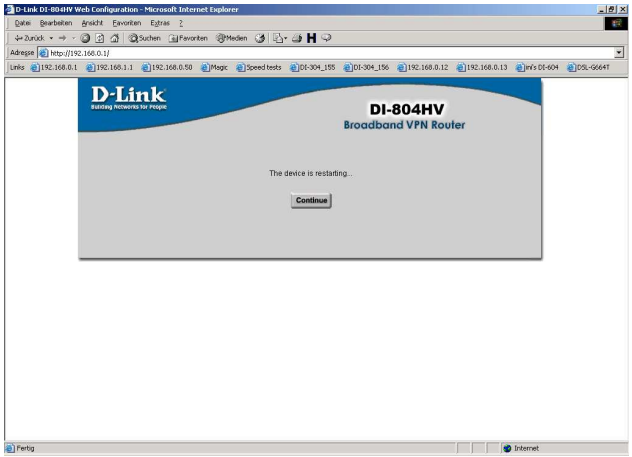
Voraussetzung für die Nutzung des DynDNS Features im Router ist
- eine abgeschlossene Registrierung beim DynDNS Provider.
- die erfolgte Hinzufügung eines Hosts beim DynDNS Provider.

Nachfolgend die Beispielkonfiguration der DynDNS Einstellungen im DI-804HV / DI-824VUP+.

a. Klicken Sie in der Konfiguration des Routers oben auf Advanced und links auf DDNS.
b. Markieren Sie Enabled um die Funktion zu aktivieren.
c. Bei Provider wählen Sie DynDNS.org (Dynamic) aus.
d. Bei Host Name tragen Sie den unter http://www.dyndns.org hinzugefügten Host ein, z.B. seite1.dyndns.org .
e. Tragen Sie bei Username und Password Ihre Zugangsdaten Ihres Account bei http://www.dyndns.org ein.
f. Klicken Sie auf Apply.



g. Klicken Sie auf Continue.



Damit ist die DynDNS Konfiguration im Router abgeschlossen.