

Konfiguration eines Lan-to-Lan VPN Tunnels

(Für DI-804HV/DI-824VUP+ zusammen mit DFL-210/260/800/860/1600/2500)

Zur Konfiguration eines Lan-to-Lan VPN Tunnels zwischen z.B. DI-804HV und DFL-800 gehen Sie bitte folgendermaßen vor.

Dies ist lediglich eine Beispielkonfiguration.

Bei der Erwähnung des DI-804HV entspricht dies dem DI-824VUP+.

Bei der Erwähnung der DFL- 800 entspricht dies der DFL-210, 260, 860, 1600 und 2500.

Konfiguration des VPN Tunnels im DI-804HV:

1. Unter Home – VPN markieren Sie „VPN“ und tragen bei „Max. numbers of tunnels“ eine 1 oder höher ein. Wir empfehlen eine 2, da wenn der Tunnel mal unterbrocht kann parallel zum abgebrochenen (für den DI-804HV vielleicht noch scheinbar vorhandenen) Tunnel ein neuer aufgebaut werden.

2. Bei der ID 1 vergeben Sie dem Tunnel einen Namen und klicken auf Apply.

D-Link DI-804HV Web Configuration – Microsoft Internet Explorer

Adresse: http://192.168.0.1/

Links: 192.168.0.1, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.50, 192.168.1.1, 192.168.15.1, DSL-321, DSL-380T

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input 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

Previous page Next page

Dynamic VPN Settings.. L2TP Server Setting.. PPTP Server Setting..

View VPN Status..

http://192.168.0.1/jpad.htm

3. Nachdem der DI-804HV neu gestartet ist klicken Sie unter Home – VPN rechts von der ID 1 auf „More“.

- Local Subnet = Das LAN IP Netz des DI-804HV, z.B. 192.168.65.0
- Local Netmask = Die LAN Subnet Maske des DI-804HV, i.d.R. 255.255.255.0
- Remote Subnet = Das LAN IP Netz der DFL-800, z.B. 192.168.60.0
- Remote Netmask = Die LAN Subnet Maske der DFL-800, z.B. 255.255.255.0
- Remote Gateway = Die WAN IP Adresse der DFL-800 oder deren DynDNS Adresse.

- Bei Preshare Key tragen Sie den Preshare Key für die Authentifizierung des VPN Tunnels ein. Merken (notieren) Sie sich diesen Preshare Key.

Erlaubt ist eine Kombination aus Zahlen und Buchstaben, allerdings keine Sonderzeichen.

- Klicken Sie auf Apply.

D-Link DI-804HV Web Configuration - Microsoft Internet Explorer

Adresse <http://192.168.0.1/>

Links 192.168.0.1 192.168.0.12 192.168.0.13 192.168.0.14 192.168.0.15 192.168.0.50 192.168.1.1 192.168.15.1 DSL-321 DSL-380T

Wizard
WAN
LAN
DHCP
VPN

Tunnel Name

Aggressive Mode Enable

Local Subnet

Local Netmask

Remote Subnet

Remote Netmask

Remote Gateway

IKE Keep Alive (Ping IP Address)

Preshare Key

Extended Authentication (AAUTH) Enable

Server mode

Client mode

User Name

Password

IPsec NAT Traversal Enable

Auto-reconnect Enable

Remote ID Type

Value

Local ID Type

Value

IKE Proposal Index

IPsec Proposal Index

Fertig Internet

4. Nachdem der DI-804HV neu gestartet ist klicken Sie unter Home – VPN rechts von der ID 1 auf „More“ und dann unten auf „Select **IKE Proposal**“.

- Vergeben Sie der Proposal 1 einen Namen.
- DH Group = Group 5
- Encrypt algorithm = 3DES
- Auth algorithm = SHA1
- Life Time = 28800

- Wählen Sie nun unten im Aufklappmenü die Proposal ID 1 aus und klicken auf “Add to”.

- Klicken Sie auf Apply.

D-Link DI-804HV Web Configuration - Microsoft Internet Explorer

Adresse: http://192.168.0.1/

Home Advanced Tools Status Help

VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
IKE Proposal index	IKE1

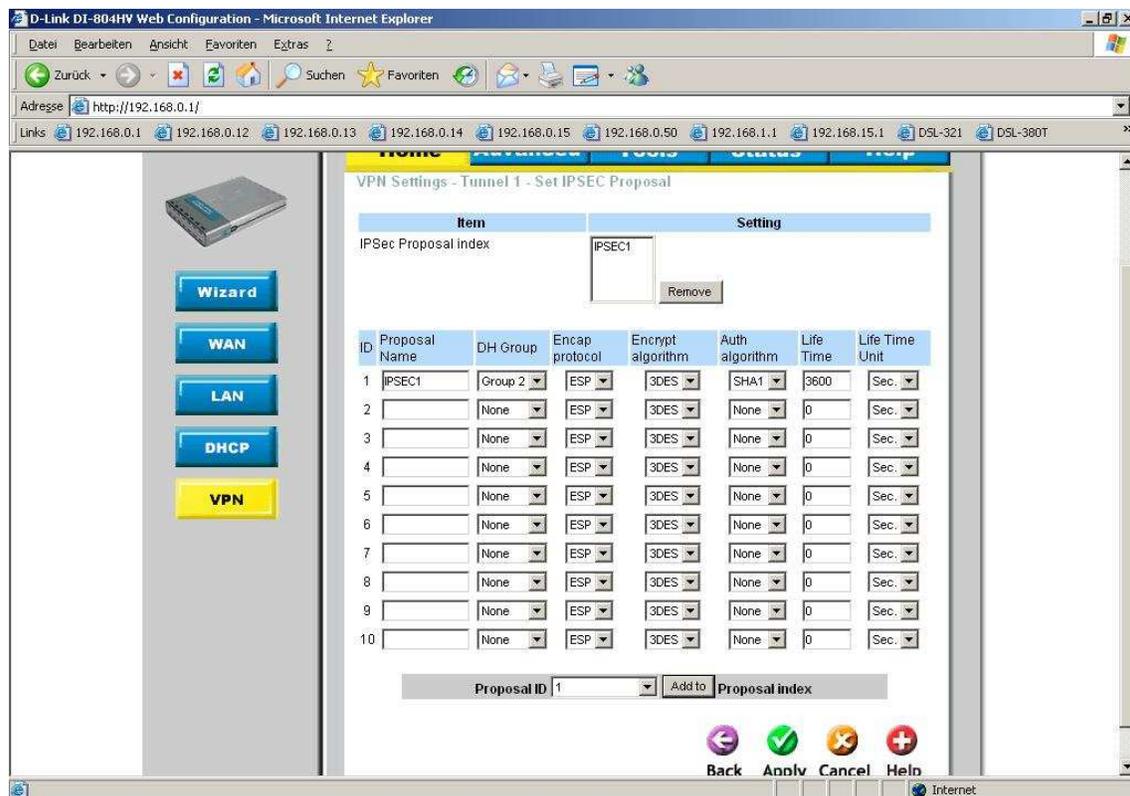
ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE1	Group 5	3DES	SHA1	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Proposal ID: 1 Add to Proposal index

Back Apply Cancel Help

5. Nachdem der DI-804HV neu gestartet ist klicken Sie unter Home – VPN rechts von der ID 1 auf „More“ und dann unten auf „Select IPsec Proposal“.

- Vergeben Sie der Proposal 1 einen Namen.
 - DH Group = Group 2
 - Encap protocol = ESP
 - Encrypt algorithm = 3DES
 - Auth algorithm = SHA1
 - Life Time = 3600
- Wählen Sie nun unten im Aufklappmenü die Proposal ID 1 aus und klicken auf “Add to”.
- Klicken Sie auf Apply.



Damit ist die VPN Tunnel-Konfiguration im DI-804HV abgeschlossen.

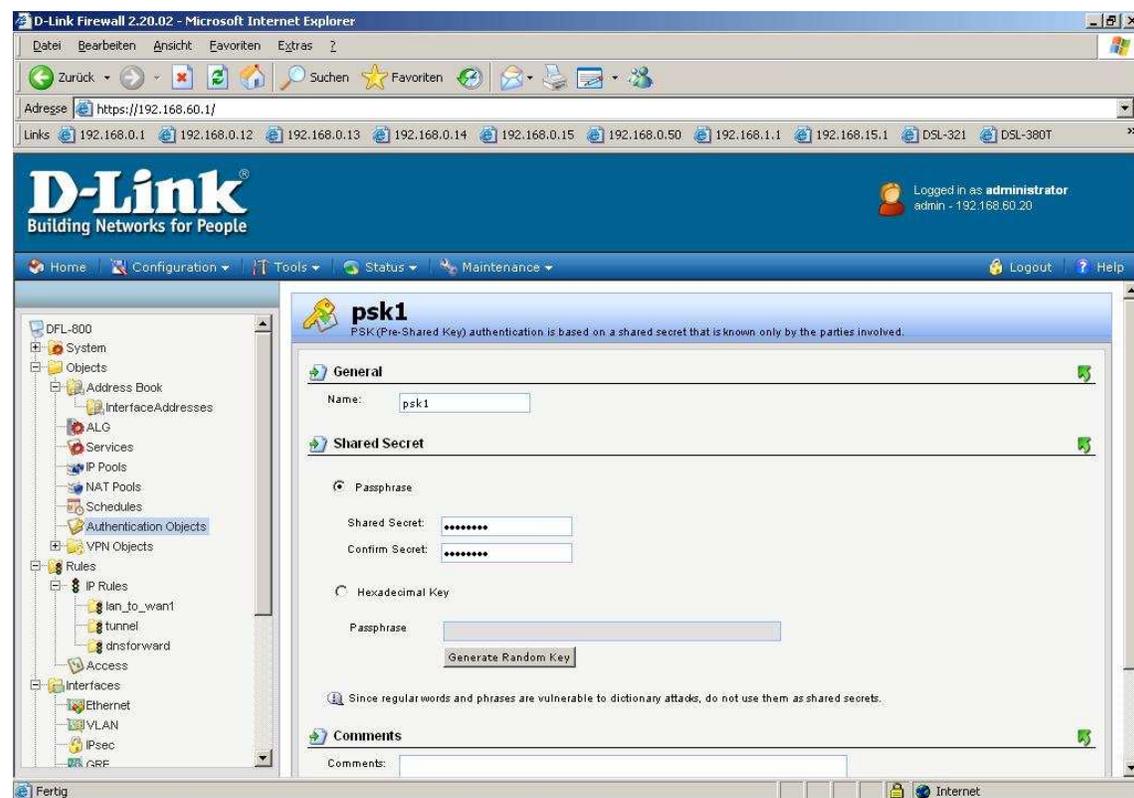
Konfiguration des VPN Tunnels in der DFL-800:

6.

Unter Objects – Authentication Objects klicken Sie auf Add und wählen Pre-shared key aus.

- Vergeben Sie einen Namen, z.B. **psk1**
- Bei Shared Secret und Confirm Secret geben Sie nun den Preshare Key für die Authentifizierung der VPN Tunnels ein. Dies muss der gleiche wie zuvor DI-804HV konfigurierte Schlüssel sein (siehe 3.)

Klicken Sie auf OK.



7. Unter Objects – Address Book – InterfaceAddresses klicken Sie auf Add, wählen IP Address aus und erstellen ein Objekt für das Remote Net.

- Name = z.B. remotenet
- IP Address = Das LAN IP Netz des DI-804HV, z.B. 192.168.65.0/24

Klicken Sie auf OK.

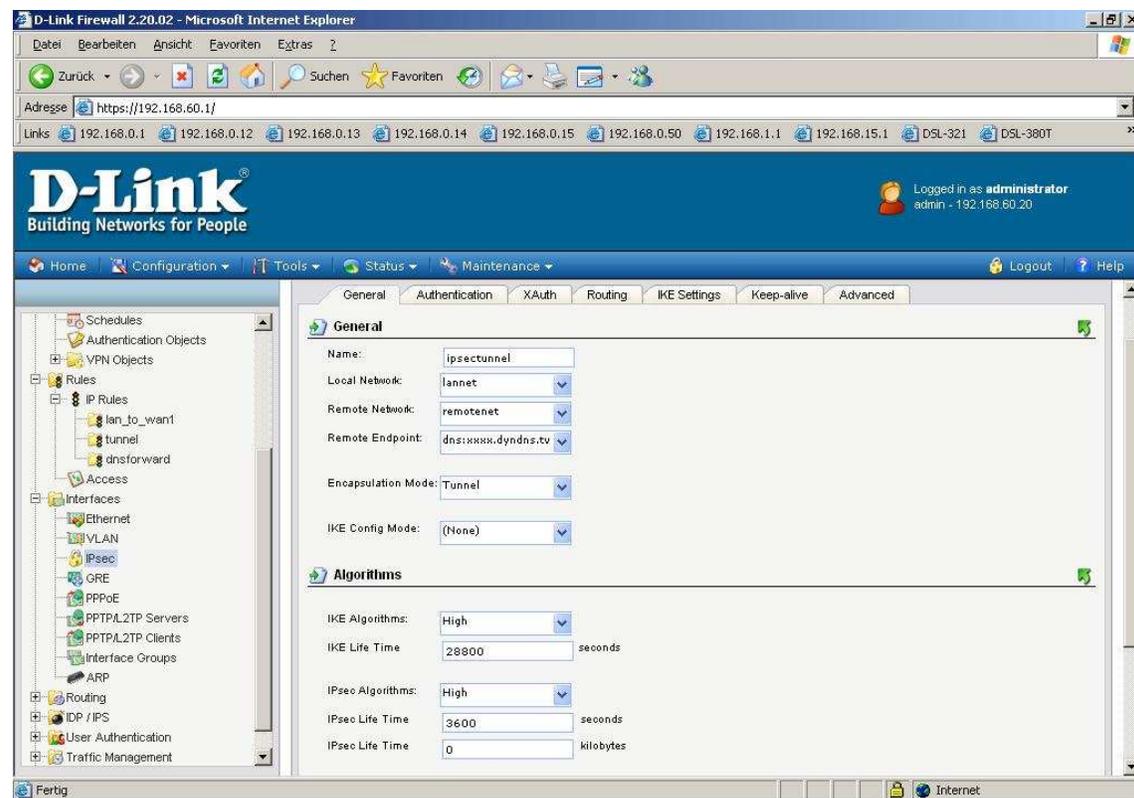
The screenshot shows the D-Link Firewall 2.20.02 web interface in Microsoft Internet Explorer. The browser address bar shows 'https://192.168.60.1/'. The interface is logged in as 'administrator' with IP '192.168.60.20'. The main content area is titled 'InterfaceAddresses' and contains a table of existing address objects. A new object named 'remotenet' with IP address '192.168.65.0/24' has been added. The table has columns for Name, Address, User Auth Groups, and Comments.

Name	Address	User Auth Groups	Comments
dmz_ip	172.17.100.254		IPAddress of interface dmz
dmznet	172.17.100.0/24		The network on interface dmz
lan_ip	192.168.60.1		IPAddress of interface lan
lanet	192.168.60.0/24		The network on interface lan
remotenet	192.168.65.0/24		
wan1_br	0.0.0.0		Broadcast address for interface wan1.
wan1_dns1	0.0.0.0		Primary DNS server for interface wan1.
wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1.
wan1_gw	0.0.0.0		Default gateway for interface wan1.
wan1_ip	0.0.0.0		IPAddress of interface wan1
wan1_phys_gw	0.0.0.0		Default gateway for interface wan1_phys.
wan1_phys_ip	0.0.0.0		IP address for interface wan1_phys.
wan1_physnet	0.0.0.0/0		Network for interface wan1_phys.
wan1net	0.0.0.0/0		The network on interface wan1
wan2_ip	192.168.120.254		IPAddress of interface wan2
wan2net	192.168.120.0/24		The network on interface wan2

8. Unter Interfaces – IPsec klicken Sie auf Add und wählen IPsec Tunnel aus.

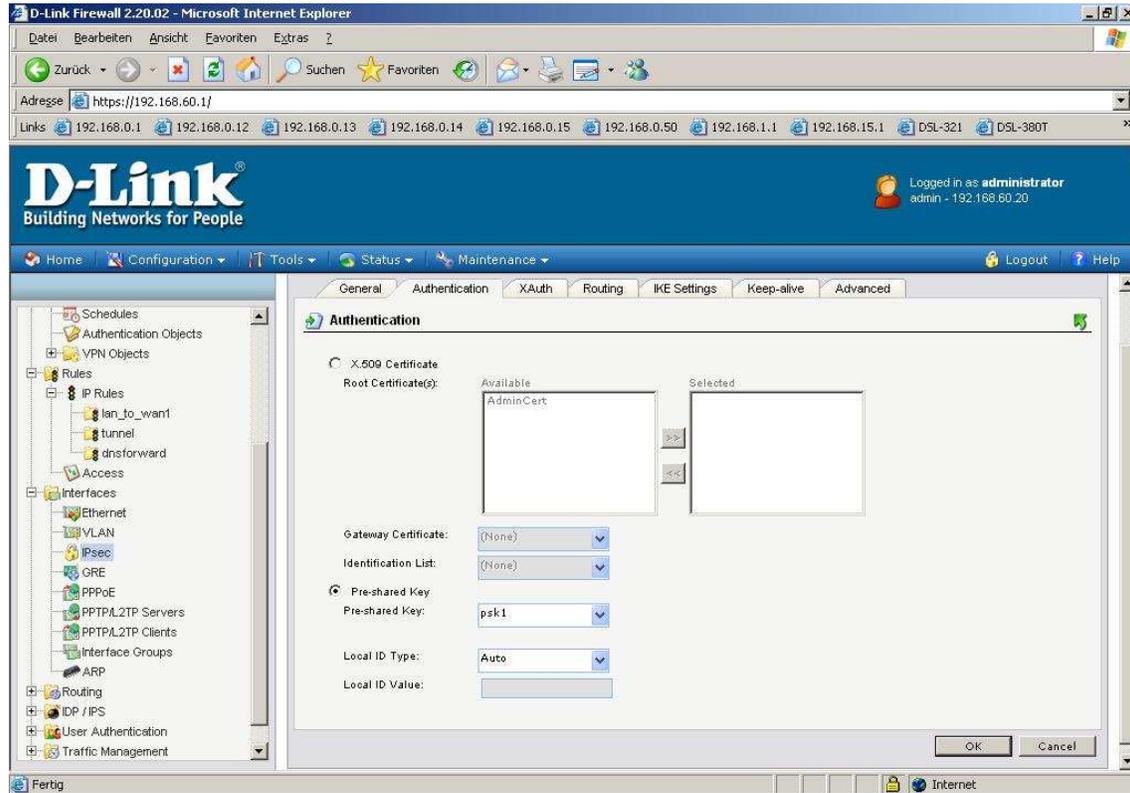
- Name = z.B. ipsectunnel
- Local Network = lannet (bei der DFL-1600/2500 ist es lan1net oder lan2net usw.)
- Remote Network = wählen Sie das bei 4. erstelle „remotenet“ aus.
- Remote Endpoint = Die WAN IP Adresse des DI-804HV oder wenn es sich um eine DynDNS Adresse handelt geben Sie **dns:diedyndnsadresse.dyndns.org** ein.
- IKE Algorithms = High
- IPsec Algorithms = High

Klicken Sie nicht auf OK.



9. Wählen Sie den Reiter Authentication aus und wählen bei Preshared Key den bei 6. erstellen **psk1** aus.

Klicken Sie nicht auf OK.

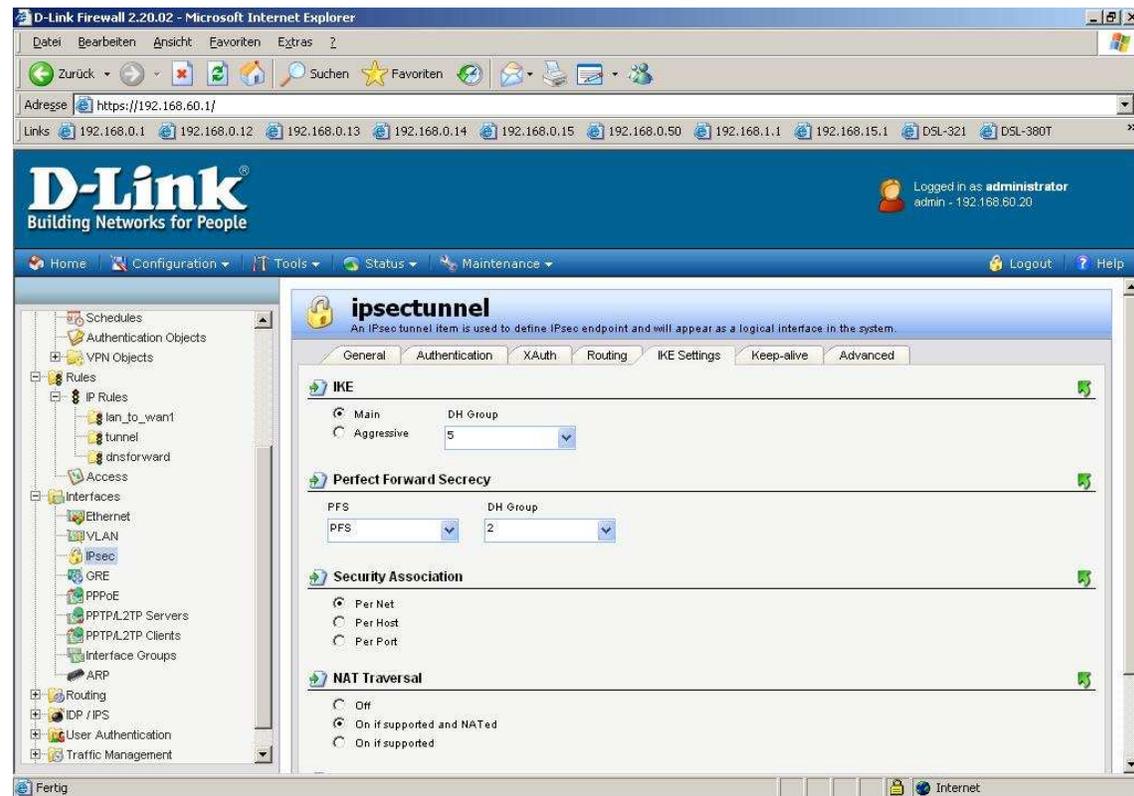


10. Wählen Sie den Reiter IKE Settings aus.

- Als IKE DH Group wählen Sie 5 aus.
- Unter PFS wählen Sie PFS aus und rechts daneben die DH Group 2.

Beide DH Groups müssen die gleichen wie im DI-804HV sein! (siehe 4. und 5.)

Klicken Sie nun auf OK.



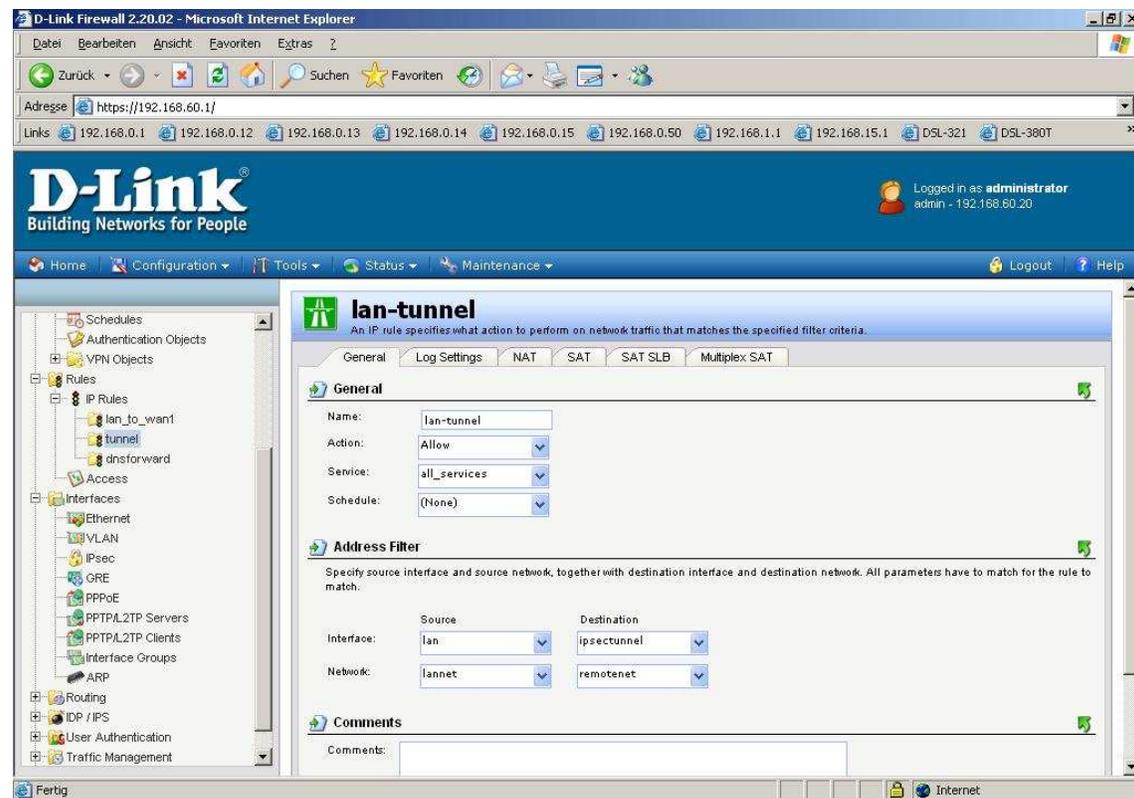
11. Um die Kommunikation über den VPN Tunnel in der DFL-800 zu erlauben, erstellen Sie unter Rules – IP Rules zwei neue Regeln.

1. Regel:

- Klicken Sie auf Add und wählen IP Rule Folder aus.
- Vergeben Sie dem Ordner einen Namen, z.B. tunnel und klicken auf OK.
- Klicken Sie auf Add und wählen IP Rule aus.
- Name = z.B. lan-tunnel
- Action = Allow
- Service = all_services

- Source Interface = lan (bei der DFL-1600/2500 ist es lan1 oder lan2 usw.)
- Source Network = lannet (bei der DFL-1600/2500 ist es lan1net oder lan2net usw.)
- Destination Interface = Wählen Sie Ihren bei 8. erstellten „ipsectunnel“ aus.
- Destination Network = Wählen Sie Ihr bei 7. erstelltes „remotenet“ aus.

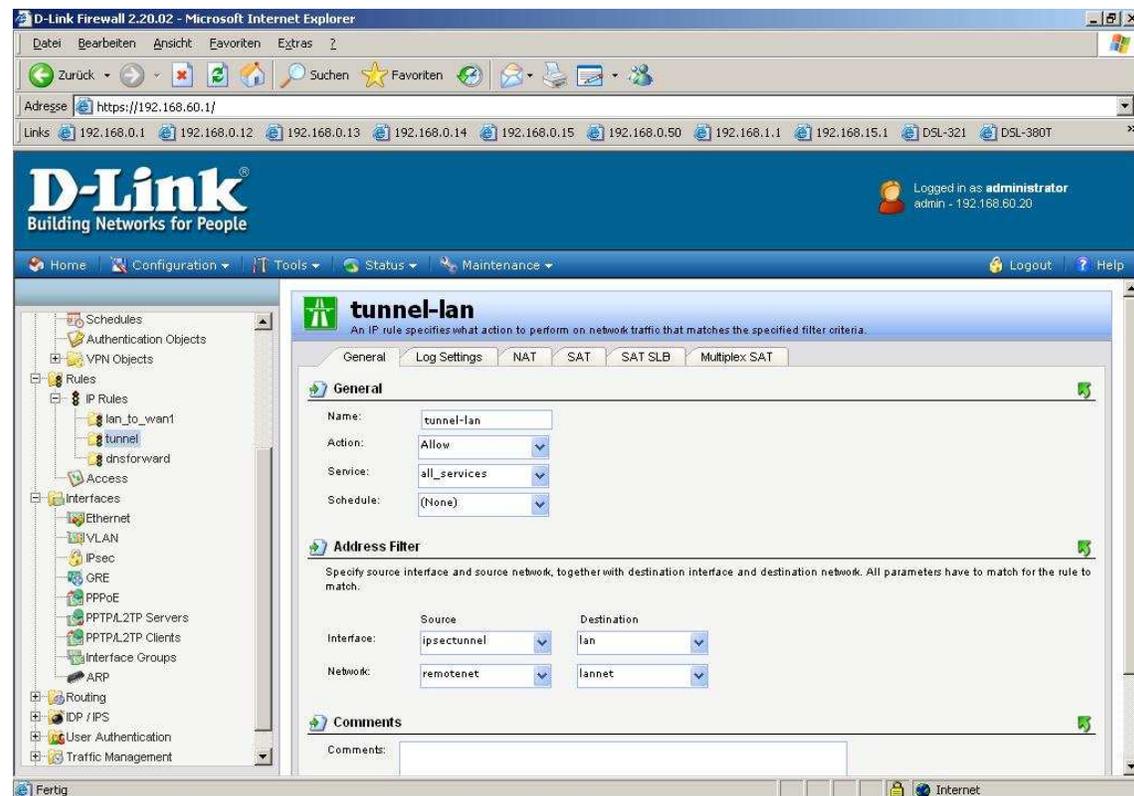
Klicken Sie auf OK.



2. Regel:

- Klicken Sie auf Add und wählen IP Rule aus.
 - Name = z.B. tunnel-lan
 - Action = Allow
 - Service = all_services
-
- Source Interface = Wählen Sie Ihren bei 8. erstellten „ipsectunnel“ aus.
 - Source Network = Wählen Sie Ihr bei 7. erstelltes „remotenet“ aus.
 - Destination Interface = lan (bei der DFL-1600/2500 ist es lan1 oder lan2 usw.)
 - Destination Network = lannet (bei der DFL-1600/2500 ist es lan1net oder lan2net usw.)

Klicken Sie auf OK.



12. Klicken Sie abschließend oben links auf Configuration und wählen „Save and Activate“ aus um die vorgenommenen Einstellungen zu übernehmen.