

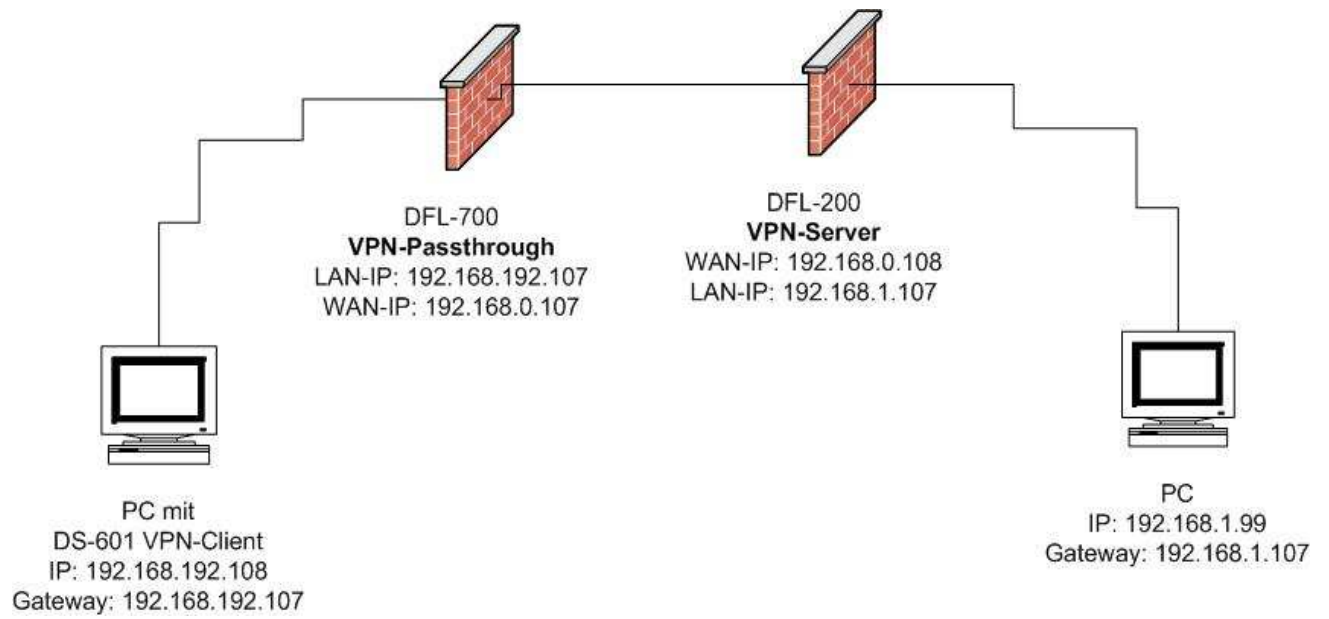
VPN Passthrough

(LAN -> VPN-PT -> WAN)

über

DFL-200, DFL-700,
DFL-1100

Testumgebung:



1.) Um VPN-Passthrough (auf der DFL-700) zu konfigurieren, richten Sie unter „Firewall/Policy/LAN->WAN“ folgendes ein:

Firewall Policy

Show policy: [LAN->WAN](#) [LAN->DMZ](#) [WAN->DMZ](#)
[WAN->LAN](#) [DMZ->LAN](#) [DMZ->WAN](#)

Edit **VPN-Passthrough_LAN_WAN** rule (#1):

Name:

Position: Moves before given position. Blank = last.

Action:

Source Nets:

... Users/Groups: "Any" = Any authenticated

Destination Nets:

... Users/Groups: "Any" = Any authenticated

Leave source and/or destination blank to match everything.

Service:

Custom source ports: Blank = any port

... destination ports:

Schedule:

2.) In der Übersicht wird daraufhin folgende Übersicht angezeigt.

Select "Add New" below, or select a rule from the list to edit it:

LAN->WAN Policy						
Name	Action	Source	Destination	Service	Move	
#1 VPN-Passthrough_LAN_WAN	Allow	Any	Any	ipsec-suite		[Edit]
[Add new]						

3.) Um den VPN-Server (auf der DFL200) zu konfigurieren, richten Sie unter „VPN/Firewall“ folgendes ein:

VPN Tunnels

Edit IPsec tunnel **test**:

Name:
Local Net:

Authentication:

PSK - Pre-Shared Key

PSK:

Retype PSK:

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:

Tunnel type:

Roaming Users - single-host IPsec clients

IKE XAuth: Require user authentication via IKE XAuth to open tunnel.

LAN-to-LAN tunnel

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route: Automatically add a route for the remote network.

Proxy ARP: Publish remote network on all interfaces via Proxy ARP.

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

XAuth Username:

XAuth Password:

Delete this VPN tunnel



Weitere Informationen bzgl. VPN Server finden Sie unter folgender URL:

ftp://ftp.dlink.de/dfi-products/dfi-700/Installationsanleitungen/dfi700_man_ger_dfi700-to-vpnclient_041004.zip

4.) In der Übersicht wird daraufhin folgende Übersicht angezeigt.

VPN Tunnels

Pick a VPN tunnel to edit from the below list:



IPsec Tunnels			
Name	Local Net	Remote Net	Remote Gateway
test	192.168.1.0/24	Any	(No gateway)
[Edit]			
[Add new]			

5.) Bitte beachten Sie bei der Einrichtung am DS-601 den Gateway und das Remote-Network (siehe Abbildung):

IPSec General Settings

Gateway : 192.168.0.108

Policies

IKE policy : AES256-SHA-DH5

IPsec policy : ESP-AES256-SHA

Policy lifetimes ... Policy editor ...

Advanced options

Exch. mode : Main Mode

PFS group : DH-Group 5 (1536 Bit)

Use IP compression (LZS)

Disable DPD (Dead Peer Detection)

Remote Networks

Enter the IP networks the tunnel should be used for. Without entries tunneling will always be used.

Network addresses :	Subnet masks :
192.168.1.0	255.255.255.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

Apply tunneling security for local networks

Weitere Informationen bzgl. DS_601 finden Sie unter folgender URL:

ftp://ftp.dlink.de/dfl-products/dfl-700/Installationsanleitungen/dfl700_man_ger_dfl700-to-vpnclient_041004.zip

6.) Sobald Sie die Verbindung über „Connect“ aufbauen, kann über die DFL-700 und die DFL-200 auf dem Remote-PC gearbeitet werden.



```
Antwort von 192.168.1.99: Bytes=32 Zeit=3ms TTL=127
Antwort von 192.168.1.99: Bytes=32 Zeit=4ms TTL=127
Antwort von 192.168.1.99: Bytes=32 Zeit=3ms TTL=127
Antwort von 192.168.1.99: Bytes=32 Zeit=2ms TTL=127
```