

## L2TP via iPhone zu USG V4.xx (/ V3.xx ähnlich)

### Einrichten der Phase-1 (VPN Gateway):

The screenshot shows the configuration for Phase 1 (VPN Gateway). The Domain Name is set to 0.0.0.0. Under Peer Gateway Address, Dynamic Address is selected. Authentication is set to Pre-Shared Key (Den\_PSK) and is unmasked. Local ID Type is IPv4, Content is 0.0.0.0, and Peer ID Type is Any. Phase 1 Settings include SA Life Time of 86400 seconds and Negotiation Mode of Main. A proposal table is shown with three entries: 1 (3DES, SHA1), 2 (3DES, MD5), and 3 (DES, SHA1). Key Group is DH2, NAT Traversal is checked, and Dead Peer Detection (DPD) is checked.

| # | Encryption | Authentication |
|---|------------|----------------|
| 1 | 3DES       | SHA1           |
| 2 | 3DES       | MD5            |
| 3 | DES        | SHA1           |

### Einrichten der Phase-2 (VPN Connection):

The screenshot shows the configuration for Phase 2 (VPN Connection). Connection Name is L2TP\_VPN\_Connection. Under VPN Gateway, Remote Access (Server Role) is selected. Local policy is Dynamic\_Host and Host 0.0.0.0. Under Mode Config, Enable Mode Config is checked. Under Phase 2 Setting, SA Life Time is 3600 seconds, Active Protocol is ESP, Encapsulation is Transport, and Perfect Forward Secrecy (PFS) is none. A proposal table is shown with three entries: 1 (3DES, SHA1), 2 (3DES, MD5), and 3 (DES, SHA1). Under Related Settings, Zone is IPSec\_VPN. Under Connectivity Check, Enable Connectivity Check is checked.

| # | Encryption | Authentication |
|---|------------|----------------|
| 1 | 3DES       | SHA1           |
| 2 | 3DES       | MD5            |
| 3 | DES        | SHA1           |

## Einstellen L2TP VPN:

### IP-L2TP Pool Range Adress Objekt erstellen:

The screenshot shows a dialog box titled "Edit Address Rule L2TP\_Pool". It contains the following fields:

- Name: L2TP\_Pool
- Address Type: RANGE
- Starting IP Address: 192.168.201.1
- End IP Address: 192.168.201.10

At the bottom, there are "OK" and "Cancel" buttons.

### L2TP VPN einstellen:

The screenshot shows the "L2TP VPN" configuration page. The "General Settings" section is expanded, showing:

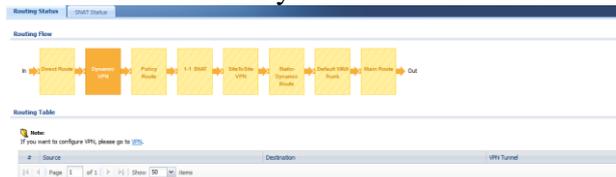
- Enable L2TP Over IPSec:
- VPN Connection: L2TP\_VPN\_Connection
- IP Address Pool: L2TP\_Pool (Range: 192.168.201.1-192.168.201.10)
- Authentication Method: default

The "Advance" section is also expanded, showing:

- Authentication Server Certificate: default
- Allowed User: any
- Keep Alive Timer: 60 (1-180 seconds)
- First DNS Server (Optional): Custom Defined (8.8.8.8)
- Second DNS Server (Optional): Custom Defined (8.8.4.4)
- First WINS Server (Optional):
- Second WINS Server (Optional):

### Policy Routes setzen und route order:

Route Order sollte Dynamic VPN nach Direct Route stehen.



### Policy Route L2TP Tunnel eingehend via WAN Interface oder Trunk.

The screenshot shows the "Edit Policy Route" configuration page. The "Configuration" section is expanded, showing:

- Enable:
- Description: (Optional)

The "Criteria" section is expanded, showing:

- User: any
- Incoming: Tunnel
- Please select one member: L2TP\_VPN\_Connection
- Source Address: L2TP\_Pool
- Destination Address: any
- DSCP Code: any
- Schedule: none
- Service: any
- Source Port: any

The "Next-Hop" section is expanded, showing:

- Type: Trunk
- Trunk: WAN\_TRUNK

The "DSCP Markang" section is expanded, showing:

- DSCP Marking: preserve

The "Address Translation" section is expanded, showing:

- Source Network Address Translation: outgoing-interface

The "Advance" section is expanded, showing:

- Healthy Check:  Disable policy route automatically while Interface link down
- Enable Connectivity Check
- Check Method: icmp

Ggf. zusätzliche Policy Routes eingehend L2TP to lan und zurück (NAT =NONE).

**Edit Policy Route**

Hide Advanced Settings Create new Object

**Configuration**

Enable  
Description: (Optional)

**Criteria**

User: any  
Incoming: Tunnel  
Please select one member: LZTP\_VPN\_Connection  
Source Address: LZTP\_Pool  
Destination Address: LAN1\_SUBNET  
DSCP Code: any  
Schedule: none  
Service: any  
Source Port: any

**Next-Hop**

Type: Interface  
Interface: lan1

**DSCP Marking**

DSCP Marking: preserve

**Address Translation**

Source Network Address Translation: none

**Advance**

**Healthy Check**

Disable policy route automatically while Interface link down  
 Enable Connectivity Check  
Check Method: icmp  
Check Period: 30 (5-600 seconds)

**Edit Policy Route**

Hide Advanced Settings Create new Object

**Configuration**

Enable  
Description: (Optional)

**Criteria**

User: any  
Incoming: Interface  
Please select one member: lan1  
Source Address: LAN1\_SUBNET  
Destination Address: LZTP\_Pool  
DSCP Code: any  
Schedule: none  
Service: any  
Source Port: any

**Next-Hop**

Type: VPN Tunnel  
VPN Tunnel: LZTP\_VPN\_Connection  
 Auto Destination Address

**DSCP Marking**

DSCP Marking: preserve

**Advance**

**Healthy Check**

Enable Connectivity Check  
Check Method: icmp  
Check Period: 30 (5-600 seconds)  
Check Timeout: 5 (1-10 seconds)  
Check Fail Tolerance: 5 (1-10)