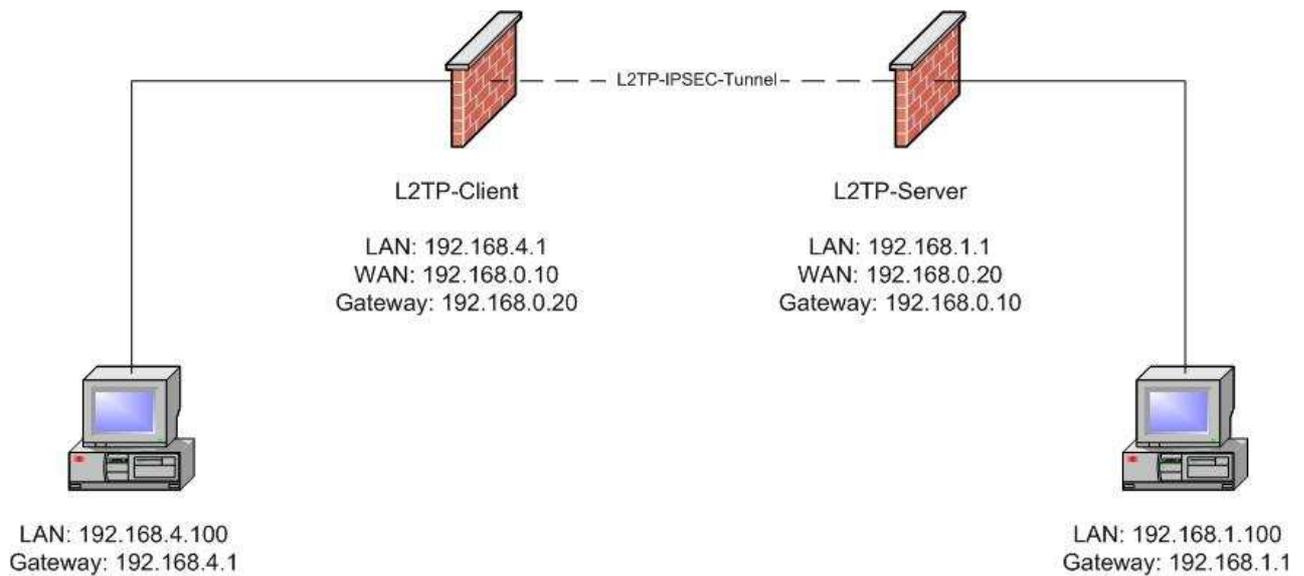


Aufbau einer
L2TP-IPSEC
Verbindung
zwischen zwei

DFL-200, DFL-700 oder
DFL-1100

Testumgebung



Vorgehensweise zur Einrichtung des L2TP/IPSEC - Client:

Um den L2TP/IPSEC Client einzurichten, sind folgende Einstellungen unter „Firewall / VPN / Add new L2TP Client“, notwendig.

- Vergeben Sie einen Namen für den VPN-Client
- Vergeben Sie einen Usernamen und ein Kennwort. Der User muss später auf dem VPN – Server angelegt werden.
- Als „Remote Gateway“ tragen Sie die WAN-IP des VPN Servers ein
- Als „Remote Net“ tragen Sie das Netz hinter dem VPN-Server ein
- Als „Authentication“ aktivieren Sie nur MS-Chapv2
- Eine MPPE Encryption wird nicht benötigt, da die Verschlüsselung über IPSEC geschieht
- Aktivieren Sie „Use IPsec encryption“
- Tragen Sie einen Pre-Shared-Key (PSK) ein

L2TP/PPTP Clients

Edit L2TP Client **L2TP_IPSEC_Client**:

Name:

Basic settings:

Username:

Password:

Retype Password:

Interface IP: Blank = get IP from server

Remote Gateway:

Remote Net:

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

Use primary DNS server from tunnel as primary DNS

Use secondary DNS server from tunnel as secondary DNS

Hint: Use Servers -> DNS Relay to easily make DNS servers available to internal clients.

Dial on demand

Idle timeout: minutes

Count sending as activity

Count receiving as activity

Count both as activity

Authentication:

Protocol: No auth

PAP

CHAP

MSCHAP (MPPE encryption possible)

MSCHAPv2 (MMPE encryption possible)

MPPE encryption:

None

40 bit

56 bit

128 bit

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

Use IPsec encryption

PSK - Pre-Shared Key

Key:

Retype key:

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:

Delete this VPN tunnel



Sobald Sie mit „Apply“ abspeichern, erhalten Sie diese Anzeige in der Übersicht.

Name	Type	Remote Gateway	User	IPsec	
L2TP_IPSEC_Client	L2TP	192.168.0.20	Test	PSK	[Edit]

[\[Add new PPTP client\]](#)
[\[Add new L2TP client\]](#)

Vorgehensweise zur Einrichtung des L2TP/IPSEC - Server:

Um den L2TP/IPSEC Server einzurichten, sind folgende Einstellungen unter „Firewall / VPN / Add new L2TP Server“, notwendig.

- Vergeben Sie einen Namen für den VPN-Server
- Vergeben Sie unter Client IP Pool eine Range von IP Adressen, damit der Client eine IP-Adresse beim Verbindungsaufbau erhalten kann. Diese Range muss zu dem Subnet am LAN-Interface passen.
- Aktivieren Sie folgende Optionen:
 - o Proxy ARP dynamically added routes
 - o Use unit's own DNS relay addresses
- Als „Authentication“ aktivieren Sie nur MS-Chapv2
- Eine MPPE Encryption wird nicht benötigt, da die Verschlüsselung über IPSEC geschieht
- Aktivieren Sie „Require Ipsec encryption“
- Tragen Sie den (im VPN-Client vergebenen) Pre-Shared-Key (PSK) ein

L2TP/PPTP Servers

Edit L2TP tunnel **l2tp_Server**:

Name:

Outer IP: Blank = WAN IP
Must be WAN IP if IPsec encryption is required

Inner IP: Blank = LAN IP

IP Pool and settings:

Client IP Pool:

Proxy ARP dynamically added routes

Primary DNS: (Optional)

Secondary DNS: (Optional)

Use unit's own DNS relay addresses

Primary WINS: (Optional)

Secondary WINS: (Optional)

Authentication protocol:

- No authentication
- PAP
- CHAP
- MSCHAP (MPPE encryption possible)
- MSCHAPv2 (MPPE encryption possible)

MPPE encryption:

- None - unencrypted
- 40 bit
- 56 bit
- 128 bit (best security)

Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol.

Require IPsec encryption

PSK - Pre-Shared Key

Key:

Retype key:

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:

Delete this VPN tunnel



Sobald Sie mit „Apply“ abspeichern, erhalten Sie diese Anzeige in der Übersicht.

L2TP / PPTP Server					
Name	Type	Outer IP	Inner IP	IPsec	
l2tp_Server	L2TP	WAN IP	LAN IP	PSK	[Edit]
[Add new PPTP server]					
[Add new L2TP server]					

Tragen Sie den im VPN-Client angegebenen User unter „ Firewall / Users / User in local database / Add new „ ein. Weiterhin muss das Subnet hinter dem VPN-Client unter „Network behind user: „ eingetragen werden.

User Management

Edit user **Test**:

User name:

Group membership:

Change password

Password:

Retype password:

L2TP/PPTP settings:

Static client IP:
If empty, the IP address will be taken from the server's IP pool

Networks behind user:

Delete user

Speichern und aktivieren Sie die Einstellungen.

Danach kann die Verbindung über einen Ping auf ein Netzwerkdevice hinter dem VPN Server getestet werden. In diesem Fall wäre das „ping 192.168.1.100“.