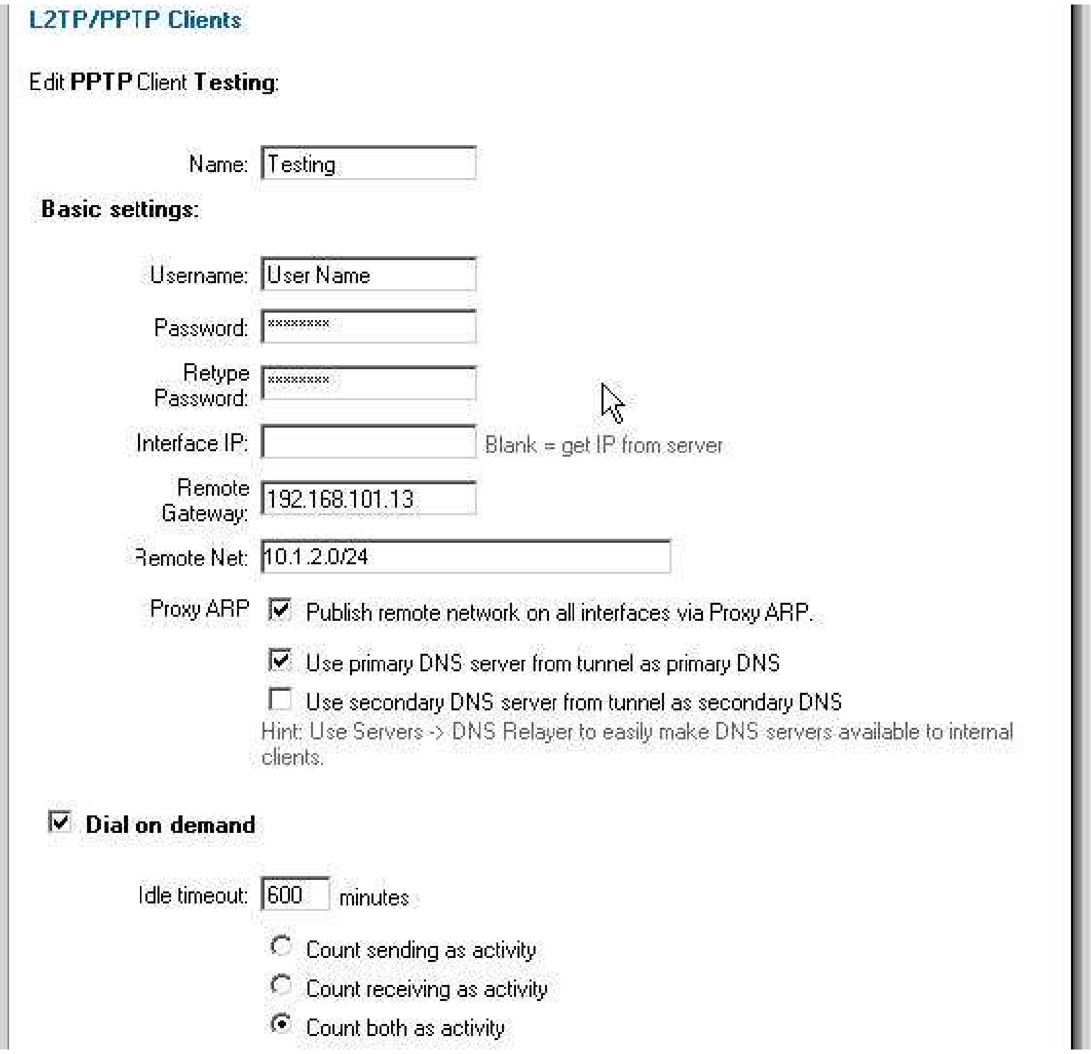
Using the built-in PPtP client against a Windows 2000/2003 Server
This document describes how to configure the built in PPtP client in DFL-700 to connect to a Windows 2000/2003 PPtP server and accessing resources on the private network from the LAN workstation.
In my example below I use the following addresses:
”Public” network: 192.168.101.0/24
Default Gateway: 192.168.101.1
WAN address: 192.168.101.170
Lan network: 10.1.0.0/24
PPtP Server: 192.168.101.13
PPtP Network: 10.1.2.0/24

- In ”**Firewall\VPN**” select “**Add new PPTP client**”. Type in the needed information.

Note:
“**Idle timeout**” value is in seconds, not minutes.



L2TP/PPTP Clients

Edit **PPTP** Client **Testing**:

Name: Testing

Basic settings:

Username: User Name

Password: ********

Retype Password: ********

Interface IP: Blank = get IP from server

Remote Gateway: 192.168.101.13

Remote Net: 10.1.2.0/24

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 Relayer to easily make DNS servers available to internal clients.

☑ **Dial on demand**

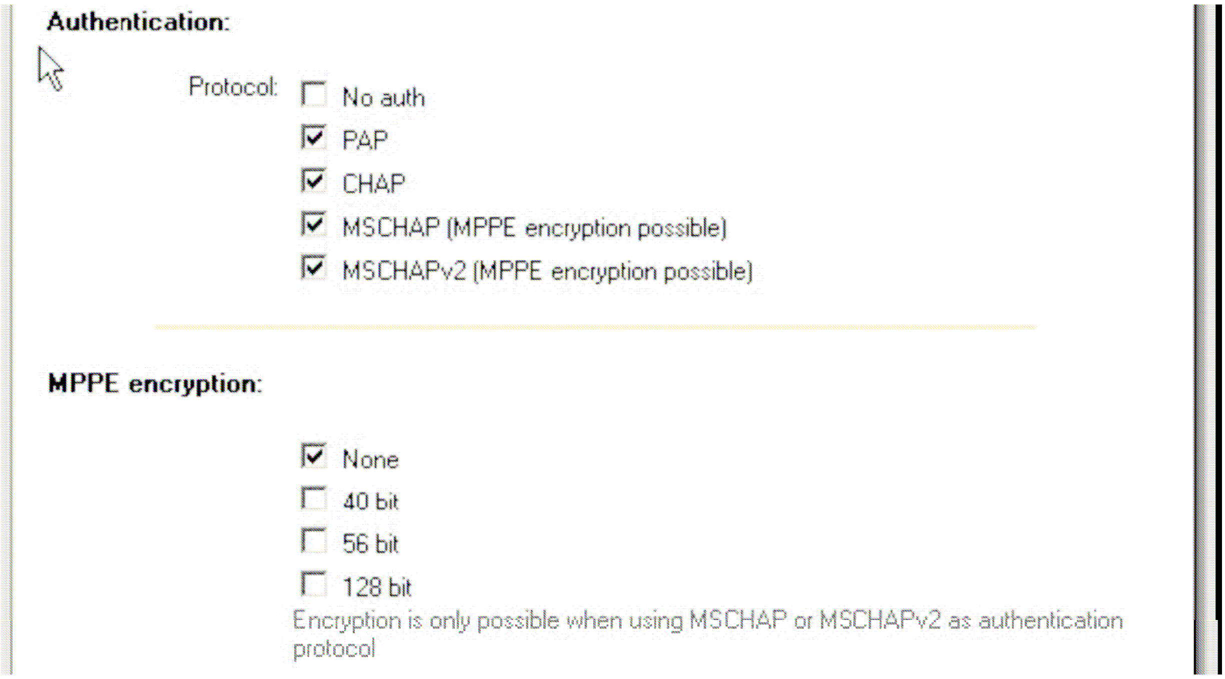
Idle timeout: 600 minutes

○ Count sending as activity

○ Count receiving as activity

● Count both as activity

- Select your encryption



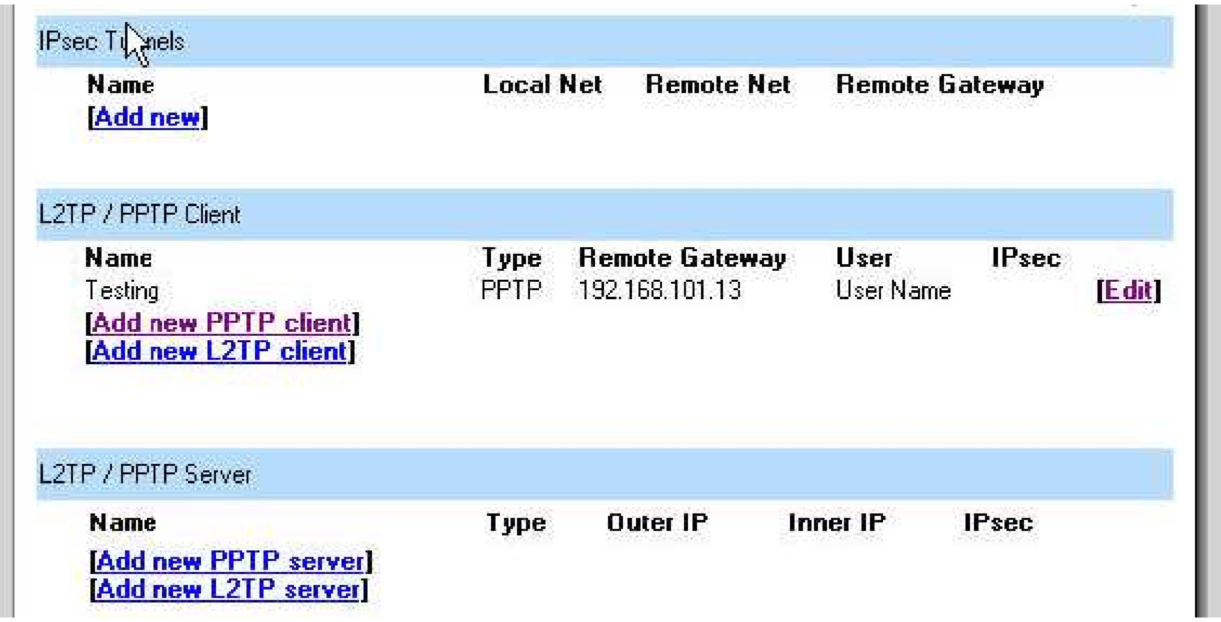
Authentication:

Protocol:
☐ No auth
☑ PAP
☑ CHAP
☑ MSCHAP (MPPE encryption possible)
☑ MSCHAPv2 (MPPE encryption possible)

MPPE encryption:

☑ None
☐ 40 bit
☐ 56 bit
☐ 128 bit
Encryption is only possible when using MSCHAP or MSCHAPv2 as authentication protocol

- Press "**Apply**"



IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway
[Add new]			

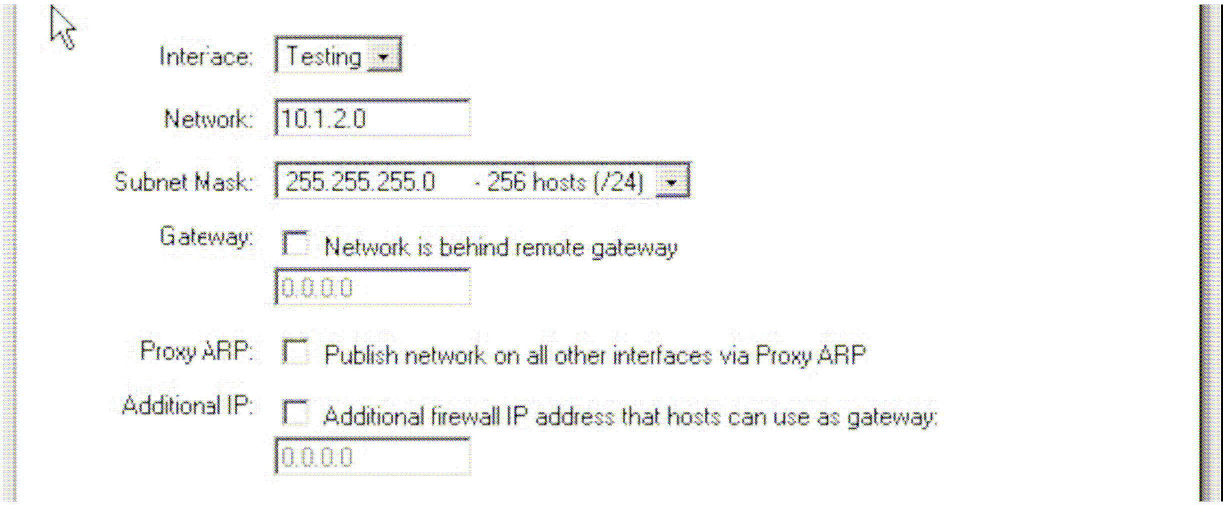
L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec	
Testing	PPTP	192.168.101.13	User Name		[Edit]
[Add new PPTP client]					
[Add new L2TP client]					

L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
[Add new PPTP server]				
[Add new L2TP server]				

- Select “**System\Routing**” and “**Add new**”. Make a new route to the remote private network behind the PPtP server



Interface: Testing

Network: 10.1.2.0

Subnet Mask: 255.255.255.0 - 256 hosts (/24)

Gateway: □ Network is behind remote gateway

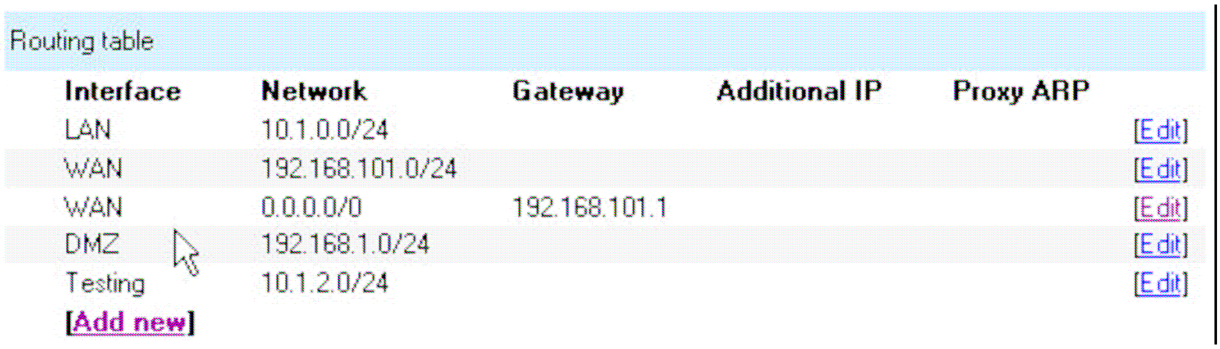
0.0.0.0

Proxy ARP: □ Publish network on all other interfaces via Proxy ARP

Additional IP: □ Additional firewall IP address that hosts can use as gateway:

0.0.0.0

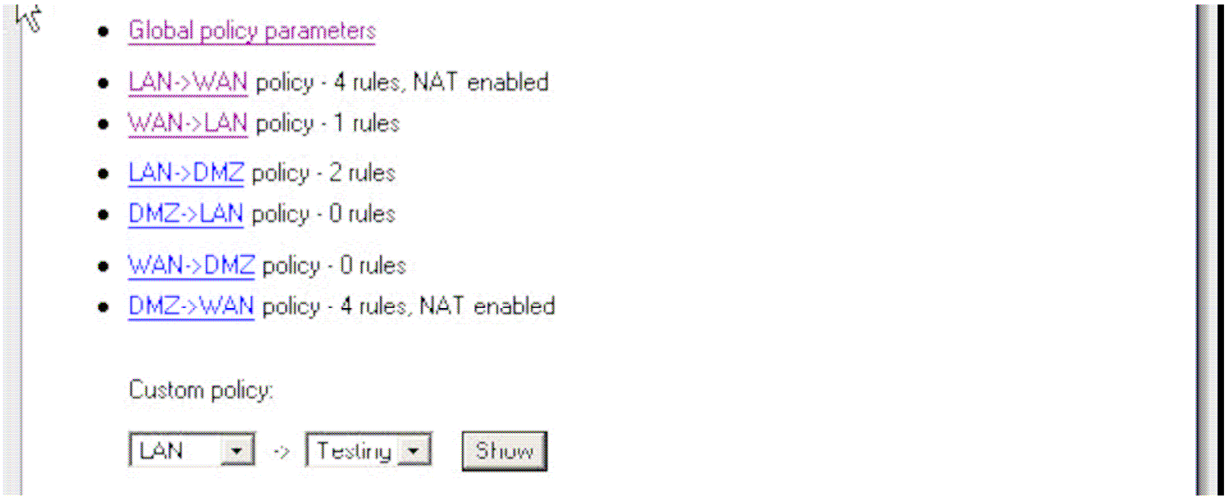
- Press “**Apply**”



Routing table

Interface	Network	Gateway	Additional IP	Proxy ARP	
LAN	10.1.0.0/24				[Edit]
WAN	192.168.101.0/24				[Edit]
WAN	0.0.0.0/0	192.168.101.1			[Edit]
DMZ	192.168.1.0/24				[Edit]
Testing	10.1.2.0/24				[Edit]
[Add new]					

- Select “**Firewall Policy**” and “**Global policy parameters**”. Remove the setting “**Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**.” Press “**Apply**”.

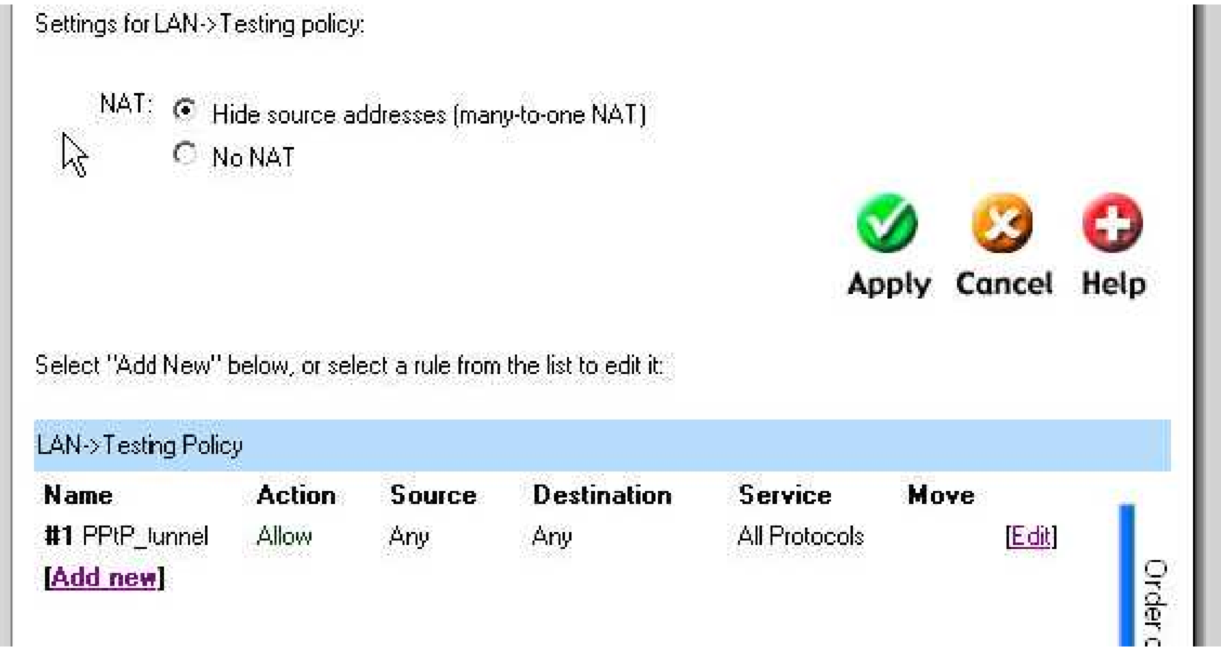


- Global policy parameters
- LAN->WAN policy - 4 rules, NAT enabled
- WAN->LAN policy - 1 rules
- LAN->DMZ policy - 2 rules
- DMZ->LAN policy - 0 rules
- WAN->DMZ policy - 0 rules
- DMZ->WAN policy - 4 rules, NAT enabled

Custom policy:

LAN -> Testing

- Select “**Lan -> Testing**”. Press “**Add New**”. Configure Policy Properties for the PPtP tunnel. Remember to enable NAT



Settings for LAN->Testing policy:

NAT: ● Hide source addresses (many-to-one NAT)
○ No NAT

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

LAN->Testing Policy

Name	Action	Source	Destination	Service	Move	
#1 PPtP_tunnel	Allow	Any	Any	All Protocols		[Edit]
[Add new]						

- Press “Apply” and Activate the changes.

Note:
When removing the “**Global policy parameters**” setting “**Allow all VPN traffic: internal->VPN, VPN->internal and VPN->VPN**”, you must manually configure a policy for each VPN tunnel you have configured in your firewall.
Also remember to configure the TCP/IP Address assignment correctly in your Windows 2000/2003 Server “Incoming Connection Properties”. In our test case 10.1.2.0/24