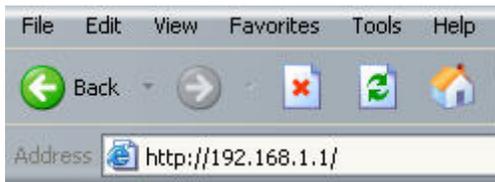


## **How to set up a PPTP server on your DFL-210**

Firstly you will need to upgrade your Firewall's firmware before you continue with the setup. Firmware can be downloaded here → <ftp://ftp.dlinktech.co.za>

Log into your firewall.

To log in, open your browser and type the IP address of the firewall in the address bar and press "Enter".



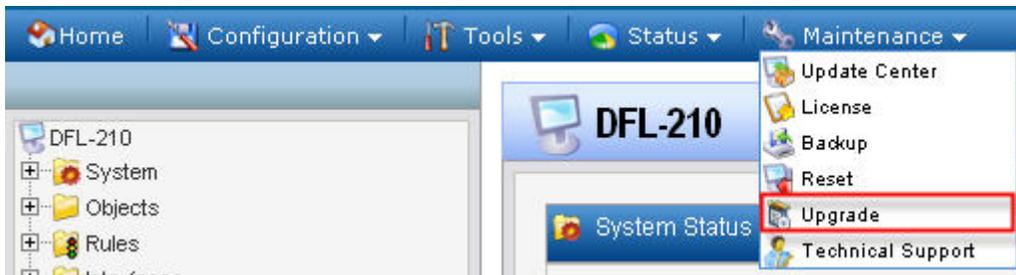
This will take you to the Login screen. Use "admin" as username and "admin" as password.

A screenshot of a web browser displaying an "Authentication Required" login screen. The page has a blue header with the text "Authentication Required". Below the header, it says "Please enter your username and password." There are two input fields: "Username:" with the text "admin" and "Password:" with six dots. A "Login" button is positioned below the password field. To the right of the input fields is a large padlock icon. At the bottom of the page, it says "Optimized for Internet Explorer 6 (and later), Firefox and Netscape 8".

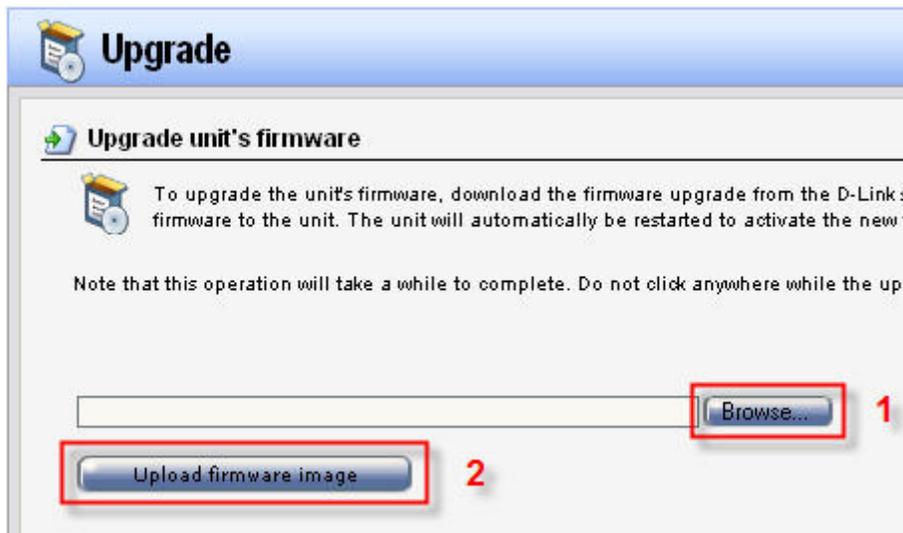
Now you are logged into your firewall.

Upgrading the firmware.

Click on Maintenance and then upgrade.

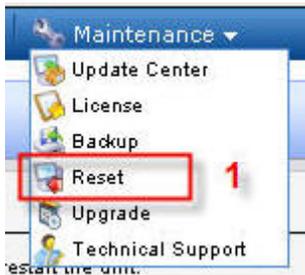


Click on the Browse button (1) to browse to the firmware you downloaded and saved on your computer, select it and click on Upload firmware (2).



You have now upgraded your firmware.

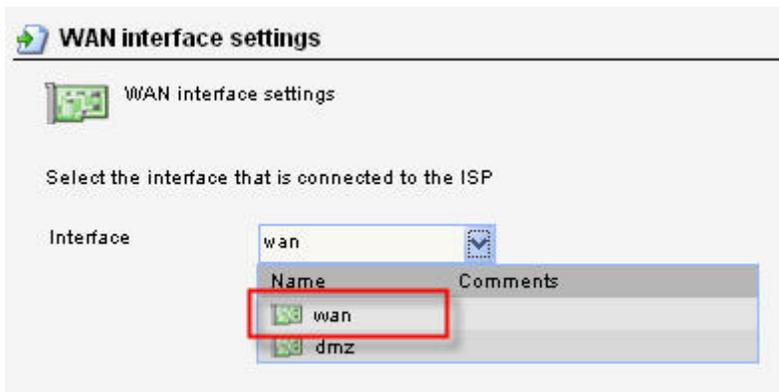
Now you have factory reset your firewall by clicking Maintenance and Reset.



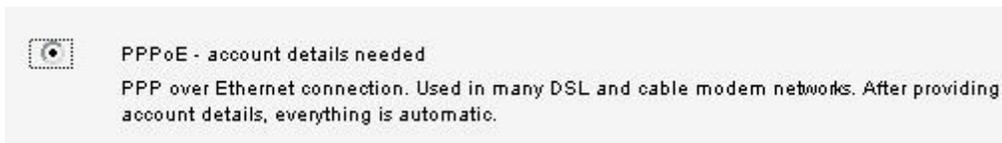
Choose the 1<sup>st</sup> option under Reset to factory defaults and click reset to factory defaults.



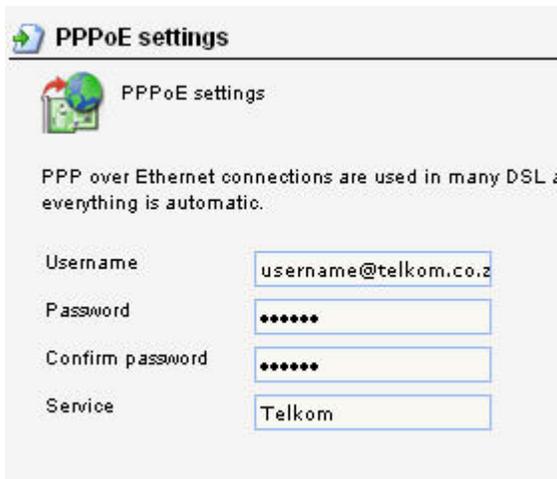
Log into your firewall again and then run the setup wizard and click next till you get to the WAN interface settings. Choose Wan in the drop-down menu and then next.



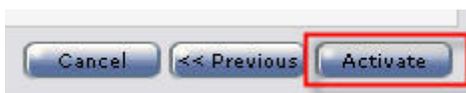
Choose the PPPoE option and click next



Fill in you username and password as per your ISP.

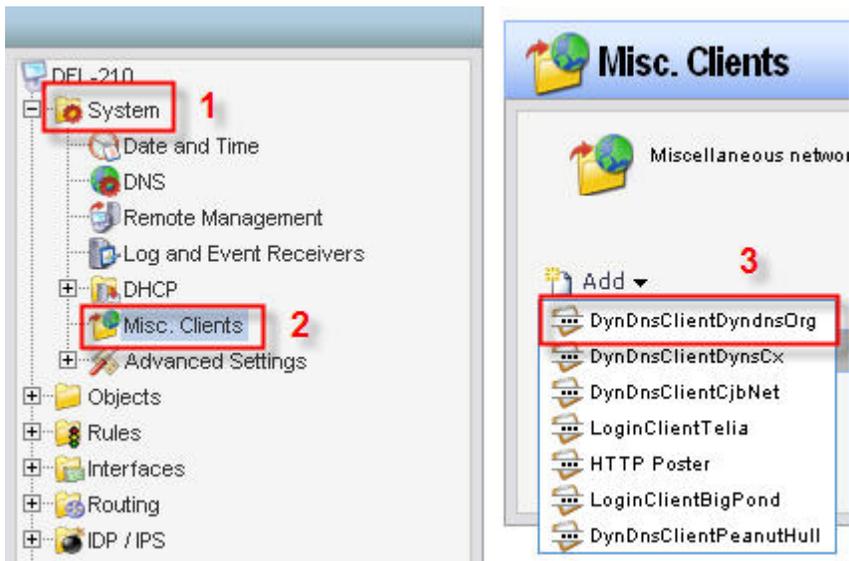


Click on activate when done.



You are done with your Internet connection setup.

Now we need to set up your DDNS account. Click System → Misc. clients → Add and choose DynDnsClientDyndnsOrg. (Note that this firewall will not accept an account from **no-ip.com**)



Fill in your hostname, username and password for you DDNS account and click OK.

*Document created by Darius Calitz (D-Link Africa)*

**Dyndns.org DynDNS Client**

Configure the parameters used to connect to the dyndns.org DynDNS service.

DNSName:  eg: test.dyndns.org

Username:

Password:

Confirm Password:

Click on Objects → Address Book to see if your DNS's was discovered by your PPPoE client.

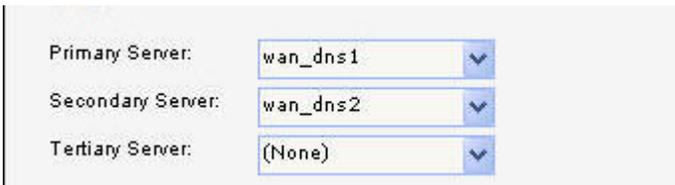
**Address Book**

The Address Book contains symbolic names for various types of addresses, including IP networks and Ethernet MAC addresses.

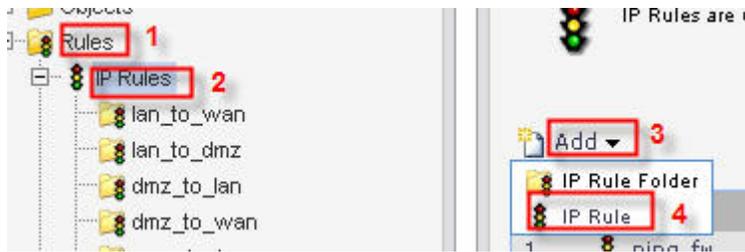
Add ▾

Name ▾	Address ▾	User Auth Groups ▾	Comments ▾
all-nets	0.0.0.0/0		All possible networks
InterfaceAddresses			This folder contains addresses for interfaces
wan1_dns1	0.0.0.0		Primary DNS server received from PPPoE client wan1.
wan1_dns2	0.0.0.0		Secondary DNS server received from PPPoE client wan1.

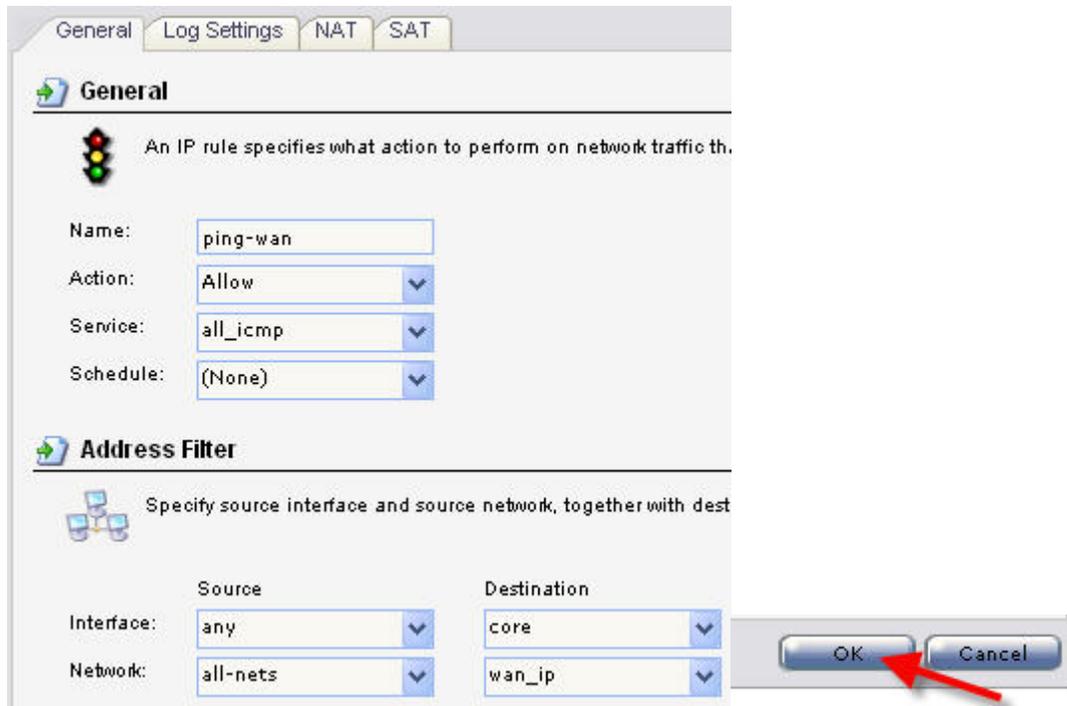
To set up your DNS settings click on System and DNS and choose wan\_dns1 for your Primary server and wan\_dns2 for your secondary server.

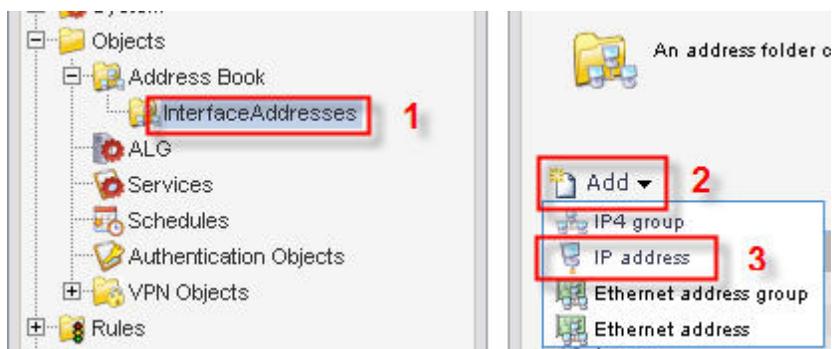
Now we need to set up a rule to allow remote users to ping the WAN side of the firewall. Click on Rules → IP Rules → Add → IP Rule.



Enter the following settings exactly as in picture below and click on OK.



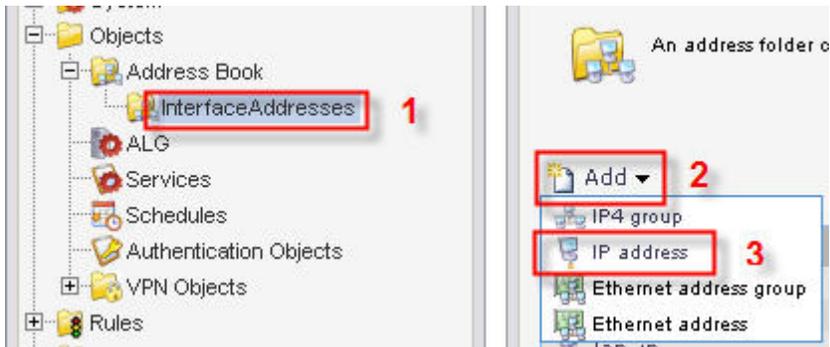
Now we need to create a PPTP server IP address. To do this click → Objects → Address Book → InterfaceAddresses → Add → IP address.



Enter settings exactly as in picture below. (Note that PPTP-server-IP needs to be different than the IP address of the firewall which is 192.168.1.1.)

Name:	<input type="text" value="pptp-server-ipaddress"/>
IP Address:	<input type="text" value="192.168.1.2"/> ← different IP

Now we need to set up an IP address range - this is the IP addresses that will be allocated to each authenticated remote user.



Enter settings exactly as in picture below. (Note that PPTP-server-IP range also needs to be different than the IP range of the network behind the firewall which is 192.168.1.x)

Name:	<input type="text" value="pptp-ip-range"/>
IP Address:	<input type="text" value="192.168.2.3-192.168.2.99"/> different IP range

The InterfaceAddresses page should look something like this now.

The screenshot shows the Mikrotik WinBox InterfaceAddresses page. It features a table with two columns: 'Name' and 'Address'. The table contains the following entries:

Name	Address
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
lan_ip	192.168.1.1
lannet	192.168.1.0/24
pptp-ip-range	192.168.2.3-192.168.2.99
pptp-server-ipaddress	192.168.1.2
wan_ip	192.168.110.254
wannet	192.168.110.0/24

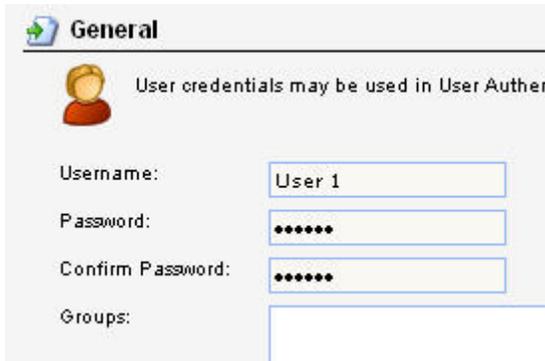
Now we need to create a Local database for PPTP authentication. Click User authentication → Local User databases → Add → Local user database.



Name the Local User Database “pptp-server”.



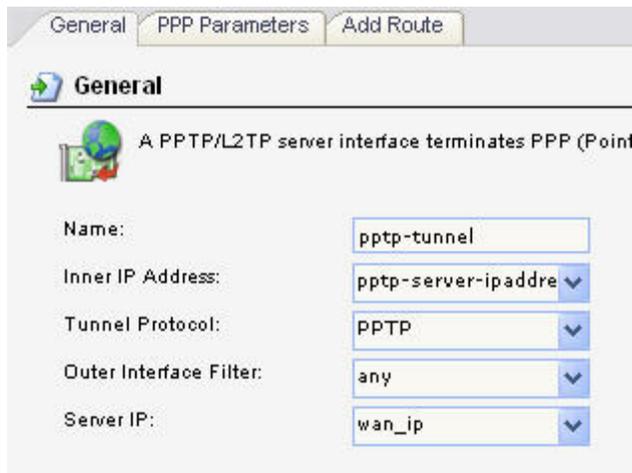
Let’s create some users on the pptp-server database. Click User authentication → Local User databases → pptp server → Add → User. Fill in the desired username and password. Repeat this step if more than one user are needed.



To create the PPTP tunnel click Interfaces → PPTP/L2TP Servers → Add → PPTP/L2TP Server.



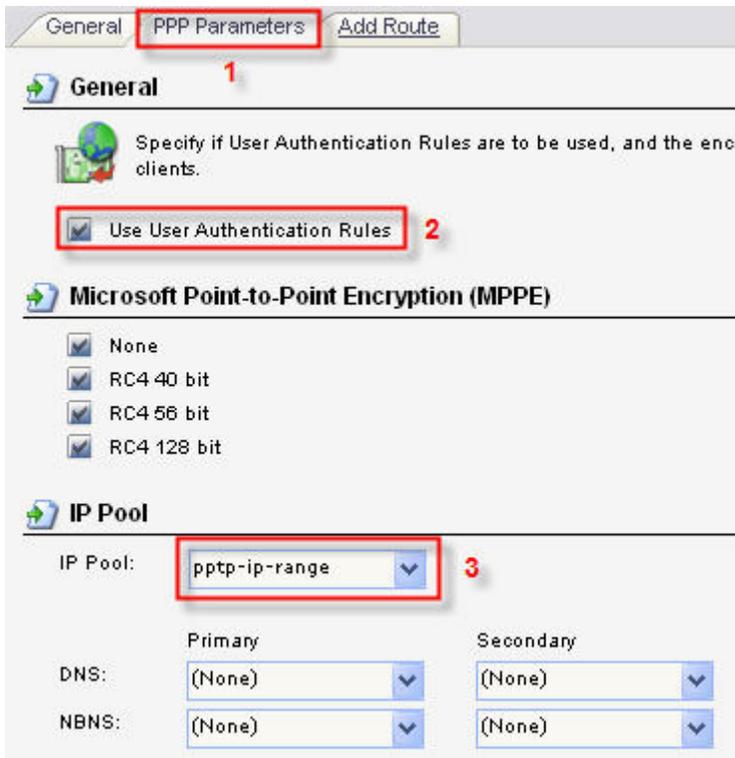
Enter settings under “General” exactly as in picture below.



The screenshot shows a web-based configuration interface with three tabs: "General", "PPP Parameters", and "Add Route". The "General" tab is active. Below the tabs, there is a sub-header "General" with a globe icon and a description: "A PPTP/L2TP server interface terminates PPP (Point-to-Point Protocol) connections." Below this, there are five configuration fields:

Name:	<input type="text" value="pptp-tunnel"/>
Inner IP Address:	<input type="text" value="pptp-server-ipaddress"/>
Tunnel Protocol:	<input type="text" value="PPTP"/>
Outer Interface Filter:	<input type="text" value="any"/>
Server IP:	<input type="text" value="wan_ip"/>

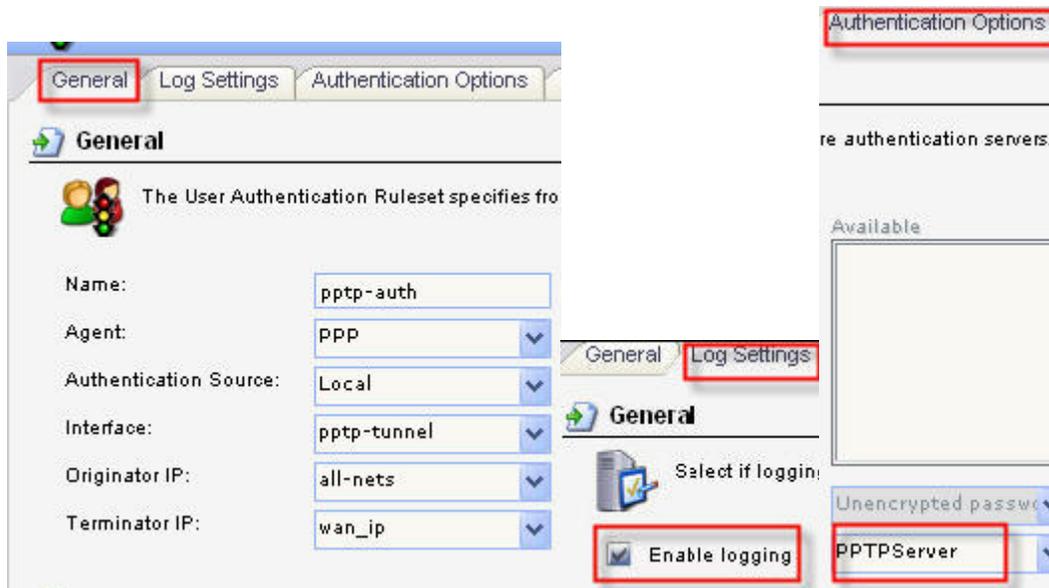
Under “PPP Parameters” select “use authentication rules” and in the “IP Pool” drop-down menu choose “pptp-ip-range”



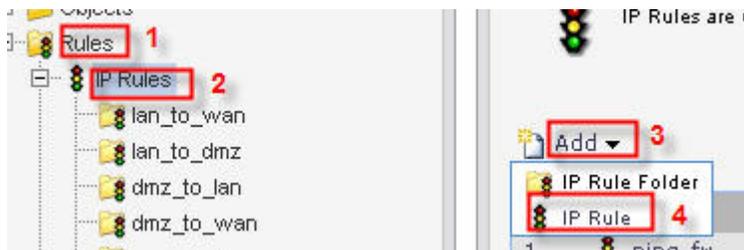
Now we need to create User Authentication rules for the PPTP tunnel. Click User Authentication → User Authentication Rules → Add → UserAuthRule.



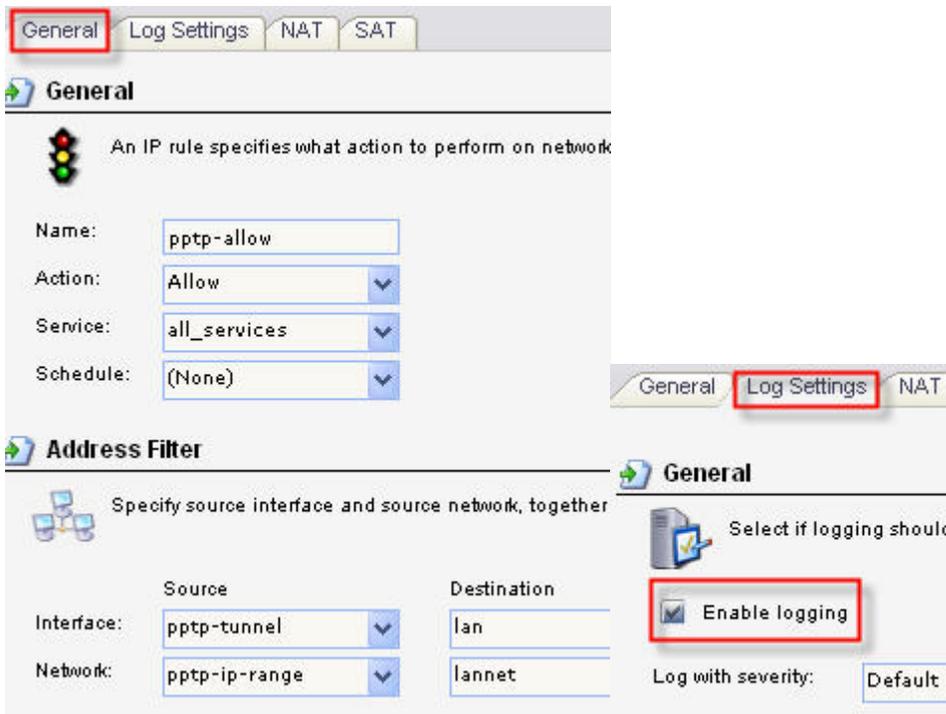
Enter settings under “General”, “Log Settings” and “Authentication Options” exactly as in pictures below.



Now we will create IP Rules for the PPTP tunnel. Click on Rules → IP Rules → Add → IP Rule.



Enter settings under “general” and “Log settings” exactly as in the picture below.



Now you “save and activate”.



Now your firewall is set up with a PPTP server to allow remote users onto your network.