

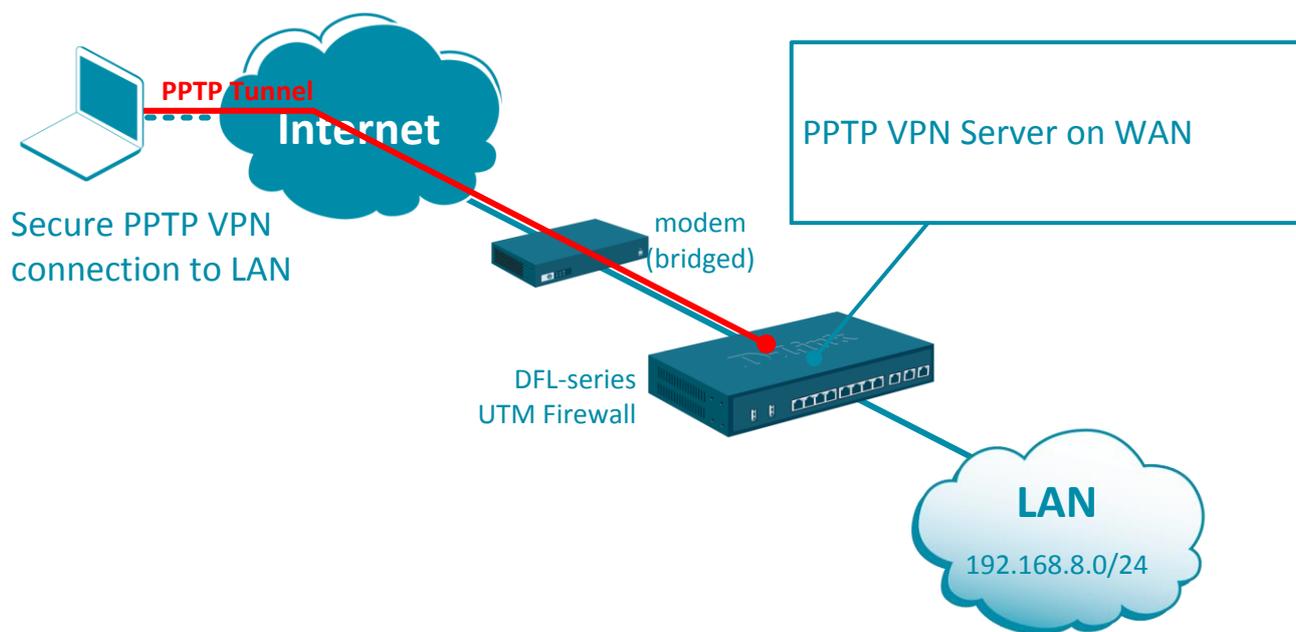
# **NETDEFEND**

## Configuration examples for the D-Link NetDefend Firewall series



## Setting up PPTP Server for remote access to LAN

This configuration example is based on the following setup:



**Step 1.** Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is "admin" and password is "admin".

**Step 2.** Set your firewall's WAN settings as per Internet provider requirements. In our example WAN is set with a static IP address.

**Step 3.** Add a new object into the Address Book: "PPTP IP Range". Specify the range of IP addresses which will be assigned to the clients connecting via PPTP. These addresses should be from the IP subnet used on your LAN. Make sure this range does not conflict with the range used by the DHCP Server on your LAN.



**Step 4.** Go to System > Device > Local User Databases.

Add new Local User Database for the PPTP Server.

The screenshot shows the 'Local User Databases' configuration page. The navigation menu on the left includes 'Device', 'Monitoring', and 'Users', with 'Local User Databases' selected. The main content area has a title 'Local User Databases' and a subtitle 'Manage the local user databases and user accounts used for authentication purposes'. There is a '+ Add' button and a 'Filter' input field. A table lists the existing databases:

#	Name	Comments
1	AdminUsers	
2	PPTP_users	

At the bottom right, there is a note: 'Right-click on a row'.

Open the newly created User Database and add your VPN users. Specify Username and Password for each remote user.

The screenshot shows the 'PPTP\_users' configuration page. The 'Users' tab is selected. A '+ Add' button is visible. A 'User' configuration dialog is open, showing the following fields:

- Name: user1
- Password: [masked]
- Confirm Password: [masked]
- Groups: [empty]

There is a note: 'Note! Existing passwords will always be with 8 characters to hide the actual length'.

**Step 5.** Go to Network > L2TP/PPTP Servers.

Add a new L2TP/PPTP Server.

Inner IP Address – set as “LAN\_IP”.

Tunnel Protocol – “PPTP”.

Outer Interface – “WAN” (or if WAN is set with PPPoE select “ANY”).

Server IP – set as “WAN\_IP”.

The screenshot shows the D-Link web interface for configuring PPTP/L2TP Servers. The top navigation bar includes Status, System, Objects, Network (selected), and Policies. Under Network, there are sub-tabs for Interfaces and VPN (selected), Routing, and Network Services. A left sidebar lists various network features, with PPTP/L2TP Servers highlighted. The main content area is titled 'PPTP/L2TP Servers' and includes a description: 'Add, remove and configure PPTP/L2TP (Point-to-Point Tunneling Protocol / Layer Protocol) servers used for terminating PPTP/L2TP-based VPN tunnels.' Below this are '+ Add' and 'Advanced Settings' buttons, and a search filter. A table lists existing servers:

#	Name	Tunnel pro...	Inner IP ad...	Outer inter...	IP pool	Outer
1	PPTP_Servi	PPTP	lan_ip	any	PPTP-IP-Ra	wa

A detailed view of the 'PPTP\_Server' configuration is shown below, with a red box highlighting the Inner IP Address, Tunnel Protocol, Outer Interface Filter, and Server IP fields. The configuration is as follows:

- Name: PPTP\_Server
- Inner IP Address: lan\_ip
- Tunnel Protocol: PPTP
- Outer Interface Filter: any
- Server IP: wan1\_ip

**Step 6.** In your PPTP Server settings click on the **PPP Parameters** tab and make sure the correct IP Pool is selected. Set the DNS parameters as well.

**PPTP\_Server**  
A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.

General **PPP Parameters** Add Route Virtual Routing

Specify if User Authentication Rules are to be used, and the encryption strengths allowed. Also specify the IP address assignment and the DNS/WINS server information to hand out to connected clients.

Use User Authentication Rules

**IP Pool**

IP Pool: PPTP-IP-Range

DNS: Primary: DHCP\_DNS1 Secondary: DHCP\_DNS2

NBNS/WINS: (None) (None)

Click on the **Add Route** tab and add “LAN” interface under Proxy ARP.

**PPTP\_Server**  
A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.

General PPP Parameters **Add Route** Virtual Routing

**Filter**  
Restricts networks for which routes may automatically be added.

Allowed Networks: all-nets

**Proxy ARP**

Available	Selected
dmz wan1	lan

+ Include      × Remove

**Step 7.** Go to Policies > User Authentication > User Authentication Rules. Add a new rule. Set Agent as “L2TP/PPPTP”, Authentication as “Local”, Interface – “PPTP\_Server”.

The screenshot shows the 'Authentication Rules' configuration page. The 'Policies' tab is selected, and the 'User Authentication' sub-tab is active. A table lists authentication rules, with 'PPTP-Auth' selected. A modal window shows the configuration for 'PPTP-Auth' with fields for Name, Authentication agent, Authentication Source, Interface, Originator IP, and Terminator IP. The 'Authentication agent' field is highlighted with a red box.

#	Name	Authentication a...	Authentication s...	Interface	Comments
1	PPTP-Auth				

**PPTP-Auth**  
The User Authentication Ruleset specifies from where users are all

**General** Log Settings Authentication Options

Name: PPTP-Auth

Authentication agent: L2TP/PPPTP/SSL VPN

Authentication Source: Local

Interface: PPTP\_Server

Originator IP: all-nets

Terminator IP: wan1\_ip

**i** For XAuth an

Click on the **Authentication Options** tab. Make sure that under Local User DB you have your User Database selected.

The screenshot shows the 'Authentication Options' tab for the 'PPTP-Auth' rule. The 'Authentication Options' tab is selected. The 'Local User DB' field is highlighted with a red box.

**PPTP-Auth**  
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

**General** Log Settings **Authentication Options** Accounting Agent Options Restrictions

RADIUS servers

LDAP servers

Available Selected

+ Include x Remove ^ v

RADIUS Method: Unencrypted password / PAP

Local User DB: PPTP\_users

**Step 8.** Go to Policies > Main IP Rules. Create a new IP Rule to allow PPTP Tunnel communication with LAN:  
Set Action as "Allow".  
Set Source Interface/Network as PPTP\_Server/PPTP-IP-Range.  
Set Destination Interface/Network as LAN/LAN Net.

### IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

**General**   Log Settings   NAT   SAT   Multiplex SAT   SLB SAT   SLI

Name: PPTP\_Allow

Action: Allow ⓘ NAT, SAT, SLB SAT and Multiplex SAT are not usable with

Service: all\_services

Schedule: (None)

#### Address Filter

Specify source interface and source network, together with destination interface and destination network match.

	Interface	Network
Source:	PPTP_Server	PPTP-IP-Range
Destination:	lan	lannet

**Step 9.** After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

**NOTE:** If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.

