

How to setup PPTP server on DFL-160

Topology:



Setup:

(1) WAN type chooses "static".

The screenshot shows the D-Link web interface for the DFL-160 device. The top navigation bar includes 'SYSTEM', 'FIREWALL', 'TOOLS', 'STATUS', and 'MAINTENANCE'. The left sidebar lists various settings categories, with 'INTERNET CONNECTION' selected. The main content area is divided into sections: 'GENERAL', 'DHCP SETUP', 'STATIC CONNECTION', and 'PPPOE CONNECTION'. The 'GENERAL' section shows 'Internet Connection Type' set to 'Static'. The 'STATIC CONNECTION' section shows the following configuration:

IP:	218.210.16.28
Network:	255.255.255.248
Default Gateway:	218.210.16.25
Primary DNS Server:	168.95.1.1
Secondary DNS Server:	8.8.8.8
MTU:	1500

The 'Helpful Hints' section on the right provides additional information: 'The default WAN interface setting is DHCP which will retrieve all required IP addresses automatically from a DHCP server without any further configuration changes. When configuring other methods to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP). If you are having trouble accessing the Internet through the firewall, double check any settings you have entered on this page and verify them with your ISP.'

(2) Go to firewall > VPN>General. Tunnel protocol chooses PPTP.

The screenshot shows the D-Link firewall configuration interface for the VPN General settings. The 'FIREWALL' tab is selected, and the 'VPN' sub-tab is active. The 'GENERAL' section is highlighted with a red box. The 'Name' field is set to 'PPTP' and the 'Tunnel Protocol' dropdown is also set to 'PPTP', both highlighted with red boxes. Below these, there are checkboxes for 'Require IPsec encryption' (unchecked), 'PSK - Pre-Shared Key' (with an empty input field), and 'Confirm PSK' (with an empty input field). A note states: 'Note! Existing PSK will always be shown with 8 characters to hide the actual length.' The 'IP POOL SETTINGS' section shows the 'IP Pool Address Range' set to '192.168.10.150' to '192.168.10.199' and the 'Relay DNS queries on behalf of clients' checkbox checked. The 'Helpful Hints' section on the right provides additional information about PPTP/L2TP authentication and IP pool configuration. The interface includes a top navigation bar with 'SYSTEM', 'FIREWALL', 'TOOLS', 'STATUS', and 'MAINTENANCE' tabs, and a left sidebar with various configuration options like 'OUTBOUND LAN TRAFFIC', 'VPN USERS', and 'SCHEDULES'. The bottom of the page shows 'Copyright © D-Link'.

(3) Go to firewall > VPN>Security. Please follow my red area to choose button.

The screenshot shows the D-Link firewall configuration interface for the VPN Security settings. The 'FIREWALL' tab is selected, and the 'VPN' sub-tab is active. The 'SECURITY' section is highlighted with a red box. The 'AUTHENTICATION' section contains four checkboxes: 'Allow un-authenticated users.' (unchecked), 'Allow users to authenticate using PAP.' (checked), 'Allow users to authenticate using CHAP.' (checked), and 'Allow users to authenticate using MS-CHAP v2.' (checked). The 'MICROSOFT POINT-TO-POINT ENCRYPTION (MPPE)' section contains five checkboxes: 'None' (unchecked), 'RC4 40 bit' (checked), 'RC4 56 bit' (checked), 'RC4 128 bit' (checked), and 'Stateful MPPE (less secure, use only for compatibility)' (unchecked). The 'Helpful Hints' section on the right provides additional information about PPTP/L2TP authentication and IP pool configuration. The interface includes a top navigation bar with 'SYSTEM', 'FIREWALL', 'TOOLS', 'STATUS', and 'MAINTENANCE' tabs, and a left sidebar with various configuration options like 'OUTBOUND LAN TRAFFIC', 'VPN USERS', and 'SCHEDULES'. The bottom of the page shows 'Copyright © D-Link'.

(4) Go to firewall > VPN users. Add new PPTP user account.

The screenshot shows the D-Link DFL-160 Firewall configuration interface. The top navigation bar includes 'SYSTEM', 'FIREWALL', 'TOOLS', 'STATUS', and 'MAINTENANCE'. The 'FIREWALL' tab is selected. On the left sidebar, 'VPN USERS' is highlighted. The main content area is titled 'VPN USERS' and contains an 'Add' button and a form with a 'Name' field containing 'test'. A note below the form says 'Right-click on a row for additional options.' On the right, there is a 'Helpful Hints' section with text: 'Clients connecting to the firewall via VPN (PPTP/L2TP/IPsec) will be authenticated using this database.'

(5) When PPTP client connect to DFL-160 successful, you can go to status>user authentication to check current login users.

The screenshot shows the D-Link DFL-160 Firewall configuration interface. The top navigation bar includes 'SYSTEM', 'FIREWALL', 'TOOLS', 'STATUS', and 'MAINTENANCE'. The 'STATUS' tab is selected. On the left sidebar, 'USER AUTHENTICATION' is highlighted. The main content area is titled 'USER AUTHENTICATION STATUS' and contains a table with the following data:

Username	IP Address	Interface	Session Timeout	Idle Timeout	Logged in as	Forcibly Log Out
test	192.168.10.150	PPTP		28m		

END