

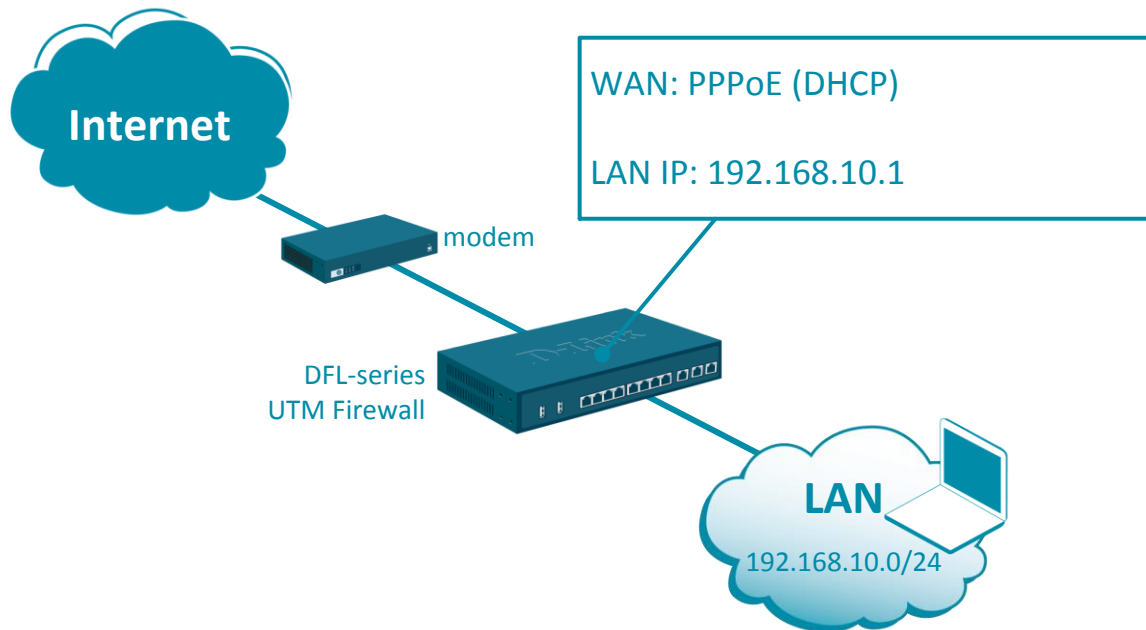
# **NETDEFEND**

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



## How to setup WAN with PPPoE authentication

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.** Go to Network > Interfaces and VPN > PPPoE. Create a new PPPoE Tunnel object. Link it to physical interface WAN. Specify username and password of the PPPoE account.

PPPoE\_on\_WAN1

A PPPoE interface is a PPP (point-to-point protocol) tunnel over an existing physical Ethernet interface. Its IP address is assigned by the remote network.

**General** Authentication Dial-on-demand Advanced Virtual Routing

Name: PPPoE\_on\_WAN1

Physical Interface: wan1

Remote Network: all-nets

Schedule: (None)

Username: account@provider.com

Password: .....

Confirm Password: .....

Service Name: MyProvider\_PPPoE

Note! Existing passwords will always be shown with 8 characters

Go to Policies > Main IP Rules > LAN\_to\_WAN. You should see the default “Allow\_Standard” rule that performs Network Address Translation (NAT) for all outgoing traffic.

Modify the existing or create a new rule - make sure that the Destination Interface is set to the newly created PPPoE tunnel.

**allow\_standard**

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 SL

Name:

Action:  **i** NAT, SAT, SLB SAT and Multiplex SAT are not usable with this configuration.

Service:

Schedule:

**Address Filter**

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

Source:

Destination:

**Step 3.** 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.

Setup Wizard Configuration Notifications 0 admin

**Status** System

Run-time Information M

**Save Configuration**

Save and activate changes n

**Save and Activate**

The configuration has been changed.

[Save and Activate](#) [View Changes](#) [Discard changes](#)

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Note: Due to configuration changes the currently active user admin (192.168.10.151) will no longer be automatically logged on after the activation of the new configuration. You will need to manually login with an administrator user account to verify the new configuration.

OK Cancel