



Configuration examples for the D-Link NetDefend Firewall series

DFL-210/260/800/860/1600/2500

Scenario: Virtual private network using
a PPTP (or L2TP) lan-to-lan tunnel

Last update: 2007-07-31

Overview

In this document, the notation *Objects->Address book* means that in the tree on the left side of the screen **Objects** first should be clicked (expanded) and then **Address Book**.

Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and lan3 not just lan.

The screenshots in this document is from firmware version 2.11.02. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

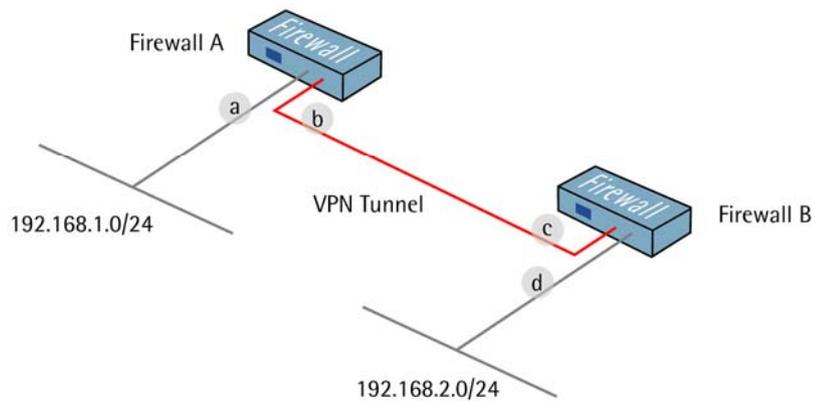
To prevent existing settings to interfere with the settings in these guides, reset the firewall to factory defaults before starting.

How to configure virtual private network using a PPTP (or L2TP) lan-to-lan tunnel

Create one lan-to-lan PPTP VPN tunnel between firewall A and B. Firewall B is the server and firewall A the client.

If a L2TP tunnel is going to be used, instead of PPTP, follow the steps in this guide but change tunnel protocol from PPTP to L2TP in step 2 and 6. The other settings are same in both cases.

- a IP: 192.168.1.1
- b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.2
- c IP: 192.168.110.2
Mask: 255.255.255.0
Gateway: 192.168.110.1
- d IP: 192.168.2.1



1. Firewall A - Addresses

Go to *Objects* -> *Address book* -> *InterfaceAddresses*.

Edit the following items:

Change **lan_ip** to **192.168.1.1**

Change **lanenet** to **192.168.1.0/24**

Change **wan1_ip** to **192.168.110.1**

Change **wan1net** to **192.168.110.0/24**

Go to *Objects* -> *Address book*.

Add a new Address Folder called **RemoteHosts**.

In the new folder, add a new IP address:

Name: **fwA-remotenet**

IP Address: **192.168.1.0/24**

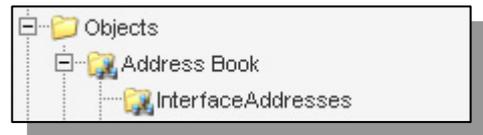
Click Ok

In the same folder, add a new IP address:

Name: **fwB-remotegw**

IP Address: **192.168.110.2**

Click Ok



2. Firewall A - PPTP client interface

Go to *Interfaces* -> *PPTP/L2TP Clients*.

Add a new PPTP/L2TP Client.

In the General tab:

General:

Name:	<input type="text" value="fwB-pptp"/>
Tunnel Protocol:	<input type="text" value="PPTP"/> ▼
Remote Endpoint:	<input type="text" value="fwB-remotegw"/> ▼
Remote Network:	<input type="text" value="fwB-remotenet"/> ▼

Name: **PPTPClient**

Tunnel Protocol: **PPTP**

Remote Endpoint: **fwB-remotegw**

Remote Network: **fwB-remotenet**

Authentication:

Username:	<input type="text" value="userA"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>

Username: userA

In the Security tab:

Authentication:

 Authentication
<input type="checkbox"/> Allow No Authentication
<input type="checkbox"/> Unencrypted Password (PAP)
<input type="checkbox"/> Challenge Handshake Authentication Protocol (CHAP)
<input type="checkbox"/> Microsoft CHAP (MS-CHAP)
<input checked="" type="checkbox"/> Microsoft CHAP Version 2 (MS-CHAP v2)

The only options that should be checked is **Microsoft CHAP Version 2 (MS-CHAP v2)**

Microsoft Point-to-Point Encryption (MPPE):

 Microsoft Point-to-Point Encryption (MPPE)
<input type="checkbox"/> None
<input type="checkbox"/> RC4 40 bit
<input type="checkbox"/> RC4 56 bit
<input checked="" type="checkbox"/> RC4 128 bit

Only **RC4 128 bit** should be checked. (Using MS-CHAP v2 and 128 bit is the most secure option.)

3. Firewall A - Rules

Go to *Rules* -> *IP Rules*.

Create a new IP Rules Folder called **lan_to_fwB-pptp**

In the new folder, create a new IP Rule.

In the **General** tab:

General:

Name:	<input type="text" value="allow_all"/>
Action:	<input type="text" value="Allow"/>
Service:	<input type="text" value="all_services"/>
Schedule:	<input type="text" value="(None)"/>

Name: **allow_all**

Action: **Allow**

Service: **all_services**

Address Filter:

	Source	Destination
Interface:	<input type="text" value="lan"/>	<input type="text" value="fwB-pptp"/>
Network:	<input type="text" value="lannet"/>	<input type="text" value="fwB-remotenet"/>

Source Interface: **lan**

Source Network: **lannet**

Destination Interface: **fwB-pptp**

Destination Network: **fwB-remotenet**

Click Ok.

Create a second rule in the same folder.

In the General tab:

General:

Name: **allow_all**

Action: **Allow**

Service: **all_services**

Address Filter:

	Source	Destination
Interface:	<input type="text" value="fwB-pptp"/>	<input type="text" value="lan"/>
Network:	<input type="text" value="fwB-remotenet"/>	<input type="text" value="lannet"/>

Source Interface: **fwB-pptp**

Source Network: **fwB-remotenet**

Destination Interface: **lan**

Destination Network: **lannet**

Click Ok.

Save and activate the configuration on firewall A.

4. Firewall B - Addresses

Go to *Objects -> Address book -> InterfaceAddresses*.

Edit the following items:

Change **lan_ip** to **192.168.2.1**

Change **lanenet** to **192.168.2.0/24**

Change **wan1_ip** to **192.168.110.2**

Change **wan1net** to **192.168.110.0/24**

Go to *Objects -> Address book*.

Add a new Address Folder called **RemoteHosts**.

In the new folder, add a new IP address

Name: **fwA-remotenet**

IP Address: **192.168.1.0/24**

Add a new Address Folder called **IPpools**.

In the new folder, add a new IP address.

Name: **fwA-ippool**

IP Address: **192.168.2.100-192.168.2.199**

Click Ok

5. Firewall B - User database

Go to *User Authentication* -> *Local User Databases*.

Add a new Local User Database called **PPPUsers**.

In the new database, add a new User:

General:

Username:	<input type="text" value="userA"/>
Password:	<input type="password" value="*****"/>
Confirm Password:	<input type="password" value="*****"/>
Groups:	<input type="text"/>

Username: **userA**

Per-user PPTP/L2TP IP Configuration:

 Per-user PPTP/L2TP IP Configuration	
Static Client IP Address:	<input type="text" value="(None)"/> ▼
Networks behind user:	<input type="text" value="fwA-remotenet"/> ▼
Metric for networks:	<input type="text" value="90"/>

Static Client IP Address: **(None)**

Networks behind user: **fwA-remotenet**

Metric for networks: **90**

6. Firewall B - PPTP Server interface

Go to *Interfaces* -> *PPTP/L2TP Server*.

Add a new PPTP/L2TP Server

In the *General* tab:

General:

Name:	fwA-pptp
Inner IP Address:	lan_ip
Tunnel Protocol:	PPTP
Outer Interface Filter:	wan1
Server IP:	wan1_ip

Name: **fwA-pptp**

Inner IP Address: **lan_ip**

Tunnel Protocol: **PPTP**

Outer Interface Filter: **wan1**

Server IP: **wan1_ip**

In the *PPP Parameters* tab:

General:

Check the **Use User Authentication Rules** option

Microsoft Point-to-Point Encryption (MPPE):

 Microsoft Point-to-Point Encryption (MPPE)
<input type="checkbox"/> None
<input type="checkbox"/> RC4 40 bit
<input type="checkbox"/> RC4 56 bit
<input checked="" type="checkbox"/> RC4 128 bit

Only **RC4 128 bit** should be checked.

IP Pool:

The screenshot shows the 'IP Pool' configuration page. At the top, there is a header with a green arrow icon and the text 'IP Pool'. Below this, there is a dropdown menu for 'IP Pool' with the value 'fwA-ippool'. Underneath, there are two columns: 'Primary' and 'Secondary'. Each column has two dropdown menus: 'DNS' and 'NBNS', both of which are currently set to '(None)'.

IP Pool: **fwA-ippool**

In the Add Route tab:

Proxy ARP:

The screenshot shows the 'Proxy ARP' configuration page. At the top, there is a header with a green arrow icon and the text 'Proxy ARP'. Below this, there is a text label 'Interface to ARP publish the added route on.'. Underneath, there are two columns: 'Available' and 'Selected'. The 'Available' column contains a list of interfaces: 'dmz', 'lan', and 'wan2'. The 'Selected' column contains the interface 'wan1'. Between the two columns, there are two buttons: a right-pointing arrow and a left-pointing arrow, used for moving items between the lists.

Proxy ARP: **wan1**

Click Ok.

7. Firewall B - User authentication rules

Go to *User Authentication* -> *User Authentication Rules*.

Add a new User Authentication Rule.

In the *General* tab:

General:

Name:	<input type="text" value="pptp-ua"/>
Agent:	<input type="text" value="PPP"/> ▼
Authentication Source:	<input type="text" value="Local"/> ▼
Interface:	<input type="text" value="fwA-pptp"/> ▼
Originator IP:	<input type="text" value="fwA-remotegw"/> ▼
Terminator IP:	<input type="text" value="wan1_ip"/> ▼

 For XAuth and PPP, this is the tunnel originator IP.

Name: **pptp-ua**

Agent: **PPP**

Authentication Source: **Local**

Interface: **fwA-pptp**

Originator IP: **fwA-remotegw**

Terminator IP: **wan1_ip**

In the *Authentication Options* tab:

General:

Radius Method:	<input type="text" value="PAP"/> ▼
Local User DB:	<input type="text" value="PPPUsers"/> ▼

Local User DB: **PPPUsers**

Click *Ok*.

8. Firewall B - Rules

Go to *Rules* -> *IP Rules*.

Create a new IP Rules Folder called **lan_to_fwA-pptp**

In the new folder, create a new IP Rule.

In the **General** tab:

General:



The screenshot shows a configuration window for an IP rule. It contains four rows of settings, each with a label on the left and a corresponding input field or dropdown menu on the right. The settings are: Name: allow_all (text input); Action: Allow (dropdown menu); Service: all_services (dropdown menu); and Schedule: (None) (dropdown menu).

Name:	allow_all
Action:	Allow
Service:	all_services
Schedule:	(None)

Name: **allow_all**

Action: **Allow**

Service: **all_services**

Address Filter:

Source Interface: **lan**

Source Network: **lanet**

Destination Interface: **fwA-pptp**

Destination Network: **fwA-remotenet**

Click Ok.

Create a second rule in the same folder.

In the General tab:

General:

Name: **allow_all**

Action: **Allow**

Service: **all_services**

Address Filter:

Source Interface: **fwA-pptp**

Source Network: **fwA-remotenet**

Destination Interface: **lan**

Destination Network: **lanet**

Click Ok.

Save and activate the configuration on firewall A.