Configuration examples for the D-Link NetDefend Firewall series

DFL-210/800/1600/2500

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

Last update: 2005-10-20

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 2.04.00. If you are using a later 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.

7b

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.

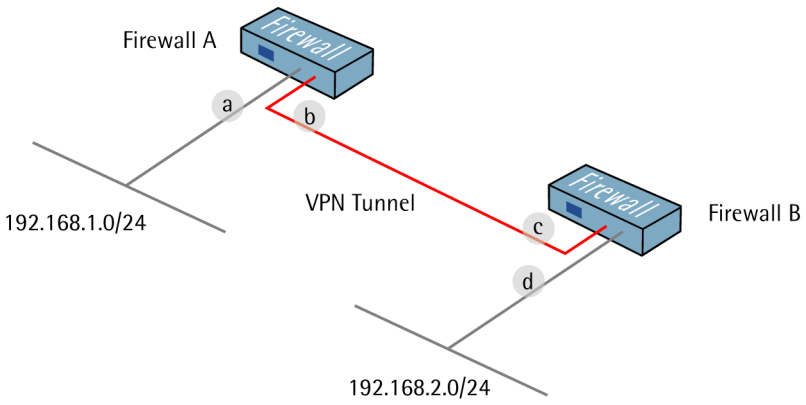
If a L2TP tunnel is going to be used, instead of PPTP, follow the steps in this guide but change tunnel protocol from PPTP to L2TP in step 2 and 6. The other settings are same in both cases.

a IP: 192.168.1.1

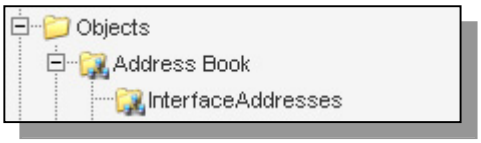
b IP: 192.168.110.1
Mask: 255.255.255.0
Gateway: 192.168.110.2

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 **lannet** 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 IP4 Host/Network:
Name: **fwA-remotenet**
IP Address: **192.168.1.0/24**

Click Ok

2. Firewall A - PPTP client interface

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

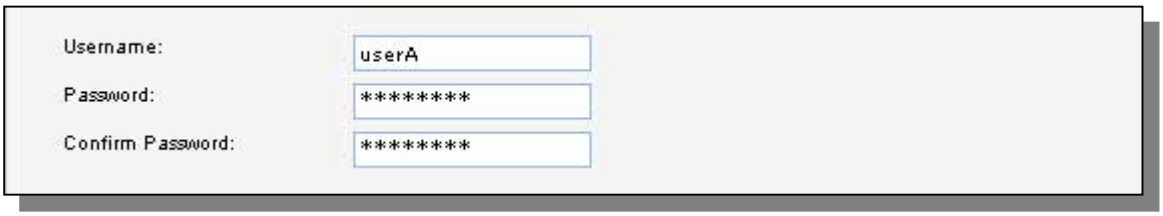
Add a new L2TP/PPTP Client.

In the General tab:

General:

Name: **PPTPClient**
Tunnel Protocol: **PPTP**
Remote Endpoint: **fwB-remotegw**
Remote Network: **fwB-remotenet**

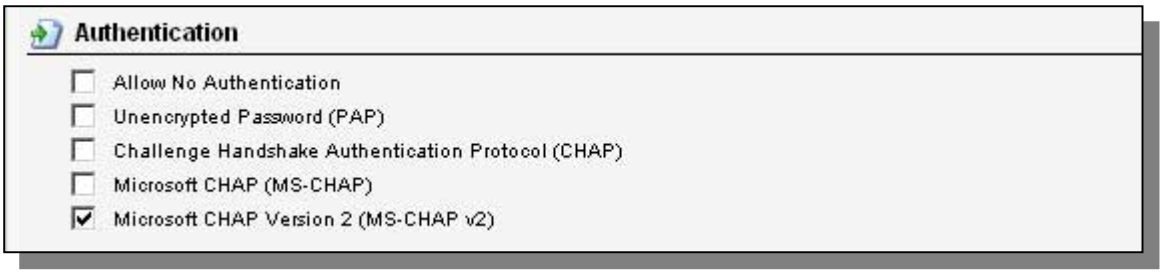
Authentication:



Username: userA

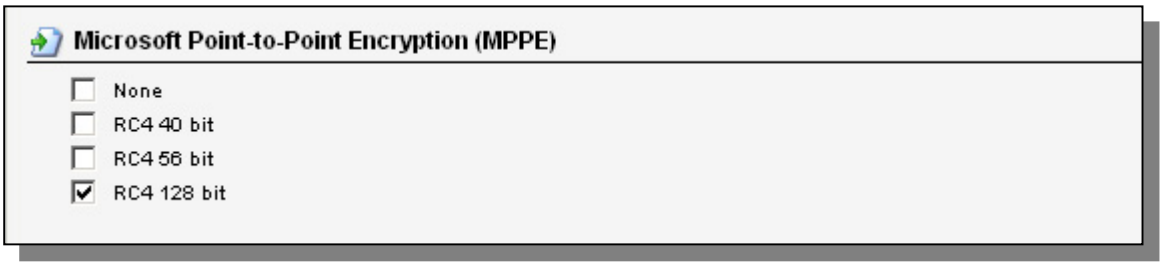
In the Security tab:

Authentication:



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

Microsoft Point-to-Point Encryption (MPPE):



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`**

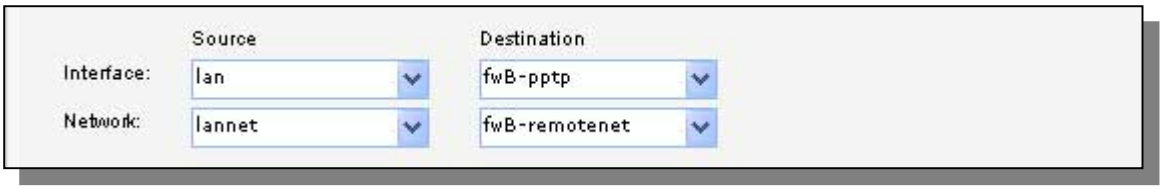
In the new folder, create a new IP Rule.

In the General tab:

General:

Name: **`allow_all`**
Action: **`Allow`**
Service: **`all_services`**

Address Filter:



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 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 **lannet** 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 IP4 Host/Network:
Name: **fwA-remotenet**
IP Address: **192.168.1.0/24**

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

In the new folder, add a new IP4 Host/Network:
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*.

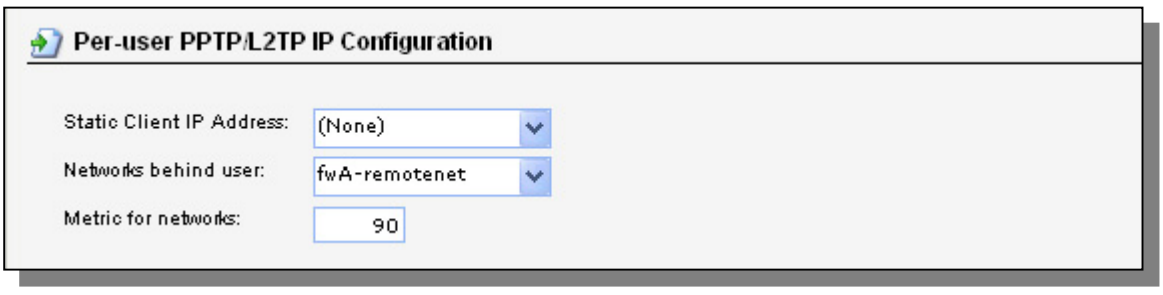
Add a new Local User Database called **PPPUsers**.

In the new database, add a new User:

General:

Username: **userA**

Per-user PPTP/L2TP IP Configuration:



Static Client IP Address: **(None)**
Networks behind user: **fwA-remotenet**
Metric for networks: **90**

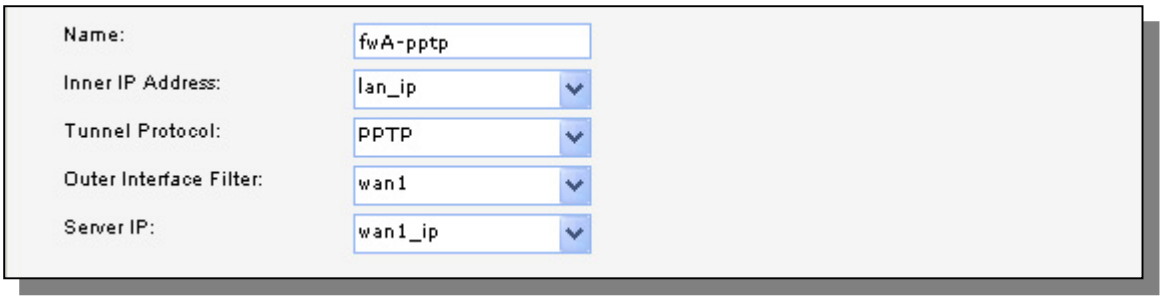
6. Firewall B - PPTP Server interface

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

Add a new L2TP/PPTP Server.

In the General tab:

General:

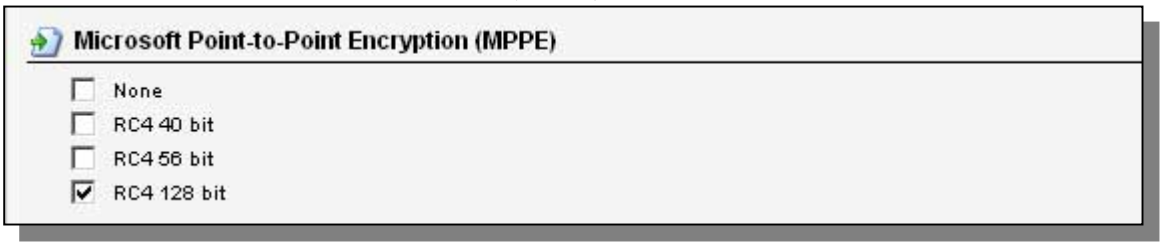


Name: **`fwA-pptp`**
Inner IP Address: **`lan_ip`**
Tunnel Protocol: **`PPTP`**
Outer Interface Filter: **`wan1`**
Server IP: **`wan1_ip`**

In the PPP Parameters tab:

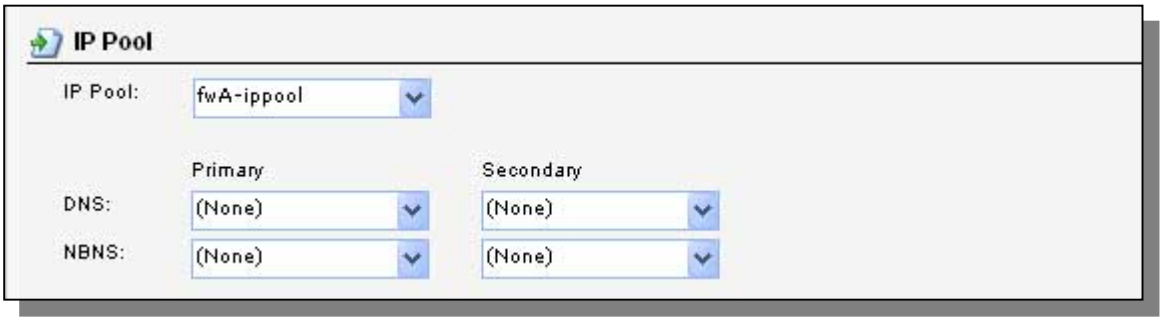
General:
Check the **`Use User Authentication Rules`** option

Microsoft Point-to-Point Encryption (MPPE):



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

IP Pool:



IP Pool: **`fwA-ippool`**

Click Ok.

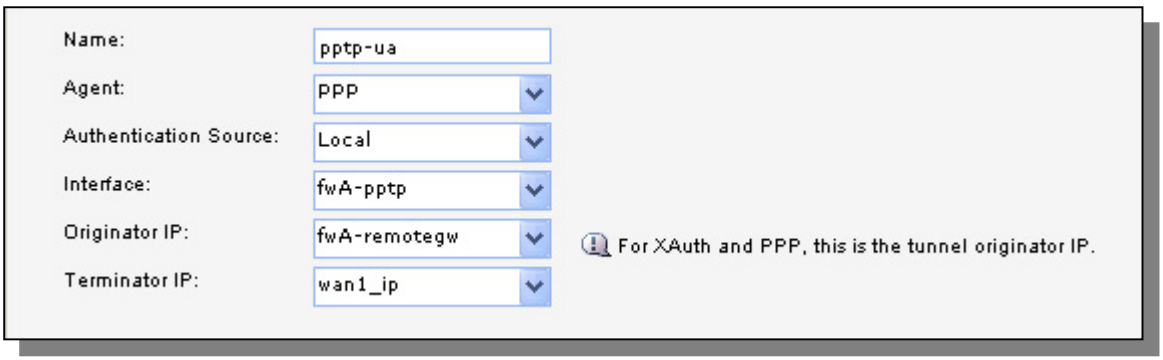
7. Firewall B - User authentication rules

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

Add a new User Authentication Rule.

In the General tab:

General:



Name: **pptp-ua**
Agent: **PPP**
Authentication Source: **Local**
Interface: **fwA-pptp**
Originator IP: **fwA-remotegw**
Terminator IP: **wan1_ip**

In the Authentication Options tab:

General:

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:

Name: **allow_all**
Action: **Allow**
Service: **all_services**

Address Filter:
Source Interface: **lan**
Source Network: **lannet**
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: **lannet**

Click Ok.

Save and activate the configuration on firewall A.