



Configuration examples for the D-Link NetDefend Firewall series

Scenario: How to configure IPSec VPN LAN-to-LAN Tunnel

Platform Compatibility: All NetDefend Firewall Series

Last update: 2008-03-07

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**.

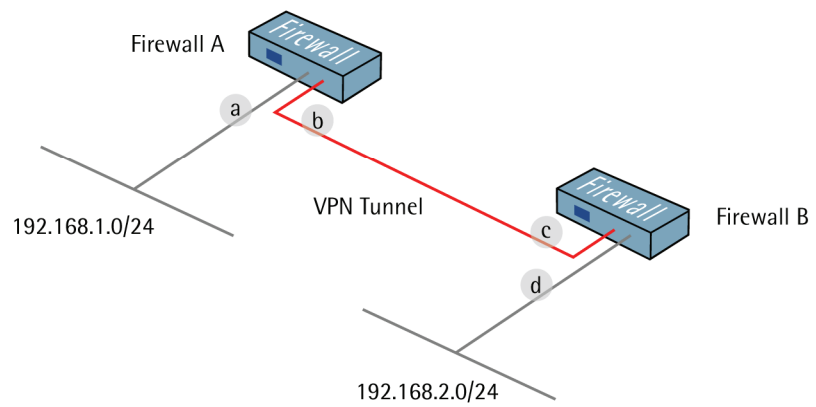
Most of the examples in this document are adapted for the DFL-800. The same settings can easily be used for all other models in the series. The only difference is the names of the interfaces. Since the DFL-1600 and DFL-2500 has more than one lan interface, the lan interfaces are named lan1, lan2 and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

The screenshots in this document is from firmware version 2.12.00. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

How to configure IPsec VPN LAN-to-LAN Tunnel

Create one lan-to-lan IPsec VPN tunnel between firewall A and B.

- 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: **fwB-remotenet**

IP Address: 192.168.2.0/24

Click Ok

In the same folder, add a new IP address:

Name: **fwB-remotegw**

IP Address: 192.168.110.2

Click Ok

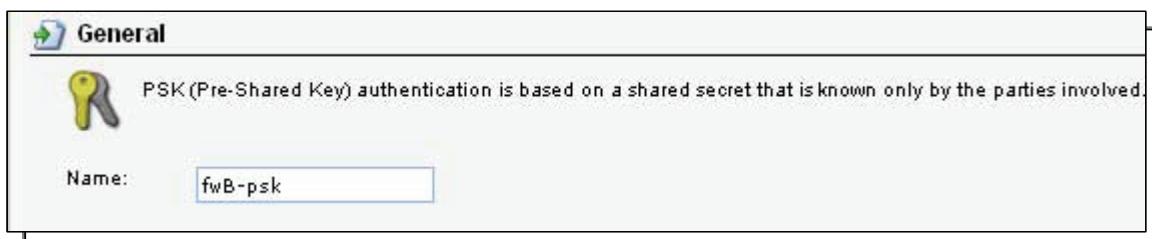


2. Firewall A - Pre-shared keys

Go to *Objects* -> *Authentication Objects*

Add a new **Pre-Shared Key**.

General:

A screenshot of a configuration window titled 'General'. It features a key icon and the text: 'PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.' Below this, there is a 'Name:' label and a text input field containing 'fwB-psk'.

Name: **fwB-psk**

Shared secret:



Passphrase

Shared Secret:

Confirm Secret:

Select **Passphrase** and enter a shared secret

Click **Ok**.

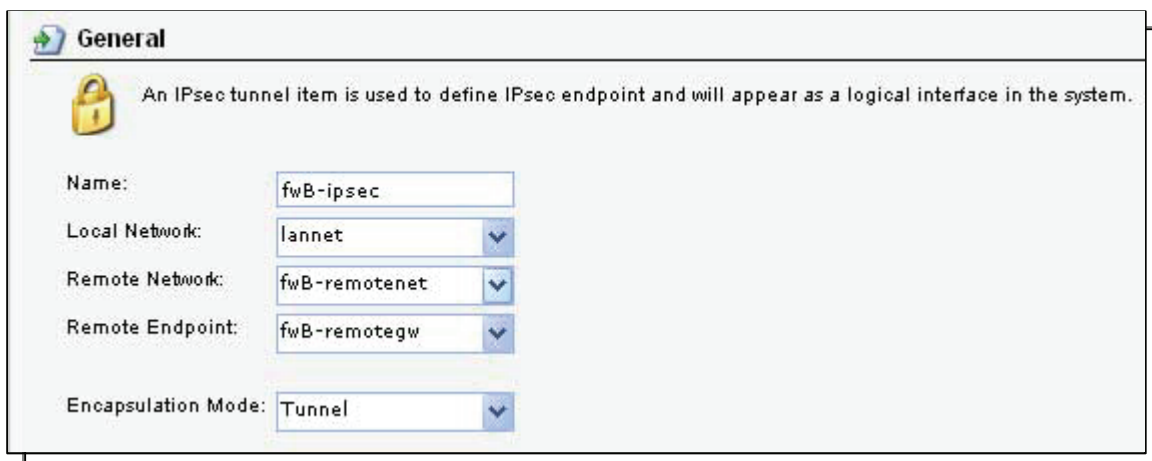
3. Firewall A - IPsec interface

Go to *Interfaces* -> *IPsec*.


Add a new IPsec Tunnel.

In the **General** tab:

General:



General

 An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Name:

Local Network: ▼

Remote Network: ▼

Remote Endpoint: ▼

Encapsulation Mode: ▼

Name: **fwB-ipsec**

Local Network: **lannet**

Remote Network: **fwB-remotenet**

Remote Endpoint: **fwB-remotegw**

Encapsulation Mode: **Tunnel**

Algorithms:

Algorithms

IKE Algorithms: High

IKE Life Time: 28800 seconds

IPsec Algorithms: High

IPsec Life Time: 3600 seconds

IPsec Life Time: 0 kilobytes

IKE Algorithms: High
IKE Life Time: 28800
IPsec Algorithms: High
IPsec Life Time: 3600
IPsec Life Time: 0

In the Authentication tab:

Authentication:

Pre-Shared Key

Pre-Shared Key: fwB-psk

Select **Pre-Shared Key** and **fwB-psk**.

Click Ok.

4. Firewall A - Rules

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

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

In the new folder, create a new IP Rule.

In the **General** tab:

General:

Name: allow_all

Action: Allow

Service: all_services

Schedule: (None)

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

Address Filter:

	Source	Destination
Interface:	lan	fwB-ipsec
Network:	lannet	fwB-remotenet

Source Interface: **lan**
Source Network: **lannet**
Destination Interface: **fwB-ipsec**
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
Schedule:	(None)

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

Address Filter:

	Source	Destination
Interface:	fwB-ipsec	lan
Network:	fwB-remotenet	lannet

Source Interface: **fwB-ipsec**
Source Network: **fwB-remotenet**
Destination Interface: **lan**
Destination Network: **lannet**

Click Ok.

Save and activate the configuration on firewall A.

5. 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 **IP4 address**:

Name: **fwA-remotenet**

IP Address: **192.168.1.0/24**

Click **Ok**

In the same folder, add a new **IP4 address**:

Name: **fwA-remotegw**

IP Address: **192.168.110.1**

Click **Ok**

6. Firewall B - Pre-shared keys

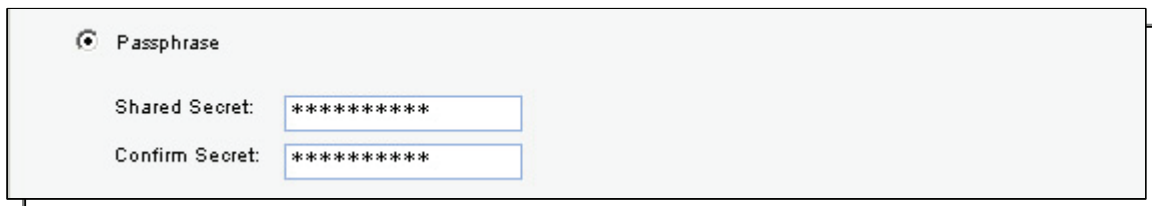
Go to *Objects -> Authentication Objects*.

Add a new **Pre-Shared Key**.

General:

Name: **fwA-psk**

Shared secret:



Passphrase

Shared Secret:

Confirm Secret:

Select **Passphrase** and enter a shared secret

Click **Ok**.

7. Firewall B - IPsec interface

Go to *Interfaces* -> *IPsec*.

Add a new IPsec Tunnel.

In the **General** tab:

General:

Name: **fwA-ipsec**

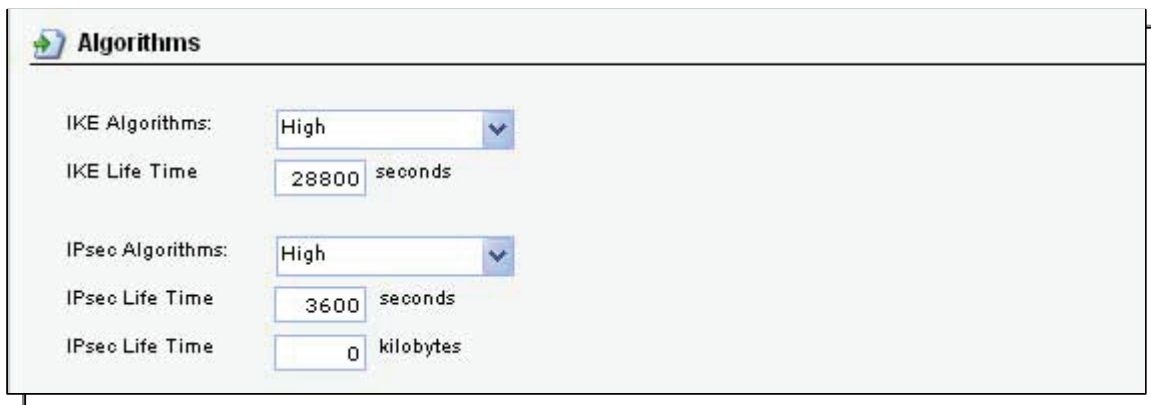
Local Network: **lanet**

Remote Network: **fwA-remotenet**

Remote Endpoint: **fwA-remotegw**

Encapsulation Mode: **Tunnel**

Algorithms:



Setting	Value	Unit
IKE Algorithms	High	
IKE Life Time	28800	seconds
IPsec Algorithms	High	
IPsec Life Time	3600	seconds
IPsec Life Time	0	kilobytes

IKE Algorithms: **High**

IKE Life Time: **28800**

IPsec Algorithms: **High**

IPsec Life Time: **3600**

IPsec Life Time: **0**

In the **Authentication** tab:

Authentication:

Select **Pre-Shared Key** and **fwA-psk**.

Click **Ok**.

8. Firewall B - Rules

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

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

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 Interface: **lan**

Source Network: **lanet**

Destination Interface: **fwA-ipsec**

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-ipsec**

Source Network: **fwA-remotenet**

Destination Interface: **lan**

Destination Network: **lanet**

Click Ok.

Save and activate the configuration on firewall B.