

Interoperability Profiles for D-Link

DFL-200 / DFL-700 / DFL-1100

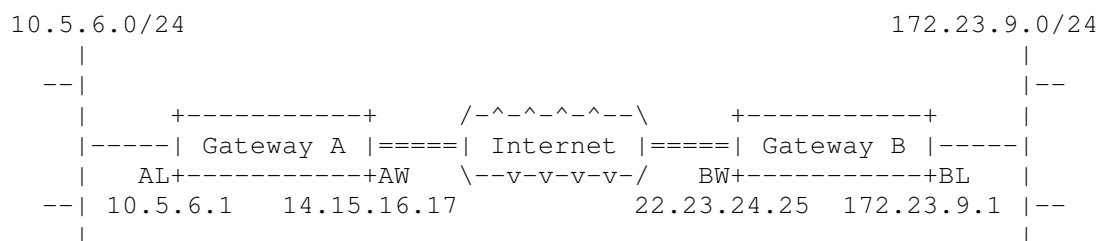
Last update: 2004-09-29

Overview

This document describes how to configure D-Link DFL-200 / DFL-700 / DFL-1100 firewalls to implement scenario 1, specified in "Documentation Profiles for IPSec interoperability" by the VPN Consortium.

Scenario 1: Gateway-to-gateway with preshared secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.



Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

Configuring D-Link DFL-200 / DFL-700 / DFL-1100

The default LAN address of the DFL is **192.168.1.1**. Connect your PC to the LAN port and use a browser to set up the DFL. In this document “Foo->Bar” indicates that you first should select the “Foo” menu (top of the page) and then the submenu “Bar” (to the left).

1. First time startup



The first time you connect to the DFL you will see a setup wizard. If this not is the first time you connect to the DFL, skip this step and continue to *2 Setting up the environment*.

Wizard welcome page: Click *Next*.

Wizard step 1: Enter a password (eg. admin) for the admin account, verify the password and click *Next*.

Wizard step 2: Choose the correct time zone and click *Next*.

Wizard step 3: Select **Static IP** and click Next.

Wizard step 3: Enter the following values:

IP Address: **14.15.16.17**
Subnet Mask: **255.255.255.0**
Gateway: **14.15.16.1**
Click *Next*.

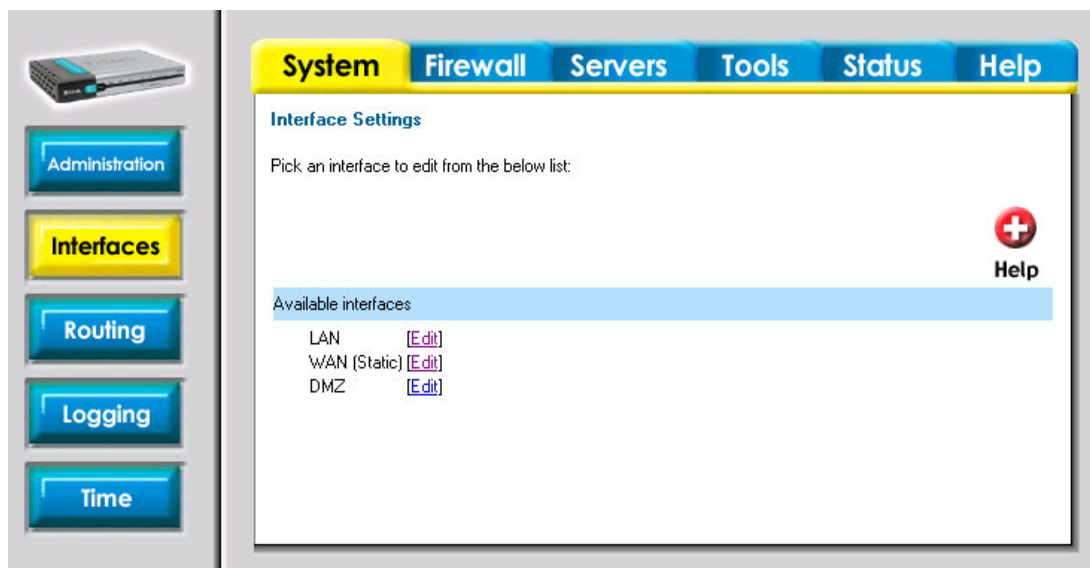
Wizard step 4: Select **Disable DHCP Server** and click *Next*.

Wizard step 5: Click *Next*.

Wizard complete: Click *Restart* and wait for the DFL to restart.

Log in using the password you choose in the wizard step 1 (eg user: *admin*, password: *admin*).

2. Setting up the environment



Go to "System->Interfaces".

Edit LAN:

IP Address: **10.5.6.1**
Subnet Mask: **255.255.255.0**

Click *Apply*

Edit WAN:

Select WAN type **Static** and click *Apply Change*.

IP Address: **14.15.16.17**
Subnet Mask: **255.255.255.0**
Gateway IP: **14.15.16.1**

Click *Apply*

Go to "Firewall->VPN".

Click *Add new*:

Name: **VPNC**
Local net: **10.5.6.0/24**

Select **PSK – Pre-shared key**

PSK: **hr5xb84l6aa9r6**
Retype PSK: **hr5xb84l6aa9r6**

Select **LAN-to-LAN tunnel**

Remote Net: **172.23.9.0/24**
Remote Gateway: **22.23.24.25**

Click *Apply*

In the list of VPN tunnels, click *Edit* on the tunnel you just created.

VPN Tunnels				
Name	Local Net	Remote Net	Remote Gateway	
VPNC	10.5.6.0/24	172.23.9.0/24	22.23.24.25	[Edit]

Click *Advanced* (near bottom of page).

Change the following settings:

Check the **PFS: Enable Perfect Forward Secrecy** option.

Change the **NAT Traversal** setting to disabled.

Change the first proposal in the *IKE Proposal List* to **3DES, SHA-1** and **28800 seconds**.

IKE Proposal List				
	Cipher	Hash	Life KB	Life Sec
#1:	3DES	SHA-1	0	28800
#2:	AES-128 Allowed:128-256	MD5	0	28800

Change the first proposal in the *IPsec Proposal List* to **3DES, SHA-1** and **3600 seconds**.

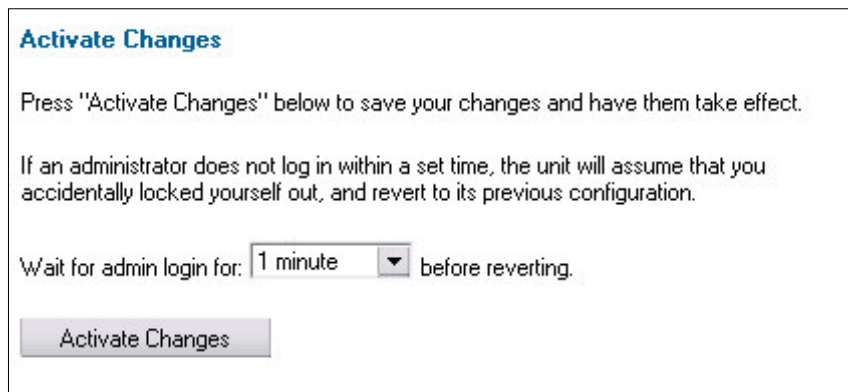
IPsec Proposal List				
	Cipher	HMAC	Life KB	Life Sec
#1:	3DES	SHA-1	0	3600
#2:	AES-128 Allowed:128-256	MD5	0	3600

Click *Apply*

Now everything is set up and we can activate the changes.



Click *Activate* (to the left on the bottom of the page).



Click *Activate Changes* to save your new setup and wait for the DFL to restart. If you don't login within the set time (default setting is one minute) the unit will revert to its previous configuration.

After you successfully reconnected to the unit you will see the following text:
The configuration was successfully finalized.

3. Status

View interface status

To view the status and IP addresses of the interfaces, go to “*Status->Interface*” and click on the interface name (LAN, WAN or DMZ).

View VPN status

To view the status of the VPN tunnel, go to “*Status->VPN*”. If you have more than one tunnel, you first have to click on the name of the tunnel to see its status.

View status of connections

To view the status of the current connections, go to “*Status->Connections*”. If you only want to see connections to/from a particular IP address or to/from a particular interface, enter an IP address in the source or destination field or/and select a source or destination interface from the dropdown boxes. Then click *apply*.

You can, for example, select the VPN tunnel interface as the destination interface to only see connections from your network through the tunnel.

Filter state table display:

	Source	Destination
IP Address:	<input type="text"/>	<input type="text"/>
Interface:	Any ▼	VPNC ▼
IP Protocol	Any ▼	
Port:	<input type="text"/>	<input type="text"/>