



## Примеры настройки межсетевых экранов D-Link серии

### NetDefend

### DFL-210/800/1600/2500

#### Сценарий: Виртуальная частная сеть, использующая туннели lan-to-lan по протоколу IPsec

Последнее обновление: 2005-10-20

#### Обзор

В этом документе условное обозначение *Objects->Address book* означает, что в дереве на левой стороне экрана сначала нужно нажать (раскрыть) **Objects** и затем **Address Book**.

Большинство примеров в этом документе даны для межсетевого экрана DFL-800. Те же самые настройки могут использоваться для всех других моделей этой серии. Единственное различие в названиях интерфейсов. Так как модели DFL-1600 и DFL-2500 имеют более одного сетевого интерфейса LAN, lan -интерфейсы называются lan1, lan2 и lan3.

Скриншоты в этом документе приведены для программного обеспечения версии 2.04.00. Если используется более поздняя версия ПО, скриншоты могут отличаться от тех, которые появятся в браузере.

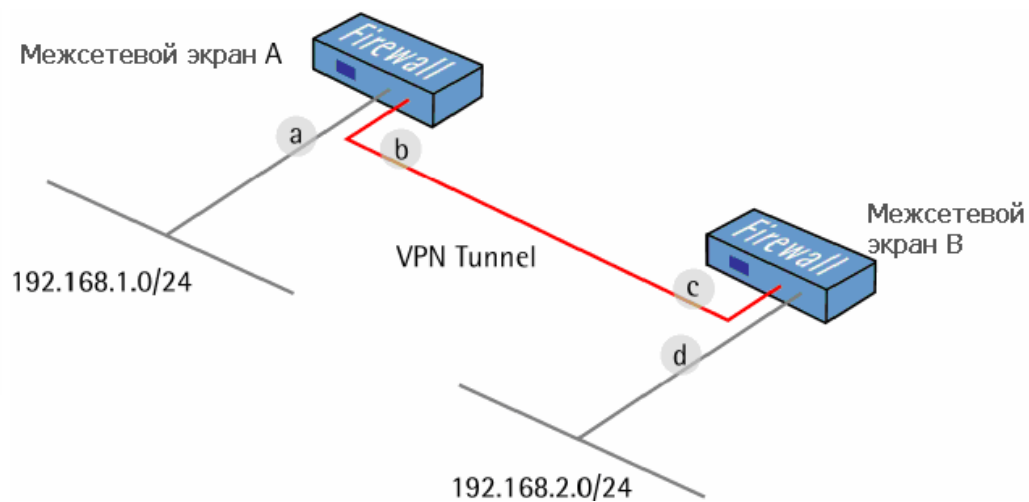
Для предотвращения влияния существующих настроек на настройки, описанные в этом руководстве, перед началом работы сбросьте межсетевой экран к заводским настройкам по умолчанию.

# 7a

## Виртуальная частная сеть, использующая туннели lan-to-lan по протоколу IPsec

Создание одного lan-to-lan IPsec туннеля между межсетевыми экранами А и В.

- a IP: 192.168.1.1
- b IP: 192.168.110.1  
Маска подсети: 255.255.255.0  
Шлюз: 192.168.110.2
- c IP: 192.168.110.2  
Маска подсети: 255.255.255.0  
Шлюз: 192.168.110.1
- d IP: 192.168.2.1



## 1. Межсетевой экран А - Адреса

Перейти в *Objects* -> *Address book* -> *InterfaceAddresses*. Изменить следующие пункты:

Заменить *Ian\_ip* на **192.168.1.1**

Заменить *Iannet* на **192.168.1.0/24**



Заменить *wan1\_ip* на **192.168.110.1**

Заменить *wan1net* на **192.168.110.0/24**

Перейти в *Objects* -> *Address book*.

Добавить новую папку **Address Folder**, называемую **RemoteHosts**.

В новой папке добавить новый **IP4 Host/Network**:

**Name: fwB-remotenet**

**IP Address: 192.168.2.0/24**

Нажать **Ok**

В той же папке добавить новый **IP4 Host/Network**:

**Name: fwB-remotegw**

**IP Address: 192.168.110.2**

Нажать **Ok**

## 2. Межсетевой экран А – ключи (Pre-shared keys)

Перейти в *Objects* -> *VPN Objects* -> *Pre-Shared keys*.

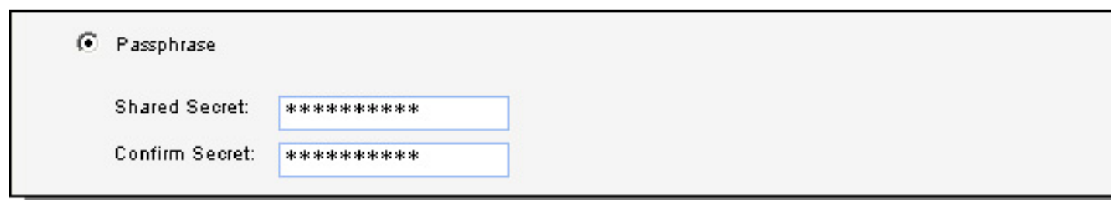
Добавить новый **Pre-Shared Key**.

**General:**



**Name: fwB-psk**

**Shared secret:**



Passphrase

Shared Secret:

Confirm Secret:

Выбрать **Passphrase** и ввести общий секретный ключ (shared secret).

Нажать **Ok**.

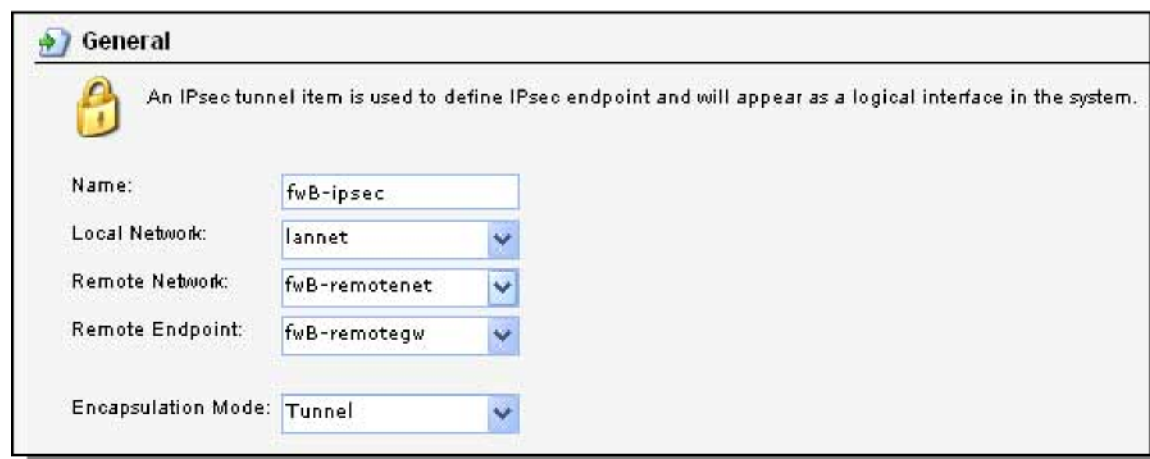
### 3. Межсетевой экран А – Интерфейс IPsec


Перейти в *Interfaces* -> *IPsec Tunnels*.

Добавить новый **IPsec Tunnel**.

Вкладка **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**

**Алгоритмы:**

**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**

Вкладка **Authentication** (аутентификация):

**Authentication:**

Pre-Shared Key

Pre-Shared Key: fwB-psk

Выбрать **Pre-Shared Key** и **fwB-psk**.

Нажать **Ok**.

#### **4. Межсетевой экран A – Правила**

Перейти в *Rules* -> *IP Rules*.

Создать новую папку **IP Rules Folder**, называемую **Ian\_to\_fwB-ipsec**

В новой папке создать новое IP-правило **IP Rule**.

Вкладка **General**:

**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-ipsec"/> ▼
Network:	<input type="text" value="lannet"/> ▼	<input type="text" value="fwB-remotenet"/> ▼

**Source Interface: lan**

**Source Network: lannet**

**Destination Interface: fwB-ipsec**

**Destination Network: fwB-remotenet**

Нажать **Ok**.

Создать второе правило в той же папке.

Вкладка **General:**

**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:	fwB-ipsec	lan
Network:	fwB-remotenet	lannet

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

Destination Network: **lannet**

Сохранить и активировать настройки межсетевого экрана А.

## 5. Межсетевой экран В - Адреса

Перейти в *Objects* -> *Address book* -> *InterfaceAddresses*.

Изменить следующие пункты:

Заменить **lan\_ip** на **192.168.2.1**

Заменить **lannet** на **192.168.2.0/24**

Заменить **wan1\_ip** на **192.168.110.2**

Заменить **wan1net** на **192.168.110.0/24**

Перейти в *Objects* -> *Address book*.

Добавить новую адресную папку **Address Folder**, называемую **RemoteHosts**.

В новой папке добавить новый **IP4 Host/Network**:

**Name: fwA-remotenet**

**IP Address: 192.168.1.0/24**

Нажать **Ok**

В той же папке добавить новый **IP4 Host/Network**:

**Name: fwA-remotegw**

**IP Address: 192.168.110.1**

Нажать **Ok**

## 6. межсетевой экран В – ключи (Pre-shared keys)

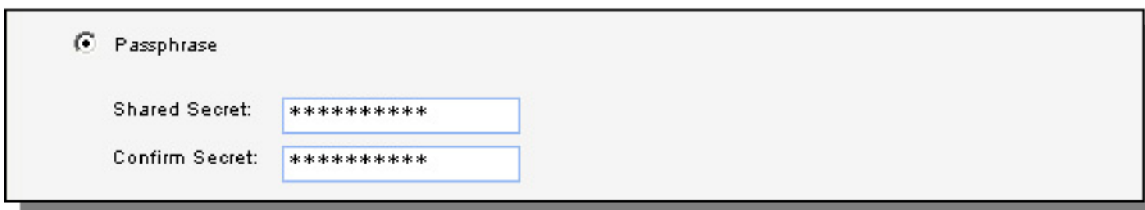
Перейти в *Objects* -> *VPN Objects* -> *Pre-Shared keys*.

Добавить новый **Pre-Shared Key**.

**General:**

Name: fwA-psk

**Shared secret:**



Passphrase

Shared Secret:

Confirm Secret:

Выбрать **Passphrase** и ввести общий секретный ключ (shared secret).

Нажать **Ок**.

## 7. Межсетевой экран В – Интерфейс IPsec

Перейти в *Interfaces* -> *IPsec Tunnels*.

Добавить новый IPsec Tunnel.

Вкладка **General**:

**General:**

Name: fwA-ipsec

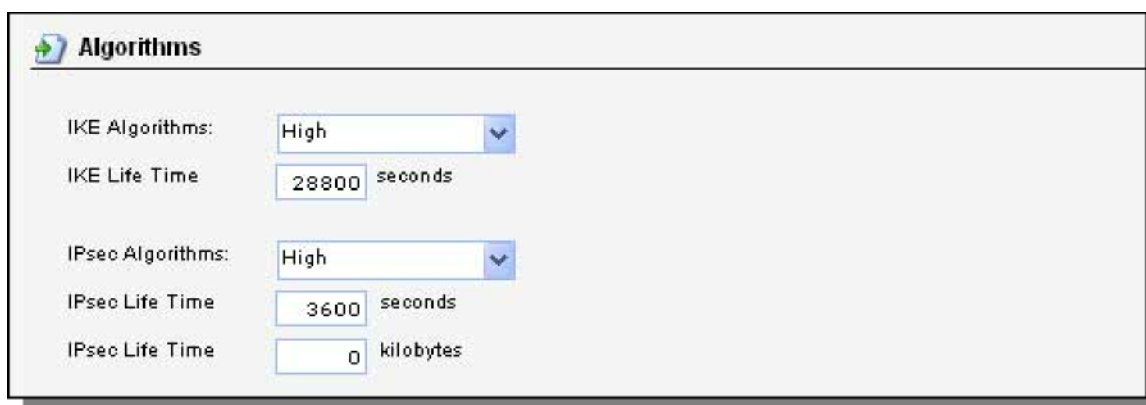
Local Network: lannet

Remote Network: fwA-remotenet

Remote Endpoint: fwA-remotegw

Encapsulation Mode: Tunnel

**Algorithms:**



**Algorithms**

IKE Algorithms:

IKE Life Time:  seconds

IPsec Algorithms:

IPsec Life Time:  seconds

IPsec Life Time:  kilobytes

IKE Algorithms: **High**

IKE Life Time: **28800**

IPsec Algorithms: **High**

IPsec Life Time: **3600**

IPsec Life Time: **0**

Вкладка **Authentication**:



**Authentication:**

Выбрать **Pre-Shared Key** и **fwA-psk**.

Нажать **Ok**.

## 8. Межсетевой экран В – Правила

Перейти в *Rules* -> *IP Rules*.

Создать новую папку **IP Rules Folder**, называемую **lan\_to\_fwA-ipsec**

В новой папке создать новое IP-правило **IP Rule**.

Вкладка **General**:

**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: lannet**

**Destination Interface: fwA-ipsec**

**Destination Network: fwA-remotenet**

Нажать **Ok**.

Создать второе правило в той же папке.

Вкладка **General**:

**General:**

**Name: allow\_all**

**Action: Allow**

**Service: all\_services**

**Address Filter:**

**Source Interface: fwA-ipsec**

**Source Network: fwA-remotenet**

**Destination Interface: lan**

**Destination Network: lannet**

Нажать **Ok**.

Сохранить и активировать настройки межсетевое экрана В.