



## Примеры настройки межсетевых экранов D-Link серии NetDefend

**DFL-210/800/1600/2500**

**Сценарий: Виртуальная частная сеть, использующая туннели lan-to-lan по протоколу PPTP (или L2TP)**

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.

# 7b

## Виртуальная частная сеть, использующая туннели lan-to-lan по протоколу PPTP (или L2TP)

Создание одного lan-to-lan туннеля между межсетевыми экранами А и В.  
Межсетевой экран В является сервером, межсетевой экран А - клиентом.

Если планируется использовать туннель L2TP вместо PPTP, выполните шаги, описанные в этом руководстве, но на шагах 2 и 6 замените туннельный протокол PPTP на L2TP.

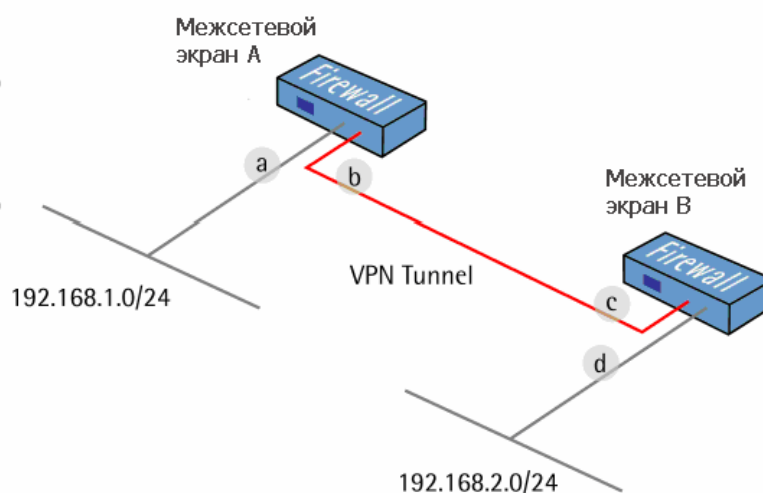
Другие настройки одинаковы в обоих случаях.

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: 192.168.110.2

d IP: 192.168.2.1

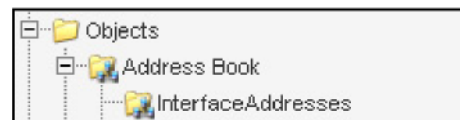


## 1. Межсетевой экран А - Адреса

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

Заменить *lan\_ip* на **192 . 168 . 1 . 1**

Заменить *lanenet* 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**

Добавить новый **IP4 Host/Network**:

**Name: fwB-remotegw**

**IP Address: 192.168.110.2**

## 2. Межсетевой экран А – интерфейс клиента PPTP

Перейти в *Interfaces* -> *L2TP/PPTP Clients*.

Добавить новый **L2TP/PPTP Client**.

Вкладка **General**:

### **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**

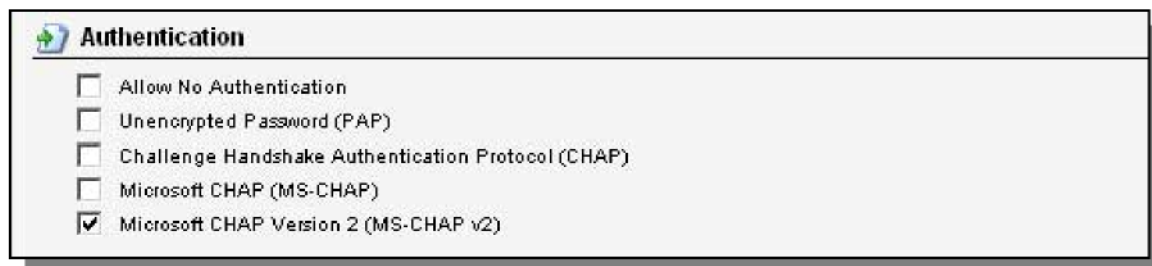
### **Authentication:**

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

**Username: userA**

Вкладка **Security**:

**Authentication:**

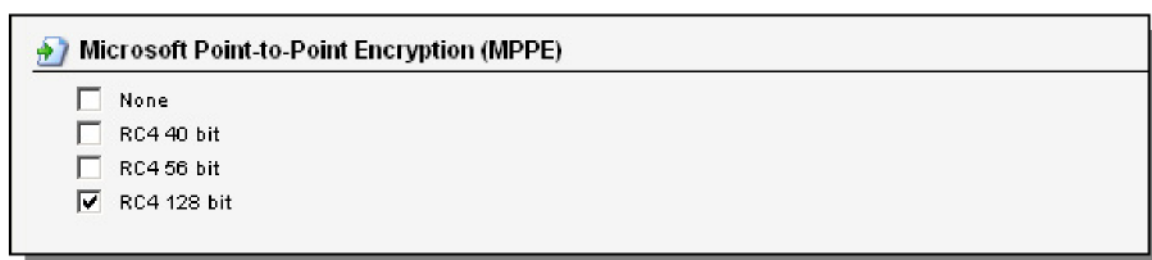


**Authentication**

- Allow No Authentication
- Unencrypted Password (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP)
- Microsoft CHAP Version 2 (MS-CHAP v2)

Единственная опция, которая должна быть отмечена – **Microsoft CHAP Version 2 (MS-CHAP v2)**

**Microsoft Point-to-Point Encryption (MPPE):**



**Microsoft Point-to-Point Encryption (MPPE)**

- None
- RC4 40 bit
- RC4 56 bit
- RC4 128 bit

Должно быть отмечено только **RC4 128 bit**. (Использование MS-CHAP v2 и 128 bit является наиболее безопасным режимом.)

### 3. Межсетевой экран A – правила

Перейти *Rules* -> *IP Rules*.

Создать новую папку **IP Rules Folder**, называемую **lan\_to\_fwB-pptp**

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

Вкладка **General**:

**General:**



Name:

Action:

Service:

Schedule:

**Name: allow\_all**

**Action: Allow**

**Service: all\_services**

**Address Filter:**

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

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

Нажать **Ok**.

Создать второе правило в той же папке.

Вкладка **General**:

**General:**

**Name: allow\_ a11**

**Action: Allow**

**Service: all\_service**

**Address Filter:**

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

**Source Interface: fwB-pptp**  
**Source Network: fwB-remotenet**  
**Destination Interface: lan**  
**Destination Network: lannet**  
Нажать **Ok**.

Сохранить и активировать настройки межсетевого экрана А.

#### **4. 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 папку **Address Folder**, называемую **RemoteHosts**.

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

**Name: fwA-remotenet**

**IP Address: 192.168.1.0/24**

Добавить новую папку **Address Folder**, называемую **IP Pools**.

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

**Name: fwA-ippool**

**IP Address: 192.168.2.100-192.168.2.199**

Нажать **Ok**

## 5. Межсетевой экран В –база данных пользователей

Перейти в *Authentication -> Local User Databases*.

Добавить новую базу **Local User Database** называемую **PPPUsers**.

В новой базе данных добавить нового пользователя **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:**

<b>Per-user PPTP/L2TP IP Configuration</b>	
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. Межсетевой экран В – интерфейс PPTP-сервера

Перейти в *Interfaces* -> *L2TP/PPTP Server*.

Добавить новый сервер L2TP/PPTP Server.

Вкладка **General**:

### **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: **ip**


**wan1\_ip**

Вкладка **PPP Parameters**:

### **General:**


Выбрать опцию **Use User Authentication Rules**

### **Microsoft Point-to-Point Encryption (MPPE):**

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

Должно быть отмечено только **RC4 128 bit**.

### **IP Pool:**

 <b>IP Pool</b>		
IP Pool:	fwA-ippool	
DNS:	Primary: (None)	Secondary: (None)
NBNS:	Primary: (None)	Secondary: (None)

IP Pool: **fwA-ippool**

Нажать **Ok**.

## 7. Firewall B – Правила аутентификации пользователя


Перейти в *User Authentication* -> *User Authentication Rules*.

Добавить новое правило **User Authentication Rule**.

Вкладка **General**:

### 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**

Вкладка

Authentication Options:

### General:

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

Local User DB: **PPPUsers**

Нажать **Ok**.

## 8. Межсетевой экран B – Правила

Перейти в *Rules* -> *IP Rules*.

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



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-pptp**

**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-pptp**

**Source Network: fwA-remotenet**

**Destination Interface: lan**

**Destination Network: lannet**

Нажать **Ok**.

Сохранить и активировать настройка межсетевого экрана А.