



Примеры настройки межсетевых экранов D-Link серии NetDefend

DFL-210/800/1600/2500

Сценарий: настроить автоматическое переключение между двумя WAN-каналами от двух провайдеров услуг при отказе одного из них, используя маршрутизацию на основе политик.

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.

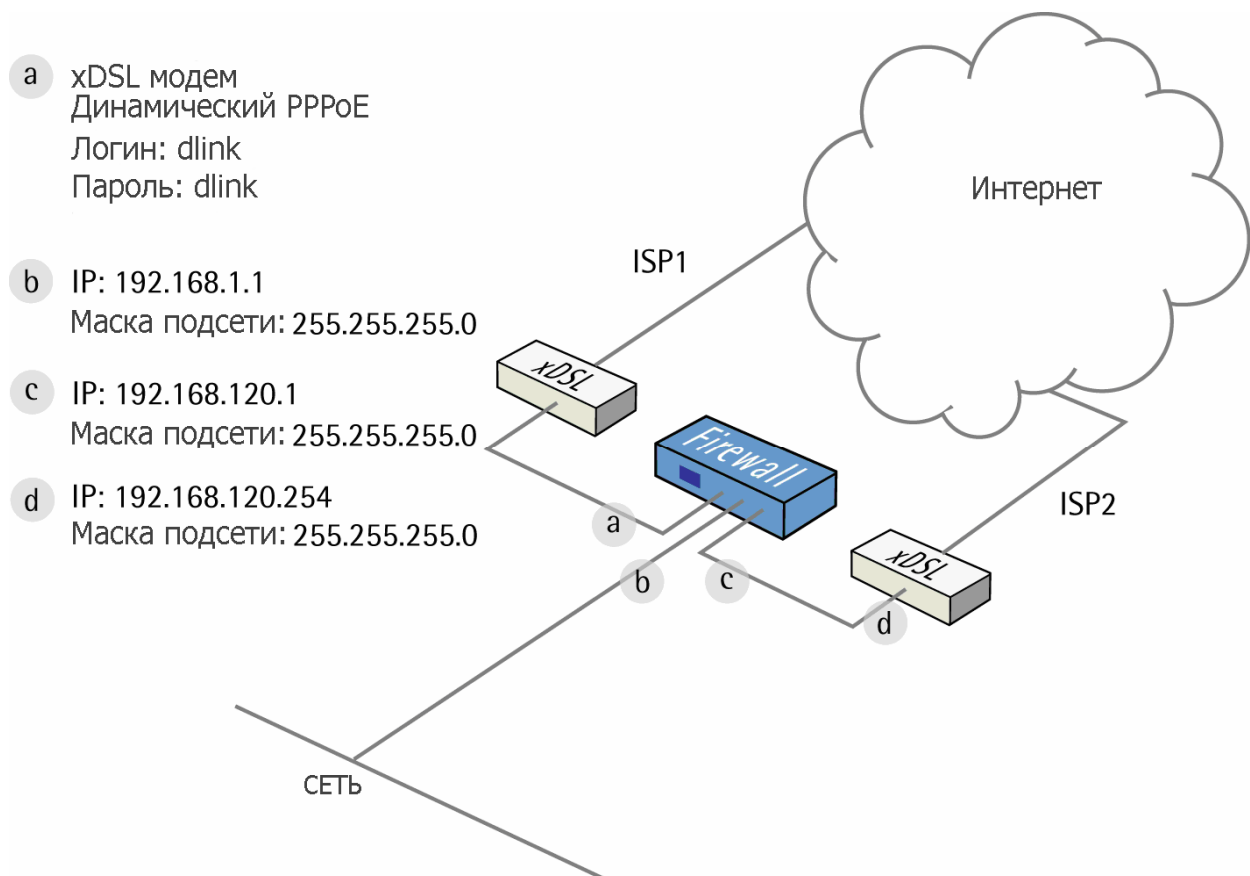
Для предотвращения влияния существующих настроек на настройки, описанные в этом руководстве, перед началом работы сбросьте межсетевой экран к заводским настройкам по умолчанию.

2 Как настроить автоматическое переключение между двумя WAN-каналами от двух провайдеров услуг при отказе одного из них, используя маршрутизацию на основе политик.

Детали этого сценария:

- **WAN1** использует динамический IP-адрес с PPPoE
- **WAN2** использует статический IP-адрес
- В направлении от LAN к WAN на интерфейсе **WAN1** разрешены сервисы HTTP, HTTPS и FTP.
- В направлении от LAN к WAN на интерфейсе **WAN2** разрешены сервисы SMTP, POP3 и Ping.

Если один из WAN-каналов откажет, все сервисы будут перенаправлены на другой интерфейс WAN. Когда отказавший канал вернется в работоспособное состояние, эти сервисы вновь будут передаваться через него.



1. Адреса

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

Изменить следующие пункты:

Заменить **lan_ip** на **192.168.1.1**

Заменить **lannet** на **192.168.1.0/24**

Заменить **wan2_ip** на **192.168.120.1**

Заменить **wan2net** на **192.168.120.0/24**



Создать новый IP4 Host/Network:

Name: wan2-gw

IP address: 192.168.120.254

Нажать **Ok**.

2. Интерфейс Ethernet

Перейти в *Interfaces* -> *Ethernet*:

Изменить интерфейс **WAN2**.

Вкладка **General**:

General:

Name:	<input type="text" value="wan2"/>
IP Address:	<input type="text" value="wan2_ip"/> ▼
Network:	<input type="text" value="wan2net"/> ▼
Default Gateway:	<input type="text" value="wan2-gw"/> ▼

Задать **IP Address** как **wan2_ip** и **Network** как **wan2net**.

Выбрать **wan2-gw** в качестве **Default Gateway** (шлюза по умолчанию).

Вкладка **Advanced**:

Automatic Route Creation (автоматическое создание маршрута):

Automatically add commonly used routes related to this interface

Add route for interface network

Add default route if default gateway is specified

Route Metric:

Убрать отметки с **Add route for interface network** и **Add default route if default gateway is specified**

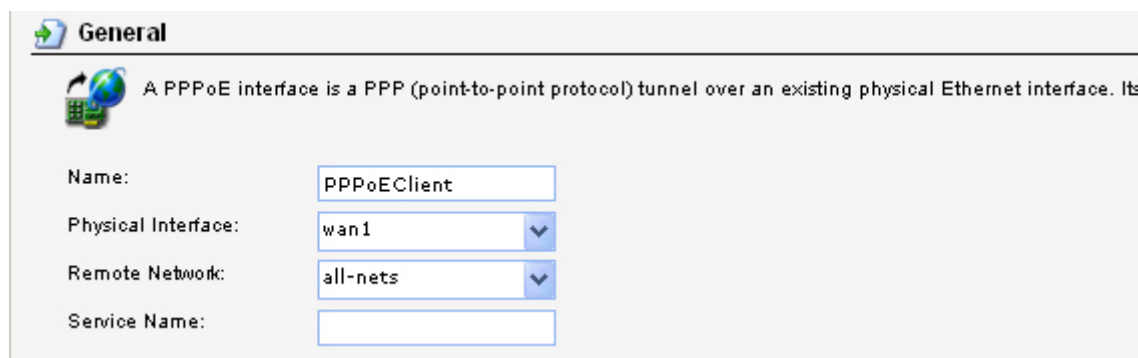
Нажать **Ok**

3. Настройка PPPoE-клиента

Под *Interfaces* -> *PPPoE Tunnels*:
Добавить новый PPPoE tunnel.

Вкладка **general**:

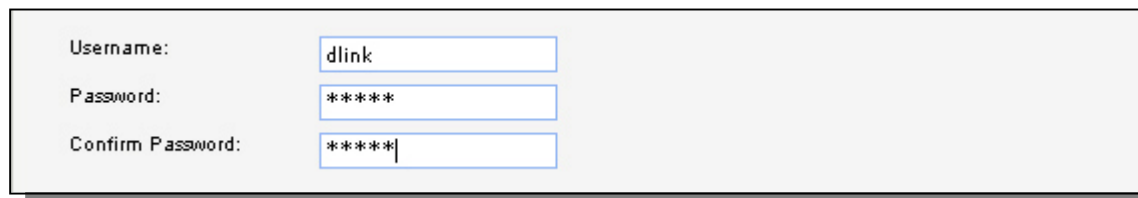
General:



The screenshot shows the 'General' tab of the PPPoE Tunnel configuration. At the top, there is a globe icon and a description: 'A PPPoE interface is a PPP (point-to-point protocol) tunnel over an existing physical Ethernet interface. Its'. Below this, there are four configuration fields: 'Name' with the value 'PPPoEClient', 'Physical Interface' with a dropdown menu showing 'wan1', 'Remote Network' with a dropdown menu showing 'all-nets', and 'Service Name' which is currently empty.

Name: PPPoEClient
Physical Interface: WAN1
Remote Network: all-nets

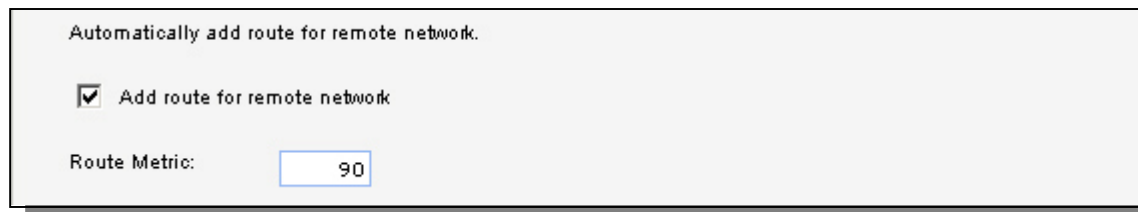
Authentication:



The screenshot shows the 'Authentication' tab of the PPPoE Tunnel configuration. It contains three input fields: 'Username' with the value 'dlink', 'Password' with the value '*****', and 'Confirm Password' with the value '*****'.

Username: dlink
Password: dlink
Confirm password: dlink

Advanced tab:



The screenshot shows the 'Advanced' tab of the PPPoE Tunnel configuration. It features a checkbox labeled 'Add route for remote network' which is checked. Below the checkbox is a 'Route Metric' input field with the value '90'.

Выбрать **Add route for remote network** и установить **Route metric** равной **90**.

Нажать **OK**.

4. Маршруты

Перейти в *Routing* -> *Main Routing Table*.

Добавить новый маршрут **Route**.

Вкладка **General**:

General:

Interface:	wan2
Network:	wan2net
Gateway:	(None)
Local IP Address:	(None)
Metric:	80

Interface: **wan2**

Network: **wan2net**

Gateway: **(None)**

Local IP Address: **(None)**

Metric: **80**

Вкладка **Monitor**:

Monitoring for Route Failover:

<input checked="" type="checkbox"/> Monitor This Route
--

Выбрать **Monitor This Route**

Method:

<input checked="" type="checkbox"/> Monitor Interface Link Status
<input type="checkbox"/> Monitor Gateway Using ARP Lookup
<input type="checkbox"/> Manual ARP Lookup Interval: 1000 milliseconds

Выбрать **Monitor Interface Link Status**

Нажать **Ok**.

Добавить новый маршрут **Route**.

Вкладка **General**:

General:

Interface:	wan2
Network:	all-nets
Gateway:	wan2-gw
Local IP Address:	(None)
Metric:	80

Interface: wan2

Network: all-nets

Gateway: wan2-gw

Local IP Address: (None)

Metric: 80

Вкладка Monitor:

Monitoring for Route Failover:

Monitor This Route

Выбрать **Monitor This Route**

Method:

Monitor Interface Link Status
 Monitor Gateway Using ARP Lookup
 Manual ARP Lookup Interval: 1000 milliseconds

Выбрать **Monitor Interface Link Status**

выбрать **Monitor Gateway Using ARP Lookup**

Нажать **Ok**.

Добавить новый маршрут **Route**.

Вкладка **General**:

General:

Interface: PPPoEClient

Network: all-nets

Gateway: (None)

Local IP Address: (None)

Metric: 90

Вкладка **Monitor**:

Monitoring for Route Failover:

Выбрать **Monitor This Route**

Method:

<input checked="" type="checkbox"/> Monitor Interface Link Status
<input checked="" type="checkbox"/> Monitor Gateway Using ARP Lookup
<input type="checkbox"/> Manual ARP Lookup Interval: <input type="text" value="1000"/> milliseconds

Выбрать **Monitor Interface Link Status**
выбрать **Monitor Gateway Using ARP Lookup**


Нажать **Ok**.

5. Группы интерфейсов

Перейти в *Interfaces* -> *Interface Groups*.

Создать новую группу интерфейсов **Interface Group**:

General:

 General	
Use an interface group to combine several interfaces for a simplified security policy.	
Name:	<input type="text" value="pppoe-wan2"/>
	<input checked="" type="checkbox"/> Security/Transport Equivalent

Name: **pppoe-wan2**

Выбрать **Security/Transport Equivalent**

Interfaces:

Available		Selected
wan1 dmz lan	<input type="button" value=">>"/> <input type="button" value="<<"/>	wan2 PPPoEClient

Добавить **PPPoEClient** и **wan2**

Нажать **Ok**

6. Правила

Перейти в *Rules* -> *IP Rules*.

Добавить новую папку **IP Rules Folder**, называемую **lan_to_pppoe-wan2**

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

Вкладка **General**:

General:

General

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

Name:

Action:

Service:

Schedule:

Name: allow-http-all

Action: NAT

Service: http-all

Address Filter:

Interface:

Source:

Destination:

Network:

Source interface: lan

Source network: lannet

Destination interface: pppoe-wan2

Destination network: all-nets

Нажать **Ok**

Теперь создайте еще четыре правила, таким же способом, как и первое правило:

Название	Действие	Сервис	Источник	Пункт назначения	Источник сети	Пункт назначения сети
allow-ftp	NAT	ftp-passthrough	Lan	pppoe-wan2	lannet	all-nets
allow-smtp	NAT	smtp	Lan	pppoe-wan2	lannet	all-nets
allow-pop3	NAT	pop3	Lan	pppoe-wan2	lannet	all-nets
allow-ping	NAT	ping-outbound	Lan	pppoe-wan2	lannet	all-nets
allow-dns	NAT	dns-all	Lan	pppoe-wan2	lannet	all-nets

7. Маршрутизация на основе политик

Под *Routing* -> *Policy-based Routing Tables*:

Добавить новую таблицу *Policy-based Routing Table*.

General:

General

A policy-based routing table is used to define an alternate routing table.

Name:

Ordering:

Remove Interface IP Routes
(make firewall totally transparent)

Name: r-pppoe

Ordering: Only

В заново созданной таблице добавить новый маршрут **Route**:

Вкладка **General**:

General:

General

A route defines what interface and gateway to use in order to reach a specified network.

Interface:

Network:

Gateway:

Local IP Address:

Metric:

Interface: PPPoEClient

Network: all-nets

Metric: 80


Нажать **Ok**

Добавить новый маршрут **Route**:

Вкладка **General**:

General:

 **General**

 A route defines what interface and gateway to use in order to reach a specified network.

Interface:

Network:

Gateway:

Local IP Address:

Metric:

Interface: wan2

Network: all-nets

Gateway: wan2-gw

Metric: 90

Нажать **Ok**

Перейти в *Routing* -> *Policy-bases Routing Policy*:

Добавить новое правило маршрутизации на основе политик **Policy-based Routing Rule**:

General:

Name:

Forward Table:

Return Table:

Service:

Schedule:

Name: pbr-http-all

Forward Table: r-pppoe

Return Table: <main>

Service: http-all

Address Filter:

	Source	Destination
Interface:	<input type="text" value="lan"/>	<input type="text" value="wan2"/>
Network:	<input type="text" value="lanet"/>	<input type="text" value="all-nets"/>

Source interface: lan

Source network: lanet

Destination interface: wan2

Destination network: all-nets

Нажать **Ок**

Создайте еще одно правило маршрутизации на основе политик, таким же способом, как и предыдущее:

Названи	Отправка	Возврат	Сервис	Источник	Пункт	Источник	Пункт
pbr-ftp	r-pppoe	<main>	ftp-outbound	lan	wan2	lannet	all-nets

Сохранить и активировать настройки.