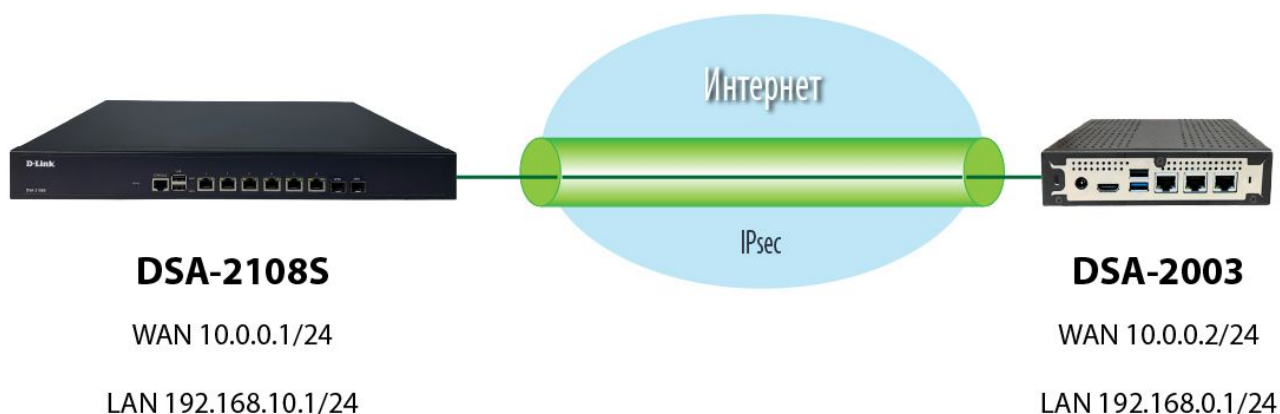


Вопрос: Как настроить IPsec-туннель между сервисными маршрутизаторами с ПО Security Edition (SE)?

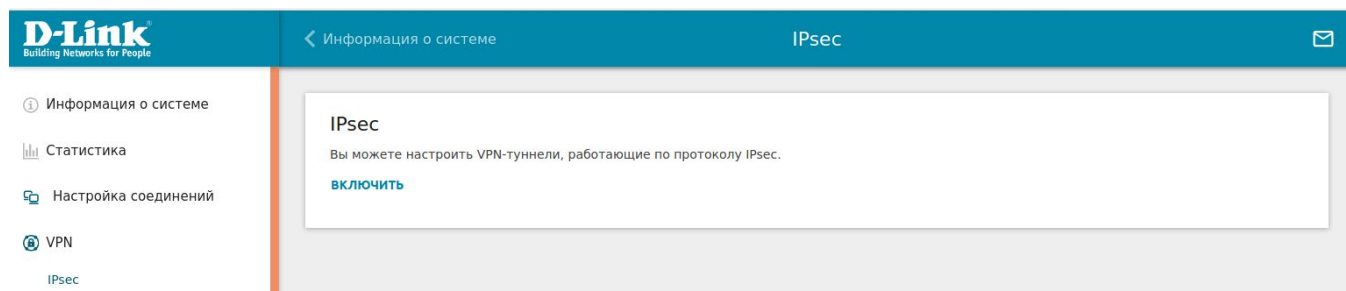
(Сервисные маршрутизаторы с программным обеспечением Security Edition: DIR-853/SE (рев. R3), DIR-1260/SE, DIR-2150/SE, DSA-2003, DSA-2006, DSA-2108S, DSA-2208X, DSA-2308X)

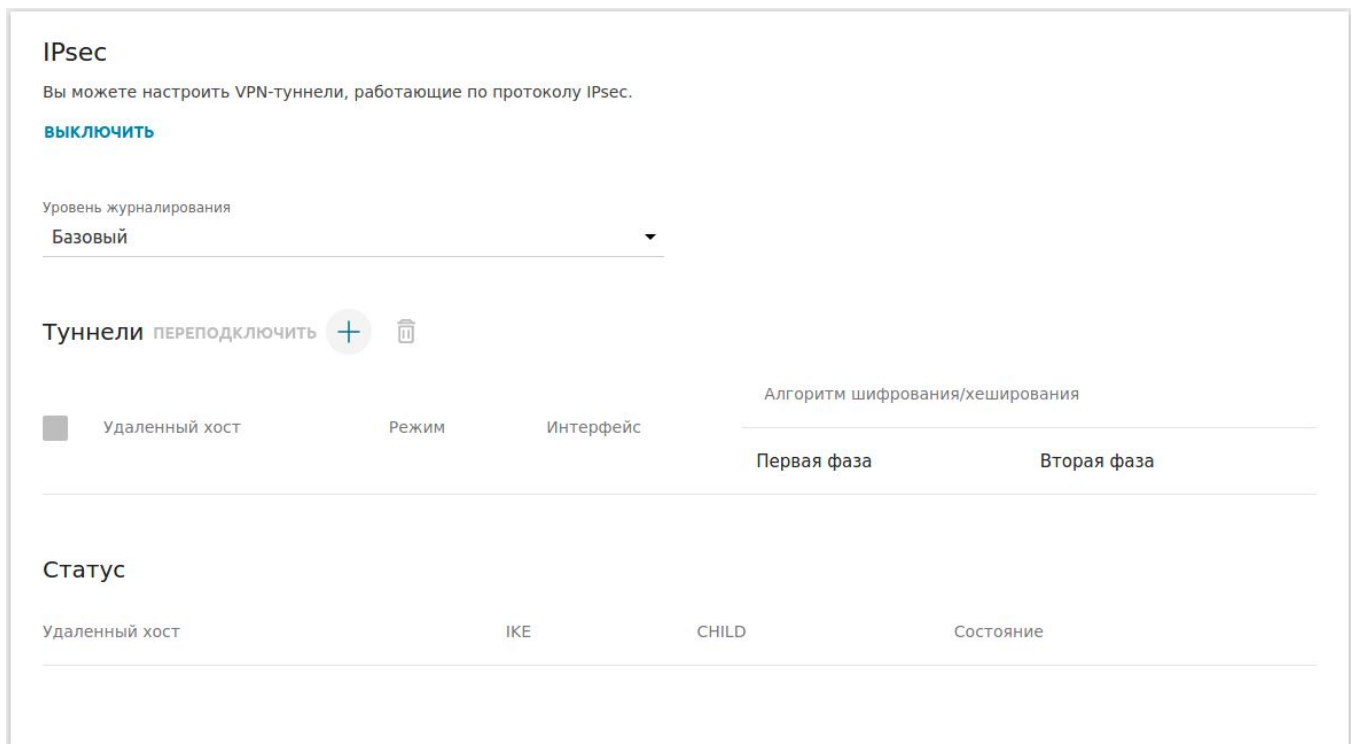
В данном примере приведена настройка IPsec-туннеля для организации безопасного VPN-подключения между DSA-2108S и DSA-2003. WAN- и LAN-интерфейсы маршрутизаторов настроены в соответствии со значениями, приведенными на рисунке. Тип соединения для DSA-2108S – **Статический IPv4** с именем *statip_50*; для DSA-2003 – **Статический IPv4** с именем *statip_25*.



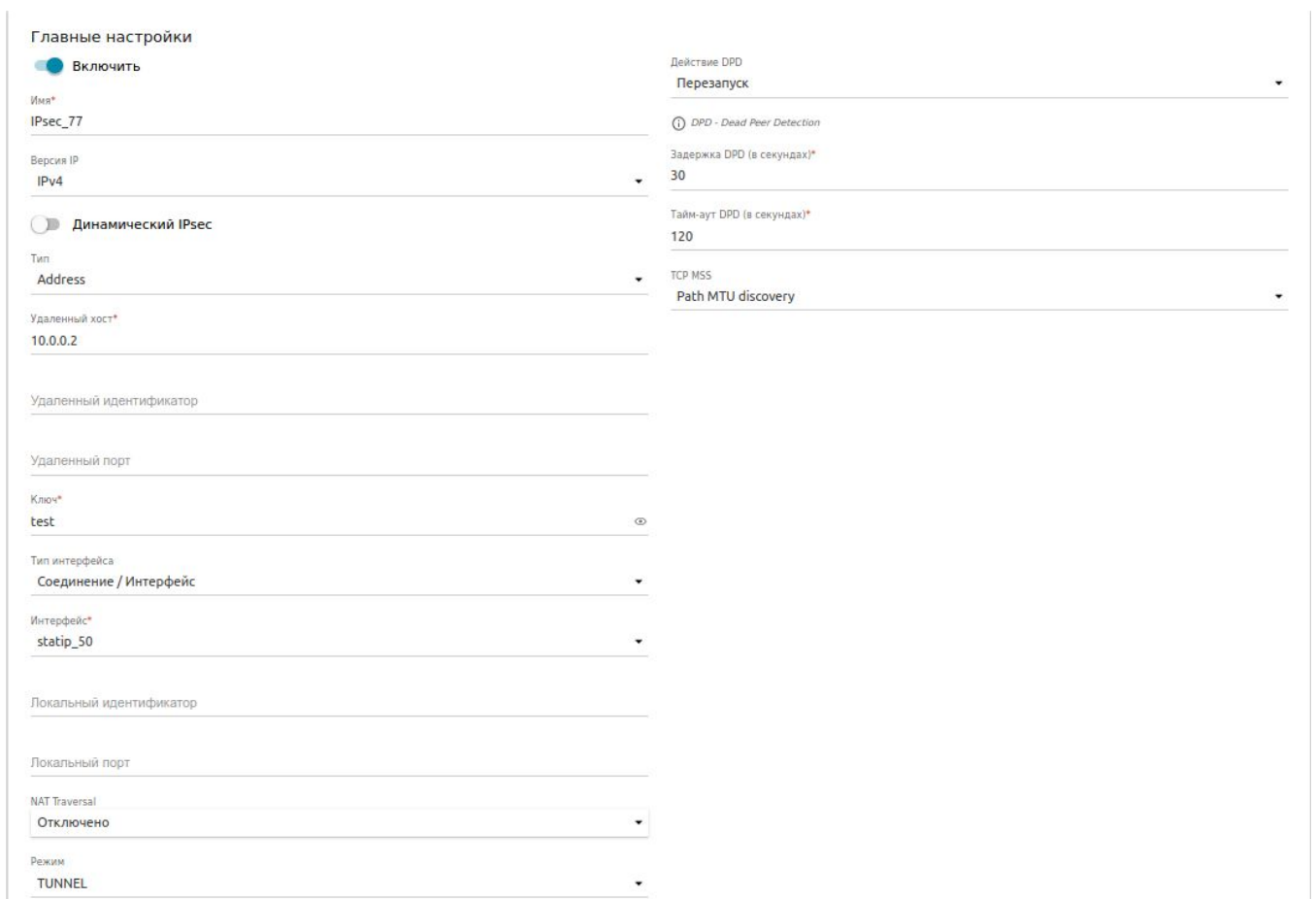
1. Настройка DSA-2108S

1.1. В основном меню слева перейдите к разделу **VPN**, далее – на страницу **IPsec**. Для включения VPN-сервиса IPsec нажмите **Включить**.





1.2. В открывшемся окне создайте туннель, нажав на «+». Заполните поля раздела **Главные настройки** следующим образом:



В графе **Удаленный хост** укажите IP-адрес WAN-интерфейса удаленного маршрутизатора – DSA-2003 (в данном примере это *10.0.0.2*).

В графе **Ключ** укажите ключ шифрования, который должен быть одинаковым на обоих маршрутизаторах (в данном примере это *test*).

Выберите **Тип интерфейса**: Соединение/Интерфейс и в графе **Интерфейс** укажите конкретное соединение, для которого организуется IPsec-туннель (в данном примере это *statip_50*).

1.3. Все остальные настройки, включая настройки времени жизни и шифрования для 1 и 2 фазы, оставьте по умолчанию. Настройки 1 и 2 фазы приведены ниже.

Первая фаза	Вторая фаза
Алгоритм шифрования первой фазы DES	Алгоритм шифрования второй фазы DES
Режим шифрования CBC	Режим шифрования CBC
Алгоритм хеширования MD5	Алгоритм хеширования MD5
Размер хеша 96	Размер хеша 96
Режим хеширования HMAC	Режим хеширования HMAC
Тип DHgroup первой фазы MODP768	<input checked="" type="checkbox"/> Включить PFS Тип DHgroup второй фазы MODP768
IKE-SA время жизни* 10800	IPsec-SA время жизни* 3600
<input type="checkbox"/> Aggressive режим	
Версия IKE 1	

1.4. В разделе **Туннелируемые подсети** необходимо добавить локальную и удаленную подсеть для настраиваемого туннеля. Нажмите кнопку «+».

Туннелируемые подсети + 🗑️

<input type="checkbox"/> Локальная подсеть	<input type="checkbox"/> Удаленная подсеть
--	--

ПРИМЕНИТЬ

Добавьте адрес локальной подсети (в данном примере это *192.168.10.0/24*) и адрес удаленной подсети (в данном примере это *192.168.0.0/24*), затем нажмите **Сохранить**.

Добавить правило ✕

Локальная подсеть*
192.168.10.0/24

📌 **Задайте локальную подсеть IPsec-туннеля (LAN-сеть маршрутизатора).**
Пример: 192.168.0.0/24

Удаленная подсеть*
192.168.0.0/24

📌 **Задайте удаленную подсеть IPsec-туннеля (LAN-сеть удаленного устройства, выполняющего роль маршрутизатора).**
Пример: 192.168.10.0/24

СОХРАНИТЬ

1.5. Нажмите кнопку **Применить**.

Туннелируемые подсети + 🗑️

<input type="checkbox"/> Локальная подсеть	<input type="checkbox"/> Удаленная подсеть
<input type="checkbox"/> 192.168.10.0/24	<input type="checkbox"/> 192.168.0.0/24

ПРИМЕНИТЬ

1.6. Для корректной работы созданный IPsec-туннель необходимо добавить в группу интерфейсов, а также добавить настройки межсетевого экрана.

1.6.1. Для маршрутизаторов DSA-2108S, DSA-2208X, DSA-2308X это можно сделать в автоматическом режиме: в открывшемся окне нажмите кнопку **ПРОДОЛЖИТЬ**.

Внимание

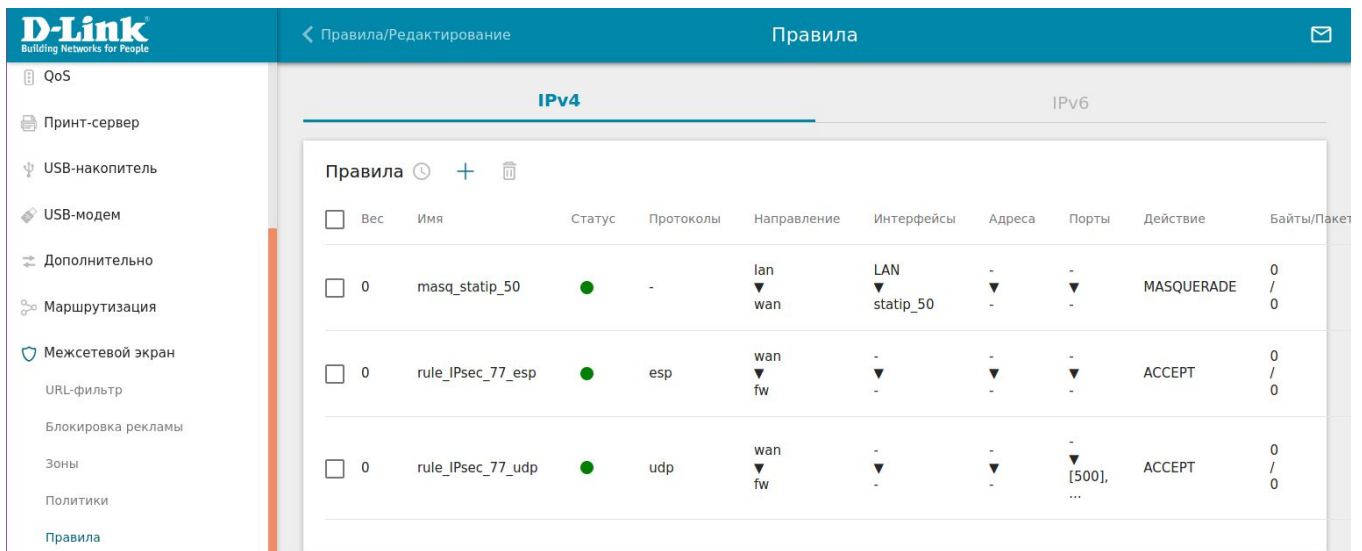
Для корректной работы VPN-соединения необходимо добавить его в группу интерфейсов, а также добавить настройки межсетевого экрана. При нажатии на кнопку **Продолжить** соединение будет добавлено в группу интерфейсов, новую зону, политики и, если необходимо, правила межсетевого экрана. При нажатии на кнопку **Настроить вручную** необходимо задать эти настройки самостоятельно.

[НАСТРОИТЬ ВРУЧНУЮ](#) [ПРОДОЛЖИТЬ](#)

IPsec-туннель автоматически добавиться в группу интерфейсов в качестве VPN, а в межсетевом экране для него будут созданы: отдельная зона с добавленным в него IPsec-туннелем (в данном примере это `zone_IPsec_77`), 2 правила по протоколам UDP и ESP и 2 политики, по которым межсетевой экран определяет, как должен обрабатываться трафик из локальной сети `lan` в зону `zone_IPsec_77` и из зоны `zone_IPsec_77` во внешнюю сеть через интерфейс `wan`.

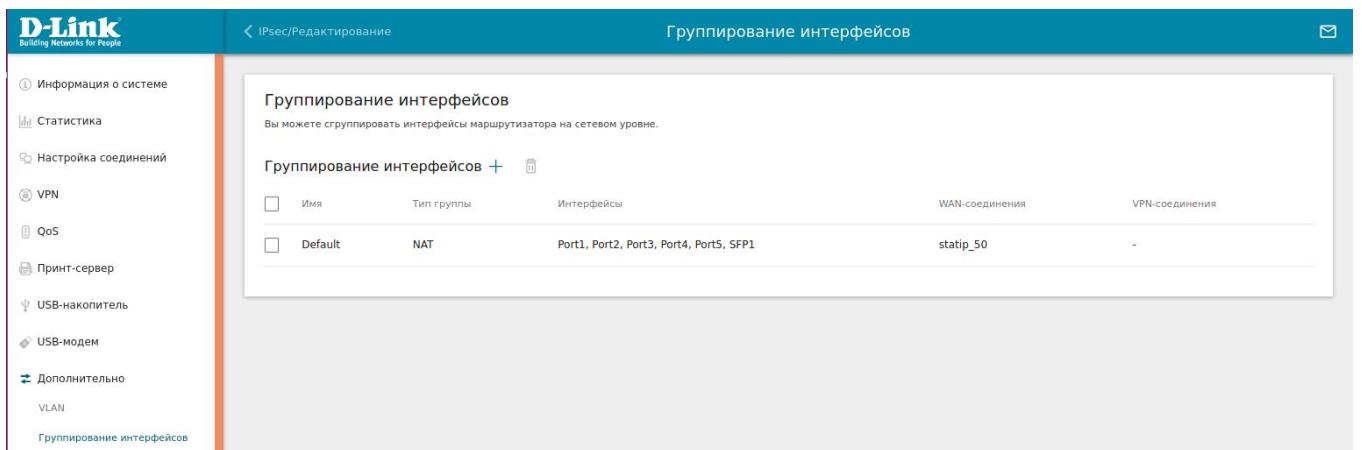
Зоны +	Имя	Тип	Интерфейсы
<input type="checkbox"/>	fw	firewall	-
<input type="checkbox"/>	wan	ipv4	statip_50
<input type="checkbox"/>	lan	ipv4	LAN
<input type="checkbox"/>	zone_IPsec_77	ipv4	IPsec_77

Политики +	Источник	Назначение	Действие	Уровень журналирования
<input type="checkbox"/>	all	all	DROP	Отключено
<input type="checkbox"/>	fw	all	ACCEPT	Отключено
<input type="checkbox"/>	lan	fw	ACCEPT	Отключено
<input type="checkbox"/>	lan	wan	ACCEPT	Отключено
<input type="checkbox"/>	lan	zone_IPsec_77	ACCEPT	Отключено
<input type="checkbox"/>	zone_IPsec_77	wan	ACCEPT	Отключено

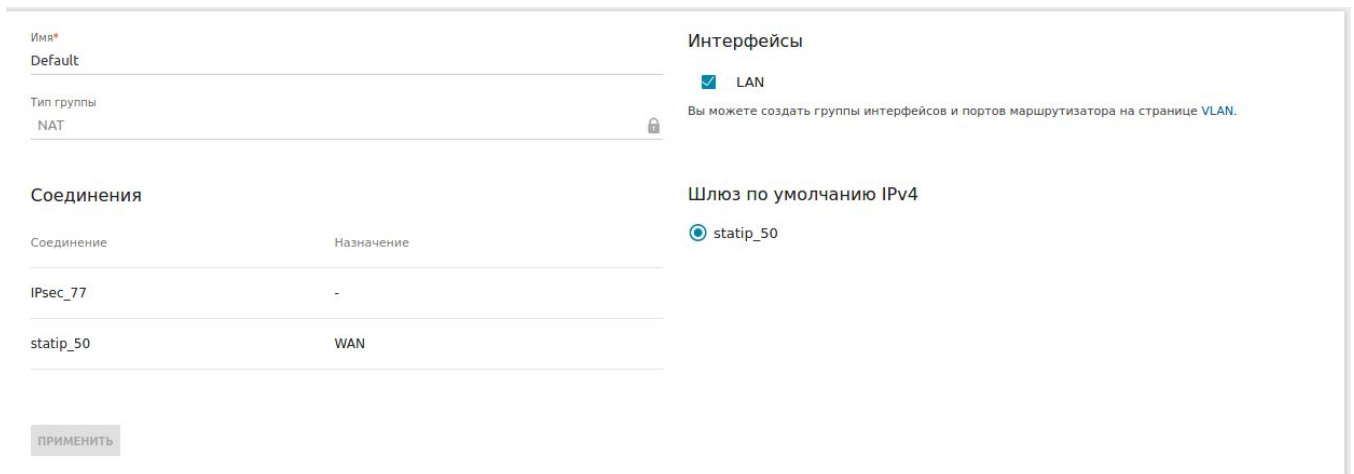


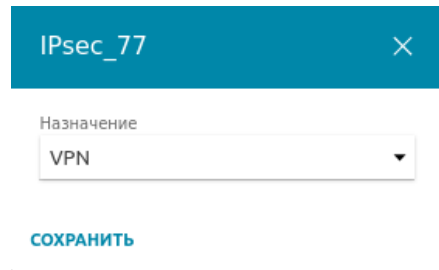
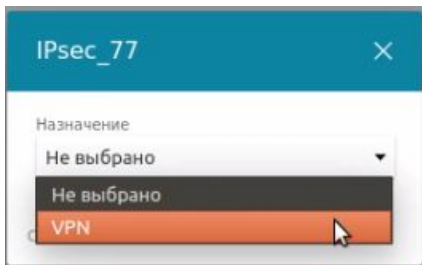
1.6.2. Для остальных сервисных маршрутизаторов группирование интерфейсов и настройки межсетевого экрана выполняются вручную. Пример настройки вручную приведен для IPsec-туннеля с именем *IPsec_77*.

В левом меню перейдите к разделу **Дополнительно**, откройте страницу **Группирование интерфейсов**.



На странице **Группирование интерфейсов** перейдите в группу с именем **Default**, в графе **Соединения** выберите IPsec-туннель *IPsec_77* и укажите его в качестве **VPN**. Нажмите **Сохранить**.





Имя*
Default

Тип группы
NAT

Интерфейсы
 LAN
Вы можете создать группы интерфейсов и портов маршрутизатора на странице [VLAN](#).

Соединения

Соединение	Назначение
IPsec_77	VPN
statip_50	WAN

Шлюз по умолчанию IPv4
 statip_50

ПРИМЕНИТЬ

Для сохранения всех настроек нажмите кнопку **Применить**.

Проверить добавленный IPsec-туннель можно в разделе **Группирование интерфейсов**.

Группирование интерфейсов
Вы можете сгруппировать интерфейсы маршрутизатора на сетевом уровне.

Группирование интерфейсов +

<input type="checkbox"/>	Имя	Тип группы	Интерфейсы	WAN-соединения	VPN-соединения
<input type="checkbox"/>	Default	NAT	Port1, Port2, Port3, Port4, Port5, SFP1	statip_50	IPsec_77

1.6.3. Далее необходимо добавить IPsec-туннель в зону. Для этого в левом меню перейдите к разделу **Межсетевой экран** и далее – на страницу **Зоны**.

D-Link Building Networks for People

Группирование интерфейсов

Зоны

IPv4

Зоны +

<input type="checkbox"/>	Имя	Тип	Интерфейсы
<input type="checkbox"/>	fw	firewall	-
<input type="checkbox"/>	wan	ipv4	statip_50
<input type="checkbox"/>	lan	ipv4	LAN

IPv6

Во вкладке **IPv4** добавьте новую зону, нажав на «+».

Добавление зоны
✕

Имя*

Доступ между интерфейсами

Доступные интерфейсы

IPsec_77

СОХРАНИТЬ

Заполните параметры, как представлено ниже, и нажмите **Сохранить**.

Редактирование зоны
✕

Имя*

IPsec_77

Доступ между интерфейсами

Доступные интерфейсы

IPsec_77

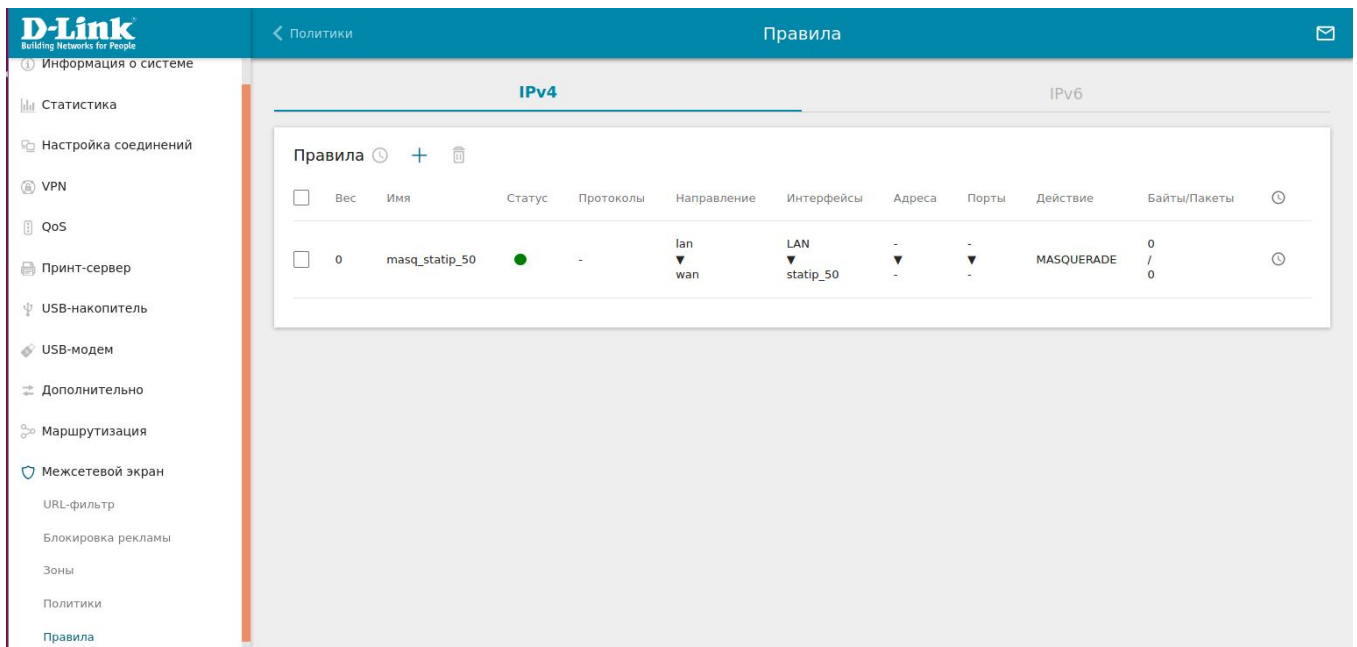
СОХРАНИТЬ

Проверить добавленную зону для IPsec можно в разделе **Межсетевой экран**, далее — страница **Зоны**.

The screenshot shows the D-Link web interface. The top navigation bar includes the D-Link logo and the text 'Building Networks for People'. The main header shows 'Группирование интерфейсов' and 'Зоны'. A left sidebar menu lists various network settings, with 'Межсетевой экран' (Inter-network Firewall) selected. The main content area is titled 'IPv4' and shows a table of zones.

Зоны +	Тип	Интерфейсы
<input type="checkbox"/> Имя		
<input type="checkbox"/> fw	firewall	-
<input type="checkbox"/> wan	ipv4	statip_50
<input type="checkbox"/> lan	ipv4	LAN
<input type="checkbox"/> IPsec_77	ipv4	IPsec_77

1.6.4. Далее для данного IPsec-туннеля потребуется создать 2 правила. Для этого в левом меню перейдите к разделу **Межсетевой экран** и далее – на страницу **Правила**.



Во вкладке **IPv4** добавьте новое правило, нажав на «+».

Заполните в правилах поля, как показано ниже, и нажмите кнопку **Применить**.

- *Правило для протокола UDP:*

Основные настройки

Включить правило

Таблица: Filter

Действие: АССЕРТ

Состояние соединения: Не добавлено ни одного состояния соединения

[ДОБАВИТЬ СОСТОЯНИЕ](#)

Источник: Зона* wan

Интерфейс: Не выбрано

Адреса источника: Исключить указанные адреса

Не добавлено ни одного адреса

[ДОБАВИТЬ АДРЕС](#)

Имя* IPsec_udp

Вес* 0

Направление: NONE

Протоколы: udp

[ДОБАВИТЬ ПРОТОКОЛ](#)

Назначение: Зона* fw

Адреса назначения: Исключить указанные адреса

Не добавлено ни одного адреса

[ДОБАВИТЬ АДРЕС](#)

[ДОБАВИТЬ ССЫЛКУ](#)

[ДОБАВИТЬ ССЫЛКУ](#)

Порты источника

Исключить указанные порты

Не добавлено ни одного порта

[ДОБАВИТЬ ПОРТ](#)

Сравнение TTL

Метод сравнения

=

Сравниваемое значение*

-1

Recent

Действия [+](#)

Не добавлено ни одного действия

[ПРИМЕНИТЬ](#)

Порты назначения

Исключить указанные порты

Вы можете указать один порт или диапазон портов через двоеточие (например, 80:90)

500

4500

[ДОБАВИТЬ ПОРТ](#)

- Правило для протокола ESP:

Основные настройки

Включить правило [🕒](#)

Таблица

Filter

Действие

АССЕРТ

Состояние соединения

Не добавлено ни одного состояния соединения

[ДОБАВИТЬ СОСТОЯНИЕ](#)

Источник

Зона*

wan

Интерфейс

Не выбрано

Адреса источника

Исключить указанные адреса

Не добавлено ни одного адреса

[ДОБАВИТЬ АДРЕС](#)

Имя*

IPsec_esp

Вес*

0

Направление

NONE

Протоколы

esp

[ДОБАВИТЬ ПРОТОКОЛ](#)

Назначение

Зона*

fw

Адреса назначения

Исключить указанные адреса

Не добавлено ни одного адреса

[ДОБАВИТЬ АДРЕС](#)

[ДОБАВИТЬ ССЫЛКУ](#)

ДОБАВИТЬ ССЫЛКУ

Сравнение TTL

Метод сравнения
=

Сравниваемое значение*
-1

Recent

Действия +

Не добавлено ни одного действия

ПРИМЕНИТЬ

Проверить настроенные правила можно в разделе **Межсетевой экран**, далее – **Правила**.

Правила

Правила	Вес	Имя	Статус	Протоколы	Направление	Интерфейсы	Адреса	Порты	Действие	Байты/Пакеты
<input type="checkbox"/>	0	IPsec_udp	●	udp	wan ▼ fw	- ▼ -	- ▼ -	- ▼ [500], ...	ACCEPT	0 / 0
<input type="checkbox"/>	0	IPsec_esp	●	esp	wan ▼ fw	- ▼ -	- ▼ -	- ▼ -	ACCEPT	0 / 0
<input type="checkbox"/>	0	masq_statip_50	●	-	lan ▼ wan	LAN ▼ statip_50	- ▼ -	- ▼ -	MASQUERADE	0 / 0

1.6.5. Затем необходимо для IPsec-туннеля создать политики для обозначения направления прохождения трафика. Для этого в левом меню перейдите к разделу **Межсетевой экран** и далее – на страницу **Политики**.

Политики

Политики	Источник	Назначение	Действие	Уровень журналирования
<input type="checkbox"/>	all	all	DROP	Отключено
<input type="checkbox"/>	fw	all	ACCEPT	Отключено
<input type="checkbox"/>	lan	fw	ACCEPT	Отключено
<input type="checkbox"/>	lan	wan	ACCEPT	Отключено

Во вкладке **IPv4** добавьте новую политику, нажав на «+».

Добавление политики ×

Источник*
Нет ▼

Назначение*
Нет ▼

Действие
DROP ▼

Уровень журналирования
Отключено ▼

СОХРАНИТЬ

В открывшемся окне укажите вариант прохождения трафика, выбрав необходимые зоны и действие (**АССЕПТ**, **DROP** или **REJECT**), затем нажмите **СОХРАНИТЬ**.

Ниже приведен пример создания политики для прохождения трафика между локальными клиентами, подключенными к LAN-интерфейсу маршрутизатора DSA-2108S, и локальными клиентами, подключенными к LAN-интерфейсу маршрутизатора DSA-2003.

Добавление политики ×

Источник*
IPsec_77 ▼

Назначение*
wan ▼

Действие
АССЕПТ ▼

Уровень журналирования
Отключено ▼

СОХРАНИТЬ

Добавление политики ×

Источник*
IPsec_77 ▼

Назначение*
lan ▼

Действие
АССЕПТ ▼

Уровень журналирования
Отключено ▼

СОХРАНИТЬ

Если потребуется обеспечить доступ LAN-клиентам маршрутизатора DSA-2003 к управлению маршрутизатором DSA-2108S, то необходимо создать разрешающую политику (**АССЕПТ**) для IPsec-туннеля, выбрав в поле **Назначение** интерфейс **fw**:

Добавление политики ×

Источник*
IPsec_77 ▼

Назначение*
fw ▼

Действие
АССЕПТ ▼

Уровень журналирования
Отключено ▼

СОХРАНИТЬ

Для проверки настроенных политик перейдите в левом меню в раздел **Межсетевой экран**, далее – в **Политики**.

Источники	Назначение	Действие	Уровень журналирования	
<input type="checkbox"/>	all	DROP	Отключено	
<input type="checkbox"/>	fw	ACCEPT	Отключено	
<input type="checkbox"/>	lan	ACCEPT	Отключено	
<input type="checkbox"/>	lan	wan	ACCEPT	Отключено
<input type="checkbox"/>	IPsec_77	wan	ACCEPT	Отключено
<input type="checkbox"/>	IPsec_77	lan	ACCEPT	Отключено
<input type="checkbox"/>	IPsec_77	fw	ACCEPT	Отключено

1.7. Для проверки настроенного IPsec-туннеля перейдите в левом меню в раздел **VPN**, далее – в **IPsec**.

IPsec
Вы можете настроить VPN-туннели, работающие по протоколу IPsec.

ВЫКЛЮЧИТЬ

Уровень журналирования: Базовый

Туннели ПЕРЕПОДКЛЮЧИТЬ +

Удаленный хост	Режим	Интерфейс	Алгоритм шифрования/хеширования	
			Первая фаза	Вторая фаза
<input type="checkbox"/>	TUNNEL	statip_50	DES/MD5	DES/MD5

Статус

Удаленный хост	IKE	CHILD	Состояние
10.0.0.2	Подключено	Подключено	Включен ●

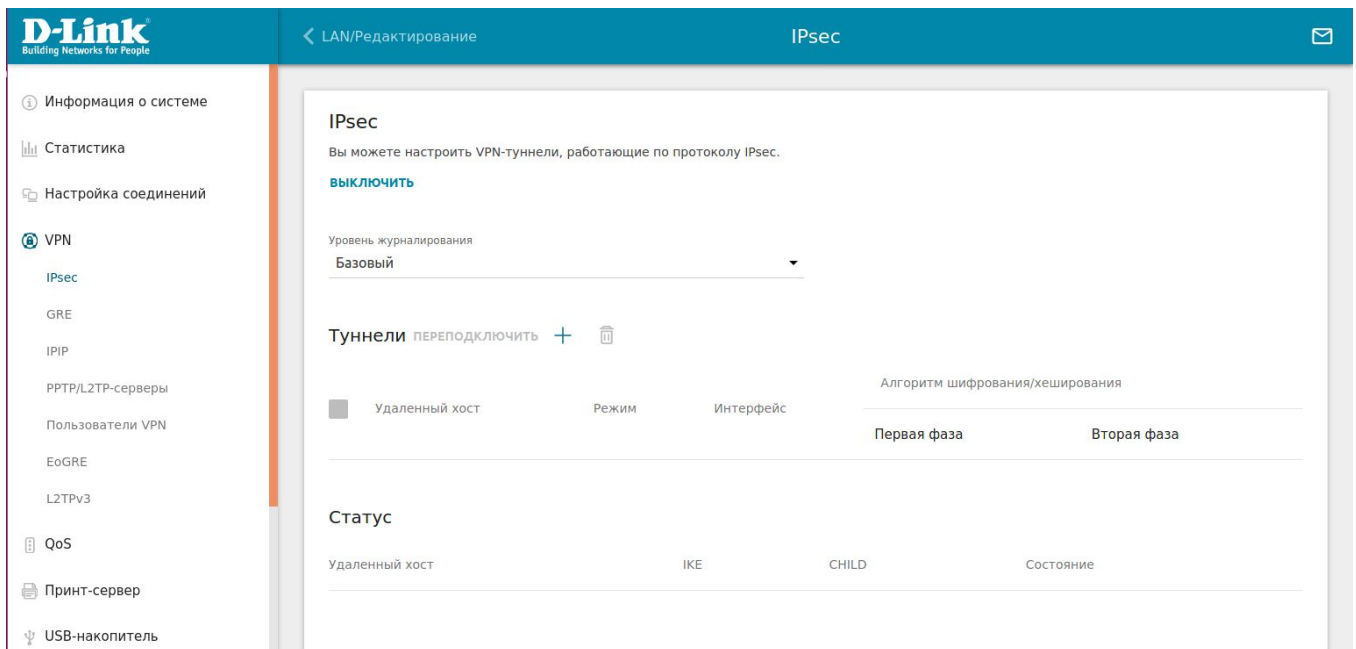
Настройка маршрутизатора DSA-2108S завершена.

2. Настройка DSA-2003

2.1. В основном меню слева перейдите к разделу **VPN**, далее – на страницу **IPsec**. Для включения VPN-сервиса IPsec нажмите **Включить**.

IPsec
Вы можете настроить VPN-туннели, работающие по протоколу IPsec.

ВКЛЮЧИТЬ



2.2. В открывшемся окне создайте туннель, нажав на «+». Заполните поля раздела **Главные настройки** следующим образом:

Главные настройки	
<input checked="" type="checkbox"/> Включить	Действие DPD Перезапуск
Имя* IPsec_63	DPD - Dead Peer Detection
Версия IP IPv4	Задержка DPD (в секундах)* 30
<input type="checkbox"/> Динамический IPsec	Тайм-аут DPD (в секундах)* 120
Тип Address	TCP MSS Path MTU discovery
Удаленный хост* 10.0.0.1	
Удаленный идентификатор	
Удаленный порт	
Ключ* test	
Тип интерфейса Соединение / Интерфейс	
Интерфейс* statip_25	
Локальный идентификатор	
Локальный порт	
NAT Traversal Отключено	
Режим TUNNEL	

В графе **Удаленный хост** укажите IP-адрес WAN-интерфейса удаленного маршрутизатора DSA-2108S (в данном примере это *10.0.0.1*).

В графе **Ключ** укажите тот же ключ шифрования, который был указан в настройках DSA-2108S (в данном примере это *test*).

Выберите **Тип интерфейса**: Соединение/Интерфейс и в графе **Интерфейс** укажите конкретное соединения, для которого организуется IPsec-туннель (в данном примере это *statip_25*).

2.3. Все остальные настройки, включая настройки времени жизни и шифрование для 1 и 2 фазы, оставьте по умолчанию. Настройки 1 и 2 фазы приведены ниже.

Первая фаза	Вторая фаза
Алгоритм шифрования первой фазы DES	Алгоритм шифрования второй фазы DES
Режим шифрования CBC	Режим шифрования CBC
Алгоритм хеширования MD5	Алгоритм хеширования MD5
Размер хеша 96	Размер хеша 96
Режим хеширования HMAC	Режим хеширования HMAC
Тип DHgroup первой фазы MODP768	<input checked="" type="checkbox"/> Включить PFS
ИKE-SA время жизни* 10800	Тип DHgroup второй фазы MODP768
<input type="checkbox"/> Aggressive режим	IPsec-SA время жизни* 3600
Версия IKE 1	

2.4. В разделе **Туннелируемые подсети** необходимо добавить локальную и удаленную подсеть для настраиваемого туннеля, для этого нажмите кнопку «+»

Туннелируемые подсети +

Локальная подсеть Удаленная подсеть

ПРИМЕНИТЬ

Добавьте адрес локальной подсети (в данном примере это *192.168.0.0/24*) и адрес удаленной подсети (в данном примере это *192.168.10.0/24*), затем нажмите **Сохранить**.

Добавить правило ×

Локальная подсеть*
192.168.0.0/24

Задайте локальную подсеть IPsec-туннеля (LAN-сеть маршрутизатора). Пример: 192.168.0.0/24

Удаленная подсеть*
192.168.10.0/24

Задайте удаленную подсеть IPsec-туннеля (LAN-сеть удаленного устройства, выполняющего роль маршрутизатора). Пример: 192.168.10.0/24

СОХРАНИТЬ

2.5. Нажмите кнопку **Применить**.

Чтобы изменить версию протокола IKE, удалите все туннелируемые подсети

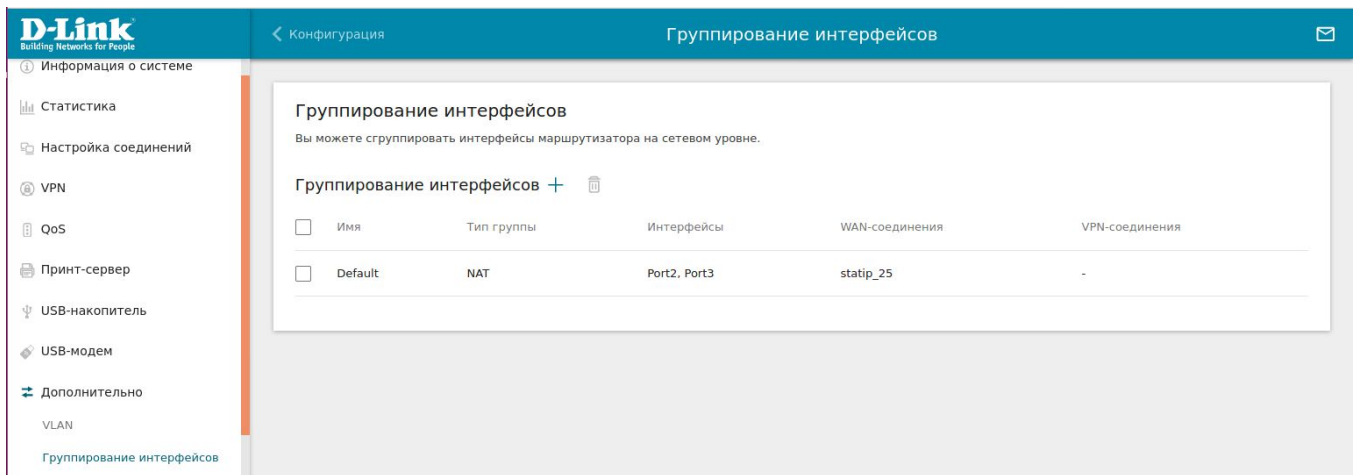
Туннелируемые подсети +

<input type="checkbox"/> Локальная подсеть	Удаленная подсеть
<input type="checkbox"/> 192.168.0.0/24	192.168.10.0/24

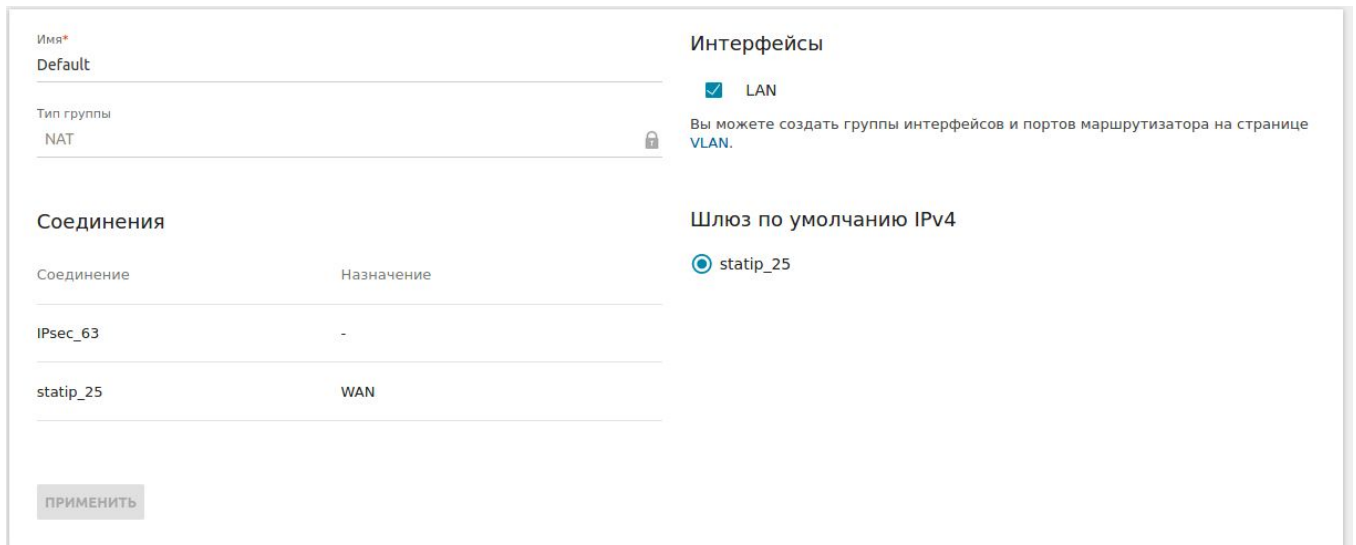
ПРИМЕНИТЬ

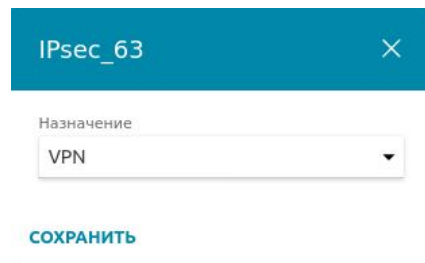
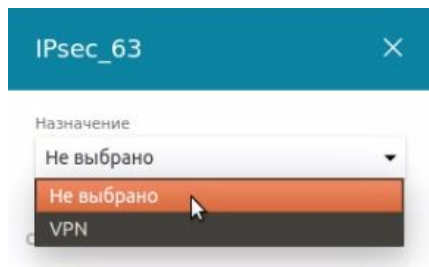
2.6. Для корректной работы созданный IPsec-туннель необходимо добавить в группу интерфейсов, а также добавить настройки межсетевого экрана. Для маршрутизатора DSA-2003 настройка выполняется вручную. Пример приведен для IPsec-туннеля с именем *IPsec_63*.

2.6.1. В левом меню перейдите к разделу **Дополнительно**, откройте страницу **Группирование интерфейсов**.



На странице **Группирование интерфейсов** перейдите в группу с именем **Default**, в графе **Соединения** выберите IPsec-туннель *IPsec_63* и укажите его в качестве **VPN**. Нажмите **Сохранить**.





Имя*
Default

Тип группы
NAT

Интерфейсы
 LAN
Вы можете создать группы интерфейсов и портов маршрутизатора на странице [VLAN](#).

Соединения

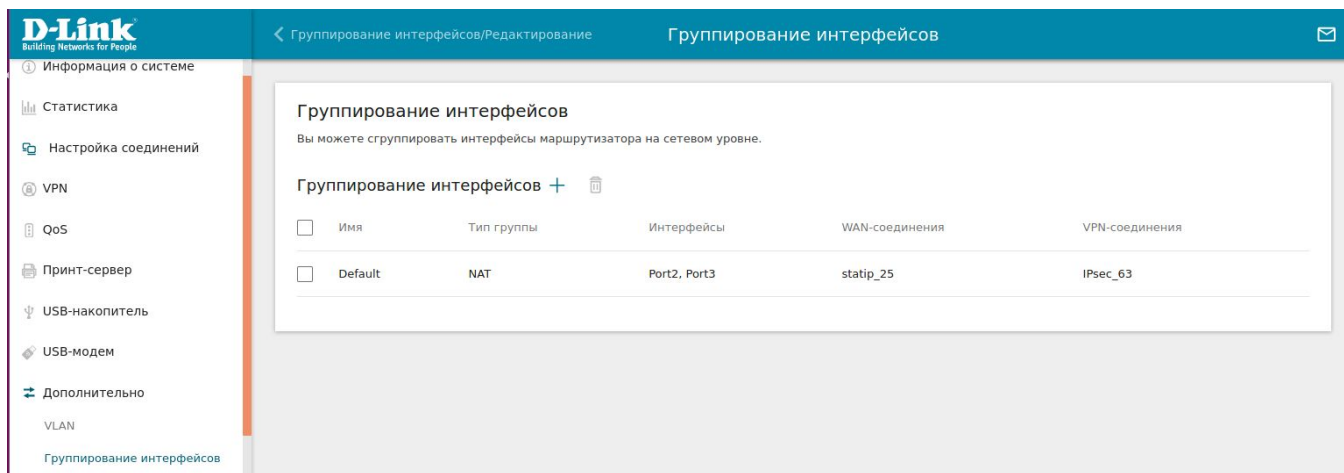
Соединение	Назначение
IPsec_63	VPN
statip_25	WAN

Шлюз по умолчанию IPv4
 statip_25

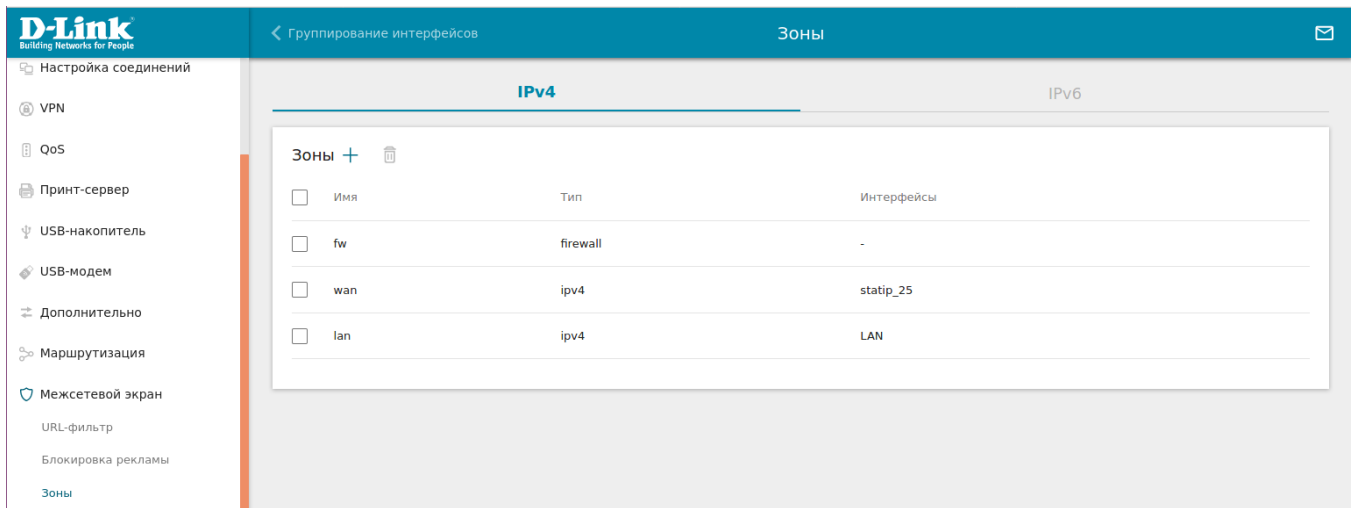
ПРИМЕНИТЬ

Для сохранения всех настроек нажмите кнопку **Применить**.

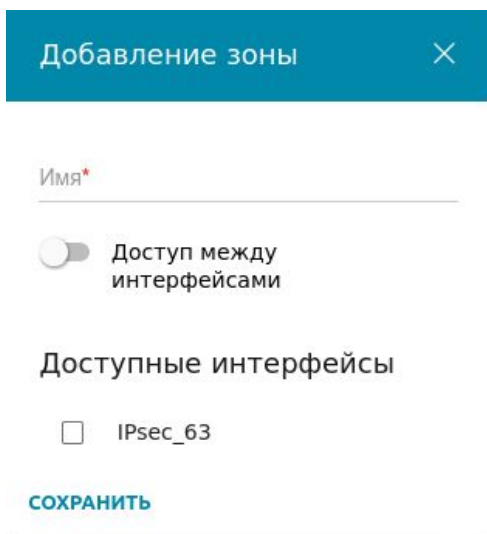
Проверить добавленный IPsec-туннель можно в разделе **Группирование интерфейсов**.



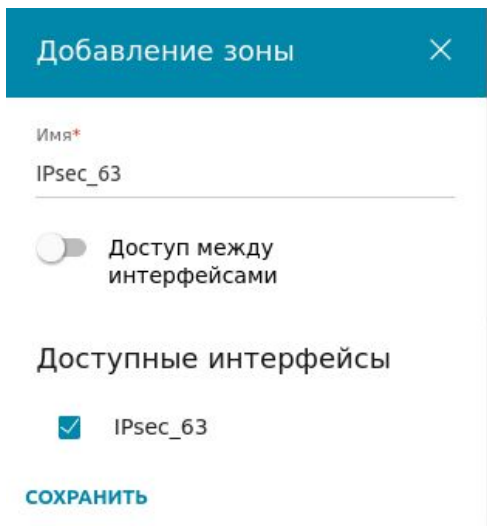
2.6.2. Далее необходимо добавить IPsec-туннель в зону. Для этого в левом меню перейдите к разделу **Межсетевой экран**, и далее – на страницу **Зоны**.



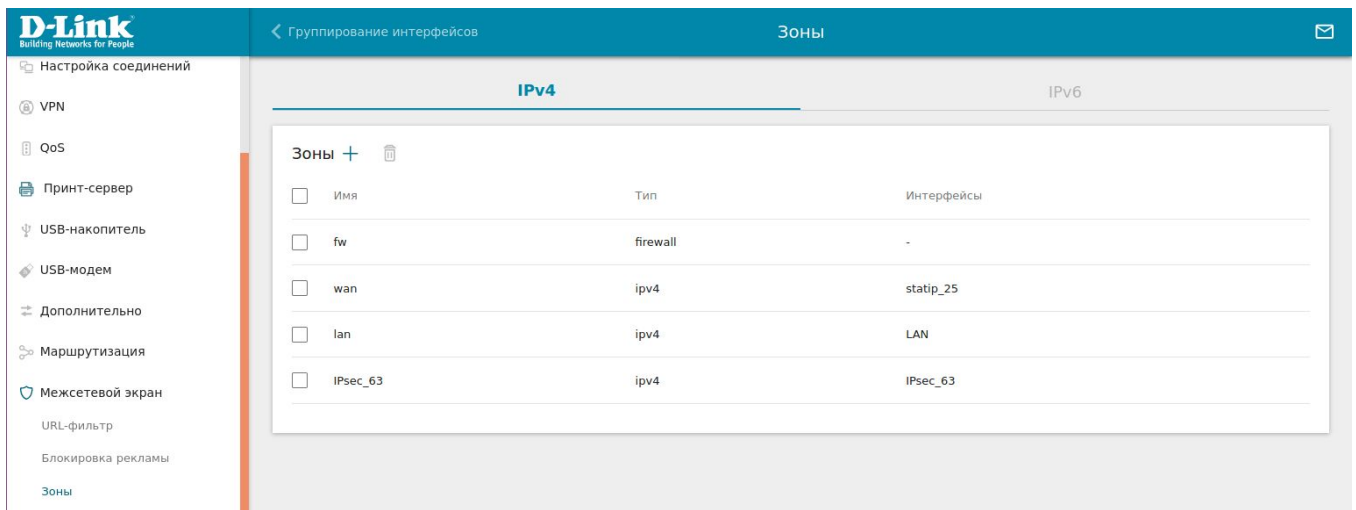
Во вкладке **IPv4** добавьте новую зону, нажав на «+».



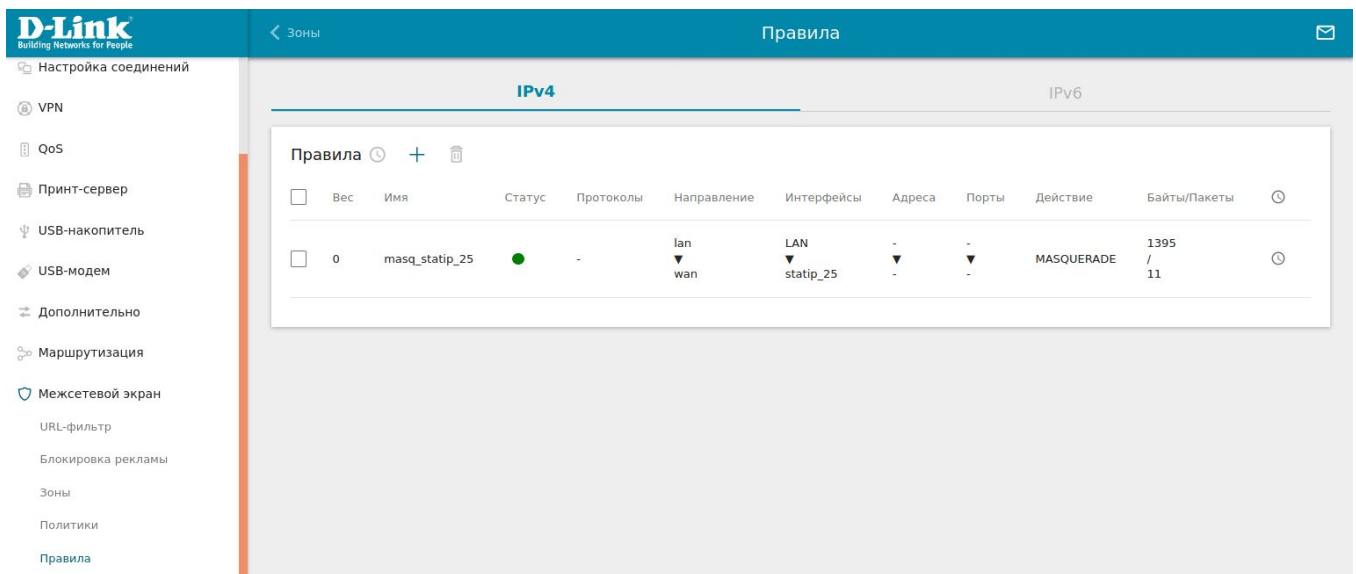
Заполните параметры, как представлено ниже, и нажмите **Сохранить**.



Проверить добавленную зону для IPsec можно в разделе **Межсетевой экран**, далее — страница **Зоны**.



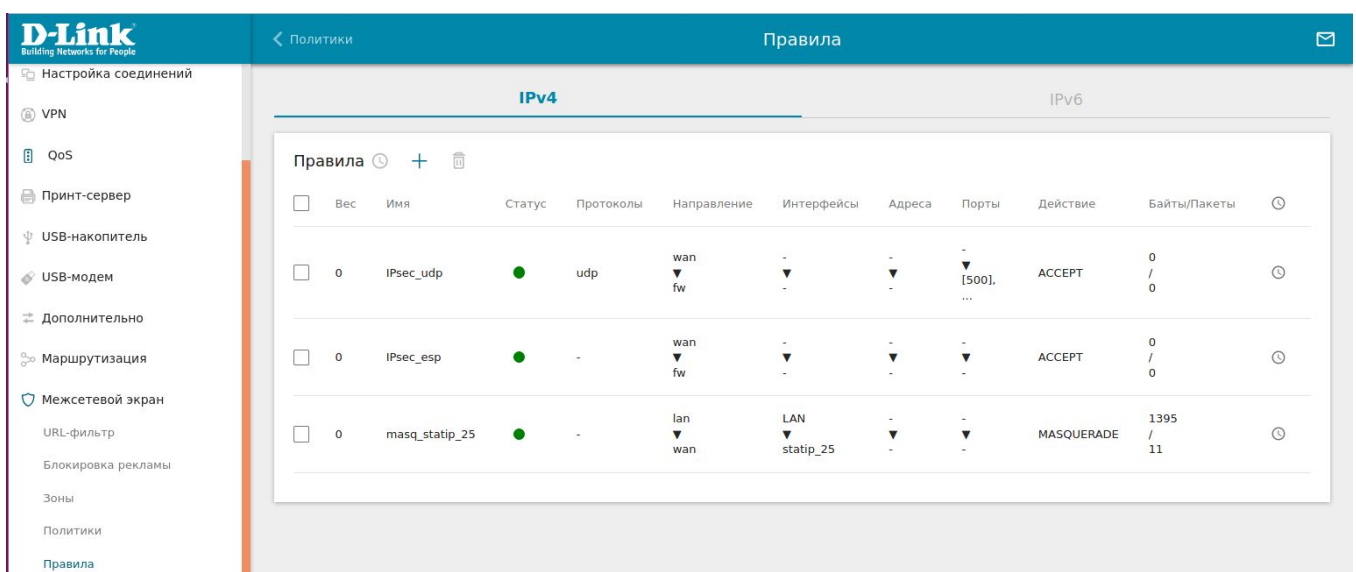
2.6.3. Далее для данного IPsec туннеля потребуется создать 2 правила. Для этого в левом меню перейдите к разделу **Межсетевой экран**, и далее – на страницу **Правила**.



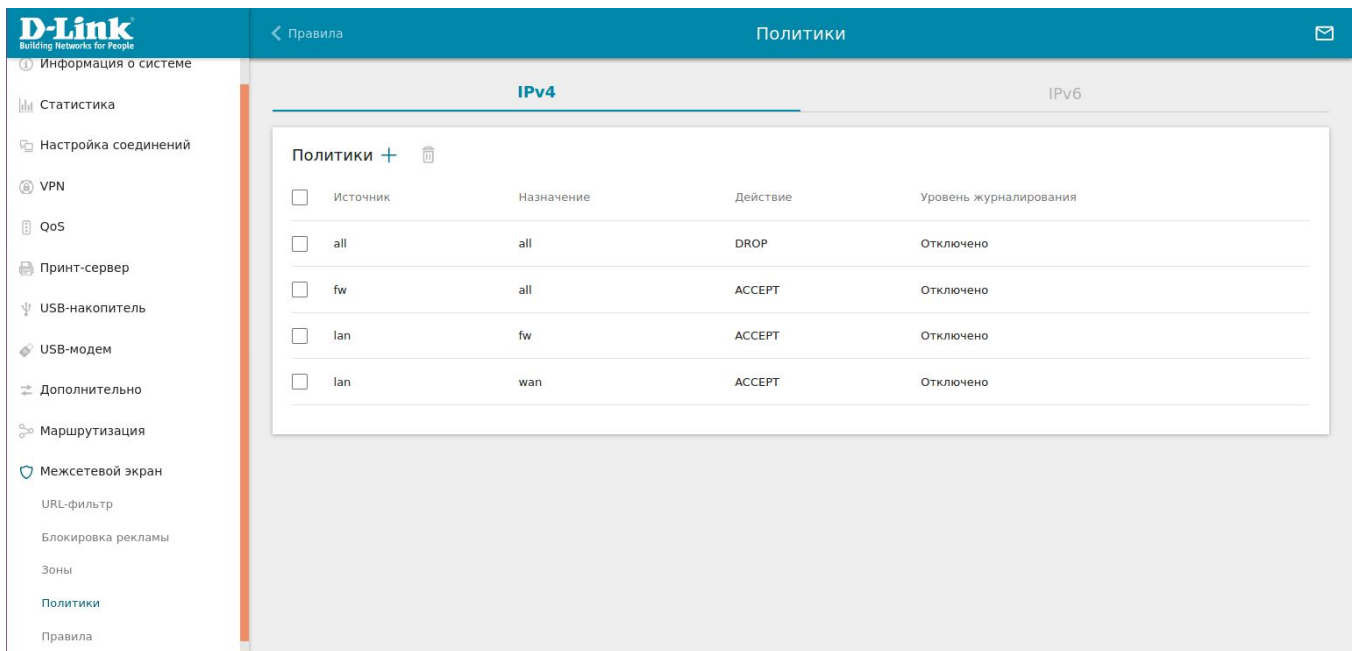
Во вкладке **IPv4** добавьте 2 новых правила по протоколам UDP и ESP, нажав на «+».

Настройка правил для DSA-2003 проводится аналогично DSA-2108S (см. п.1.6.4).

Для проверки настроенных правил перейдите в левом меню в раздел **Межсетевой экран**, далее – в **Правила**.



2.6.4. Затем потребуется для IPsec-туннеля создать политики для обозначения направления прохождения трафика. Для этого в левом меню перейдите к разделу **Межсетевой экран**, и далее – на страницу **Политики**.



Во вкладке IPv4 добавьте новую политику, нажав на «+».

Добавление политики
✕

Источник*

Нет ▾

Назначение*

Нет ▾

Действие

DROP ▾

Уровень журналирования

Отключено ▾

СОХРАНИТЬ

В открывшемся окне укажите вариант прохождения трафика, выбрав необходимые зоны и действие (ACCEPT, DROP или REJECT), затем нажмите СОХРАНИТЬ.

Ниже приведен пример создания политики для прохождения трафика между локальными клиентами, подключенными к LAN-интерфейсу маршрутизатора DSA-2003, и локальными клиентами, подключенными к LAN-интерфейсу маршрутизатора DSA-2108S.

Добавление политики
✕

Источник*

IPsec_63 ▾

Назначение*

wan ▾

Действие

ACCEPT ▾

Уровень журналирования

Отключено ▾

СОХРАНИТЬ

Добавление политики
✕

Источник*

IPsec_63 ▾

Назначение*

lan ▾

Действие

ACCEPT ▾

Уровень журналирования

Отключено ▾

СОХРАНИТЬ

Если потребуется обеспечить доступ LAN-клиентам маршрутизатора DSA-2108S к управлению маршрутизатором DSA-2003, то необходимо создать разрешающую политику (ACCEPT) для IPsec-туннеля, выбрав в поле **Назначение** интерфейс **fw**:

Добавление политики

Источник*
IPsec_63

Назначение*
fw

Действие
ACCEPT

Уровень журналирования
Отключено

СОХРАНИТЬ

Для проверки настроенных политик перейдите в левом меню в раздел **Межсетевой экран**, далее – в **Политики**.

Политики

Источник	Назначение	Действие	Уровень журналирования
all	all	DROP	Отключено
fw	all	ACCEPT	Отключено
lan	fw	ACCEPT	Отключено
lan	wan	ACCEPT	Отключено
IPsec_63	wan	ACCEPT	Отключено
IPsec_63	lan	ACCEPT	Отключено
IPsec_63	fw	ACCEPT	Отключено

2.7. Для проверки настроенного IPsec-туннеля перейдите в левом меню в раздел **VPN**, далее – в **IPsec**.

D-Link
Building Networks for People

← Политики IPsec

Информация о системе
Статистика
Настройка соединений
VPN
IPsec
GRE
IPIP
PPTP/L2TP-серверы
Пользователи VPN
EoGRE
L2TPv3
QoS
Принт-сервер
USB-накопитель
USB-модем
Дополнительно

IPsec

Вы можете настроить VPN-туннели, работающие по протоколу IPsec.

ВЫКЛЮЧИТЬ

Уровень журналирования
Базовый

Туннели

переключить +

	Удаленный хост	Режим	Интерфейс	Алгоритм шифрования/хеширования	
				Первая фаза	Вторая фаза
<input type="checkbox"/>	10.0.0.1	TUNNEL	statip_25	DES/MD5	DES/MD5

Статус

Удаленный хост	IKE	CHILD	Состояние
10.0.0.1	Подключено	Подключено	Включен ●

Настройка маршрутизатора DSA-2003 завершена.