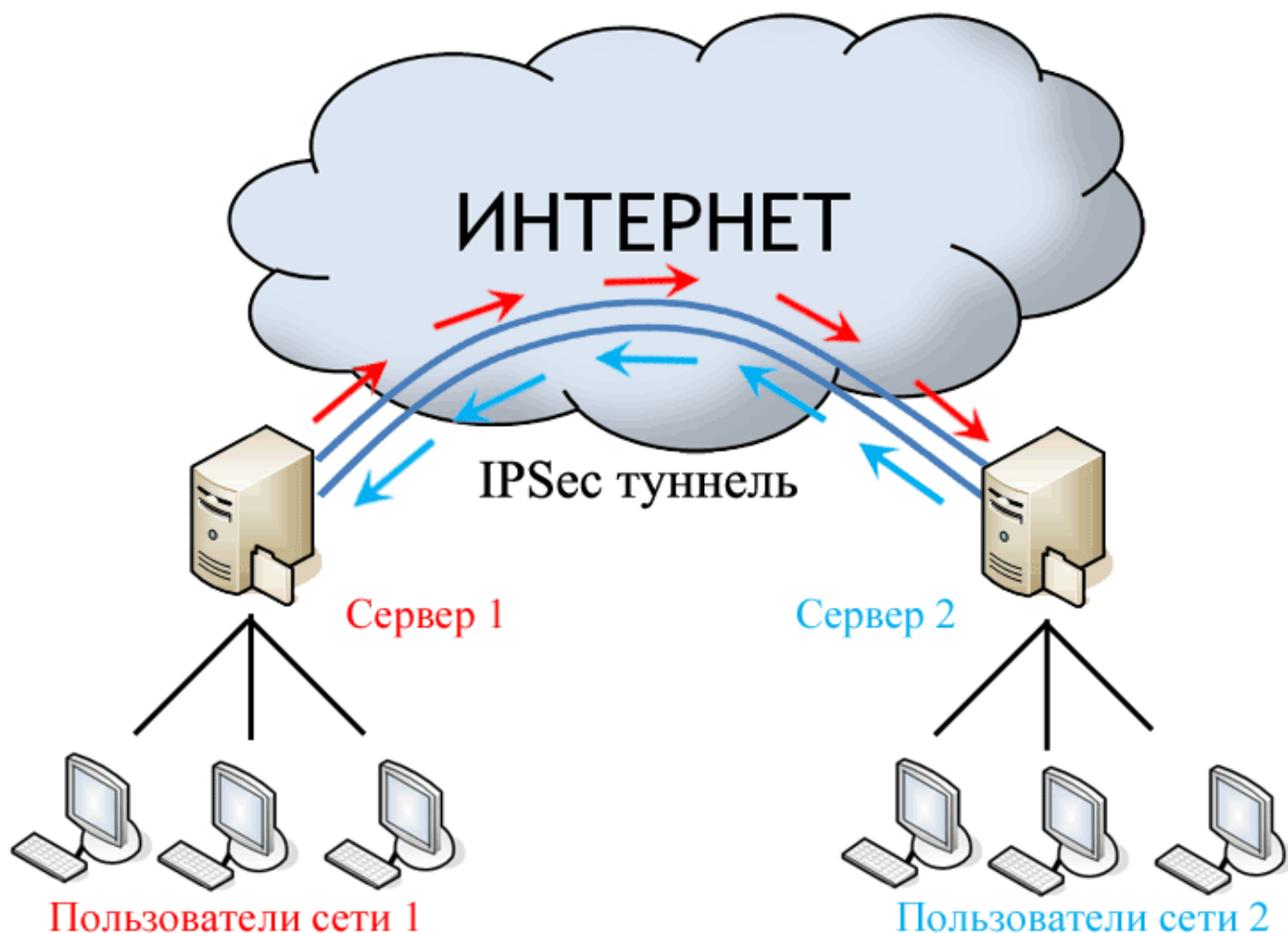


# Настройка IPsec-туннеля.

Если в вашей компании имеется удаленный филиал, то для объединения локальных сетей безопасным способом наиболее подходящим решением будет являться настройка зашифрованного туннеля между ними.



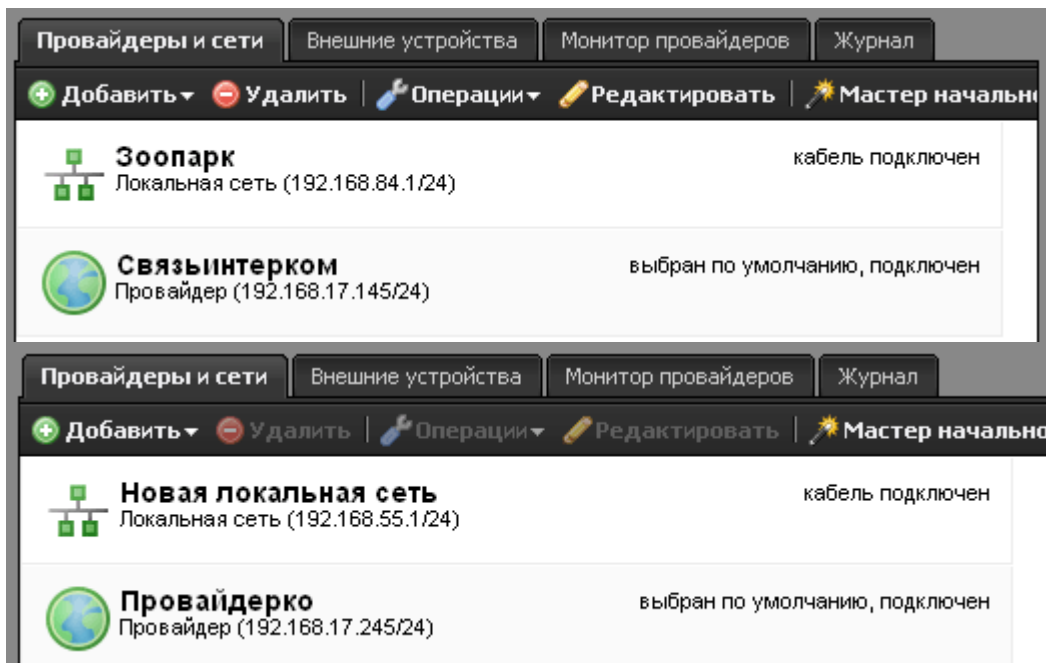
Для настройки IPsec или GRE-туннеля между двумя ИКС необходимо выполнить следующие действия:

1. Добавить новый туннель IPsec или GRE
2. Указать список локальных и удаленных сетей для маршрутизации между ними
3. Настроить параметры шифрования
4. Добавить в межсетевой экран необходимые разрешающие правила.

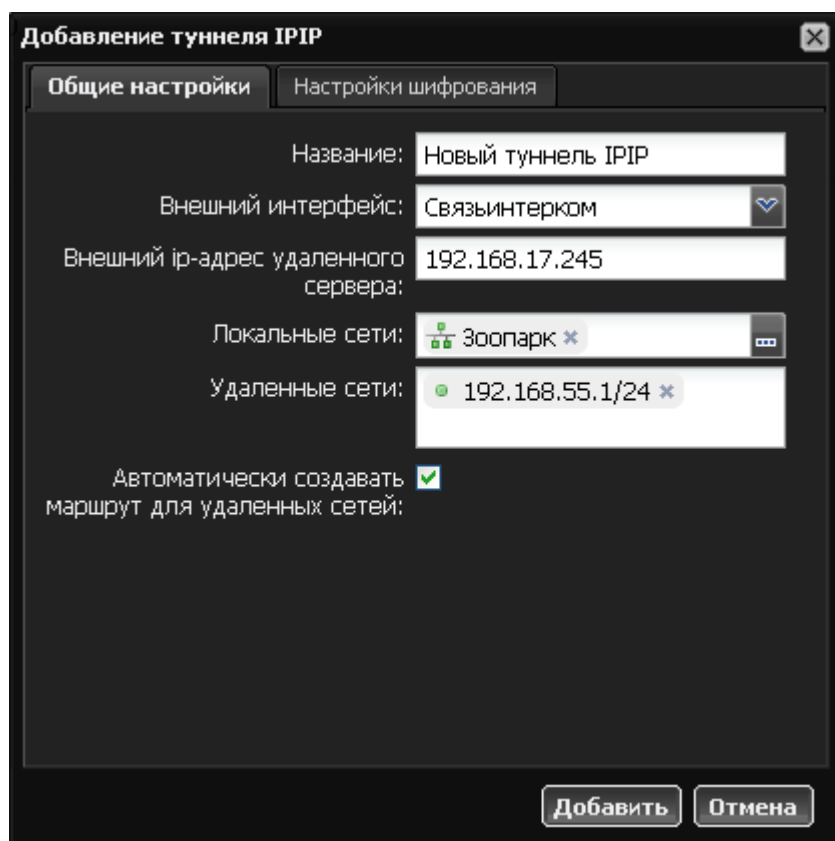
После чего все действия необходимо произвести на втором конце туннеля.

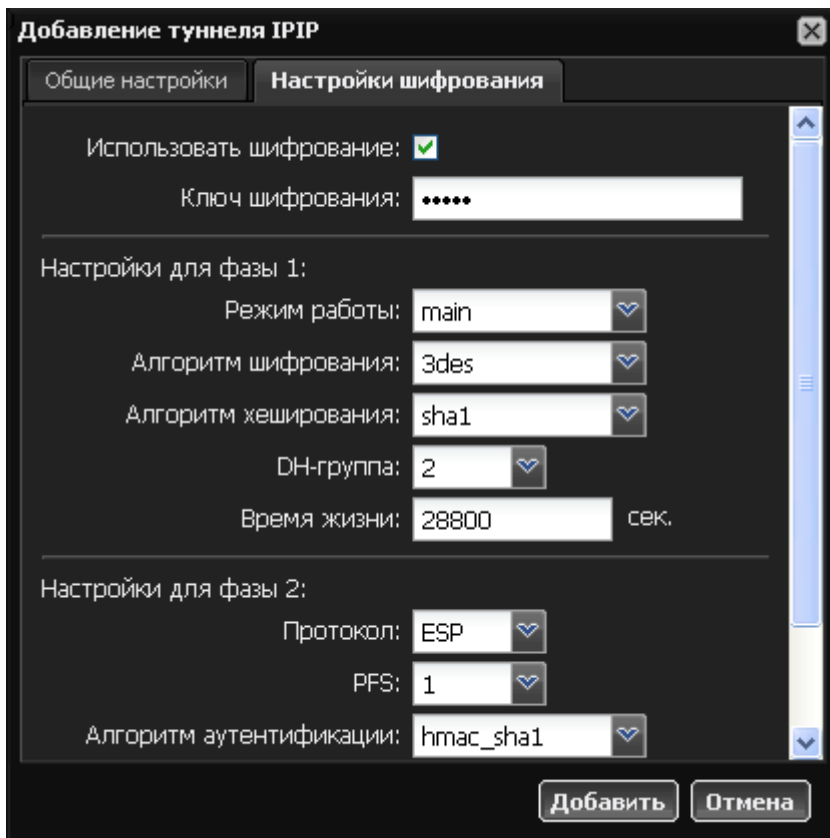
В нашем примере мы создадим туннель между двумя серверами.

	Сервер 1	Сервер 2
Внешний адрес	192.168.17.145	192.168.17.245
Адрес локальной сети	192.168.84.1/24	192.168.55.1/24



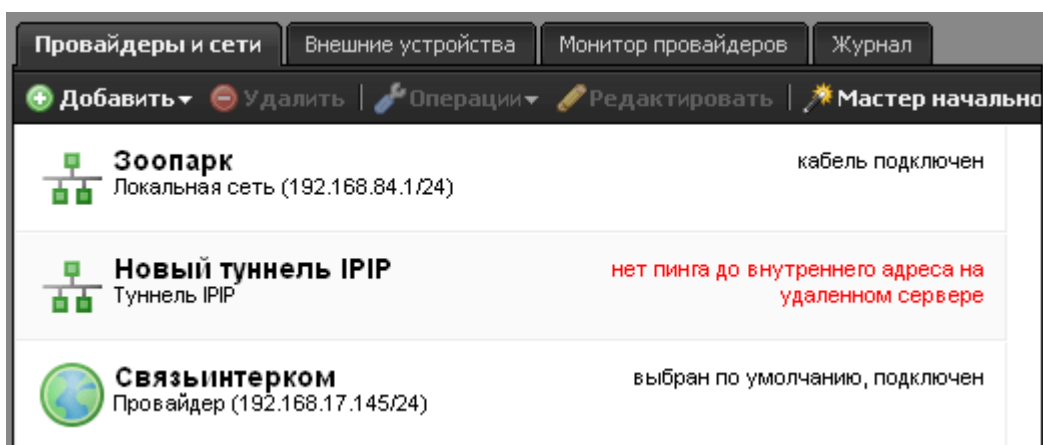
Сначала добавим новый IP-туннель в модуле «Провайдер и сети».





Выбираем в качестве исходящего интерфейса нашего провайдера, указываем внешний адрес Сервера 2, выбираем локальную сеть и прописываем в удаленной сети сеть Сервера 2. Чтобы пользователи автоматически могли получить доступ к хостам в локальной сети Сервера 2, устанавливаем флажок «Автоматически создавать маршрут для удаленных сетей».

Затем переходим во вкладку «Шифрование», включаем его и устанавливаем pre-shared key. Остальные параметры имеют оптимальные настройки, их можно оставить по умолчанию.



Красный статус «нет пинга до внутреннего адреса на удаленном сервере» сигнализирует о том, что туннель создан, но не установлен. Продолжаем настройку.

Чтобы разрешить Серверу 1 принимать пакеты через туннель от Сервера 2, необходимо создать разрешающее правило. Для этого нужно перейти в модуль «Межсетевой экран» и добавить новое разрешающее правило.

**Добавление разрешающего правила**

Описание: Тестовый туннель

Направление: Входящий и исходящий

Источник: 192.168.17.245

Назначение: (любой)

Протокол: (любой)

Порт источника: (любой)

Порт назначения: (любой)

Интерфейс: (любой)

Время действия: (всегда)

Добавить Отмена

В правиле достаточно указать ip-адрес Сервера 2 в качестве источника. Остальные параметры указывать не обязательно. Также необходимо проверить, что в списке правил присутствует и включено правило по умолчанию «Доступ к серверу через GRE тоннели», разрешающее прохождение GRE-трафика.

Теперь всю процедуру необходимо повторить на Сервере 2.

**Добавление туннеля IP/IP**

Общие настройки | Настройки шифрования

Название: Тестовый туннель

Внешний интерфейс: Провайдерко

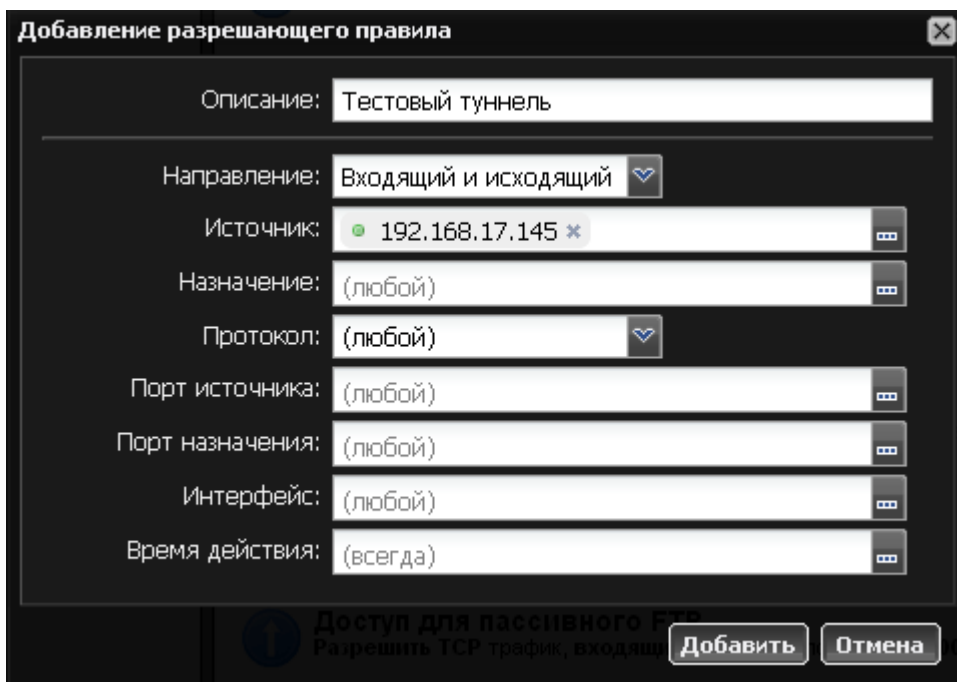
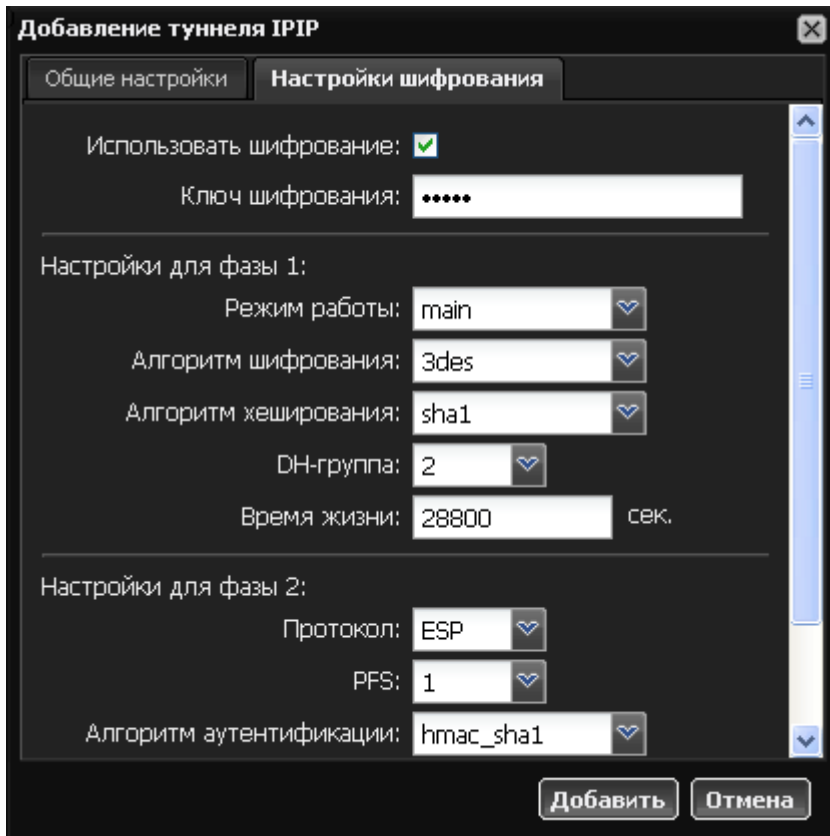
Внешний ip-адрес удаленного сервера: 192.168.17.145

Локальные сети: Новая локальная сеть

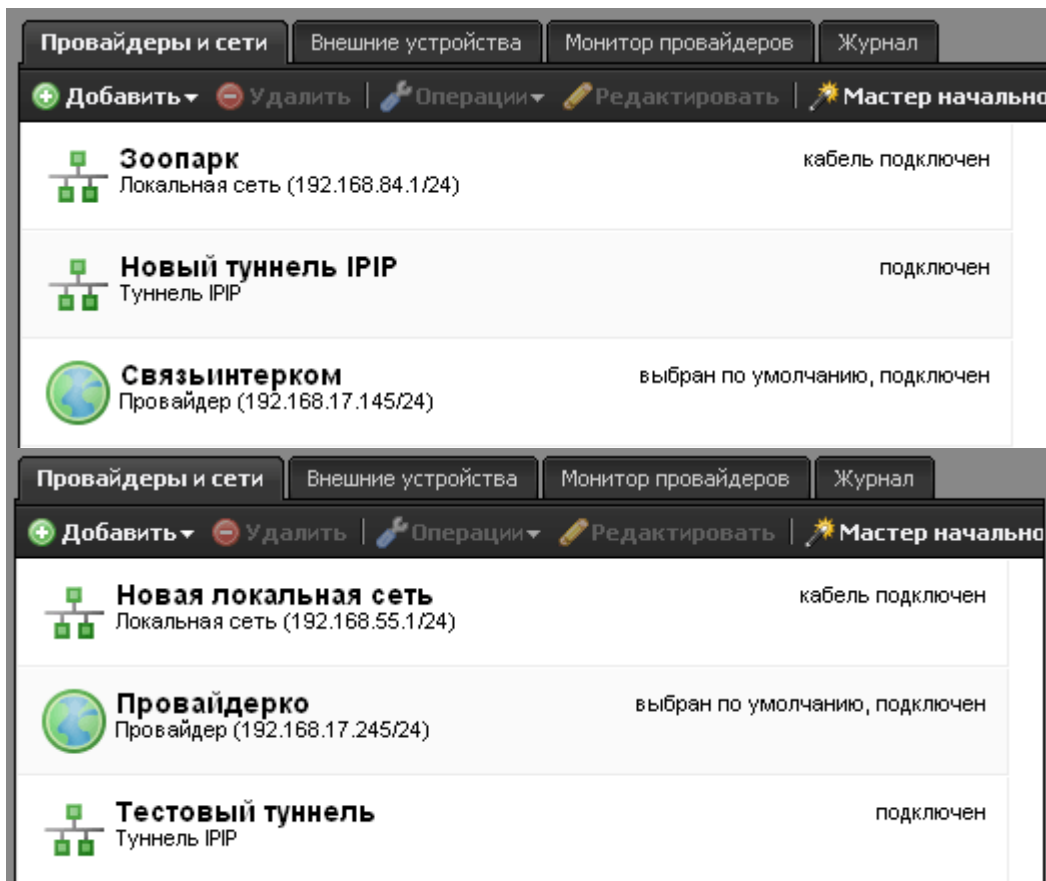
Удаленные сети: 192.168.84.1/24

Автоматически создавать маршрут для удаленных сетей:

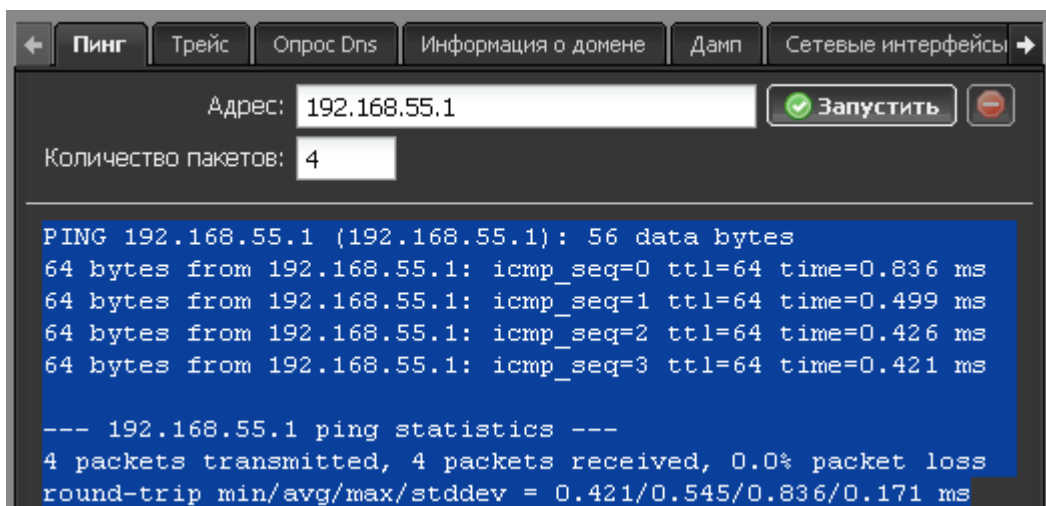
Добавить Отмена



Теперь, если все настроено верно, в статусе созданного туннеля на каждом сервере должна появиться надпись «подключен».



Проверить работу туннеля можно с помощью модуля «Сетевые утилиты», запустив пинг с Сервера 1 на внутренний интерфейс Сервера 2.



Ваш туннель настроен и работает. Теперь вы можете использовать ресурсы обоих филиалов одновременно.

From: <https://doc.a-real.ru/> - **Документация**

Permanent link: [https://doc.a-real.ru/doku.php?id=en:%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80\\_ipip](https://doc.a-real.ru/doku.php?id=en:%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D1%80_ipip)

Last update: **2020/01/27 16:28**

