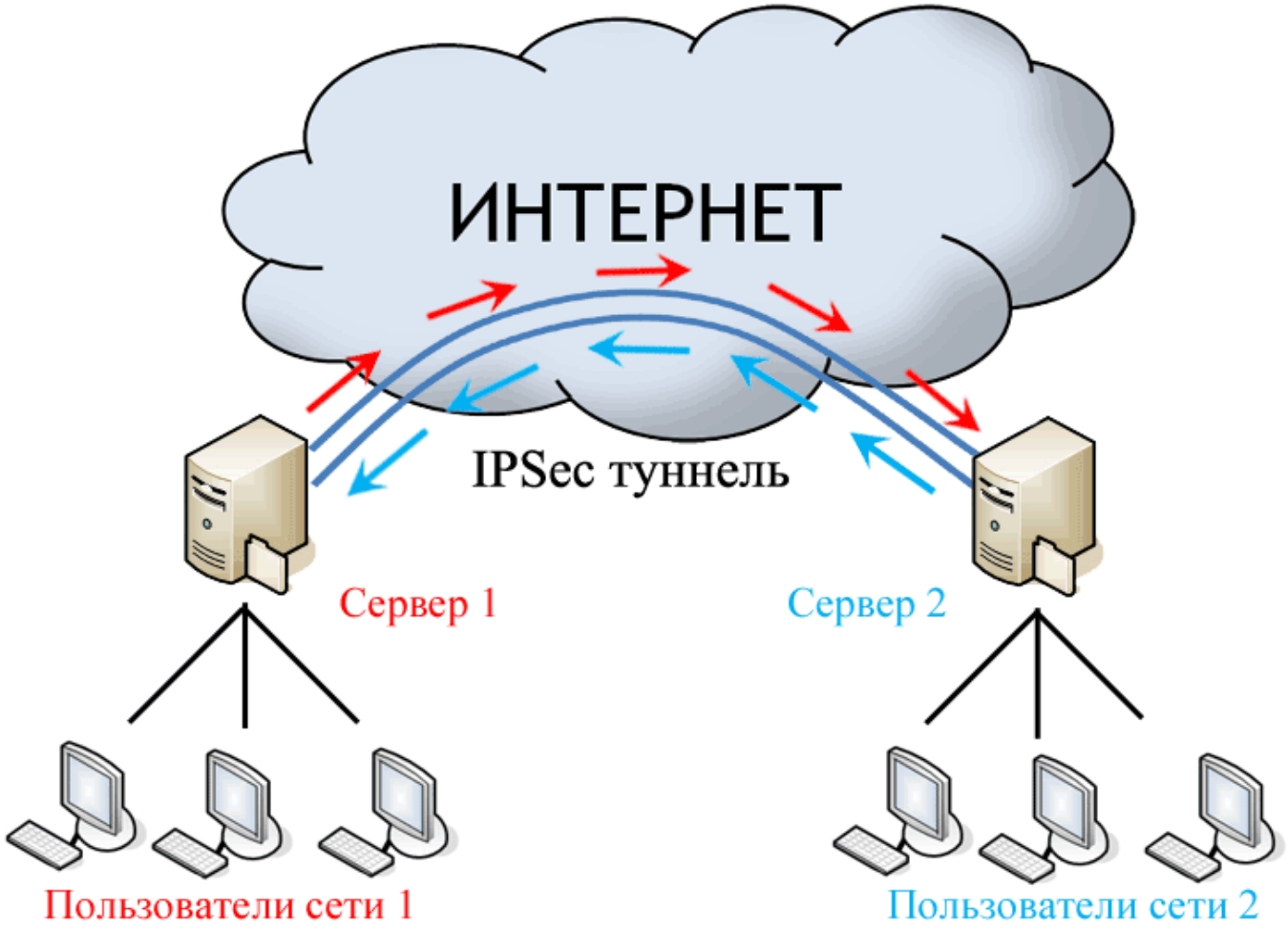
Настройка IPIP-туннеля.

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



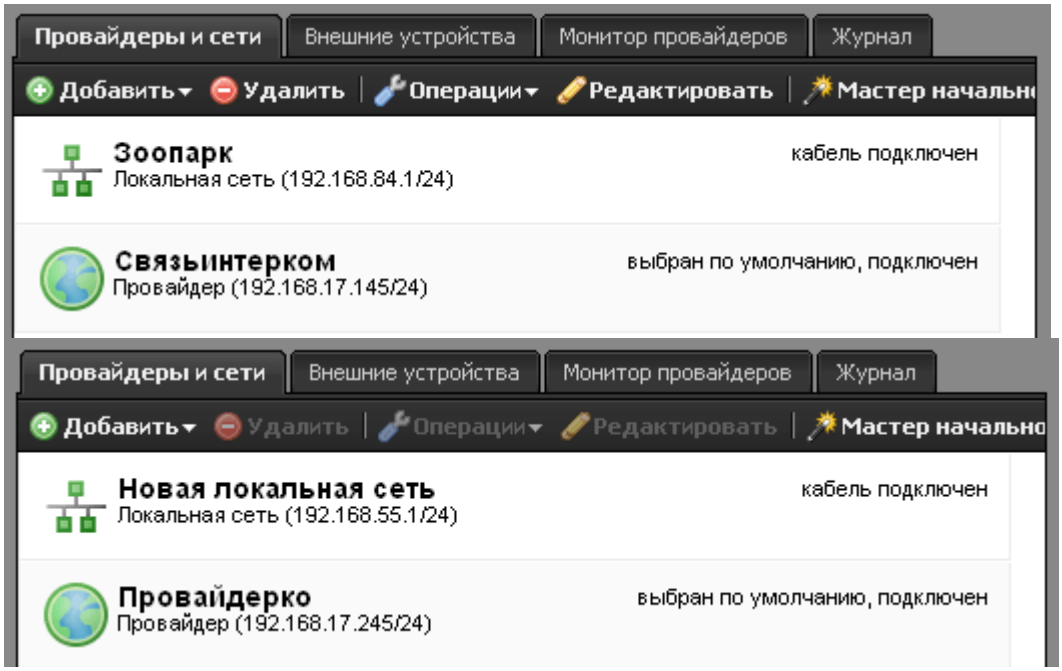
Для настройки IPIP или GRE-туннеля между двумя ИКС необходимо выполнить следующие действия:

1. Добавить новый туннель IPIP 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.

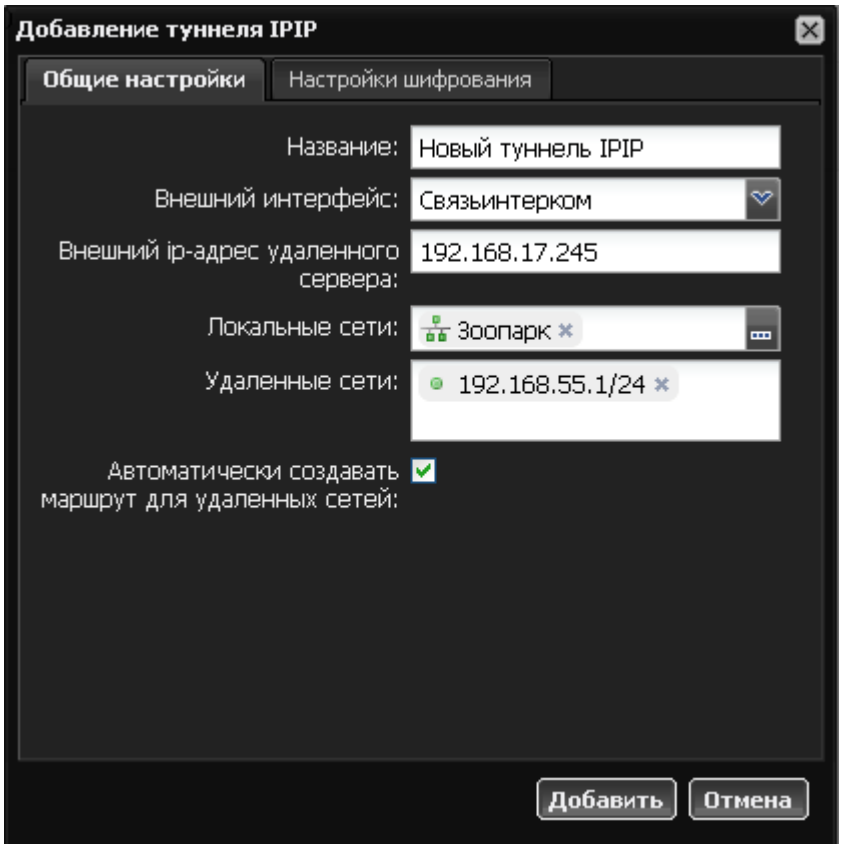
После чего все действия необходимо произвести на втором конце туннеля.

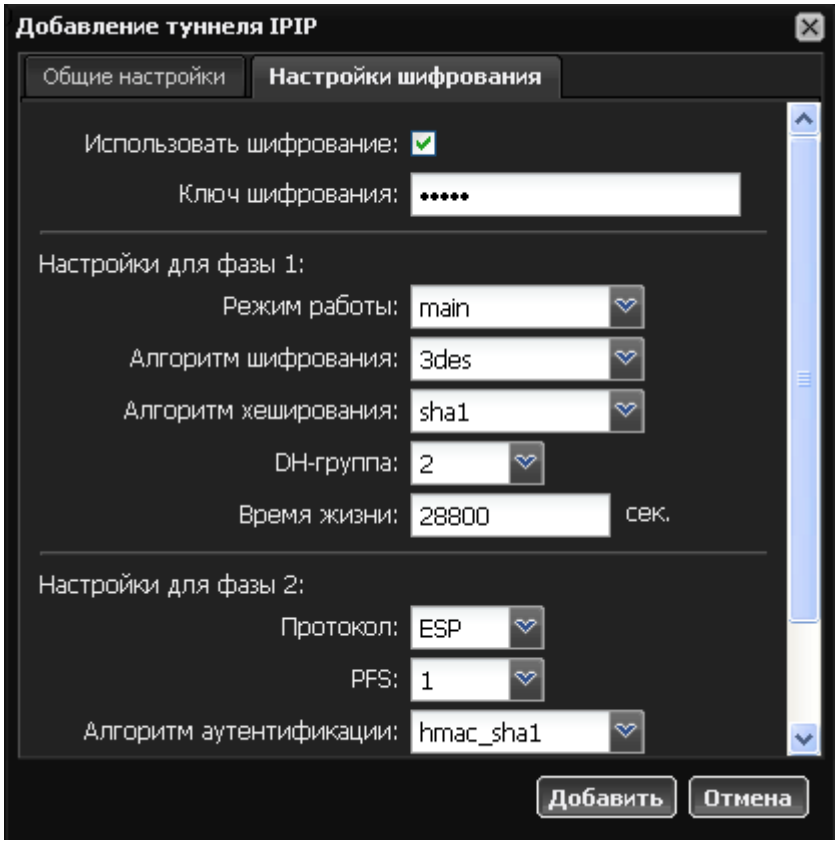
В нашем примере мы создадим туннель между двумя серверами.

	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



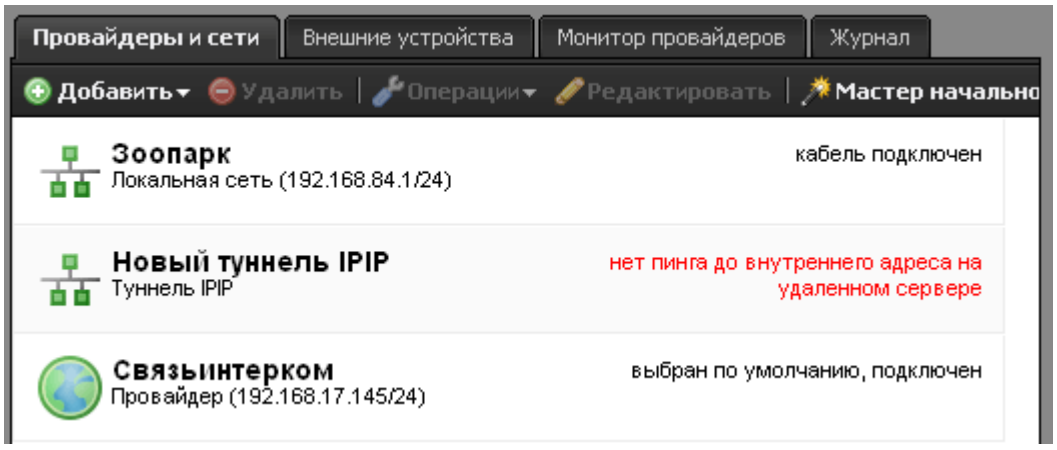
Сначала добавим новый IPIP-туннель в модуле «Провайдере и сети».





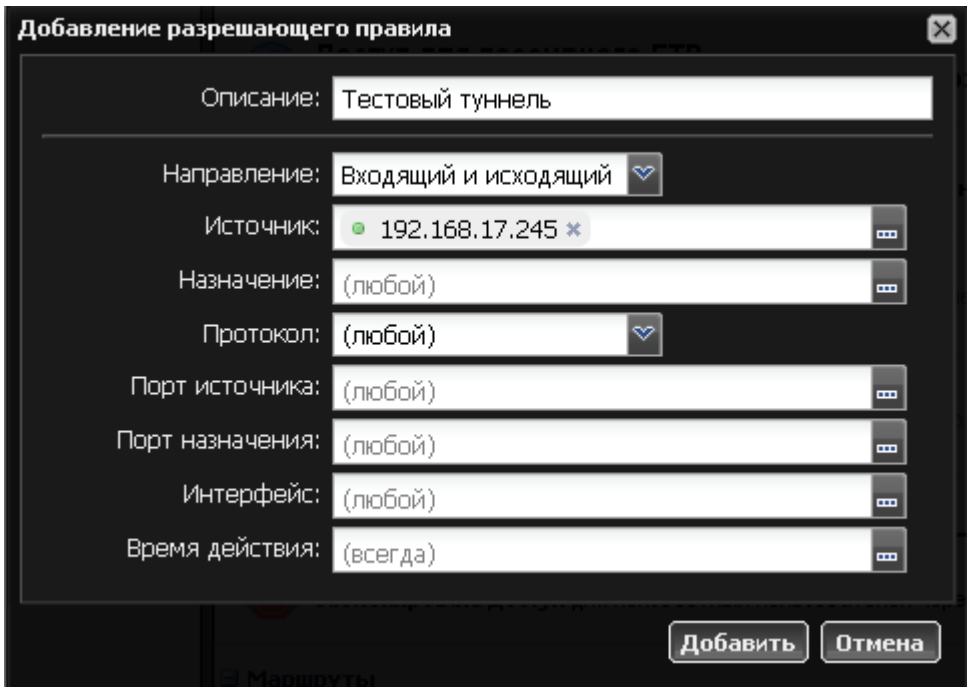
Выбираем в качестве исходящего интерфейса нашего провайдера, указываем внешний адрес Сервера 2, выбираем локальную сеть и прописываем в удаленной сети сеть Сервера 2. Чтобы пользователи автоматически могли получить доступ к хостам в локальной сети Сервера 2, устанавливаем флажок «Автоматически создавать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



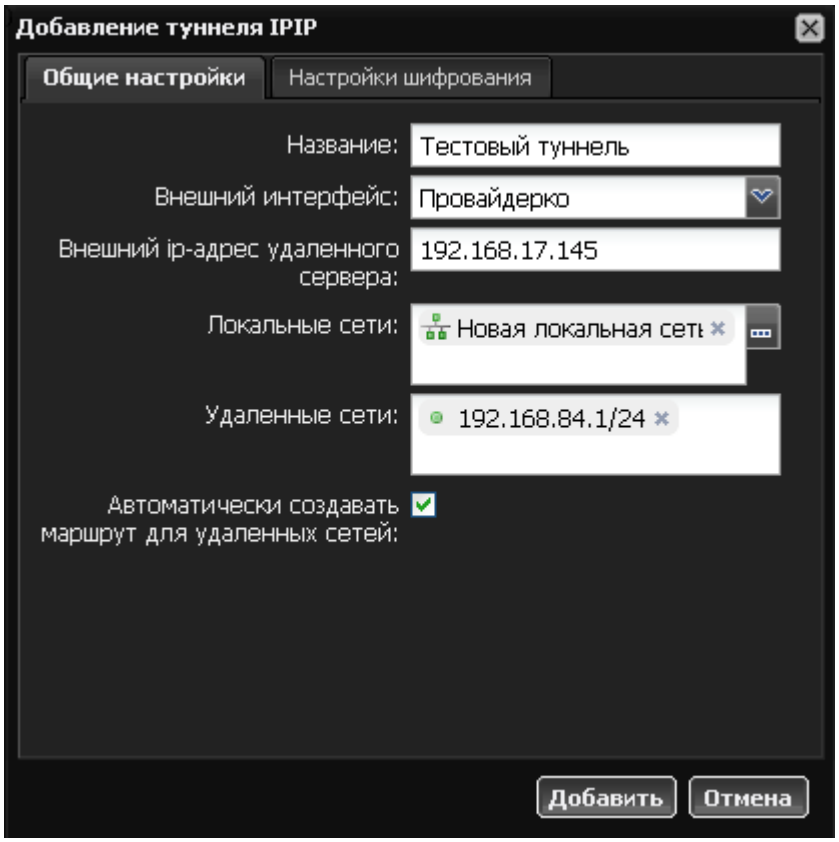
Красный статус «нет пинга до внутреннего адреса на удаленном сервере» сигнализирует о том, что туннель создан, но не установлен. Продолжаем настройку.

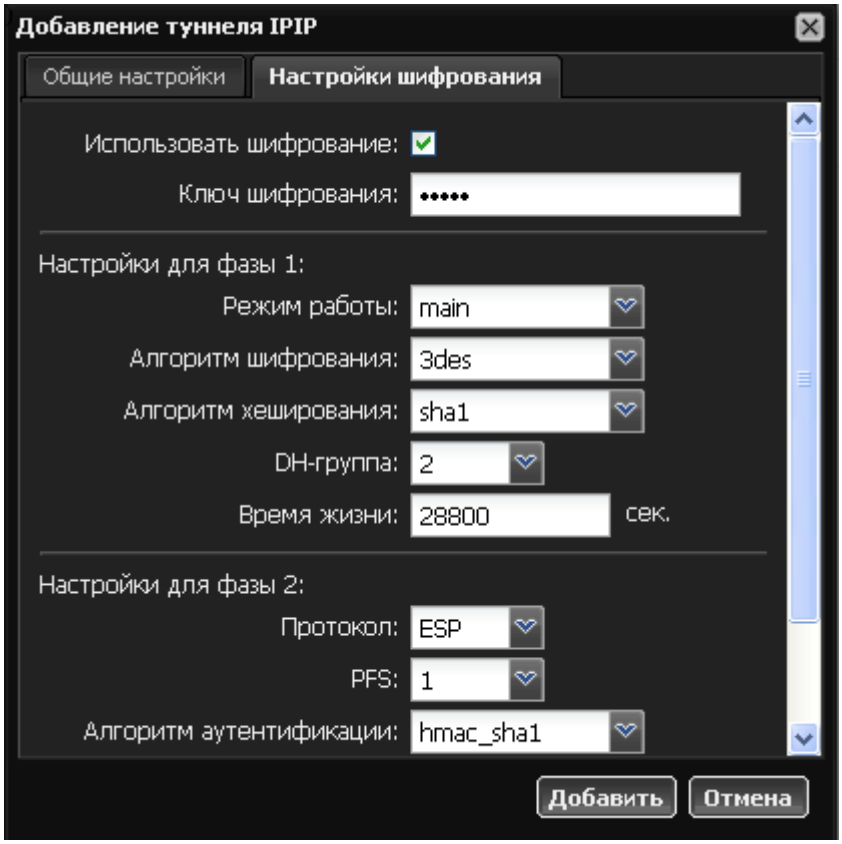
Чтобы разрешить Серверу 1 принимать пакеты через туннель от Сервера 2, необходимо создать разрешающее правило. Для этого нужно перейти в модуль «Межсетевой экран» и добавить новое разрешающее правило.

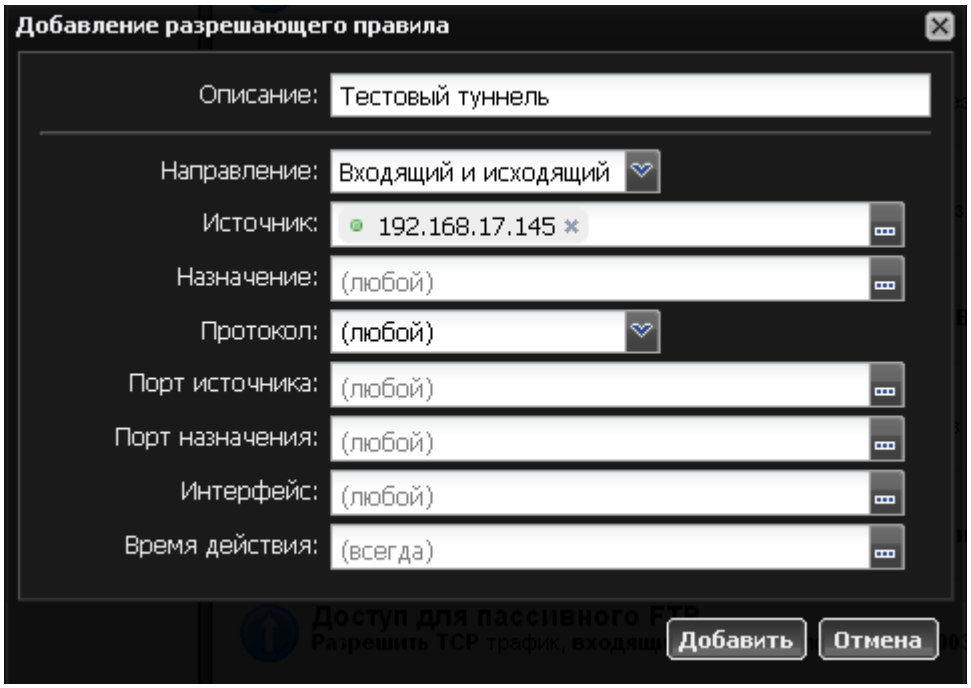


В правиле достаточно указать ip-адрес Сервера 2 в качестве источника. Остальные параметры указывать не обязательно. Также необходимо проверить, что в списке правил присутствует и включено правило по умолчанию «Доступ к серверу через GRE тоннели», разрешающее прохождение GRE-трафика.

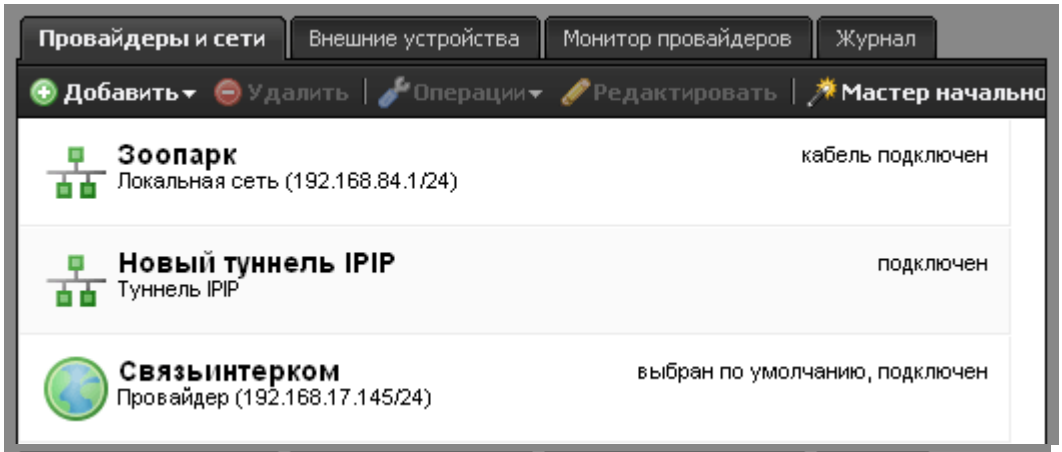
Теперь всю процедуру необходимо повторить на Сервере 2.

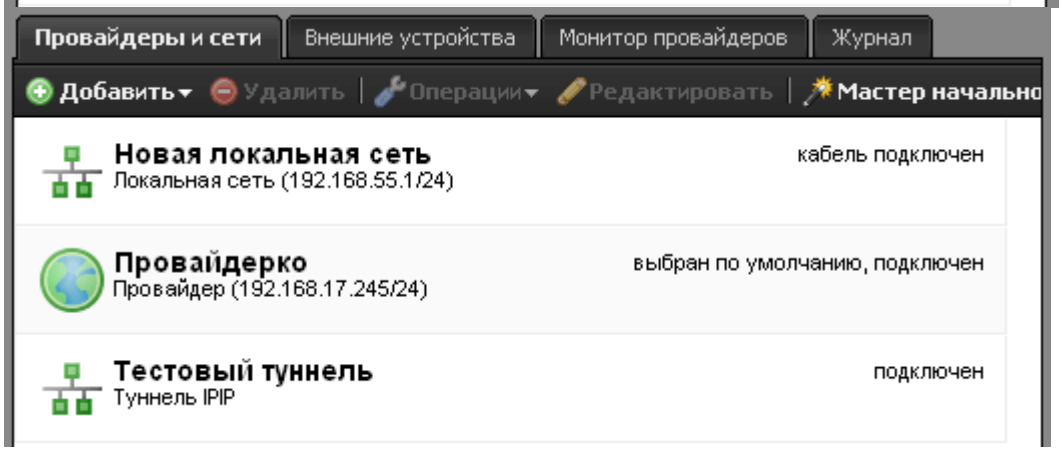




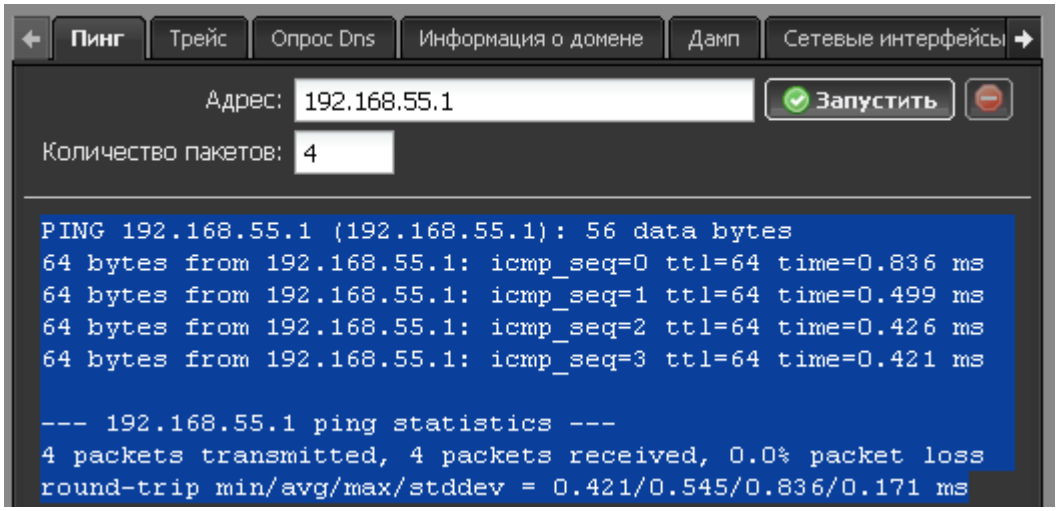


Теперь, если все настроено верно, в статусе созданного туннеля на каждом сервере должна появиться надпись «подключен».





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.