Туннели

Общие положения

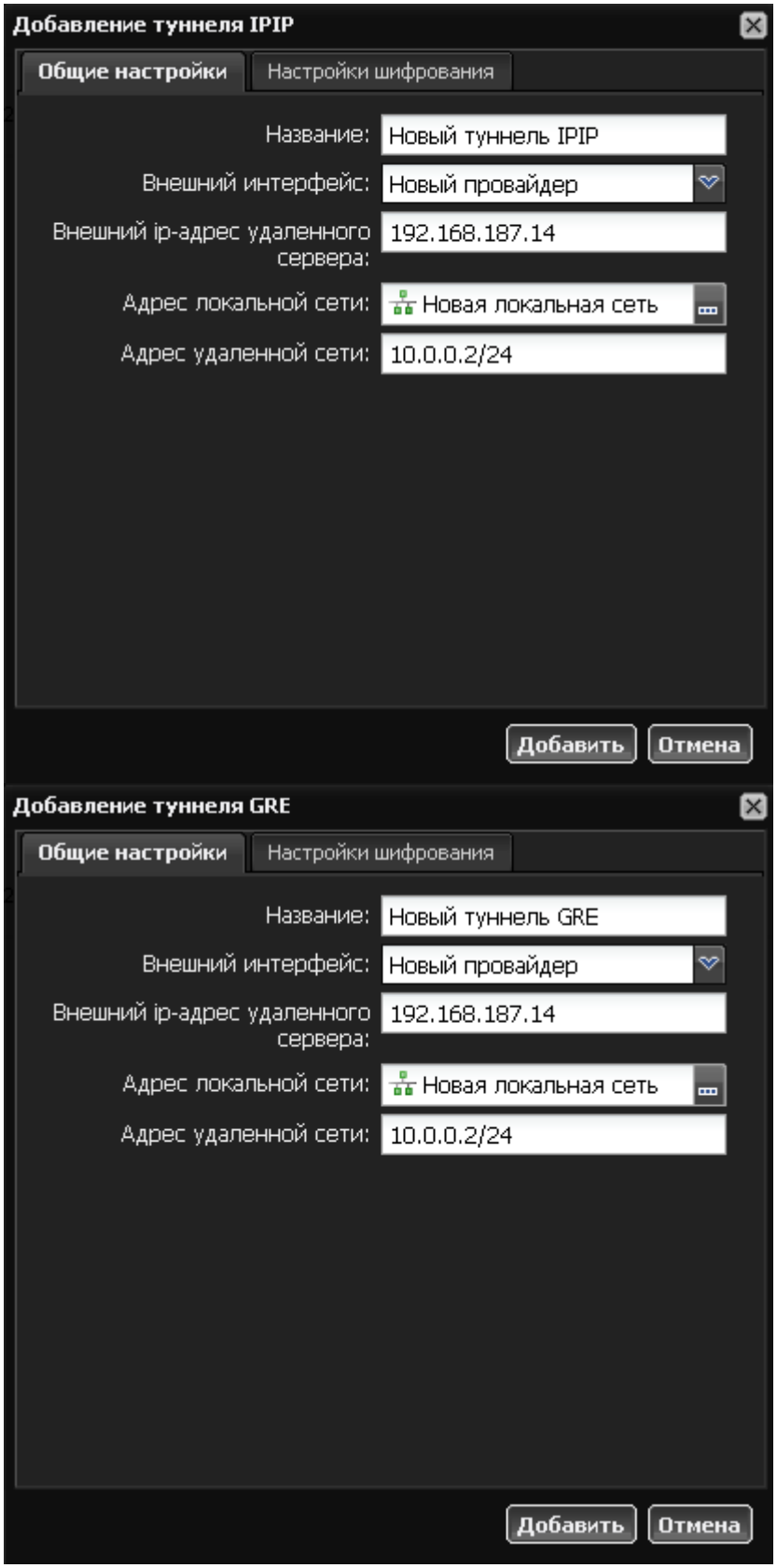
Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру. Статические туннели используются для объединения нескольких локальных сетей в одну: например при объединении нескольких удалённых офисов в одну локальную сеть таким образом, чтобы пользователи одной сети могли обращаться к ресурсам других. Туннели настраиваются на пограничных маршрутизаторах этих сетей и весь промежуточный трафик передаётся через интернет инкапсулированным в IP или GRE-пакеты.

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

Для обеспечения безопасности передачи данных в туннеле используется IPSec — набор протоколов, передаваемых по межсетевому протоколу IP, что позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

В ИКС вы можете настроить подключение между серверами статическим туннелем по IPIP или GRE протоколу.

Обычно выбор типа туннеля зависит от промежуточных провайдеров, которые по каким-либо причинам они могут блокировать траффик GRE или IPIP что приводит к невозможности использования какого-то одного типа туннеля. Принципиальной же разницы между этими типами туннелей нет.



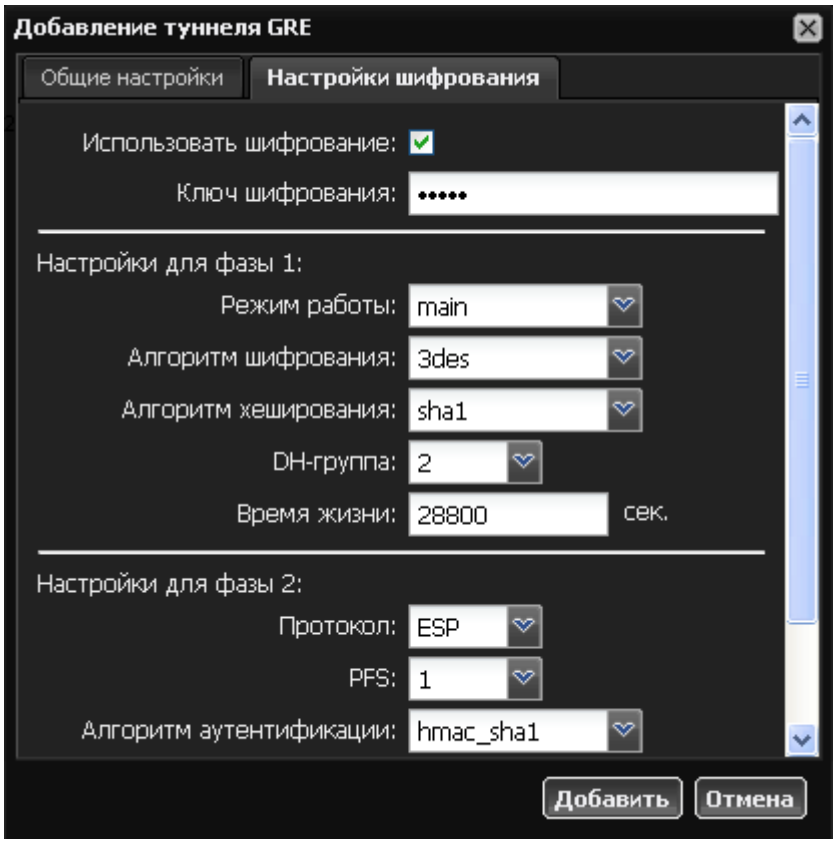
Настройки туннелей также не отличаются. Вам необходимо указать, на каком интерфейсе будет настроен данный туннель и прописать параметры маршрутизации: внешний адрес удаленного сервера, адрес локальной сети и адрес удаленной сети. Аналогичные настройки необходимо произвести на другом конце тоннеля.

Важно: для того, чтобы туннель работал корректно, необходимо, чтобы в межсетевом экране ИКС был разрешен GRE-трафик, а также разрешены входящие соединения с

ip-адреса удаленного сервера.

IPsec

IPsec (сокращение от IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.



Защита передачи данным по туннелям позволяет избежать многих проблем, связанных с утечкой информации и получения ложных данных. Вы можете защитить туннельный трафик, перейдя на вкладку «Шифрование» и установив флажок «Использовать шифрование». После этого вы можете произвести необходимые настройки параметров. **Внимание! Данную процедуру необходимо произвести на обоих концах туннеля, в противном случае передача данных работать не будет.**