

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 зашифрованного 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 IPsec или GRE протоколу.

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

Добавление туннеля IPsec

Общие настройкиНастройки шифрования

Название:

Новый туннель IPsec

Внешний интерфейс:

Новый провайдер

Внешний ip-адрес удаленного сервера:

192.168.187.14

Адрес локальной сети:

Новая локальная сеть

Адрес удаленной сети:

10.0.0.2/24

ДобавитьОтмена

Добавление туннеля GRE

Общие настройкиНастройки шифрования

Название:

Новый туннель GRE

Внешний интерфейс:

Новый провайдер

Внешний ip-адрес удаленного сервера:

192.168.187.14

Адрес локальной сети:

Новая локальная сеть

Адрес удаленной сети:

10.0.0.2/24

ДобавитьОтмена

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 туннеля.

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.

The screenshot shows a window titled "Добавление туннеля GRE" with a close button in the top right. It has two tabs: "Общие настройки" and "Настройки шифрования", with the latter being active. The "Использовать шифрование:" checkbox is checked. Below it is a "Ключ шифрования:" field with masked characters. The "Настройки для фазы 1:" section includes "Режим работы:" set to "main", "Алгоритм шифрования:" set to "3des", "Алгоритм хеширования:" set to "sha1", "DH-группа:" set to "2", and "Время жизни:" set to "28800" seconds. The "Настройки для фазы 2:" section includes "Протокол:" set to "ESP", "PFS:" set to "1", and "Алгоритм аутентификации:" set to "hmac_sha1". At the bottom are "Добавить" and "Отмена" buttons.

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.**

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

Permanent link:
<https://doc.a-real.ru/doku.php?id=en:%D1%82%D1%83%D0%BD%D0%BD%D0%B5%D0%BB%D0%B8>

Last update: 2020/01/27 16:28

