


Настройка VPN-подключения на роутерах Mikrotik если подсети клиента и офиса совпадают

 interface31.ru/tech_it/2020/10/nastroyka-vpn-podklyucheniya-na-routerah-mikrotik-esli-podseti-klienta-i-ofisa-sovpadayut.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка VPN-подключения на роутерах Mikrotik если подсети клиента и офиса совпадают

Для организации удаленного доступа сотрудников к офисной сети широко используется VPN, при этом крайне желательно сделать этот процесс для пользователя максимально простым и удобным. В идеале он должен только указать свой логин и пароль для подключения, все остальное, включая маршрутизацию, должно быть настроено автоматически. И это вполне достижимо, например с помощью технологии Proxy ARP, которая позволяет как-бы поместить клиента в сеть офиса на канальном уровне. Но как быть, если подсети клиента и офиса совпадают?



Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Описанная нами во вступлении ситуация не нова, чаще всего она встречается в небольших сетях, где вопросом сетевого планирования никто никогда не занимался. Как это обычно бывает: купили роутер, быстро его настроили и начали использовать, не озадачившись сменить стандартные 192.168.0.0/24 или 192.168.1.0/24 на что-либо иное. До определенной поры такая адресация не вызывает проблем и очень часто переходит "по наследству" в достаточно крупные сети.

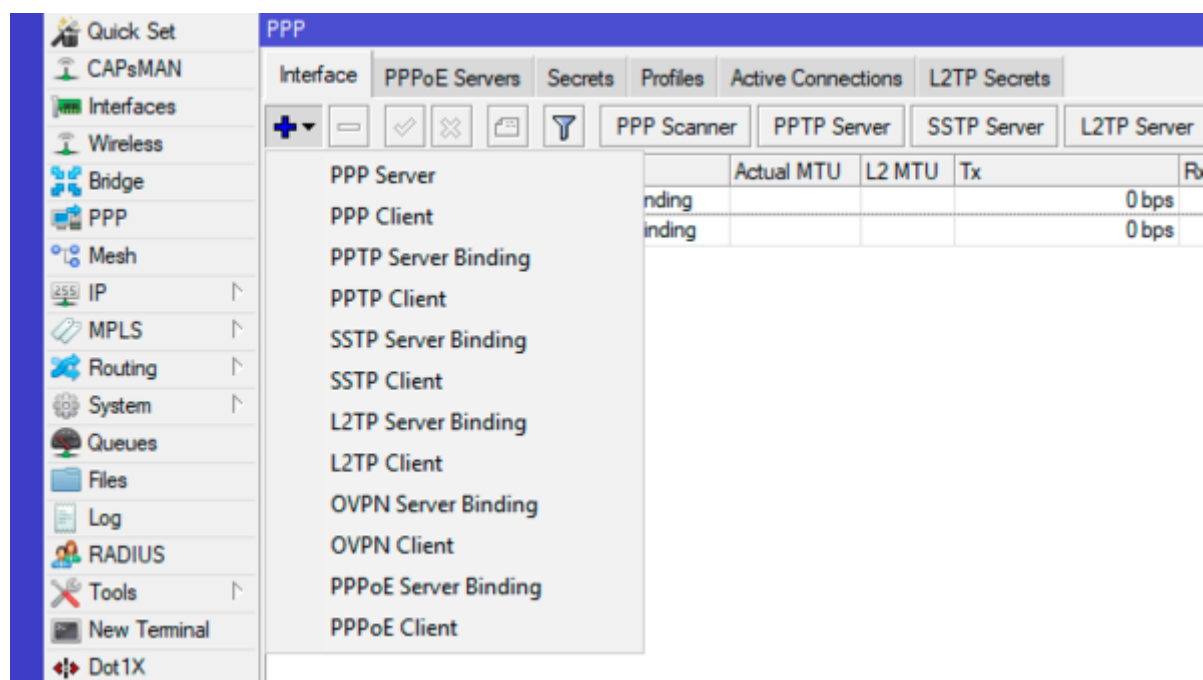
Но все меняется, если требуется обеспечить удаленный доступ сотрудников, у которых дома стоит такое же стандартное оборудование, с теми же 192.168.0.0/24 или 192.168.1.0/24. Если говорить о том, как правильно, то правильно будет сменить адресацию офисной сети, но это не всегда возможно и может быть сопряжено со

значительными сложностями. Особенно в текущей ситуации, когда по эпидемиологическим причинам удаленный доступ может потребоваться буквально здесь и сейчас, без времени на преобразования.

Как быть? Нам снова на помощь придет оборудование Mikrotik и широкие возможности RouterOS. При этом наша задача - сохранить удобство работы пользователя. Будем считать что у вас уже настроен VPN-сервер с использованием ProxyARP, как это описано в нашей статье: [Настройка Proxy ARP для VPN-подключений на роутерах Mikrotik](#). Все хорошо работало, но ровно до тех пор, пока не выяснилось, что часть сотрудников имеют дома подсеть, совпадающую с подсетью офиса.

Чтобы решить данную проблему мы будем использовать **netmap** - одну из разновидностей сетевой трансляции адресов (NAT), которая позволяет преобразовывать адреса одной подсети в другую один к одному. Таким образом мы можем отдавать клиенту некую "виртуальную" подсеть, адреса которой затем будут преобразоваться в реальные адреса офисной сети средствами RouterOS.

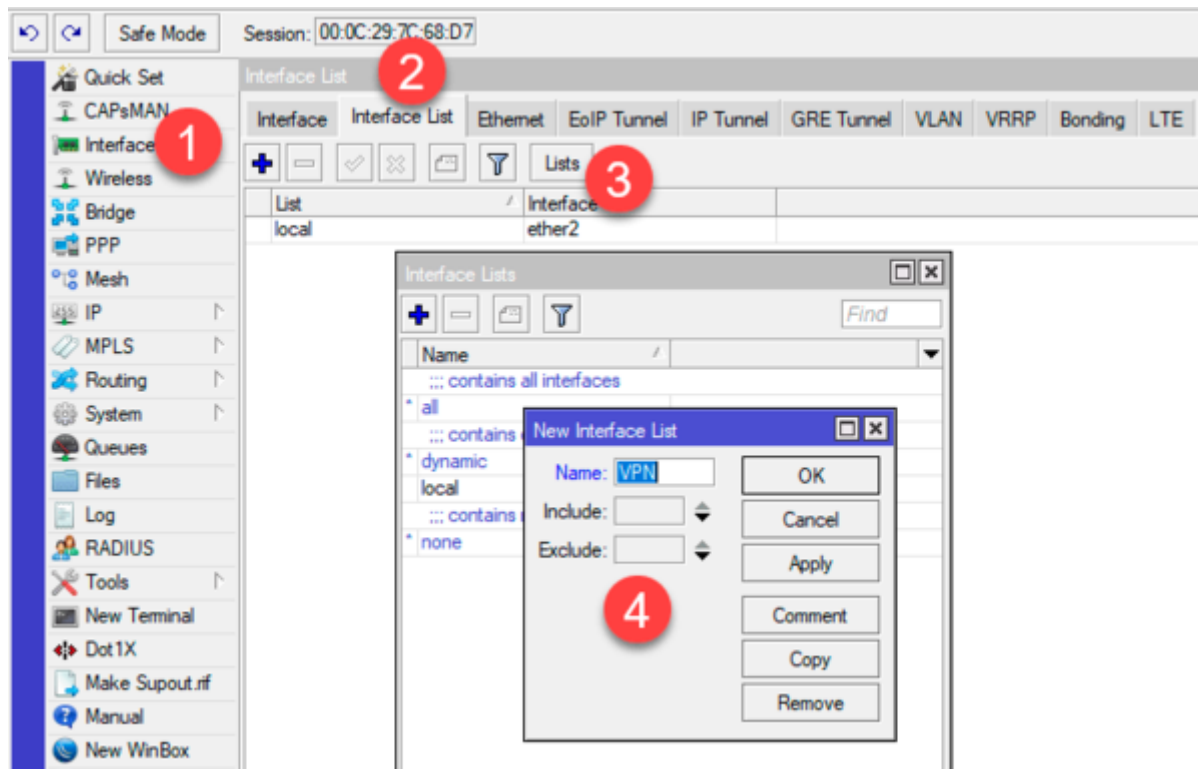
Прежде всего нам потребуются некоторые дополнительные действия. Как правило для клиентов удаленного доступа используется динамическое создание интерфейсов, это вполне оправдано, но в нашем случае для каждого из них потребуется выполнить привязку интерфейса. Для этого перейдем в **PPP - Interface** и создадим новую привязку интерфейса выбрав в выпадающем списке один из пунктов **Server Binding**, в зависимости от типа подключения, в нашем случае это **L2TP Server Binding**.



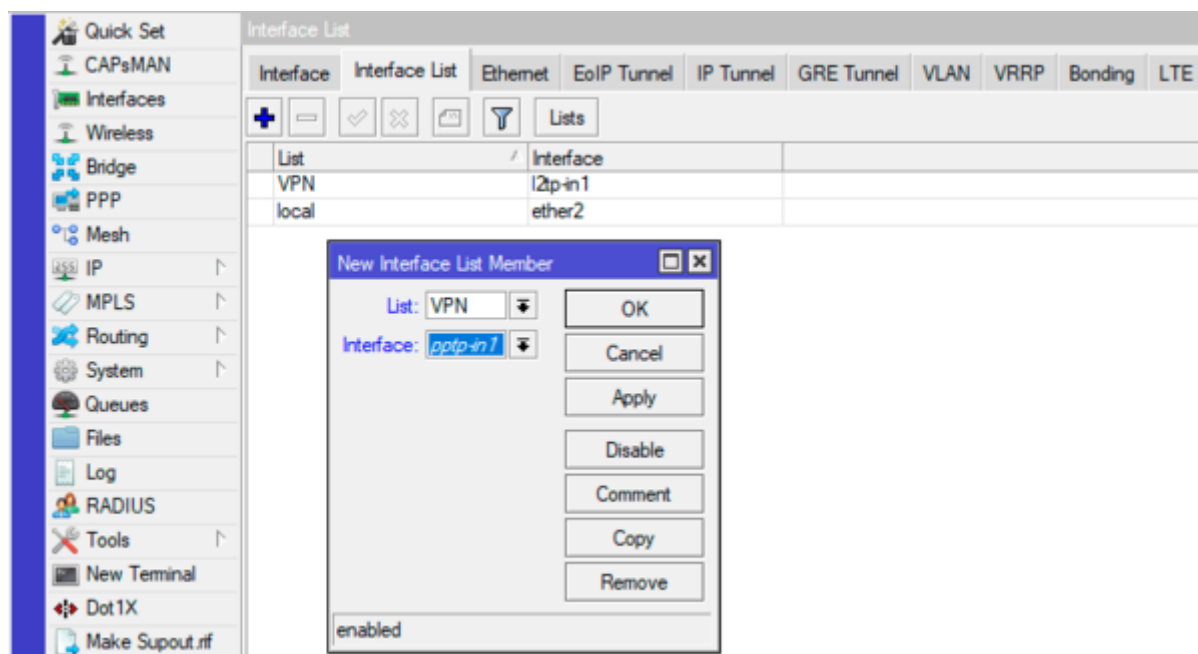
В открывшемся окне заполняем поля **Name** и **User**. Первое можно оставить и без изменения, оно ни на что не влияет, кроме удобства восприятия, но согласитесь, что запись **l2tp-ivanov** более информативна, нежели **l2tp-in1**. В поле **User** укажите

логин того пользователя, к которому будет производиться привязка. Повторите это действие для всех пользователей VPN-сервера.

После чего создадим новый список интерфейсов и поместим в него все привязки. Откройте **Interfaces - Interface List - Lists** и создайте новый список, назовем его VPN.

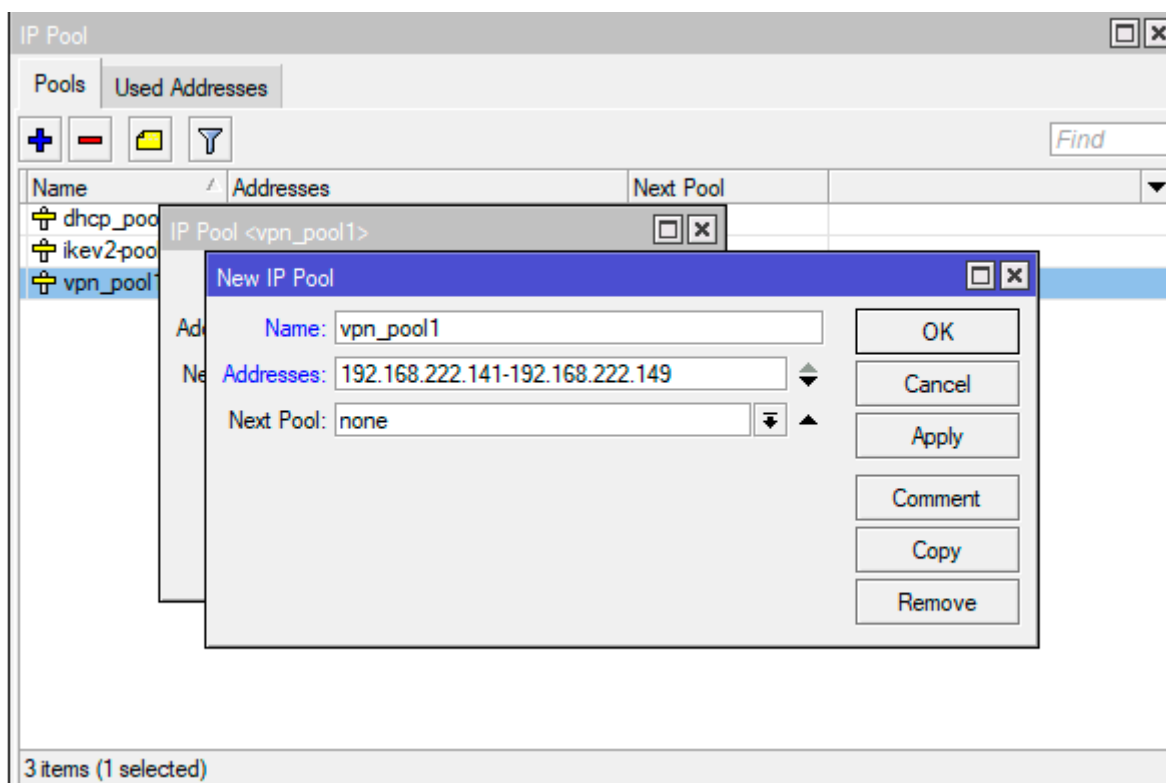


После чего добавим все привязанные интерфейсы в этот список.

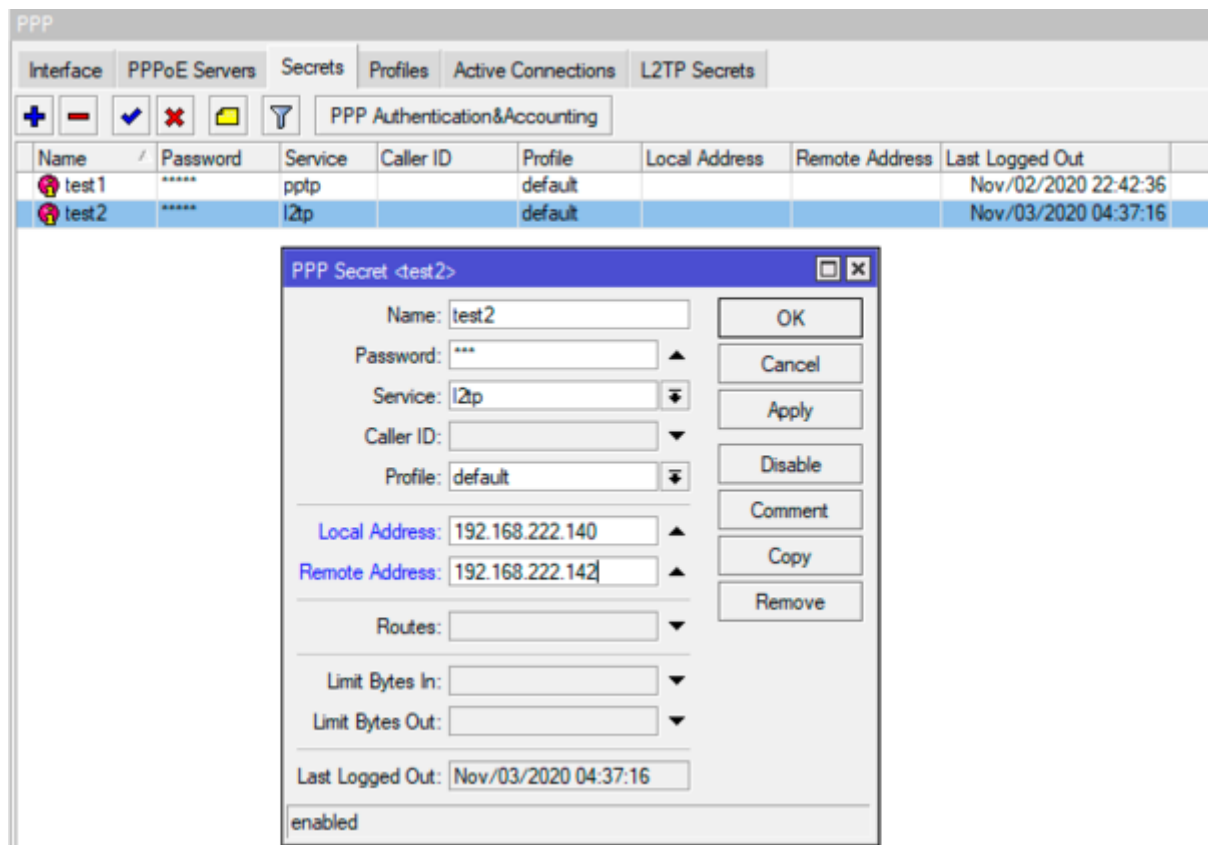


Теперь можно заняться изменением адресации. В нашем примере сеть офиса - **192.168.111.0/24**, будем считать, что она пересекается с клиентскими сетями и поэтому для VPN-подключений мы будем отдавать виртуальную сеть

192.168.222.0/24. Перейдем в **IP - IP Pool** и изменим в пуле адресов, выдаваемом клиентам сеть с 111-й, на 222-ю. Вы можете как изменить существующий пул, так и создать новый.

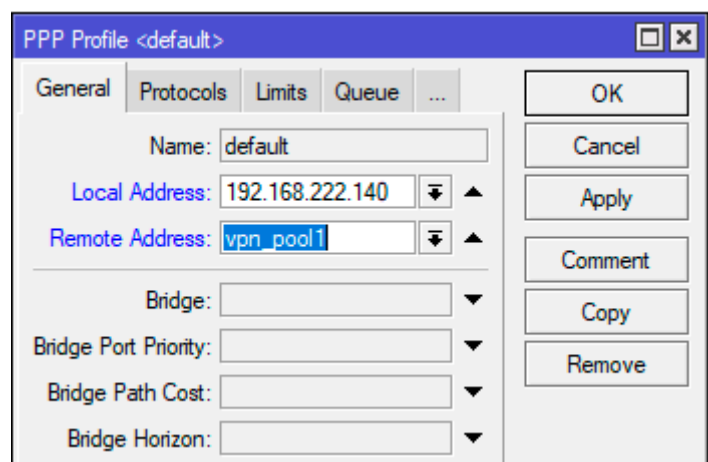


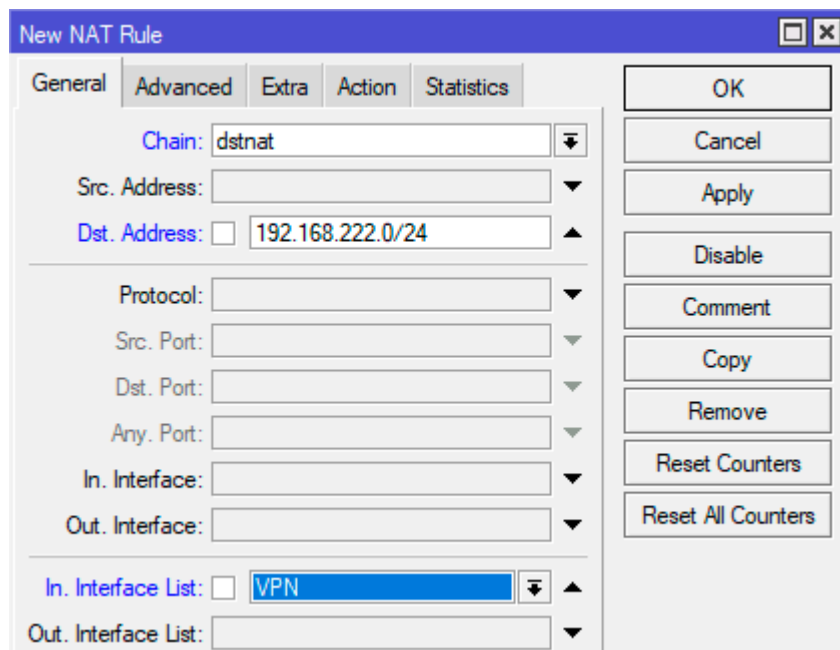
Если же адреса клиентов заданы непосредственно в настройках их учетных записей, то переходим в **PPP - Secrets** и исправляем адреса для каждой учетной записи клиента (при этом может быть задан только один - **Remote Address**, в этом случае **Local Address** будет взят из **профиля**).



Потом откроем **PPP - Profiles** и открыв профиль, указанный для клиентов VPN-сервера, исправим в нем собственно адрес сервера - **Local Address**, также следует убедиться, что указанный пул адресов в **Remote Address** соответствует нужной подсети (в нашем случае 222-й).

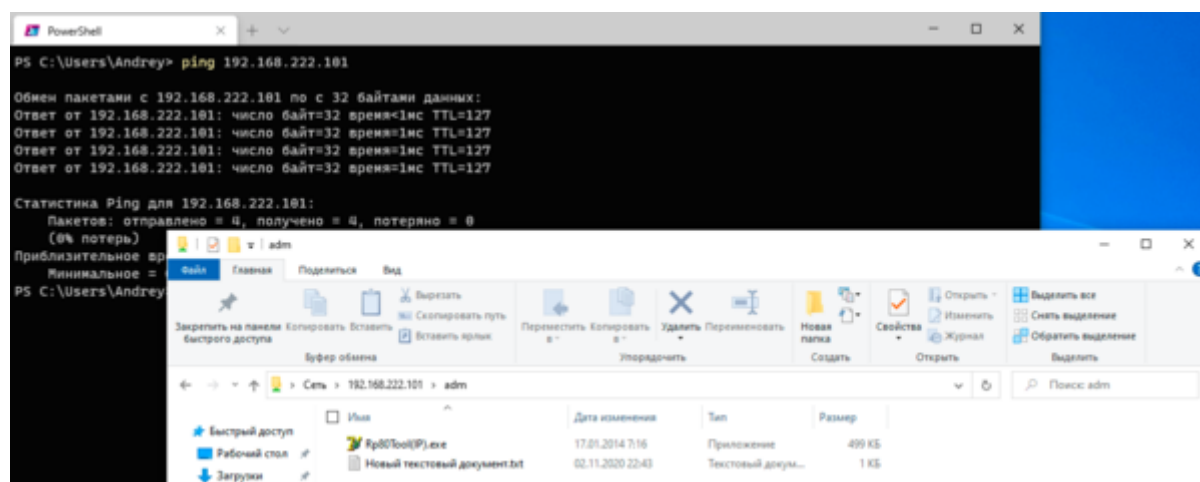
Если теперь мы выполним переподключение удаленного клиента, то он получит адрес из 222-й подсети, но доступа в сеть офиса у него не будет, так как мы еще не выполнили отображение этой сети, на локальную сеть офиса. Для этого перейдем в **IP - Firewall - NAT** и создадим новое правило. На закладке **General** укажем: **Chain - dstnat**, **Dst. Address - 192.168.222.0/24**, **In Interface List - VPN**, эти условия говорят, что данное правило будет применяться в цепочке **dstnat (PREROUTING)** к пакетам, пришедшим из привязанных интерфейсов списка **VPN** с адресом назначения в сети **192.168.222.0/24**.





На закладке **Action** указываем действие **Action - netmap** и в поле **To Addresses** - диапазон адресов локальной сети - **192.168.111.0/24**, таким образом теперь в каждом пришедшем из VPN-пакете адрес назначения будет прозрачно заменен на соответствующий ему адрес локальной сети. Т.е. 192.168.222.101 -> 192.168.111.101, 192.168.222.202 -> 192.168.111.202 и т.д.

Теперь можем попробовать на клиенте подключиться к адресу в нашей виртуальной сети, как видим все работает, клиент попал на требуемый узел сети офиса, только уже по новому адресу.



Таким образом мы достаточно несложно решили серьезную проблему - организацию прозрачного удаленного доступа в сеть офиса с пересекающимся диапазоном адресов.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет

лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.
