Лабораторная работа №4. Конфигурация L2TP IPSEC VN на Mikrotik.

В настоящей работе будет указана возможность конфигурации технологии IPSEC поверх сконфигурированного в прошлых лабораторных работах L2TP VPN.

IPSEC – это целый набор протоколов, обеспечивающих защиту данных IP через сеть интернет. На данный момент это одна из самых безопасных реализаций VPN, но ложкой дегтя является сложность его конфигурации. Некоторые модели RouterBOARD (коммерческое наименование плат Mikrotik) имеют встроенные аппаратные средства, микрочипы, для разгрузки центрального процессора от алгоритмов шифрования AES. Ознакомиться более подробно со списком оборудования, поддерживающего аппаратную разгрузку можно на сайте mikrotik.com.

В нижеизложенной инструкции будет продемонстрировано конфигурирование классического IPSEC, а не IKEv2. В работы будет рассмотрено два режима настройки L2TP\IPSec в транспортном режиме на маршрутизаторе Mikrotik. По сложившейся практике, настройки предпочтительно делать именно в транспортном режиме, т.к. удобнее прописать маршруты в локальные сети через адреса в туннелях вместо создания NAT правил. Вдобавок про NAT отметим, что IPSEC может некорректно работать с классической трансляцией сетевых адресов. Выходом из ситуации является использование NAT-T. Взяв во внимание вышеизложенную информацию приступим.

1. **Схема сети (аналогично лабораторной работе №3)**

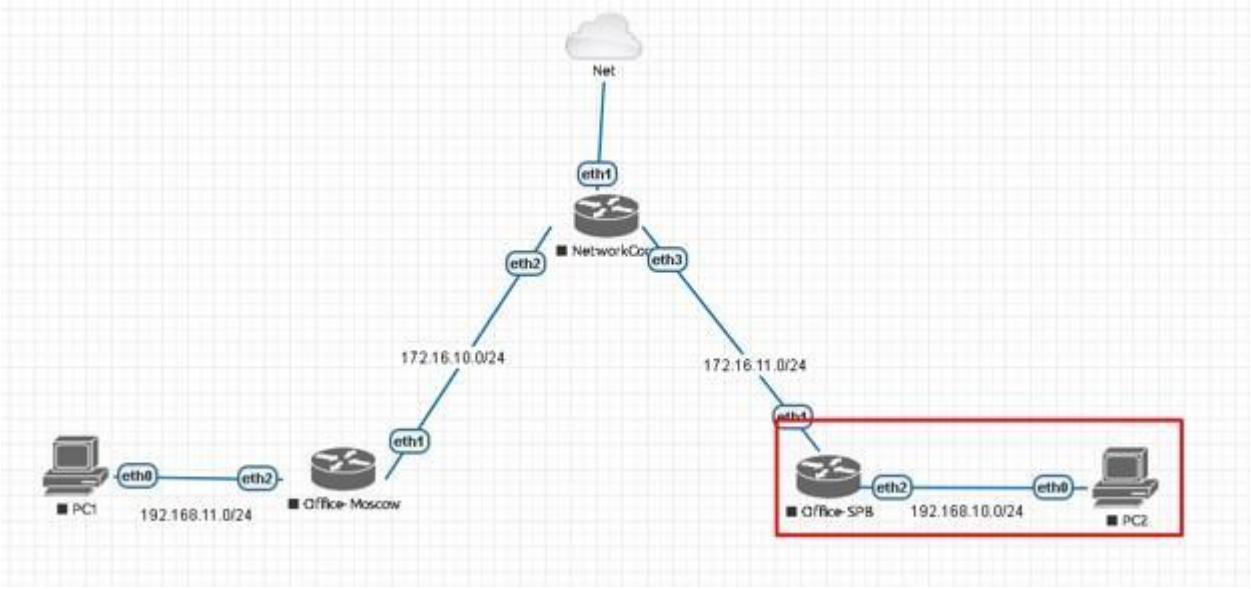

Рисунок 1 – Топология моделируемой сети связи

Используем лабораторный стенд с Mikrotik CHR версии 6.46.2. Вводные данные:

- Office-SPB сервер;
- Office-Moscow клиент;
- NetworkCore выполняет роль провайдера, он будет заниматься обычной маршрутизацией;
- Office-Moscow ether1 смотрит в интернет 172.16.10.2/24;
- Office-SPB ether1 смотрит в интернет 172.16.11.2/24;
- Office-Moscow имеет bridge “General-Bridge” в локальной сети 192.168.11.1/24;
- Office-SPB имеет bridge “General-Bridge” в локальной сети 192.168.10.1/24;
- IP ПК в локальной сети Office-Moscow 192.168.11.2;
- IP ПК в локальной сети Office-SPB 192.168.10.2;
- Адресация в VPN сети 172.16.25.0/24;
- Активный L2TP туннель между офисами (лабораторная работа №3).

Схема адресации приведена в качестве примера и может быть изменена.

2. «Простая» конфигурация IPsec

Предполагает быстрое развертывание на сервере и клиенте. Такая конфигурация подходит для инсталляций, когда планируется подключение множества мобильных устройств или устройств находящихся за NAT-ом. На «московском» роутере проверим состояние клиентского подключения. Переходим PPP – Interface – SPB-Office – Status.

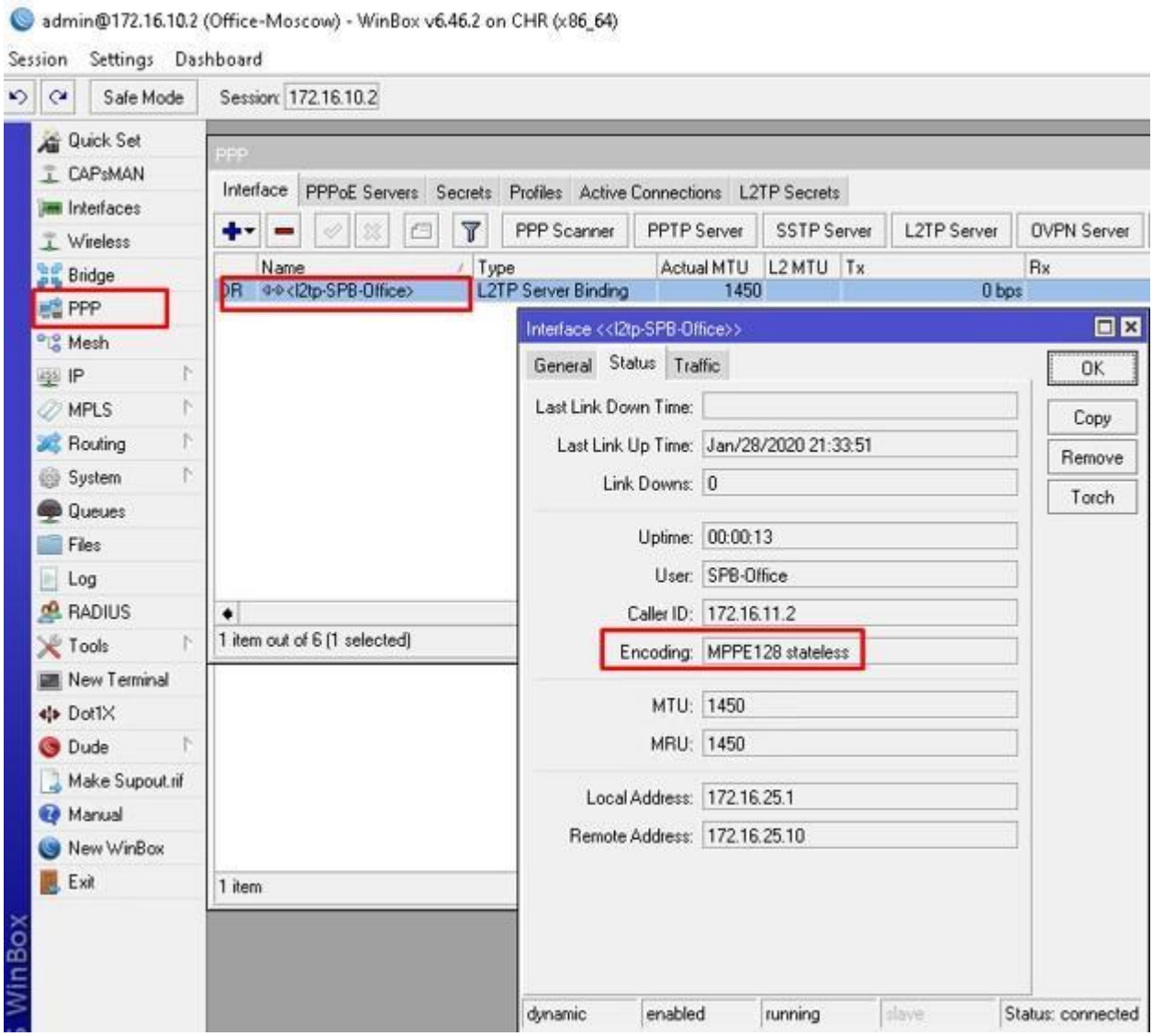

Рисунок 2 – Проверка соединения L2TP

Статус соединения должен быть в состоянии «connected». В строке Encoding видим стандартное шифрование протокола L2TP. Открываем свойства сервера L2TP. Ставим required на параметре Use IPsec и указываем пароль.

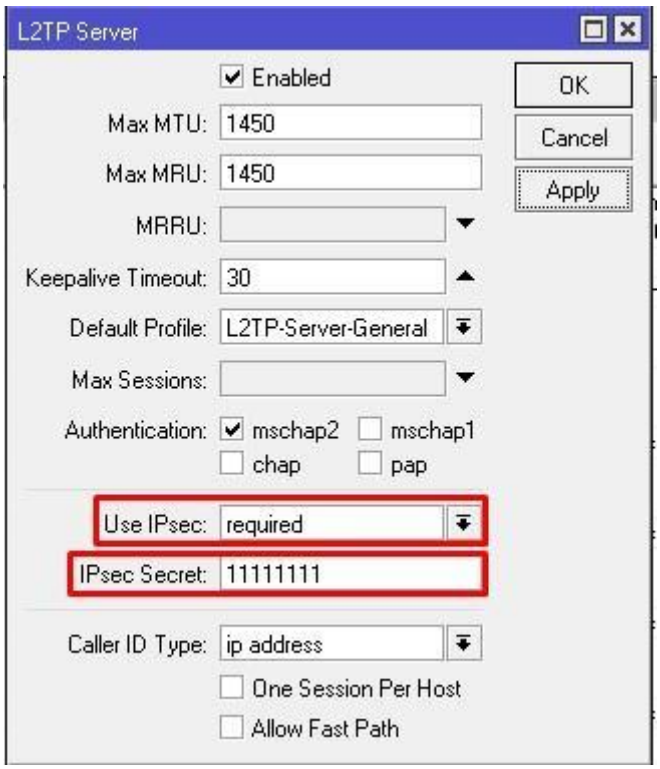

Рисунок 3 – Конфигурация IPSEC

Сохраняем. Клиентское соединение пропадает, т.к. теперь требуется согласование протокола IPSEC. При этом отображается соответствующее сообщение в логах сервера. Оно говорит о том, что подключение было отброшено.

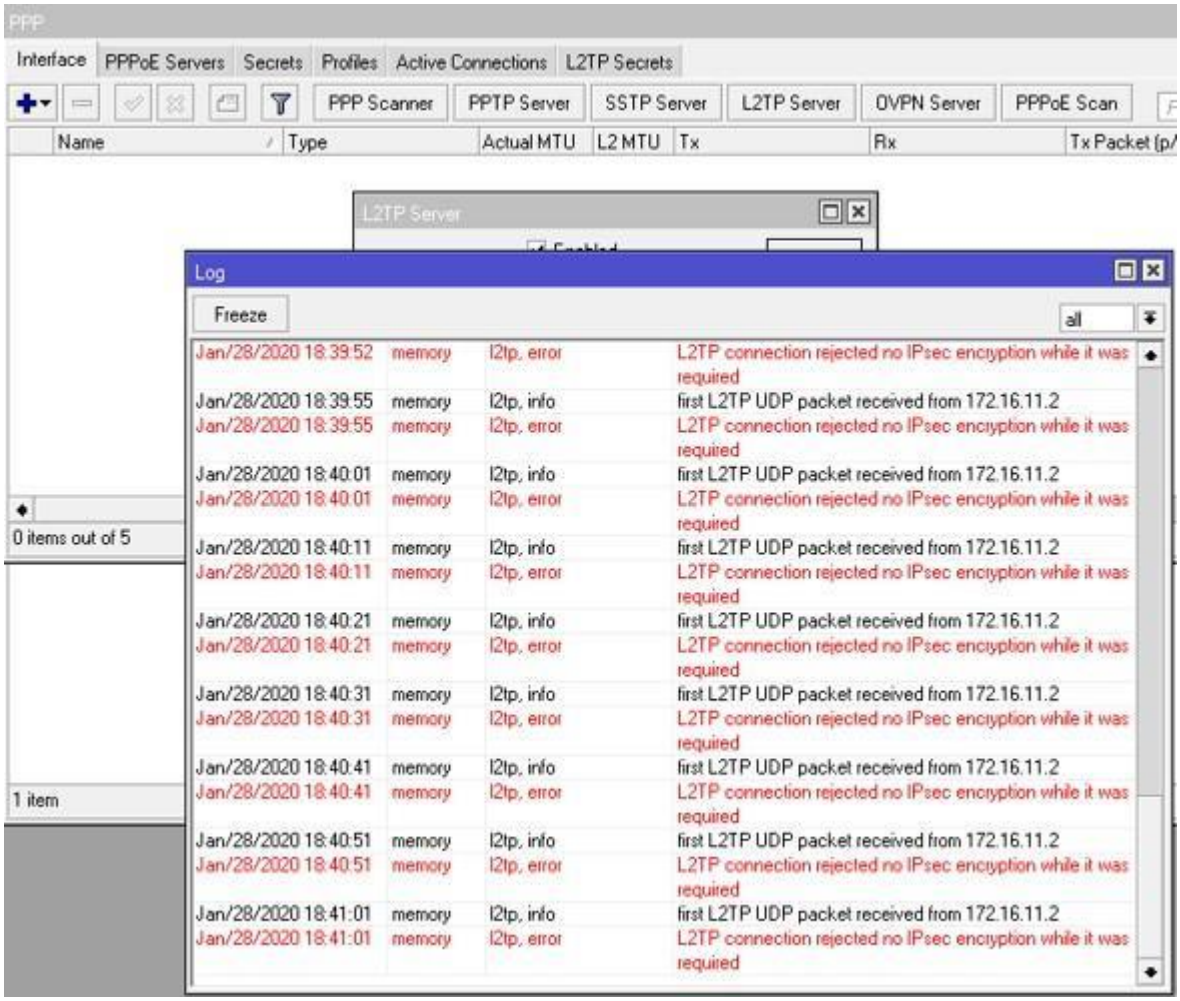

Рисунок 4 – Журнал «сервера» L2TP

При этом если установить значение поля «Use IPsec» в состояние «yes», то все желающие подключиться без использования IPSEC – подключатся.

Подключаемся к клиентскому Mikrotik, открываем PPP – Interface – выбираем интерфейс «to-MSC» и открываем вкладку Dial Out. Ставим галочку на UseIPsec и задаем пароль, установленный на сервере.

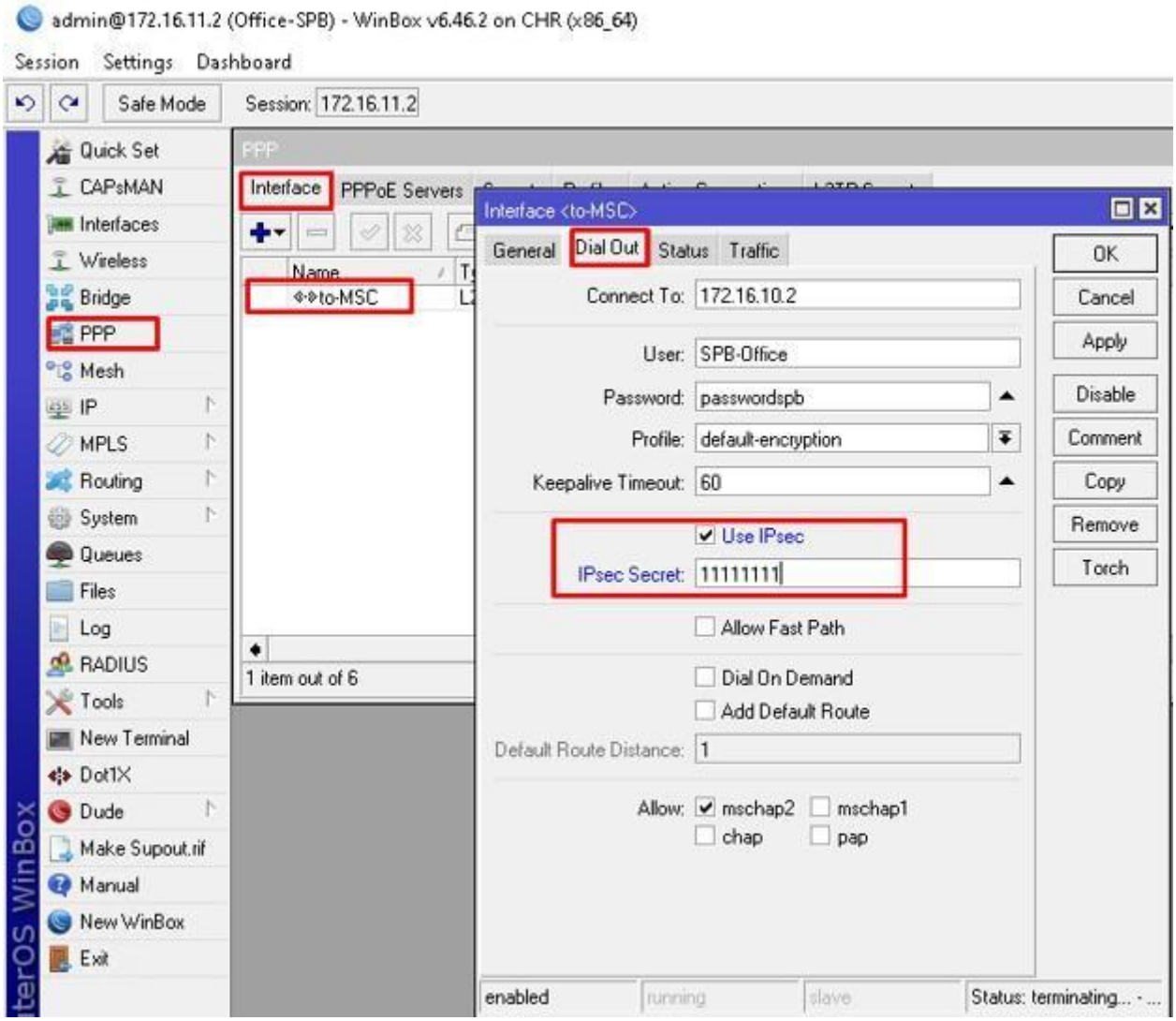

Рисунок 5 – Конфигурация клиента L2TP

После нажатия кнопки Apply проверим состояние подключения на вкладке Status.

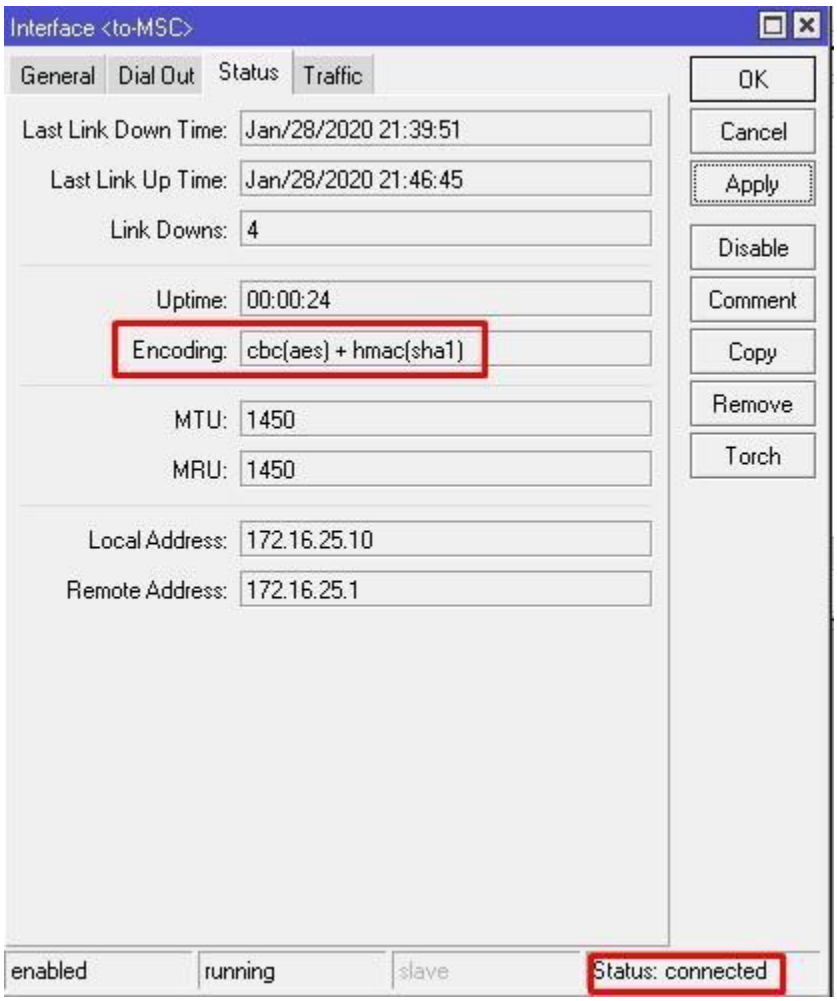

Рисунок 6 – Проверка соединения L2TP

Строка Encoding изменилась на более внушительное значение, что символизирует об успешном согласовании.

3. Site to site VPN

Все настройки находятся в IP – IPSEC. Данный метод предназначен для развёртывания VPN между удаленными площадками. Обязательным условием является наличие статических публичных адресов для обоих участников туннеля. Параметры идентичны, за исключением маленьких деталей. Отлично подходит для голосового трафика, т.к. все данные будут инкапсулированы в UDP. Первым шагом создаем одинаковый профиль на обоих устройствах.

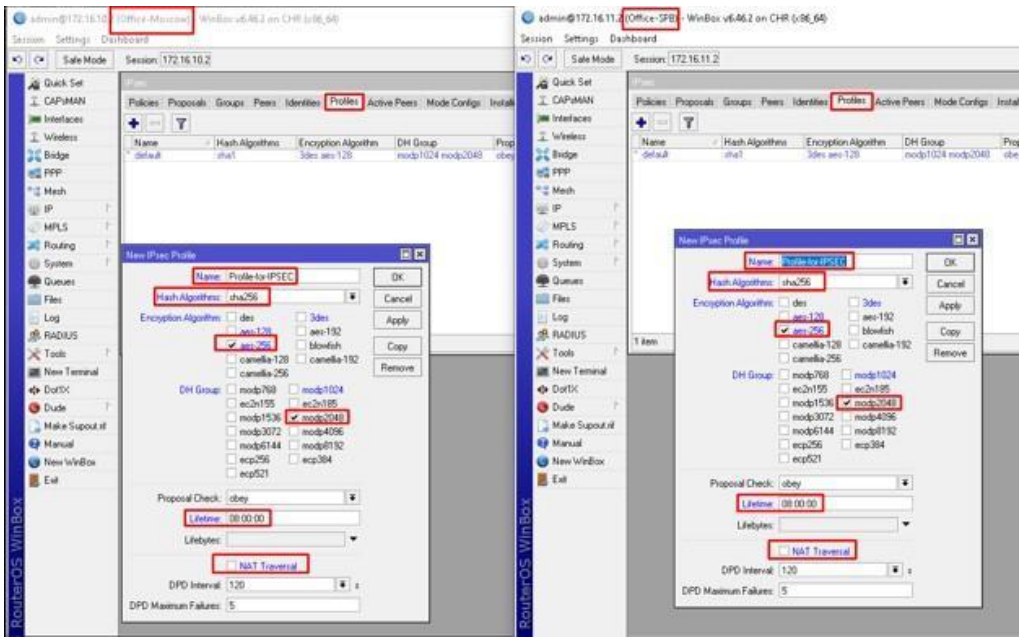

Рисунок 7 – Конфигурация профиля IPSEC (IP-IPsec-Profiles)

Далее создаем предложения.

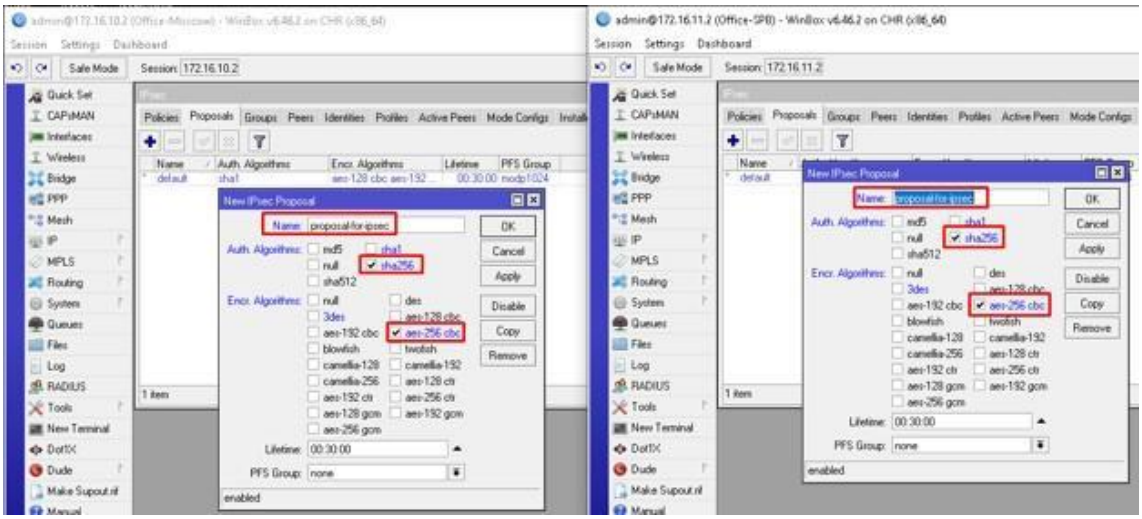

Рисунок 8 – Конфигурация предложений IPsec (IP-IPsec-Proposal)

Далее нужно создать пиров. Направляем их друг на друга и указываем ранее созданные профили. Пишем в поле «Local Address» тот адрес роутера, с которого инициируем соединение. Это особенно актуально если имеется несколько адресов или нужно инициировать соединение с определенного.

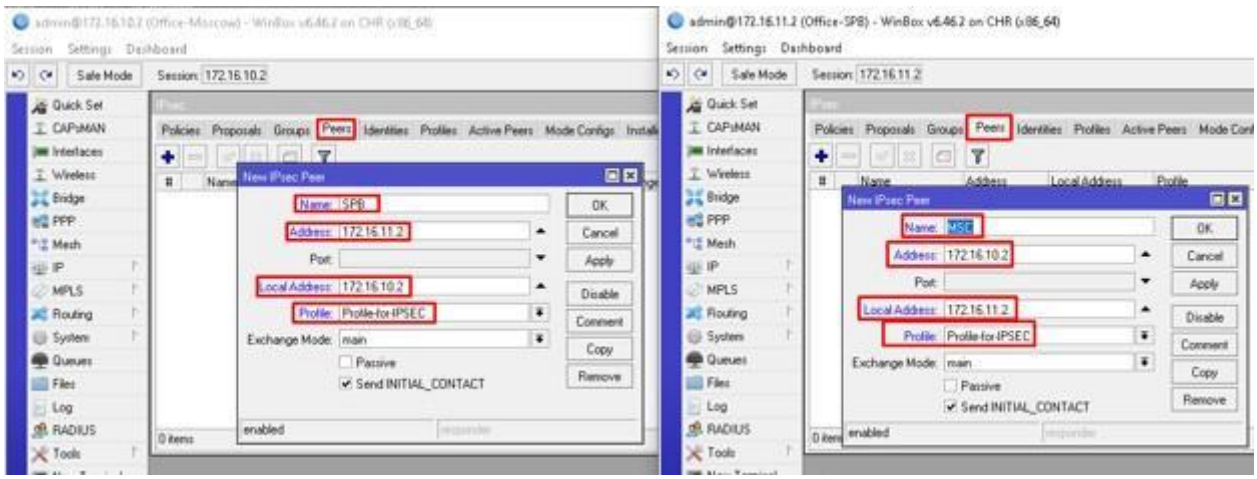

Рисунок 9 – Конфигурация Peer соединений

Далее создаем группы.

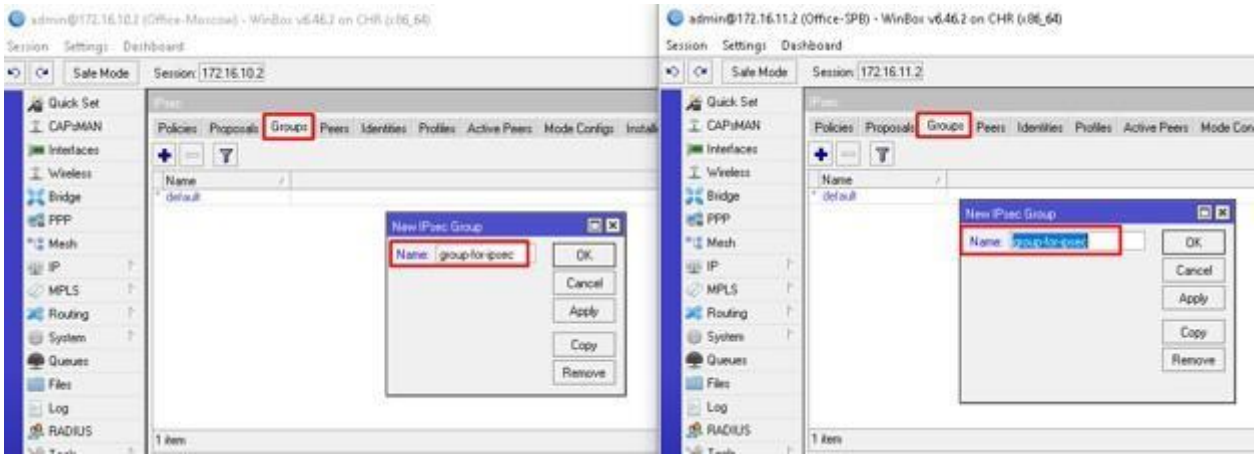

Рисунок 10 – Конфигурация групп IPsec

Следующий пункт — конфигурация «Identity».

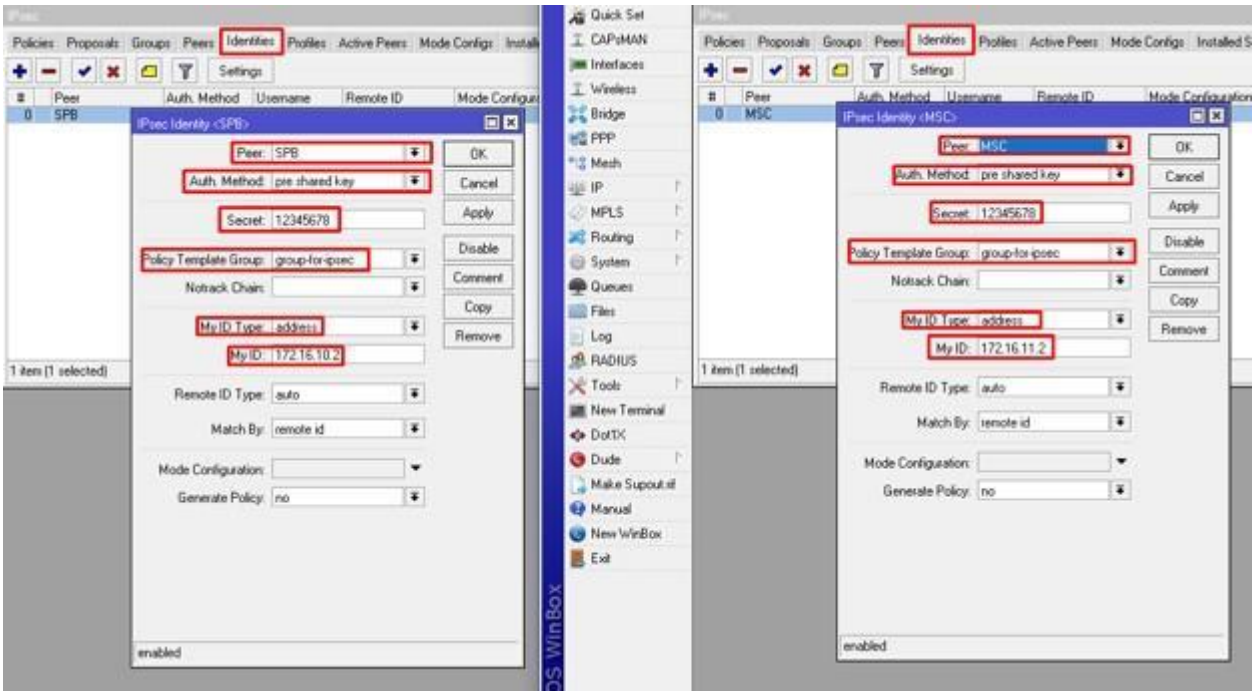

Рисунок 11 – Конфигурация Identity

Заключительным этапом является конфигурация политик «Policies». На вкладке General указываем адреса источника и назначения. Соответственно направляем друг на друга. 1701 это UDP порт L2TP.

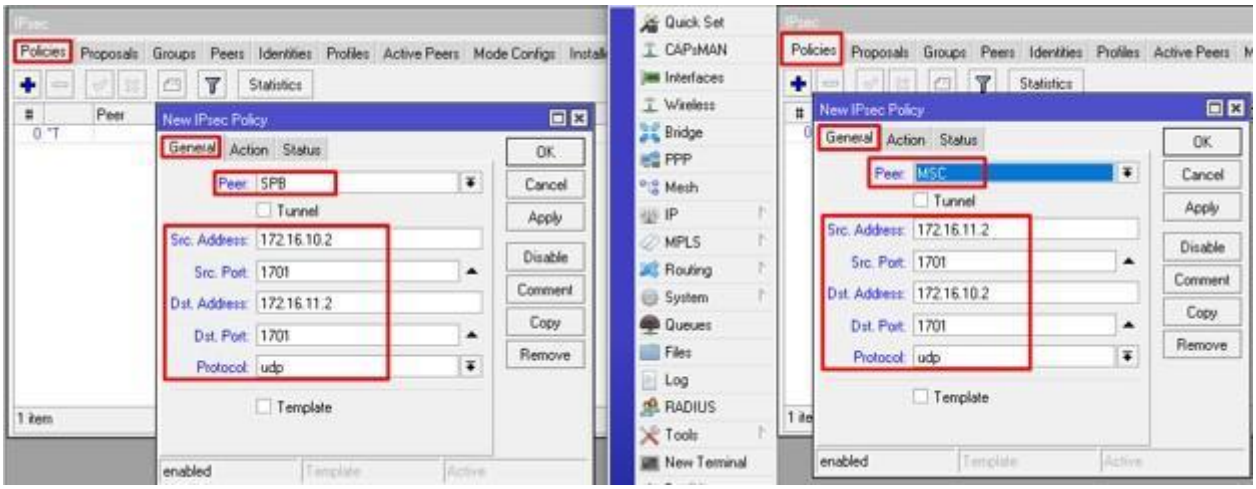

Рисунок 12 – Конфигурация политик IPsec

Переходим в вкладку Action. Обязательно выбираем параметр «Level» в «unique». Особенно полезно будет для тех, кто планирует много шифрованных туннелей.

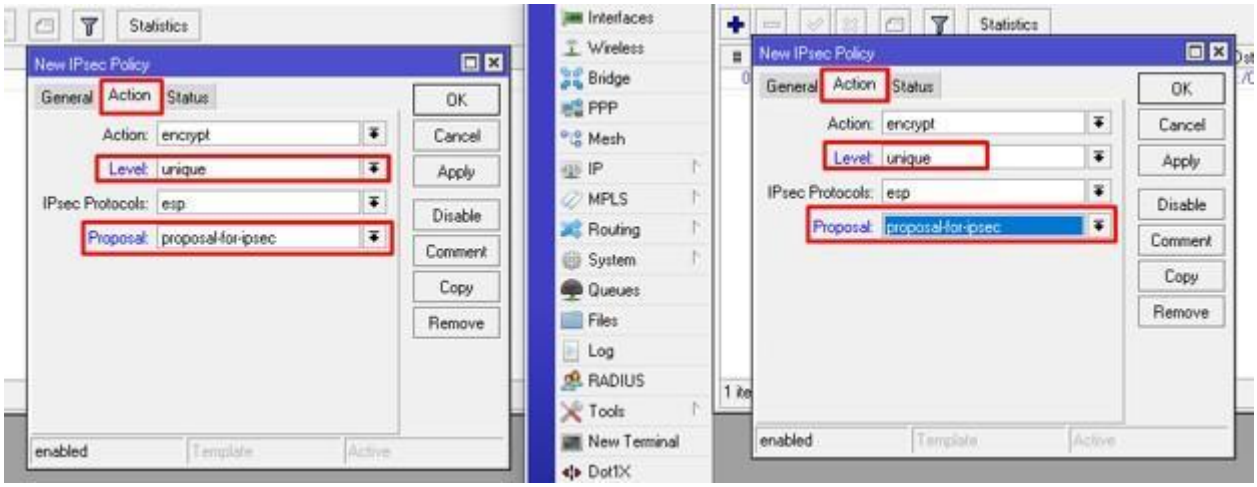

Рисунок 13 – Конфигурация политик IPsec

Сохраняем и проверяем.

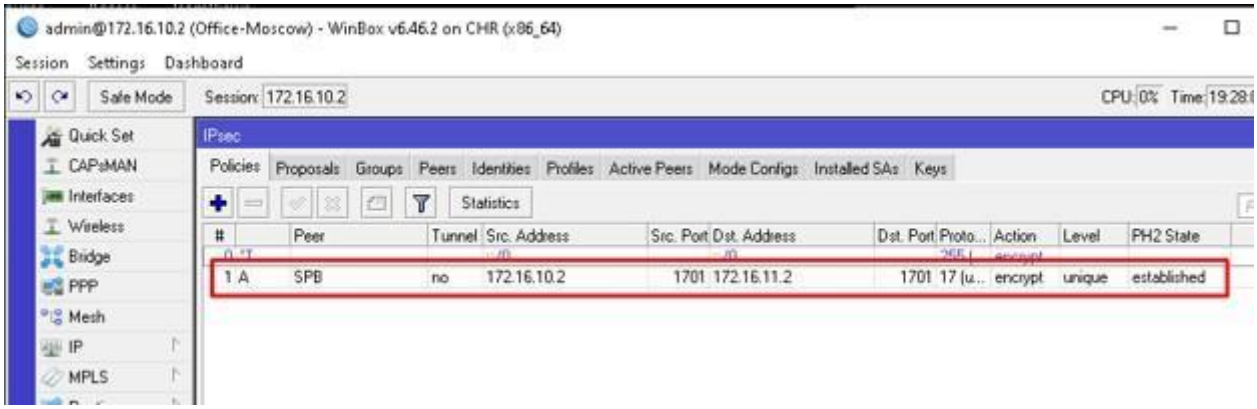

Рисунок 14 – Политики IPsec

Established в конце строки пира SPB означает что согласование прошло успешно и оно устоялось. Откроем вкладку «Installed SAs» и посмотрим на используемые ключи.

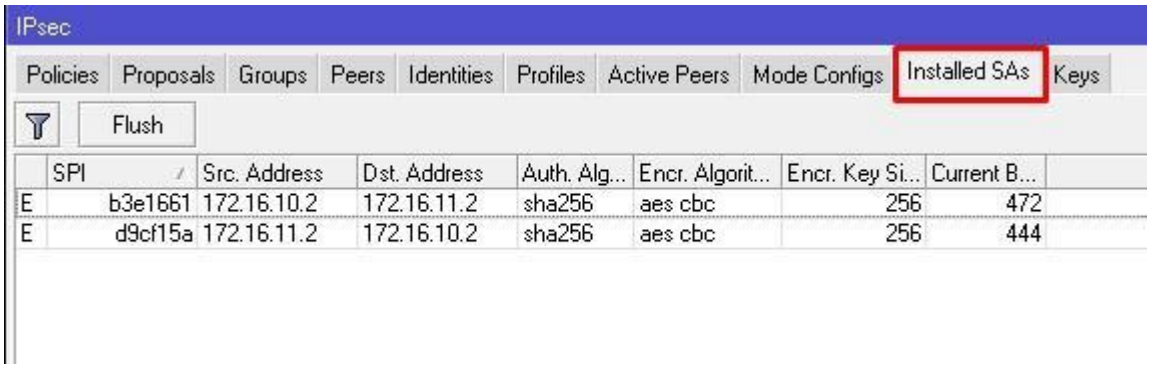

Рисунок 15 – Проверка создания ключей SAs

Ну и наконец, проверим L2TP соединение. Все должно зашифроваться без переподключений.

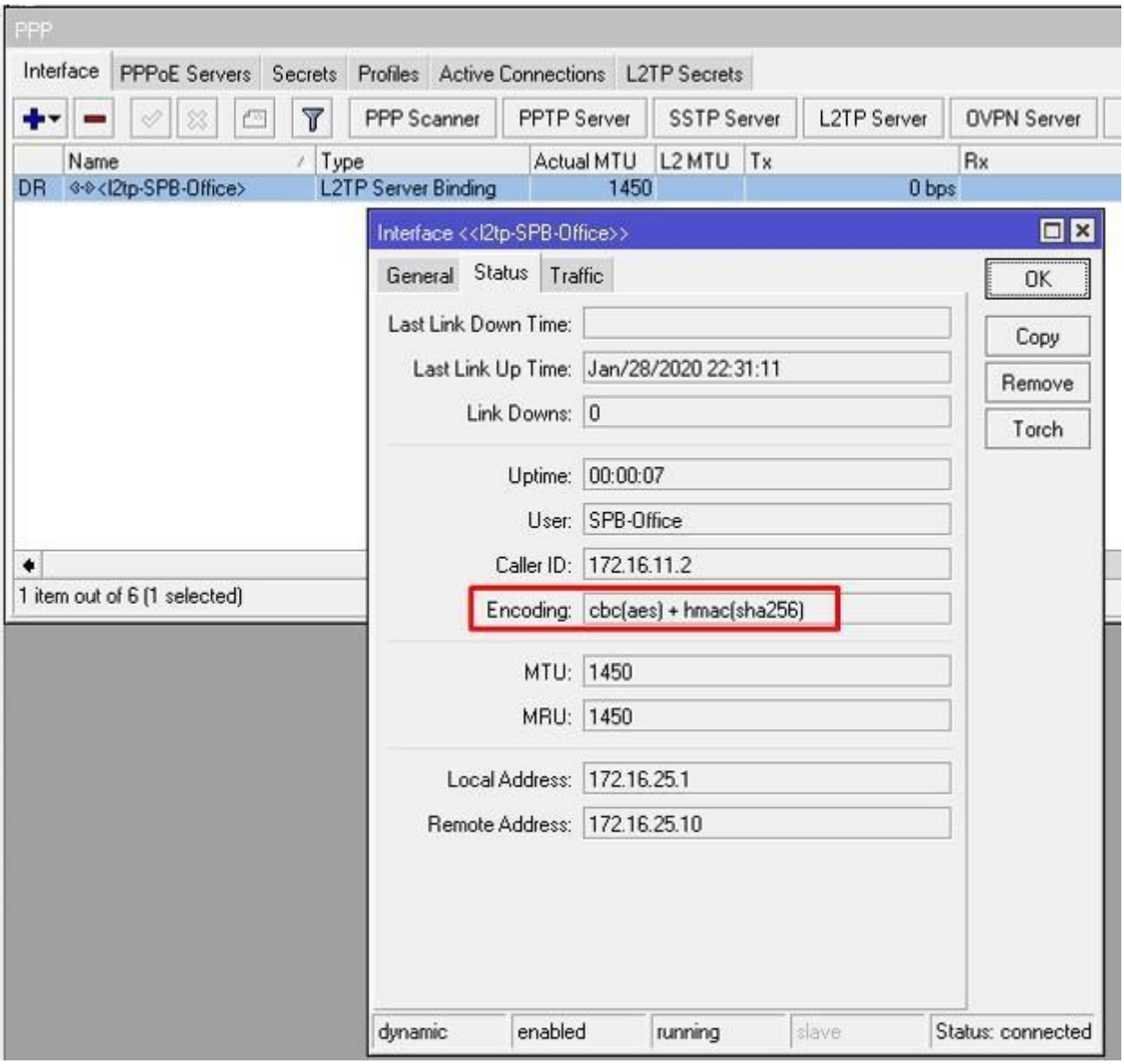

Рисунок 16 – Проверка L2TP IPsec

4. Настройка firewall

Тут также, как и с предыдущим пунктом. Настраиваем одинаково с обоих сторон. Нужно отредактировать созданные правила на «московском» роутере, а на «питерском» создаем с нуля аналогичные. В первом правиле кроме порта для L2TP добавляем еще два:

- 500;
- 4500.

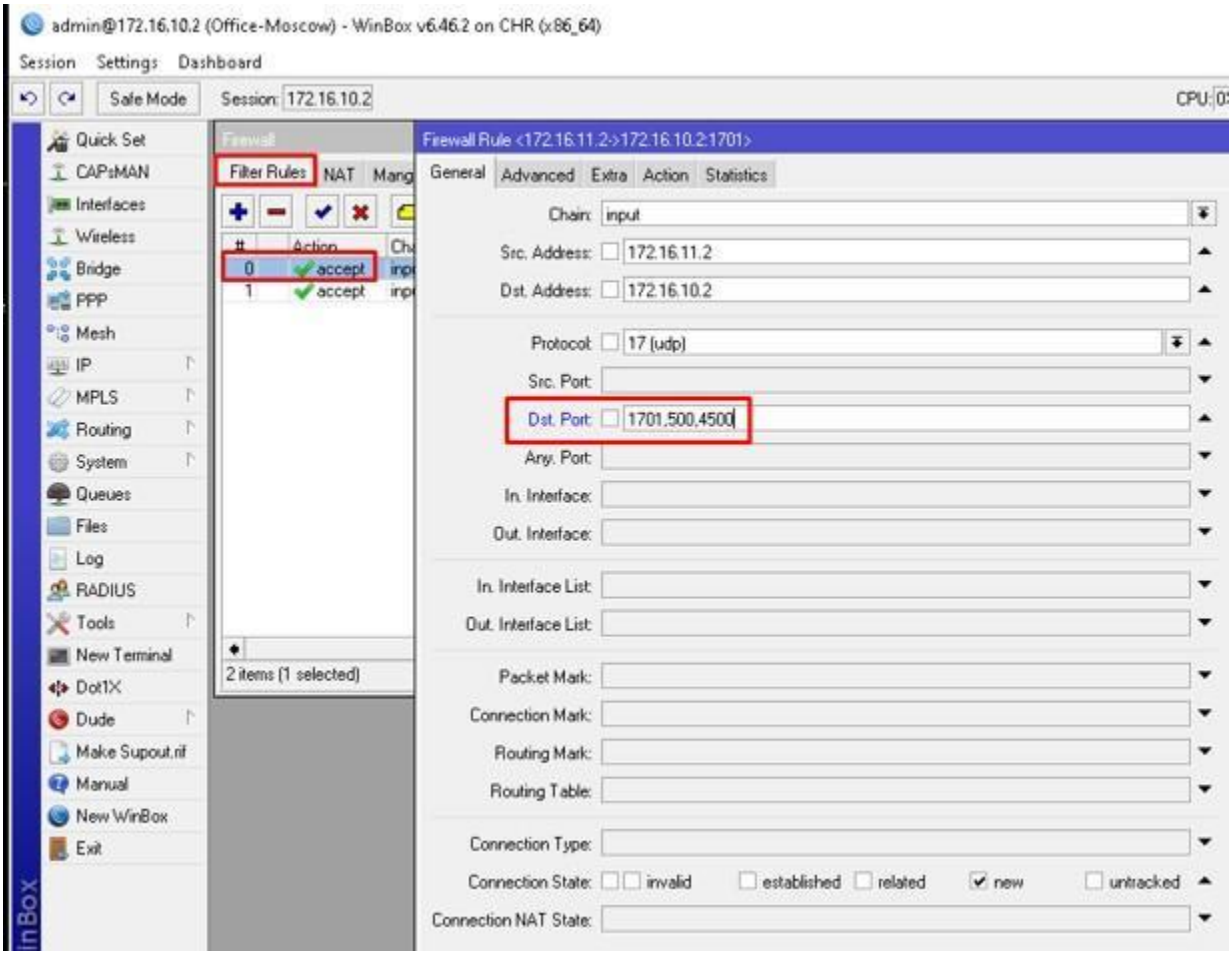

Рисунок 17 – Конфигурация межсетевого экрана

Создадим еще одно правило для IPSEC-ESP.

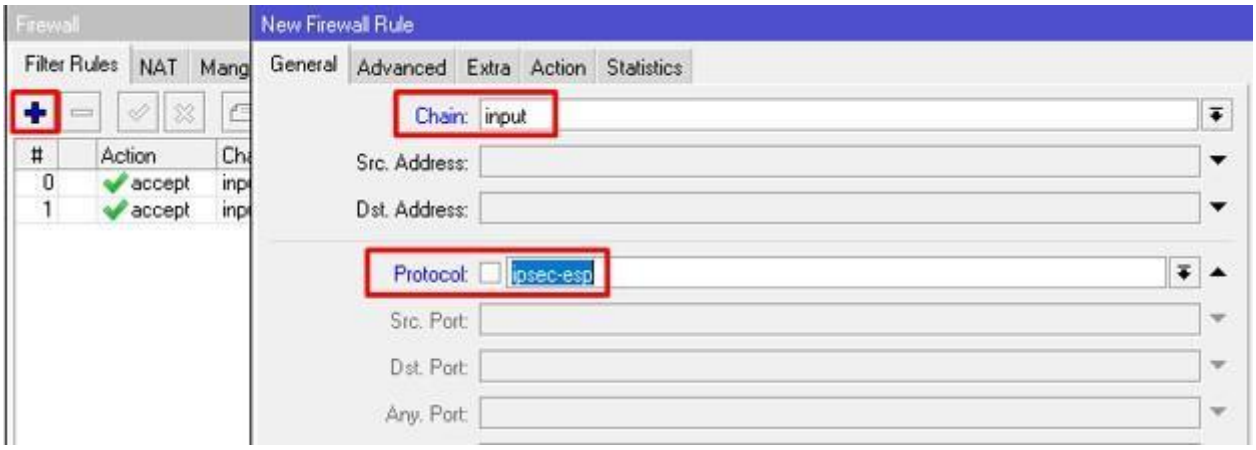

Рисунок 18 – Создание нового правила IPsec

Перемещаем его над последним правилом.

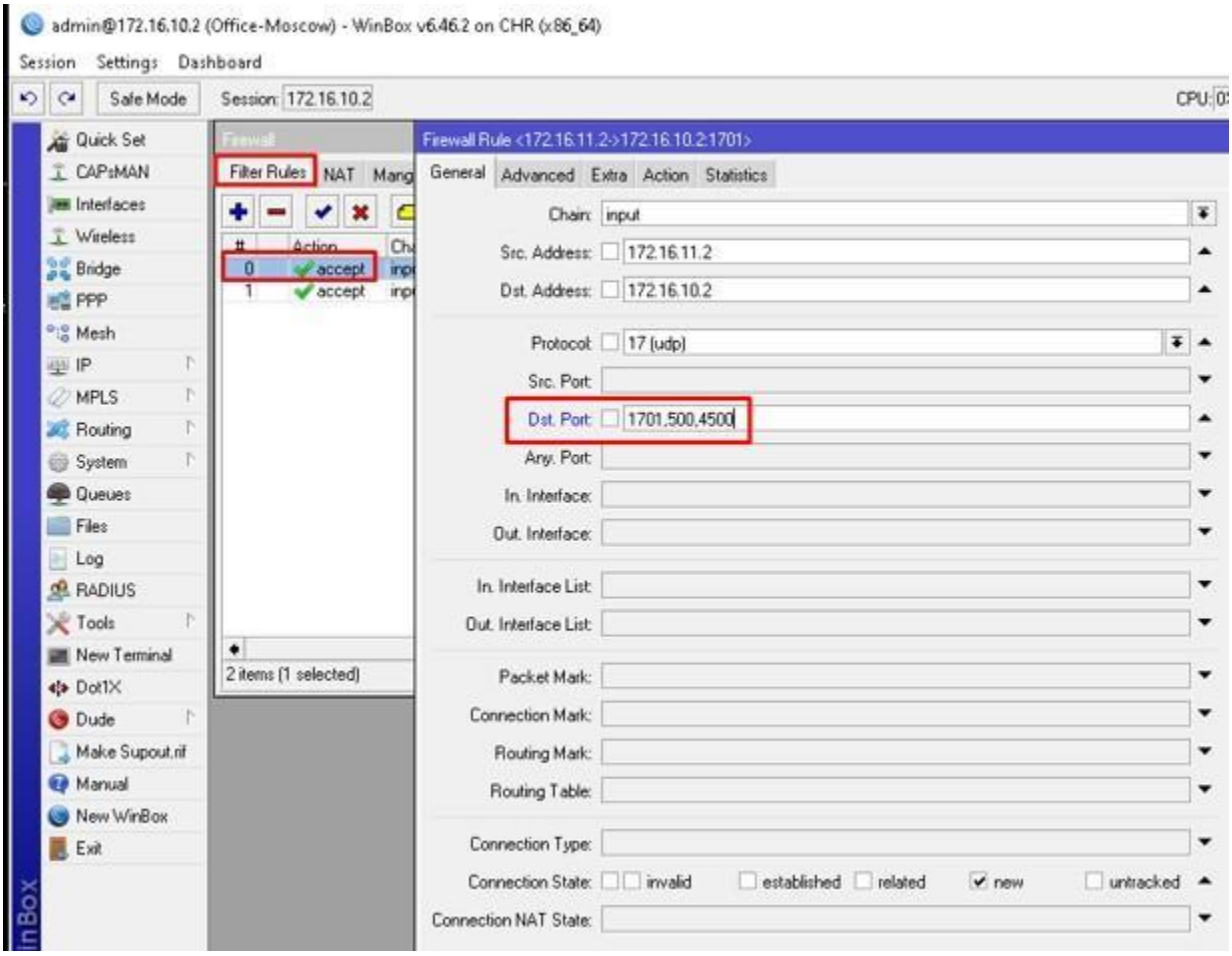

Рисунок 19 – Итоговая конфигурация межсетевого экрана

Повторив параметры межсетевого на «питерском» роутере, обязательно проверьте, что соединение L2TP подключается и шифруется соответствующими алгоритмами.

5. Формат отчета

- конфигурация обоих маршрутизаторов (аналогично предыдущим лабораторным работам);
- снимок экрана с отображением успешного подключения L2TP IPsec VPN;
- аналогично ЛР№3 провести тест скорости передачи данных с использованием IPsec, сравнить с значениями, полученными без использования последнего.