Задание № 4.4. Туннелирование в ViPNet Coordinator

Формулировка задания

В настоящем задании необходимо:

1.4.1. Настроить сетевые узлы таким образом, чтобы на узле *Координатор Центр офис* был доступен *незащищенный узел (VM_4)*, расположенный в *Филиале*, и при этом связь осуществлялась по шифрованному каналу (полутуннель).

1.4.2. Настроить сетевые узлы таким образом, чтобы открытый узел (*VM_5*) из подсети *Центр офис* имели доступ к *незащищенному узлу (VM_4)*, расположенному в *Филиале*, и при этом связь осуществлялась по шифрованному каналу (туннель).

Предварительные настройки

Для подготовки к заданию № 4.4 выполните следующие действия:

1. На виртуальной машине VM_1 в программе ViPNet Policy Manager удалите шаблон политики безопасности *Координатор Центр офис, Координатор Филиал,* отвечающие за настройку правил фильтрации транзитного трафика и отправьте измененные политики безопасности на узлы *Координатор Центр офис и Координатор Филиал*.
2. На виртуальной машине VM_1 в программе *ViPNet Центр управления сетью* перейдите в представление *Моя сеть > Координаторы* и зайдите в свойства узла *Координатор Центр офис*. В открывшемся окне на вкладке *Туннелирование* установите максимальное число одновременно туннелируемых соединений равным 15 (*Рисунок 1*). Аналогичное значение этого параметра задайте для узла *Координатор Филиал.* Сформируйте справочники и отправьте на все узлы сети.

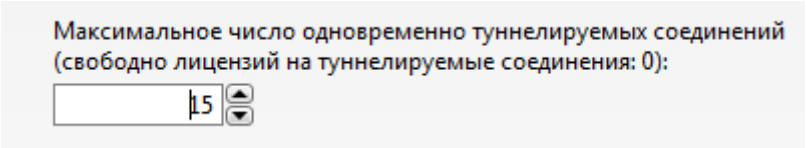

Рисунок 1 – Максимальное число одновременно туннелируемых соединений

3. На виртуальной машине VM_2 и VM_3 в программе *ViPNet Coordinator Монитор* удалите созданные в рамках предыдущего задания транзитные фильтры и фильтры трансляции адресов. После удаления фильтров нажмите кнопку *Применить* для сохранения изменений.

4.4.1. Полутуннель

Формулировка задания

Настроить сетевые узлы таким образом, чтобы на рабочем месте *Координатор Центр офис* был доступен *незащищенный узел (VM_4)*, расположенный в *Филиале*, и при этом связь осуществлялась по шифрованному каналу. Проверка выполняется с помощью команды ping.

Пояснение к заданию

Нередко возникает задача защитить обмен данными между узлами на потенциально опасном участке сети или включить узел в сеть ViPNet в условиях, когда нельзя установить на узел программное обеспечение ViPNet. Такая ситуация возможна, если узлы сети представляют собой специализированные устройства (например, IP-АТС или аппаратные IP-телефоны) или серверы (SQL, 1С, DHCP), на которые нежелательно устанавливать дополнительное ПО.

В таких случаях используется технология туннелирования. Данная технология предполагает направление трафика узла не напрямую на другой узел, а через ViPNet Coordinator, где трафик фильтруется и защищается криптографическими методами.

Работа полутуннеля происходит по следующим правилам (Рисунок 2):

1. От защищенного узла до туннелирующего координатора трафик передается в зашифрованном виде.
2. На координаторе трафик подвергается фильтрации, после чего передается дальше по цепочке назначения в зашифрованном виде (если необходимо).
3. На координаторе, туннелирующем узел получателя, трафик расшифровывается и передается на узел в открытом виде.

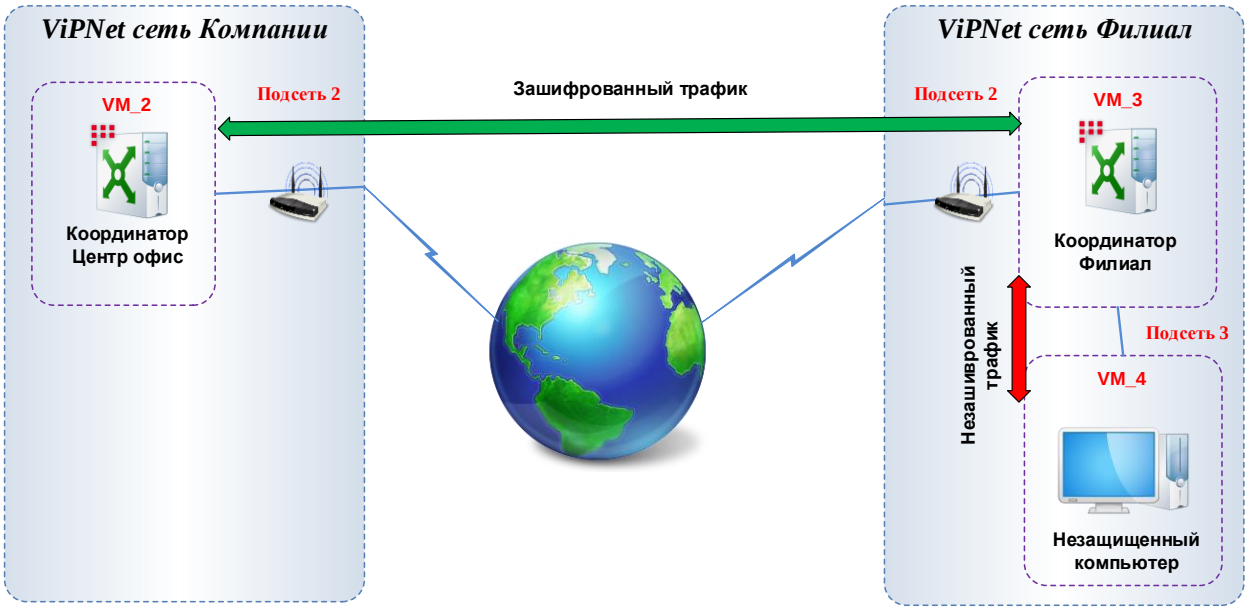

Рисунок 2 – Схема полутуннеля

Стоит также отметить, что термин полутуннель является проприетарным и используется для описания различных сценариев применения технологии туннелирования. В случае когда речь идет о полутуннеле, подразумевается подключение к туннелируемому ресурсу с помощью клиента.

Существует два способа задания узлов для туннелирования:

- В программе *ViPNet Центр управления сетью*. В этом случае после рассылки новых справочников адреса туннелируемых узлов будут переданы и на туннелирующий координатор, и на все клиенты и координаторы, связанные с этим координатором.
- В программе *ViPNet Coordinator Монитор*. В этом случае адреса туннелируемых узлов необходимо вручную задать на туннелирующем координаторе и на каждом сетевом узле, который должен иметь доступ к туннелируемым узлам. Те узлы ViPNet, на которых не были указаны туннелируемые адреса, не будут иметь доступа к туннелируемым узлам.

Первый способ удобен тем, что позволяет задавать адреса для туннелирования централизованно. Рекомендуется использовать именно этот способ.

Второй способ можно применить, когда доступ к туннелируемым адресам нужно организовать для небольшого числа клиентов.

Необходимо выбрать один из способов задания туннелируемых узлов и придерживаться его при изменении конфигурации сети, так как задание адресов в программе *ViPNet Центр управления сетью* перекрывает все настройки, сделанные вручную на координаторах и клиентах.

В настоящем задании будет использован первый способ задания узлов для туннелирования. Для узла *Координатор Филиал* будет добавлен диапазон туннелируемых ресурсов *Подсеть Филиал* (*x.x.x.x-y.y.y.y*).

Порядок выполнения задания

Для настройки полутуннеля выполните следующие действия в окне программы *ViPNet Центр управления сетью* на рабочем месте *Главный администратор*:

1. В представлении *Моя сеть* > *Координаторы* зайдите в свойства узла *Координатор Филиал*.
2. В открывшемся окне на вкладке *Туннелирование* нажмите кнопку *Добавить…* и укажите диапазон адресов *x.x.x.x-y.y.y.y (Подсеть Филиал)(Рисунок 3)*.
3. В меню *Сервис* выберите пункт *Справочники и ключи* > *Сформировать справочники*.
4. Сформируйте и отправьте справочники на все узлы.
5. Проконтролируйте прохождение обновлений на узлах *Координатор Центр офис* и *Координатор Филиал*.

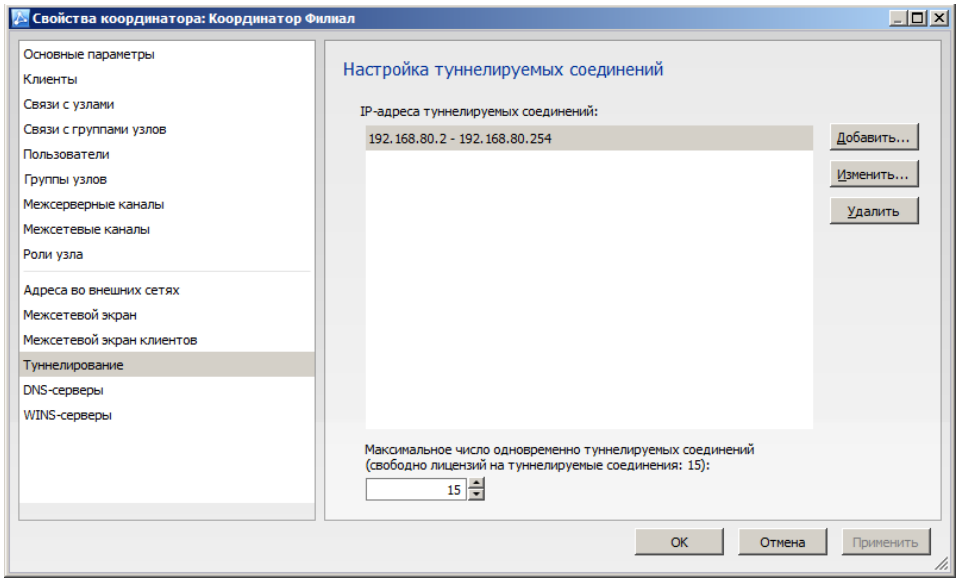

Рисунок 3 – Добавление диапазона туннелируемых адресов

6. После прохождения обновлений перейдите на узел *Координатор Филиал*.
7. Откройте программу ViPNet Coordinator Монитор в меню *Сервис* выберите пункт *Настройка приложения*.
8. В открывшемся окне на вкладке *Туннелирование* должен быть отображен диапазон *x.x.x.x-y.y.y.y (Рисунок 154)*.

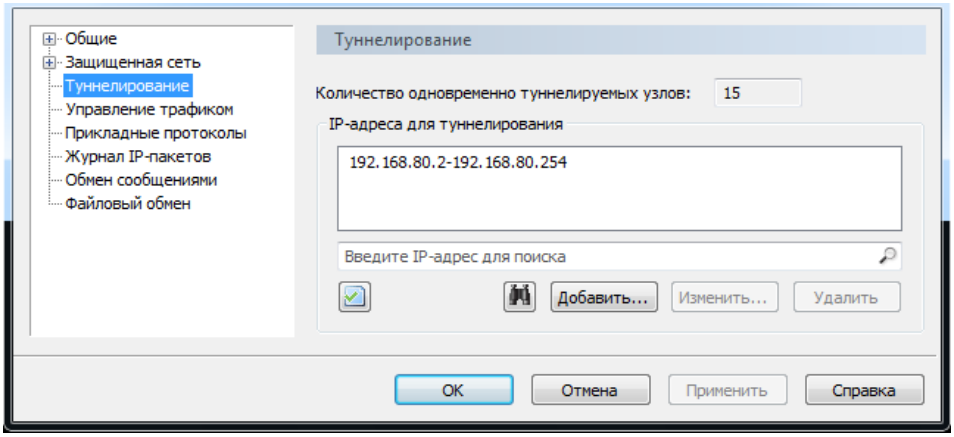

Рисунок 4 – Вкладка *Туннелирование* узла *Координатор Филиал*

9. Теперь перейдите на узел *Координатор Центр офис*.
10. В программе *ViPNet Coordinator Монитор* на панели навигации откройте раздел *Защищенная сеть*.
11. Дважды щелкните узел *Координатор Филиал*.

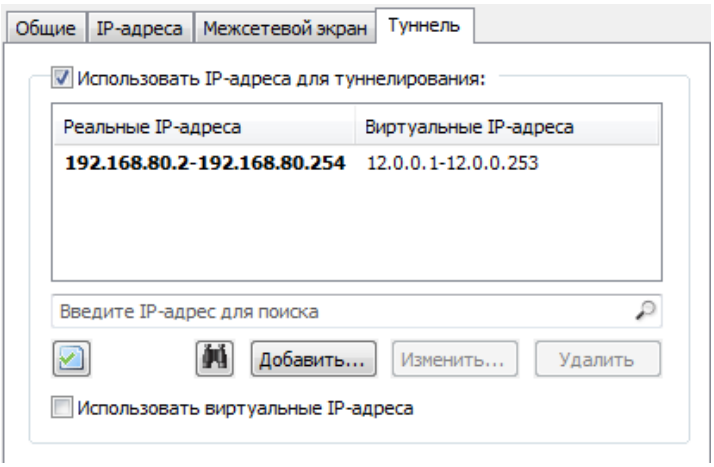

Рисунок 5 – Вкладка *Туннель* узла *Координатор Филиал*

12. В открывшемся окне на вкладке *Туннель* должен быть отображен диапазон x.x.x.x-*y.y.y.y* (Рисунок 5). Откройте командную строку и с помощью команды *ping* проверьте доступность адреса *незащищенного узла (VM_4)*.
13. Зайдите в журнал регистрации IP-пакетов, отфильтруйте трафик по IP-адресу незащищенного узла, проанализируйте ситуацию, убедитесь, что трафик до узла идет шифрованный (пакет туннелируемого узла).

4.4.2. Туннель

Формулировка задания

Настройте сетевые узлы таким образом, чтобы на *узле VM_5* из *подсети Центр офис* был доступен *незащищенный узел (VM_4*), расположенный в

Филиале, и при этом связь осуществлялась по шифрованному каналу. Проверка выполняется с помощью команды ping.

Пояснение к заданию

Работа туннеля происходит по следующим правилам *(Рисунок 156)*:

1. От незащищенного узла до туннелирующего координатора трафик передается в незашифрованном виде.
2. На координаторе трафик подвергается фильтрации, после чего передается дальше по цепочке назначения в зашифрованном виде.
3. На координаторе, туннелирующем узел получателя, трафик расшифровывается и передается на узел в открытом виде.

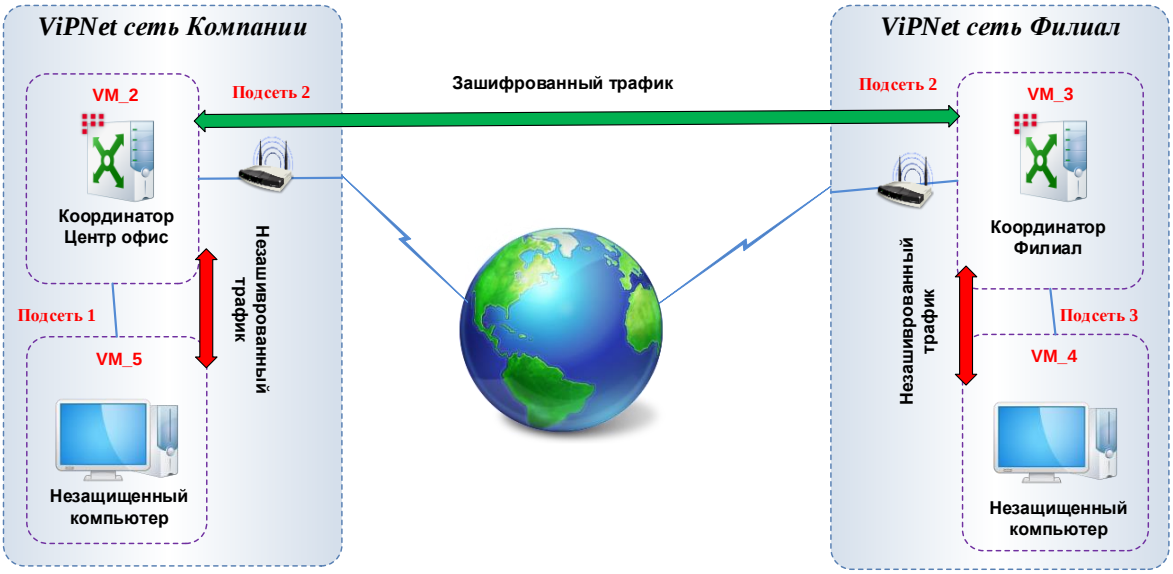

Рисунок 6 – Схема туннеля

В настоящем задании будет использован способ задания узлов для туннелирования – вручную на координаторах в программе *ViPNet Coordinator Монитор*. Для узла *Координатор Центр офис* будет добавлен диапазон туннелируемых ресурсов *Подсеть Центр офис* (*x.x.x.x-y.y.y.y*).

Порядок выполнения задания

Для настройки туннеля выполните следующие действия:

1. На узле *Координатор Центр офис* откройте программу *ViPNet Coordinator Монитор* > *Верхнее меню Сервис* > *Настройка приложения*.
2. В открывшемся окне на вкладке *Туннелирование* нажмите кнопку *Добавить* и задайте диапазон *x.x.x.x-y.y.y.y* (Рисунок 7).
3. На узле *Координатор филиал* откройте программу *ViPNet Coordinator Монитор* > *Защищенная сеть*.
4. Дважды щелкните узел *Координатор Филиал.*

5. В открывшемся окне на вкладке *Туннель* нажмите кнопку *Добавить* и задайте диапазон *x.x.x.x-y.y.y.y* (Рисунок 8).

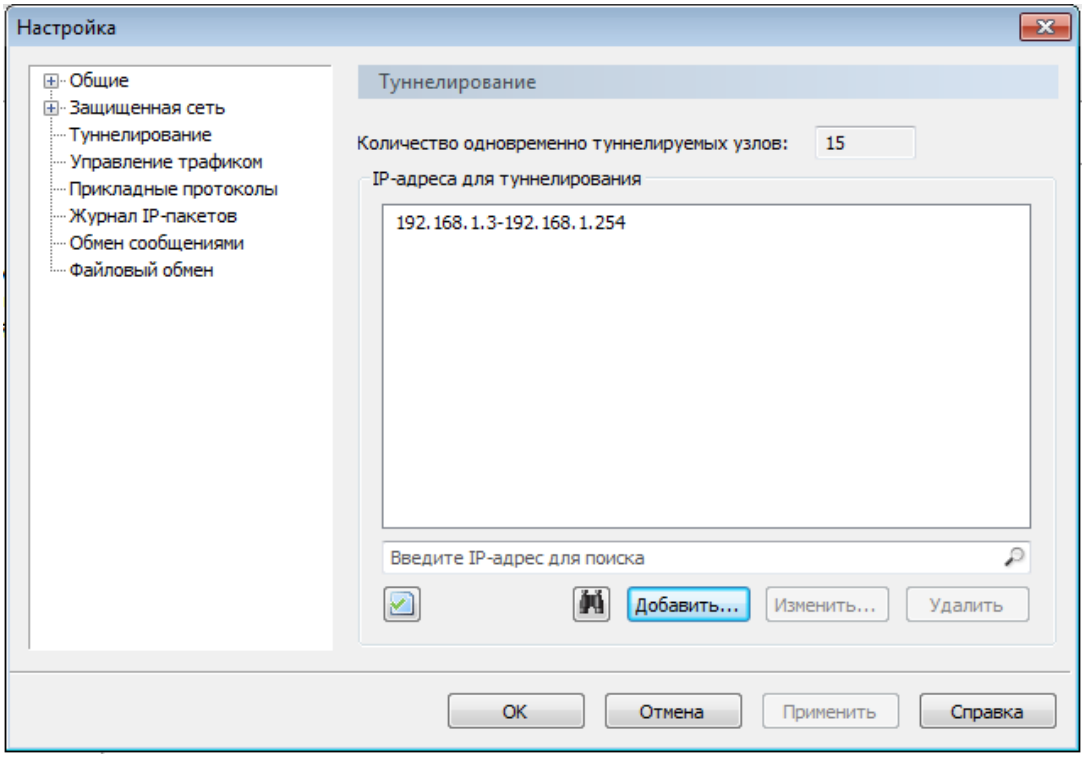

Рисунок 7 – Вкладка *Туннелирование* узла *Координатор Центр офис*

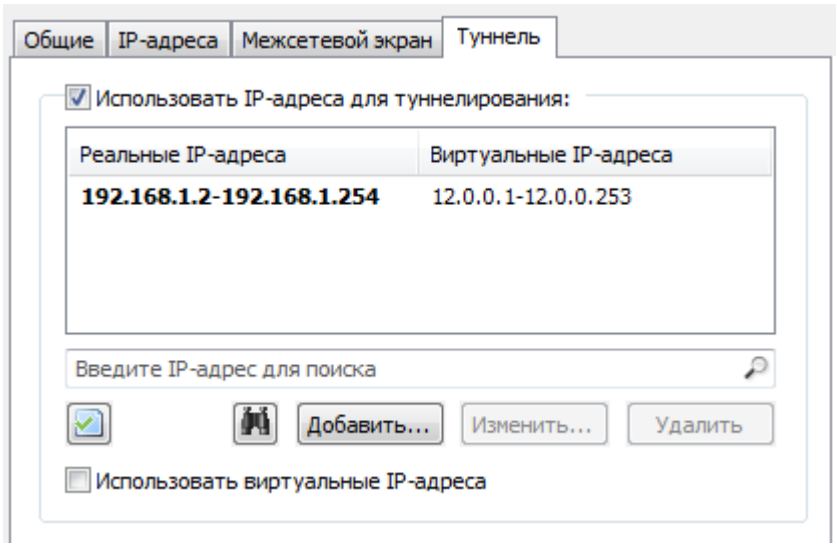

Рисунок 8 – Вкладка *Туннель* узла *Координатор центральный офис*

6. На виртуальной машине VM_5 откройте командную строку и с помощью команды *ping* проверьте доступность адреса *незащищенного узла (VM_4).*
7. На рабочем месте *незащищенный узел (VM_4)* откройте командную строку и с помощью команды *ping* проверьте доступность IP-адреса виртуальной машины *VM_5*.

8. Зайдите в журнал регистрации IP-пакетов, проанализируйте ситуацию, убедитесь, что трафик до узла идет шифрованный (пакет туннелируемого узла).