## Практическое занятие № 4. Работа с ViPNet Coordinator 4 for Windows

Целью практического занятия является закрепление полученных знаний на лекционных занятиях в части настройки фильтров открытой сети, фильтров защищенной сети, трансляции адресов, антиспуфинга, туннелирования, групп объектов, работы с журналом IP-пакетов, а также других аспектов настройки ViPNet Coordinator for Windows (далее – ViPNet Coordinator).

### Содержание практического занятия

1.1.Настройка локальных и транзитных фильтров открытой сети.
1.2.Настройка фильтров защищенной сети.
1.3.Настройка трансляции адресов.
1.4.Настройка туннелирования.
1.5.Дополнительное задание.

На предыдущих практических занятиях неоднократно проводилась модификация сети, а также настраивалось межсетевое взаимодействие в связи с этим рекомендуется подготовить стенд в соответствии с общей типовой схемой (см. стр. 17), необходимой для выполнения задания *(Рисунок 141)*.

| | |
|---|---|
| | **Примечание.** Необходимо учитывать, что на приведенной ниже схеме дополнительно введены еще две виртуальные машины (VM_5 и VM_6 – незащищенные узлы, без ViPNet). В качестве VM_5 и VM_6 могут быть задействованы любые свободные виртуальные машины с минимальными системными требованиями (например, с развернутой Windows XP).<br>Стоит также обратить внимание на то, что в процессе выполнения практического задания не требуется одновременного запуска всех виртуальных машин. Поэтому стоит следовать алгоритму выполнения задания, чтобы обеспечить продуктивную работу стенда. |

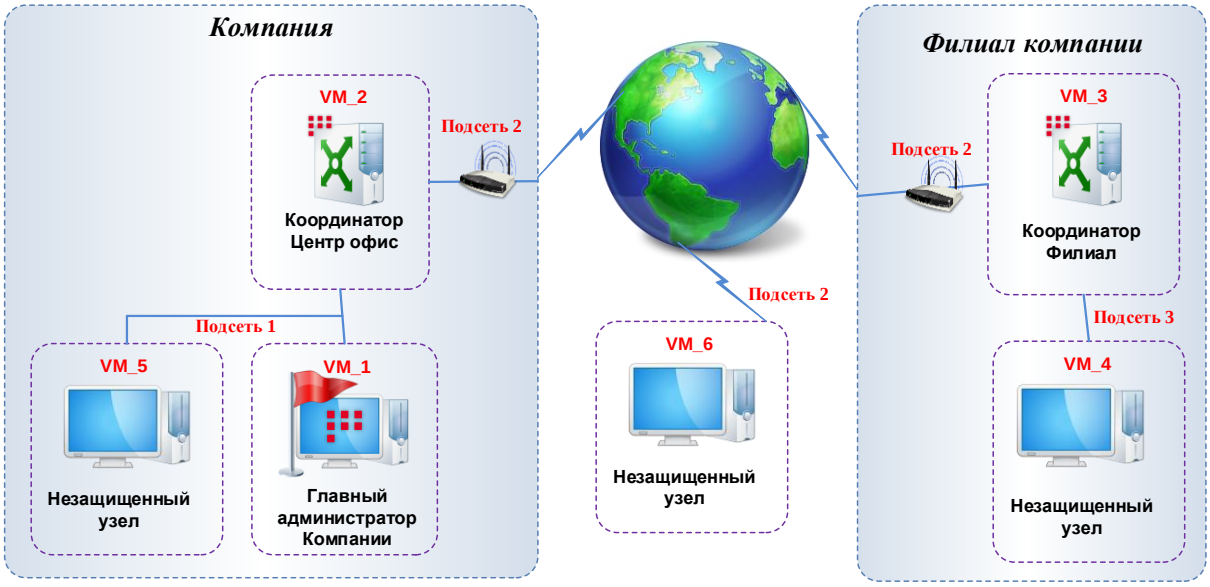


Рисунок 1 – Схема стенда для практического задания №4

## Задание № 4.1. Настройка локальных и транзитных фильтров открытой сети

### Формулировка задания

В настоящем задании необходимо:

1.1.1. Настроить локальные фильтры на узле *Координатор Филиал* таким образом, чтобы получить доступ к нему по RDP с незащищенного узла (VM_4).

1.1.2. Настроить транзитные фильтры открытой сети на узлах *Координатор Центр офис и Координатор Филиал* таким образом, чтобы обеспечить прохождение в обоих направлениях незащищенного транзитного трафика между удаленными компьютерами (VM_4 и VM_5).

### Предварительные настройки

Для подготовки к заданию № 4.1 выполните следующие действия:

1. Проверьте, что на виртуальной машине VM_1 установлены программы ViPNet Administrator, ViPNet Policy Manager и ViPNet Client.
2. Проверьте, что на виртуальной машине VM_2 установлена программа ViPNet Coordinator с установленным дистрибутивом ключей *Координатор Центр офис*.
3. На виртуальных машинах VM_3 и VM_4 удалите программное обеспечение ViPNet (если установлено).
4. На виртуальной машине VM_3 проверьте настройки удаленного доступа в операционной системе.
5. В качестве VM_5 выберите любую свободную виртуальную машину без программного обеспечения ViPNet.
6. На виртуальной машине VM_3 установите ViPNet Coordinator и дистрибутив ключей пользователя *Координатор Филиал,* а также проверьте доступность узла *Координатор Центр офис*.
7. На виртуальной машине VM_4 с помощью команды ping проверьте доступность виртуальной машины VM_3.

## 1.1.1. Настройка локальных фильтров открытой сети

### Формулировка задания

Произвести настройку программного обеспечения *ViPNet Coordinator* таким образом, чтобы при вводе IP-адреса узла *Координатор Филиал* в диалоговом окне *Подключение к удаленному рабочему столу* на незащищенном узле (VM_4) *(Рисунок 142)*, открывалось окно авторизации на удаленном узле (*Координатор Филиал*) *(Рисунок 143)*.

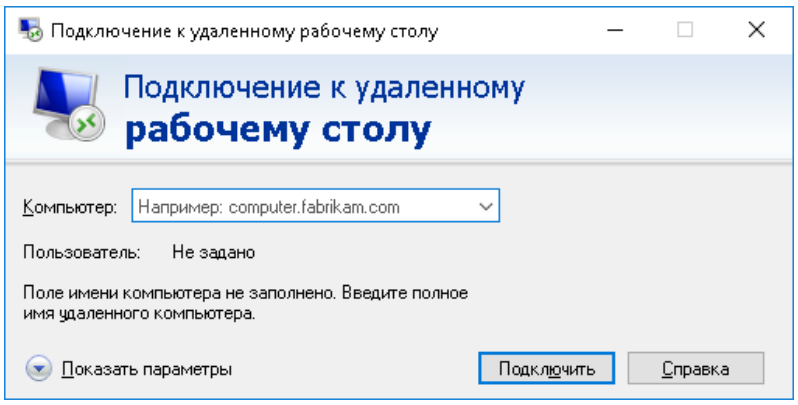


Рисунок 2 – Диалоговое окно *Подключение к удаленному рабочему столу*

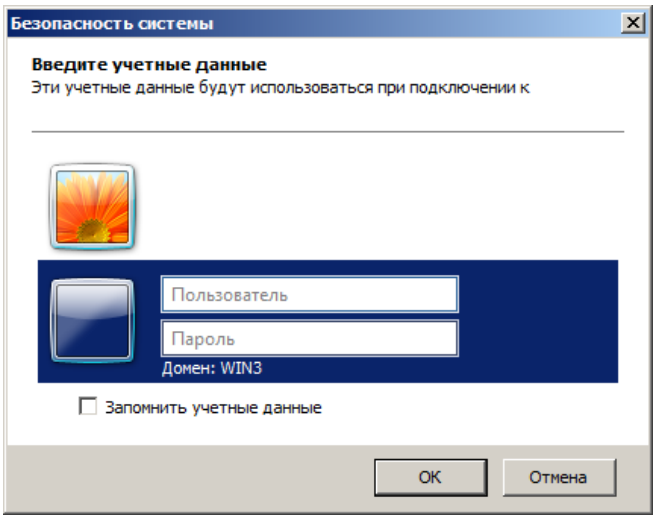


Рисунок 3 – Окно авторизации на удаленном узле

**Пояснение к заданию**

Доступ по RDP осуществляется с использованием протокола TCP порт 3389. Таким образом, для выполнения задания на *Координаторе Филиал* должны быть разрешены соединения по протоколу *TCP*, порту назначения *3389* и IP-адресу источника (VM_4).

На узле *Координатор Филиал* выполните настройку локальных фильтров открытой сети, добавив разрешающее правило. Сформулируем такое правило следующим образом:

*Разрешить доступ от IP-адрес незащищенного узла VM_4 к Координатор Филиал по протоколу TCP и порту 3389.*

Локальные фильтры открытой сети предназначены для обработки открытых (незашифрованных) сетевых пакетов.

Настройка сетевых фильтров может осуществляться централизованно в программе *ViPNet Policy Manager* и локально в программе *ViPNet Coordinator* непосредственно на узле.

**Порядок выполнения задания**

| | |
|---|---|
|  | **Примечание.** Перед настройкой фильтров рекомендуется попробовать подключиться по RDP к узлу Координатор Филиал с незащищенного узла и посмотреть в журнал регистрации IP-адресов в программе ViPNet Монитор. Убедиться в том, что пакеты от незащищенного узла проходят и блокируются. Обратите внимание, на то по какому событию происходит блокировка. Так как во многих ситуациях может помочь в решении проблем с доступом и прохождением трафика, а также написанием соответствующих событиям блокировки правил фильтрации как разрешающих, так и запрещающих. |

Для настройки доступа по RDP к узлу *Координатор Филиал* выполните следующие действия в окне программы *ViPNet Coordinator Монитор* на рабочем месте *Координатор Филиал*:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел *Сетевые фильтры> Локальные фильтры открытой сети*.
2. На панели просмотра нажмите кнопку *Создать*, после чего в появившемся окне задайте параметры нового фильтра открытого трафика.
3. В разделе Основные параметры укажите имя фильтра *Доступ по RDP* и его действие: блокировать или пропускать трафик.

В разделе *Источники* задайте отправителя открытых IP-пакетов. Для этого добавьте IP-адрес незащищенного узла (VM_4)

*Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми открытыми узлами, и вашим узлом в том числе.*

4. При необходимости укажите сетевой интерфейс вашего узла, на котором должны быть приняты открытые IP-пакеты от указанных источников, либо с которого они должны быть отправлены (в случае, если в качестве отправителя был выбран Мой узел). Для этого установите флажок Сетевой интерфейс и добавьте:
   - отдельный IP-адрес интерфейса или диапазон IP-адресов интерфейсов;
   - один из доступных интерфейсов узла;
   - группу интерфейсов, если такая создана.
5. В разделе Назначения задайте получателя открытых IP-пакетов. Для этого добавьте системную группу объектов Мой узел. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.

   *Если вы не укажете получателя, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой открытый узел.*

   *При необходимости укажите сетевой интерфейс вашего узла, с которого должны отправляться IP-пакеты заданным получателям.*
6. В разделе Протоколы укажите протокол RDP, для этого нажмите кнопку *Добавить > Группы протоколов > RDP*.

7. В разделе Расписания в случае необходимости можно указать дату и время работы данного фильтра.
8. Нажмите кнопку OK. В результате в списке на панели просмотра появится новый фильтр.
9. Проверьте появление нового фильтра *Доступ по RDP* в разделе *Сетевые фильтры* > *Локальные фильтры открытой сети* и нажмите кнопку *Применить* (Рисунок 4). В случае если кнопка *Применить* не будет нажата, новый фильтр не будет использоваться при работе программы *ViPNet Coordinator*.

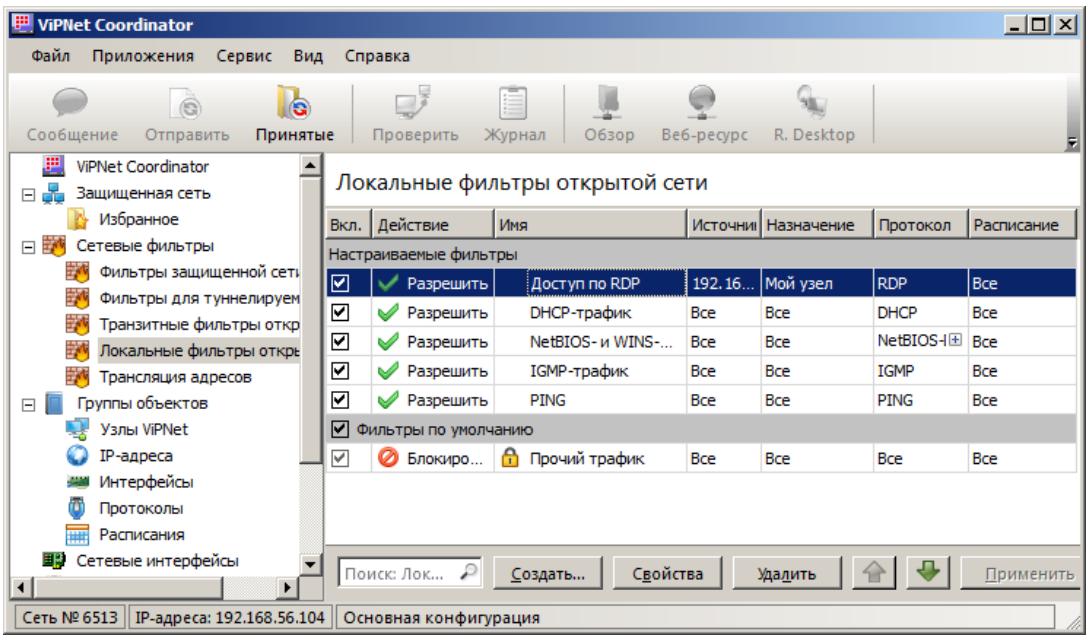


Рисунок 4 – Новый фильтр *Доступ по RDP*

10. Введите IP-адреса узла *Координатор Филиал* в диалоговом окне *Подключение к удаленному рабочему столу* на незащищенной машине (VM_4), после чего должно открыться окно авторизации на удаленном узле (*Координатор Филиал*).
11. Введите имя пользователя удаленного узла и попробуйте авторизоваться.
12. Зайдите в Журнал IP-пакетов, поставьте фильтр по порту 3389 и посмотрите по какому событию пропускается данный трафик.

### 1.1.2. Настройка транзитных фильтров открытой сети

**Формулировка задания**

Произвести настройку программного обеспечения ViPNet Coordinator таким образом, чтобы рабочие станции (VM_4 и VM_5) из подсетей *Центр офис* и *Филиал* имели доступ друг к другу (в рамках практического занятия доступность проверяется командой ping).

**Пояснение к заданию**

| | |
|---|---|
| | **Примечание.** В рамках выполнения данного практического задания задействовано 5 виртуальных машин. Поэтому, в случае, если компьютер с развернутым стендом недостаточно мощный, то рекомендуется сперва создать правила фильтрации и другие настройки на рабочем месте с Главным администратором, разослать обновления на координаторы, после чего выключить виртуальную машину с Главным администратором и запустить виртуальные машины с координаторами (VM_2 и VM_3) и две незащищенные (без ViPNet) с Windows XP (VM_4 и VM_5). |

Транзитные фильтры определяют действия для открытых транзитных IP-пакетов, проходящих через координатор (то есть пакетов, адреса источника и назначения которых не совпадают ни с одним из адресов координатора).

Настройку сетевых фильтров будем производить в программе *ViPNet Policy Manager*. Настройка будет производиться для узлов *Координатор Центр офис* и *Координатор Филиал.*

Правило для транзитных пакетов:

1. *Разрешить доступ из подсети Филиал компании к подсети Центр офис по протоколу ICMP*
2. *Разрешить доступ из подсети Центр офис к подсети Филиал компании по протоколу ICMP*

**Порядок выполнения задания**

Для настройки доступа рабочих станций из подсети *Филиал* к рабочим станциям *Центр офис* и в обратном направлении, выполните следующие действия на рабочем месте *Главный администратор* в окне программы *ViPNet Policy Manager*:

1. В разделе *Группы объектов> IP-адреса* нажмите кнопку *Создать*.
    a. В открывшемся окне Свойства группы IP-адресов на вкладке Основные параметры задайте имя *Подсеть Филиал*.
    b. На вкладке *Состав* нажмите *Добавить> IP-адрес или диапазон адресов* и в открывшемся окне *IP-адрес* задайте подсеть Филиал (адрес подсети и маску подсети нужно указывать в соответствии с настройками ваших виртуальных машин входящих в подсеть *Филиала*) *(Рисунок 145)*.

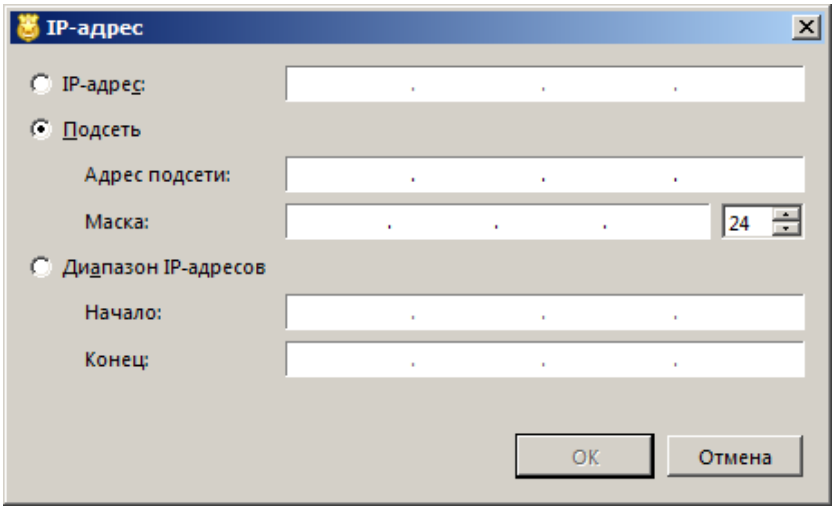


Рисунок 5 – Окно *IP-адрес*

2. Аналогичным образом создайте объект *Подсеть Центр офис*
3. В разделе *Шаблоны политики* нажмите кнопку *Создать*.
4. В открывшемся окне Свойства шаблона политики на вкладке *Основные параметры* задайте имя *Координатор Филиал*.
5. На вкладке *Сетевые узлы* добавьте узел *Координатор Филиал*.
6. На вкладке *Транзитные фильтры открытой сети* нажмите кнопку *Создать* (необходимо будет создать два разрешающих фильтра для исходящего и входящего транзитного трафика):
    a. В открывшемся окне *Свойства транзитного фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Доступ в подсеть Центр офис* и установите переключатель в положение *Пропускать трафик (Рисунок 146)*.

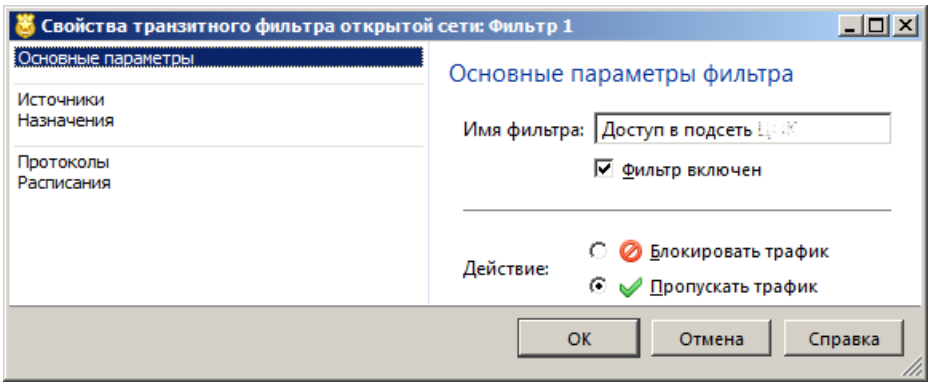


Рисунок 6 – Основные параметры окна свойств транзитного фильтра

    i. На вкладке *Источники* нажмите кнопку *Добавить> Группа IP-адресов* и выберите *Подсеть Филиал*.
    ii. На вкладке *Протоколы* нажмите кнопку *Добавить> IP-протокол…> ICMP > OK*.

b. В открывшемся окне *Свойства транзитного фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Доступ из подсети Центр офис* и установите переключатель в положение *Пропускать трафик*.
    i. На вкладке *Источники* нажмите кнопку *Добавить > Группа IP-адресов* и выберите *Подсеть Центр офис*.
    ii. На вкладке *Назначения* нажмите кнопку *Добавить > Группа IP-адресов* и выберите *Подсеть Филиал.*
    iii. На вкладке *Протоколы* нажмите кнопку *Добавить > IP-протокол…> ICMP > ОК*.

7. Аналогичным образом настройте шаблон политики для правила обработки транзитного трафика для *Подсети Центр офис.*
8. Отправьте политики на узлы *Координатор Центр офис и Кординатор Филиал* (в окне программы ViPNet Policy Manager раздел *Сетевые узлы > Выбрать узлы Координатор Центр офис Координатор Филиал > Отправить политики*).

Если все сделано правильно, то на узлах в программе *ViPNet Coordinator Монитор* будут добавлены новые правила в разделах *Транзитные фильтры открытой сети.*

При успешном выполнении данного задания должны стать доступны друг другу VM_4 и VM_5 (проверка выполняется с использованием команды ping).