Задание № 4.2. Настройка фильтров защищенной сети

Формулировка задания

Произвести настройку программного обеспечения *ViPNet Coordinator* таким образом, чтобы закрыть доступ по RDP с защищенного узла *Координатор Филиал* на защищенный узел *Координатор Центр офис.*

Пояснение к заданию

Фильтры защищенной сети могут ограничивать обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь.

Например, на координаторах в фильтрах защищенной сети по умолчанию разрешен доступ по RDP со всех узлов на все узлы. И если на координаторе в настройках операционной системы будет разрешено подключаться к удаленному рабочему столу это может создать потенциально уязвимое место. Поэтому в рамках практического задания предлагается более гибко настроить фильтры защищенной сети. Есть два пути развития в данном случае:

- полностью запретить доступ по RDP к координатору (но данный вариант приемлем, если данное оборудование расположено в шаговой доступности администратору и было принято максимально ограничить открытые порты, даже для защищенных узлов);
- разрешить доступ по RDP только с определенных защищенных узлов (в данном случае с узла *Главного администратора*)

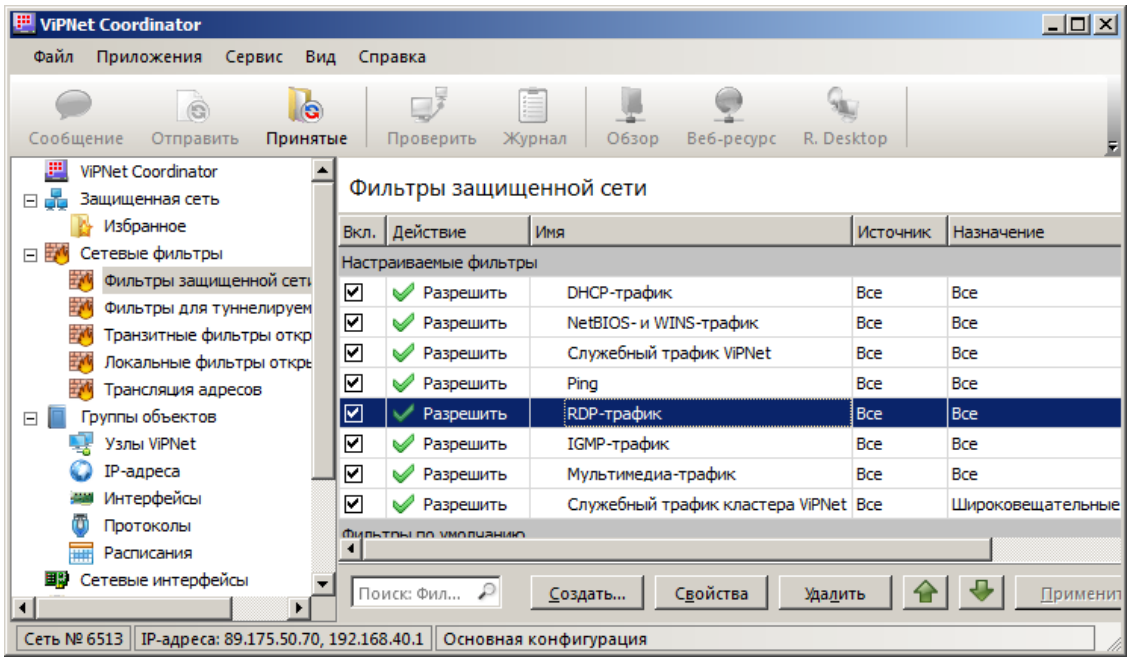

Рисунок 1 – Предустановленные фильтры защищенной сети на координаторе

Порядок выполнения задания

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

1. В окне программы ViPNet Монитор на панели навигации выберите раздел *Сетевые фильтры* > *Фильтры защищенной сети*.
2. На панели просмотра выберите фильтр разрешающий доступ по RDP, два раза щелкните по фильтру, после чего он откроется для редактирования.
3. В разделе Основные параметры укажите действие: *Блокировать трафик (Рисунок 148)*.

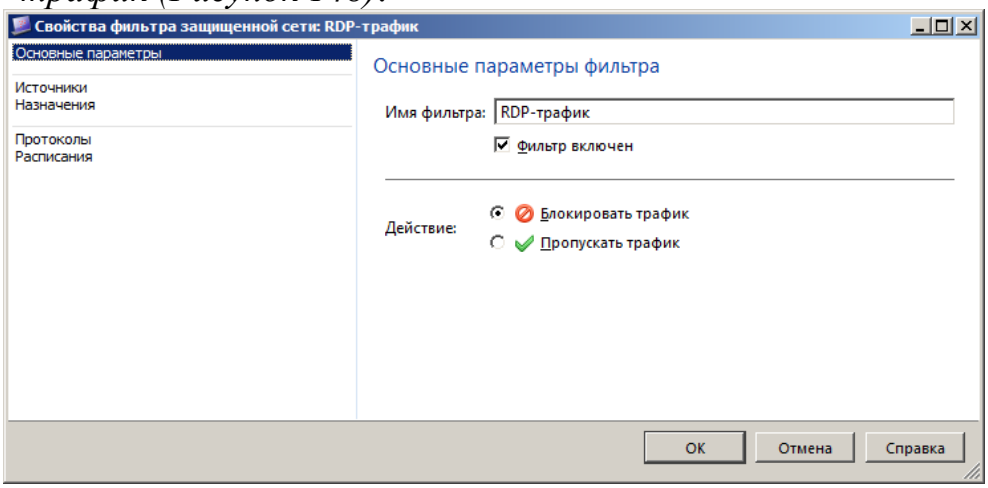

Рисунок 2 – Редактирование фильтра *RDP*

4. Введите IP-адреса узла *Координатор Центр офис* в диалоговом окне *Подключение к удаленному рабочему столу* на узле *Координатор Филиал*, после чего окно авторизации на удаленном узле (*Координатор Центр офис*) не должно открыться.
5. Зайдите в журнал регистрации IP-пакетов на *Координатор Центр офис*, отфильтруйте по порту 3389. Проанализируйте ситуацию.