МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«14» сентября 2017 г.

СЕТЕВЫЕ ФИЛЬТРЫ.

Методические указания по выполнению практической работы по дисциплине «Безопасность электронного документооборота» для студентов специальности 38.05.01.

Курск 2017

УДК 004
Составители: И.В. Калуцкий, А.А. Чеснокова

Рецензент
Кандидат технических наук, доцент кафедры
защиты информации и систем связи *А.Г. Спеваков*

Сетевые фильтры: Методические указания по выполнению практической работы по дисциплине «Безопасность электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, А.А. Чеснокова. Курск, 2017. 26 с.: ил. 8. Библиогр.: с. 25

Содержат сведения по вопросам настройки и управления фильтрами для защищенных и открытых сетей, а так же основные правила фильтрации.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности и направлению подготовки «Экономическая безопасность».

Предназначены для студентов специальности 38.05.01 дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать 24.04.17 . Формат 60x84 1/16.
Усл.печ.л. 2,32 .Уч. –изд.л. 2,10 .Тираж 30 экз. Заказ . Бесплатно. 1391
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Нельзя не сказать об угрозах защищаемому компьютеру из сети Internet: как входящие на компьютер данные могут нанести вред ему, так и выходящая за предел информация может потерять свою ценность. Однако можно найти решение ряд проблем с безопасностью в Интернете, или, по крайней мере, сделать их менее опасными, если использовать существующие и хорошо известные технологии и меры защиты на уровне хостов. Брандмауэр может значительно повысить уровень безопасности сети организации и сохранить в то же время доступ ко всем ресурсам Интернете.

Несмотря на то, что VPN сети считаются более защищенными по сравнению с обычной сетью, в них так же существует проблема контролирования входящих и исходящих данных. Если решением для обычно сети будет брандмауэр, то каким решением будет для виртуальной сети?

Для виртуальной сети ViPNet такое решение есть – сетевой фильтр. Сетевой фильтр позволяет контролировать данные, циркулирующие в сети, а так же блокировать данные с неизвестных источников. Так же в сетевых фильтрах ViPNet возможна гибкая настройка, что позволяет создавать фильтры для любых целей, будь-то блокирование данных с определенного порта или работа сетевого фильтра по расписанию.

Однако, для того, чтобы настраивать сетевые фильтры необходимо иметь представления о правилах фильтрации в сети ViPNet. Именно об этом и пойдет речь в лабораторной работе.

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – усвоить правила фильтрации и способы настройки сетевых фильтров, которые в дальнейшем позволить защитить сеть ViPNet от сетевых атак и несанкционированного доступа.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Описать со скриншотами предметную область
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Описание предметной области со скриншотами
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Общие сведения о фильтрах

Фильтры предназначены для блокирования/пропускания IP-пакетов в зависимости от протокола, параметров протокола, направления соединения или направления пакета, внешних адресов пакета, времени прохождения пакета.

Основные принципы фильтрации

Фильтрации подвергается весь трафик, который проходит через узел:

- открытый (нешифрованный) трафик (локальный или транзитный);
- защищенный трафик (перед его шифрованием и после расшифровки):
- туннелируемый трафик (перед его шифрованием и после расшифровки);

Существуют 4 режима фильтрации:

В **первом режиме** блокируется весь открытый IP-трафик без исключений.

Во **втором режиме** блокируется весь IP-трафик, за исключением следующих соединений:

- все соединения для работы службы DHCP в независимости от направления соединения по протоколу UDP и портам источника и назначения 67-68;
- исходящие соединения netbios-ns по протоколу UDP с портами источника и назначения 137;
- исходящие соединения netbios-dgm по протоколу UDP с портами источника и назначения 138;
- исходящие соединения для работы службы DNS по протоколу UDP с любым портом источника и 53 портом назначения;

В **третьем режиме** пропускаются все исходящие соединения и входящие соединения службы DHCP (протокол UDP, порты источника и назначения 67-68).

В **четвертом** режиме разрешен весь открытый IP-трафик, защита снята.

Для того чтобы правильно настроить правила фильтрации, необходимо понимать основные принципы фильтрации трафика различного типа:

1. Наибольшую опасность представляет трафик из открытой сети, где при умелом действии атакующего источник атаки очень сложно обнаружить. Также непросто принять адекватные оперативные меры по пресечению атаки. Поэтому такой трафик подвергается последовательной комплексной фильтрации:

- Правила фильтрации открытого IP-трафика, в том числе трафика между координатором и туннелируемыми устройствами, являются результатом действия:
  - выбранного режима безопасности для каждого сетевого интерфейса;
  - списка сетевых фильтров для соединений;
  - системы обнаружения атак;
- Фильтрация трафика осуществляется с учетом установленных соединений. Соединение устанавливается, когда в соответствии с правилами фильтрации трафика пропускается входящий или исходящий IP-пакет. Параметры такого IP-пакета регистрируются. На основании этих параметров создается временное правило для пропускания последующих пакетов в прямом и обратном направлении. Правило существует, пока есть трафик, соответствующий параметрам данного соединения.
  - Кроме того, в рамках созданного соединения по протоколам TCP, UDP, ICMP всегда пропускаются следующие ICMP-сообщения об ошибках.
  - Блокирующие правила системы обнаружения атак – если обнаружена атака, то пакет блокируется, иначе – следующая проверка.
  - Пропускающее правило Антиспуфинга – если IP-пакет имеет адрес, разрешенный правилом Антиспуфинга, пакет пропускается. В противном случае – блокируется.

- Блокирующее правило первого режима безопасности – если на сетевом интерфейсе включен первый режим, то пакет блокируется, иначе – следующая проверка.
- Правило второго режима безопасности направляет пакет на дальнейшую проверку.
- Пропускающее правило третьего режима безопасности – если на сетевом интерфейсе включен третий режим и это исходящий локальный пакет, то пакет пропускается, иначе следующая проверка.
- Пропускающее правило четвертого режима безопасности – если на сетевом интерфейсе включен данный режим и это локальный пакет, то пакет пропускается.
- Пропускающее правило пятого режима безопасности – если на сетевом интерфейсе включен данный режим, то пакет пропускается.
- Блокирующие и пропускающие правила пользователя – если пакет соответствует одному из правил фильтрации, заданных пользователем, то пакет пропускается или блокируется в соответствие с этим правилом, иначе – следующая проверка.
- Блокирующее правило для всех открытых пакетов – пакет, не соответствующий ни одному из предыдущих правил, блокируется.

2. Внутри защищенной сети (в том числе для туннелируемых ресурсов со стороны защищенной сети), благодаря криптографической аутентификации трафика, невозможно провести атаку, источник которой нельзя было бы однозначно идентифицировать и устранить.

- Любые правила фильтрации применяются к IP-пакетам только после их успешной расшифровки и идентификации сетевого узла-источника. В этом случае IP-адреса сетевых узлов не имеют никакого значения. Также для координатора не имеет значения, со стороны какого сетевого интерфейса находятся те или иные узлы.
- Поэтому трафик между защищенными узлами проходит только фильтры , заданные по умолчанию или настроенные пользователем. Эти сетевые фильтры не зависят от сетевого ин-

терфейса, с которого поступил пакет, и определяют правила пропускания трафика для конкретных протоколов, портов и направления передачи. Эти правила в основном предназначены для разграничения прав пользователей защищенных узлов сети ViPNet.

Структура фильтров для открытого трафика (в том числе трафика между координатором и его туннелируемыми устройствами) отличается от структуры фильтров защищенной сети.

Выбор режима безопасности (раздел Режимы)

Программа ViPNet Client [Монитор] имеет несколько режимов безопасности. Режим безопасности определяет типовое правило фильтрации открытого трафика, которое в дальнейшем можно модифицировать настройками сетевых фильтров для пакетов определенного типа (для конкретных адресов, протоколов и портов) в окне ***Открытая сеть.***

В защищенной сети трафик считается доверенным, поэтому по умолчанию любой трафик с защищенными узлами, с которыми связан Ваш сетевой узел (в окне ***Защищенная сеть***), разрешен без каких-либо ограничений в любом режиме безопасности.

Для работы в открытой сети предусмотрено три основных рабочих режима безопасности:

- 1 режим **Блокировать IP-пакеты** всех соединений. В этом режиме любой открытый трафик блокируется, независимо от сетевых фильтров, настроенных в окне ***Открытая сеть***. Это режим максимальной защиты компьютера и эквивалентен физическому отключению Вашего компьютера от открытых источников сети. Компьютер доступен только для узлов защищенной сети.
- 2 режим **Блокировать все соединения кроме разрешенных.** В этом режиме без дополнительных настроек сетевых фильтров в окне ***Открытая сеть*** Ваш компьютер не сможет взаимодействовать с другими открытыми ресурсами. По умолчанию, разрешены лишь некоторые безопасные типы трафика, позволяющие компьютеру получить IP-адрес и подготовиться к работе в локальной сети. Компьютер доступен

для взаимодействия с узлами защищенной сети. Данный режим обычно используется опытными пользователями для тонкой настройки самых необходимых видов открытого трафика.

- 3 режим **Пропускать все исходящие соединения кроме запрещенных** (Бумеранг). В этом режиме по умолчанию пропускаются все инициативные исходящие открытые соединения с Вашего компьютера, и блокируется любой несанкционированный входящий трафик. Данный режим предназначен для использования на сетевых узлах, которые должны взаимодействовать с другими узлами защищенной сети и иметь возможность получать безопасный доступ к открытым ресурсам локальной или внешней сети.
-

Для тестовых целей существуют следующие режимы:

- 4 режим **Пропускать все соединения**. В этом режиме компьютер не защищен от несанкционированного доступа из сети, независимо от сетевых фильтров, настроенных в окне ***Открытая сеть***, но может взаимодействовать с узлами защищенной сети. Режим предназначен для тестовых кратковременных проверок.
- 5 режим **Пропускать IP-пакеты без обработки**. В этом режиме отключается вся криптографическая обработка трафика и его фильтрация. Режим предназначен для тестовых кратковременных проверок. В этом режиме не ведется журнал регистрации IP-пакетов.

По умолчанию ViPNet Client [Монитор] устанавливается в 3 режим – **Пропускать все исходящие соединения кроме запрещенных**. Режим 3 является оптимальным режимом защиты и при этом практически во всех случаях обеспечивает всю необходимую функциональность компьютера при его работе в сети.

Установка режима безопасности работы Вашего компьютера в сети производится в окне

Режимы.

Для выбора режима, следует установить переключатель напротив нужного режима. Если требуется, чтобы при последующих запусках ViPNet Client [Монитор] устанавливался такой же режим, то выберите этот режим из выпадающего списка ***При старте программы.***

Для сохранения изменений нажмите кнопку **Применить**.

Внимание! При смене конфигурации устанавливается тот режим обработки открытых IP-пакетов, который в момент создания (сохранения) конфигурации был выбран в списке **При старте программы** в разделе **Режимы**.

Сетевые фильтры

Чтобы блокировать или пропускать IP-пакеты в зависимости от IP-адреса отправителя, используемого протокола или порта, требуется настроить фильтрацию сетевого трафика.

10 Windows Security Center (Центр обеспечения безопасности Windows) – компонент Windows XP (SP2) и Windows Vista, предназначенный для централизованного управления параметрами безопасности компьютера.

Сетевые фильтры создаются отдельно для защищенного, открытого и туннелируемого трафика. Древовидная структура сетевых фильтров представлена на правой панели окна ViPNet [Монитор], если на левой панели выбраны элементы **Защищенная сеть**, **Открытая сеть** или **Туннелируемые ресурсы**.

Основные отличия сетевых фильтров для открытого трафика (в том числе трафика между туннелируемым узлом и координатором, за которым этот узел расположен) от фильтров защищенной сети:

- Фильтрация открытого трафика для всех протоколов осуществляется в соответствии с установленными соединениями. Если фильтром разрешен некоторый трафик в определенном направлении, для пропускания такого трафика создается временное соединение.

Автоматически будет пропущен и ответный трафик, удовлетворяющий параметрам данного соединения. При фильтрации защищенного трафика такое правило действует для всех протоколов: TCP, UDP, ICMP.

- Фильтры открытого трафика могут быть применены к различным сетевым интерфейсам координатора. Фильтры защищенной сети к интерфейсам не привязаны.

- Фильтры открытого трафика действуют в соответствии с порядком их размещения внутри каждой группы для разных типов трафика, и этот порядок можно изменять. Логика работы фильтров защищенной сети носит более жесткий характер.
- Фильтры открытого и защищенного трафика имеют двухуровневую структуру.
- Фильтр открытого трафика первого уровня, называемый правилом доступа, определяет адреса и интерфейсы, на которые распространяют свое действие фильтры протоколов, создаваемые на втором уровне. Фильтры протоколов привязаны к конкретным правилам доступа и определяют действие фильтра в соответствии с заданными параметрами: протокол, порты, типы, коды, направление соединения, расписание действия данного фильтра.
- Для защищенного трафика фильтр первого уровня определяет действие (пропускать или блокировать) для всех фильтров протоколов, создаваемых на втором уровне. Для фильтров защищенного трафика не задается расписание действия фильтра.

Общие сведения о фильтрах защищенной сети

В разделе **Защищенная сеть** по умолчанию определены следующие правила доступа (фильтры первого уровня):

- **IP-пакеты всех адресатов** – основной фильтр для всех узлов сети ViPNet. С его помощью можно разрешить или заблокировать трафик со всеми сетевыми узлами ViPNet, перечисленными в окне **Защищенная сеть**.
- **Широковещательные IP-пакеты всех адресатов** – фильтр для широковещательных IP-пакетов от сетевых узлов, перечисленных в окне **Защищенная сеть**.
- Действие этого фильтра зависит от связанных с ним фильтров протоколов.

- По умолчанию фильтр **Широковещательные пакеты всех адресатов** пропускает только те широковещательные пакеты, которые соответствуют заданным по умолчанию фильтрам протоколов:

  - Фильтры netbios-ns (порт 137) и netbios-dgm (порт 138) обеспечивают пропускание пакетов службы NetBIOS, которая осуществляет регистрацию и проверку имен компьютеров в локальной сети.
  - Служба DHCP – фильтры bootps, (порт 67) и bootps (порт 68) обеспечивают пропускание пакетов службы DHCP, которая позволяет компьютерам автоматически получать IP-адреса для работы в сети.
  - Фильтр iplirdatagram (порт 2046) обеспечивает пропускание служебных пакетов сети ViPNet.
  - Фильтр clusterdatagram (порт 2060) обеспечивает пропускание служебных пакетов кластера ViPNet (этот фильтр отображается только при использовании ПО ViPNet Cluster).

- **Индивидуальные фильтры для каждого сетевого узла** – фильтры для конкретных узлов ViPNet. Индивидуальные фильтры задаются отдельно для каждого узла из списка узлов в окне **Защищенная сеть**.
- С помощью индивидуальных фильтров можно запретить обмен трафиком с каким-либо узлом ViPNet, даже если этот трафик разрешен основным фильтром. Также можно разрешить пропускание трафика, который блокируется основным фильтром.

Для каждого из фильтров первого уровня можно добавить следующие фильтры:

- Фильтры протоколов (некоторые из них добавлены по умолчанию). Фильтр протоколов определяет правила фильтрации IP-пакетов по протоколу, направлению установления соединения и номеру порта.
- Для индивидуальных фильтров можно также добавить фильтр Microsoft SQL.Фильтр Microsoft SQL действует только при установке ПО ViPNet Client на компьютер, на котором также

установлен Microsoft SQL Server, и работает на уровне протокола TDS (протокол передачи данных MS SQL).

В защищенной сети действие фильтра протоколов всегда противоположно действию фильтра первого уровня. То есть фильтр первого уровня определяет, следует ли пропускать или блокировать пакеты данного типа для всех протоколов, кроме протоколов, которые определяются фильтром второго уровня (фильтром протоколов). К протоколам, заданным в фильтре второго уровня, всегда применяется действие, противоположное действию фильтра первого уровня.

Фильтр Microsoft SQL применяется только в том случае, если соответствующий пакет был пропущен другими фильтрами.

Фильтры первого уровня нельзя удалять. Однако при наличии соответствующих полномочий можно инвертировать их действие (Подробнее о полномочия см. приложение к документации ViPNet "Классификация полномочий", глава "Интерпретация полномочий программами Монитор"). При этом действие всех фильтров протоколов, связанных с данным фильтром первого уровня, также будет инвертировано. Фильтры протоколов можно изменять или удалять.

Общие сведения о фильтрах открытой сети

В окне **Открытая сеть** представлены следующие типы фильтров:

- **Локальные фильтры** определяют правила фильтрации для открытых нешироковещательных IP-пакетов, которыми ViPNet-узел обменивается с внешними устройствами.
- **Широковещательные фильтры** определяют правила фильтрации широковещательных пакетов.

Фильтры в окнах **Открытая сеть** состоят из правил доступа и связанных с ними фильтров протоколов. Правило доступа определяет IP-адреса узлов и IP-адреса сетевых интерфейсов координатора, на которые распространяется действие фильтра. Фильтры протоколов задают параметры фильтрации и определяют, пропускать или блокировать соответствующие IP-пакеты.

Фильтры протоколов можно легко создавать, изменять и удалять. Также можно создавать дополнительные правила доступа.

При работе с фильтрами для открытой сети и туннелируемых ресурсов следует учитывать следующие обстоятельства:

- Настройки фильтров каждого типа независимы друг от друга.
- Внутри группы проверка соответствия пакета правилам фильтрации выполняется по порядку сверху вниз в соответствии с расположением правил в списке. Когда пакет блокируется или пропускается первым подходящим правилом, последующие фильтры уже не оказывают никакого влияния на данный пакет. Правила можно свободно перемещать и копировать внутри группы.
- Внутри правила проверка соответствия пакета фильтрам протоколов также выполняется по порядку сверху вниз в соответствии с положением фильтров протоколов в списке. Когда срабатывает первый подходящий фильтр протокола, последующие фильтры не оказывают на данный пакет никакого влияния. Фильтры протоколов могут свободно перемещаться и копироваться пользователем внутри своего правила доступа.

Фильтры, созданные по умолчанию

В программе ViPNet Client по умолчанию определены следующие фильтры:

1. В группе **Локальные фильтры**:

- **<Все IP-адреса>** . Это правило содержит фильтры протоколов с действием **Пропускать**, разрешающие создание соединений для локальных нешироковещательных пакетов следующих протоколов и направлений:
  - Исходящие пакеты bootps (порт 67) и входящие пакеты bootpc (порт 68),предназначенные для организации работы службы DHCP (автоматическое назначение IP-адресов).
  - Пакеты netbbios-dgm (порт 138), предназначенные для организации работы службы NetBIOS, осуществляющей регистрацию и проверку имен компьютеров в локальной сети.
- **Windows Mobile-based device**. Это правило содержит фильтры протоколов с действием **Пропускать**, предназначенные

для обеспечения синхронизации компьютера с КПК (на базе Windows Mobile 5.0/6.0) при помощи ActiveSync 4.x (или Windows Mobile Device Center на Windows Vista). По умолчанию это правило выключено, включать его следует только для синхронизации с КПК.

2. В группе **Широковещательные фильтры** правило **< Все IP-адреса>**. Это правило содержит фильтры протоколов с действием **Пропускать**, разрешающие создание соединений для локальных широковещательных пакетов следующих протоколов и направлений:

- Исходящие пакеты bootps (порт 67) и входящие пакеты bootpc (порт 68), предназначенные для организации работы службы DHCP (автоматическое назначение IP-адресов).
- Пакеты netbios-ns (порт 137) и netbios-dgm (порт 138), предназначенные для организации работы службы NetBIOS, осуществляющей регистрацию и проверку имен компьютеров в локальной сети.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Фильтры для защищенной сети

Для начала рассмотрим настройку фильтров в защищенной среде. Для этого запускаем VIPNet Monitor и выбираем слева вкладку Защищенная сеть.

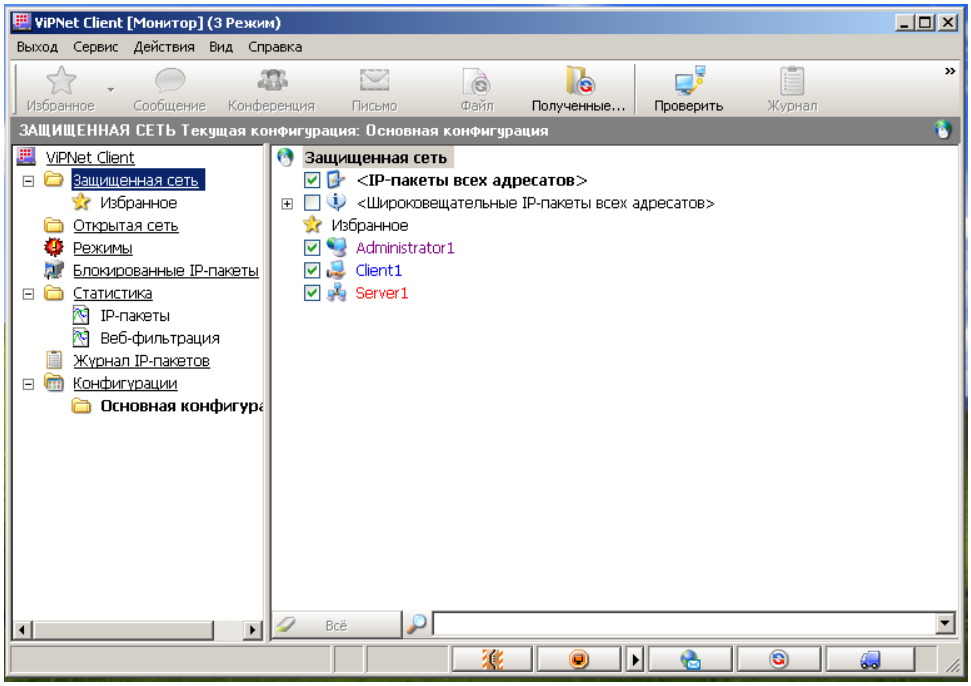

Рис.1 – Окно Защищенная сеть

В правом окне появляются пункты, которые отвечают за весь IP-трафик и широковещательные фильтры, а так же во вкладке Избранное отображаются все АП и СУ, работающие в данной сети.

Пункт IP-пакеты всех адресатов – это основной фильтр для всех узлов сети ViPNet. С его помощью можно разрешить или заблокировать трафик со всеми сетевыми узлами ViPNet, перечисленными в окне **Защищенная сеть**. Для его настройки необходимо правой кнопкой мыши на данном пункте и выбрать правило доступа/добавить фильтр протоколов.

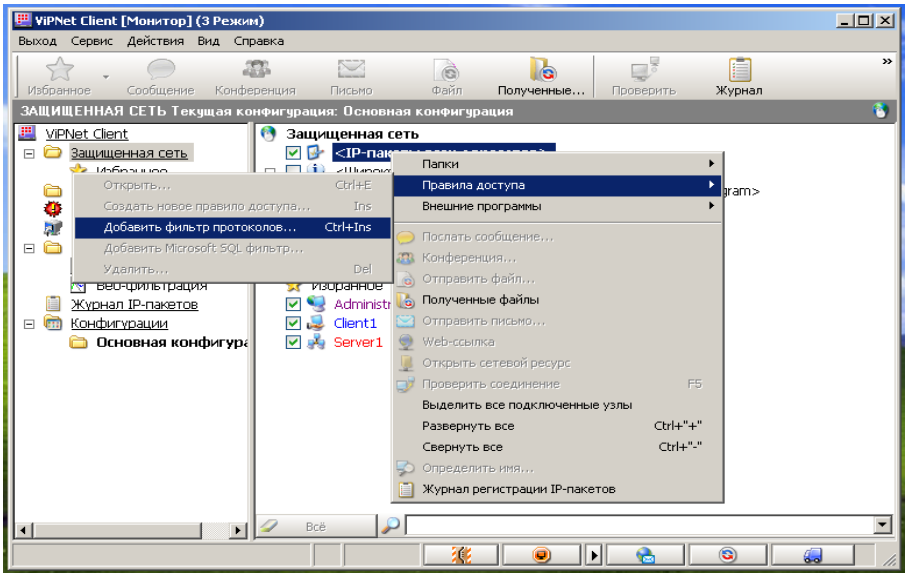

Рис.2 – Добавление фильтра протокола

Далее появится окно настройки правил доступа:

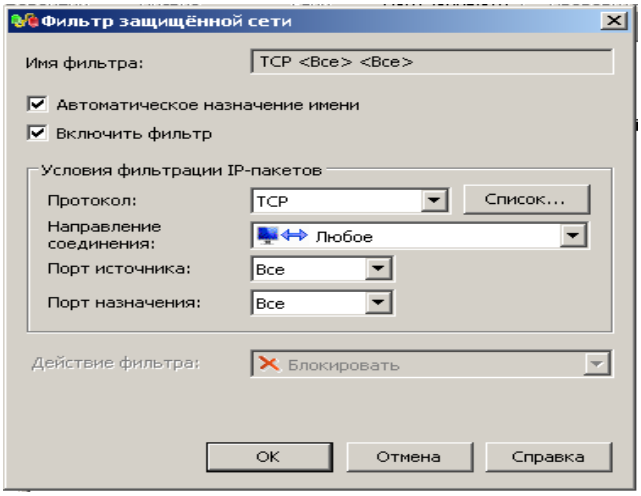

Рис.3 – Настройка фильтра защищенной сети

У всех сетевых фильтров есть две функции: они могут или полностью блокировать входящий трафик, или принимать его от всех соединений. Так же, можно настроить фильтр таким образом, чтобы он не принимал (или принимал) трафик с определенных портов. Настройка фильтров производится следующим образом:

1. Для начала необходимо указать имя фильтра. Если выбран пункт Автоматическое назначение имени, то имя устанавливать не надо.

2. Так же имеется возможность отключать фильтр.

3. Фильтрацию можно настроить на прием данных с определенных протоколов. Выделяют три основных протокола:TCP, UDP, ICMP.Так же, можно задать и другие.

4. Можно указать, на запрет (или разрешения) какого трафика действует фильтр: исходящего или входящего.

5. В пунктах Порт источника и пункт приемника можно указать номера портов, которые будут блокироваться или пропускаться. Существуют три способа установки порта: номер, диапазон и все. В пункте номер можно указать порт по своему вкусу. При выборе пункта диапазон можно указать диапазон портов, на которые будет действовать фильтр. Соответственно, при выборе вкладки “ВСЁ” будут блокироваться все порты.

Таким образом, можно заблокировать любые порты во всей сети.

Для настройки данного фильтра необходимо щелкнуть правой кнопкой мыши по пункту Широковещательные фильтры, а затем выбрать пункт **Правила доступа/Добавить фильтр протоколов.**

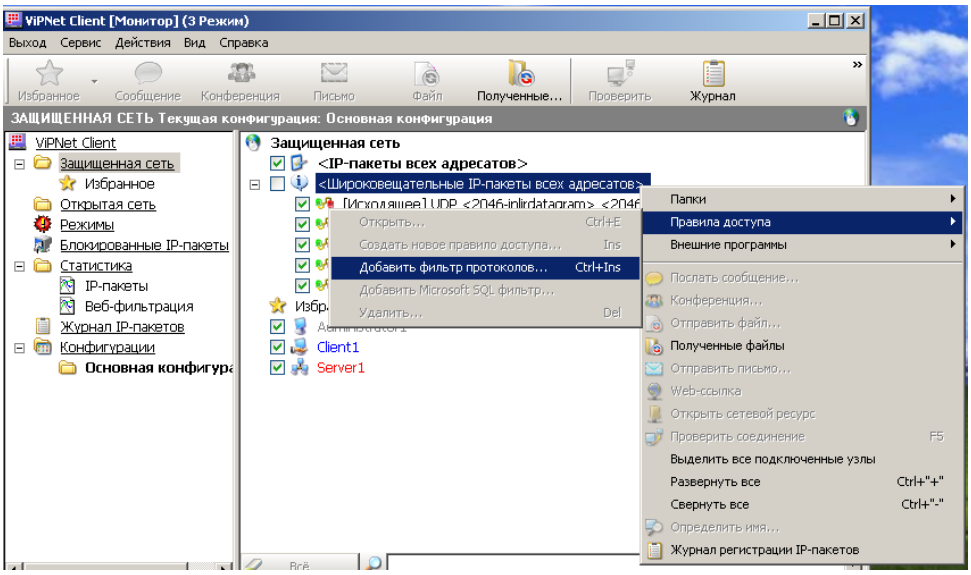

Рис.4 – Создание фильтра защищенной сети

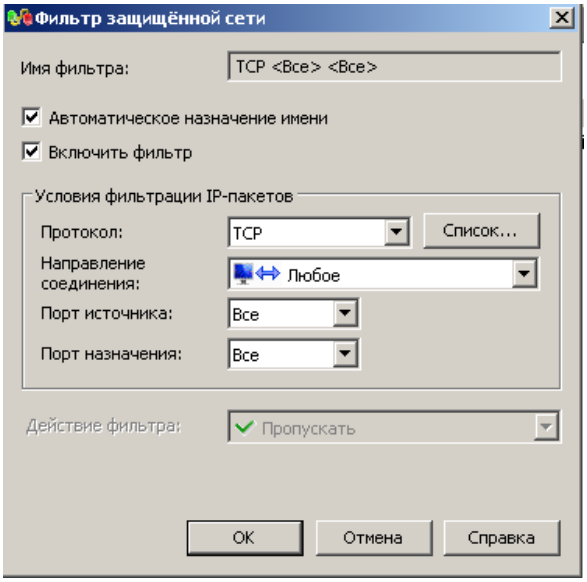

Рис.5 – Настройка фильтров защищенной сети

Настройка данного фильтра производится аналогично настройке фильтра Защищенной сети.

Для настройки индивидуальных фильтров необходимо из вкладки Избранное выделить СУ, для которого необходимо его создать. Для этого выбираем СУ из списка, щелкаем правой кнопкой мыши и выбираем Правила доступа/Добавить фильтр протоколов. Настройка производится аналогично пункту 1.(т.е описание первого фильтра).Главным условием для настройки индивидуальных фильтров является наличие пользователя в сети. В противном случае вкладка для создания индивидуального фильтра будет неактивна.

Фильтры и правила доступа для открытой сети.

Теперь рассмотрим практическую реализацию фильтров для открытой сети.

Для начала рассмотрим настройку Локальных правил доступа. Для этого необходимо:

1. На левой вкладке выбрать пункт Открытая сеть.

2. Щелкнуть правой кнопкой мыши на пункте Локальные фильтры и выбрать Правила доступа /Создать новое правило доступа.

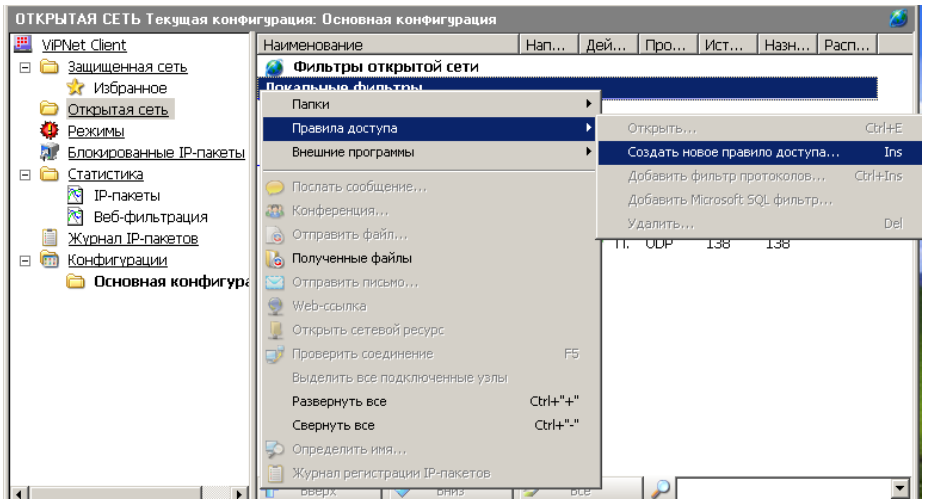

Рис.6 – Создание правила доступа для Открытой сети

3. Если вы хотите самостоятельно задать Имя правила, тогда необходимо снять флажок с пункта Автоматическое назначение имени.

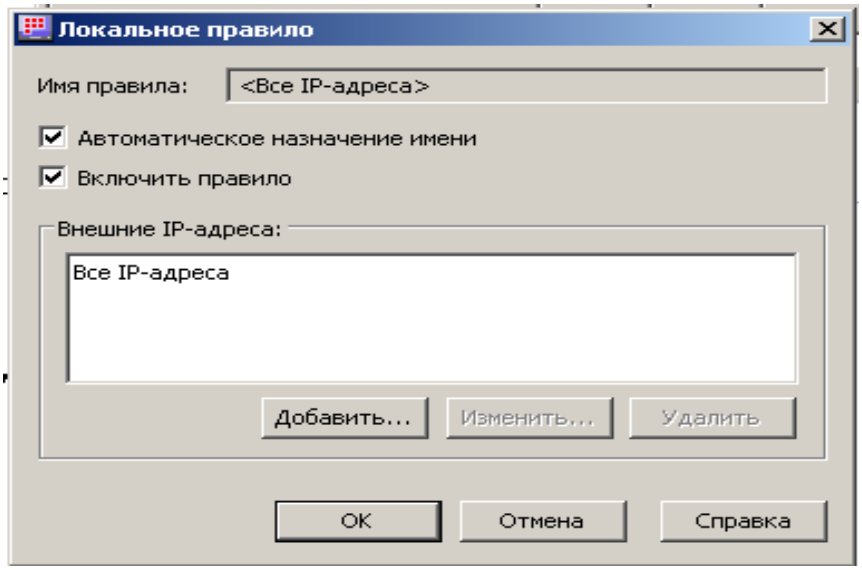

Рис.7 – Настройка правил доступа

4. Так же необходимо, чтобы флажок Включить правило был установлен, в противном случае правило будет выключено.

5. Необходимо задать IP-адреса внешних устройств, трафик с которыми должен фильтроваться в соответствии с создаваемым правилом.

Для добавления IP-адреса нужно:

1. Нажать кнопку Добавить.
2. В появившемся окне необходимо выполнить одно из следующих действий:

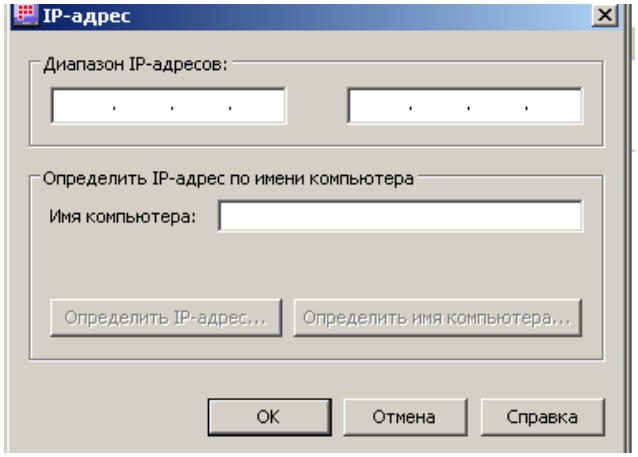

Рис.8 – Задание диапазон IP-адресов

В поле **Диапазон IP-адресов** введите IP-адрес или диапазон IP-адресов для фильтрации. При вводе диапазона IP-адресов задайте начальный и конечный адрес диапазона.

А. Вы можете нажать кнопку **Определить имя компьютера**, чтобы найти имя компьютера по введенному IP-адресу. Если удастся определить имя компьютера, оно отобразится в поле **Имя компьютера**, в противном случае в окне **Поиск компьютера** будет выдано сообщение о неудаче.

Если вы не знаете IP-адресов, но знаете сетевые имена компьютеров или их URL-адреса (для веб-сайтов, FTP-серверов и пр.):

В поле **Имя компьютера** введите имя или URL-адрес компьютера, трафик с которым должен фильтроваться в соответствии с создаваемым правилом.

Нажмите кнопку **Определить IP-адрес**, чтобы найти IP-адрес компьютера по введенному имени. Если удастся определить IP-адрес компьютера, он отобразится в поле **Диапазон IP-адресов**, в противном случае в окне **Поиск компьютера** будет выдано сообщение о неудаче.

Таким образом, можно создавать правила фильтрации для локальных и широковещательных сетей. Настройка локальных и широковещательных фильтров производится аналогично настройке фильтров в защищенной сети.

ВАРИАНТЫ ЗАДАНИЙ

1. Создать фильтр протоколов для защищенной сети для всех IP-адресов. Фильтр должен блокировать входящие соединения протокола ICMP с любого порта источника на порт приемника 25.
2. Создать локальный фильтр для открытой сети. Фильтр должен пропускать любые соединения протокола TCP. Настроить время работы фильтра с 8 до 18.
3. Создать локальное правило для IP-адресов своей сети. Добавить фильтр протоколов для блокирования входящего соединения протокола TCP и настроить время работы с 13 до 14.
4. Создать фильтр протоколов для защищенной сети для широковещательной сети. Фильтр должен пропускать любые соединения протокола UDP.
5. Создать локальный фильтр протоколов для открытой сети. Фильтр должен блокировать любые соединения протокола ICMP.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего предназначены сетевые фильтры? Основные правила фильтрации трафика.
2. Режимы безопасности. Рассказать о четырех режимах безопасности.
3. Фильтры для защищенной сети. В чем заключается особенность каждого из фильтров?
4. Фильтры для открытой сети. В чем заключается их особенность?
5. Как настраиваются сетевые фильтры?
6. Предназначение локальных и широковещательных фильтров.
7. Основные функции фильтров, созданных по умолчанию.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ViPNet Client [Монитор] версия 3.1 – Руководство пользователя [Электронный ресурс]/ - http://www.infotecs.ru.