Министерство образования и науки Российской Федерации

Федеральное агентство по образованию

Московский Государственный Технический Университет им. Н.Э. Баумана

Факультет «Информатика и системы управления»

Кафедра «Компьютерные системы и сети»

Сурков Л.В.

Методические указания к лабораторной работе

по курсу

Корпоративные сети

Защита сетевого трафика с использованием IPsec и сертификатов

2010

Содержание

Основы протокола IPsec

Назначение IPsec

Протокол IPsec– это открытый промышленный стандарт IP-сетей для защиты передаваемых по сетям IP-пакетов. IPsec является неотъемлемой частью протокола IPv6 и расширением существующей версии протокола IPv4. Протокол IPsec работает на сетевом уровне (уровень 3 модели OSI). Это делает IPsec гибким, поскольку он может использоваться для защиты любых протоколов, базирующихся на транспорте TCP/UDP.

IPSec обеспечивает аутентификацию источника данных, шифрование передаваемых IP пакетов, проверку их целостности и подлинности, защиту от навязывания повторных сообщений, а также частичную защиту от анализа трафика.

Реализация IPsec на сетевом уровне обеспечивает защиту для всех протоколов семейства TCP/IP, начиная с уровня IP и выше, передающих данные на уровне IP. Основным преимуществом защиты на этом уровне является то, что все приложения и службы, использующие IP для транспортировки данных, могут быть защищены с помощью IPsec без внесения каких-либо изменений в эти приложения или службы. Заметим, что для защиты других протоколов, отличных от IP, пакеты должны быть инкапсулированы в IP пакеты.

IPsec защищает данные так, что расшифровать их при несанкционированном доступе крайне трудно или просто невозможно. Высокий уровень безопасности достигается посредством использования криптографических алгоритмов и ключей

Фактически протокол IPsec представляет собой *комбинацию* нескольких групп протоколов:

- аутентификации,
- целостности данных (цифровых подписей),
- шифрования данных,
- обмена криптографическими ключами.

Служба IPsec использует протоколы безопасности AH и ESP, обеспечивающие проверку подлинности и защиту данных для каждого пакета IP.

Протокол обмена криптографическими ключами IKE (Internet Key Exchange) состоит из трех протоколов: ISAKMP, Oakley и SKEME.

Протокол согласования параметров виртуального канала и управления ключами (Internet Security Association Key Management Protocol — ISAKMP) обеспечивает общее

управление защищенным виртуальным соединением, включая согласование используемых алгоритмов криптозащиты, а также генерацию и распределение ключевой информации.

Протокол Oakley, основанный на алгоритме Диффи-Хеллмана, создает секретные ключи, используемые для защиты данных.

Описание службы IPSEC

IPsec добавляет возможности шифрования и аутентификации в стек протокола TCP/IP на более низком уровне, чем протоколы прикладного уровня (такие как SSL и TLS: Secure Socket Layer и Transport Layer Security). Поскольку процесс защиты осуществляется на нижнем уровне стека TCP/IP, защита IPsec прозрачна для приложений. Для защиты приложений средствами IPsec необходимо, чтобы они передавали информацию через определенный порт. Если для всех соединений приложения применяют произвольные порты, определить фильтр IPsec, идентифицирующий потоки сетевых данных этих программ, практически невозможно.

Приложения не обязательно должны быть IPsec-совместимы, так как данные от клиента к серверу передаются открытым текстом. Процесс IPsec шифрует полезные данные пакета после их отправки приложением-клиентом и расшифровывает до того, как они достигнут приложения на сервере.

Согласование безопасности IPSEC

Перед началом безопасного обмена данными между двумя хостами должно быть установлено соглашение о способе обмена и защиты данных, которое принимается в процессе переговоров. Это соглашение называется *сопоставлением безопасности* SA (Security Associations)—безопасное соединение, представляющее собой виртуальный однонаправленный канал для передачи данных. Для двунаправленной связи требуется два SA. Как показано на рисунке 1, путем сопоставления безопасности два хоста принимают соглашение о способе обмена и защиты данных.

Для создания соглашения между двумя компьютерами рабочая группа IETF ввела стандартный метод сопоставления безопасности и разрешения обмена ключами, сочетающий использование протокола ISAKMP (Internet Security Association and Key Management Protocol) и протокола создания ключей Oakley. ISAKMP централизует управление сопоставлением безопасности, сокращая время подключения. Oakley создает секретные ключи, используемые для защиты данных, и управляет ими. Для обеспечения успешной безопасной связи ISAKMP/Oakley выполняет две фазы согласования.

В первой фазе, или главном режиме (main mode), хосты аутентифицируют друг друга. На этом этапе два компьютера устанавливают первое сопоставление безопасности, называемое согласованием безопасности ISAKMP. Создается общий секретный ключ (основной ключ) для сопоставления безопасности ISAKMP. Обмен ключами как таковыми никогда не выполняется; передаются только общие сведения, необходимые группе Диффи-Хелмана для создания общего секретного ключа. Служба Oakley на каждом из хостов создает основной ключ, используемый для защиты проверки подлинности. Хосты выполняют попытку проверить подлинность предоставленных сведений.

Инициирующая сторона посылает отвечающей стороне предлагаемый список возможных уровней безопасности. Отвечающая сторона не может изменить предложение. В случае изменения предложения инициирующая сторона отклоняет сообщение отвечающей стороны. Отвечающая сторона либо отправляет ответ о принятии предложения, либо просто отбрасывает предложение и отправляет сообщение о том, что ни один из предложенных вариантов не был выбран. Затем процесс начинается сначала.

Сообщения согласования автоматически повторяются пять раз. Если допускается небезопасная связь с компьютерами, не поддерживающими IPSec, через три секунды устанавливается мягкое сопоставление безопасности. Если отклик ISAKMP будет получен до окончания цикла, мягкое сопоставление безопасности будет удалено и начнется согласование стандартного сопоставления безопасности.

Возможное число формируемых сопоставлений безопасности ограничено лишь ресурсами системы. Сопоставление безопасности ISAKMP используется для начала второго фазы согласования безопасности.

Во второй фазе, быстром режиме (quick mode), хосты договариваются, какой протокол будет использоваться для цифровой подписи и/или шифрования IP-пакетов. От имени службы IPSec согласовывается пара сопоставлений безопасности IPSec. Обновление сведений о ключе или создание нового ключа выполняется службой Oakley в том случае, если включен режим PFS, или ограничено время жизни ключа или закончился срок действия сопоставления безопасности ISAKMP.

Благодаря возможности использовать одно сопоставление безопасности ISAKMP для нескольких согласований сопоставления безопасности IPSec, процесс согласования безопасности выполняется очень быстро. Повторное согласование безопасности и проверка подлинности не требуются до тех пор, пока не закончится срок действия сопоставления безопасности ISAKMP. Число повторов определяется активной политикой IPSec.

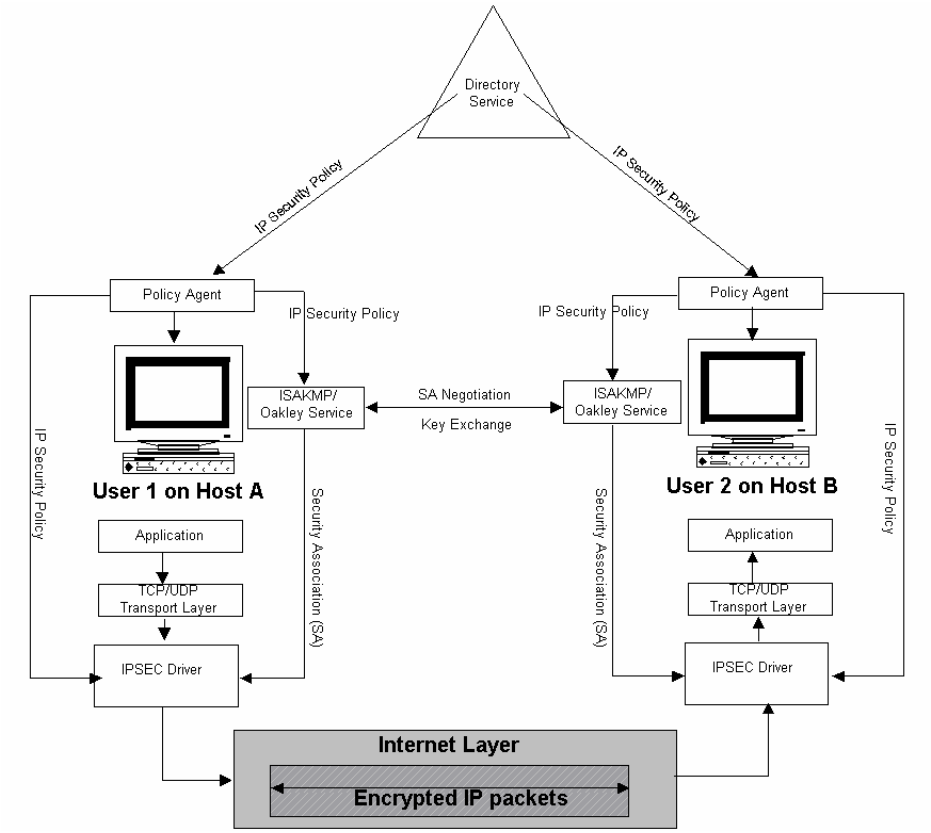

Рисунок 1 - Служба обеспечения безопасности IP Security

На рисунке 1 обозначены:

Directory Service – Служба каталогов

IP Security Policy – Политика безопасности IP

Policy Agent – Агент политики безопасности

IPSEC driver – Драйвер IPSEC

ISAKMP/Oakley Service – Служба ISAKMP/Oakley

SA Negotiation Key Exchange – Переговоры и обмен ключами

Application – Приложение

Transport Layer – Транспортный уровень

Internet Layer – Уровень Интернета

Encrypted IP packets – Зашифрованные IP-пакеты

По завершении времени жизни основного ключа или ключа сеанса соответствующее сопоставление безопасности согласовывается заново. Отвечающей стороне посылается сообщение Oakley, предписывающее отвечающей стороне пометить сопоставление безопасности ISAKMP как устаревшее. Это предотвращает создание недействительных сопоставлений безопасности IPSec из устаревшего сопоставления безопасности. Oakley помечает как устаревшие сопоставления безопасности ISAKMP, а драйвер IPSEC — сопоставления безопасности IPSec.

Обработка пакетов драйвером IPSEC

При загрузке агент политики Policy Agent IPSEC обновляет список фильтров IP, хранящийся в драйвере IPSEC. Все сопоставления безопасности, связанные с устаревшими фильтрами, более не существующими в политике, удаляются вместе с устаревшими фильтрами в кэше драйвера IPSEC.

Драйвер IPSEC получает список активных фильтров от агента политики IPSEC, а затем сверяет все входящие и исходящие пакеты с фильтрами в этом списке. Если пакет совпадает с фильтром, к нему применяется действие фильтра.

Если действие фильтра разрешает передачу, то пакет принимается или отправляется без изменений. Если действие блокирует передачу, пакет отбрасывается.

При обработке входящих и исходящих пакетов используются согласованные сопоставления безопасности и ключи. Драйвер IPSEC хранит все текущие сопоставления безопасности во внутренней базе данных. При наличии нескольких сопоставлений безопасности драйвер использует индекс параметров безопасности SPI для правильного применения сопоставлений безопасности к пакетам. Драйвер IPSEC защищает исходящий пакет IP и отправляет его на сетевую плату для передачи.

На рисунке 1 показана общая схема работы IPsec. Во время передачи пакетов с узла A на узел B выполняются следующие действия:

1. Драйвер IPSEC на компьютере A проверяет список фильтров IP в активной политике на наличие совпадающего адреса или типа трафика исходящих пакетов.
2. Драйвер IPSEC предоставляет ISAKMP сведения для начала согласования безопасности с компьютером B.
3. Служба ISAKMP на компьютере B получает запрос для согласования безопасности.
4. Два компьютера выполняют обмен ключами, устанавливают соответствие безопасности ISAKMP и создают общий секретный ключ.
5. Два компьютера согласовывают уровень безопасности для передачи данных, устанавливая пару соответствий безопасности IPSEC и ключей для защиты пакетов IP.
6. Используя сопоставление безопасности IPSEC для исходящего трафика и ключ, драйвер IPSEC на компьютере A подписывает пакеты для проверки целостности и зашифровывает пакеты, если было согласовано шифрование.
7. Драйвер IPSEC на компьютере A отправляет пакеты на соответствующий тип

подключения для передачи на компьютер B.

8. Компьютер B получает защищенные пакеты и передает их драйверу IPSEC.
9. Используя сопоставление безопасности IPSEC для входящего трафика и ключ, драйвер IPSEC на компьютере B проверяет подпись целостности и, при необходимости, расшифровывает пакеты.
10. Драйвер IPSEC на компьютере B передает расшифрованные пакеты драйверу TCP/IP, который передает их в принимающее приложение.

Для пользователей и прикладных программ все эти процессы не видны. Стандартные маршрутизаторы и коммутаторы, передающие данные между сторонами подключения, не требуют использования IPSEC. Они автоматически пересылают зашифрованные пакеты IP в место назначения.

Параметры политик безопасности и сопоставления безопасности SA хранятся в двух таблицах (рисунок 2):

- базе данных политик безопасности (SPD—Security Policy Database) и
- базе данных безопасных соединений (SAD—Security Association Database).

Записи в SPD определяют, в каких случаях нужно выполнить шифрование или контроль целостности, в то время как в SAD хранятся криптографические ключи, которые будут использованы для шифрования или подписи передаваемых данных. Если согласно SPD передаваемый пакет должен быть зашифрован, но в SAD нет соответствующего SA, служба IPsec по протоколу IKE согласовывает с другой стороной создание нового SA.

Документ RFC 4301 дополнительно определяет третью таблицу—базу данных для авторизации хостов (PAD, Peer Authorization Database), предназначенную для хранения сведений о хостах, которым разрешено создавать SA с данным хостом и о допустимых параметрах этих SA.

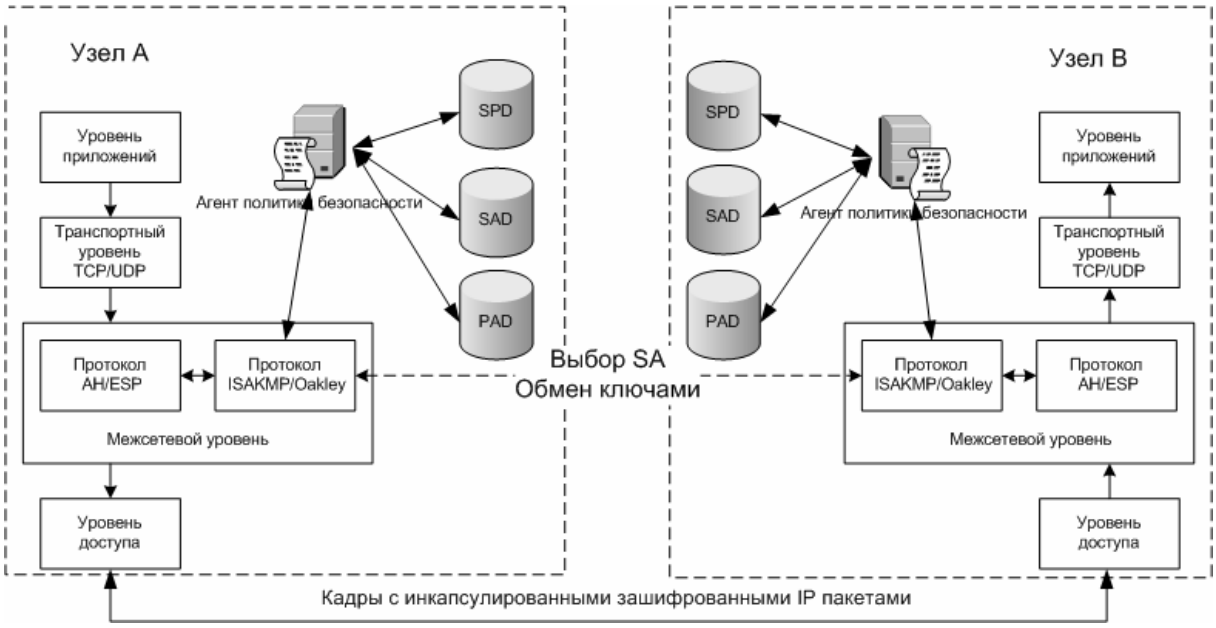

Рисунок 2 - Компоненты обеспечения безопасности IPsec

IPsec можно рассматривать как границу между внутренней (защищённой) и внешней (незащищённой) сетью. Эта граница может быть реализована как на отдельном хосте, так и на шлюзе, защищающем внутреннюю сеть. Заголовок любого пакета, проходящего через границу, анализируется на соответствие *политикам безопасности*, то есть критериям, заданным администратором сети. Пакет может быть либо передан дальше без изменений, либо уничтожен, либо обработан заданным образом с помощью протоколов защиты данных.

Защита даных

Для защиты передаваемого потока данных применяются два протокола:

- AH (Authentication Header—аутентифицирующий заголовок). Протокол предусматривает аутентификацию источника данных, проверку целостности и подлинности данных после приема, а также защиту от навязывания повторных сообщений, что гарантирует только целостность потока (передаваемые данные не шифруются).
- ESP (Encapsulating Security Payload—инкапсуляция зашифрованных данных). Протокол обеспечивает шифрование (конфиденциальность) передаваемых данных, а также выполнение всех функций протокола аугентифицирующего заголовка (AH).

Протоколы ESP и AH зарегистрированы организацией IANA (Internet Address Naming Authority) и занесены в реестр протоколов под порядковыми номерами 50 и 51 соответственно.

Протоколы защиты данных могут работать в двух режимах—в транспортном режиме и в режиме тунелирования. При работе в транспортном режиме IPsec работает только с информацией транспортного уровня TCP/UDP, в режиме туннелирования—с целыми IP-пакетами.

Аутентификация

Аутентификация (проверка подлинности) может выполняться тремя различными способами, используя:

- протокол безопасности **Kerberos V5**;
- **сертификаты** открытого ключа;
- **общий ключ** (парольная фраза).

Протоколы IPsec

Протокол обмена ключами IKE

Для согласования параметров и управления ключами при формировании общего защищенного канала и создании в его рамках отдельных защищенных соединений наибольшее распространение получил протокол ISAKMP (Internet Security Association Key Management Protocol — протокол управления ключами и контекстами безопасности в Internet). Данный протокол разработан организацией Internet Engineering Task Force (IETF) и определен в качестве обязательного стандарта по управлению ключами в спецификации IPSec протокола IPv6.При использовании ISAKMP снижается уязвимость закрытых основных ключей, служащих для распределения временных ключей шифрования.

Протокол ISAKMP описывает базовые процедуры аутентификации сторон, обмена ключами и согласования всех остальных параметров защищенного IPSec-туннеля. В IPSec в качестве протокола обмена ключами, используемого при формировании общего защищенного туннеля, выбран протокол Oakley, основанный на алгоритме Диффи-Хеллмана. Объединение протоколов ISAKMP и Oakley обозначают как ISAKMP/Oakley или IKE (The Internet Key Exchange — протокол обмена ключами в Internet).

В соответствии с протоколом ISAKMP согласование параметров защищенного взаимодействия необходимо как при формировании IPSec-канала, так и при создании в его рамках каждого защищенного однонаправленного соединения. Глобальные параметры защищенного канала образуют *управляющее сопоставление* и при их согласовании

помимо протокола ISAKMP используется протокол распределения ключей Oakley. Параметры каждого защищенного соединения согласуются на основе созданного управляющего сопоставления и образуют *сопоставление безопасности* SA. Криптографические ключи для каждого защищенного соединения, входящие в его контекст безопасности, генерируются на основе ключей, выработанных в рамках управляющего сопоставления. При этом учитываются также алгоритмы аутентификации и шифрования, которые будут использоваться в защищенном соединении.

Согласование глобальных параметров защищенного канала

Согласование глобальных параметров выполняется при формировании общего защищенного канала между сетевыми узлами. Эти параметры служат для создания в рамках сформированного туннеля отдельных защищенных соединений. В терминологии ISAKMP согласованные глобальные параметры защищенного туннеля называют *управляющим сопоставлением.*

Протокол ISAKMP предусматривает следующую последовательность действий по формированию управляющего сопоставления, образующего согласованные глобальные параметры защищенного туннеля (Рисунок 3).

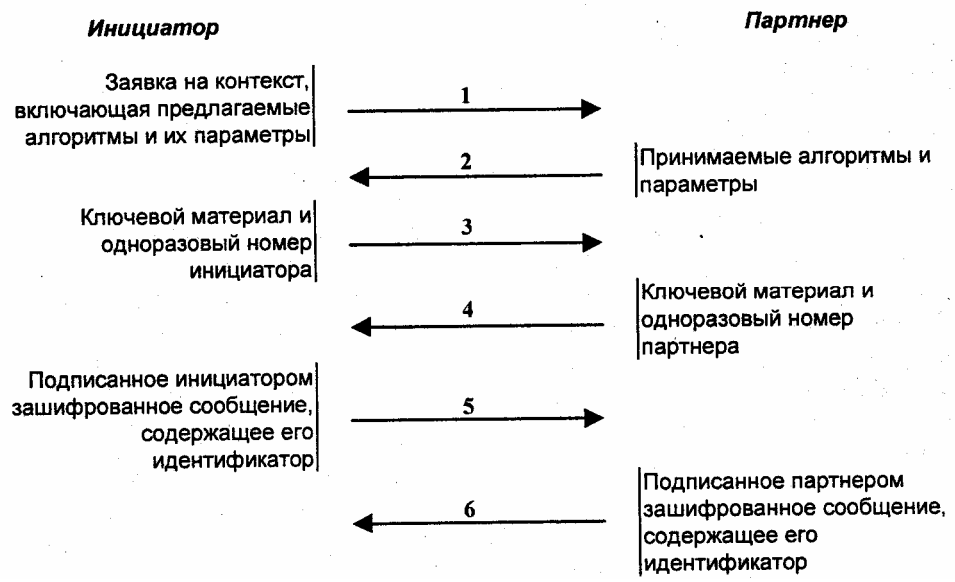

Рисунок 3 - Схема согласования глобальных параметров защищенного канала

При необходимости защищенного взаимодействия инициатор направляет противоположной стороне (партнеру) запрос на формирование защищенного канала, включающий предложения по набору защитных алгоритмов и их параметров (шаг 1). В запросе инициатора предложения по набору защитных алгоритмов и их параметров упорядочены по степени предпочтительности. В ответном сообщении (шаг 2) партнер

информирует о тех алгоритмах защиты и параметрах, которые его устраивают. Для каждой защитной функции (генерация и распределение ключей, аутентификация, шифрование) выбирается один алгоритм и его параметры.

На третьем и четвертом шагах взаимодействия инициатор и партнер отправляют друг другу свои открытые ключи, необходимые для выработки общего секретного ключа. В соответствии с протоколом Oakley для взаимодействующих сторон *A и B* этими открытыми ключами являются $\mathbf{y_A}$ ($\mathbf{y_A = a^{x}{}_A \bmod p}$) и $\mathbf{y_B}$ ($\mathbf{y_B = a^{x}{}_B \bmod p}$), где **a** и **p** **(a<p)** — заданные для защищенной виртуальной сети большие простые числа, а $\mathbf{x_A}$ и $\mathbf{x_B}$ — закрытые ключи абонентов *A и B,* сгенерированные как большие случайные числа. Общий секретный ключ вычисляется в соответствии со следующим выражением:

$$\mathbf{K_{AB}=(Y_A)^{X}{}_B \bmod p=(Y_B)^{X}{}_A \bmod p}$$

Открытые ключи направляются друг другу вместе со случайными одноразовыми номерами, служащими для защиты от воспроизведения сообщений.

На основе общего секретного ключа вырабатываются три вида ключей:

SKEYID_d - ключевой материал, используемый для генерации временных (протокольных) ключей для защищенных соединений;

SKEYID_a — сеансовые ключи, используемые для аутентификации сторон и согласовываемых параметров;

SKEYID_e — сеансовые ключи, используемые для шифрования согласовываемых параметров.

Пятый и шестой шаги формирования управляющего контекста служат для обмена идентификационной информацией, зашифрованной и подписанной по ключам SKEYID_e и SKEYID_a.

Формирование управляющего сопоставления защищенного канала на основе протокола ISAKMP/Oakley требует больших ресурсных затрат на вычисление общего секретного ключа, а также генерацию сеансовых ключей. Но за счет этого снижаются затраты на генерацию временных ключей для защищенных соединений. В зависимости от условий использования протокола ISAKMP/Oakley возможен компромисс между криптостойкостью и необходимым объемом вычислений. При формировании управляющего контекста на основе более коротких открытых ключей снижается объем вычислений, но по причине уменьшения криптостойкости также снижается и безопасность коммуникаций.

Протокол ISAKMP предусматривает не только защиту от нарушений конфиденциальности и подлинности согласовываемых глобальных параметров, но и

защиту от повтора, задержек и удаления защищенных сообщений. Для защиты от перечисленных атак применяются так называемые идентифицирующие цепочки. Эти цепочки формируются инициатором и его партнером с использованием текущего времени и присутствуют во всех ISAKMP-сообщениях.

<table>
<tr><td colspan="4">Идентифицирующая цепочка инициатора</td></tr>
<tr><td colspan="4">Идентифицирующая цепочка партнера</td></tr>
<tr><td>След.</td><td>Номер</td><td>Тип</td><td>Флаг</td></tr>
<tr><td colspan="4">Индикатор сообщения</td></tr>
<tr><td colspan="4">Длина</td></tr>
</table>

Рисунок 4 - Формат заголовка lSAKMP-сообщения

Как инициатор, так и партнер для каждого отправляемого сообщения генерирует на основе текущего времени свою идентифицирующую цепочку и вставляет ее в это сообщение (Рисунок 4). В каждое ответное сообщение помимо идентифицирующей цепочки отправителя вставляется также цепочка противоположной стороны, полученная в сообщении, для которого формируется этот ответ. При получении ответного сообщения получатель проверяет наличие посланной им идентифицирующей цепочки. При задании максимального времени следования ожидаемого сообщения использование идентифицирующих цепочек позволяет обнаружить повторные, задержанные и удаленные сообщения.

Для защиты от маскировки под санкционированного участника взаимодействия на третьем и четвертом шагах согласования глобальных параметров совместно с обменом открытых ключей должны выполняться функции проверки подлинности взаимодействующих сторон.

Для передачи ISAKMP-сообщений в спецификации IPSec определен протокол UDP с номером порта ***500***.

Согласование параметров каждого защищенного соединения

После создания общего защищенного канала параметры каждого защищенного соединения согласуются на основе сформированных глобальных параметров канала и образуют *сопоставление безопасности* SA. Каждое защищенное соединение, создаваемое в рамках общего защищенного канала, является однонаправленным соединением, т. е. соединением от отправителя пакета сообщения к его получателю. При этом в одном защищенном IPSec-соединении может быть использован только один из двух протоколов криптозащиты пакетов сообщений.

При симметричном взаимодействии партнерам придется сформировать как минимум два защищенных соединения, и соответственно два сопоставления безопасности SA — по одному в каждом направлении. Если протоколы криптозащиты AH и ESP используются вместе, то потребуется сформировать *четыре* контекста безопасности.

В состав согласовываемых параметров каждого защищенного соединения, образующих сопоставление безопасности, входят следующие элементы:

номер используемого протокола криптозащиты (AH, ESP или протокол криптозащиты, не входящий в спецификацию IPSec);

номера алгоритмов криптозащиты и их параметры;

режим криптозащиты (транспортный или туннельный);

временные ключи шифрования, действительные только для текущего защищенного соединения;

срок существования защищенного соединения;

максимальный размер пакетов;

дополнительные параметры (счетчик, окно, флаги) для защиты от повтора, задержки и удаления пакетов сообщений.

Согласно сроку существования защищенного соединения определяется, как скоро, в зависимости от времени или объема переданных данных, потребуется закрытие текущего защищенного соединения и, возможно, открытие нового. Время жизни задается не только для каждого защищенного соединения, но и для каждого защищенного канала. Этот параметр может быть задан максимальным интервалом времени или максимальным объемом переданных данных.

Пара сетевых хостов может одновременно поддерживать несколько защищенных каналов, если имеются приложения с совершенно разными криптографическими требованиями. Защищенное соединение, соответствующее спецификации IPSec, идентифицируется целевым IP-адресом, используемым протоколом криптозащиты (AH или ESP), а также дополнительной характеристикой — *индексом параметров безопасности* (Security Parameter Index — SPI). Индекс параметров безопасности необходим для идентификации каждого из сопоставлений безопасности (SA), так как может существовать несколько защищенных соединений с одинаковыми IP-адресами и протоколами криптозащиты. Этот индекс включается в заголовки защищенных IPSec-пакетов, чтобы принимающая сторона смогла правильно расшифровать и аутентифицировать эти пакеты, воспользовавшись указанным SA.

Согласование параметров для двух симметричных однонаправленных соединений осуществляется на основе сформированного управляющего контекста с помощью трех шагов (Рисунок 5).

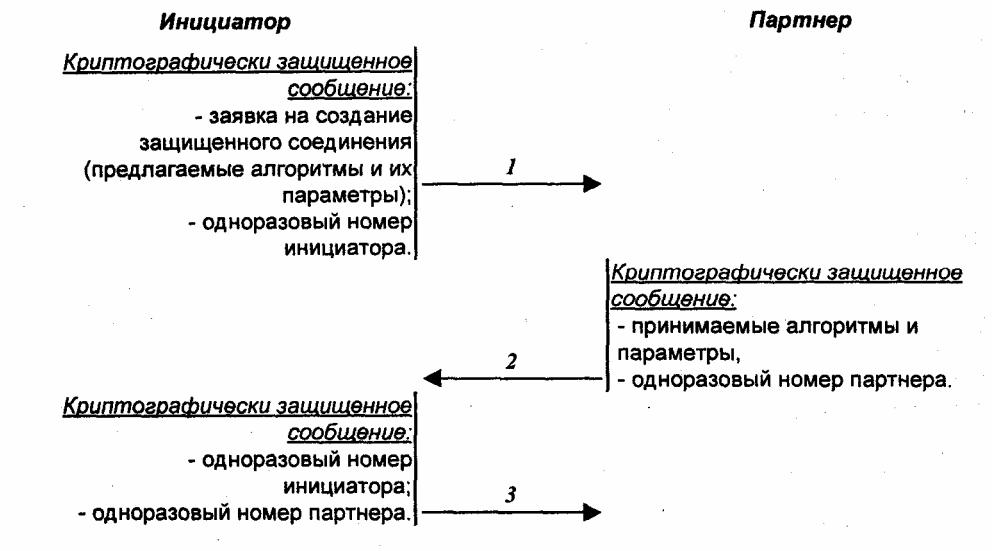

Рисунок 5 - Шаги согласования параметров двух симметричных соединений

За один информационный обмен по согласованию параметров, состоящий из трех шагов, формируются два однонаправленных соединения — по одному в каждом направлении. Принимающая сторона соединения задает для него индекс параметров безопасности (SPI), с помощью которого она будет находить сопоставление безопасности (SA) для обработки получаемых криптозащищенных пакетов.

Согласование параметров защищенного соединения, включая генерацию и распределение временных ключей, не требует большого объема вычислений, так как здесь используется набор простых математических операций. Могут быть заданы ограничения на допустимое число защищенных соединений в рамках одного защищенного канала.

Методы безопасности, основанные на IPSEC, могут значительно усложнить администрирование. Windows Server 2008/2003 избегает этого неудобства, внедряя для IPSEC администрирование *на основе политик*. Вместо приложений для настройки IPSEC используются политики. Можно настроить политики как для одного компьютера, так и для домена, сайта или организационного подразделения Active Directory.

Протокол AH

Протокол AH обеспечивает проверку подлинности, целостность и отсутствие повторов для всего IP - пакета (заголовка IP и полезных данных). AH подписывает весь пакет. Данные не шифруются, поэтому конфиденциальность не обеспечивается. Данные

доступны для чтения, но защищены от изменения. Протокол AH использует для подписания пакетов алгоритмы хэширования HMAC

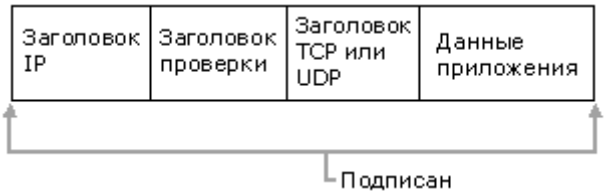

Рисунок 6 - Пакет IP с заголовком проверки AH

Заголовок проверки AH, как правило, располагается между основным заголовком IP-пакета и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня.

Next Header	Payload Len	Зарезервировано
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data (переменная длина)		

Рисунок 7 - Формат заголовка AH

Полнота защиты полей IP-заголовков зависит от используемого режима работы — туннельного или транспортного.

Формат заголовка AH (Рисунок 7), состоит из следующих полей:

Next Header — однобайтовое поле, содержащее код типа следующего заголовка, вложенного в IPSec-пакет. Например, если в IPSec-пакете содержится TCP-пакет, то данное поле будет содержать число 6 — код протокола TCP.

Payload Len — длина заголовка AH в 32-битных словах минус 2.

SPI — 32-битный индекс параметров безопасности, определяющий структуру SA (Security Association), содержащую все параметры туннеля IPSec, включая типы криптографических алгоритмов и ключи шифрования.

Sequence Number — беззнаковое 32-битное целое, увеличиваемое на единицу после передачи каждого защищенного по протоколу AH IP-пакета. Данное поле обеспечивает защиту от воспроизведения ранее посланных IP-пакетов. Отправитель обязан поддерживать этот счетчик. При формировании каждого защищенного сеанса информационного обмена в рамках туннеля IPSec обе взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их.

Authentication Data — поле переменной длины, содержащее информацию, используемую для аутентификации пакета, называемую цифровой подписью, имитовставкой, хэш-значением или криптографической контрольной суммой пакета ICV (Integrity Check Value). Способ вычисления этого поля определяется алгоритмом аутентификации. В настоящее время обязательной является поддержка алгоритмов HMAC-MD5 и HMAC-SHA1, основанных на применении односторонних хэш-функций с секретными ключами. Секретные ключи генерируются в соответствии с протоколом ISAKMP.

Аутентификация по протоколу AH *не допускает* изменение основных полей IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов (Network Address Translation — NAT), так как NAT манипулирует IP-заголовками.

Протокол ESP

Обобщенно все функции защиты, поддерживаемые протоколом инкапсуляции защищенных данных ESP, можно свести к аутентификации и криптографическому закрытию передаваемых IP-пакетов. В протоколе ESP функции аутентификации и криптографии могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NAT, поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать.

Независимо от режима использования протокола ESP его заголовок формируется как инкапсулирующая оболочка для зашифрованного содержимого.

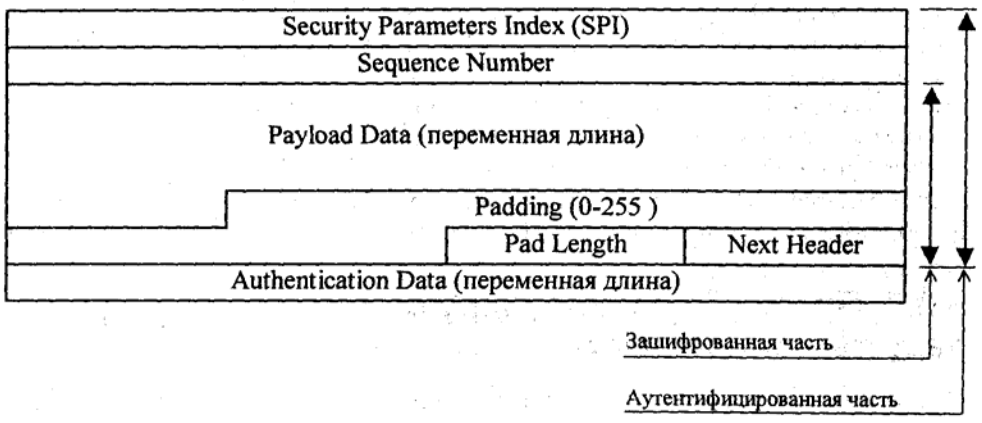

Рисунок 8 - Формат заголовка ESP

Поля SPI, Sequence Number, Next Header и Authentication Data имеют тот же смысл, что и для AH. Поле Authentication Data помещается в заголовок ESP только при включенной аутентификации. В поле Payload Data, имеющее переменную длину, включается инкапсулируемый пакет, который шифруется вместе с полями Padding, Pad Length и Next Header. Поле Padding представляет собой байты, добавляемые для обеспечения кратности длины инкапсулируемого пакета и размера блока алгоритма шифрования. Поле Pad Length содержит длину области Padding.

В *туннельном режиме* использования ESP в качестве инкапсулируемого пакета выступает весь исходный IP-пакет, а в *транспортном* - только его содержимое, т.е. исходный TCP- или UDP-пакет.

Алгоритм применения протокола ESP к исходящим IP-пакетам включает следующие шаги:

1. Инкапсулируемый пакет копируется в буфер.

2. Далее к этому пакету в буфере приписываются дополняющие байты (поле Padding), их число (поле Pad Length) и тип первого заголовка инкапсулируемого пакета (поле Next Header); поле Padding выбирается таким, чтобы поле Next Header было прижато к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования.

3. Текущее содержимое буфера зашифровывается.

4. В начало буфера приписываются поля SPI и Sequence Number с соответствующими значениями.

5. Пополненное содержимое буфера обрабатывается по используемому алгоритму аутентификации, и после окончания этой процедуры в конец буфера помещается поле Authentication Data.

6. Формируется результирующий IP-пакет путем приписывания соответствующего IP-заголовка в начало буфера.

Два режима работы IPsec

IPsec можно использовать в одном из двух режимов: транспортном или туннельном.

Иногда требуется обеспечить защиту IPsec на всем протяжении пути от клиента до сервера назначения (рисунок 9). Этот режим называется транспортным. Защита пересылаемых данных осуществляется с помощью протоколов AH, ESP или обоих одновременно. Данные защищаются на всем пути между двумя компьютерами.

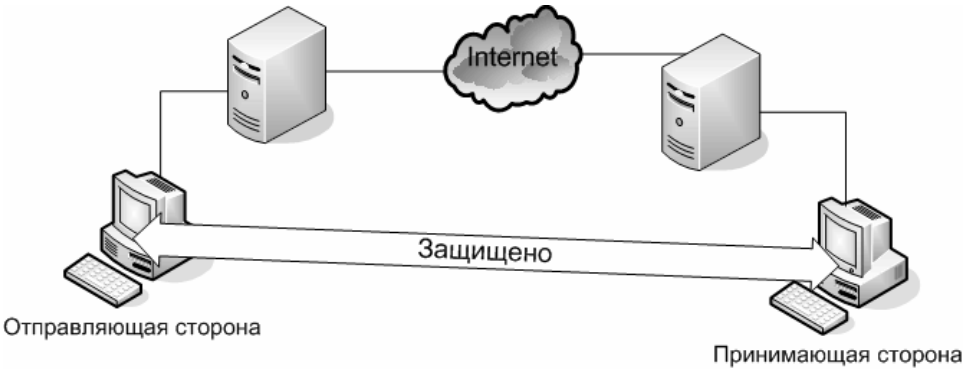

Рисунок 9 - Транспорт

При использовании туннельного режима IPsec защита данных осуществляется только между двумя определенными точками туннеля или шлюзами (рисунок 10). Туннельный режим IPsec обеспечивает защиту данных, пересылаемых между шлюзами.

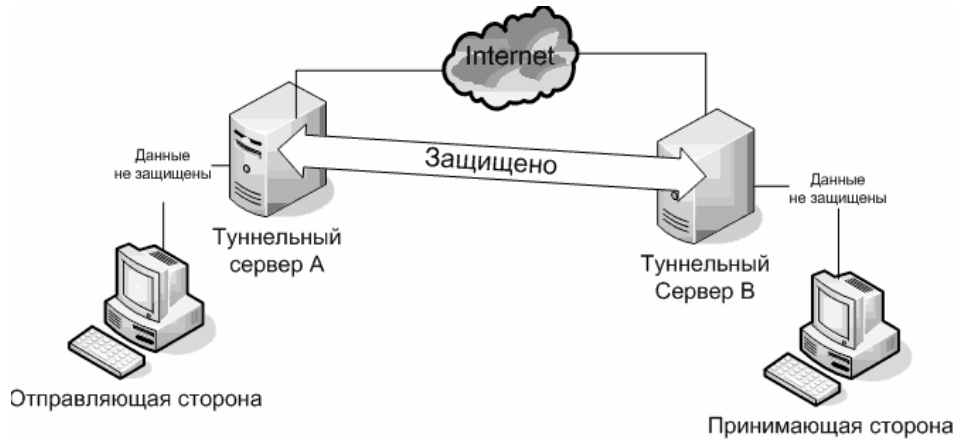

Рисунок 10 - Туннель

От клиента к серверу данные до достижения начального шлюза пересылаются в незащищенном виде. Затем при передаче пакетов в сеть назначения к ним применяются определенные в SA протоколы AH или ESP. На принимающем шлюзе происходит процесс расшифровки и верификации данных. В конце процесса данные в виде открытого текста передаются на целевой компьютер.

Рекомендация к выбору режима IPsec

Транспортный режим:

- Соединение осуществляется в рамках частной сети или в отдельном сегменте ЛВС, где необходимо предотвратить просмотр данных.

- Данные должны быть зашифрованы по всему пути от компьютера источника до компьютера приемника.
- Соединение осуществляется только между двумя компьютерами.
- На пути передачи данных отсутствует NAT.

Туннельный режим:

- Данные должны быть защищены на открытых участках сети, риска просмотра данных в частных сегментах сети нет.
- Во избежание прохождение нежелательного трафика через брандмауэр (он же пограничный сервер, выполняющий NAT), шифрование возможно только между пограничными серверами.

При туннельном режиме работы безопасность IPsec настраивается на туннельных серверах, в случае транспортного режима – на конечных компьютерах, непосредственно участвующих в безопасном обмене.

Туннелированием называется процесс инкапсуляции, маршрутизации и деинкапсуляции. При туннелировании исходный пакет помещается (инкапсулируется) внутрь нового пакета. Этот новый пакет может содержать новые сведения об адресации и маршрутизации, что позволяет передавать его через сеть. Когда туннелирование сочетается с секретностью, данные исходного пакета (а также исходные адреса источника и назначения) недоступны для других членов сети. Сеть при этом может быть любая: как частная интрасеть, так и Интернет. Когда инкапсулированные пакеты достигают места назначения, заголовок инкапсуляции удаляется, а для маршрутизации пакета к конечной точке используется заголовок исходного пакета.

Туннель представляет собой логический путь данных, по которому передаются инкапсулированные пакеты. Для исходных сторон подключения (источника и места назначения) туннель обычно прозрачен и выглядит как еще одна связь от точки к точке в сетевом пути. Для них маршрутизаторы, коммутаторы, прокси-серверы или другие шлюзы безопасности между начальной и конечной точками туннеля незаметны и не имеют значения. В сочетании с секретностью туннелирование может использоваться для виртуальных частных сетей (VPN).

Инкапсулированные пакеты проходят через сеть по туннелю. (В данном примере сеть представляет собой Интернет.) Шлюз может находиться между Интернетом и частной сетью – маршрутизатор, брандмауэр, прокси-сервер или другой шлюз безопасности. Кроме того, два шлюза могут использоваться в пределах частной сети для защиты трафика в менее доверительной части сети.

Туннельный режим AH

Туннельный режим AH не обеспечивает шифрование содержимого туннеля, а только строгую проверку целостности и подлинности.

Для проверки подлинности подписан весь пакет, включая новый туннельный заголовок. Таким образом, после отправки пакета из начальной точки туннеля изменения адресов источника или назначения невозможны. Структура, описанная в документе RFC рабочей группы IETF, все же допускает изменение компонентами сети нескольких полей нового заголовка IP для предоставления некоторым пакетам приоритета, а также удаление потерянных или устаревших пакетов. Допускается сочетание ESP и AH для обеспечения туннелирования, которое включает как проверку целостности всего пакета, так и конфиденциальность исходного пакета IP.

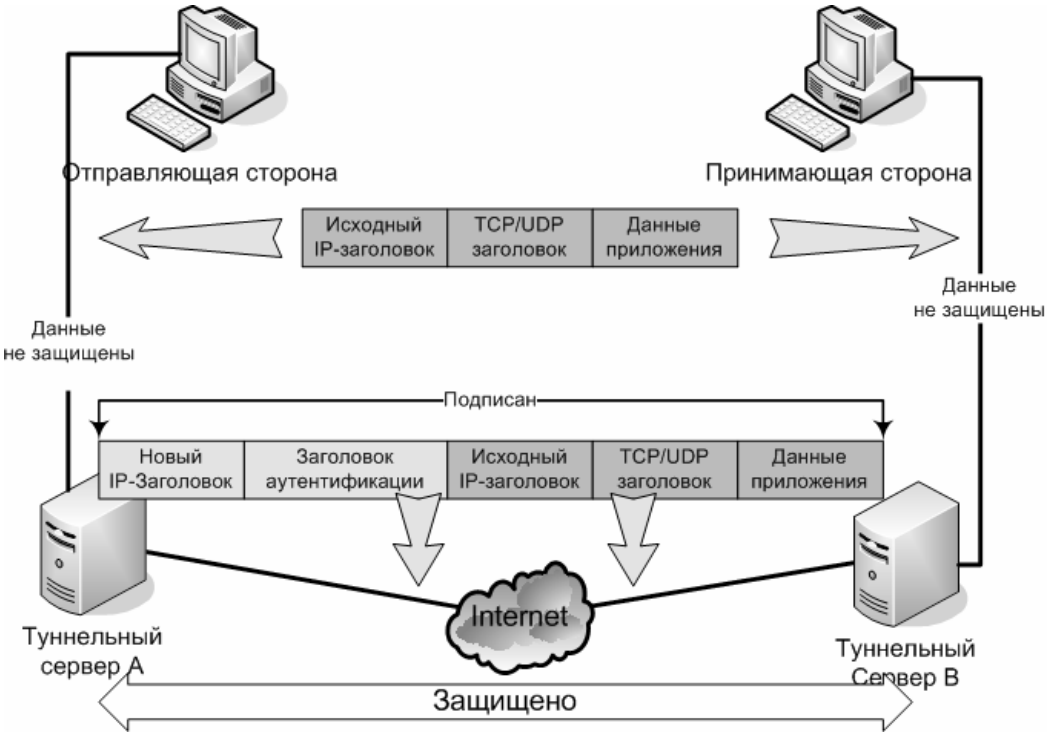

Рисунок 11 - Туннельный режим AH

Туннельный режим ESP

Исходный заголовок IP (исходный заголовок пакета) обычно содержит полные адреса источника и назначения, в то время как внешний заголовок IP обычно содержит адреса исходного и конечного шлюзов безопасности.

Формат туннеля ESP всегда обеспечивает надежную проверку целостности и подлинности для передаваемого по туннелю трафика. Туннель ESP используется главным образом для обеспечения секретности туннелированных пакетов с шифрованием по

алгоритму DES или 3DES. Уровень шифрования задается в настройках действия фильтра для правила туннеля, поэтому, если содержимое туннельного трафика не требует секретности, шифрование можно не использовать.

На приведенной иллюстрации исходный пакет между первичным источником и местом назначения инкапсулируется новыми заголовками IP и ESP. Область **Подписан** указывает часть пакета, защищенную проверкой целостности. Область **Зашифрован** указывает, что зашифрован может быть весь исходный пакет.

Сведения в новом заголовке IP используются для маршрутизации пакета от исходной точки до конечной точки туннеля, обычно шлюза безопасности. Новый заголовок IP не защищен подписью проверки целостности. Данная структура, описанная в документе RFC рабочей группы IETF, разрешает изменение заголовка пакета компонентами сети при необходимости обеспечения дополнительных служб, таких как изменение IP-адресов источника или назначения или повышение приоритета относительно других пакетов.

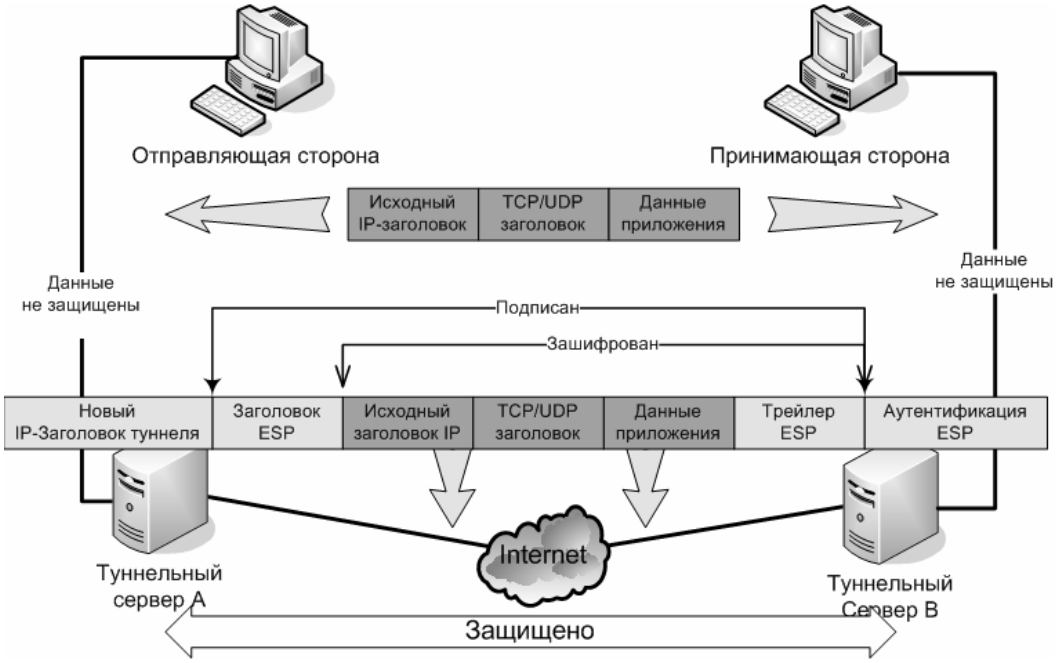

Рисунок 12 - Туннельный режим ESP

При использовании протокола ESP в туннельном режиме каждый исходный IP-пакет в криптозащищенном виде помещается целиком в конверт IPSec, а тот, в свою очередь, инкапсулируется в другой IP-пакет (Рисунок 13). В защищенном IP-пакете

внутренний (исходный) IP-заголовок, располагаемый в зашифрованной части, содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля.

Рисунок 13 - IP-пакет до и после применения протокола ESP

Когда ESP используется в транспортном режиме, в конверт IPSec в криптозащищенном виде помещается только содержимое исходного IP-пакета и к полученному конверту добавляется исходный IP-заголовок.

Транспортный режим AH и ESP

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), поля которых, в свою очередь, содержат информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные хосты на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6).

Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, и как следствие возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

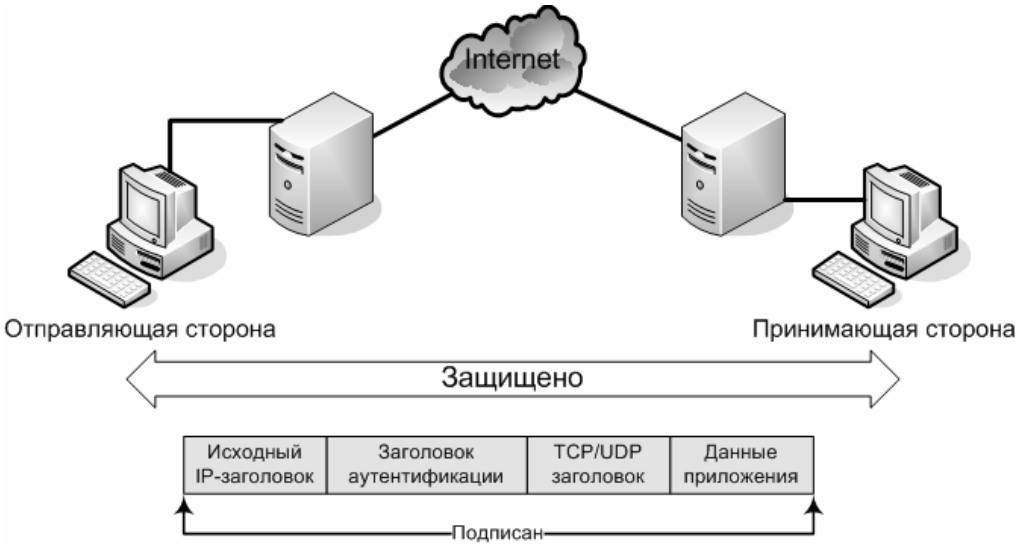

Рисунок 14 - Транспортный режим AH

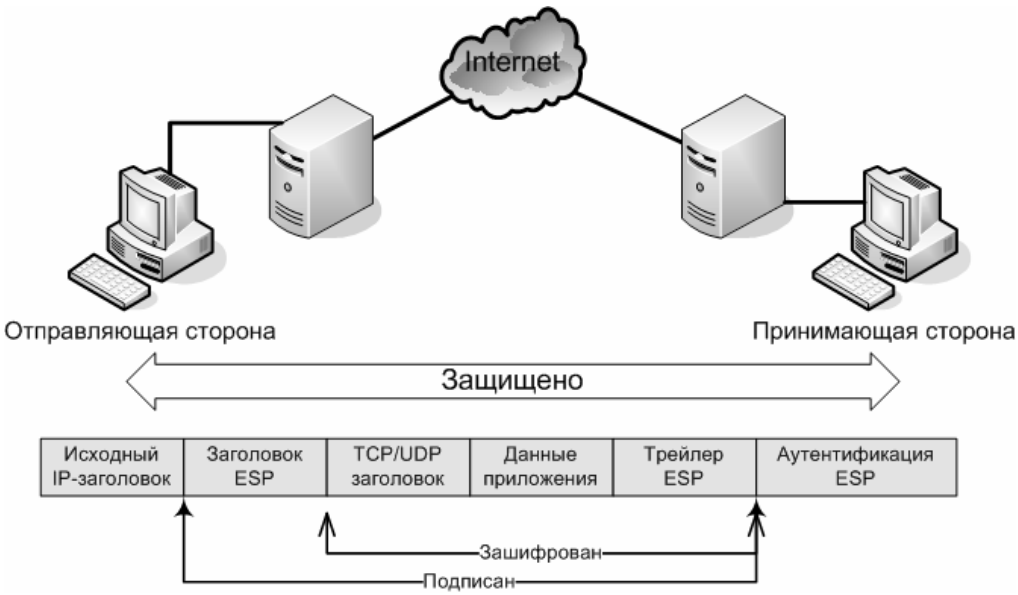

Рисунок 15 - Транспортный режим ESP

Протоколы AH и ESP могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ESP аутентификация идет следом за шифрованием, протокол AH должен применяться после протокола ESP. В туннельном режиме протоколы AH и ESP применяются к разным вложенным пакетам и, кроме того, в данном режиме допускается многократная вложенность туннелей с различными начальными и/или конечными точками. Поэтому в случае туннельного режима число возможных комбинаций по совместному использованию протоколов AH и ESP существенно больше.

Фильтры IPsec и их действия

Для идентификации протоколов, которые необходимо защитить, надо определить IPsec-фильтры. Из оснастки «IP Security Policies on Local Computer» (доступна через Start->Administrative Tools->Local Security Policy) выбираем «Manage IP filter lists and filter actions…».

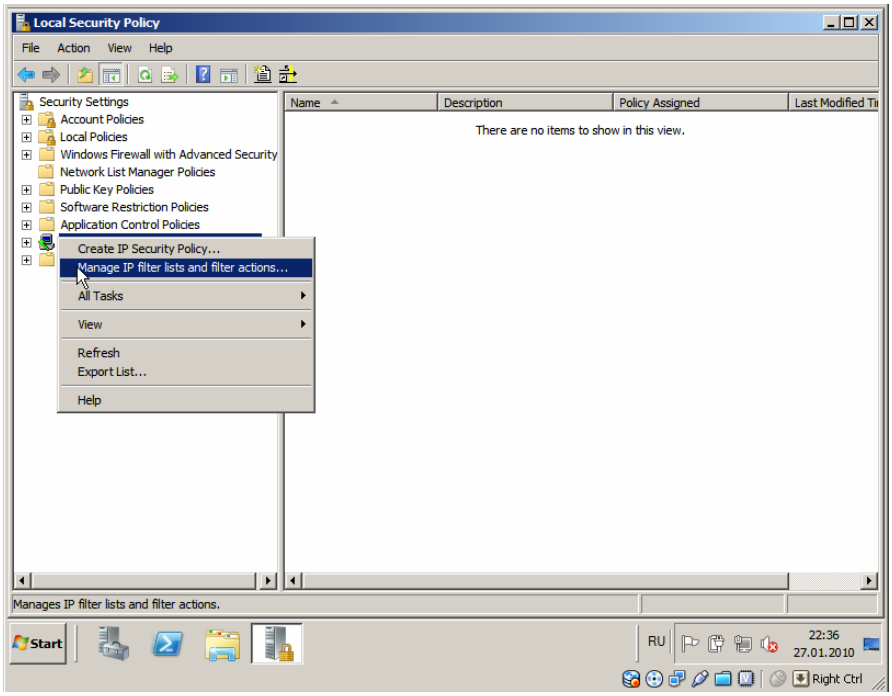

Рисунок 16

Рисунок 17 - Управление списками IP-фильтров

Далее нажимаем «Add…» и появляется следующее окно «IP filter list», показанное на рисунке 18.

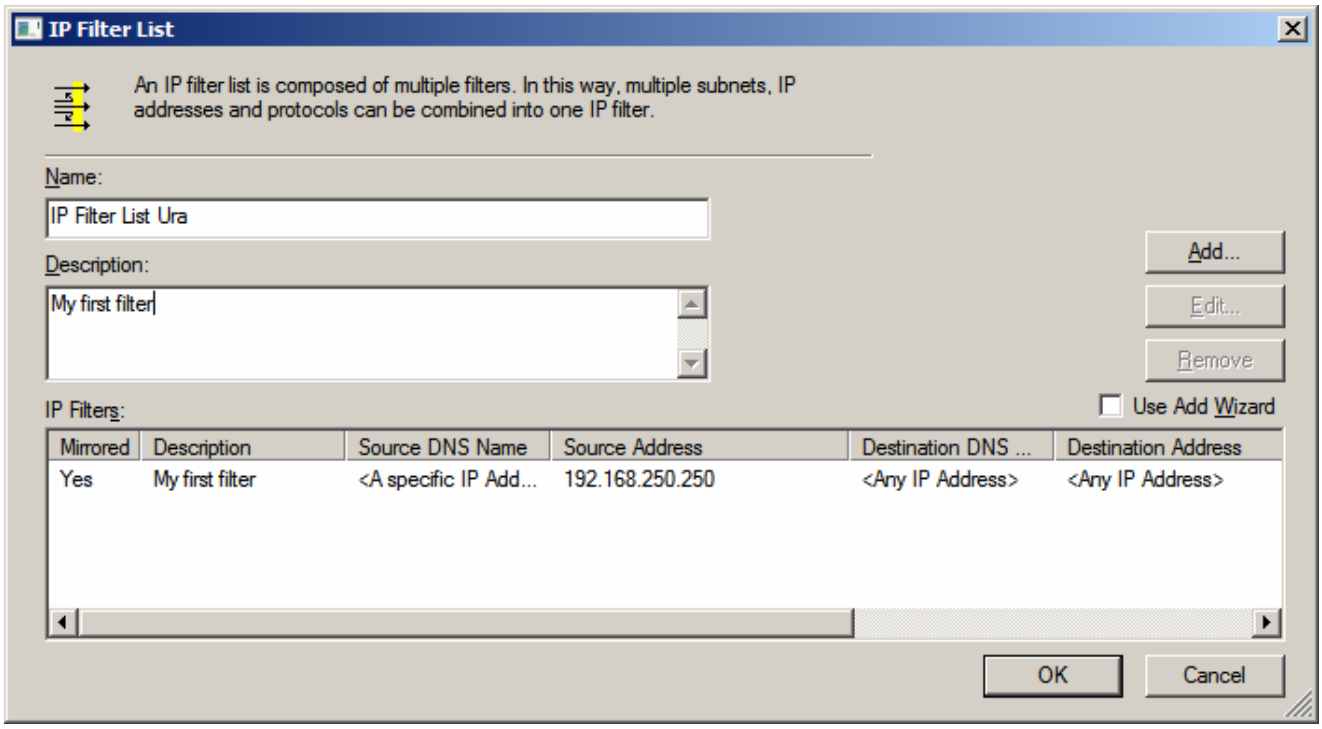

Рисунок 18 - Список IP-фильтров

Для идентификации протокола используются следующие характеристики:

- IP-адрес источника. Может быть конкретным IP-адресом, IP-адресом определенной подсети или любым адресом.
- IP-адрес назначения. Может быть конкретным IP-адресом, IP-адресом определенной подсети или любым адресом.
- Тип протокола. Это идентификатор протокола или используемый транспортный протокол. Например, PPTP использует пакеты GRE, которые определяются по их идентификатору протокола(47).
- Порт источника. Если используются протоколы TCP или UDP для защищенного соединения можно определить порт источника. Большинство протоколов в качестве порта источника используют случайный порт.
- Порт назначения. Если применяется TCP или UDP, то для получения данных служит конкретный порт на сервере.

Все характеристики доступны для настройки при редактировании/добавлении (Add/Edit) фильтра. Свойства IP-фильтра показаны на рисунке 19.

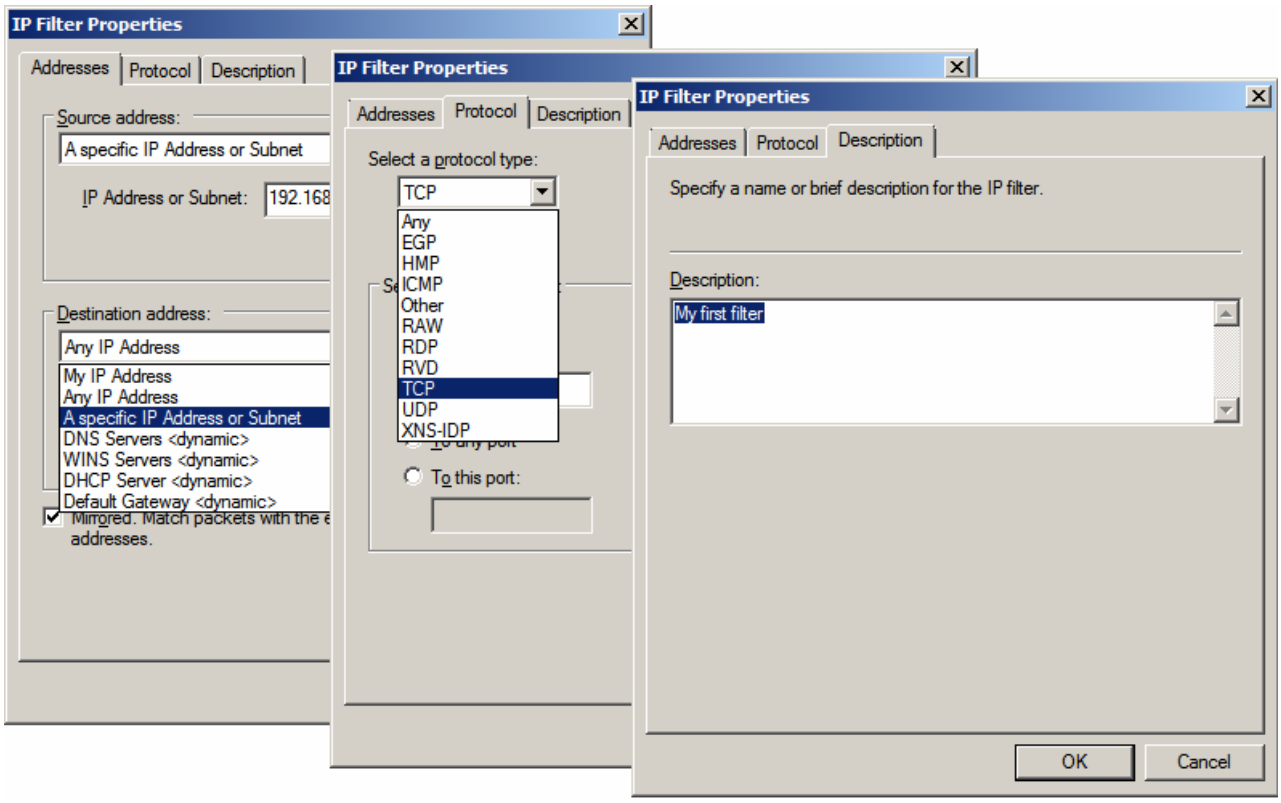

Рисунок 19 - Свойства IP-фильтра

При добавлении нового фильтра также можно использовать мастер для этого нужно поставить галочку «Use add wizard» в окне «IP filter list». Работа мастера проиллюстрирована на рисунке 20.

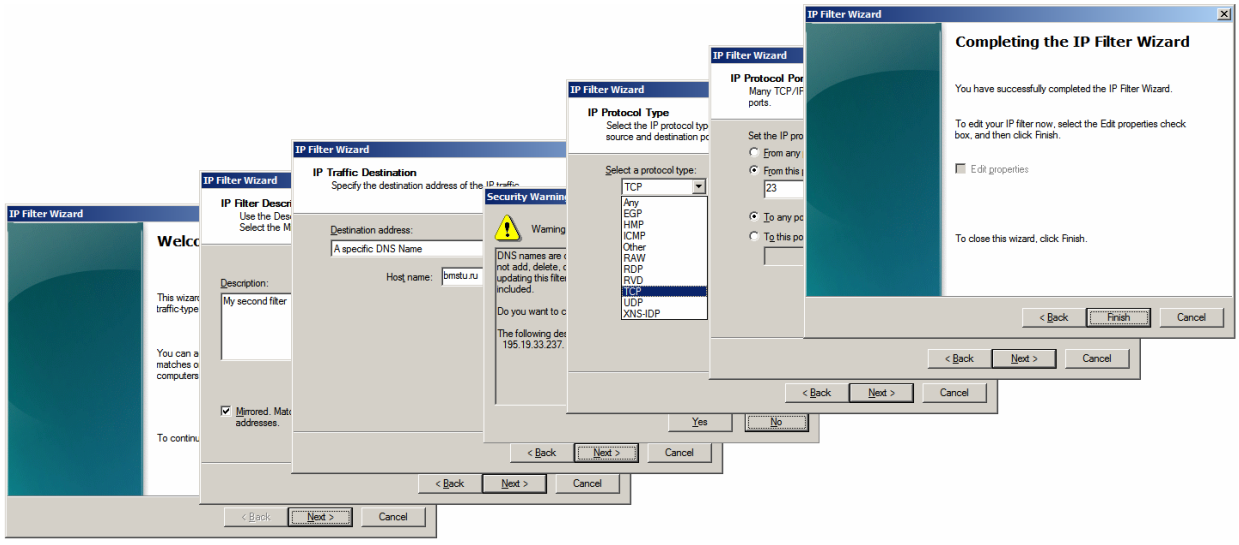

Рисунок 20 – Мастер добавления фильтра

Для зашиты ответных пакетов средствами IPsec нужно настроить все фильтры IPsec как отраженные (галка mirrored на вкладке addresses). Такой фильтр обращает информацию источника и назначения, так что ответные пакеты, отправляемые сервером обратно клиенту, также будут защищены IPsec. Не следует применять правила отражения при определении фильтров для туннельного режима IPsec. В этом случае следует создать

отдельные фильтры для отражения конечной точки туннеля, используемые на обоих концах туннеля.

Случаи, когда применение фильтров нецелесообразно:

- Layer Two Tunneling Protocol (L2TP защищен средствами ESP автоматически)
- Широковещательные и групповые адреса (т.к. SA может быть установлен между парой компьютеров)
- Resource ReSerVation Protocol (для запроса части пропускной способности сети компьютер использует протокол RSVP, идентификатор протокола 46. Можно защитить протокол, для которого RSVP запрашивает качество обслуживания, но не сами RSVP-пакеты этого запроса)
- Протокол Kerberos (т.к. используется для аутентификации перед IPsec)
- Протокол Internet Key Exchange (т.к. IKE применяется для согласования SA между двумя компьютерами – процессом, используемым перед безопасной передачей данных)

Список портов, используемых типичными службами можно найти по адресу http://www.iana.org/assignments/port-numbers.

Каждому списку фильтров необходимо поставить в соответствие действие (разрешить, блокировать или иное)

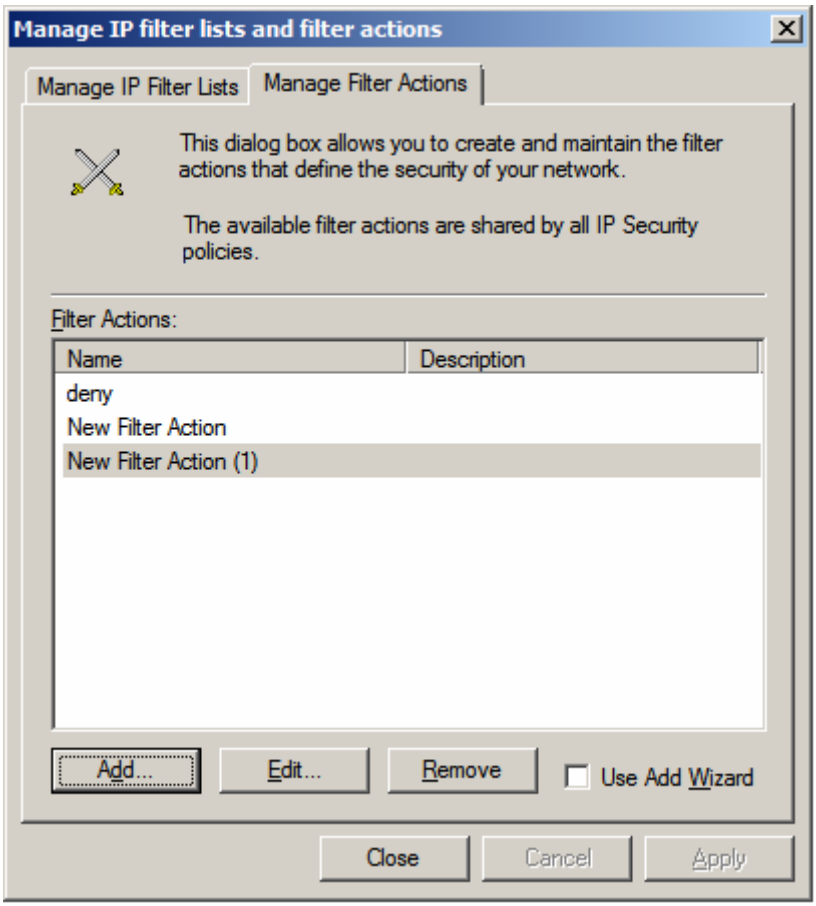

Рисунок 21 - Управление списками действий фильтров

Список действий можно редактировать на вкладке «Manage Filter Actions», доступной из меню «Manage IP filter lists and filter actions…» оснастки «IP Security Policies on Local Computer» (Start->Administrative Tools->Local Security Policy)

Действия фильтра IPsec могут быть следующие:

- Permit (Разрешить) передачу пакетов без защиты IPsec. Например: протокол SNMP включает поддержку устройств, не совместимых с IPsec. Включение IPsec для протокола SNMP может помешать этим устройствам управлять сетью. Для разрешения передачи пакетов SNMP без защиты IPsec в сетях с высокой безопасностью можно создать специальный фильтр IPsec для SNMP.
- Block (Блокировать) запрещает существование в сети протокола, соответствующего IPsec-фильтру. Все пакеты, подпадающие под условия этого фильтра, отбрасываются. Данный фильтр используется на имеющих доступ в Интернет компьютерах с Windows Server 2008 для предотвращения типичных атак, например средствами протокола Finger.
- Negotiate Security (Согласовать безопасность) позволяет администратору определить уровень шифрования и алгоритм хеширования для защиты трафика, соответствующего фильтру IPsec.

Кроме трех основных, можно определить действия компьютера с Windows 2008 в случае получения не защищенных IPsec данных и частоту определения новых сеансовых ключей для защиты данных IPsec. Имеются следующие параметры.

- Accept Unsecured Communication, But Always Respond Using IPsec

  Принимать небезопасную связь, но отвечать с помощью IPsec

  Используется, когда защита IPsec принудительно устанавливается на серверах, а не на клиентских компьютерах. В типичной среде IPsec клиентские компьютеры настраиваются для применения IPsec, если это требуется сервером, но никогда не инициируют SA. Этот параметр разрешает получение исходного пакета сервером, который затем начинает процесс IKE для согласования SA между клиентом и сервером. Хотя довольно рискованно использовать открытый текст для исходного пакета данных, ответный пакет не передается с сервера, пока не будет установлено SA.
- Allow Unsecured Communication With Non-IPsec-Aware Computers

  Разрешать связь с компьютерами, не поддерживающими IPSEC.

  В смешанной сети этот параметр разрешает подключаться к серверу клиентским компьютерам, не поддерживающим IPsec. Клиенты с IPsec соединятся с сервером по защищенному каналу. Не поддерживающим IPsec клиентам будет разрешено соединяться, используя незащищенные потоки данных.
- Session Key Perfect Forward Secrecy

  Сеансовые циклы безопасной пересылки.

  Шифрование данных для пакетов IPsec осуществляется с помощью сеансовых ключей. Этот параметр запрещает использовать существующий ключ для создания нового ключа, что уменьшает риск компрометации данных, поскольку предыдущий ключ не может быть использован для определения следующего ключа.

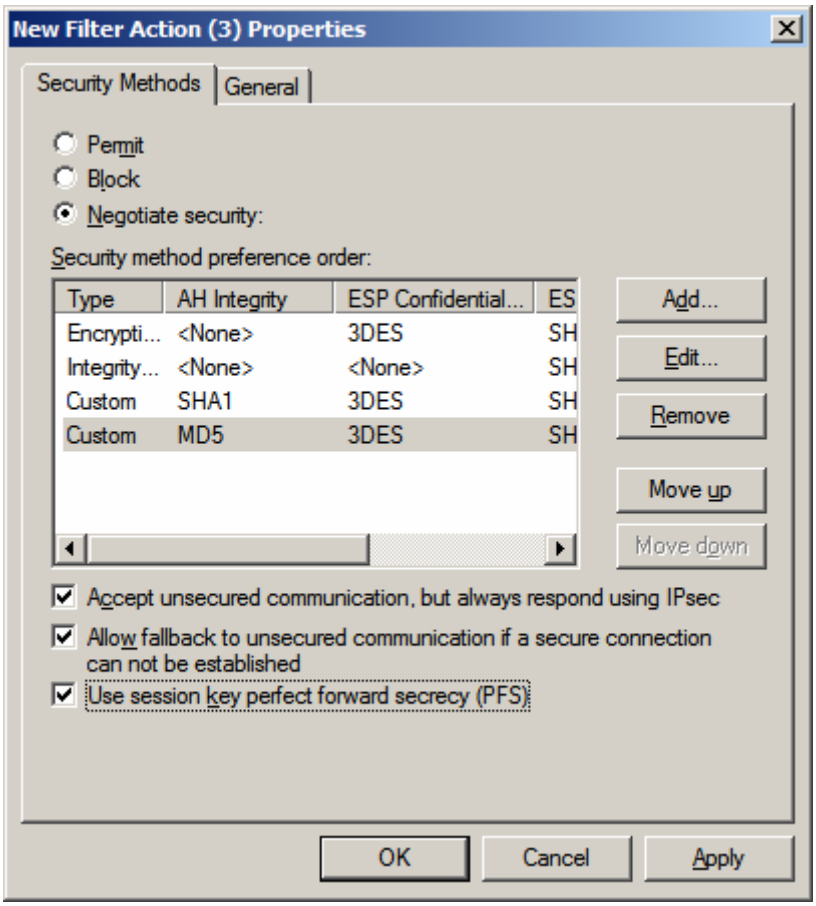

Рисунок 22

В случае положительного результата на установление безопасного соединения (рассматривается случай Negotiate security), то метод защиты выбирается из списка методов защиты. Рекомендуется выстраивать методы защиты в убывающем монотонном порядке: от сильной (верхняя строчка) к слабой (нижняя строчка) защите.

Шифрование и проверка целостности в IPsec

Добавим метод безопасности. Для этого нажмем кнопку **Add…** из предыдущего окна, показанного на рисунке 22. Результат показан на рисунке 23.

Рисунок 23

Методы безопасности:

- Integrity and encryption (целостность и шифрование **данных**);
- Integrity only (целостность **данных**);
- Custom (выборочно).

Настройка метода безопасности вручную позволяет обеспечить целостность не только **данных**, но и **ip-адресов**. Это означает, что подмена ip-адреса в пакете злоумышленником будет определена.

Для обеспечения целостности доступны два алгоритма Message Digest v5 (MD5) и Secure Hash Algorithm (SHA1).

Для обеспечения конфиденциальности доступны два алгоритма Data Encryption Standard (DES) и Triple DES (3DES).

Считается, что SHA1 сильнее MD5, а 3DES сильнее DES.

Обеспечить большую надежность позволяет установка параметров смены ключа сессии. Ключ сессии может изменяться каждый определенный промежуток времени или через определенный объем информации обмена.

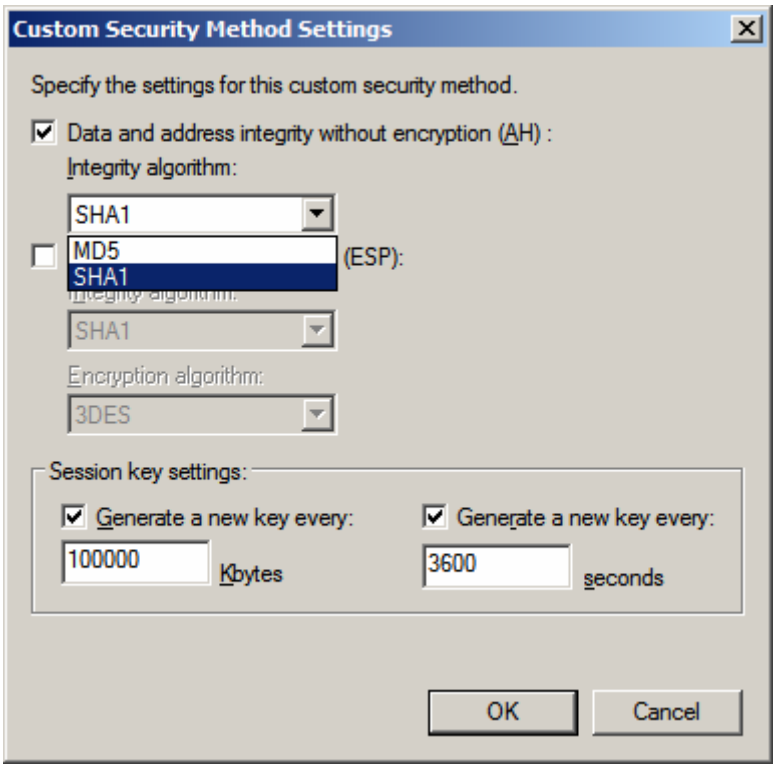

Рисунок 24

Аутентификация IPsec

Методы проверки подлинности (или иначе методы аутентификации) задают требования по выполнению **проверки подлинности** для безопасных подключений. Независимо от числа настроенных методов проверки подлинности для пары компьютеров может быть задан только один.

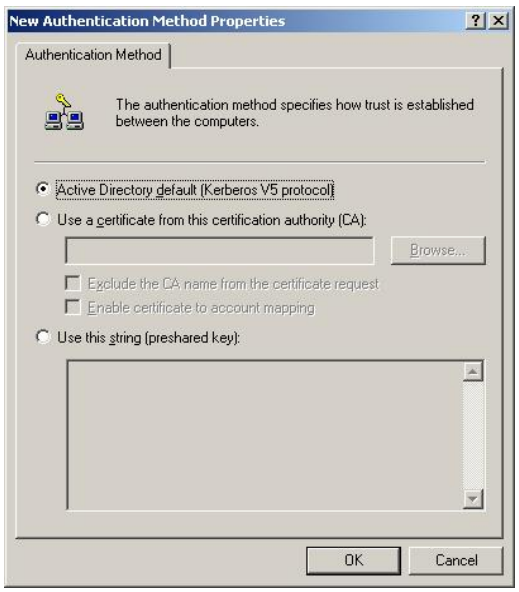

Рисунок 25 - Выбор Метода Аутентификации

Стандартные методы проверки подлинности следующие:

- протокол безопасности **Kerberos V5**.

  Клиенты должны быть включены в доверенный домен Windows 2008;

- **сертификаты** открытого ключа

  Ограничений на членство в домене не накладывается – возможна аутентификация между лесами;

  Требуется наличие общего корневого Центра Сертификации;

  Требуется наличие сертификата у каждого компьютера (предполагающего установку безопасного соединения IPsec);

- **общий ключ**.

  Это текстовая строка, используемая двумя пользователями по предварительной договоренности. Обе стороны должны вручную настроить IPSEC на использование общего ключа. Рекомендован к применению, если нет возможности использовать Kerberos V5 или сертификаты, а так же в случае тестирования IPsec фильтров. Предназначен только для защиты проверки подлинности.

Выбор между протоколом Kerberos и открытыми ключами определяется простотой настройки. В лесу Windows Server 2008 протокол Kerberos — самый простой в использовании механизм, поскольку он уже внедрен на все компьютеры в данном лесу. Открытый ключ чаще применяют, когда существует инфраструктура PKI или для связи между организациями требуется IPsec.

Внедрение политики IPsec в средах рабочей группы и домена

В Windows 2008 отсутствую стандартные политики IPsec в отличие от предыдущих серверных операционных систем Windows.

В среде рабочей группы политики IPsec можно настроить, только корректируя параметры безопасности локального компьютера. Согласованные параметры IPsec на схожих компьютерах можно получить путем **экспорта** правильно настроенных параметров IPsec в **IPsec-файл** и их последующего импорта на все необходимые компьютеры.

Active Directory позволяет стандартизировать настройку IPsec за счет применения политик IPsec в составе объектов групповой политики (ОГП). Вы можете определить политики IPsec для сайта, домена или ОП, чтобы согласованные политики применялись ко

всем объектам компьютеров в соответствующем контейнере. Групповая политика не позволяет локальному администратору изменять параметры IPsec на своем компьютере, поскольку наследованные параметры групповой политики всегда приоритетнее параметров локальной. Для определения политик IPsec необходимо создать политику на отдельном компьютере, экспортировать ее параметры в IPsec-файл, а затем импортировать его в ОГП, где нужно внедрить эту политику.

Практическая часть

При выполнении лабораторной работы на виртуальной машине, следует знать «физическую» связь между виртуальными машинами, которая представлена на рис.

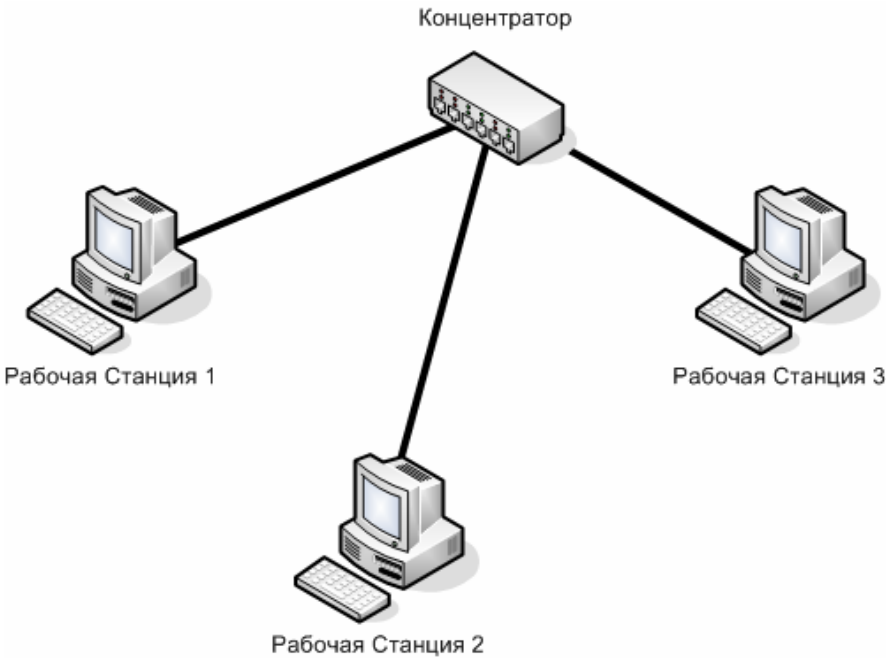

Рис. 26 - Физическая коммутация

Добавление оснастки

На каждом из компьютеров нажмите кнопку **Start (Пуск)** и выберите команду **Run (Выполнить)**. Введите **mmc**. В появившемся окне выберите **Add/Remove Snap-in (Добавить или удалить оснастку)** в меню **Console (Консоль)** (рис. 22). В окне Add/Remove Snap-in (Добавление и удаление оснастки) выберите **IP Security Policy Management (Управление политикой IP-безопасности)** нажмите кнопку Add (Добавить) (рис. 23). После этого будет предложено выбрать компьютер или домен для которого будет производиться управление политикой IPsec (рис. 24). Выберите **Local computer (Локальный компьютер)** и нажмите **Finish (Готово)**. Закройте окно Add/Remove Snap-in (Добавление и удаление оснастки) кнопкой **OK**. После этого закройте окно оснастки и, в ответ на предложение сохранить получившуюся оснастку, сохраните ее под любым именем (например, IPsec).

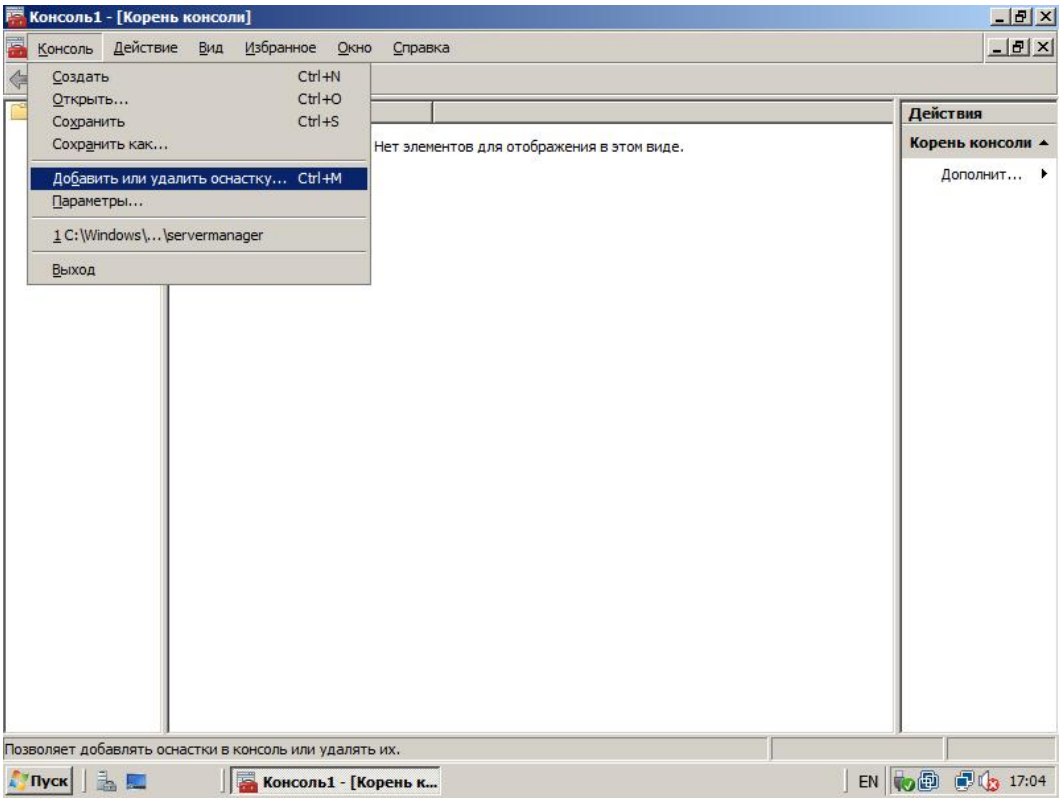
Консоль1 - [Корень консоли]
Консоль Действие Вид Избранное Окно Справка
Создать Ctrl+N
Открыть... Ctrl+O
Сохранить Ctrl+S
Сохранить как...
Добавить или удалить оснастку... Ctrl+M
Параметры...
1 C:\Windows\...\servermanager
Выход
Нет элементов для отображения в этом виде.
Действия
Корень консоли
Дополнит...
Позволяет добавлять оснастки в консоль или удалять их.
Пуск
Консоль1 - [Корень к...
EN
17:04

Рис. 27.

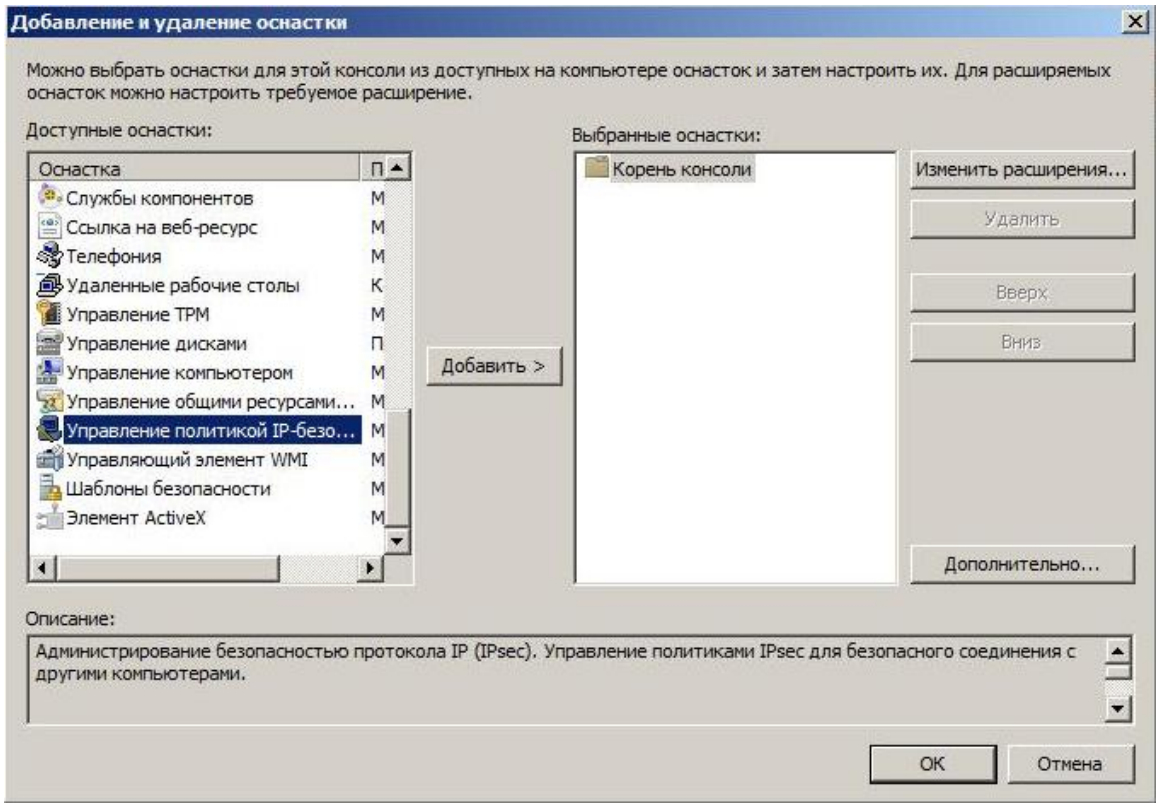
Добавление и удаление оснастки
Можно выбрать оснастки для этой консоли из доступных на компьютере оснасток и затем настроить их. Для расширяемых оснасток можно настроить требуемое расширение.
Доступные оснастки:
Оснастка
Службы компонентов
Ссылка на веб-ресурс
Телефония
Удаленные рабочие столы
Управление TPM
Управление дисками
Управление компьютером
Управление общими ресурсами...
Управление политикой IP-безо...
Управляющий элемент WMI
Шаблоны безопасности
Элемент ActiveX
Добавить >
Выбранные оснастки:
Корень консоли
Изменить расширения...
Удалить
Вверх
Вниз
Дополнительно...
Описание:
Администрирование безопасностью протокола IP (IPsec). Управление политиками IPsec для безопасного соединения с другими компьютерами.
OK
Отмена

Рис. 28.

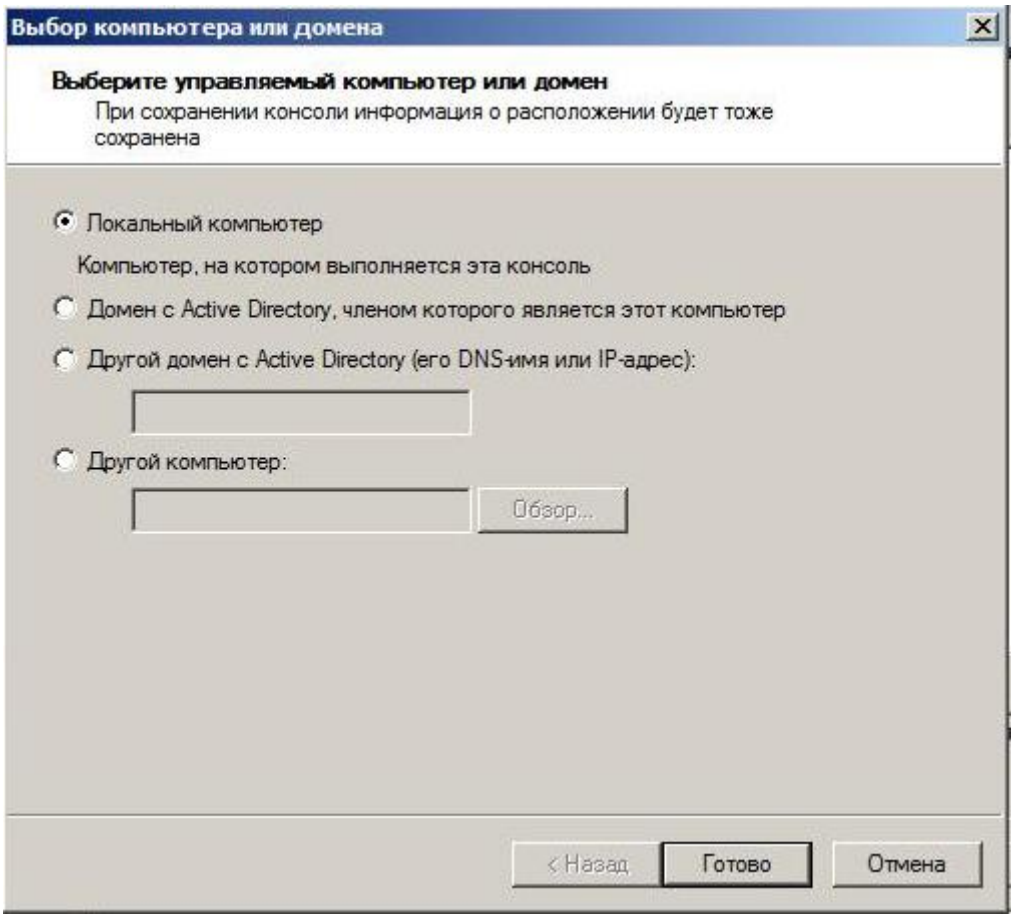

Рис. 29.

Также до оснастки «IP Security Policy Management (Управление политикой IP-безопасности)» можно было бы добраться более простым способом: Start (Пуск)->Administrative Tools (Администрирование)->Local Security Policy (Локальная политика безопасности).

Создание политики безопасности

Вообразим гипотетическую задачу, в которой имеется сервер и ряд рабочих станций. Все PC находятся в одной сети 172.16.0.0/16. Задачей сервера является секретный сбор однотипных данных с разных PC. Данные PC отправляют на порт 5555 сервера 172.16.7.15. У сервера существует необходимость открыто общаться с любым IP по telnet (порт 23).

Процесс создания политики безопасности начнем с создания фильтров и действий к фильтрам, и завершим непосредственным созданием политики. Хотя возможно создать все необходимые фильтры и действия к фильтрам уже в поцессе создания самой политики безопасности. Для этого необходимо выбрать «Manage IP filter lists and filter actions… (Управление списками IP-фильтра и действиями фильтра…)»:

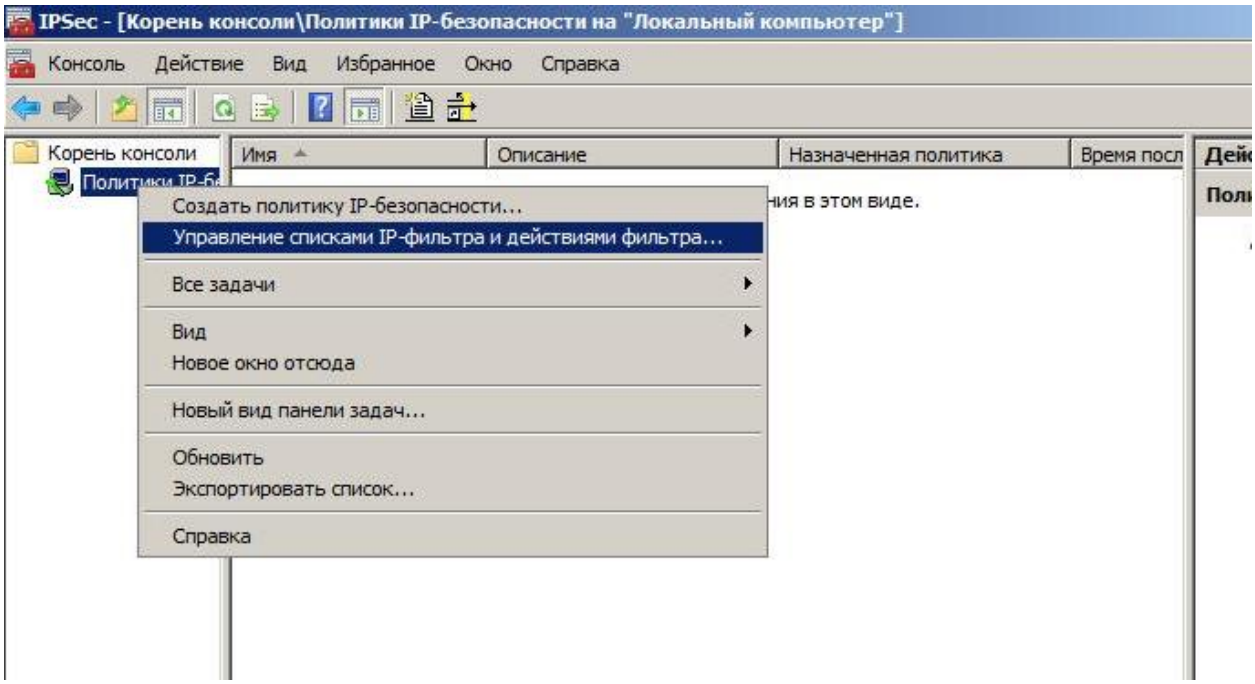

Рис. 30.

Порядок действий:

Добавляем новый список фильтров EssentialProtocol

Добавляем новый фильтр (устанавливаем параметры: source address (адрес источника пакетов) – A specific IP subnet (Определенный IP-адрес или подсеть), 172.16.0.0/255.255.0.0; destination address (адрес назначения) – My IP address (Мой IP-адрес); Select protocol type (Выберите тип протокола) – TCP; to this port (пакеты на этот порт) - 5555)

Добавляем новый список фильтров Telnet

Добавляем новый фильтр (устанавливаем параметры: source address (адрес источника пакетов) – My IP address (Мой IP-адрес); destination address (адрес назначения) – Any IP address (Любой IP-адрес); Select protocol type (Выберите тип протокола) – TCP; to this port (пакеты на этот порт) - 23)

Ниже все действия проиллюстрированы.

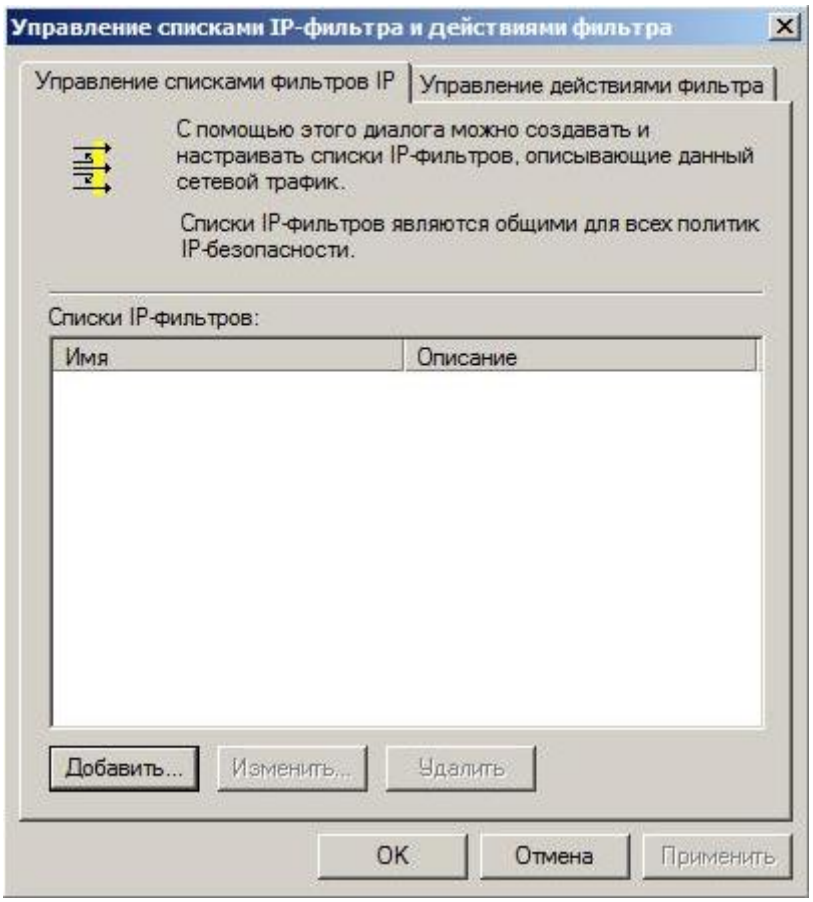
Управление списками IP-фильтра и действиями фильтра
Управление списками фильтров IP
Управление действиями фильтра
С помощью этого диалога можно создавать и настраивать списки IP-фильтров, описывающие данный сетевой трафик.
Списки IP-фильтров являются общими для всех политик IP-безопасности.
Списки IP-фильтров:
Имя
Описание
Добавить...
Изменить...
Удалить
OK
Отмена
Применить

Рис. 31.

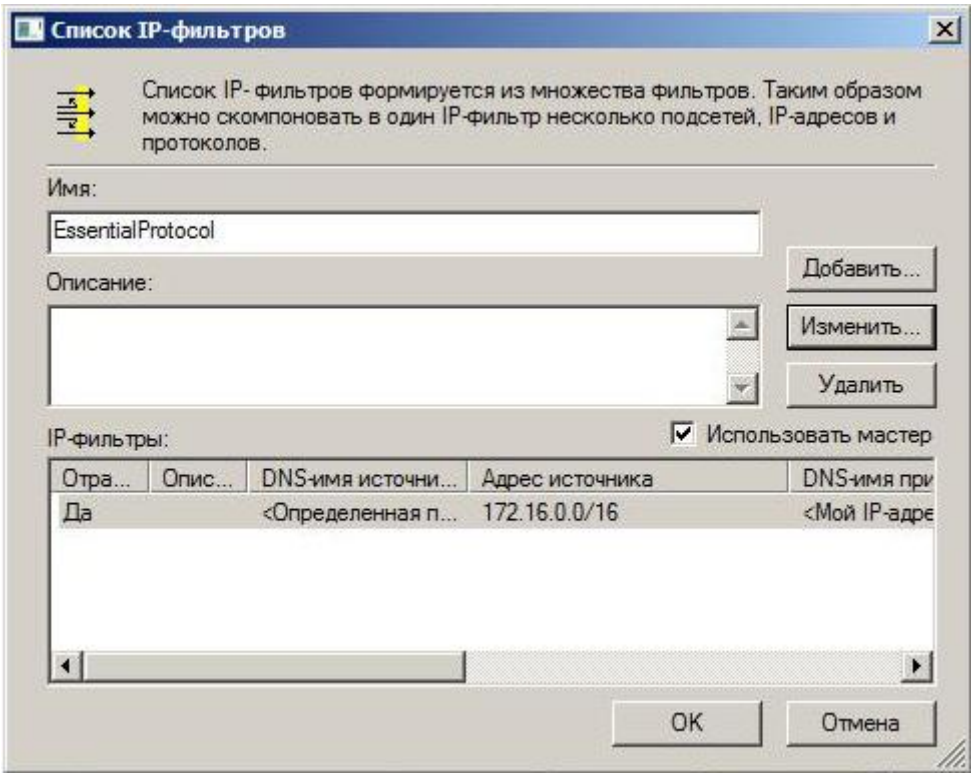
Список IP-фильтров
Список IP- фильтров формируется из множества фильтров. Таким образом можно скомпоновать в один IP-фильтр несколько подсетей, IP-адресов и протоколов.
Имя:
EssentialProtocol
Описание:
Добавить...
Изменить...
Удалить
IP-фильтры:
Использовать мастер
Отра...
Опис...
DNS-имя источни...
Адрес источника
DNS-имя при
Да
<Определенная п...
172.16.0.0/16
<Мой IP-адре
OK
Отмена

Рис. 32.

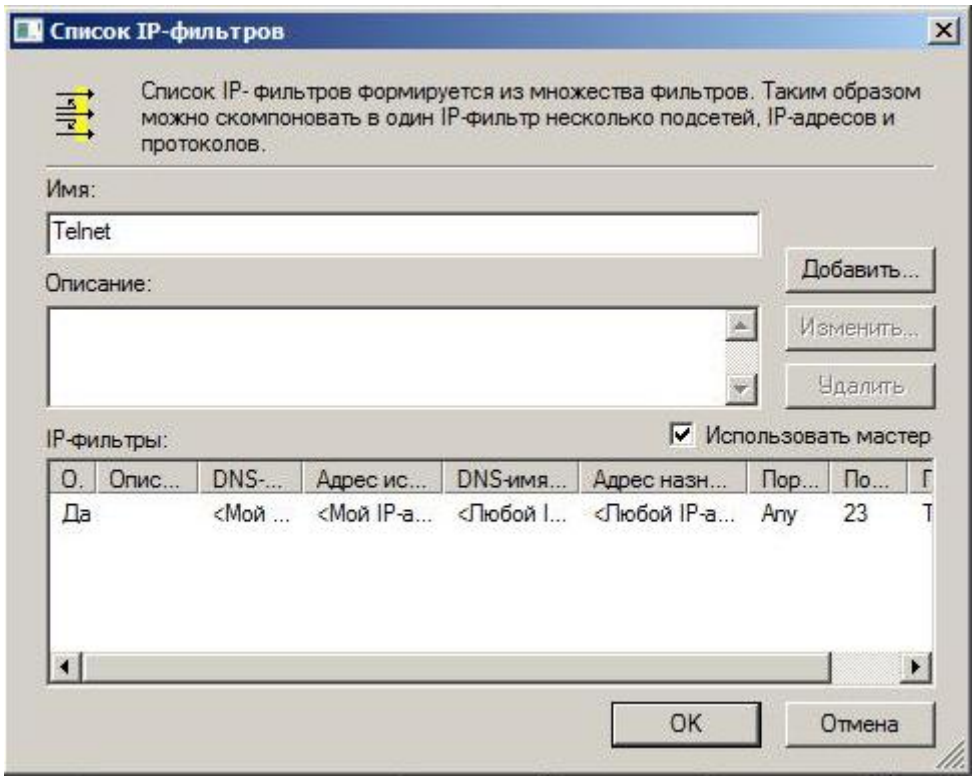
Список IP-фильтров
Список IP- фильтров формируется из множества фильтров. Таким образом можно скомпоновать в один IP-фильтр несколько подсетей, IP-адресов и протоколов.
Имя:
Telnet
Описание:
Добавить...
Изменить...
Удалить
IP-фильтры:
Использовать мастер
О.
Опис...
DNS-...
Адрес ис...
DNS-имя...
Адрес назн...
Пор...
По...
Да
<Мой ...
<Мой IP-а...
<Любой I...
<Любой IP-а...
Any
23
OK
Отмена

Рис. 33.

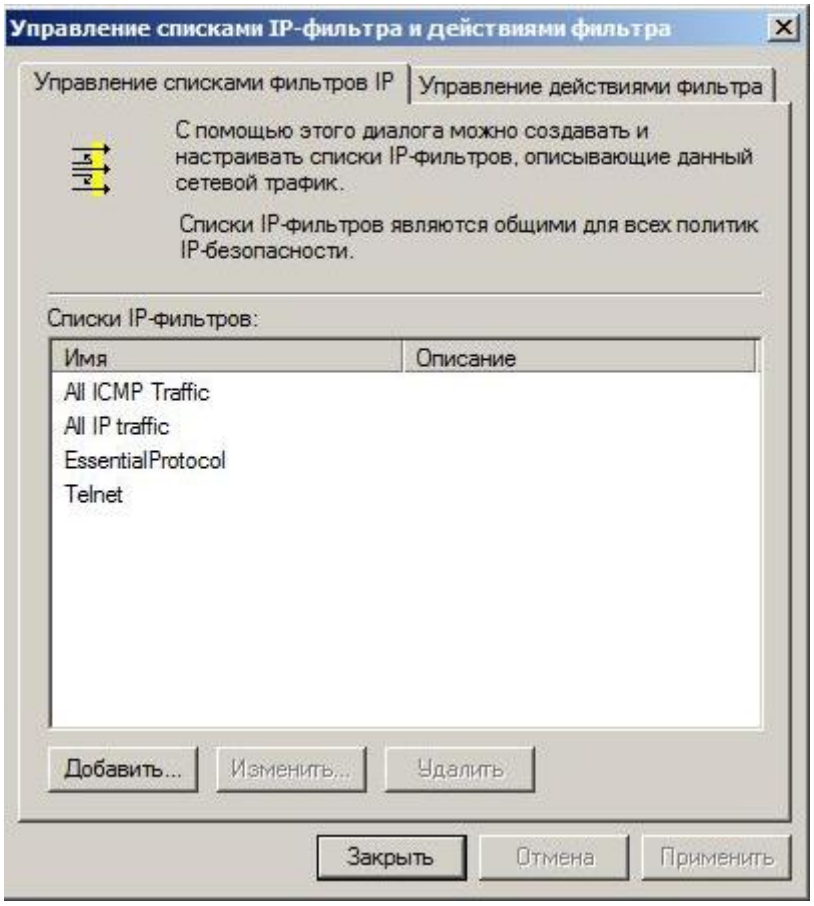
Управление списками IP-фильтра и действиями фильтра
Управление списками фильтров IP
Управление действиями фильтра
С помощью этого диалога можно создавать и настраивать списки IP-фильтров, описывающие данный сетевой трафик.
Списки IP-фильтров являются общими для всех политик IP-безопасности.
Списки IP-фильтров:
Имя
Описание
All ICMP Traffic
All IP traffic
EssentialProtocol
Telnet
Добавить...
Изменить...
Удалить
Закрыть
Отмена
Применить

Рис. 34.

В WS2003 для использования пригодны встроенные действия к фильтрам. Для большей наглядности создадим одно собственное действие к фильтру. Фильтр будем создавать без использования мастера (следует убрать галочку Use Add Wizard (Использовать мастер)).

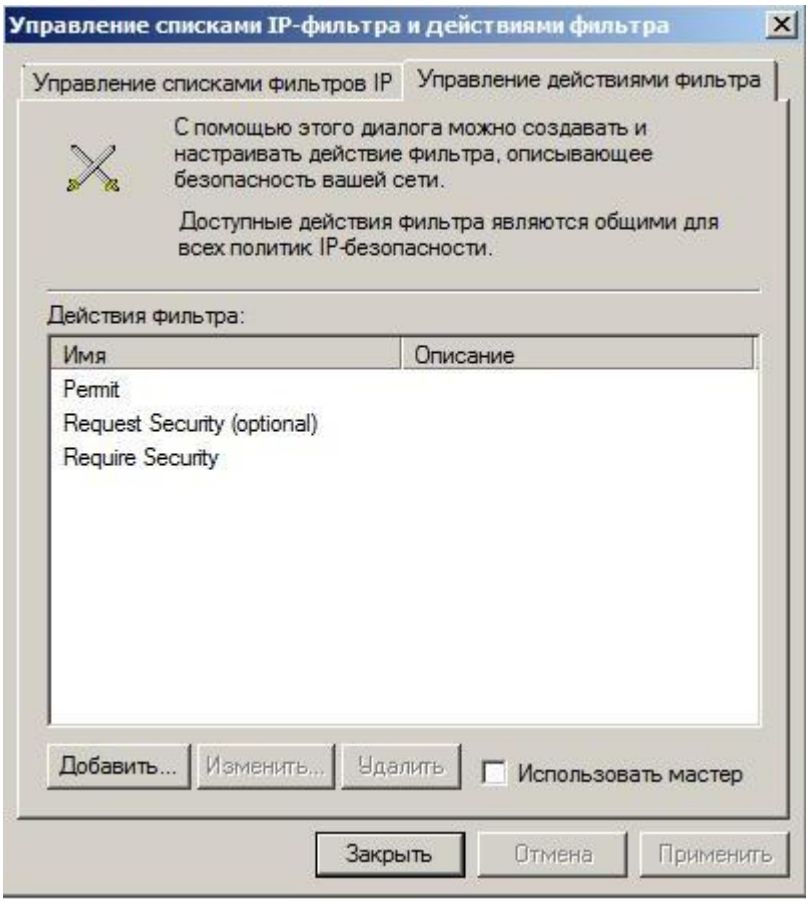

Рис. 35.

Действие к фильтру создалось с именем New Filter Action (Создание действия фильтра), тк на вкладке General (Общие) необходимо было ввести его имя. Исправим это, отредактировав его на SecurityAction.

На данном этапе были созданы фильтры и действия к ним. Перейдем к созданию непосредственно политике безопасности.

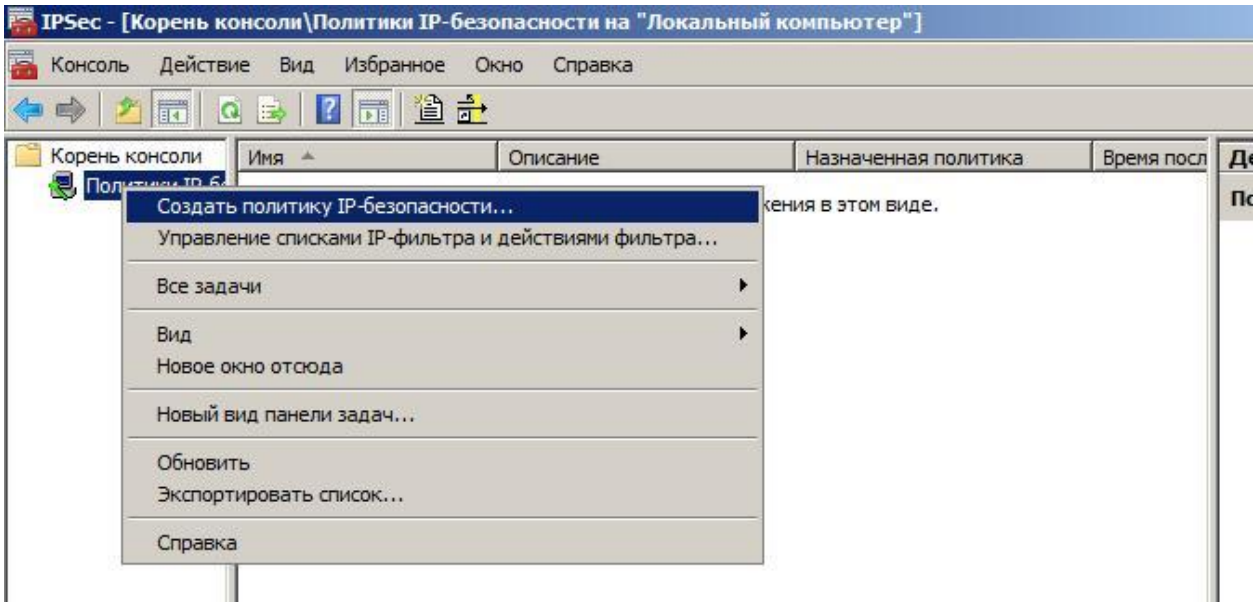

Рис. 36.

Мастер предложит ввести имя политики безопасности, далее мастер спросит о создании правила по умолчанию. Оно необходимо в случае, если входящее соединение предлагает его сделать безопасным, а фильтр на соответвующее соединение отсутсвует. В этом случае безопасное соединение будет установлено, несмотря на отсутствие фильтра.

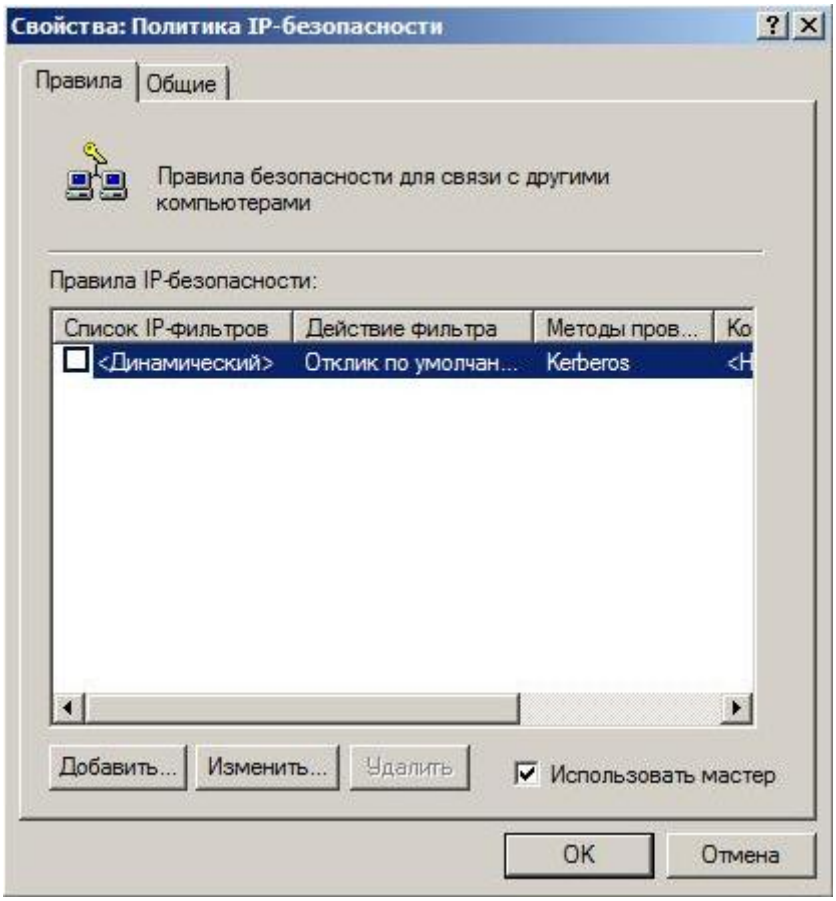

Рис. 37.

Выбор метода аутентификации. Предлагается выбрать последний метод.

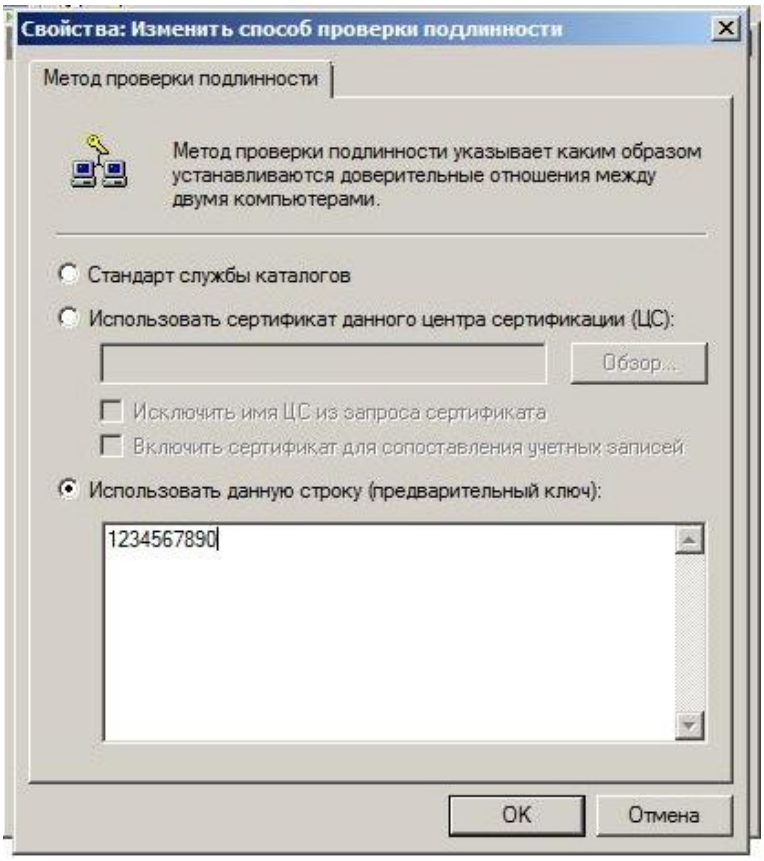
Свойства: Изменить способ проверки подлинности
Метод проверки подлинности
Метод проверки подлинности указывает каким образом устанавливаются доверительные отношения между двумя компьютерами.
Стандарт службы каталогов
Использовать сертификат данного центра сертификации (ЦС):
Обзор...
Исключить имя ЦС из запроса сертификата
Включить сертификат для сопоставления учетных записей
Использовать данную строку (предварительный ключ):
1234567890
OK
Отмена

Рис. 38.

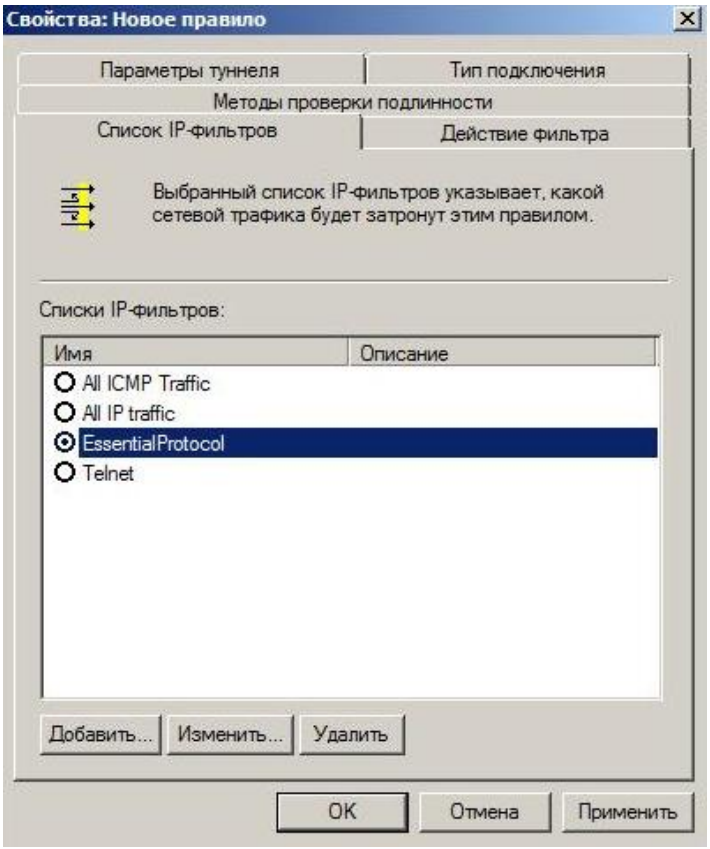
Свойства: Новое правило
Параметры туннеля
Тип подключения
Методы проверки подлинности
Список IP-фильтров
Действие фильтра
Выбранный список IP-фильтров указывает, какой сетевой трафика будет затронут этим правилом.
Списки IP-фильтров:
Имя
Описание
All ICMP Traffic
All IP traffic
EssentialProtocol
Telnet
Добавить...
Изменить...
Удалить
OK
Отмена
Применить

Рис. 39.

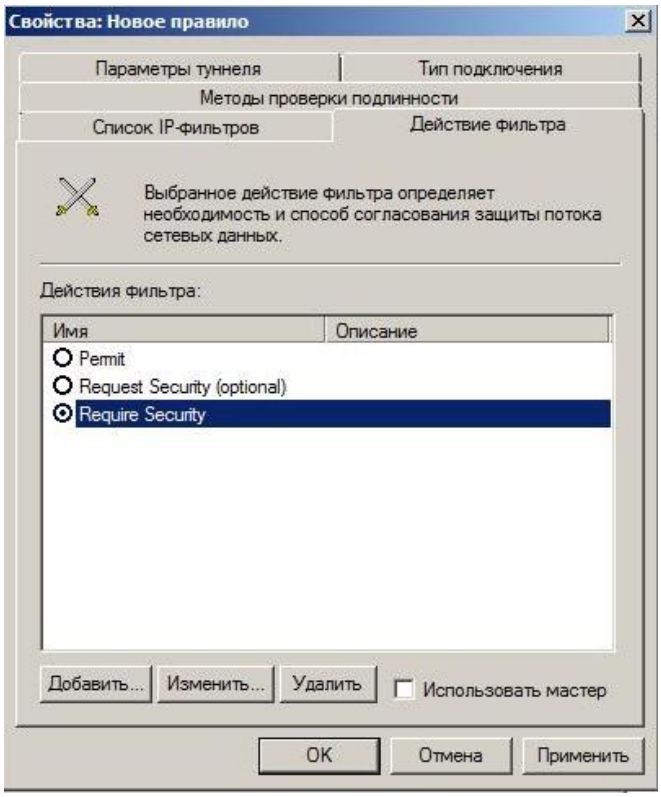
Свойства: Новое правило
Параметры туннеля
Тип подключения
Методы проверки подлинности
Список IP-фильтров
Действие фильтра
Выбранное действие фильтра определяет необходимость и способ согласования защиты потока сетевых данных.
Действия фильтра:
Имя
Описание
Permit
Request Security (optional)
Require Security
Добавить...
Изменить...
Удалить
Использовать мастер
OK
Отмена
Применить

Рис. 40.

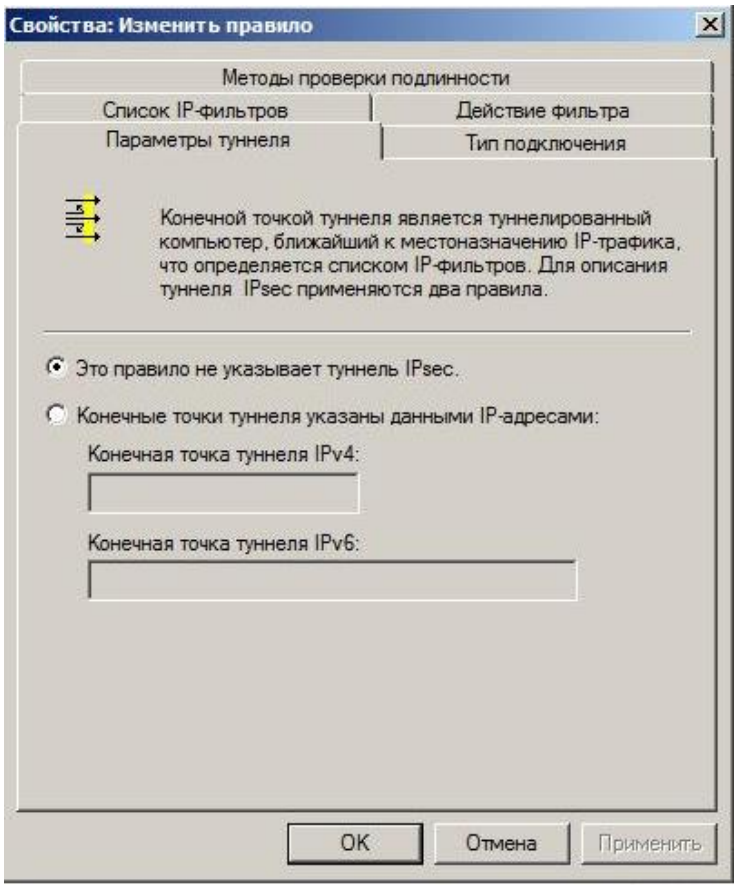
Свойства: Изменить правило
Методы проверки подлинности
Список IP-фильтров
Действие фильтра
Параметры туннеля
Тип подключения
Конечной точкой туннеля является туннелированный компьютер, ближайший к местоназначению IP-трафика, что определяется списком IP-фильтров. Для описания туннеля IPsec применяются два правила.
Это правило не указывает туннель IPsec.
Конечные точки туннеля указаны данными IP-адресами:
Конечная точка туннеля IPv4:
Конечная точка туннеля IPv6:
OK
Отмена
Применить

Рис. 41.

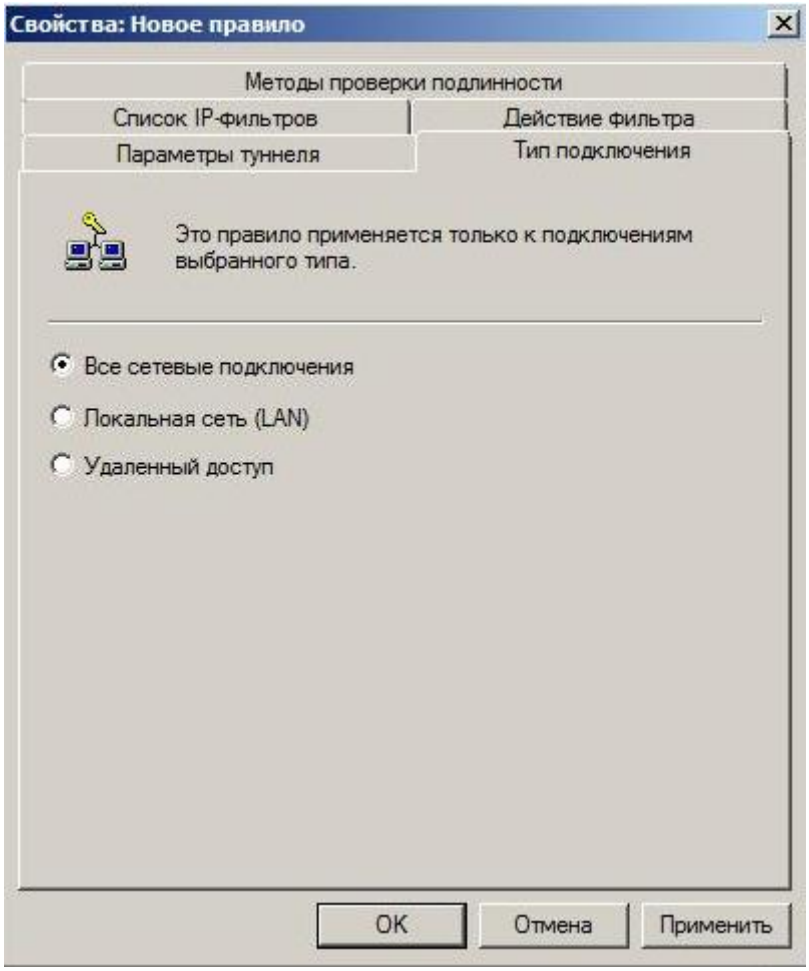

Рис. 42.

Списки добавлены, политика сформирована.

Теперь ее необходимо применить (assign (Применить))

Задание 1

Задание: Установить транспортное безопасное соединение между двумя компьютерами, находящимися в разных сетях. Компьютеры обмениваются секретной информацией по TCP на порт 5050. Для удостоверения в правильности настройки безопасное соединение будем устанавливать и по протоколу ICMP. Схема соединения представлена на рисунке.

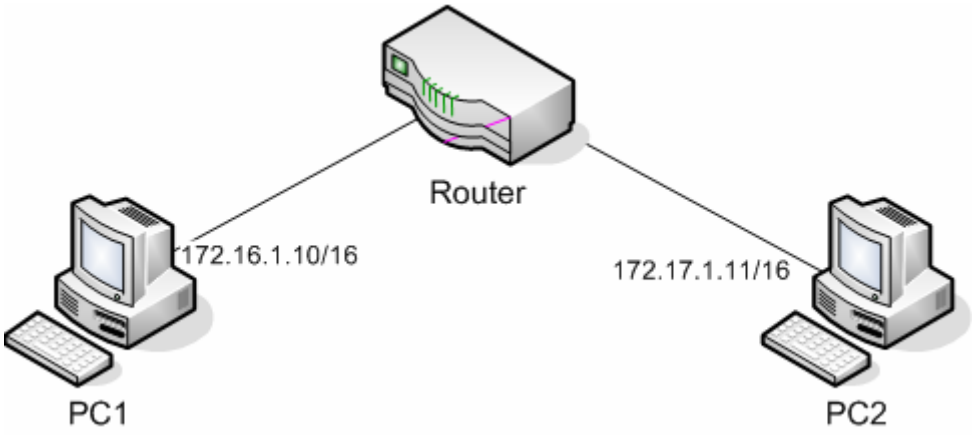

Рис. 43.

План выполнения:

- настроить маршрутизацию на одной машине (172.16.1.10/16<=>172.17.1.11)
- настроить сеть на остальных двух машинах
- настройка IPsec на машинах
    - настройка IP-фильтров
    - настройка действий IP-фильтров
    - настройка политики

IPsec настраивается только на конечных машинах.

Подразумеваем, что маршрутизация и сеть настроены.

Настройка на обоих компьютерах абсолютно идентична. Поэтому, настроив одну из машин, можно экспортировать политику в IPsec-файл и импортировать на другой.

Настройка фильтров:

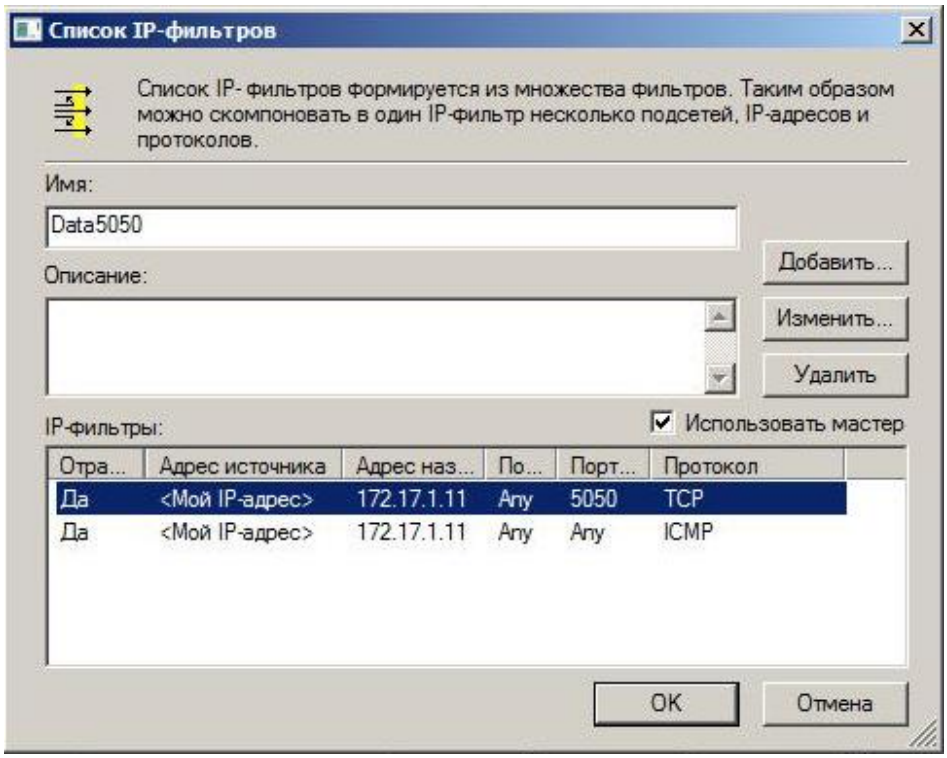

Рис. 44.

Поля Description (Описание), Source DNS Name (DNS-имя источника) и Destination DNS Name (DNS-имя приемника) скрыты.

Настройка действий IP-фильтров.

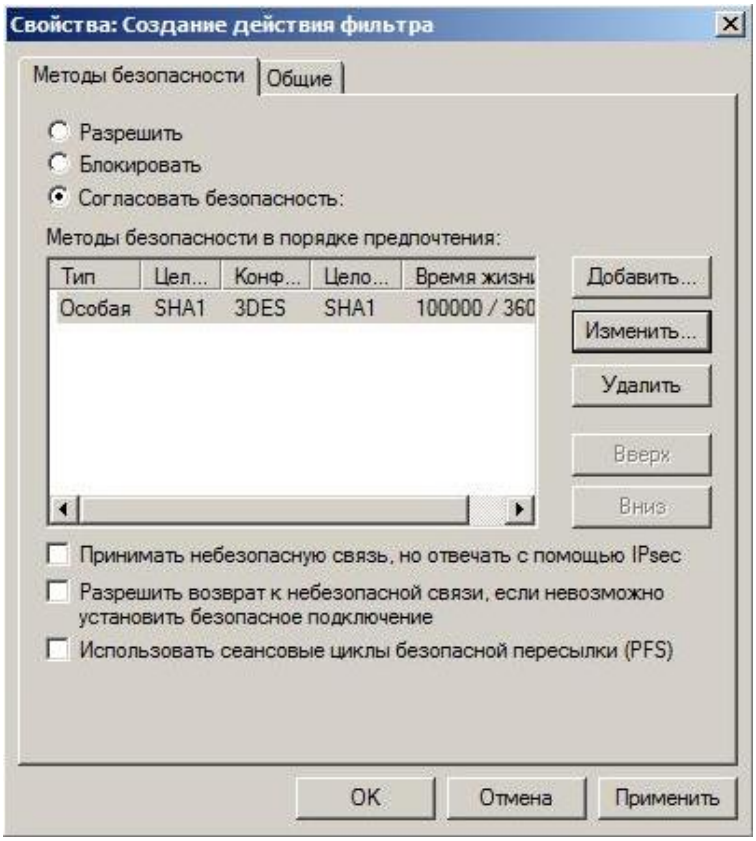

Рис. 45.

Устанавливаем имя действию и выбираем самое сильное шифрование.

Теперь создадим политику

Зададим имя потитике, правило по умолчанию использовать не будем, оставим галочку на Edit properties (изменить свойства), что бы сразу открылось окно свойств политики.

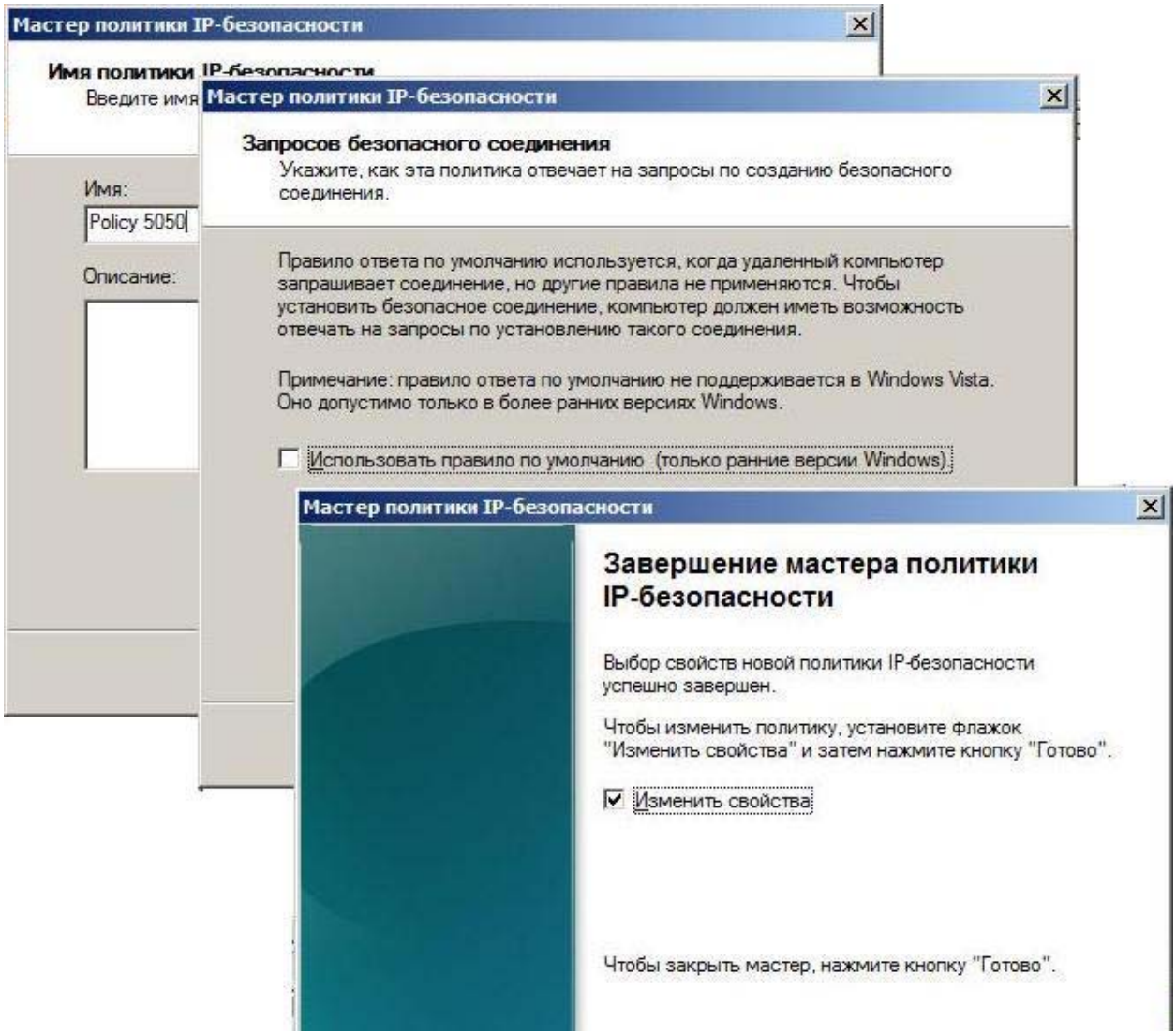

Рис. 46.

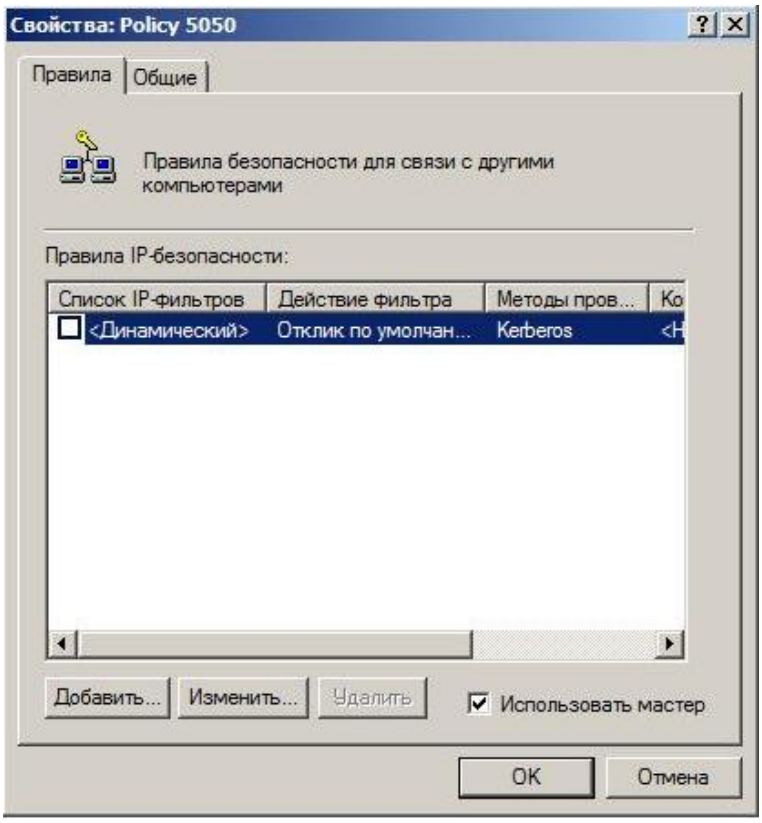
Свойства: Policy 5050
Правила
Общие
Правила безопасности для связи с другими компьютерами
Правила IP-безопасности:
Список IP-фильтров
Действие фильтра
Методы пров...
<Динамический>
Отклик по умолчан...
Kerberos
Добавить...
Изменить...
Удалить
Использовать мастер
OK
Отмена

Рис. 47.

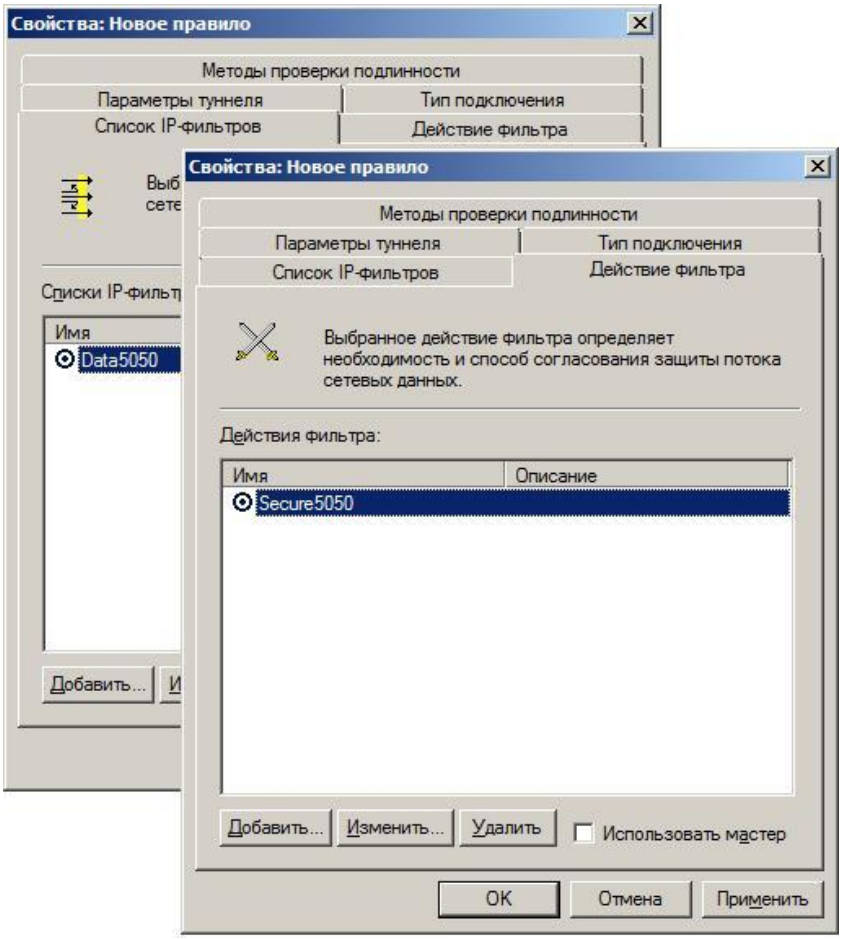
Свойства: Новое правило
Методы проверки подлинности
Параметры туннеля
Тип подключения
Список IP-фильтров
Действие фильтра
Свойства: Новое правило
Методы проверки подлинности
Параметры туннеля
Тип подключения
Список IP-фильтров
Действие фильтра
Выбранное действие фильтра определяет необходимость и способ согласования защиты потока сетевых данных.
Действия фильтра:
Имя
Описание
Secure5050
Добавить...
Изменить...
Удалить
Использовать мастер
OK
Отмена
Применить
Имя
Data5050
Добавить...

Рис. 48.

Вкладки Tunnel Settings (Параметры туннеля) и Connection Type (Тип подключения) оставляем без изменения.

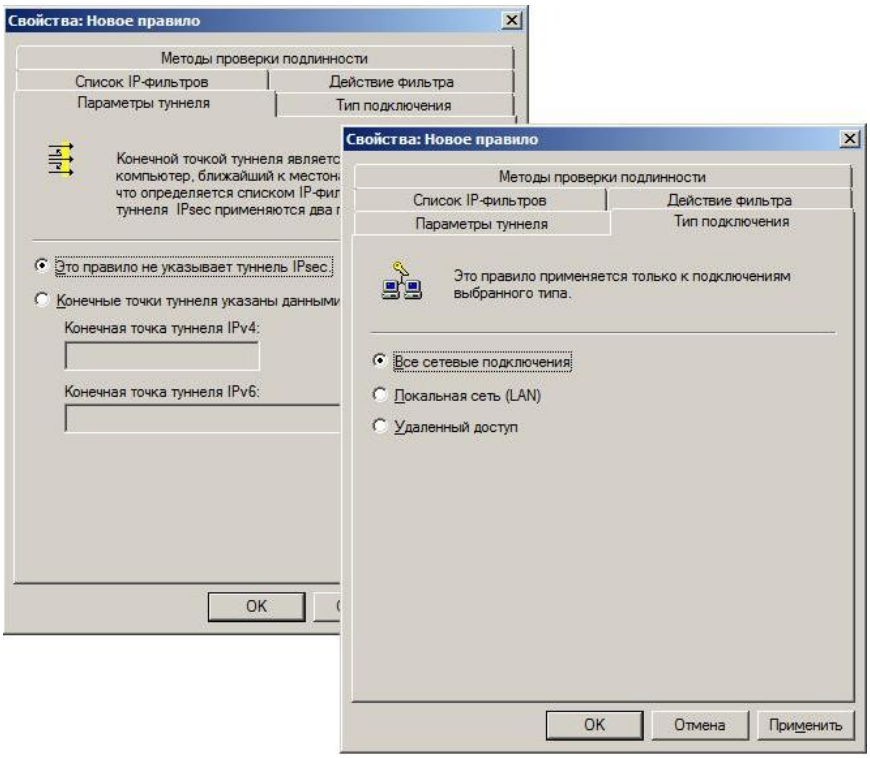

Рис. 49.

Изменим лишь метод аутентификаци, т.к. в нашей структуре о домене ничего не сказано.

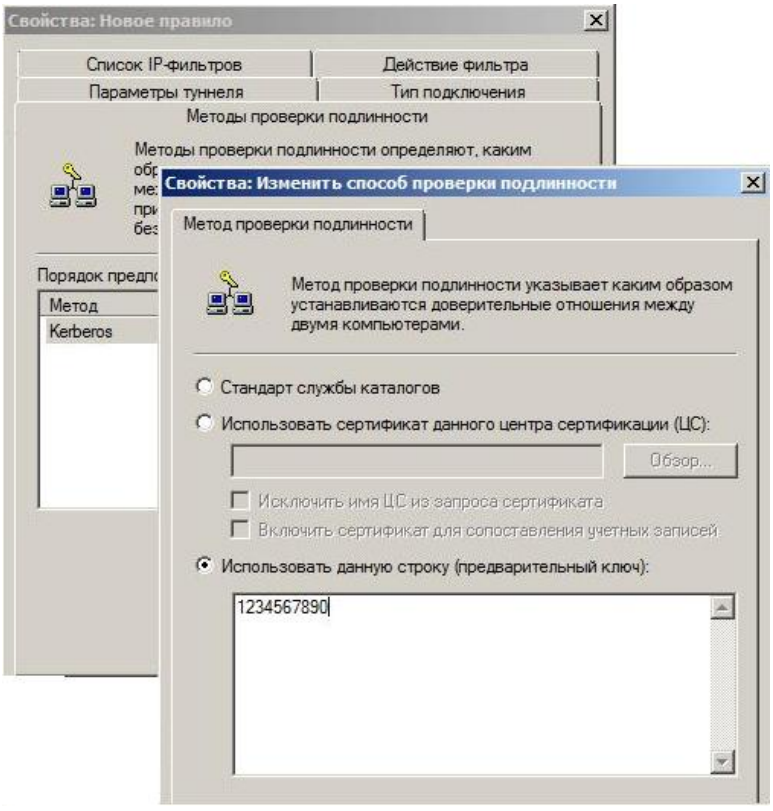

Рис. 50.

Настройка политики завершена, осталось ее активизировать:

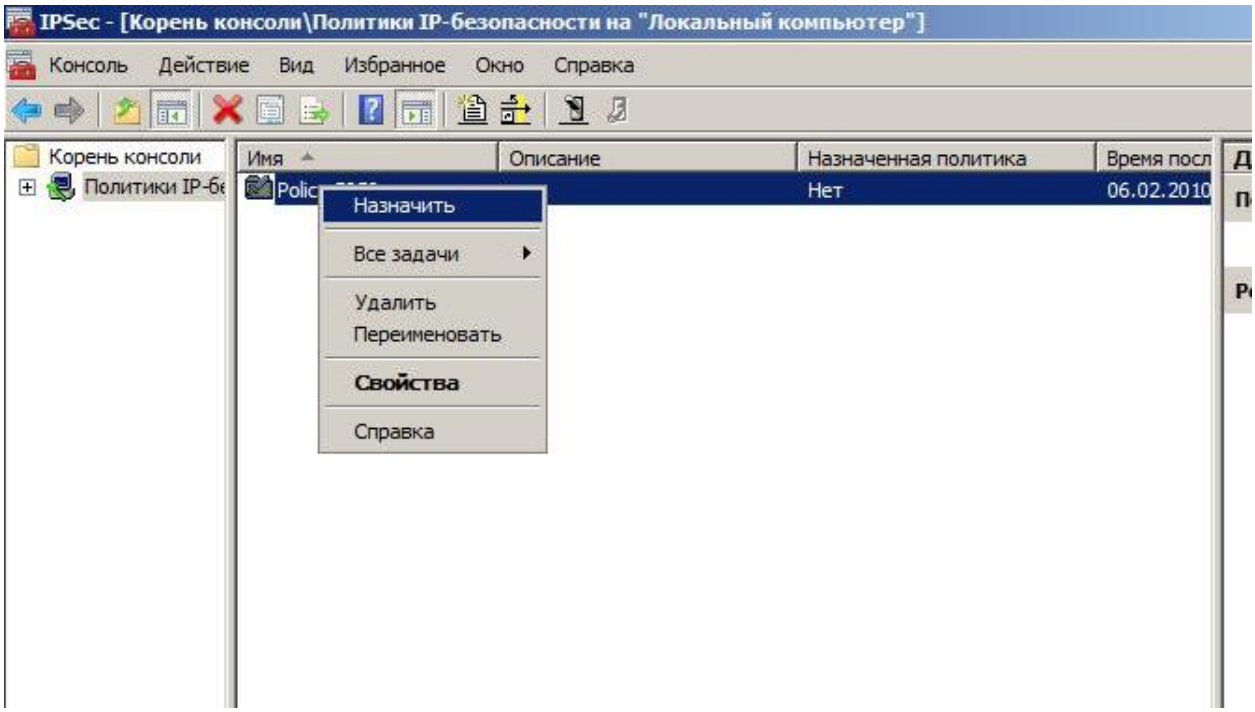

Рис. 51.

Теперь аналогичную настройку проведем на другой машине, перед этим экспортировав политики в IPsec-файл и импортируем ее на другую машину:

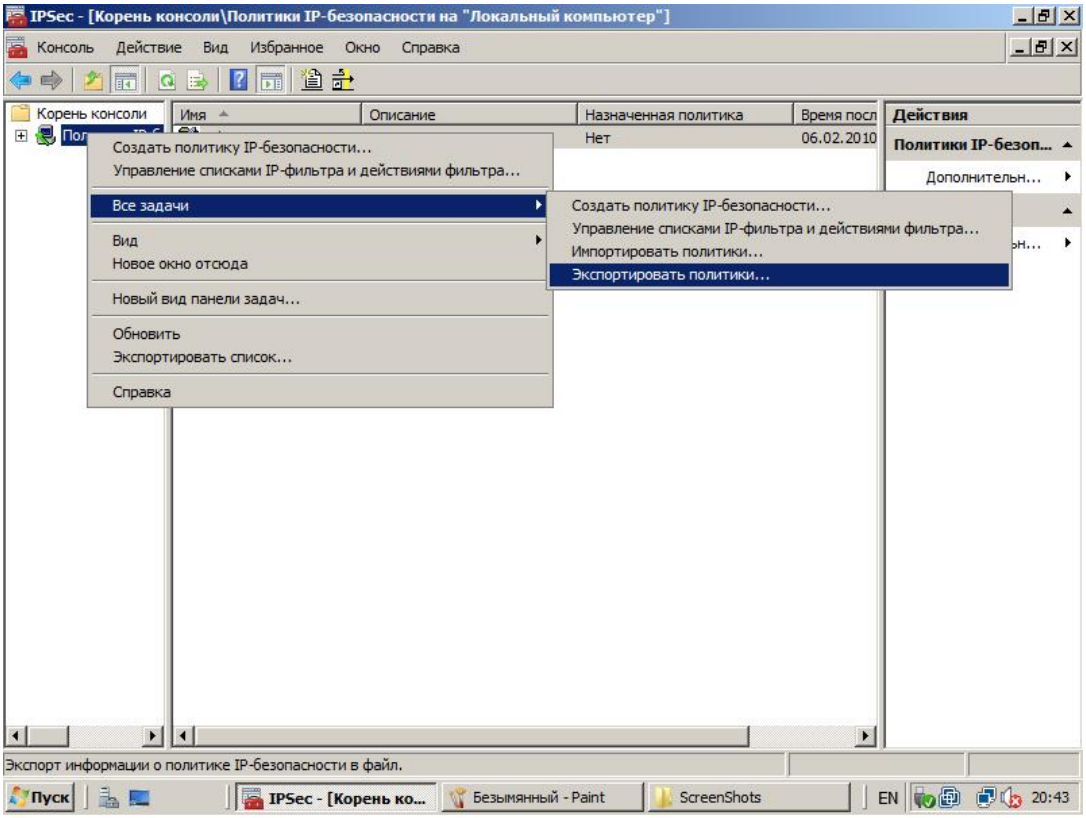

Рис. 52.

Теперь убедимся, что все настройки привели к нужному результату.

- выполним команду ping с одной машины до маршрутизатора
- выполним команду ping с одной машины до другой машины

Задание 2

Задание: Установить туннельное безопасное соединение между двумя сетями. Весь трафик обмена между сетями необходимо подписать. Схема соединения представлена на рисунке.

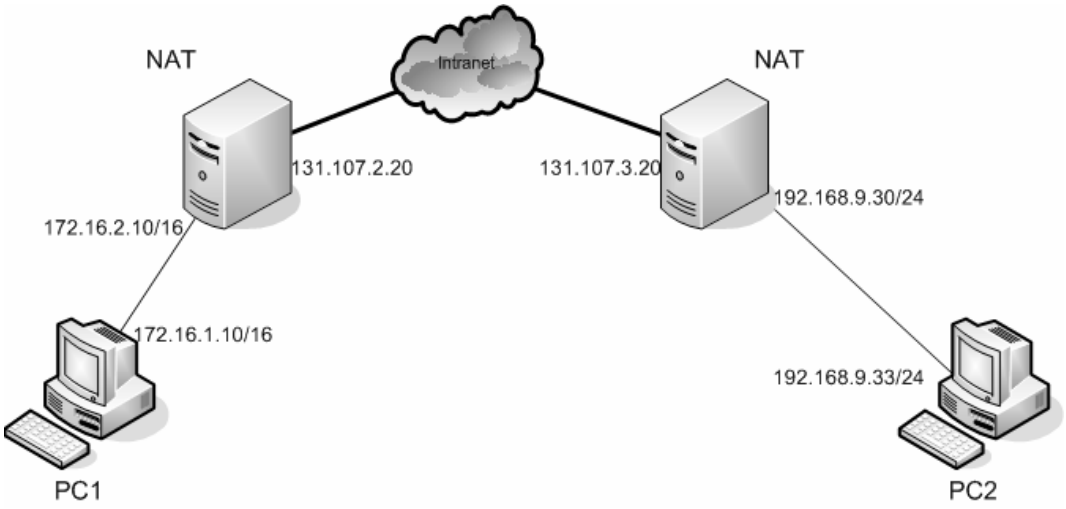

Рис. 53.

Фактически сеть выглядит следующим образом (если упростить облако Internet до одного маршрутизатора).

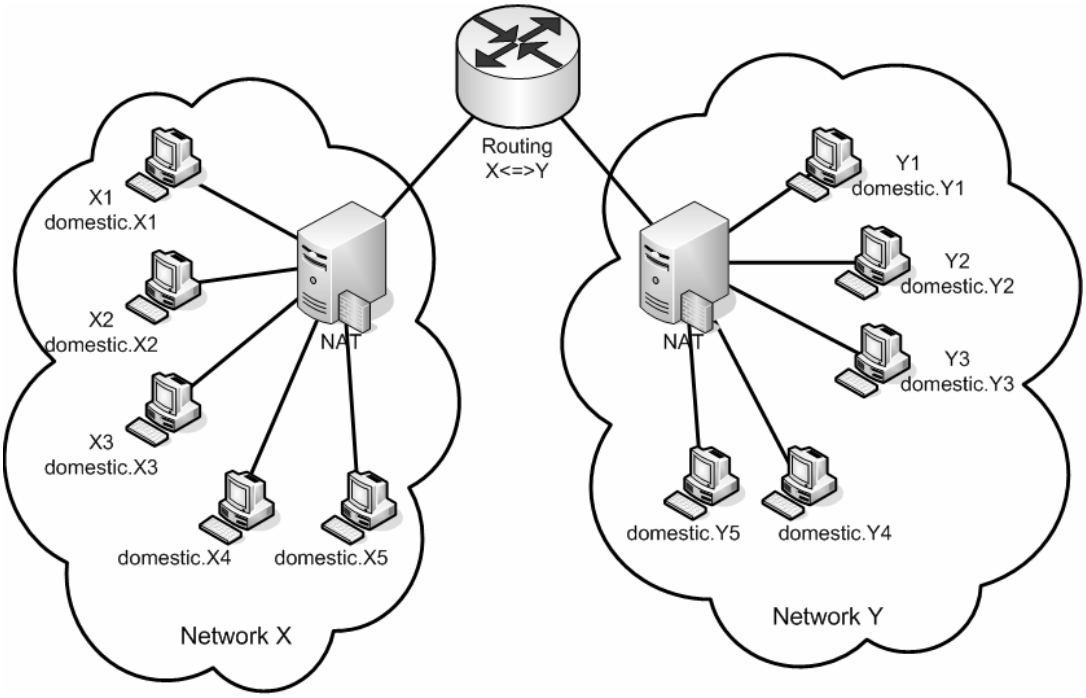

Рис. 54.

С точки зрения интернета сеть выглядит так:

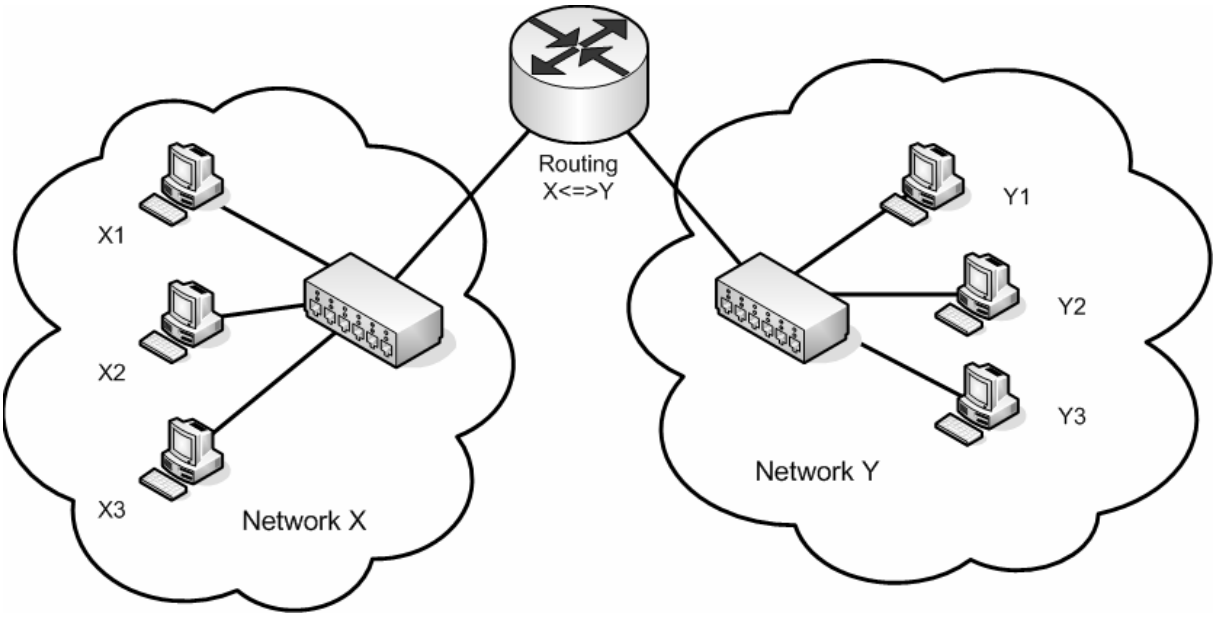

Рис. 55.

Поэтому если безопасная передача (или вообще обмен) устанавливается между компьютерами X3 и Y1, то X3 должен знать внешний адрес Y1 или если инициатором передачи выступает другой компьютер - Y1 должен знать внешний адрес X3.

Из предыдущих высказываний следует что путь безопасного соединения IPsec не может лежать через технологию NAT, тк NAT исправляет адреса источника либо приемника, что нарушает целостность пакета. Из этого следует, для того чтобы локальные сети могли выходить в интернет и имели возможность безопасного обмена между собой необходимо поставить туннельные сервера в каждой сети:

Рис. 56.

Такое решение позволит трафику направленному из одной сети в другую идти в обход серверов NAT, что позволит установить безопасное соединение.

План выполнения:

- Настроим на туннельном сервере 1 сеть 192.168.9.0/24 и сеть 131.107.0.0/16
- Настроим на туннельном сервере 2 сеть 172.16.0.0/24 и сеть 131.107.0.0/16
- Настроим сеть на машине 1.
- настройка IPsec на туннельных серверах
    - настройка IP-фильтров
    - настройка действий IP-фильтров
    - настройка политики

В связи с ограниченными ресурсами – виртуальных машин всего три, создадим аналогичную, но измененную структуру:

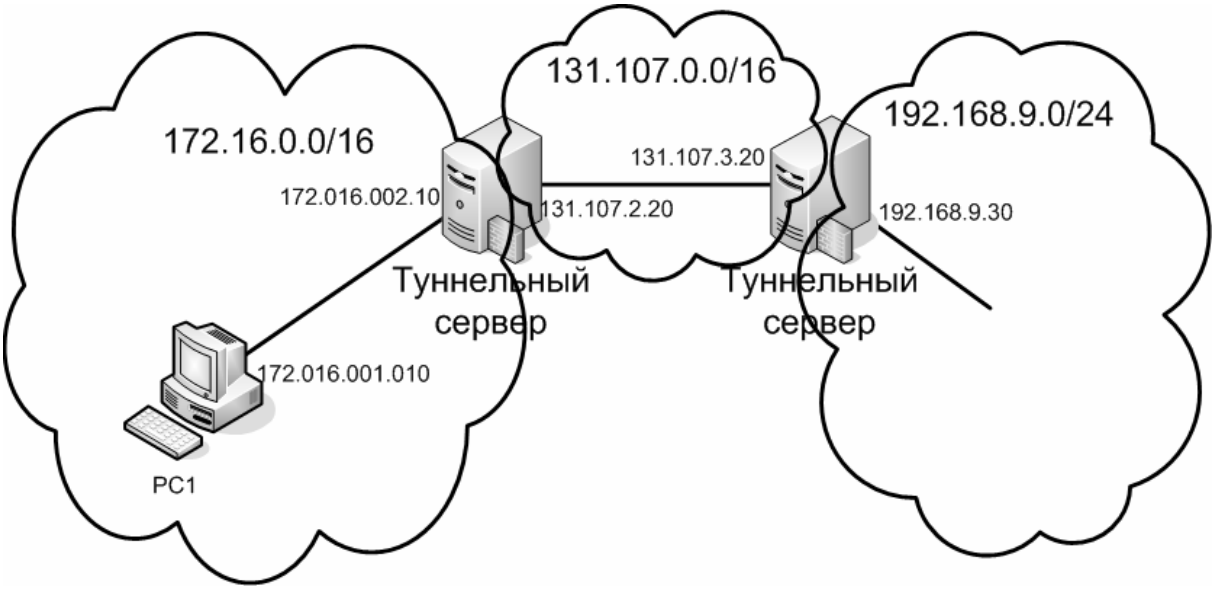

Рис. 57.

Тесты будем проводить с машины PC1 на интерфейс 192.168.9.30

Настройка IPsec проводится только на серверах. Предположим настраиваем туннельный сервер сети 172.16.0.0/16.

Фильтры и действия для туннельного сервера 1

Источник	Назначение	Протокол	Конечная точка	Действие
172.16.0.0/16	192.168.9.0/24	Любой	131.107.3.20	Согласовать
192.168.9.0/24	172.16.0.0/16	Любой	131.107.2.20	Согласовать

Покажем основные пункты настройки.

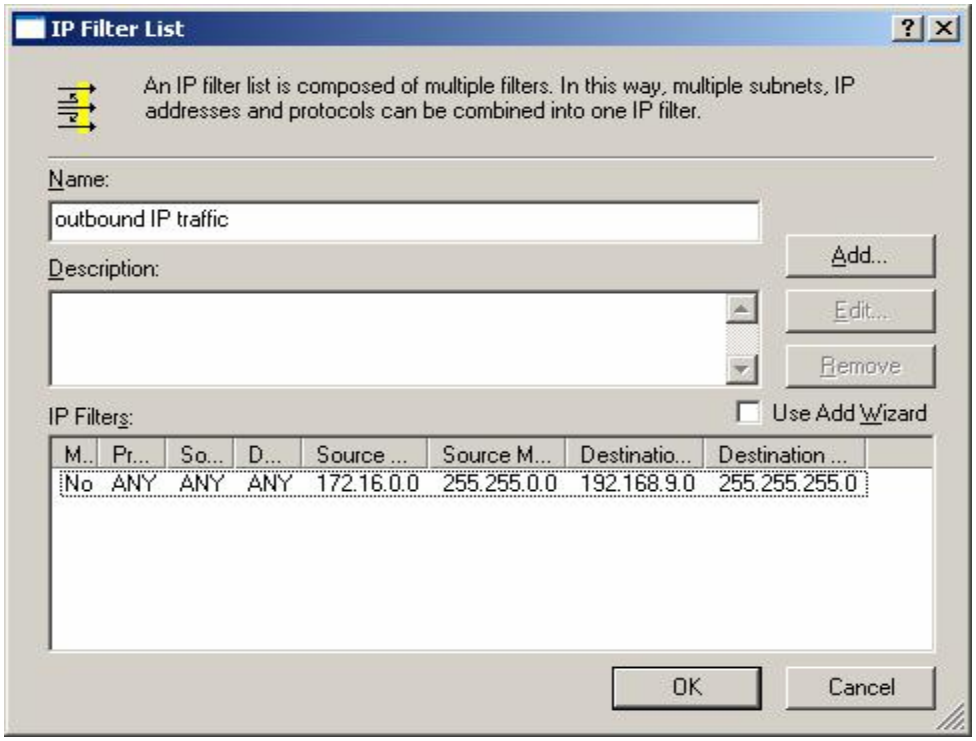

Рис. 58.

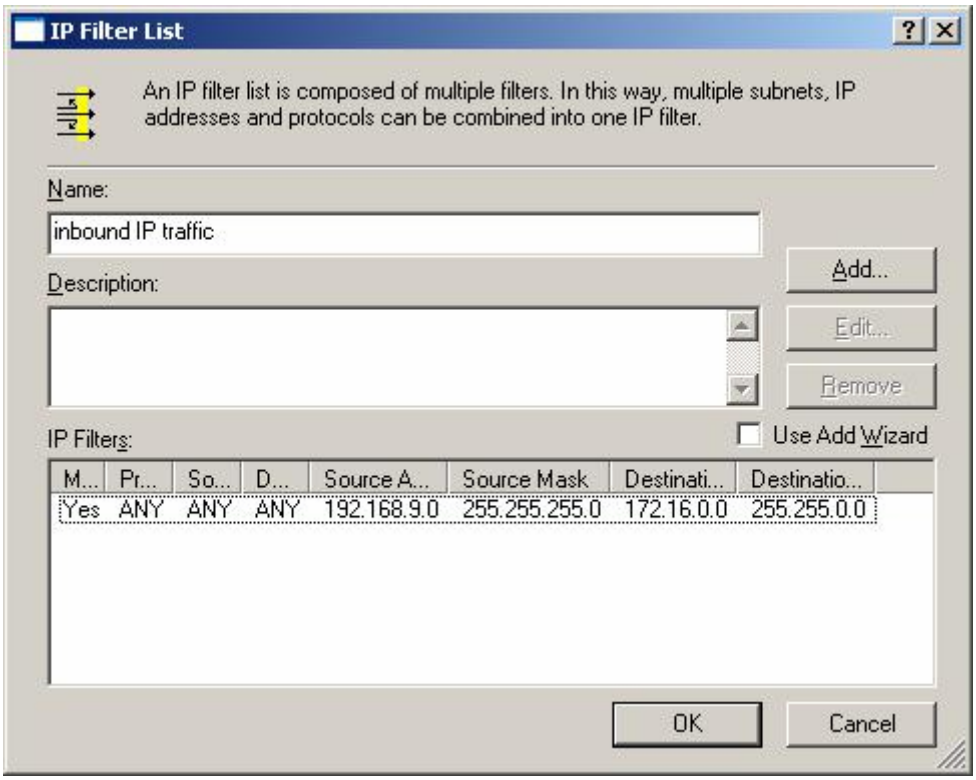

Рис. 59.

При настройке туннельного режима галочку mirrored необходимо обязательно снимать, и настраивать вручную отражение конечной точки туннеля. Иными словами создавать обратное правило если это необходимо нужно вручную без использования mirrored.

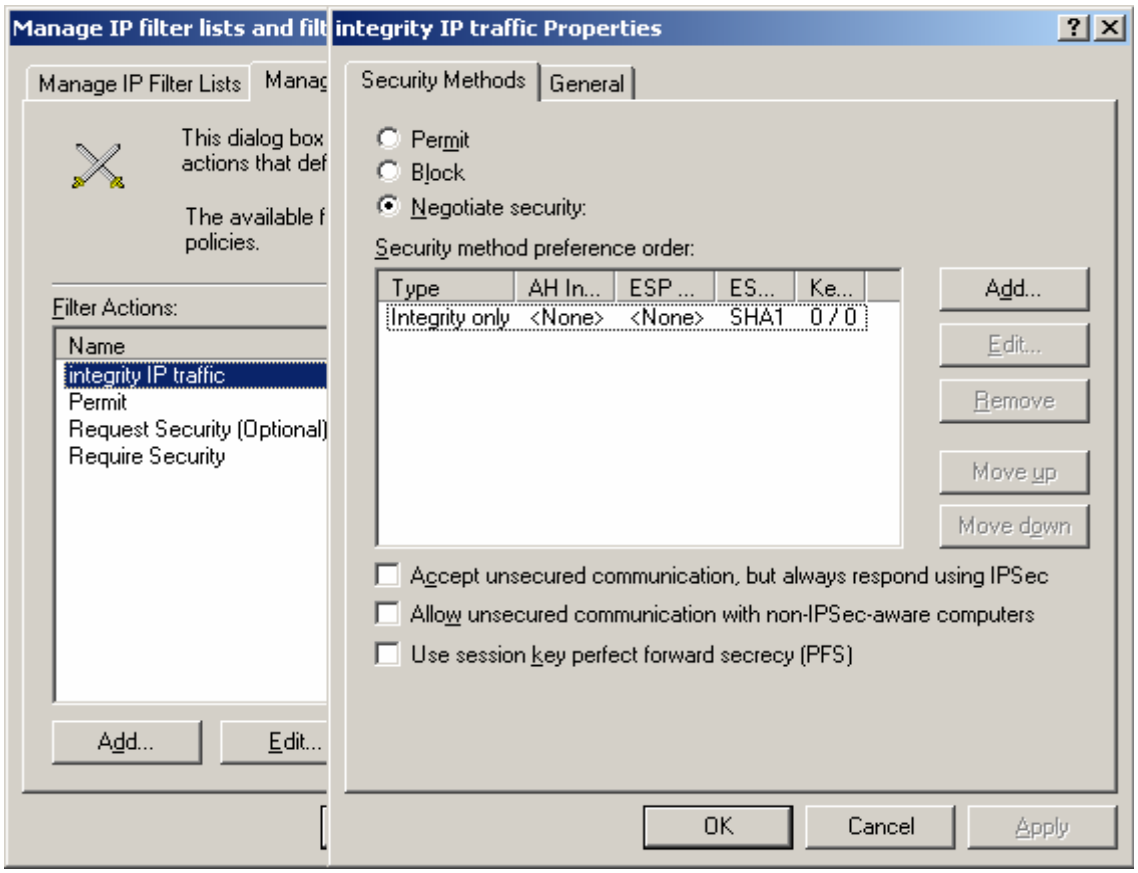
Manage IP filter lists and filt
Manage IP Filter Lists
Manag
This dialog box
actions that def
The available f
policies.
Filter Actions:
Name
integrity IP traffic
Permit
Request Security (Optional)
Require Security
Add...
Edit...
integrity IP traffic Properties
Security Methods
General
Permit
Block
Negotiate security:
Security method preference order:
Type
AH In...
ESP ...
ES...
Ke...
Integrity only
<None>
<None>
SHA1
0 / 0
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non-IPSec-aware computers
Use session key perfect forward secrecy (PFS)
OK
Cancel
Apply

Рис. 60.

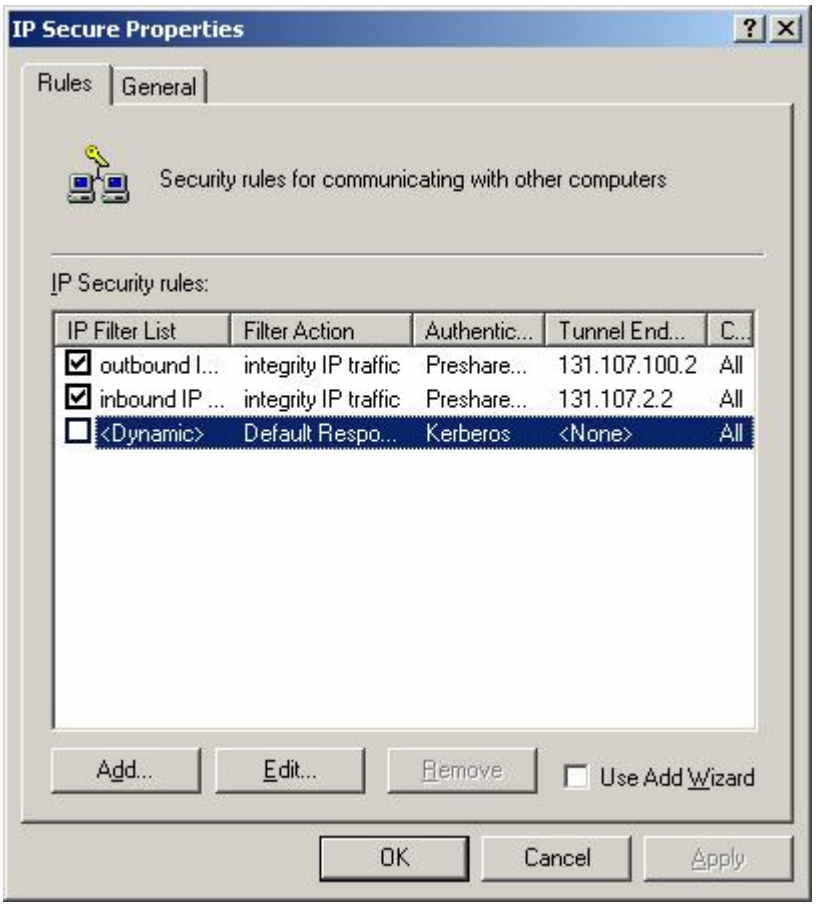
IP Secure Properties
Rules
General
Security rules for communicating with other computers
IP Security rules:
IP Filter List
Filter Action
Authentic...
Tunnel End...
C...
outbound I...
integrity IP traffic
Preshare...
131.107.100.2
All
inbound IP ...
integrity IP traffic
Preshare...
131.107.2.2
All
<Dynamic>
Default Respo...
Kerberos
<None>
All
Add...
Edit...
Remove
Use Add Wizard
OK
Cancel
Apply

Рис. 61.

На рисунке показана настройка для туннельного сервера с адресом 131.107.2.20. Настройка политики для другого туннельного аналогична, стоит лишь поменять названия фильтров inbound IP traffic и outbound IP traffic на противоположные.
Теперь для полной работоспособности осталось добавить статические маршруты на обоих серверах. Выход в 192.168.9.0/24 из 172.16.0.0/16 осуществляется через шлюз 131.107.3.20. А выход в 172.16.0.0/16 из 192.168.9.0/24 через шлюз 131.107.2.20.

Необходимо проверить работоспособность политики.

Наблюдать за соединениями IPsec можно используя IPsecmon.exe (можно вызвать из командной строки Start->Run, если установлена система Windows 2000, либо добавив оснастку IP Security Monitor – для Windows 2003)

Практическая часть (детальные операции)

Запуск оснастки управления политикой безопасности IP

1. Нажмите кнопку **Пуск**, выберите команду **Выполнить**, введите **MMC** и нажмите кнопку **OK**.
2. Выберите **Управление политикой безопасности IP** и нажмите кнопку **Добавить**.
3. Выберите компьютер, политиками IPSEC которого требуется управлять.

Чтобы	**Выполните следующие действия**
Управлять только компьютером, на котором выполняется консоль.	Выберите **Локальный компьютер**.
Управлять политиками IPSEC для любого члена домена	Выберите **Управлять политикой домена для этого компьютера**.
Управлять политиками IPSEC для домена, членом которого компьютер, на котором выполняется консоль, не является	Выберите **Управлять политикой домена для другого домена**.
Управлять удаленным компьютером	Выберите **Другой компьютер**.

4. Нажмите кнопку **Готово**, кнопку **OK**, а затем в меню **Консоль** выберите команду **Сохранить**, чтобы сохранить настройки консоли.

Чтобы добавить или изменить политику IPSEC

1. В оснастке «Управление политикой безопасности IP» выберите создание новой политики или изменение текущей.

Чтобы	**Выполните следующие действия**
Создать новую политику	Выберите в дереве консоли **Политики безопасности IP на** *описание*, а затем выберите в меню **Действие** команду **Создать политику безопасности IP**. Выполняйте инструкции мастера политики безопасности IP до вывода на

	экран диалогового окна новой политики.
Изменить существующую политику	Щелкните нужную политику правой кнопкой мыши и выберите команду **Свойства**.

2. На вкладке **Общие** введите уникальное имя в поле **Имя**.
3. В поле **Описание** введите описание политики безопасности, например укажите группы или домены, которые она затрагивает.
4. Если компьютер является частью домена, введите значение в поле **Проверять политику на наличие изменений каждые** *число* **минут**, чтобы задать частоту выполнения агентом политики проверки групповой политики на наличие обновлений
5. При наличии особых потребностей в безопасности при обмене ключами нажмите кнопку **Дополнительно**.
6. Перейдите на вкладку **Правила** и создайте все необходимые правила для политики.

Чтобы добавить и изменить правила

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите, следует ли использовать мастер добавления:
   - чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению правила безопасности, убедитесь в том, что флажок **Использовать мастер** установлен, нажмите кнопку **Далее** и следуйте выводимым на экран инструкциям;
   - для того чтобы добавить или изменить правило вручную, снимите флажок **Использовать мастер**, нажмите кнопку **Добавить** или **Изменить** и выполните следующие шаги данной процедуры.
3. На соответствующих вкладках задайте список фильтров IP, действие фильтра, тип подключения, методы проверки подлинности и параметры туннеля.

Чтобы активизировать правила

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Установите флажки для правил, которые требуется активизировать, или снимите флажки для отключения правил.

Чтобы определить методы проверки подлинности IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.
3. На вкладке **Методы проверки подлинности** нажмите кнопку **Добавить**. При изменении настроек существующего метода выберите изменяемый метод проверки подлинности и нажмите кнопку **Изменить**.

4. Определите методы проверки подлинности:
   - выберите **Стандарт Kerberos V5**, чтобы использовать для служб проверки подлинности протокол безопасности Kerberos V5, если данное правило применяется к компьютерам, которые заверены доверенным доменом Windows;
   - чтобы использовать для служб проверки подлинности сертификат открытого ключа, выберите **Использовать сертификат данного Центра сертификации**.
   - Если выбрано использование сертификата, нажмите кнопку **Обзор** для выбора корневого центра сертификации.
   - Чтобы указать для использования при проверке подлинности собственный ключ, выберите **Использовать данную строку для защиты обмена ключами**.

Чтобы добавить или изменить списки фильтров IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. В диалоговом окне свойства политики безопасности IP выберите правило, в которое требуется добавить новый список фильтров IP, и нажмите кнопку **Изменить**.
3. При добавлении нового списка фильтров IPSEC нажмите кнопку **Добавить** на вкладке **Список фильтров IP**. При изменении существующего списка фильтров выберите нужный список фильтров и нажмите кнопку **Изменить**.
4. Введите уникальное имя для списка.
5. Введите описание, например, типы трафика, которые представляет данный список.
6. Создайте фильтры.

Чтобы добавить или изменить фильтры IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, содержащее фильтр IP, который следует изменить, и нажмите кнопку **Изменить**.
3. Выполните одно из следующих действий.
   - При добавлении фильтра IPSEC нажмите кнопку **Добавить** на вкладке **Список фильтров IP**.
   - При изменении существующего списка фильтров IP выберите нужный фильтр и нажмите кнопку **Изменить**.
4. В диалоговом окне **Список фильтров IP** выполните одно из следующих действий.

Чтобы	**Выполните следующие действия**
Воспользоваться мастером фильтров IP для создания фильтра	Убедитесь, что флажок **Использовать мастер** установлен.
Создать фильтр вручную	Снимите флажок **Использовать мастер** и нажмите кнопку **Добавить**.

Изменить существующий фильтр	Снимите флажок **Использовать мастер** и нажмите кнопку **Изменить**.

5. На вкладке **Адресация** выберите **Адрес источника пакетов**.

Значение	**Задает защиту для пакетов, полученных**
Мой IP-адрес	со всех IP-адресов на компьютере, для которого предназначается данный фильтр.
Любой IP-адрес	от любого компьютера
Определенный IP-адрес	с IP-адреса, указанного в поле **IP-адрес**.
Определенная подсеть IP	с IP-адреса, указанного в поле **Маска подсети**.

6. Перейдите в группу **Адрес назначения пакетов** и повторите шаг 5 для адреса назначения.
7. Установите флажок **Отраженные** в нужное положение.

Чтобы	**Выполните следующие действия**
Создать фильтр для защиты трафика между исходным и конечным компьютером. (Фильтрация для защиты трафика в одном направлении не поддерживается.)	Установите флажок **Отраженные**
Создать фильтр, разрешающий или запрещающий трафик.	Можно установить флажок **Отраженные**, но не обязательно.
Создать фильтр для туннеля IPSEC	Снимите флажок **Отраженные** и создайте два правила с различными списками фильтров.

8. На вкладке **Описание** введите описание фильтра. (Например, укажите, к каким узлам и типам трафика он применяется.)
9. (Необязательно.) При необходимости в дополнительной фильтрации IP по конкретному протоколу или номеру порта настройте дополнительные параметры фильтра на вкладке **Протокол**.

Чтобы настроить дополнительные параметры фильтра IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, содержащее фильтр IP, который следует изменить, и нажмите кнопку **Изменить**.
3. На вкладке **Список фильтров IP** выберите фильтр, который требуется изменить, и нажмите кнопку **Изменить**.
4. Перейдите на вкладку **Протокол**.
5. Выберите нужное значение в поле **Выберите тип протокола**:

Чтобы фильтровать	**Выполните следующие действия**
Любые пакеты, отправленные и принятые по любому из протоколов семейства TCP/IP	Выберите значение **Любой**.
Пакеты, отправленные по конкретному протоколу	Выберите нужный протокол.
Пакеты, отправленные по протоколу, не входящему в список	Выберите **Другое** и введите номер протокола.

6. (Необязательно.) При выборе протокола TCP или UDP можно также фильтровать пакеты по порту источника.
   - Для того чтобы выполнялась попытка защитить каждый пакет, отправленный на любой порт, используемый выбранным типом протокола, выберите **Пакеты из любого порта**.
   - Для того чтобы выполнялась попытка защитить каждый пакет, отправленный на конкретный порт, используемый выбранным типом протокола, выберите **Пакеты из этого порта**.
7. Выберите порт назначения:
   - Для фильтрации пакетов, полученных на любой порт, используемый выбранным типом протокола, выберите **Пакеты на любой порт**.
   - Чтобы фильтровать только пакеты, полученные на порт с указанным номером, выберите **Пакеты на этот порт**.

Чтобы активизировать список фильтров IP

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.
3. На вкладке **Список фильтров IP** выберите список фильтров IP, который требуется назначить в качестве активного списка для данного правила.

Выбранный список фильтров IP станет активным списком для данного правила.

Чтобы добавить и изменить действия фильтра

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, нажмите кнопку **Изменить**, а затем перейдите на вкладку **Действие фильтра**.
3. Выберите, следует ли использовать мастер добавления:
   - чтобы использовать мастер, помогающий последовательно выполнить операции по добавлению действия фильтра, убедитесь в том, что флажок **Использовать мастер** установлен, а затем следуйте выводимым на экран инструкциям;
   - для того чтобы выполнить добавление или изменение действий фильтра вручную, снимите флажок **Использовать мастер**, а затем нажмите кнопку **Добавить** для добавления действия фильтра или кнопку **Изменить** для изменения настроек действия фильтра.
4. Выберите действие фильтра.
   - Выберите **Разрешить**, чтобы разрешить получение или отправку незашифрованных пакетов. Безопасность для этих пакетов запрашиваться не будет.
   - Выберите **Блокировать**, чтобы пакеты, совпадающие с данным фильтром, немедленно отбрасывались. Безопасность для этих пакетов запрашиваться не будет.
   - Выберите **Согласовать безопасность**, чтобы использовать для обеспечения безопасности пакетов, совпадающих с фильтром, методы безопасности из списка **Методы безопасности в порядке предпочтения**. Запросы безопасности для этих пакетов будут приниматься.
5. Если входящие незащищенные пакеты блокировать не требуется, но необходимо обеспечить безопасность исходящих запросов и последующего двустороннего обмена данными, установите флажок **Принимать небезопасную связь, но отвечать с помощью IPSEC**.
6. Если требуется сделать возможной связь с другими компьютерами, не поддерживающими IPSEC, и обеспечить продолжение связи при отсутствии ответа на запрос согласования безопасности IPSEC, установите флажок **Разрешать связь с компьютерами, не поддерживающими IPSEC**. Если этот параметр включен, то после сбоя согласования IPSEC с конкретным узлом безопасность IPSEC для связи с этим узлом отключается на некоторое время.
7. Установка флажка **Сеансовые циклы безопасной пересылки (PFS)** гарантирует, что основные ключи или исходные данные ключа не используются для создания ключа сеанса более одного раза.
8. На вкладке **Общие** введите уникальное имя.
9. Введите описание. Например, можно указать уровни безопасности, представляемые данным действием ключа.
10. Если выбрано действие **Согласовать безопасность**, добавьте новые или измените существующие методы безопасности для действия фильтра.

Чтобы добавить или изменить методы безопасности IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.

3. На вкладке **Действие фильтра** выберите действие фильтра, которое требуется изменить, и нажмите кнопку **Изменить**.
4. Выберите добавление нового метода безопасности или изменение существующего:
   - чтобы добавить новый метод безопасности, нажмите кнопку **Добавить** на вкладке **Методы безопасности**;
   - при изменении настроек существующего метода выберите изменяемый метод безопасности и нажмите кнопку **Изменить**.
5. Задайте уровень безопасности.

Чтобы	**Выполните следующие действия**
Использовать протокол ESP для шифрования данных (обеспечивает защиту) по алгоритму DES с проверкой целостности по алгоритму MD5 и стандартными параметрами ключа (100 000 Кбайт, 1 час).	Выберите **Высокая безопасность (ESP)**.
Использовать протокол AH для подписания (обеспечения целостности) сведений об адресации пакета (заголовок IP) и данных с применением алгоритма проверки целостности MD5 и стандартных параметров ключа (100 000 Кбайт, 1 час).	Выберите **Средняя безопасность (AH)**.
Использовать настраиваемые уровни безопасности.	Выберите **Настраиваемая безопасность**, нажмите кнопку **Настроить**, а затем установите нужные параметры.

6. Повторите эту процедуру для настройки дополнительных методов безопасности для действия фильтра.

Чтобы настроить дополнительные методы безопасности IPSEC

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.
3. На вкладке **Действие фильтра** выберите действие фильтра, которое требуется изменить, и нажмите кнопку **Изменить**.
4. Выберите добавление нового метода безопасности или изменение существующего.

5. Чтобы добавить новый метод безопасности, нажмите кнопку **Добавить** на вкладке **Методы безопасности**.
6. Чтобы изменить существующий метод, выберите изменяемый метод безопасности и нажмите кнопку **Изменить**.
7. Выберите вариант **Настраиваемая безопасность** и нажмите кнопку **Параметры**.
8. Чтобы обеспечить целостность сведений об адресации пакета (заголовок IP) и данных, установите флажок **Целостность данных и адресов без шифрования (AH)**.
9. При выборе протокола **AH** выберите алгоритм проверки целостности:
   - для использования 128-разрядного значения ключа выберите **MD5**;
   - для использования 160-разрядного значения выберите **SHA1**.
10. Чтобы обеспечить целостность и шифрование (защиту) данных, установите флажок **Целостность данных с шифрованием (ESP)**
11. При выборе протокола **ESP** выберите алгоритм проверки целостности данных. Если включено использование протокола **AH**, то для улучшения быстродействия можно выбрать значение **Нет**. Если протокол **AH** не используется, необходимо выбрать алгоритм проверки целостности для ESP. Варианты перечислены на шаге 9.
12. При выборе протокола **ESP** выберите алгоритм шифрования.

Чтобы	**Выполните следующие действия**
Использовать алгоритм, обеспечивающий максимальную безопасность	Выберите **3DES**.
Шифровать данные для обеспечения конфиденциальности, но не использовать максимальную безопасность 3DES	Выберите **DES**.
Не использовать шифрование	Выберите **Нет**.

Чтобы активизировать действие фильтра

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Выберите правило, которое требуется изменить, и нажмите кнопку **Изменить**.
3. На вкладке **Действие фильтра** выберите действие фильтра, которое требуется активизировать для данного правила.

Чтобы настроить обмен ключами

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Общие** и нажмите кнопку **Дополнительно**.
3. Чтобы задать создания нового основного ключа для каждого сеанса, установите флажок **Основной ключ безопасной пересылки (PFS)**.

4. Если требуется задать другой режим, введите значение в поле **Проверять подлинность и создавать новый ключ через каждые (минут)**, что вызовет проверку подлинности и создание нового ключа через заданный интервал.
5. Если требуется задать другой параметр, введите значение в поле **Проверять подлинность и создавать новый ключ через каждые (сеансов)**, чтобы задать максимальное число сеансов использования одного основного ключа или его базовых данных для создания ключа сеанса. По достижении этого предела будет выполняться проверка подлинности и создание нового ключа.
6. При наличии особых потребностей в отношении методов безопасности при обмене ключами нажмите кнопку **Методы**.

Чтобы создать методы обмена ключами

1. В оснастке «Управление политикой безопасности IP» щелкните правой кнопкой политику, которую требуется изменить, и выберите команду **Свойства**.
2. Перейдите на вкладку **Общие**, нажмите кнопку **Дополнительно**, а затем нажмите кнопку **Методы**.
3. Нажмите кнопку **Добавить** или, в случае изменения существующего метода, выберите нужный метод безопасности и нажмите кнопку **Изменить**.
4. Выберите **Алгоритм проверки целостности**:
   - для использования 128-разрядного значения выберите **MD5**;
   - для использования 160-разрядного значения (более надежно) выберите **SHA**.
5. Выберите **Алгоритм шифрования**:
   - для использования алгоритма максимальной безопасности выберите **3DES**;
   - при необходимости подключения к компьютеру, не имеющему 3DES, или в случае, если высокая безопасность не требуется, выберите **DES**. Дополнительные сведения о криптографических параметрах см. в разделе «Специальные аспекты IPSEC».
6. Выберите значение в поле **Группа Диффи-Хелмана**, чтобы задать длину базовых данных для создания ключа:
   - для использования 768 бит данных выберите **Низкая (1)**;
   - для использования 1024 бит данных выберите **Средняя (2)**.

Чтобы назначить политику IPSEC групповой политике

1. В консоли, из которой выполняется управление групповой политикой, выберите объект групповой политики, которому требуется назначить политику IPSEC.
2. Раскройте узлы **Конфигурация компьютера**, **Конфигурация Windows** и **Параметры безопасности**.
3. Щелкните папку **Политики безопасности IP**.
4. Щелкните правой кнопкой политику, которую требуется назначить, и выберите команду **Назначить**.

Чтобы активизировать политику IPSEC на компьютере

1. В оснастке «Управление политикой безопасности IP» щелкните папку **Политики безопасности IP**.

2. Щелкните правой кнопкой политику, которую требуется назначить, и выберите команду **Назначить**.

Контрольные вопросы

Литература