65535 allow ip from any to any

9) На хосте А добавить правила файрвола, которые обеспечивают политику доступа, указанную в задании, для файрвола открытого типа.

10) Выполнить действия, изложенные в пункте 4).

11) На хосте А сохранить правила файрвола в файл таким, например, образом:

#ipfw list > file_list2.txt

Требования к содержанию отчета

Отчет должен включать:

- цели и программу проведения исследований;
- листинги или скриншоты выполненных команд;
- результаты экспериментов (дамп пакетов и вывод утилит telnet и traceroute);
- выводы по работе.

Контрольные вопросы

1. Что такое межсетевой экран и для чего он применяется?
2. Принципы функционирования пакетного фильтра.
4. Какой основной принцип настройки файрвола?
5. Для чего предназначено правило по умолчанию?
6. Какие действия может применять к пакетам файрвол IPFW?
7. При помощи каких команд работает утилита ipfw?
8. Синтаксис построения правила для утилиты ipfw.
9. Каким образом можно проверить возможность TCP-соединения?
10. Каким образом можно проверить работу UDP протокола?

1.6 Использование Internet Protocol Security (IPSec) для защиты конфиденциальных данных, которые передаются по протоколу TCP/IP

Цель и задачи работы

1. Изучить архитектуру стека протоколов IPSec.
2. Настроить политики IPSec в ОС семейства Windows для организации защиты передаваемых данных между двумя компьютерами в сети.
3. Провести эксперименты для проверки работоспособности настроек политик IPSec.

Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:
- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 утилиту Microsoft Network Monitor 3.4, инсталлировать ее на компьютерах лаборатории, ознакомиться с правилами ее использования.

Теоретический материал

Стек протоколов IPSec обеспечивает защищенную передачу данных в IP-сетях с использованием служб шифрования, а также защиту сетевого доступа в окружении Windows. Протоколы IPSec обеспечивают защиту информации на сетевом уровне, что делает их работу прозрачной для приложений. Архитектура IPSec совместима с протоколами IPv4 и IPv6.

Архитектура средств безопасности IPSec представлена на рис. 1.

На верхнем уровне расположены три протокола, составляющих ядро IPSec:

а) протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange), определяющий способ инициализации защищенного канала, включая согласование используемых алгоритмов криптозащиты, а также процедуру обмена и управления секретными ключами в рамках защищенного соединения;

б) протокол аутентифицирующего заголовка AH (Authentication Header), обеспечивающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;

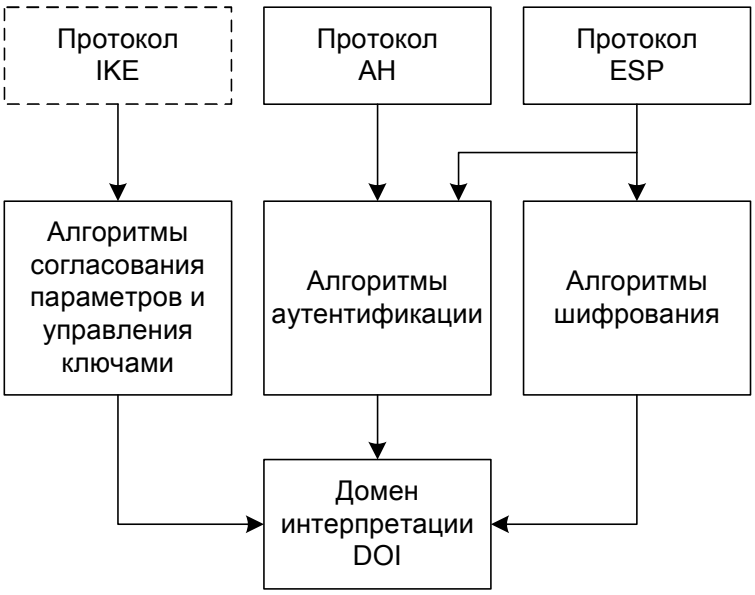

Рис. 1. Архитектура стека протоколов IPSec

в) протокол инкапсулирующей защиты содержимого ESP (Encapsulation Security Payload), обеспечивающий криптографическое закрытие, аутентификацию и целостность передаваемых данных, а также защиту от навязывания повторных сообщений.

Средний уровень образуют алгоритмы согласования параметров и управления ключами, применяемые в протоколе IKE, а также алгоритмы аутентификации и шифрования, используемые в протоколах AH и ESP. Для шифрования данных в IPSec (в протоколе ESP) может быть использован любой симметричный алгоритм шифрования с секретными ключами, такие как DES, 3Des, AES. Для обеспечения целостности и аутентификации данных (в протоколах AH и ESP) применяется шифрование с использованием односторонней хеш-функции, например, MD5 или SHA-1.

Нижний уровень образует домен интерпретации DOI (Domain of Interpretation). DOI в качестве БД хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т.п. Этот модуль обеспечивает совместную работу всех применяемых и вновь подключаемых протоколов и алгоритмов.

Протокол IPSec работает следующим образом:

1) агент политик считывает политики безопасности из SPD в реестре;

2) если политика указывает на использование IPSec, то агент посылает уведомление драйверу;

3) затем агент использует службы Security Association (SA) и IKE для обмена секретным ключом;

4) IKE создает защищенный канал между двумя компьютерами;

5) драйвер IPSec использует открытый ключ для создания SA-идентификаторов каждому из компьютеров для передачи данных;

6) при шифровании (ESP) и/или подписи (AH) пакетов, драйвер IPSec использует SA-key для создания ключа на входящее и исходящее соединение, а также Security Parameters Index (SPI), который будет вставлен в заголовок IPSec пакета;

7) после чего пакет передается на транспортный уровень;

8) на принимающей стороне происходят обратные процедуры.

Важным параметром безопасной ассоциации является так называемый ключевой материал, то есть секретные криптографические ключи, которые используются в работе протоколов AH и ESP. В целях безопасности, эти ключи никогда не пересылаются по сети, а передаются данные, необходимые каждому конечному узлу для локальной генерации ключей.

Параметры SA должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления безопасной ассоциации протоколы IKE, работающие по разные стороны канала, выбирают параметры на основании взаимных согласований. Для каждой задачи, которые решаются протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования.

Безопасная ассоциация является однонаправленным логическим соединением, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA (одну для входящих пакетов, другую – для исходящих). Для идентификации каждой SA предназначен индекс параметров безопасности SPI.

Протоколы AH и ESP могут работать в туннельном или транспортном режимах.

Для выполнения своих задач по обеспечению безопасной передачи данных протоколы AH и ESP включают в пакеты, которые обрабатываются ими, дополнительную служебную информацию, оформляя ее в виде заголовков.

На рис. 2 представлена структура IP-пакета после применения протокола AH в транспортном и туннельном режимах.

В транспортном режиме заголовок исходного IP-пакета становится внешним заголовком, за ним следует заголовок AH, а затем все данные защищаемого пакета (т.е. пакет протокола верхнего уровня). Протокол AH защищает весь полученный таким образом пакет, включая заголовок IP и собственно сам заголовок AH. Таким образом, любое изменение данных в пакете или заголовков будет обнаружено. Следует также заметить, что в этом режиме данные пакета отсылаются открытыми, т.е. данные пакета защищены от изменений, но не защищены от просмотра. В частности, не удается скрыть IP-адреса источника и назначения от возможного просмотра посторонними лицами, поскольку эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.

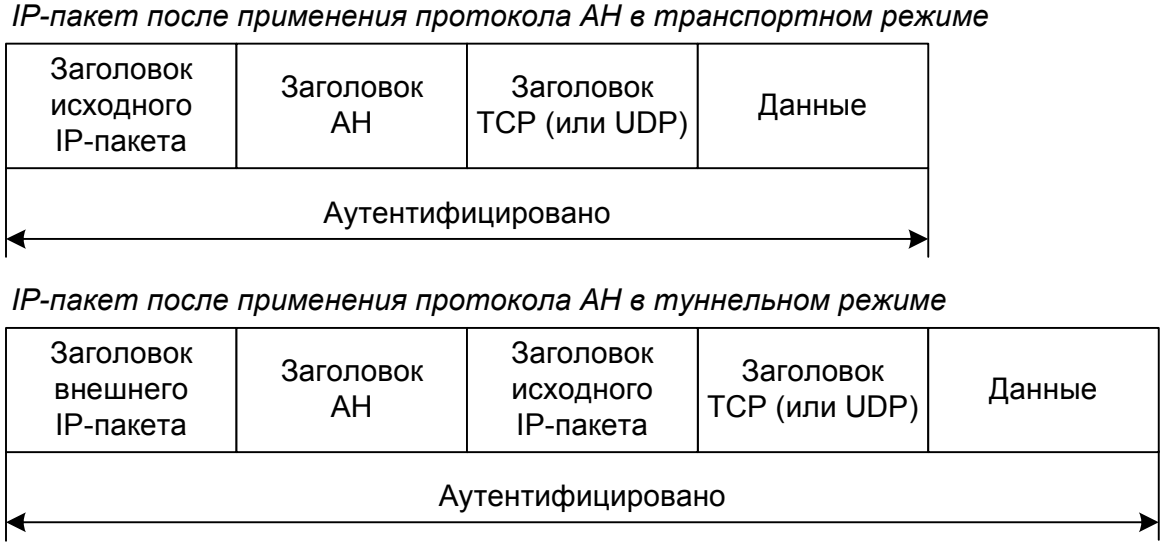

Рис. 2. IP-пакет после применения протокола AH в транспортном и туннельном режимах

В туннельном режиме в качестве заголовка внешнего IP-пакета создается новый заголовок IP. IP-адреса посылающей и принимающей сторон могут отличаться от адресов в заголовке исходного IP-пакета. В защищенном IP-пакете внутренний (первоначальный) IP-заголовок содержит целевой адрес пакета, а внешний IP-заголовок содержит адрес конца туннеля. За новым заголовком внешнего IP-пакета следует заголовок AH, а затем весь исходный пакет (заголовок IP и сами данные). Как и в случае транспортного режима, протокол AH защищает весь созданный пакет (два заголовка IP, заголовок AH и данные), что также позволяет обнаружить любые изменения в пакете. Как и в транспортном режиме, сам пакет не защищен от просмотра.

Не зависимо от режима работы, протокол AH предоставляет меры защиты от атак, направленных на нарушение целостности и подлинно-

сти пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов. Однако следует иметь в виду, что аутентификация по протоколу AH не допускает манипулирования основными полями IP-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов NAT (Network Address Translation), поскольку для его работы необходимо манипулирование IP-заголовками.

Протокол AH может применяться как отдельно, так и в комбинации с протоколом ESP или даже с пакетом, который уже содержит AH-заголовок (вложенное применение).

Протокол инкапсулирующей защиты содержимого ESP обеспечивает конфиденциальность, аутентичность, целостность и защиту от повторов для пакетов данных. Следует отметить, что конфиденциальность данных протокол ESP обеспечивает всегда, а целостность и аутентичность являются для него опциональными требованиями. Конфиденциальность данных обеспечивается путем шифрования содержимого отдельных пакетов. Целостность и аутентичность данных обеспечиваются на основе вычисления дайджеста.

Функциональность протокола ESP шире, чем у протокола AH. Протокол ESP поддерживает все функции протокола AH по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения, а также обеспечивает конфиденциальность данных.

В протоколе ESP функции аутентификации и криптографического закрытия 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.

На рис. 3 представлена структура IP-пакета после применения протокола ESP в транспортном и туннельном режимах.

В транспортном режиме зашифрованные данные транспортируются непосредственно между хостами. В транспортном режиме протокола ESP заголовок исходного IP-пакета остается внешним. Заголовок ESP помещается в передаваемый пакет между заголовками протоколов третьего (IP) и четвертого (например TCP) уровней. Следует заметить, что поля протокола ESP следуют после стандартного IP-заголовка, а это означает, что такой пакет может маршрутизироваться в сети с помощью обычного оборудования, поддерживающего IP.

Шифрованию подвергаются только данные исходного IP-пакета (пакет верхнего уровня) и заключительная часть ESP-заголовка (ESP trailer). В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями.

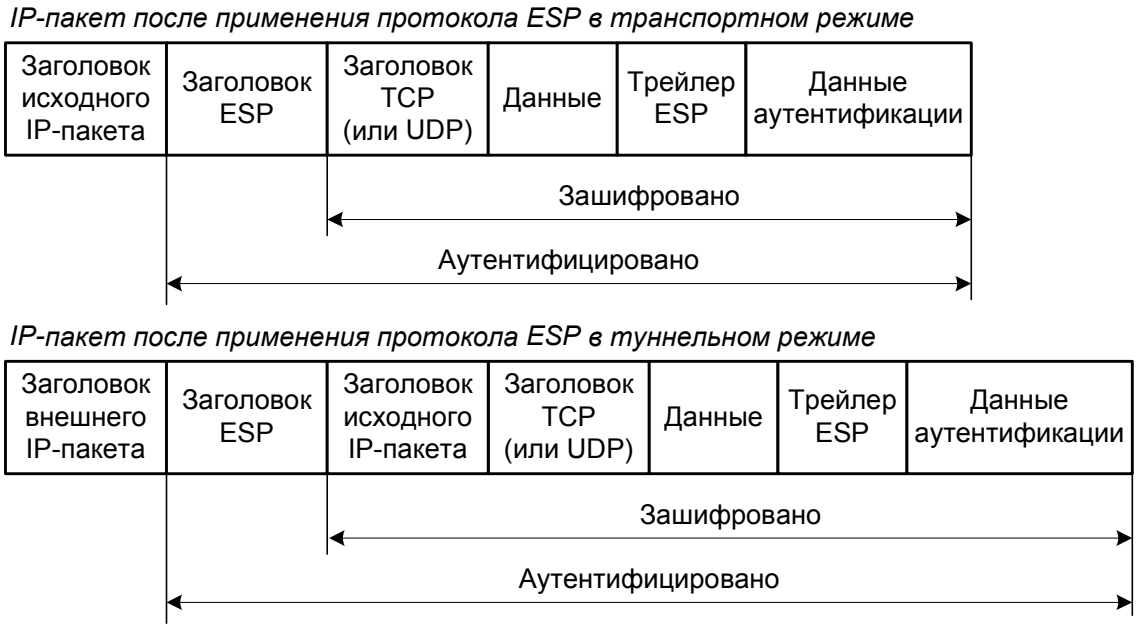

Рис. 3. IP-пакет после применения протокола ESP в транспортном и туннельном режимах

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета, и по этой причине имеет смысл применять оба протокола совместно – ESP для шифрования, а AH – для контроля целостности.

Таким образом, адресная информация (IP-адреса отсылающей и принимающей сторон) видна при пересылке пакета по сети и несанкционированное изменение этих IP-адресов не будет замечено.

В туннельном режиме основная роль отводится шлюзам безопасности, поскольку предполагается, что клиентские станции (или серверы) могут не поддерживать IPSec и отправляют в сеть обычный IP-трафик. Перед тем, как достичь каналов глобальной сети, каждый исходный IP-пакет сначала попадает в шлюз, который помещает этот пакет целиком в оболочку IPSec, зашифровывая его содержимое вместе с исходным IP-заголовком. Чтобы обеспечить возможность маршрутизации получившегося пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет в сеть. Шлюз, находящийся на противоположном конце соединения, расшифровывает этот пакет и передает его на

оконечное устройство в первоначальном виде. Описанная процедура называется туннелированием.

В туннельном режиме в качестве внешнего заголовка создается новый заголовок IP. Весь исходный IP-пакет (и данные и заголовок) и заключительная часть заголовка ESP (ESP trailer) шифруются. Поэтому адресная информация исходного IP-пакета не доступна для просмотра. Заголовок внешнего IP-пакета протоколом ESP не защищается.

Туннелирование позволяет распространить действие средств защиты на сетевой уровень модели OSI и, в частности, скрыть истинные адреса источника и получателя. При этом уменьшается риск атак, основанных на детальном анализе трафика.

Сравнивая протоколы ESP и AH можно заметить, что они дублируют функциональность друг друга в области обеспечения аутентификации данных. Главным отличием протокола AH от ESP в данном вопросе является, то что протокол AH обеспечивает аутентификацию всего пакета, в то время как протокол ESP аутентифицирует только данные из пакета. При шифровании в протоколе ESP используется симметричный секретный ключ, т.е. передаваемые данные зашифровываются и расшифровываются с помощью одного и того же ключа. Протокол ESP также определяет перечень обязательных алгоритмов шифрования – DES, MD5 и SHA-1.

Протокол ESP может применяться как отдельно, так и совместно с протоколом AH.

Этапы выполнения работы

1. Организация соединения компьютеров в локальной сети.
2. Настройка политики IPSec для компьютера с именем Host-A с операционной системой Windows 7.
3. Настройка политики IPSec для компьютера с именем Host-B с операционной системой Windows XP.
4. Проведение экспериментов для проверки работоспособности настроек политик IPSec.
5. Возобновление обычного режима связи между компьютерами.

Для выполнения лабораторной работы необходимо наличие двух компьютеров, физически объединенных в единую сеть с ОС Windows XP или Windows 7. На рис. 4 показана логическая структура такой сети.

На хостах A и B будет настроена политика IPSec для защищенной передачи данных. Если имеется третий хост (не обязательно), то с помощью него можно проверить возможность перехвата данных путем

сканирования сети или прямого взаимодействия с защищаемыми компьютерами. Данные будут передаваться в транспортном режиме работы протоколов.

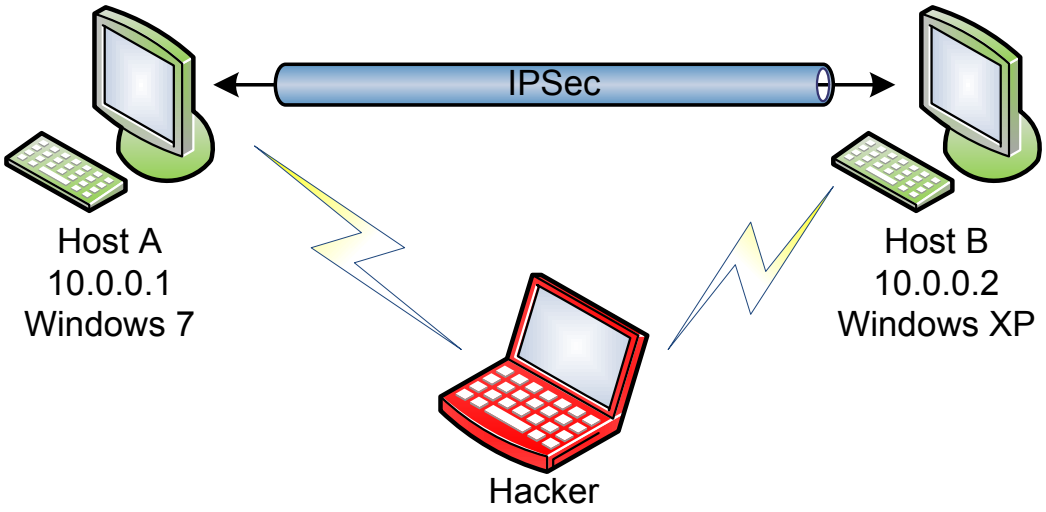

Рис. 4. Логическая структура сети

Этап 1 – Организация соединения компьютеров в локальной сети

Примечание. Если локальная сеть между компьютерами уже настроена, то этап настройки можно пропустить и перейти к шагу 3 данного подраздела для определения установленных IP-адресов и имен компьютеров.

а) Настройка сети на хосте А с ОС Windows 7:

1) войти в систему с правами администратора;
2) Пуск ⇨ Панель управления ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера;
3) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ выбрать Свойства;
4) в окне «Подключение по локальной сети» во вкладке Сеть выбрать «Протокол Интернета версии 4 (TCP/IPv4)» ⇨ Свойства;
5) установить значения, показанные на рис. 5 и нажать ОК;
6) закрыть окно «Подключение по локальной сети»;
7) если состояние иконки «Подключение по локальной сети» – «отключено», включить его двойным кликом мыши.

б) Изменение рабочей группы на хосте А:

1) Пуск ⇨ Компьютер ⇨ Свойства системы;

2) в разделе «Имя компьютера, имя домена и параметры рабочей группы», кликнуть на «Изменить параметры» ⇨ в окне «Свойства системы» во вкладке «Имя компьютера» ⇨ Изменить;

3) в данной работе используется: «Имя компьютера» – Host-A, «Является членом рабочей группы» – WORKGROUP;

4) после закрытия окна свойств, необходимо перезагрузить ОС.

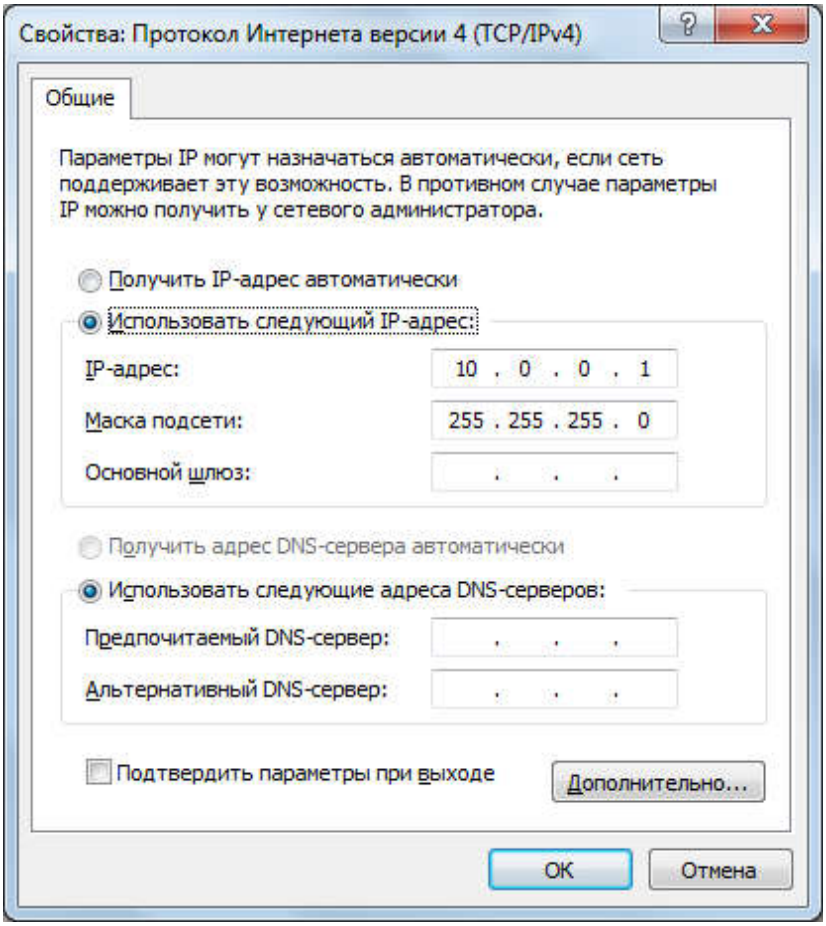

Рис. 5. Настройка TCP/IP на хосте A

в) Настройка сети на хосте B с ОС Windows XP:

1) войти в систему с правами администратора;

2) Пуск ⇨ Настройки ⇨ Панель управления ⇨ Сетевые подключения;

3) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ выбрать Свойства;

4) в окне «Подключение по локальной сети – свойства» во вкладке Общие выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

5) установить значения, показанные на рис. 6 и нажать ОК;

6) закрыть окно «Подключение по локальной сети»;

7) если состояние иконки «Подключение по локальной сети» – «отключено», включить его двойным кликом мыши.

г) Изменение рабочей группы на хосте B:

1) Мой компьютер ⇨ Свойства ⇨ Перейти во вкладку «Имя компьютера» ⇨ Изменить;

2) в данной работе используется: «Имя компьютера» – Host-B, «Является членом рабочей группы» – WORKGROUP;

3) после закрытия окна свойств, необходимо перезагрузить ОС.

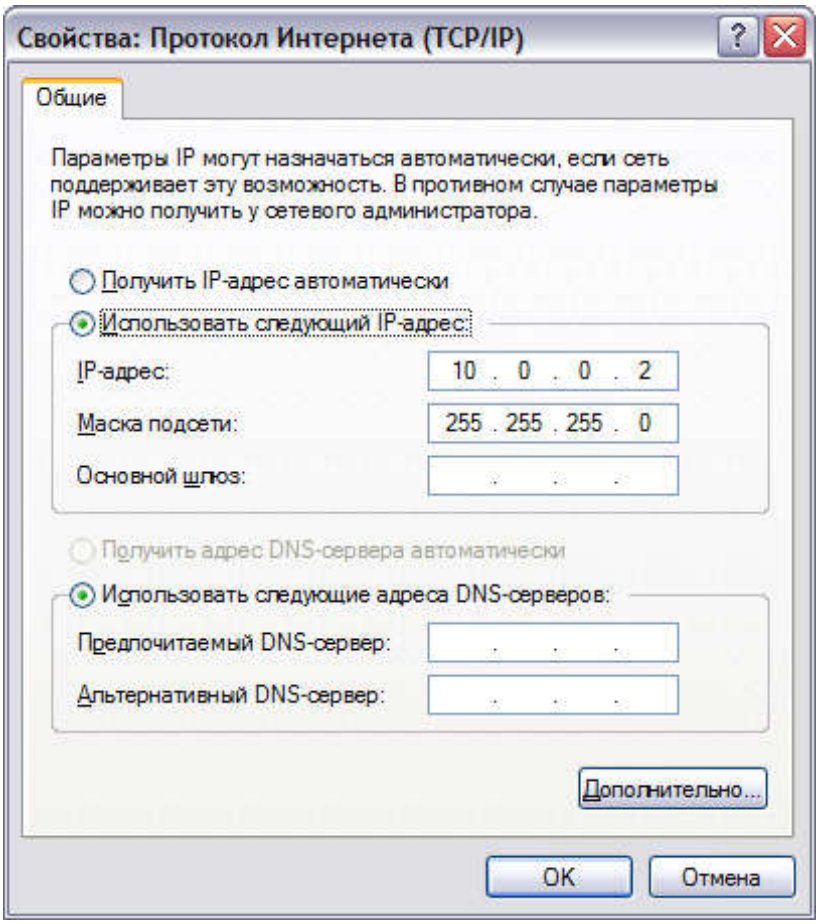

Рис. 6. Настройка TCP/IP на хосте B

д) Проверка локального соединения. Для определения установленных имен компьютеров и IP-адресов, на каждой машине необходимо выполнить следующее:

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);

2) ввести cmd.exe и нажать на клавишу Enter;

3) выполнить команду ipcongfig /all – среди отображенной информации есть установленное ранее «Имя компьютера» и «IP-адрес адаптера подключения по локальной сети»;

4) в окне утилиты cmd.exe на компьютере А выполнить команду: ping 10.0.0.2.

Полученные ответы от хоста 10.0.0.2 свидетельствуют об успешном прохождении ICMP-пакетов и правильно выполненной настройке.

Этап 2 – Настройка политики IPSec для компьютера Host-A с Windows 7

а) Создание файла консоли:

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);

2) ввести mmc.exe и нажать на клавишу Enter;

3) пункт меню Файл ⇨ Добавить или удалить оснастку;

4) в списке доступных оснасток выделить «Управление политикой IP-безопасности» ⇨ Добавить ⇨ оставить флажок «Локальный компьютер» ⇨ Готово;

5) среди оснасток Добавить «Монитор IP-безопасности»;

6) аналогично добавить «Службы» и «Просмотр событий» для локального компьютера;

7) закрыть окно «Добавление и удаления оснасток» кнопкой OK;

8) Файл ⇨ Сохранить как... ⇨ выбрать путь к рабочей папке и сохранить файл консоли управления ipsec.msc ⇨ OK.

В результате получается четыре оснастки, что показано на рис. 7.

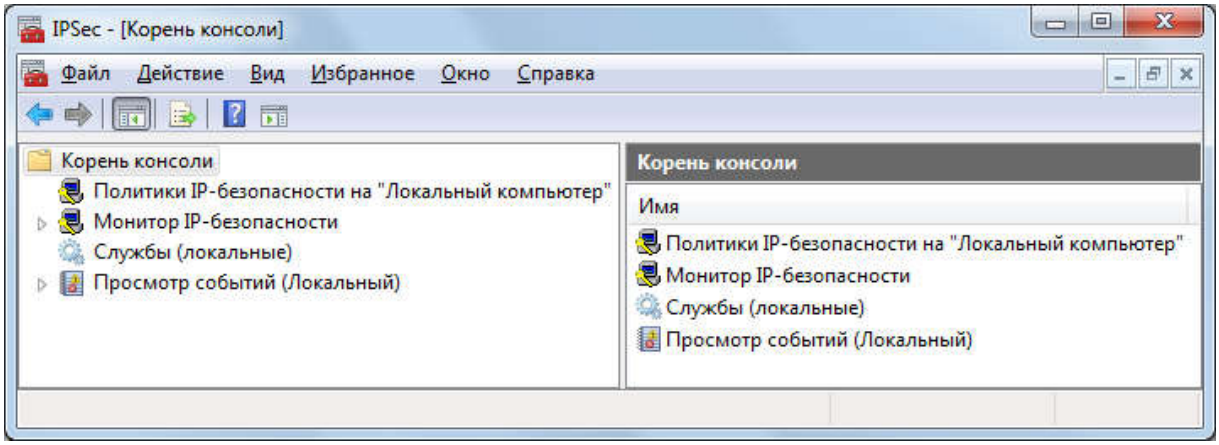

Рис. 7. Консоль mmc с файлом ipsec.msc

б) Запуск службы:

1) в корне консоли выбрать Службы;

2) в области описания окна найти службу «Агент политики IPSec» ⇨ запустить службу двойным кликом.

в) Создание политики безопасности и настройка IP-фильтров:

1) в корне консоли кликнуть правой кнопкой мыши на «Политики IP-безопасности»;

2) выбрать «Создать политику безопасности»;

3) в открывшемся мастере нажать Далее ⇨ ввести имя «Политика IPSec» ⇨ Далее ⇨ оставить снятым флажок «Использовать правило по умолчанию» ⇨ Далее ⇨ оставить установленным флажок «Изменить свойства» ⇨ Готово;

4) в открывшемся окне Свойства ⇨ зайти во вкладку Общие ⇨ открыть Параметры ⇨ Методы;

5) в открывшемся окне «Методы безопасности при обмене ключами» (IKE) установить параметры, показанные на рис. 8 ⇨ нажать ОК и вернуться в окно Свойств во вкладку Правила.

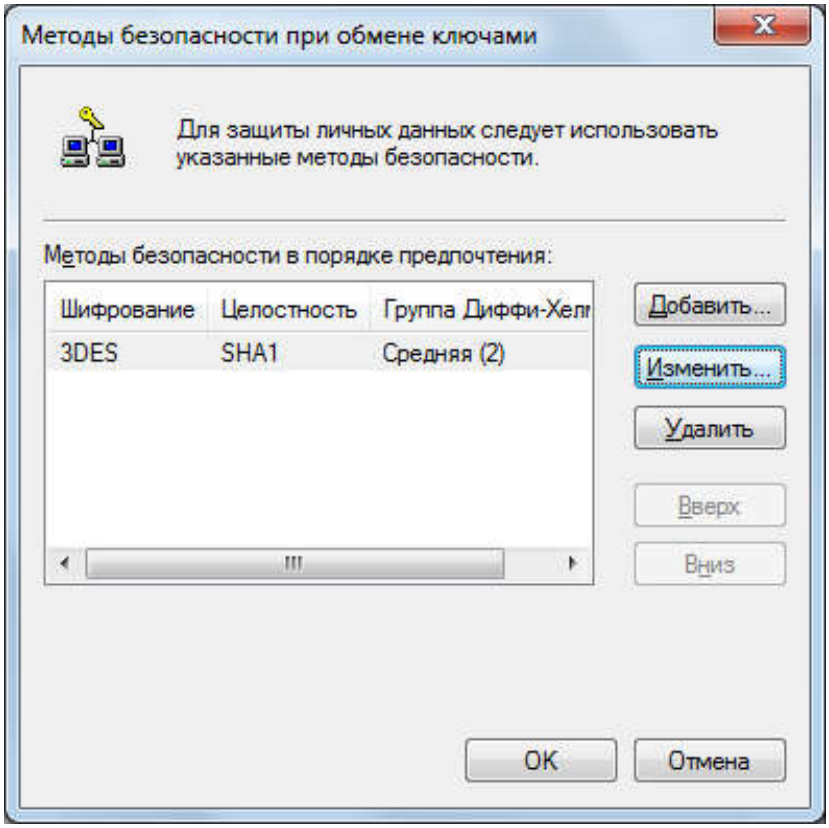

Рис. 8. Методы безопасности при обмене ключами в Windows 7

6) Добавить ⇨ в «Мастере создания новых правил» нажать Далее;

7) установить флажок «Это правило не определяет туннель» ⇨ Далее (таким образом, устанавливается транспортный режим работы стека протоколов IPSec);

8) тип сети «Все сетевые подключения» ⇨ Далее ⇨ Добавить;

9) в открывшемся окне «Список IP-фильтров» ввести имя «Защищенный IP-трафик с хостом B» ⇨ Добавить;

10) во вкладке Адреса выбрать опции показанные на рис. 9;

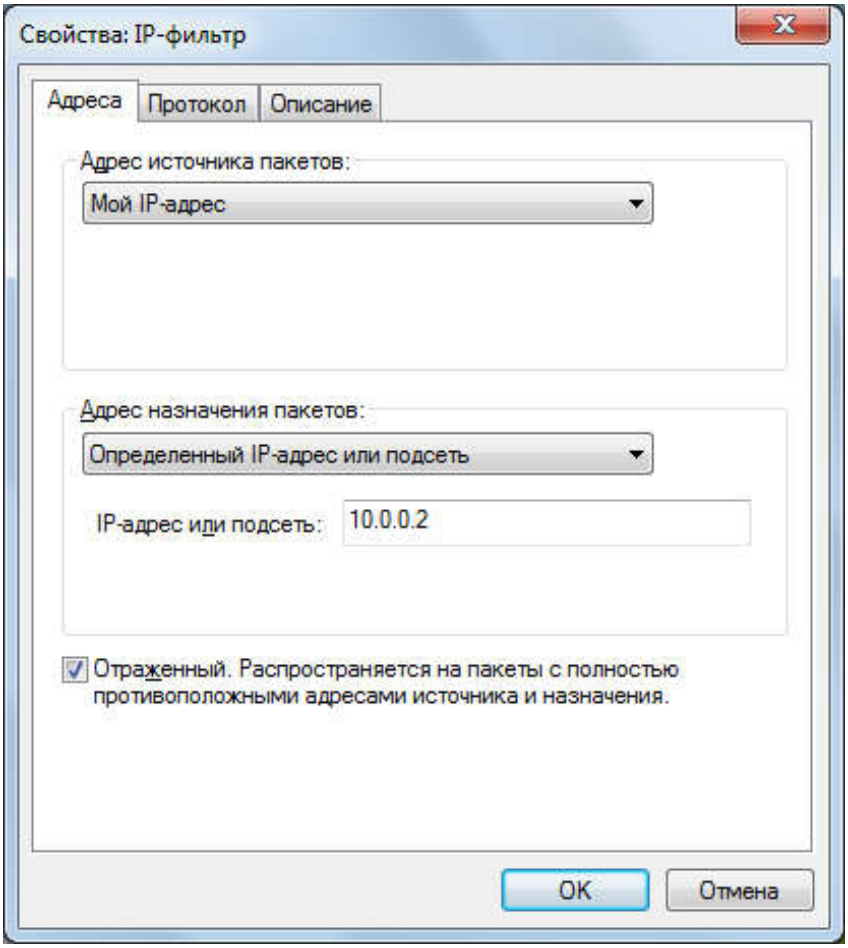

Рис. 9. Свойства IP-фильтра компьютера с именем Host-A

11) во вкладке Протокол указать «Тип протокола: Любой» ⇨ ОК;

12) в списке IP-фильтров выбрать созданный «Защищенный IP-трафик с хостом B» ⇨ Далее;

13) в окне «Действие фильтра» оставить флажок «Использовать мастер» ⇨ Добавить ⇨ Далее ⇨ Имя: Шифровать ⇨ Далее ⇨ Согласовать безопасность ⇨ Далее ⇨ Запретить небезопасное соединение ⇨ Далее ⇨ Другой ⇨ Параметры;

14) установить настройки соответствующие рис. 10 ⇨ ОК ⇨ ДА ⇨ Далее ⇨ Готово;

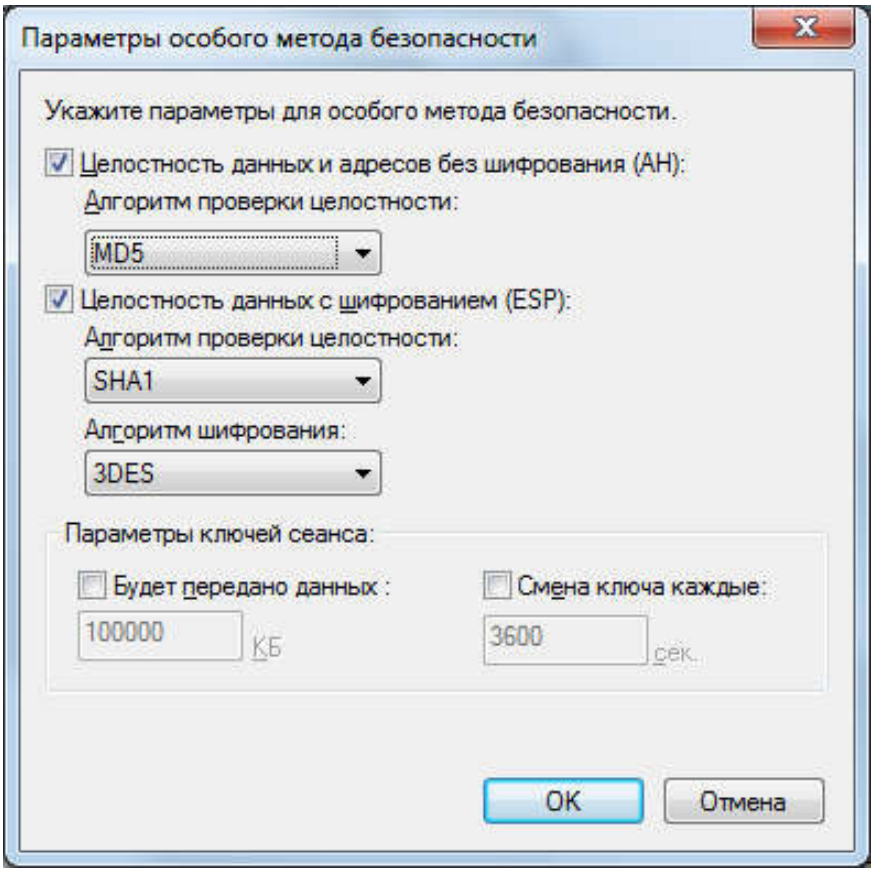

Рис. 10. Параметры метода безопасности

15) Действие фильтра: Шифровать ⇨ Далее;

16) в окне «Метод проверки подлинности» выбрать «Использовать данную строку для защиты обмена ключами» и набрать: Pre-Shared Key ⇨ Далее ⇨ Готово ⇨ закрыть окно ОК;

17) нажать правой кнопкой на «Политика IPSec» ⇨ Назначить.

г) Добавление нового фильтра:

1) открыть свойства Политики IPSec через контекстное меню;

2) выполнить аналогичные действия описанные выше по добавлению нового фильтра со следующими параметрами:

- Тип сети: Все сетевые подключения;
- Имя фильтра: Полный IP-трафик;
- Адрес источника пакетов: Мой IP-адрес;
- Адрес назначения пакетов: Любой IP-адрес;
- Отраженный; Протокол: Любой;
- Действие фильтра: Блокировать.

Таким образом создается фильтр закрывающий весь трафик для компьютера А, кроме защищенного взаимодействия с компьютером В.

Этап 3 – Настройка политики IPSec для компьютера Host-B с Windows XP

Примечание. Для защиты передаваемых данных, оба компьютера должны иметь согласованные методы безопасности при обмене ключами и шифровании данных.

а) Создание файла консоли:

1) Пуск ⇨ Выполнить (либо сочетанием клавиш Win+R);
2) ввести mmc.exe и нажать на клавишу Enter;
3) меню Консоль ⇨ Добавить или удалить оснастку ⇨ Добавить;
4) в списке доступных оснасток выделить «Управление политикой IP-безопасности» ⇨ Добавить ⇨ оставить флажок «Локальный компьютер» ⇨ Готово ⇨ Закрыть ⇨ OK;
5) Консоль ⇨ Сохранить как... ⇨ выбрать путь к рабочей папке и сохранить файл консоли управления ipsec.msc нажав OK;

б) Запуск службы IPSec:

Пуск ⇨ Выполнить ⇨ cmd.exe ⇨ Enter ⇨выполнить команду: net start PolicyAgent;

в) Создание политики безопасности и настройка IP-фильтров:

1) кликнуть правой кнопкой мыши на «Политики IP-безопасности»;
2) Создать политику безопасности;
3) в открывшемся мастере нажать Далее ⇨ ввести имя «Политика IPSec» ⇨ Далее ⇨ снять флажок «Использовать правило по умолчанию» ⇨ Далее ⇨ оставить установленным флажок «Изменить свойства» ⇨ Готово.
4) в открывшемся окне Свойства ⇨ зайти во вкладку Общие ⇨ Дополнительно ⇨ Методы;
5) в окне «Методы безопасности при обмене ключами» (IKE), установить параметры, аналогичные рис. 8;

Примечание. В ОС Windows XP по умолчанию задано четыре метода безопасности при обмене ключами, что изображено на рис. 11.

6) нажать OK и вернуться в окно Свойств во вкладку Правила;
7) Добавить ⇨ в «Мастере создания новых правил» нажать Далее;
8) установить флажок «Это правило не определяет туннель» ⇨ Далее.
9) выбрать тип сети «Все сетевые подключения» ⇨ Далее;
10) использовать данную строку для защиты обмена ключами, набрать: Pre-Shared Key ⇨ Далее;

11) нажать на кнопку Добавить, в открывшемся окне «Список IP-фильтров», ввести имя «Защищенный IP-трафик с хостом B» ⇨ Добавить;

12) во вкладке Адреса выбрать значения, как на рис. 12;

13) во вкладке Протокол выбрать тип протокола: Любой ⇨ ОК;

14) в списке IP-фильтров выбрать созданный «Защищенный IP-трафик с хостом B» ⇨ Далее;

15) в окне «Действие фильтра» оставить флажок «Использовать мастер» ⇨ Добавить ⇨ Далее ⇨ Имя: Шифровать ⇨ Далее ⇨ Согласовать безопасность ⇨ Далее ⇨ Не соединяться с компьютерами, не поддерживающими IPSEC ⇨ Далее ⇨ Другой ⇨ Параметры;

16) установить настройки соответствующие рисунку 2.9 ⇨ ОК ⇨ ДА ⇨ Далее ⇨ Готово;

17) выбрать действие фильтра: Шифровать ⇨ Далее ⇨ Готово ⇨ Применить ⇨ ОК;

18) нажать правой кнопкой на «Политика IPSec» ⇨ Назначить.

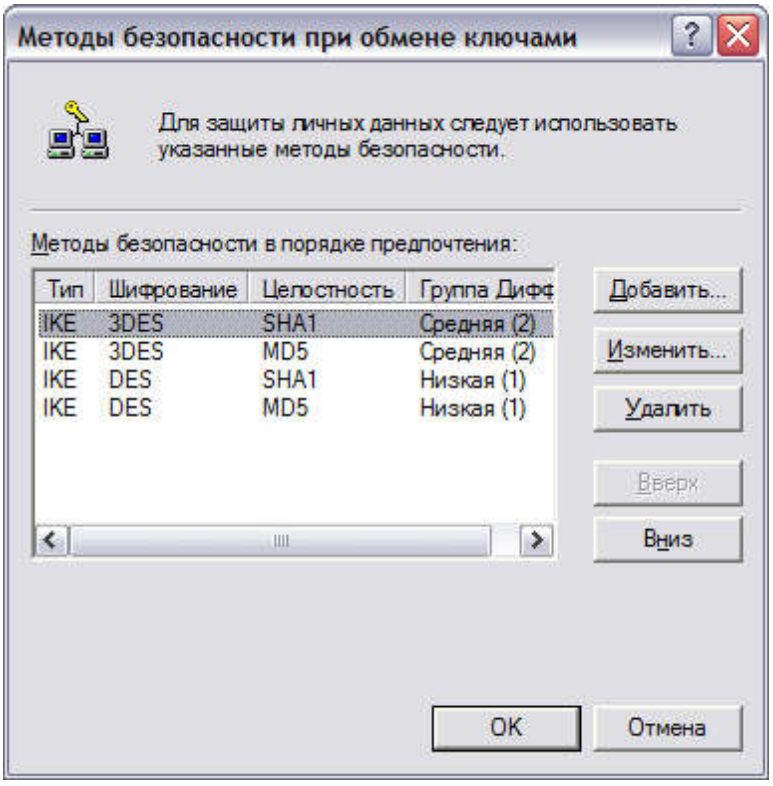

Рис. 11. Методы безопасности при обмене ключами в Windows XP

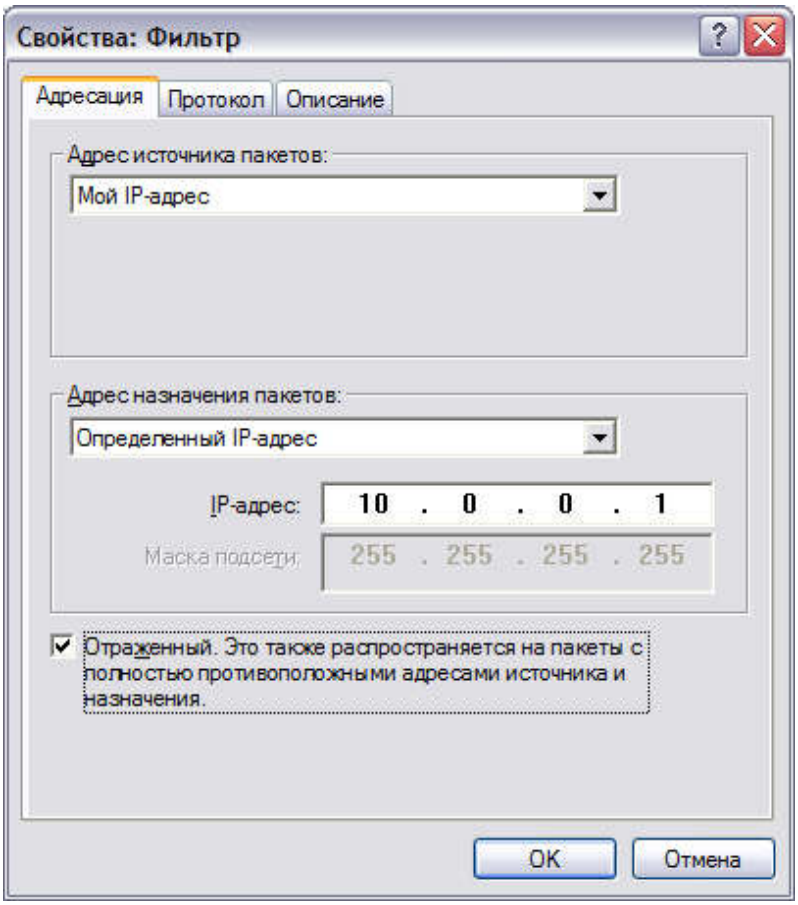

Рис. 12. Свойства IP-фильтра компьютера с именем Host-B

Этап 4. Проведение экспериментов для проверки работоспособности настроек политик IPSec

Эксперимент 1 – Просмотр журнала безопасности:

Открыть общий доступ к рабочей папке на хосте A (действие выполняется через контекстное меню);

Выполнить вход с хоста B на хост A по адресу \\10.0.0.1, который вводится в проводнике – данное событие фиксируется в журнале безопасности Windows;

На компьютере с именем Host-A:

1) развернуть ветвь «Просмотр событий (локальный)» в консоли;
2) Журналы Windows ⇨ Безопасность;
3) просмотреть общие сведения последних по времени событий, зафиксировать результат.

Эксперимент 2 – Проверка достижимости узла с включенными политиками:

На компьютере Host-B:

1) запустить утилиту cmd.exe;

2) выполнить команду: ping 10.0.0.1;

3) убедиться в успешном прохождении ICMP-пакетов, получив ответы от хоста 10.0.0.1.

Провести аналогичный тест с любым хостом в глобальной сети Интернет, например с google.com, получить ответ;

Повторить аналогичные действия на компьютере Host-A.

Зафиксировать результаты. При попытке осуществить выход в Интернет Host-B имеет такие возможности, а Host-A – нет (с чем это связано?).

Эксперимент 3 – Проверка достижимости узла с отключенной политикой:

Отключить политику IPSec на компьютере A (правая клавиша мыши ⇨ Снять);

На компьютере B выполнить команду: ping 10.0.0.1;

На компьютере A выполнить команду: ping 10.0.0.2;

Ззаново запустить политику IPSec на компьютере A.

Зафиксировать и объяснить полученные результаты.

Эксперимент 4 – Просмотр событий в «Мониторе IP-безопасности»:

На компьютере с именем Host-A развернуть ветвь «Просмотр событий (локальный)» в корне консоли;

Развернуть ветвь HOST-A;

В подпапках находятся статистические данные по IP-безопасности.

Зафиксировать и объяснить полученные результаты.

Примечание. Оснастка «Монитор IP-безопасности» может быть использована для просмотра и наблюдения за статистическими данными и политикой IPSec. Эта информация может быть полезна при устранения неполадок в IPSec и тестировании создаваемых политик. Эти статистические данные могут использоваться при обнаружении возможных атак на данный компьютер или другие компьютеры, добавленные к оснастке. При просмотре сопоставлений безопасности данного компьютера можно определить, какие компьютеры с ним соединены, какой тип целостности данных и шифрации используется в этих соединениях, а также получить другую информацию.

Эксперимент 5 – Сканированием сети анализатором трафика:

Примечание. Для данного эксперимента на одном из компьютеров устанавливается утилита Microsoft Network Monitor 3.4, которую можно бесплатно скачать с официального сайта:

http://www.microsoft.com/en-us/download/details.aspx?id=4865 (для 32- и 64-разрядных систем).

Сканирование трафика при выполнении команды ping с отключенной политикой безопасности:

1) отключить политику IPSec на обоих компьютерах;
2) запустить программу Microsoft Network Monitor 3.4;
3) создать новый захват: File ⇨ New ⇨ Capture или Ctrl+N;
4) нажать на кнопку Capture Settings на панели инструментов;
5) в открывшемся окне параметров захвата установить флажок напротив имени «Подключение по локальной сети» для текущего сетевого адаптера (IPv4 = 10.0.0.1 или 10.0.0.2), остальные снять ⇨ Close;
6) запустить сканирование кнопкой Start на панели инструментов;
7) провести ping со второго хоста;
8) по завершении ping нажать на Pause (F6);
9) раскрыть ветвь All Traffic и кликнут мышью на ветке My Traffic в окне Network Conversations;
10) в окне Display Filter ввести ICMP и нажать Apply.

Изучить содержимое окон Frame Summary и Frame Details, объяснить и сохранить полученные результаты.

Перехват данных, передаваемых в открытом виде:

1) сбросить фильтр нажав Remove Filter и запустить сканирование отжав кнопку Pause (F6);
2) передать с одного хоста на другой предварительно созданный txt-файл, содержимое которого составляют пару сотен «1» (единиц), по завершении передачи нажать на паузу;
3) создать и применить новый TCP-фильтр;
4) поочередно выбирая фреймы в окне Frame Summary и просматривая содержимое окна Hex Details, обнаружить переданные «1».

Сканирование трафика при выполнение команды ping с включенной политикой безопасности:

1) сбросить фильтр ⇨ остановить сканирование Stop! ⇨ Start!;
2) включить политики безопасности на обоих компьютерах;
3) выполните ping с одного хоста на другой;
4) создать и применить ICMP-фильтр, объяснить результат;
5) создать и применить ESP-фильтр, объяснить результат.

Просмотр сообщений IKE-согласований:

1) создать и примените IKE-фильтр;

2) изучить содержимое окон Frame Summary и Frame Details, объяснить и сохранить полученные результаты;

3) повторить эксперимент с передачей файла, содержащего «1», объяснить полученный результат.

Этап 5. Возобновление обычного режима связи между компьютерами

1. На обоих компьютерах в консоли mmc, вызвав контекстное меню, снять ранее назначенные политики IPSec.

2. Закрыть окна программ mmc.exe, cmd.exe, MS Network Monitor.

3. Возобновить первоначальные значения настроек сетевого интерфейса.

4. Выйти из системы, завершив сеанс работы от имени администратора.

Требования к содержанию отчета

Отчет должен включать:

- номер, тема и цель работы;
- краткие теоретические сведения по работе;
- ход выполнения работы со скриншотами основных окон настроек;
- распечатки результатов экспериментов с комментариями к ним;
- выводы по работе.

Контрольные вопросы

1. Какие три протокола представляют ядро IPSec и какое назначение каждого из них?

2. Какова последовательность работы протокола IPSec?

3. Какая структура IP-пакета после применения протокола AH в транспортном и туннельном режимах?

4. Какая структура IP-пакета после применения протокола ESP в транспортном и туннельном режимах?

5. Чем отличаются транспортный и туннельный режимы работы IPSec?

6. Какие методы проверки подлинности (IKE) обеспечиваются ОС Windows? Опишите их отличительные особенности.

7. Назовите алгоритмы проверки целостности и шифрования используемые в ОС Windows для обеспечения безопасности при обмене ключами и передачи данных.

8. Из каких полей состоят заголовки AH и ESP?

9. Структура IKE-сообщения.