ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 9
по учебной дисциплине
«Защита информации»
на тему:

«**Работа с МЭ Agnitum Outpost FireWall**»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » _____ 202_ г. протокол № ___

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Тема практического занятия: «*Работа с МЭ Agnitum Outpost FireWall*».

Учебная цель:

1. Приобрести практические навыки в использовании МЭ Agnitum Outpost Firewall

2. Закрепить знания о механизмах защиты от несанкционированного доступа к информации.

Время - 180 мин.

Место – аудитория (класс) по расписанию занятий.

Учебно-материальное и методическое обеспечение

1. Лабораторные установки – персональные ЭВМ с установленным на них программным обеспечением.
2. Электронный практикум по ЗИ.
3. Варианты типовых заданий на практическое занятие.

II. УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п\п	Учебные вопросы	Время, мин.
1.	***Вступительная часть. Контрольный опрос.***	10
2.	***Учебные вопросы.*** ОСНОВНАЯ ЧАСТЬ: 1.Освоить работу по настройке политики безопасности на ПЭВМ путём разрешения, запрещения доступа другим пользователям с помощью МЭ.	160
3.	Заключительная часть. Задание и методические указания курсантам на самостоятельную подготовку	5

III. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПРЕПОДАВАТЕЛЮ ПРИ ПРОВЕДЕНИИ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

Во вступительной части занятия производится контроль присутствия и готовности обучающихся к занятию. Объявляется тема, цель, учебные вопросы занятия и особенности его проведения.

Готовность группы к занятию проверяется контрольным опросом.

Вопрос 1: Что такое МЭ?

Вопрос 2: Какими механизмами защиты обладают МЭ?

Вопрос 3: Перечислите основные функции МЭ?

При отработке первого вопроса занятия основное внимание обратить на усвоение обучающимися на контроль и фильтрацию проходящих через него МЭ сетевых пакетов в соответствии с заданными правилами.

В заключительной части занятия подвести итоги, оценить действия обучающихся, ответить на вопросы.

Дать задание на самоподготовку. Объявить тему следующего занятия.

Практическое занятие № 7
«Работа с МЭ Agnitum Outpost FireWall»

Цели работы:

1. Приобрести практические навыки в использовании МЭ Agnitum Outpost Firewall
2. Закрепить знания о механизмах защиты от несанкционированного доступа к информации

1. Задание на практическое занятие

Освоить работу по настройке политики безопасности на ПЭВМ путём разрешения, запрещения доступа другим пользователям с помощью МЭ.

Ознакомиться с интерфейсом Agnitum Outpost Firewall. Произвести настройку МЭ во всех режимах политики безопасности. Осуществить формирование правил пользователем для любого пользовательского приложения установленного на ПЭВМ (Например, Internet Explorer). практически осуществить и описать в отчёте, что при этом наблюдалось при настройке запрещения на вход и выход с ПЭВМ. На всех этапах осуществить попытки допуска на защищаемую ПЭВМ, используя различные приложения. Отразить и отчете результаты этих попыток и сделать выводы об эффективности применения МЭ.

2. Подготовка к работе

Подготовка к работе проводится в часы самоподготовки. В ходе её каждый курсант обязан:

2.1. Изучить полученное задание.
2.2. Изучить методические указания настоящего руководства.
2.3. Повторить материал занятий, на которых рассматривались назначение и использование межсетевых экранов.

3. Выполнение работы

3.1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя выполняют задания, изучив п.4 данного руководства.

3.2. При выполнении задания работу следует спланировать таким образом, чтобы в первую очередь изучить назначение, основные возможности, порядок настройки и режимы работы МЭ Agnitum Outpost Firewall, а затем приступить к его использованию для обеспечения защиты от НСД к информации на данной ПЭВМ, согласно требованиям задания.

3.3. В ходе практической работы необходимо проверить защищенность ПЭВМ, на которой выполнялось задание до подключения МЭ и после завершения его настройки. Сделать выводы по эффективности применения данного средства ЗИ.

3.4. Ход выполнения работы, ее результаты и сделанные выводы отразить в письменном отчете.

4. Методические указания

Используемое оборудование и программное обеспечение

- аппаратная платформа x86;
- программный продукт виртуализации Oracle VirtualBox;

– операционная система Windows 2003, Windows XP;

– межсетевой экран Agnitum Outpost Firewall.

Время выполнения: 4 ч.

5. Теоретические сведения

Межсетевой экран (МСЭ) или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей МСЭ является защита компьютерных сетей или отдельных хостов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Межсетевой экран - это средство, которое разграничивает доступ между двумя сетями с различными требованиями по обеспечению безопасности. В самом распространенном случае межсетевой экран устанавливается между корпоративной сетью и Internet. Он ограничивает информацию, поступающую на компьютер с других компьютеров, позволяя лучше контролировать данные на компьютере и обеспечивая линию обороны компьютера от людей или программ (включая вирусы и черви), которые несанкционированно пытаются подключиться к компьютеру.

Можно считать брандмауэр пограничным постом, на котором проверяется информация (часто называемая трафик), приходящая из Интернета или локальной сети. В ходе этой проверки брандмауэр отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами (рис.1).

Рисунок 1 - Общая схема работы брандмауэра

Межсетевой экран призван решить две задачи, каждая из которых по-своему важна:

– ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам.

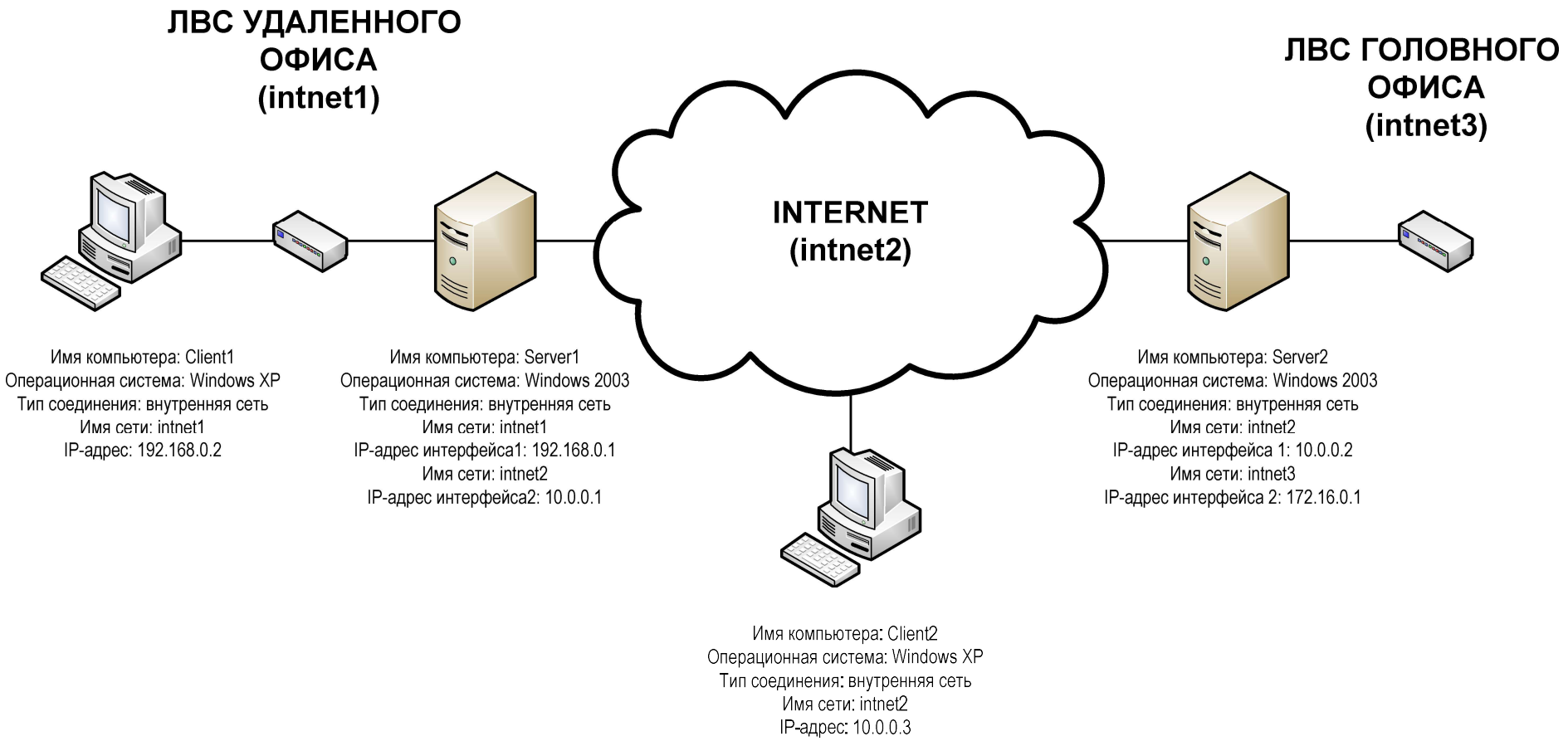
– разграничение доступа пользователей защищаемой сети к внешним ресурсам.

Все межсетевые экраны используют в своей работе один из двух взаимоисключающих принципов:

1. «Разрешено все, что не запрещено в явном виде». Данный принцип облегчает администрирование межсетевого экрана, так как от администратора не требуется никакой предварительной настройки. Любой сетевой пакет, пришедший на МСЭ, пропускается через него, если это не запрещено правилами. С другой стороны, в случае неправильной настройки данное правило делает межсетевой экран дырявым решетом, который не защищает от большинства несанкционированных действий.

2. «Запрещено все, что не разрешено в явном виде». Этот принцип делает межсетевой экран практически неприступной стеной. Однако, повышая защищенность, мы тем самым нагружаем администратора безопасности дополнительными задачами по предварительной настройке базы правил межсетевого экрана. После включения такого МСЭ в сеть, она становится недоступной для любого вида трафика. Администратор должен на каждый тип разрешенного взаимодействия задавать одно и более правил.

СХЕМА СЕТИ ДЛЯ ВЫПОЛНЕНИЯ ЗАДАНИЯ



3. ЗАДАНИЯ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИХ ВЫПОЛНЕНИЮ

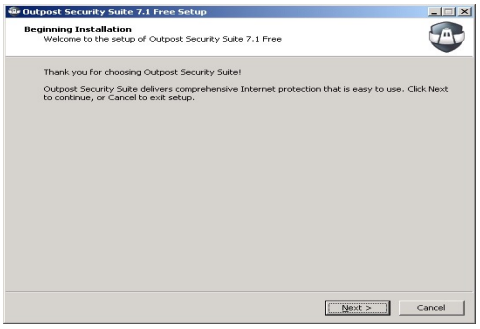
3.1. Установка межсетевого экрана Agnitum Outpost

Установите межсетевой экран Agnitum Outpost на виртуальной машине Server2.

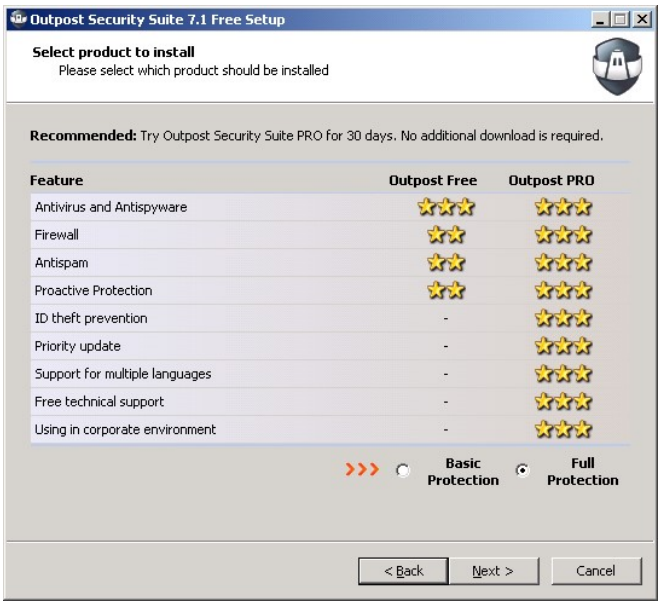
Для этого скопируйте дистрибутив программы на локальный жесткий диск и запустите на исполнение файл OutpostSecuritySuiteInstall.exe.

В качестве языка инсталлятора доступны английский и немецкий языки. Выберите один из них и нажмите OK[1].

В окне приветствия нажмите Next.

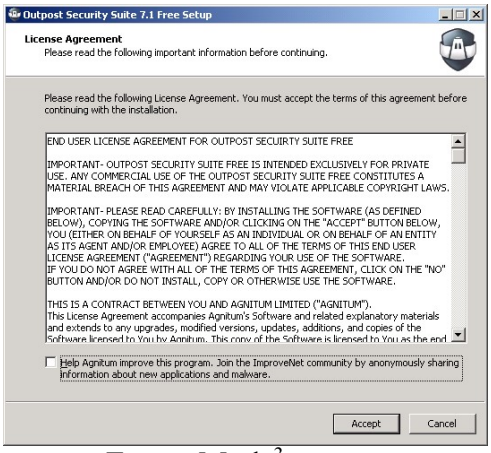


Установка бесплатной версии программы возможна только на домашние версии операционной системы Windows. Для установки на серверную версию выберите опцию установки пробной 30 дневной версии программы (Outpost PRO) и нажмите OK.

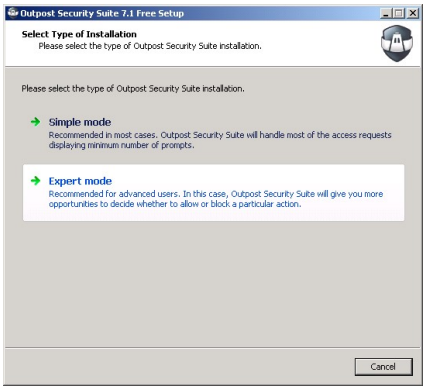


[1] Дальнейшее описание процесса установки приводится применительно к английскому языку интерфейса.

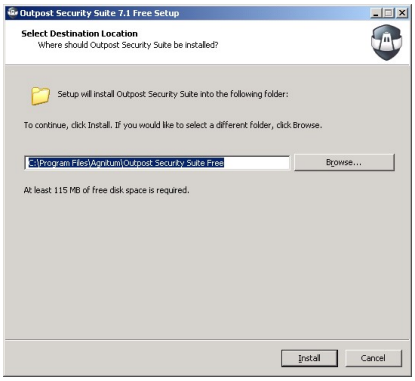
Снимите флажок Help Agnitum…[2] и нажмите Accept.



Выберите режим установки Expert Mode[3].



Оставьте путь установки программы по умолчанию и нажмите Install.

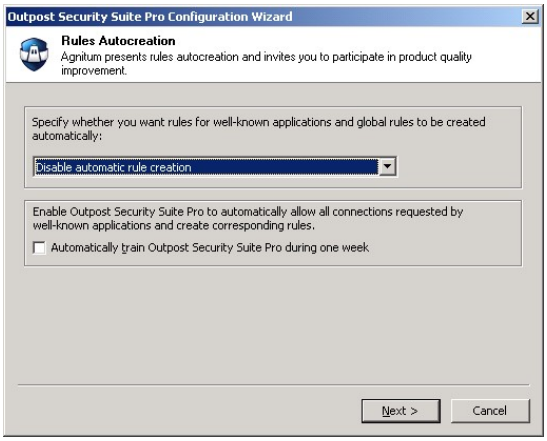


По окончании процесса установки отключите автоматическое создание правил работы МСЭ[4] для чего в выпадающем списке выберите Disable automatic rule creation. Нажмите кнопку Next.

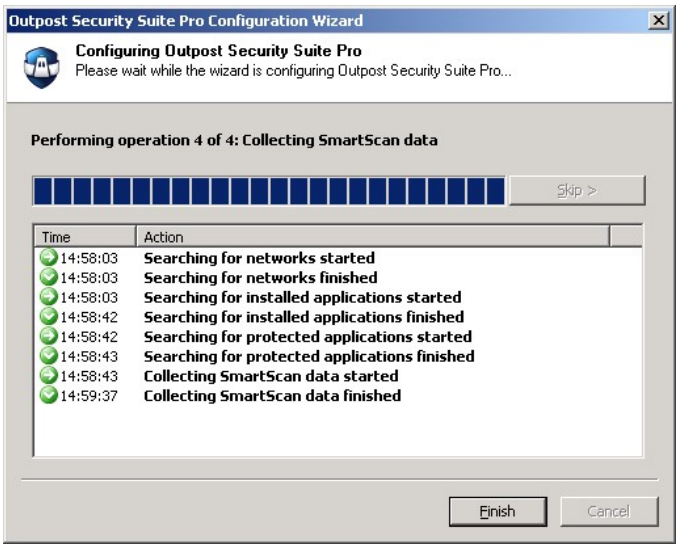
[2] Данная опция предназначена для обеспечения обратной связи между производителем межсетевого экрана Agnitum Outpost и пользователями. Ввиду отсутствия доступа к Интернет, реализация данной функции при выполнении практического занятия невозможна.

[3] Режим выбран в целях углубленного изучения настроек межсетевого экрана. В повседневной деятельности можно использовать простой режим установки.

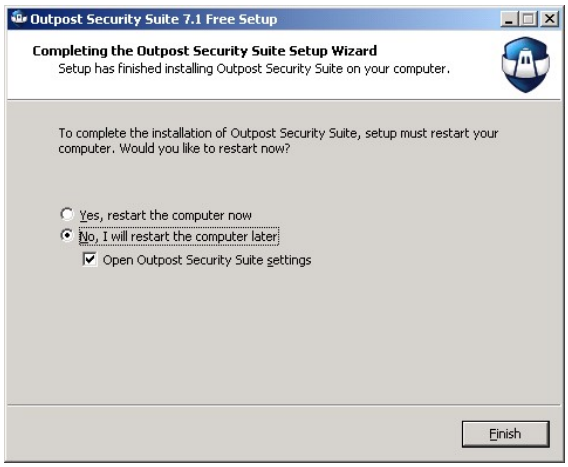
[4] Режим выбран в целях углубленного изучения настроек межсетевого экрана. В повседневной деятельности можно использовать простой режим автоматической установки правил



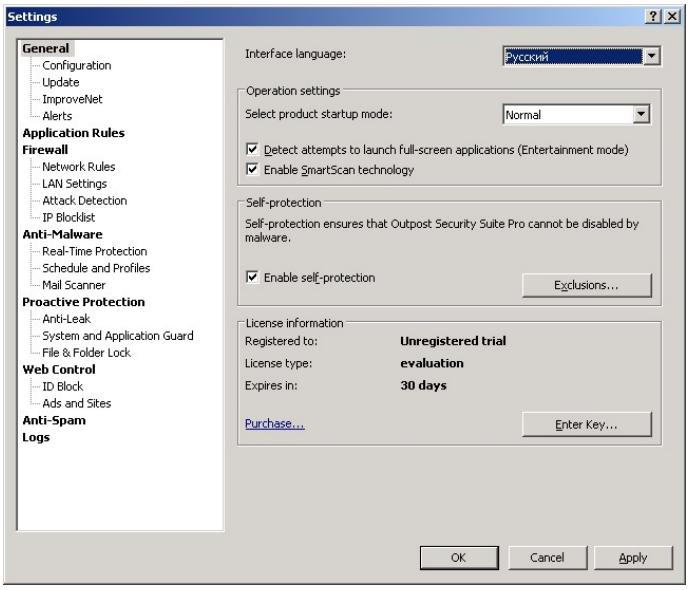
По окончании процесса конфигурирования межсетевого экрана нажмите кнопку Finish.



Откажитесь от немедленной перезагрузки компьютера (перед перезагрузкой необходимо осуществить ряд настроек), выбрав опцию No, I will restart the computer later. Убедитесь, что флажок Open Outpost Security Suite settings установлен и нажмите кнопку Finish.

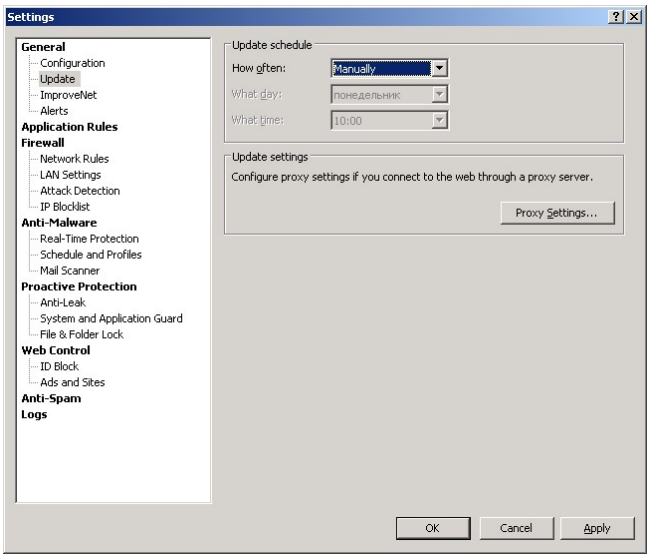


В появившемся окне на вкладке General установите русский язык интерфейса программы. Нажмите кнопку Apply.



В появившемся диалоговом окне нажмите кнопку ОК.

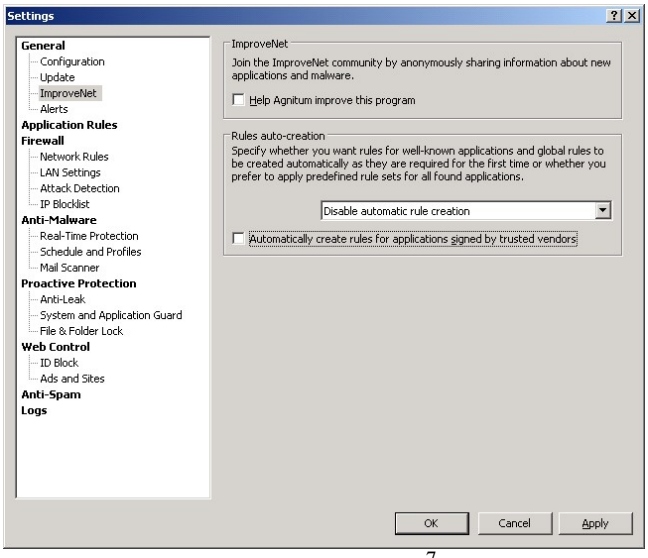
Перейдите на вкладку Обновление и в выпадающем списке выберите ручной (Manually) режим обновления[5].



На вкладке ImproveNet снимите флажок Automatically create rules…[6] Нажмите кнопки Apply и ОК.

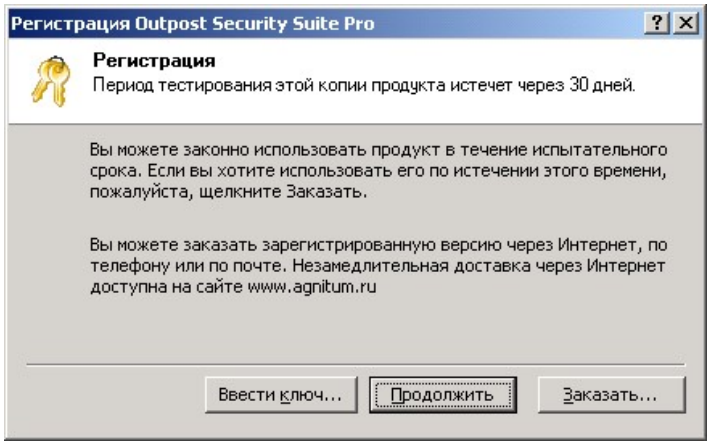
[5] При выполнении работы данный режим выбран в связи с отсутствием доступа к серверу обновлений в Интернет.

[6] Режим выбран в целях углубленного изучения настроек межсетевого экрана. В повседневной деятельности можно использовать автоматическое создание правил для приложений, подписанных доверенными издателями.



Закройте все окна и перезагрузите компьютер[7].

После перезагрузки в окне регистрации нажмите кнопку Продолжить (это позволит бесплатно тестировать продукт в течение 30 дней).



3.2. Создание правил запуска сетевых процессов

После перезагрузки межсетевой экран работает в режиме обучения, поэтому в процессе работы возможно появление всплывающих окон с сообщениями о разрешении продолжения запуска различных сетевых процессов. Сетевые процессы могут запускаться даже в тех случаях, когда компьютер не подключен к компьютерным сетям. Дело в том, что некоторые компоненты Windows работают по клиент-серверным технологиям, похожими на те, которые используются в сетях. Аналогичные способы взаимодействия могут использовать и вредоносные программы.

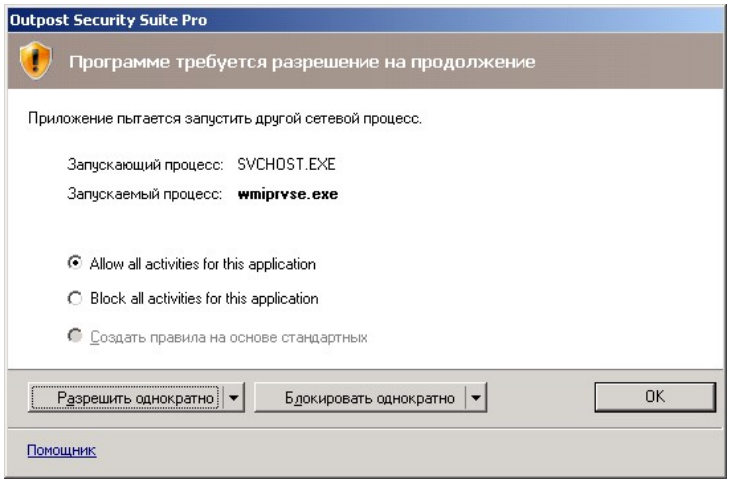
В режиме автоматического создания правил работы межсетевого экрана (этот режим был отключен нами) правила для многих сетевых процессов Windows создаются

[7] Если в процессе перезагрузки Windows виртуальная машина зависает (это может быть связано с некорректным взаимодействием Windows 2003, Agnitum Outpost и Oracle VirtualBox) принудительно выключите виртуальную машину и включите ее снова.

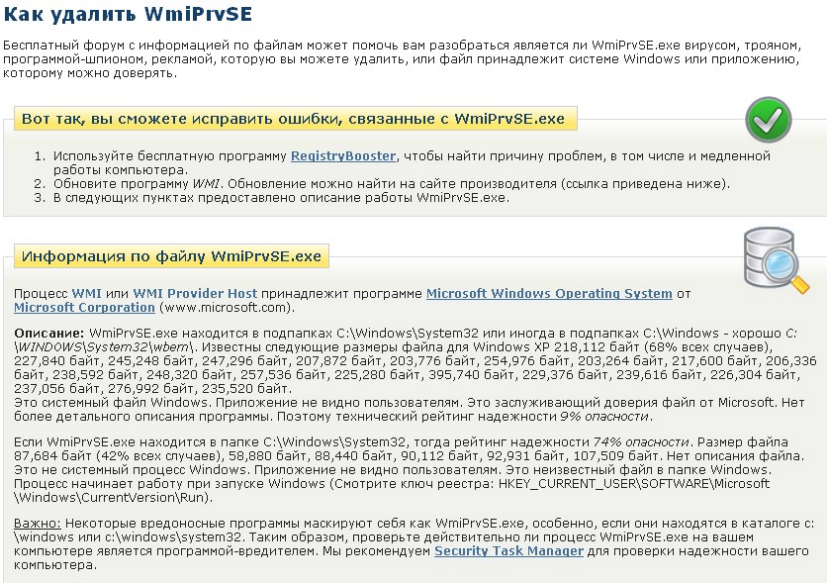
автоматически. В режиме ручного создания правил требуется вмешательство администратора.

Если есть уверенность в том, что запускаемый процесс является действительно штатным компонентом ОС или установленного программного обеспечения выделите опцию Allow all activities for this application и нажмите ОК. Если вы уверены, что данный сетевой процесс не должен запускаться выделите опцию Block all activities for this application и нажмите ОК. В случае сомнений можно либо разрешить однократный запуск, либо блокировать однократный запуск процесса для того, чтобы посмотреть насколько корректно при этом работает ОС или программное обеспечение.

В окне, представленном на рисунке ниже, запрашивается разрешение на запуск процесса wmiprvse.exe процессом SVHOST.EXE.

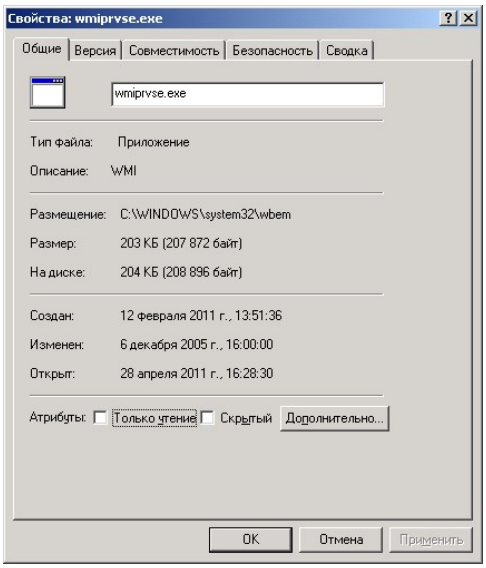


Для того чтобы определить есть ли необходимость разрешить запуск этого процесса можно обратиться на один из специализированных сайтов в Интернет. Ниже приведено описание процесса wmiprvse.exe, размещенное на сайте http://www.filecheck.ru.

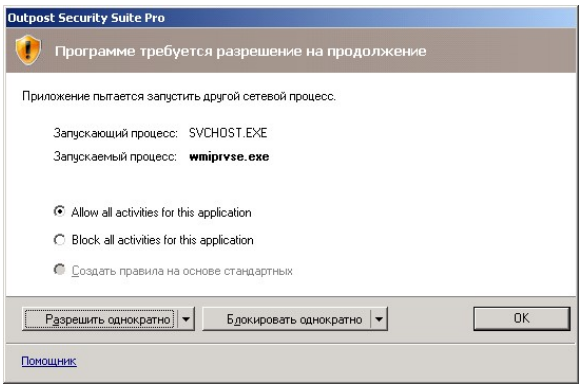


Найдите файл и посмотрите его свойства. В вашем случае (ОС Windows Server 2003 R2 Etnerprise Edition SP1 VL (rus)) файл располагается в папке

C:\WINDOWS\System32\wbem. Размер файла (см. рис. ниже) 207872 байта, что соответствует одной из версий файла.

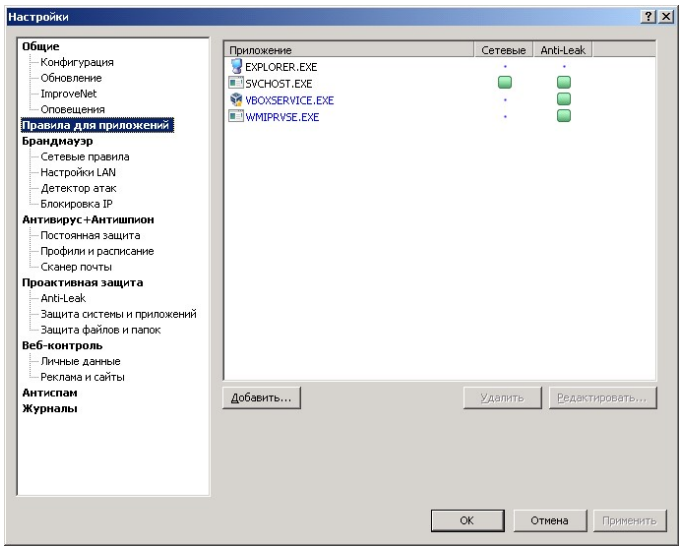


Создайте правило, разрешающее использование оттого процесса (выделите опцию Allow all activities for this application и нажмите OK).



Аналогичным образом осуществляется создание правил для других сетевых процессов (создайте эти правила при появлении запросов).

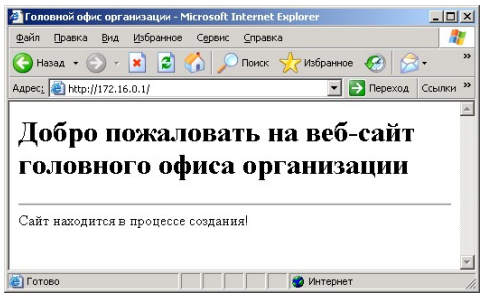
Созданные правила можно увидеть на вкладке Правила для приложений окна Настройки межсетевого экрана.



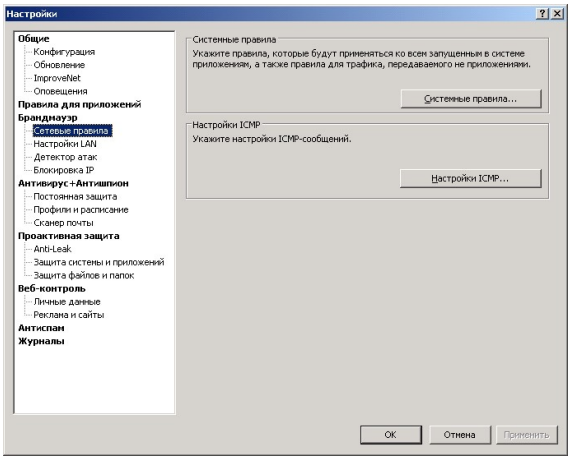
3.3. Настройка системных правил

Задача: запретить виртуальной машине Client2[8] (IP-адрес 10.0.0.3) любые подключения к виртуальной машине Server2 по протоколу TCP.

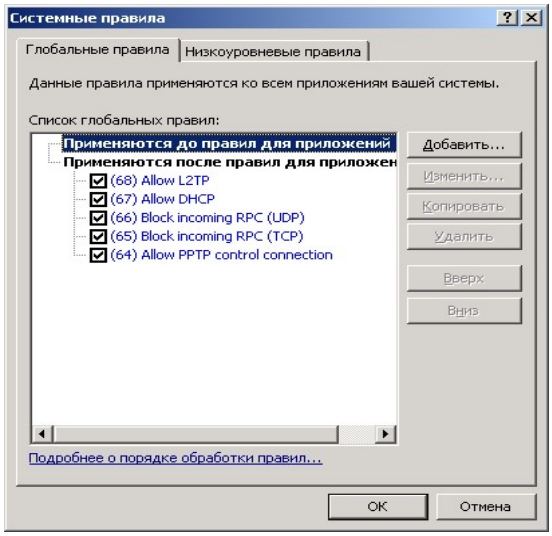
Предварительно запустите на виртуальной машине Client2 Internet Explorer и убедитесь, что имеется доступ к веб-страничке головного офиса организации.



Создайте новое правило на межсетевом экране Server2. Для этого запустите окно настроек (Меню Пуск → Программы → Agnitum → Outpost Security Suite Free → Outpost Security Suite Free → Настройки), перейдите на вкладку Сетевые правила и нажмите кнопку Системные правила.

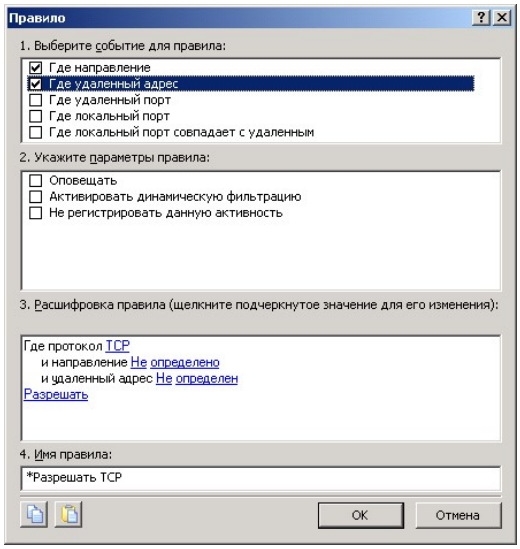


Нажмите кнопку Добавить



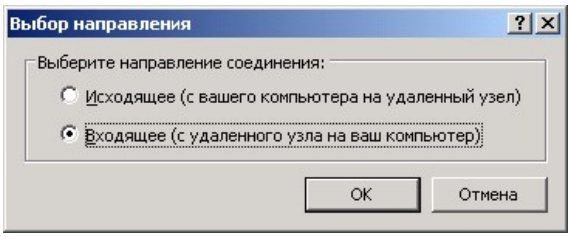
[8] См. схему сети

Установите флажки Где направление и Где удаленный адрес в поле 1.

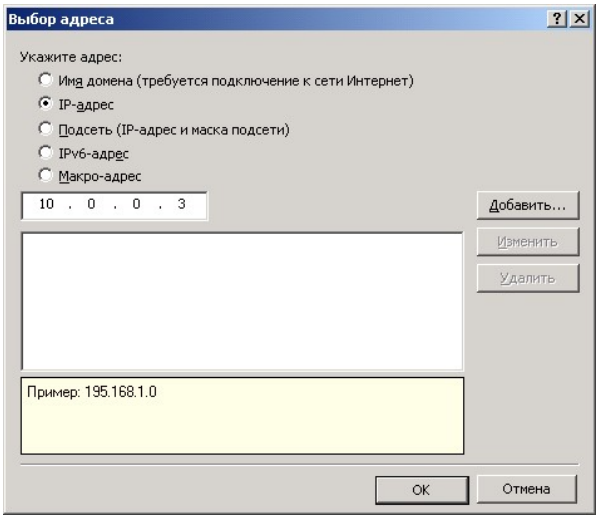


Щелкните клавишей мыши на подсвеченном тексте Не определено в поле 3.

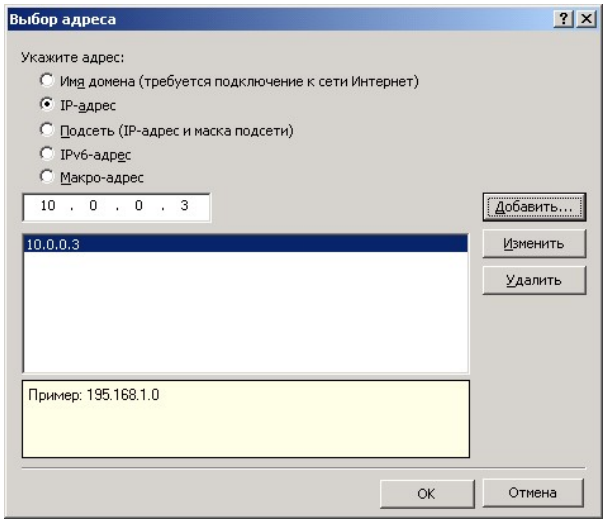
Выберите направление соединения Входящее (с удаленного узла на ваш компьютер).



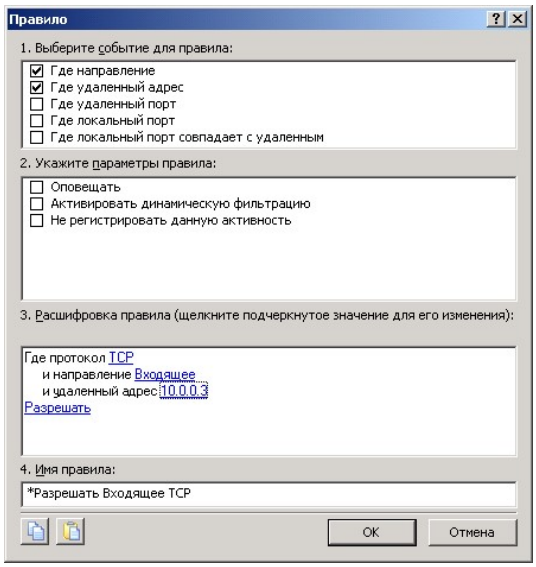
Щелкните клавишей мыши на подсвеченном тексте Не определен в поле 3. В открывшемся окне укажите IP-адрес 10.0.0.3. Нажмите кнопку Добавить



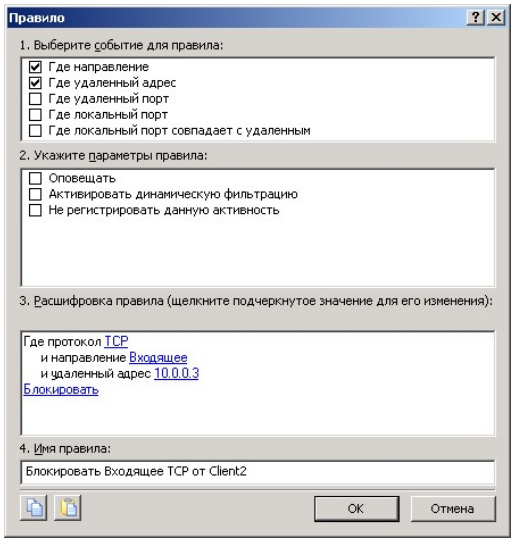
Нажмите кнопку ОК.



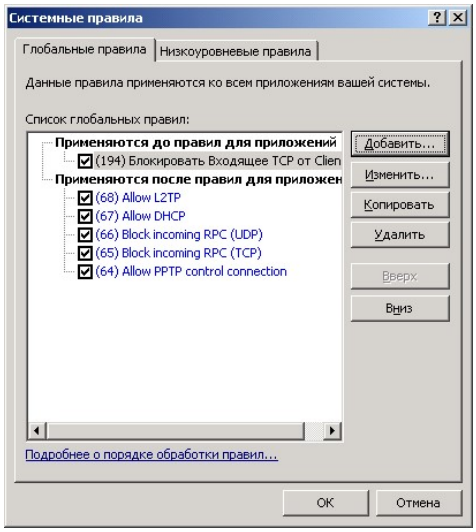
Щелкните клавишей мыши на подсвеченном тексте Разрешать в поле 3.



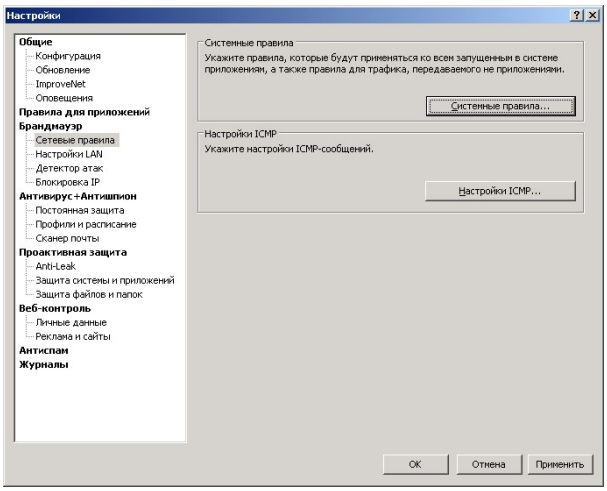
Текст изменится на Блокировать. Измените имя правила на Блокировать Входящее TCP от Client2 и нажмите ОК.



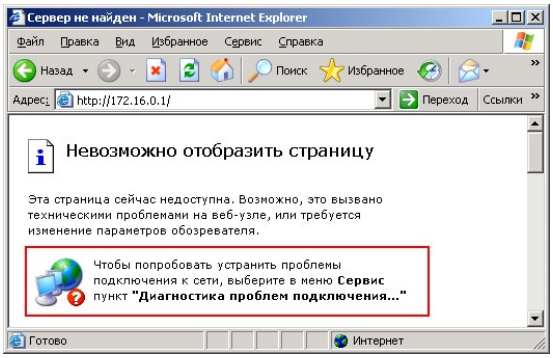
В окне Системные правила появилось созданное правило. Нажмите ОК.



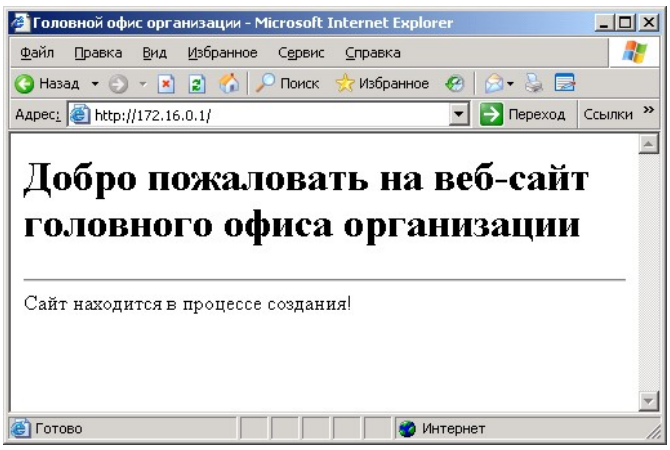
Нажмите Применить и ОК.



Перейдите в виртуальную машину Client2 и снова запустите Internet Explorer. В адресной строке укажите http://172.16.0.1 Если все действия были выполнены правильно входящее соединение к веб-серверу Server2 будет заблокировано и удаленные пользователи работающие на машине Client2 не получат запрошенную веб-страничку.



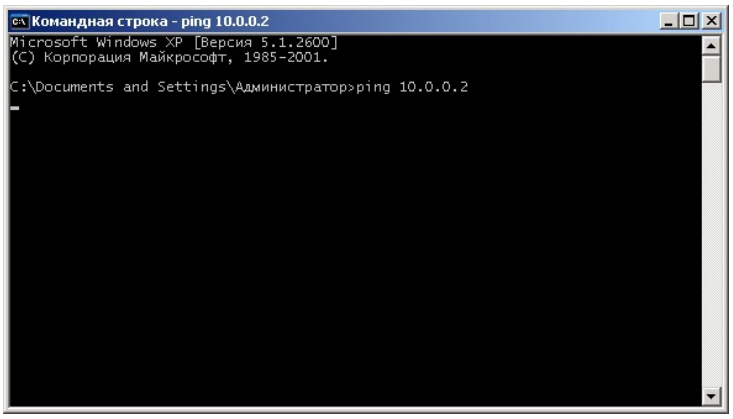
Проверьте доступ к веб-серверу с виртуальных машин Server1 и Client1. Запрошенная веб-страничка должна возвращаться.



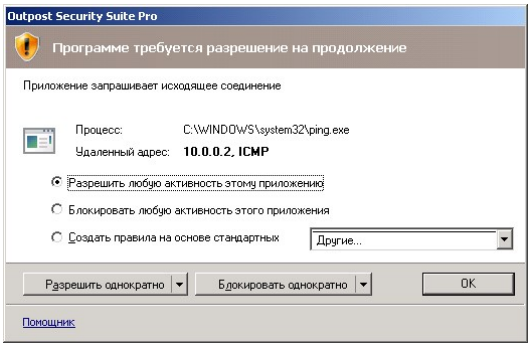
3.4. Настройка ICMP

Задача: Настройте на виртуальной машине Client1 разрешение на отправку эхо-запросов и запрет на отправку ответов на эхо-запросы.

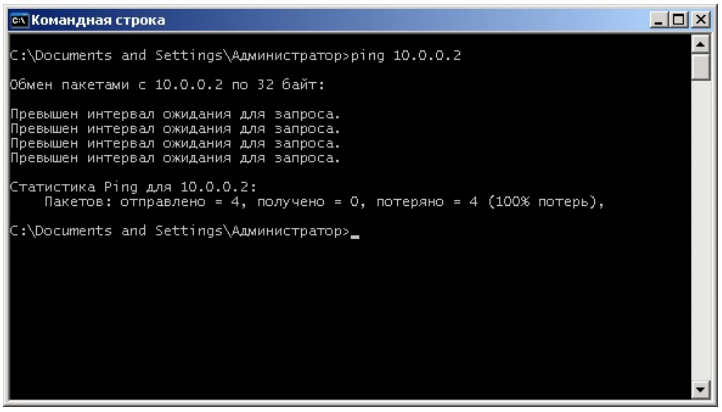
Отправьте эхо-запрос с виртуальной машины Client1 на Server2.



Разрешите любую сетевую активность процессу ping.exe и нажмите кнопку ОК.

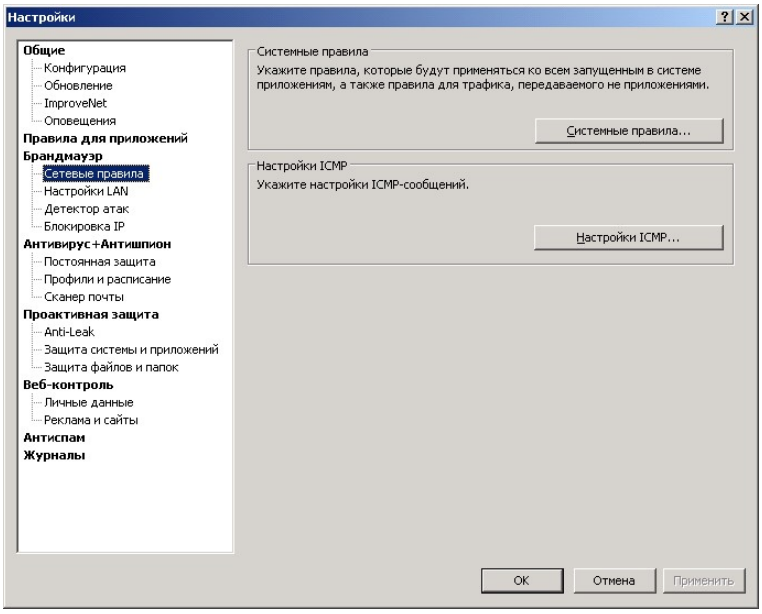


Так как по умолчанию на межсетевом экране установлена настройка, запрещающая эхо-ответы на эхо-запросы можно увидеть, что ответы не приходят.

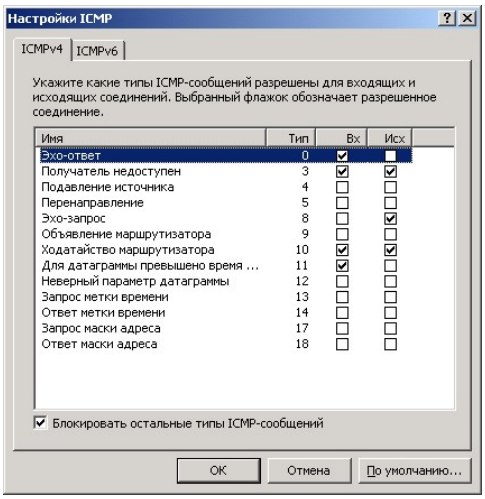


Настройте межсетевой экран на Server2 так, чтобы разрешить отправку эхо-ответов.

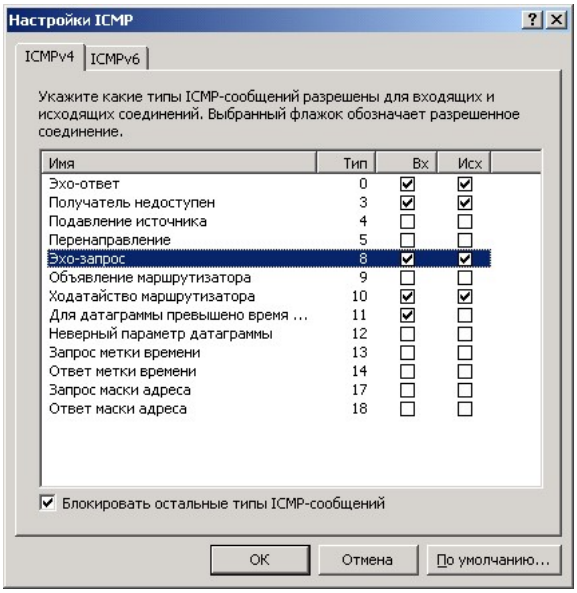
Для этого откройте окно настроек межсетевого экрана на Server2. Перейдите на вкладку Сетевые правила и нажмите кнопку Настройки ICMP.



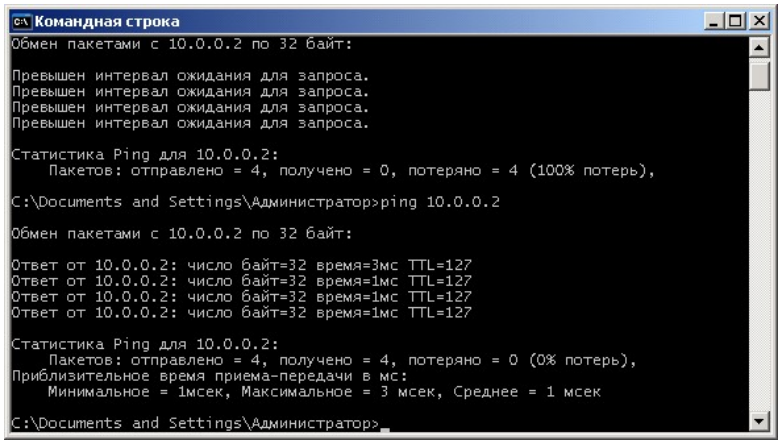
Видно, что в настройках прием входящих эхо-ответов (тип сообщения 0) и исходящих эхо-запросов (тип сообщения 8).



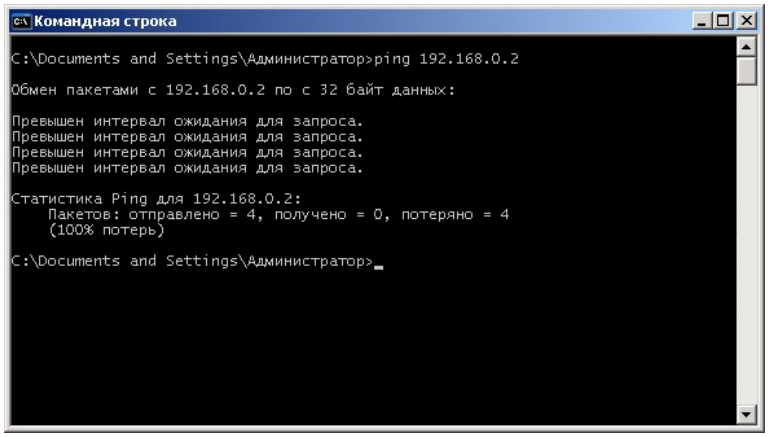
Разрешите исходящие эхо-ответы и входящие эхо-запросы. Для этого установите флажки в соответствии с рисунком ниже. Нажмите кнопку ОК. Нажмите кнопку Применить. Закройте окно настроек межсетевого экрана.



Повторите эхо-запросы с виртуальной машины Client1. Если все действия выполнены правильно они должны проходить.



В обратную сторону от Server2 к Client1 запросы не проходят.



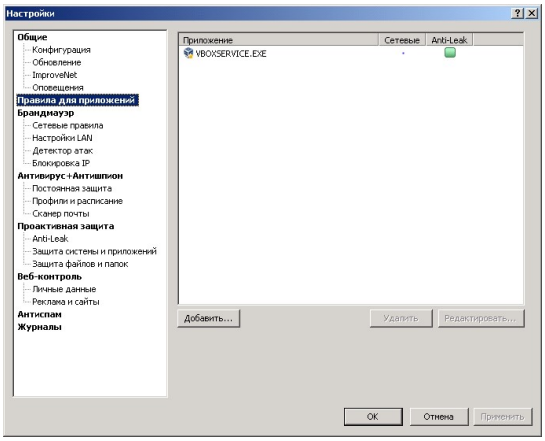
С точки зрения сетевой безопасности для Client1 это хорошо. Многие сетевые утилиты для обнаружения работающих хостов используют отправку эхо-запросов за правильно настроенным межсетевым экраном Client1 для них остается невидимым.

3.5. Настройка правил для приложений

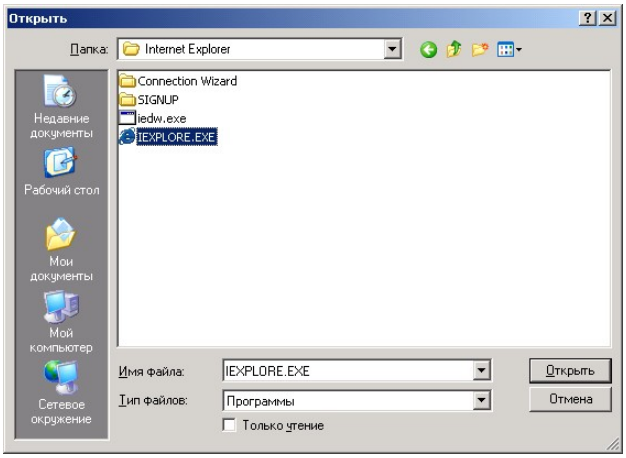
Разрешите на виртуальной машине Client1 сетевой доступ к веб-серверу, установленному на виртуальной машине Server2 с использование программы Internet Explorer.

Установите межсетевой экран на виртуальной машине Client1.

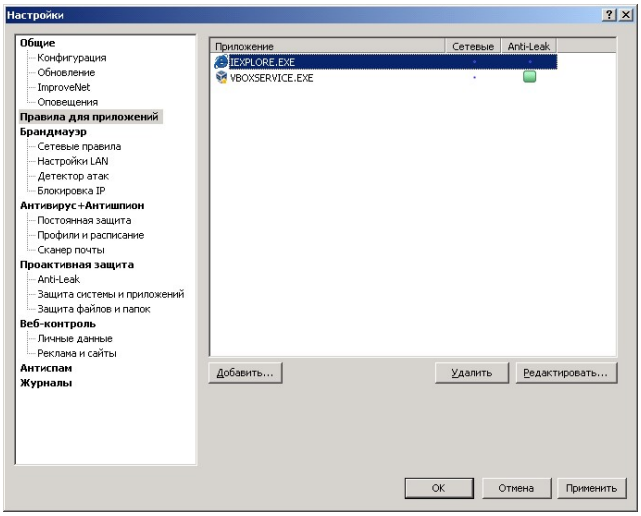
После перезагрузки откройте меню настройки и перейдите на вкладку Правило для приложений. Нажмите кнопку Добавить.



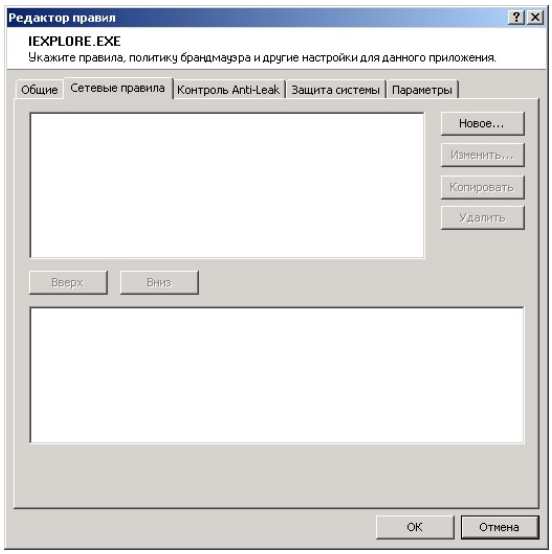
Укажите путь к программе Internet Explorer (C:\Program files\Internet Explorer\ IEXPLORE.EXE) и нажмите кнопку Открыть.



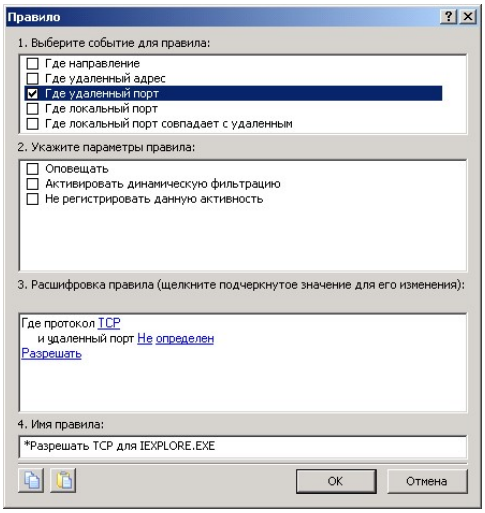
Выделите приложение IEXPLORE.EXE и нажмите кнопку Редактировать.



Перейдите на вкладку Сетевые правила и нажмите кнопку Новое…

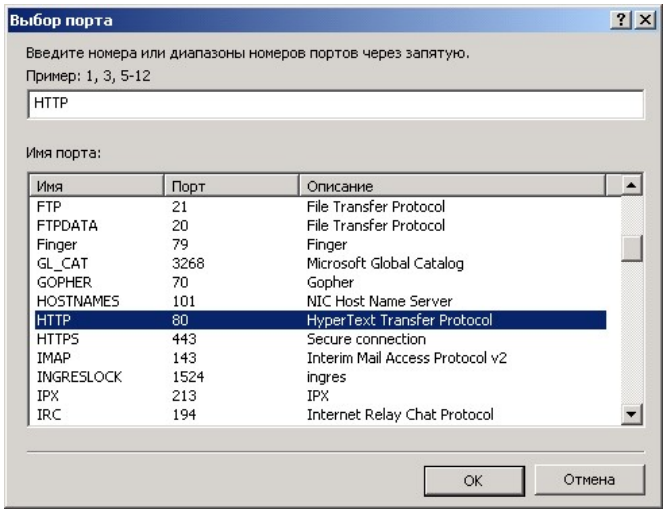


Установите флажок Где порт в поле 1.

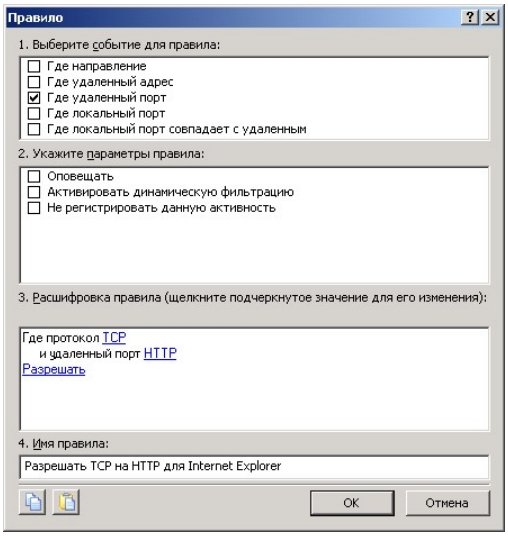


Щелкните клавишей мыши на подсвеченном тексте Не определен в поле 3.

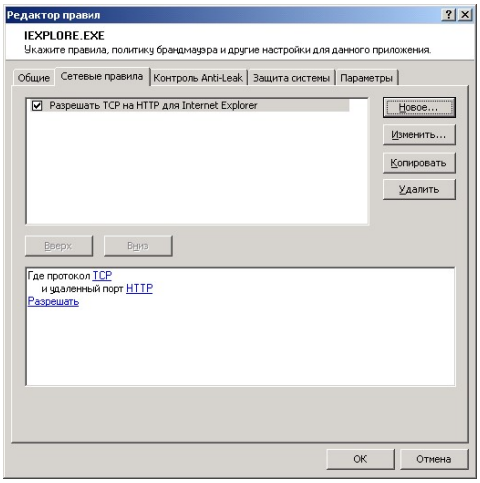
В поле ввода введите номер порта 80 – это стандартный порт, по которому работает веб-сервер (либо найдите в списке имен портов имя протокола HTTP и дважды щелкните по нему). Нажмите кнопку OK.



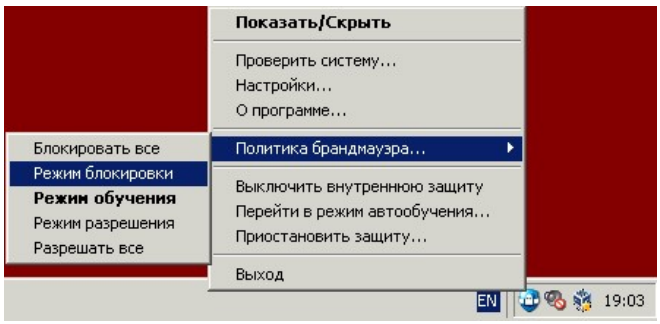
В поле Имя правила введите Разрешать TCP на HTTP для Internet Explorer и нажмите ОК.



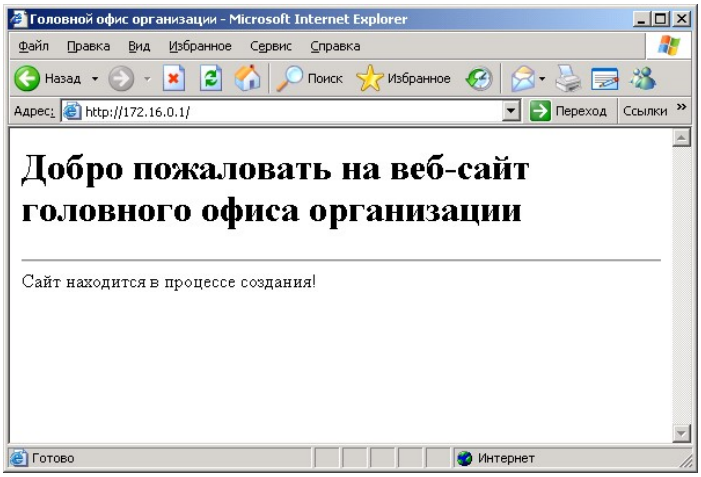
Во вкладке Сетевые правила должно появиться созданное правило. Нажмите ОК и применить. Закройте окно настроек.



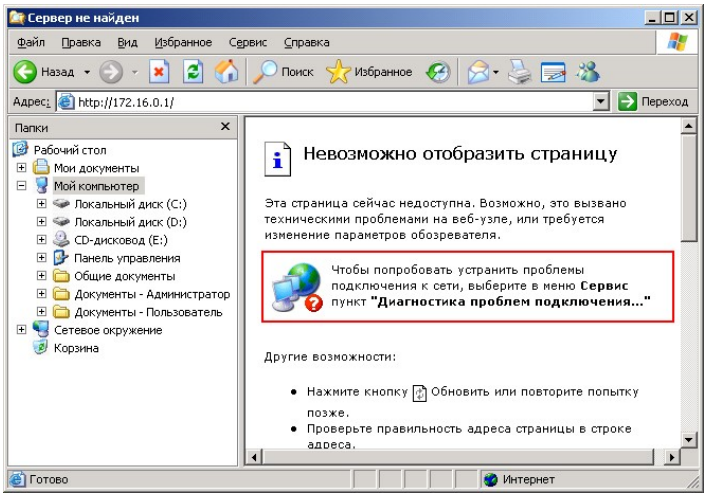
Переведите межсетевой экран в режим блокировки.



Запустите Internet Explorer и войдите на сайт головного офиса организации.



Проверьте возможность войти на сайт головного офиса организации с помощью программы Проводник. При правильной настройке доступ не должен предоставляться.



Аналогичный запрет доступа во внешние сети по протоколу HTTP с помощью других программ будет невозможен. Данный запрет позволит блокировать работу троянских программ и сетевых червей.

6. Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

– название практического занятия;

– текст индивидуального задания;

– цель работы;

– результаты проделанной работы;

– Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

7. Заключительная часть

В заключительной части подводятся итоги проделанной работы, дается краткая оценка действиям участников, прослеживается связь с теоретическими положениями и перспективой на будущую деятельность.

8.Задание и методические указания курсантам на самостоятельную подготовку:

1. Повторить по конспекту лекций и рекомендованной литературе основные возможности МЭ.
2. Быть готовыми к самостоятельной настройке МЭ.

V. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Руководство по администрированию *Agnitum Outpost FireWall*»;

2. Информационная безопасность: – учебное пособие / В.М.Зима, СПб.: ВКА имени А.Ф.Можайского, 2017 с.

2. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Ч.2. Сетевые ОС и принципы обеспечения информационной безопасности в сетях / С.И. Макаренко, А.А. Ковальский, С.А. Краснов СПб.: Наукоемкие технологии 2020.

3. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: МГТУ им. Н.Э. Баумана, 2002. –304 с.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.