МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Юго-Западный государственный университет»

(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2017 г.

КОНФИГУРИРОВАНИЕ МЕЖСЕВОГО ЭКРАНА

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Курск 2017

УДК 004
Составители: И.В. Калуцкий, А.Г. Спеваков., А.А. Асютиков.

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» *М.О. Таныгин*

Конфигурирование межсетевого экрана: методические указания к выполнению лабораторных и практических работ по дисциплинам / Юго-Зап. гос. Ун-т; сост. И.В. Калуцкий, А.Г. Спеваков. А.А. Асютиков. Курск, 2017, 16 с.: ил. 13.; Библиогр.: с. 16.

Содержат сведения по вопросам конфигурирования межсетевого экрана. Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл. печ. л. 0,93. Уч. –изд.л. 0,84 . Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

Введение 4
Цель работы 4
Порядок выполнения работы 4
Содержание отчета 4
Теоретическая часть 5
Выполнение работы 10
Варианты заданий 14
Контрольные вопросы 15
Список информационных источников 16

ВВЕДЕНИЕ

Интенсивное развитие глобальных компьютерных сетей, появление новых технологий поиска информации привлекают все большее внимание к сети Интернет со стороны частных лиц и различных организаций. Многие организации принимают решения по интеграции своих локальных и корпоративных сетей в Интернет. Использование Интернета в коммерческих целях, а также при передаче информации, содержащей сведения конфиденциального характера, влечет за собой необходимость построения эффективной системы защиты данных.

Использование глобальной сети Интернет обладает неоспоримыми достоинствами, но, как и многие другие новые технологии, имеет и свои недостатки. Развитие глобальных сетей привело к многократному увеличению атак на компьютеры, подключенные к Интернету. Ежегодные потери из-за недостаточного уровня защищенности компьютеров оцениваются десятками миллионов долларов. Поэтому при подключении к Интернету локальной сети необходимо позаботиться об обеспечении ее информационной безопасности.

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – определение основных понятий, которые изучает предмет передачи информации, изучение конфигурирования межсетевого экрана.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Сделать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Выполненное задание
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Теоретические основы защиты сетей

Обеспечение информационной безопасности - это процесс, опережающий управление риском, а не следующий за ним. В отличие от ответной модели, когда вначале происходит чрезвычайное происшествие, а только потом принимаются меры по защите информационных ресурсов, предупредительная модель работает до того, как что-то случится.

Предупредительное принятие необходимых мер - это правильный подход к информационной безопасности. В этом случае организация определяет свои уязвимые места, выявляет величину риска и выбирает экономически эффективные контрмеры. Это первый шаг в процессе обеспечения информационной безопасности.

Обеспечение информационной безопасности - это непрерывный процесс, включающий в себя пять ключевых этапов (рис. 1): оценку, политику, реализацию, квалифицированную подготовку и аудит.

Каждый из этих этапов по отдельности повышает уровень защищенности организации; однако только взятые вместе они обеспечивают основу, которая позволит эффективно управлять риском.

Рисунок 1 - Обеспечение информационной безопасности

Firewall’s защищают компьютеры и сети от попыток несанкционированного доступа с использованием уязвимых мест, существующих в семействе протоколов TCP/IP. Дополнительно они помогают решать проблемы безопасности, связанные с использованием уязвимых систем и с наличием большого числа компьютеров в локальной сети. Существует несколько типов firewall’ов, начиная от пакетных

фильтров, встроенных в пограничные роутеры, которые могут обеспечивать управление доступом для IP-пакетов, до мощных firewall’ов, которые могут закрывать уязвимости в большом количестве уровней семейства протоколов TCP/IP, и еще более мощных firewall'ов, которые могут фильтровать трафик на основании всего содержимого пакета.

Технологические возможности firewall’ов с начала 1990-х годов существенно улучшились. Сперва были разработаны простые пакетные фильтры, которые постепенно развивались в более сложные firewall’ы, способные анализировать информацию на нескольких сетевых уровнях. Сегодня firewall’ы являются стандартным элементом любой архитектуры безопасности сети.

Современные firewall’ы могут работать совместно с такими инструментальными средствами, как системы обнаружения проникновений и сканеры содержимого e-mail или web с целью нахождения вирусов или опасного прикладного кода. Но в отдельности firewall не обеспечивает полной защиты от всех проблем, порожденных Интернетом. Как результат, firewall’ы являются только одной частью архитектуры информационной безопасности. Обычно они рассматриваются как первая линия обороны, однако их лучше воспринимать как последнюю линию обороны в организации; организация в первую очередь должна делать безопасными свои внутренние системы. Для внутренних серверов, персональных компьютеров и других систем должны своевременно выполняться все обновления как самих систем, так и других систем обеспечения безопасности, например, антивирусного ПО.

Типичные конфигурации межсетевого экрана корпоративной сети и наборы правил. Системы за пределами межсетевого экрана, доступные из интернет

Для рассмотрения типовых конфигураций необходимо определить, что интернет-политика организации позволяет внутренним пользователям использовать следующие службы: HTTP, HTTPS, FTP, Telnet, SSH.

На рисунке 2 показано размещение доступных из интернета систем между сетевым экраном и внешним маршрутизатором. В таблице 1 приведены правила межсетевого экрана.

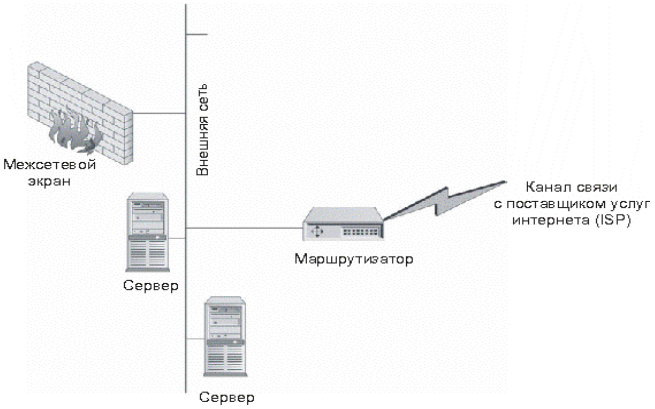

Рисунок 2 - Системы за пределами межсетевого экрана, доступные из интернета

На маршрутизаторе может быть установлена фильтрация, позволяющая только внешним данным HTTP поступать на веб-сервер и передавать на почтовый сервер только поступающие извне данные SMTP. Как видно из приведенных правил, независимо от того, какой тип межсетевого экрана используется, веб-сервер и почтовый сервер не защищены межсетевым экраном. В данном случае межсетевой экран лишь защищает внутреннюю сеть организации.

Таблица 1 - Системы за пределами межсетевого экрана, доступные из интернета

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие
2	Внутренняя сеть	Почтовый сервер	Любой HTTP, HTTPS, FTP, telnet, SSH	Принятие
3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

Один межсетевой экран

Вторая стандартная архитектура показана на рисунке 3. В данной архитектуре используется один межсетевой экран для защиты как внутренней сети, так и любых других систем, доступных из интернета. Эти системы располагаются в отдельной сети. В таблице 2 приведены правила межсетевого экрана.

Рисунок 3 - Один межсетевой экран

Таблица 2 - Правила межсетевого экрана для архитектуры с одним межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Как видно из таблицы 2, правила практически аналогичны правилам архитектуры 1. Межсетевой экран дополняет правила, которые использовались в маршрутизаторе в предыдущей архитектуре. Также мы видим, что не существует явного правила, позволяющего внутреннему почтовому серверу подключаться к почтовому серверу в отдельной сети. Причиной этому является правило 2, позволяющее любой системе (внутренней или внешней) подключаться к упомянутой системе.

Двойные межсетевые экраны

Третья архитектура, о которой пойдет речь, использует двойные межсетевые экраны (рис. 4). Доступные из интернета системы располагаются между межсетевыми экранами, а внутренняя сеть расположена за вторым межсетевым экраном. В таблице 3 приведены правила для межсетевого экрана 1.

Хорошим примером секретных сетей являются банковские сети. Каждый вечер банки связываются с системой федерального резерва для передачи денежных средств. Ошибки в этих сетях могут стоить банкам больших денег. Системы, управляющие такими соединениями, являются

крайне секретными и жизненно важными для банковских структур. Для ограничения доступа к этим системам из других подразделений банка можно установить межсетевой экран.

Рисунок 4 - Двойные межсетевые экраны

Как видно из таблицы 3, правила в данном случае аналогичны правилам межсетевого экрана в архитектуре 2. Но еще имеется и второй межсетевой экран. Правила для межсетевого экрана 2 приведены в таблице 4.

Таблица 3 - Правила межсетевого экрана 1 в архитектуре с двумя межсетевыми экранами

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Любой	Веб-сервер	HTTP	Принятие
2	Любой	Почтовый сервер	SMTP	Принятие
3	Почтовый сервер	Любой	SMTP	Принятие
4	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
5	Внутренняя DNS	Любой	DNS	Принятие
6	Любой	Любой	Любая	Сброс

Таблица 4 - Правила межсетевого экрана 2 в архитектуре с двойным межсетевым экраном

Номер	Исходный IP	Конечный IP	Служба	Действие
1	Внутренний почтовый сервер	Почтовый сервер	SMTP	Принятие
2	Внутренняя сеть	Любой	HTTP, HTTPS, FTP, telnet, SSH	Принятие
3	Внутренняя DNS	Любой	DNS	Принятие
4	Любой	Любой	Любая	Сброс

ВЫПОЛНЕНИЕ РАБОТЫ

Установка персонального межсетевого экрана

Для проведения исследования использовался межсетевой экран «Comodo Internet Security»[4]. (рис. 5).

Рисунок 5 - Вид сайта для скачивания дистрибутива

После скачивания дистрибутива необходимо запустить его и выбрать нужный язык из предложенных вариантов (рис. 6).

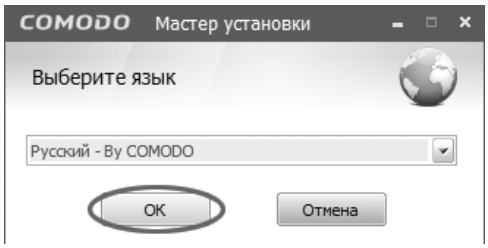

Рисунок 6 - Окно выбора языка установки

Выбрав нужный язык необходимо ознакомиться с настройками установки firewall. Для этого используем опцию «Опции установки» (рис. 7).

Рисунок 7 - Мастер установки

Окно опций установок содержит три вкладки: «Варианты установки», «Варианты конфигурации» и «Расположение файлов». Активной является вкладка «Варианты установки», которой содержит программы которые содержит дистрибутив (рис. 8). Так как темой данной лабораторной работы является исследование межсетевых экранов оставили только опцию «COMODO Firewall» и перешли на вкладку «Варианты конфигурации».

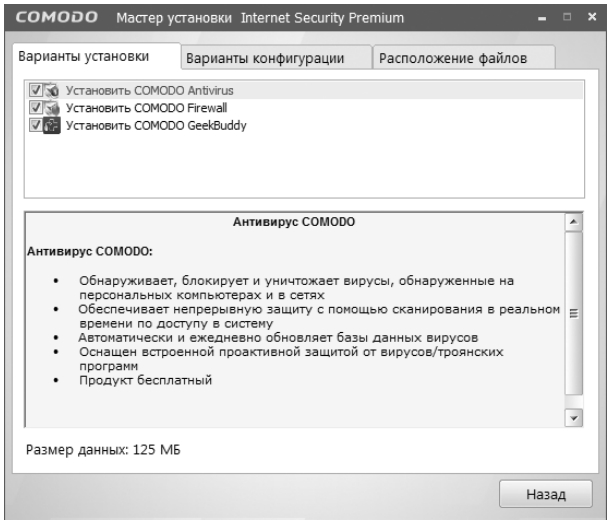

Рисунок 8 - Варианты установки

Данная вкладка содержит опции, которые можно отключить сразу перед установкой COMODO. А именно опции: «Включить Проактивную Защиту» и «Если возможно, не показывать оповещения, требующие от пользователя принятия решений по безопасности». Описание этих опции приведено на рисунке 9.

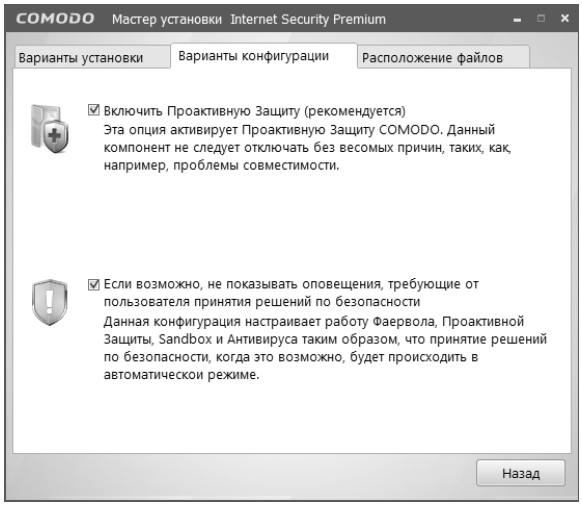

Рисунок 9 - Варианты конфигурации

Далее перешли на вкладку «Расположение файлов», которая указывает на каталог, который будет использован в качестве корневого для данной программы (рис. 10).

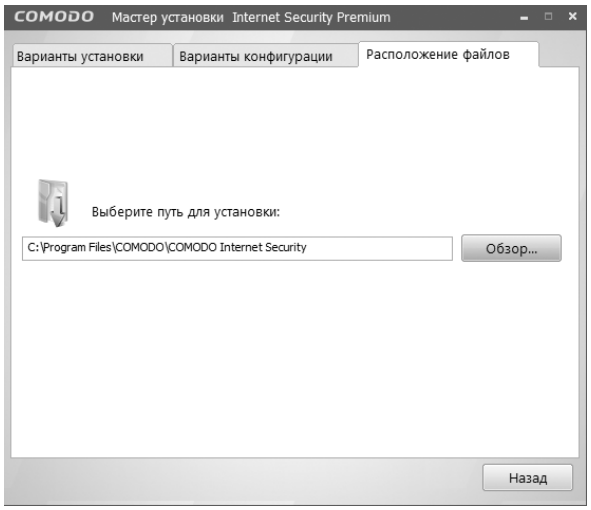

Рисунок 10 - Расположение файлов

После проведения данных операций вернулись на вкладку «Мастера установки» и нажали на кнопку «Согласен, Установить» (рис. 7). После установщик приступит к распаковке файлов. Распаковка продлиться несколько минут, время зависит от конфигурации компьютера.

Настройка персонального межсетевого экрана

После установки межсетевого экрана «Comodo Internet Security» необходимо выполнить его настройку. Для этого необходимо перейти на вкладку «Фаервол» на верхней панели (рис. 11).

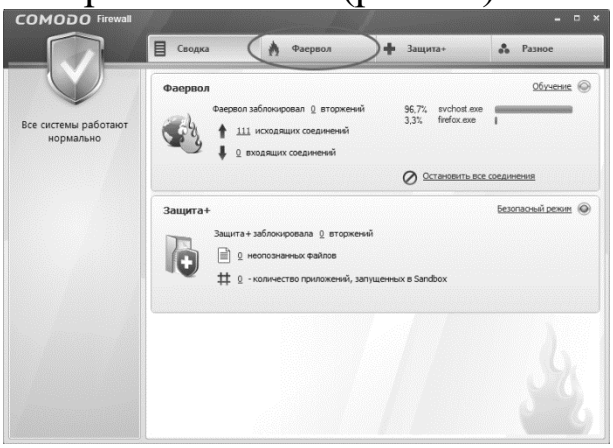

Рисунок 11 - Главное окно программы

Для того чтобы выполнить настройку межсетевого экрана необходимо перейти в раздел «Настройки фаервола» (рис. 12).

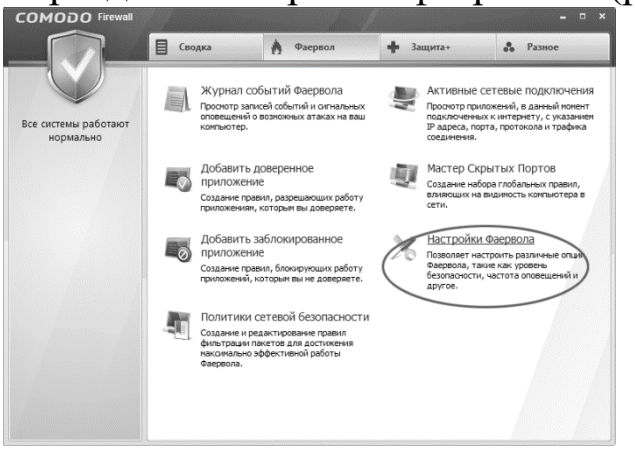

Рисунок 12 - Окно мониторинга и настроек

Далее нам предоставляется выбор режима работы межсетевого экрана. Всего существует 5 режимов (рис. 13):

«Блокировать всё» - в данном режиме межсетевой экран блокирует любую сетевую активность.

«Пользовательская политика» - в данном режиме межсетевой экран блокирует любую сетевую активность, противоречащую заданной политике безопасности системы. Действует постоянное оповещение.

«Безопасный режим» - в данном режиме межсетевой экран следует строго приведенной политике безопасности заданной политике

безопасности системы и оповещает пользователя об активности неизвестных приложений.

«Режим обучения» - в данном режиме межсетевой экран сохраняет все запросы приложений и запоминает все действия пользователя по отношению к ним. Этот режим наиболее подходящий для реализации домашнего межсетевого экрана.

«Неактивен» - в данном режиме межсетевой экран отключен.

Также предоставляется выбор периодов оповещения межсетевого экрана.

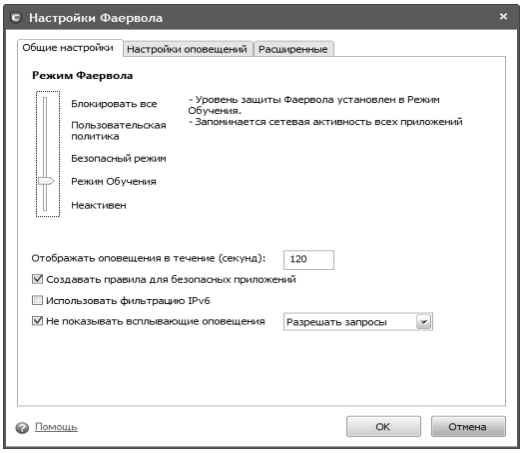

Рисунок 13 - Окно настроек режима фаервола

ЗАДАНИЕ:

1. Разобраться в назначении параметров и ключей следующих утилит:
   - sc;
   - netsh с дерективами firewall и diag;
   - netstat.
2. Создать скрипт, который:
   - включает автоматическую загрузка Брандмауэра Windows;
   - запускает брандмауэр;
   - включает протоколирование входящих соединений;
   - настраивает службу Telnet на ручной запуск;
   - добавляет правило, разрешающее доступ с IP адресов сети компьютерного класса к службе Telnet;
   - разрешает системе отвечать на запросы echo-request ICMP;
   - запускает службу Telnet;
3. Запустить сеанс Telnet из реального компьютера в гостевую ОС.

4. В гостевой ОС вывести на экран данные только об установленных соединениях со службой Telnet, с указанием IP адресов и портов в численной форме.
5. В гостевой ОС проверить доступность службы Telnet на виртуальной машине.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. От чего не способен защитить классический firewall?
2. Можно ли организовать доступ к Web серверу, если у клиентов закрыт доступ к 80 порту?
3. В чем отличие правил Deny и Drop?
4. Каким образом осуществляется оптимизация правил, используемых в работе firewall?
5. Перечислите ограничения брандмауэра Windows относящиеся к фильтрации трафика TCP/IP.

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. Межсетевые экраны. Способы организации защиты. [Электронный ресурс]:/Internet. -http://www.compress.ru/article.aspx?id=10145&iid=420#11 - 2017
2. Безопасность сетей. [Электронный ресурс]: / Internet. - http://www.intuit.ru/department/security/netsec/10/netsec_10.html (17.09.2017)
3. Межсетевое экранирование. [Электронный ресурс]: / Internet. - http://www.intuit.ru/department/network/firewalls/ (25.09.2017)
4. Официальный сайт «Comodo Internet Security». [Электронный ресурс]: / Internet. - http://www.comodorus.ru/ (25.09.2017)