ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 2022 г.

Практическое занятие № 14
по учебной дисциплине
«Защита информации»
на тему:

«Настройка межсетевого экрана в МСВС 3.0»

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

Санкт-Петербург
2022

I. ТЕМА И ЦЕЛЬ САМОСТОЯТЕЛЬНГО ЗАНЯТИЯ ПОД РУКОВОДСТВОМ ПРЕПОДАВАТЕЛЯ

Тема занятия: Настройка межсетевого экрана в МСВС 3.0

Цели работы:

1. Приобрести знания и навыки по созданию правил фильтрации пакетов межсетевым экраном.
2. Приобрести практические навыки по настройке межсетевого экрана для МСВС 3.0.

Время - 90 мин
Место - класс ПЭВМ

Учебно-материальное обеспечение

1. ПЭВМ
2. Дистрибутив ОС МСВС 3.0, DrWeb

1.УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ

№ п.п.	Учебные вопросы	Время, мин
1	2	3
1.	Вступительная часть Проверка готовности слушателей к занятию	5
2.	Учебные вопросы	
	1. Настройка правил фильтрации пакетов межсетевым экраном.	45
	2. Настройка межсетевого экрана для МСВС 3.0	35
3.	Заключительная часть Задание и методические указания слушателям на самостоятельную подготовку	5

III. УЧЕБНЫЕ МАТЕРИАЛЫ

Вступительная часть

Товарищи курсанты, целью сегодняшнего занятия является - приобретение практических навыков в настройке межсетевого экрана для МСВС 3.0.

Итак, тема сегодняшнего занятия – «Настройка межсетевого экрана в МСВС 3.0».

Для достижения поставленных учебных целей вам требуется отработать два учебных вопроса занятия:

1. Правила фильтрации пакетов межсетевым экраном.
2. Настройка межсетевого экрана для МСВС 3.0.

Порядок проведения занятия будет следующий - сначала вы ответите на ряд контрольных вопросов, что позволит оценить вашу теоретическую готовность к занятию, а затем в рамках рассматриваемых вопросов занятия вы будете исполнять задания с использованием ПЭВМ. Ваша работа будет оцениваться на местах.

Контрольные вопросы до начала занятия.

Вопрос № 1: Для чего необходимы МЭ?

Вопрос № 2: При помощи какого средства в МС ВС осуществляется межсетевое экранирование?

Вопрос № 3: Для чего формируются правила фильтрации пакетов МЭ?

Выполнение самостоятельного занятия под руководством преподавателя проводится в соответствии с заданием на практическое занятие № 2, приведенного в Приложении.

Заключительная часть

Товарищи курсанты, на сегодняшнем занятии вы практически отработали вопросы связанные с настройкой МЭ и формированием правил фильтрации пакетов МЭ .

На занятии активно и правильно выполняли задания курсанты:___им выставлены оценки.

Задание и методические указания курсантам на самостоятельную подготовку

1. Повторить материалы лекции «Комплексное обеспечение информационной безопасности АС».
2. Продолжить работу над курсовым проектированием и быть готовым доложить полученные результаты.

IV. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

Старший преподаватель 63 кафедры
майор

С.Краснов

ЗАДАНИЕ
НА САМОСТОЯТЕЛЬНОЕ ЗАНЯТИЕ ПОД РУКОВОДСТВОМ ПРЕПОДАВАТЕЛЯ № 2.

«НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА В МСВС 3.0».

Цели работы: *1.Приобрести знания и навыки по созданию правил фильтрации пакетов межсетевым экраном.*
2.Приобрести практические навыки по настройке межсетевого экрана для МСВС 3.0.

1. Задание на практическое занятие

1.1. Изучить назначение и основные возможности межсетевого экрана п. 4.1. п. 4. 2 данного руководства.
1.2. Изучить формирование правил МЭ.
1.3. Настроить межсетевой экран.

2. Подготовка к работе

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

2.1. Изучить настоящее задание.

2.2. Повторить материал занятий, на которых рассматривались назначение, классификация и принципы работы межсетевого экрана.

3. Методические указания

3.1. В классе ПЭВМ курсанты самостоятельно под руководством преподавателя изучают п. 4.1. п. 4. 2 настоящего задания.

3.2. При выполнении задания работу следует спланировать таким образом, чтобы в первую очередь изучить назначение, основные возможности межсетевого экрана, порядок работы, формирование правил, а затем приступить к настройке межсетевого экрана.

3.3. В ходе практической работы со средствами управления запрещается вносить изменения, удалять или добавлять какие-либо компоненты, настройки и параметры ОС, кроме указанных ниже.

3.4 В конце ПЗ вернуть все настройки МЭ в исходное состояние.

4. Выполнение работы

4.1. Назначение и основные возможности межсетевого экрана .

4.1.1. Общие положения фильтра пакетов.

Межсетевой экран представляет собой фильтр пакетов, с помощью которого можно контролировать сетевой трафик, проходящий через данный компьютер.

Все ОС, использующие протокол IP, передают данные в виде пакетов. В начале каждого пакета есть заголовок, в котором написано, от кого и кому этот пакет (в виде IP-адресов), к какому протоколу более высокого уровня он относится (TCP, UDP и т.п.), в некоторых случаях (для протоколов UDP и TCP) - номера портов отправителя и получателя, а также другая специфическая информация. На

пути от отправителя к получателю пакет может проходить через промежуточные узлы. В зависимости от информации, которая содержится в заголовке IP-пакета, они могут этот пакет переслать на следующий узел (forward), передать локальной программе для обработки, уничтожить (deny), отвергнуть, т.е. уничтожить и отправить об этом уведомление отправителю (reject). Выбор и осуществление одного из этих действий называется фильтрацией пакетов. Для осуществления фильтрации пакетов в составе СЗИ ОС МСВС 3.0 работает фильтр пакетов ipchains. Данный фильтр пакетов позволяет выполнять следующие три задачи:

1. фильтрацию пакетов;

2. трансляцию сетевых адресов;

3. прозрачное проксирование.

Фильтрация пакетов - это механизм, который, основываясь на некоторых правилах, разрешает или запрещает передачу информации, проходящей через него, с целью ограждения некоторой подсети от внешнего доступа, или, наоборот, для недопущения выхода наружу. Фильтр пакетов может определять правомерность передачи информации на основе только заголовков IP-пакетов, а может анализировать и их содержимое, т.е. использовать данные протоколов более высокого уровня.

4.1.2. Включение фильтра пакетов.

Чтобы фильтр пакетов начал работать, надо записать '1' в файл /proc/sys/net/ipv4/ip_forward:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Соответственно, если туда записать 0, то он работать перестанет. Эту строку рекомендуется вписать в какой-нибудь скрипт, автоматически запускаемый при загрузке системы. Ядро запускается с тремя встроенными наборами правил фильтрации пакетов, которые называются входной (input), выходной (output) и пересылочный (forward). В дополнение к встроенным можно создавать новые наборы правил.

Наборы правил состоят из правил. Каждое правило содержит условие и, возможно, действие, которое надо произвести с пакетом, если его параметры соответствуют заданному условию. Если пакет не соответствует условию, то проверяется следующее правило в наборе правиле. Если пакет не удовлетворяет ни одному условию, используется политика по умолчанию данного набора правил. В защищенных системах эта политика требует уничтожить или отвергнуть пакет. Пакеты, сгенерированные локальными процессами и адресованные на локальный интерфейс (loopback, lo), проверяются через выходной с интерфейсом lo, а затем по входному набору правил также с интерфейсом lo. (Интерфейс, через который проходит пакет, может влиять на обработку его фильтром пакетов). Таким образом, встроенные наборы правил используются в следующих случаях: если пакет пришел извне или адресован на данный компьютер (или и то, и другое), то он проверяется

по входному набору правил, если пакет адресован на другой компьютер, или сгенерирован на данном компьютере, (или и то и другое), то он проверяется по выходному набору правил, если пакет не был сгенерирован локальным процессом и не подвергался демаскарадингу, то он проверяется по пересылочному набору правил.

4.1.4. Формирование правил

Команды операций с отдельными правилами

Имеется несколько команд управления правилами внутри набора правил:

- '-A', add - добавить новое правило к набору правил;
- '-I', insert - вставить новое правило в определенную позицию набора правил;
- '-R', replace - заменить правило в определенной позиции набора правил;
- '-D', delete - удалить правило в определенной позиции набора правил;
- '-D', delete - удалить первое правило в наборе правил, удовлетворяющее условию.

Условия проверки пакетов, которые можно задавать в правилах

Ниже приводятся условия проверки пакетов задаваемые в правилах:

- '-s', source - адрес отправителя;
- '-d', destination - адрес получателя;
- '!', not - инверсия условия;
- '-p', protocol - протокол;
- номера портов для протоколов TCP и UDP
- тип (type) и код (code) для протокола ICMP
- '-i', interface - интерфейс;
- '-y' - флаг - только TCP SYN-пакеты;
- '-f', fragment - флаг - только фрагменты пакетов.

Действия над пакетами, которые можно задавать в правилах

Действия над пакетами, задаваемые в правилах:

- '-j',? выполнить действие;
- '-l', - регистрация пакета в журнале;
- '-t', - изменение типа обслуживания.

Команды операций с целыми наборами правил

Ниже приводится перечень команд операций с целыми наборами правил:

- '-N', new - создать новый ;
- '-X' - удалить пустой ;
- '-F', flush - удалить все правила из набора правил;
- '-L', list - распечатать правила набора правил;
- '-Z', zero - обнулить счетчики байт и пакетов для всех правил в наборе правил;
- '-P', policy - изменить политику для встроенного набора правил.

Команды маскарадинга

Ниже приведены две команды управления маскарадингом:

- '-M -L', masquerade list - вывести текущие параметры маскарадинга;
- '-M -S', masquerade set - установить значения таймаутов для маскарадинга.

Изменение нескольких правил одной командой

Необходимость изменения нескольких правил одной командой возникает:

- при разрешении одного символического адреса в несколько IP-адресов;
- при использовании флага '-b' (bidirectional);
- при использовании флага '-v' (verbose).

Команды операций с правилами в наборах правил

Добавление нового правила к набору правил производится командой '-A' (add), за которой следует имя набора правил и все другие необходимые параметры и флаги, например:

ipchains -A input -s 127.0.0.1 -p icmp -j DENY

будет уничтожать ICMP-пакеты с адреса 127.0.0.1 при проверке по входному набору правил. Правила, добавляемые командой -A, приписываются в конец набора правил.

Новое правило можно вставить в определенную позицию набора правил командой '-I' (insert), после которой должно быть указано имя набора правил и номер, а также другие необходимые параметры. Остальные правила в наборе правил (если они есть) будут сдвинуты на следующие позиции. Первое правило в наборе правил имеет номер 1. Например:

ipchains -I forward 1 -p tcp -d 0/0 unv -j DENY - запрещает пересылку tcp-пакетов на unv-порт.

Заменить правило в определенной позиции набора правил можно командой '-R' (replace), после которой должно быть указано имя набора правил и номер, а также другие необходимые параметры. Синтаксис полностью совпадает с командой '-I'.

Удалить правило в определенной позиции набора правил можно командой '-D' (delete), например:

ipchains -D forward 1

Остальные правила в наборе правил (если они есть) сдвигаются на 1 позицию.

Если не известен номер правила в наборе правил и нет необходимости его определять, то можно применить команду удаления по условию. Для этого после команды -D и названия набора правил надо указать тот же набор параметров, который использовался при создании правила командами '-A', '-I' или '-R', например:

ipchains -D input -s 127.0.0.1 -p icmp -j DENY

Однако если в наборе правил было несколько одинаковых правил, будет удалено только первое из них.

Условия проверки пакетов, которые можно задавать в правилах

Адреса отправителя и получателя могут быть заданы, соответственно, после параметров '-s' и '-d', в следующих формах:

- в виде символического адреса (localhost, unv.kernel.org и т.п.)
- в виде IP-адреса (127.0.0.1)
- в виде IP-адреса с маской в виде четырех десятичных чисел (1.2.3.0/255.255.255.0 - означает все адреса от 1.2.3.0 до 1.2.3.255)
- в виде IP-адреса с битовой маской (1.2.3.0/24 эквивалентно 1.2.3.4/255.255.255.0, а 1.2.3.4/32 эквивалентно 1.2.3.4/255.255.255.255). Если маска после адреса не указана, то подразумевается /32, то есть правило распространяется только на сам указанный адрес. Чтобы указать любой адрес, можно использовать маску 0, сам адрес при этом может быть любым, хотя обычно тоже используется 0:

ipchains -A input -s 0/0 -j DENY

Тот же эффект будет достигнут, если в правиле вовсе не указывать адрес. Единственный случай, когда применяется адрес 0/0 - это когда необходимо указать номер порта или тип и код ICMP-пакетов, поскольку их невозможно указать без адреса.

Инверсия условия

Многие условия (в частности, -s и -d) допускают инвертирование путем указания '!' перед параметром. Например, чтобы указать все пакеты, кроме пришедших с localhost, надо использовать параметр
'-s ! localhost'

Протокол ('-p') может указываться в виде названия (большими или маленькими буквами) - TCP, UDP, ICMP, или в виде номера (см. /etc/protocols). К протоколам также может применяться инверсия:

'-p ! TCP' -означает любой протокол, кроме TCP.

Для протоколов TCP и UDP в параметрах '-s' и '-d' после адреса могут указываться номера портов. Порты могут указываться в виде символического имени, например, unv (см. /etc/services), в виде десятичного номера (например, 80) и в виде диапазона (80:82 включает порты 80, 81, 82). Если в диапазоне пропущена нижняя граница, то подразумевается 0 (например, :19 означает все порты с 0 по 19 включительно), если верхняя, то подразумевается 65535. Если порт не указан вовсе, то подразумеваются все. К портам также может применяться инверсия:

'-p TCP -d 0.0.0.0/0 ! unv' - означает все пакеты протокола TCP, кроме адресованных на 80 порт.

Внимание. Условие '-p TCP -d ! 192.168.1.unv' сильно отличается от условия

'-p TCP -d 192.168.1.1 ! unv'

Первое означает любой TCP-пакет на unv-порт любого компьютера, кроме как на 192.168.1.1. Второе означает любой TCP-пакет на любой порт компьютера 192.168.1.1, кроме порта unv.

А запись '-p TCP -d ! 192.168.1.1 ! unv' означает любой TCP-пакет, кроме адресованных на любой порт компьютера 192.168.1.1 и кроме адресованных на unv-порт любого компьютера.

Для протокола ICMP могут указываться тип (type) и код (code) ICMP-пакетов. Тип может указываться после адреса в параметре '-s', а код - в параметре '-d'. Они могут указываться в виде чисел, а тип - и в виде символического имени. Чтобы получить список символических имен типов, необходимо набрать команду

ipchains -h icmp

В таблице 1 указаны наиболее распространенные типы ICMP-пакетов.

Таблица 1

Номер типа	Название типа	Кем используется
0	echo-reply	ping
3	destination-unreachable	любой TCP/UDP-трафик
5	redirect	маршрутизация в отсутствие демона маршрутизации
8	echo-request	ping
11	time-exceeded	traceroute

В ipchains имена типов не могут инвертироваться с помощью '!'.

Примечание

Нельзя запрещать передачу ICMP-пакетов типа 3. Это может сильно замедлить или вообще заблокировать передачу данных.

В данном случае под интерфейсом понимается физическое или логическое устройство, через которое могут приниматься или передаваться пакеты. Чтобы узнать, какие интерфейсы присутствуют в компьютере и активны (up), необходимо воспользоваться командой ifconfig. Параметр '-i' позволяет задать проверку интерфейса в правиле.

Интерфейсом для входящих пакетов (т.е. проверяемых по входному набору правил) является тот интерфейс, через который они получены. Интерфейсом для выходящих пакетов (т.е. проверяемых по выходному набору правил) считается тот, через который они будут отправлены. Интерфейсом для транзитных пакетов (т.е. проверяемых по пересылочному набору правил) также считается тот, через который они будут отправлены дальше. При проверке по пользовательскому набору правил интерфейс определяется в зависимости от того, из какого встроенного набора правил он был вызван.

Допускается, при задании правил, указывать неактивный (down) или вообще отсутствующий в данный момент интерфейс. Такое правило просто не будет соответствовать ни одному пакету, пока интерфейс не активизируется.

Можно указать сразу некоторую группу интерфейсов, написав '+' после имени. Так, '-i ppp+' означает все интерфейсы, имена которых начинаются с 'ppp' (в том числе, и не существующие на момент задания правила).

К интерфейсам также применима инверсия: '-i ! eth0' означает все интерфейсы, кроме eth0.

При необходимости можно разрешить создание TCP-соединений только в одну сторону (например, из локальной сети в остальной интернет, но не наоборот). Фильтрация пакетов только по адресам здесь не поможет, потому что TCP-соединение требует передачи пакетов в обе стороны. Решение проблемы состоит в том, чтобы уничтожать пакеты с запросом на установку соединения, идущие в нежелательную сторону.

Пакеты с запросом на установку TCP-соединения отличаются тем, что у них установлен флаг SYN, а флаги FIN и ACK сброшены, и по традиции называются

SYN-пакетами. Проверка этого условия включается флагом '-y'. Он допустим только в правилах с указанным протоколом TCP, например:

-p TCP -s 192.168.1.1 -y - означает пакеты на установку соединения, отправленные с компьютера 192.168.1.1. Флаг -'y' может инвертироваться с помощью '!' для указания всех пакетов, кроме SYN.

Если пакет превышает максимально возможный размер для передачи по некоторому каналу (MTU - maximum transfer unit). В этом случае он разбивается на несколько пакетов (фрагментов), которые посылаются по отдельности. Это называется фрагментацией (fragmentation). На принимающей стороне фрагменты собираются обратно (дефрагментация - defragmentation).

Проблема состоит в том, что некоторые данные, необходимые для проверки условий фильтрации, содержатся только в первом фрагменте (в частности, порт отправителя, порт получателя, тип ICMP, код ICMP, TCP флаг SYN). Если пользовательский компьютер является единственным шлюзом, соединяющим локальную сеть с остальной коммуникационной сетью, можно указать ей дефрагментировать все проходящие через нее пакеты (надо собрать ядро с параметром CONFIG_IP_ALWAYS_DEFRAG).

Если компьютер не дефрагментирует транзитные пакеты, то, если правило содержит проверки информации, которая отсутствует во фрагменте, условие считается не выполненным, и правило не срабатывает. Таким образом, первый фрагмент обработается как любой нефрагментированный пакет, а все остальные фрагменты - нет.

Например, если условие '-p TCP -s 192.168.1.1 unv' не сработает на втором и последующих фрагментах пакета, то также не сработает и обратное условие '-p TCP -s 192.168.1.1 ! unv' - поскольку во втором и последующих фрагментах вообще нет информации о номере порта.

Можно указывать правила для второго и последующих фрагментов с помощью флага '-f'. Очевидно, его нельзя применять вместе с номерами портов TCP/UDP, типом и кодом ICMP, и TCP SYN флагом, поскольку эта информация во втором и последующих фрагментах отсутствует. Можно также указать, что правило не применяется ко второму и последующим фрагментам, указав '!' перед '-f'.

Некорректно сформированные пакеты (TCP, UDP, ICMP до того короткие, что из них нельзя извлечь информацию о номерах портов или коде и типе ICMP) также считаются фрагментами и обрабатываются по правилам для фрагментов.

Следующий пример уничтожает фрагменты, адресованные на 192.168.1.1:

ipchains -A input -f -d 192.168.1.1 -j DENY

4.2.Действия с правилами, которые можно задавать в правилах.

4.2.1. Основное действие с пакетом, если он соответствует условию правила, задается с помощью параметра '-j' (jump to).

Существует шесть специальных действий:

ACCEPT - принять пакет;

DENY - уничтожить;

REJECT - отвергнуть, т.е. уничтожить и послать квитанцию отправителю в виде ICMP-пакета, если, конечно, отвергаемый пакет сам не был ICMP;

MASQ - замаскарадить пакет - допустимо только в пересылочном наборе правил и только если ядро было скомпилировано с поддержкой маскарадинга;

REDIRECT - переадресовать пакет на определенный порт локального компьютера, независимо от того, куда он был отправлен (прозрачное проксирование). Допустимо только во входном наборе правил. Номер порта указывается после ключевого слова REDIRECT;

RETURN - вызывает прекращение дальнейших проверок в наборе правил и применение к пакету политики набора правил.

Любое другое действие означает переход к набору правил, определенным администратором. Пакет начинает проверяться по правилам в указанном наборе правил. Если ни одно из них не выполнено, то продолжается проверка по правилам в текущем наборе правил. Если действие правила не указано, то даже при соответствии пакета его условиям продолжается проверка следующих правил в наборе правил. Такие правила называются учетными (accounting) и используются для учета трафика. Например, чтобы считать трафик от 192.168.1.1, можно использовать правило:

ipchains -A input -s 192.168.1.1 и проверять трафик командой ipchains -L -v

Флагом '-l' (log) можно указать, что пакет следует записать в системный журнал. Обычно это применяется для регистрации возможных атак или при отладке сетевых настроек. Не следует злоупотреблять регистрацией в системном журнале, а то он начнет быстро переполняться. Изменение типа обслуживания (TOS, Type Of Service) задается параметром '-t'. В заголовке IP-пакета есть 4 специальных редко используемых битовых флага, которые могут влиять (а могут и не влиять) на обслуживание пакета некоторыми маршрутизаторами:

Minimum Delay - минимальная задержка

Maximum Troughput - максимальная пропускная способность

Maximum Reliability - максимальная надежность

Minimum Cost - минимальная цена

Возможна установка только одного из этих флагов. Наиболее часто они применяются так: для telnet и управляющего соединения ftp устанавливается флаг Minimum Delay, а для данных ftp - Maximum Throughput. Это делается следующими командами:

ipchains -A output -p tcp -d 0.0.0.0/0 telnet -t 0x01 0x10

ipchains -A output -p tcp -d 0.0.0.0/0 ftp -t 0x01 0x10

ipchains -A output -p tcp -s 0.0.0.0/0 ftp-data -t 0x01 0x08

Флаг '-t' имеет 2 шестнадцатеричных параметра, которые применяются так: новыйTOS = (старыйTOS AND первый параметр) XOR второй параметр.

Для простоты приводится таблица 2 со значениями параметров:

Таблица 2

Название типа обслуживания	Значения параметров	Типичное применение
Minimum Delay	0x01 0x10	ftp, telnet
Maximum Throughput	0x01 0x08	ftp-data
Maximum Reliability	0x01 0x04	snmp
Minimum Cost	0x01 0x02	nntp

4.2.2. Ручная проверка работы фильтра пакетов.

Для проверки того, как будет работать фильтр на некотором пакете, используется команда '-C' (check). Параметры этого фиктивного пакета задаются точно так же, как и в правилах: '-p' для протокола, '-s' для адреса отправителя, '-d' для адреса получателя, '-i' для интерфейса. Если используется протокол TCP или UDP, то в адресах отправителя и получателя должен быть указан порт, а для ICMP - код и тип ICMP, кроме случая, когда проверяется не первый фрагмент пакета ('-f') - там этой информации быть не должно. Для протокола TCP и в отсутствие флага '-f' (т.е. проверяемый пакет не является фрагментом) можно указать флаг '-y' для имитации SYN-пакета. Пример: проверяем по входному набору правил TCP SYN-пакет от 192.168.1.1 порт 60000 на 192.168.1.2 порт unv, пришедший через интерфейс eth0, (типичный запрос на установку www-соединения):

ipchains -C input -p tcp -y -i eth0 -s 192.168.1.1 60000 -d 192.168.1.2 unv

В ответ на эту команду ipchains сообщит судьбу пакета, например 'Packet accepted'.

4.2.3. Пример настройки фильтра пакетов.

Если необходимо чтобы локальные процессы не соединялись с адресами 195.46.160.46 и 212.24.32.76 необходимо:

ipchains -A output -d 195.46.160.46 -j REJECT

ipchains -A output -d 212.24.32.76 -j REJECT

Устанавливаются приоритеты для исходящих пакетов (для входящих этого делать нет смысла). Поскольку этих правил довольно много, можно выделить их в отдельный набор правил по имени ppp-out:

ipchains -N ppp-out

ipchains -A output -i ppp0 -j ppp-out

Минимальная задержка для www-трафика и telnet'a:

ipchains -A ppp-out -p TCP -d proxy.virtual.net 8080 -t 0x01 0x10

ipchains -A ppp-out -p TCP -d 0.0.0.0/0 telnet -t 0x01 0x10

Низкая стоимость для данных ftp, nntp, pop3:

ipchains -A ppp-out -p TCP -d 0.0.0.0/0 ftp-data -t 0x01 0x02

ipchains -A ppp-out -p TCP -d 0.0.0.0/0 nntp -t 0x01 0x02

ipchains -A ppp-out -p TCP -d 0.0.0.0/0 pop-3 -t 0x01 0x02

Существуют некоторые ограничения на пакеты, приходящие по интерфейсу ppp0, выделим их в отдельный набор правил по имени ppp-in:

ipchains -N ppp-in

ipchains -A input -i ppp0 -j ppp-in

Никакие пакеты, приходящие из ppp0 не должны притворяться, что они с адресов 192.168.1.*, т.е. из локальной сети. Если же таковые появятся, то их надо занести в журнал ('-l') и уничтожить:

ipchains -A ppp-in -s 192.168.1.0/24 -l -j DENY

Разрешим UDP-пакеты для DNS (поскольку работает кэширующий DNS-сервер, который пересылает все запросы на 203.29.16.1, то и ответов следует ожидать только оттуда), а также входящие ftp-пакеты и ответные ftp-data (которые должны быть с портов выше 1023, но не с портов X11 в районе 6000):

ipchains -A ppp-in -p UDP -s 203.29.16.1 -d $LOCALIP dns -j ACCEPT

ipchains -A ppp-in -p TCP -s 0.0.0.0/0 ftp-data -d $LOCALIP 1024:5999 -j ACCEPT

ipchains -A ppp-in -p TCP -s 0.0.0.0/0 ftp-data -d $LOCALIP 6010: -j ACCEPT

ipchains -A ppp-in -p TCP -d $LOCALIP ftp -j ACCEPT

Ну и, наконец, все локальные пакеты на этот же компьютер вполне допустимы:

ipchains -A input -i lo -j ACCEPT

Политика по умолчанию для входного набора правил - DENY, то есть все остальное уничтожается:

ipchains -P input DENY

Примечание: правила не обязательно добавлять именно в таком порядке, поскольку пока вы их добавляете, некоторые нежелательные пакеты могут проскочить через фильтр. С точки зрения безопасности наиболее правильно сначала установить политику DENY для входного набора правил, а потом добавлять новые правила. Однако, если добавляемые правила потребуют разрешения символических имен с помощью DNS, у вас могут возникнуть неприятности.

4.2.4. Изменение нескольких правил одной командой

Иногда одна команда может воздействовать сразу на несколько правил. Это может происходить по двум причинам.

Во-первых, если указывается символический адрес компьютера, а его разрешение через DNS дает несколько различных IP-адресов, то ipchains будет действовать так, как если бы было введено несколько команд со всеми возможными сочетаниями IP-адресов. Например, если unv.foo.com разрешается в 3 адреса, а unv.bar.com - в 2 адреса, и введена команда ipchains -A input -j reject -S unv.bar.com -d unv.foo.com то к входному набору правил добавится 6 правил. Во-вторых, ipchains может выполнить несколько действий, если указан флаг '-b' (bidirectional). При этом ipchains будет действовать так, как если бы была введена команда дважды, во втором случае поменяв местами параметры '-s' и '-d'.

Например, чтобы запретить пересылку пакетов от и к 192.168.1.1, можно воспользоваться командой:

ipchains -b -A forward -j REJECT -s 192.168.1.1

4.3. Выполнение работы.

4.3.1. Для проверки результата, полученного входе выполнения работы, как минимум два компьютера должны быть подключены в сеть.

4.3.2. Выполнить загрузку ОС МСВС 3.0 (например с ip адресом 192.168.25.10 и маской 255.255.255.0).

4.3.3. Запустить консоль из панели управления. Прописать в строке

[root@localhost/root]# ***mc*****. Появится два окна (Midnight Commander).**

4.3.4. Настройка межсетевого экрана .

Установить 1 в файле ip-forward:

echo 1>/proc/sys/net/ipv4/**ip-forward**

можно прописать эту команду в /etc/rc.d/init.d/function

- Запустить команду **ping 192.168.25.8**, ответ должен быть положительным.
- На компьютере приёмнике с IP- адресом 192.168.25.8(или любого другого компьютера сети) запустить команду **ping 192.168.25.10**, ответ должен быть положительным.

4.3.5. Уничтожение пакетов переданных с IP-адреса 192.168.25.10 на IP- адрес 192.168.25.8.

[root@localhost/root]# ipchains -A input –s 192.168.25.10 –d 192.168.25.8 -j DENY

***192.168.25.10 – источник
***192.168.25.8 – приемник

- Запустить команду **ping 192.168.25.8**, ответ должен быть отрцательным.
- На компьютере приёмнике с IP- адресом 192.168.25.8 запустить команду **ping 192.168.25.10**, ответ должен быть отрицательным.

4.3.6. Запрет в пересылке пакетов от одного компьютера (например, arm- 8 с IP- адресом 192.168.25.8) к arm- 10 (с IP- адресом 192.168.25.10).

[root@localhost/root]# ipchains -b -A input –j REJECT -s 192.168.25.10 -d 192.168.25.8

-Запустить команду **ping 192.168.25.8**, ответ должен быть отрицательным.
- Запустить команду **ping 192.168.25.9**, ответ должен быть положительным.
- На компьютере приёмнике с IP- адресом 192.168.25.8 запустить команду **ping 192.168.25.10**, ответ должен быть отрицательным.
- На компьютере приёмнике с IP- адресом 192.168.25.9 запустить команду **ping 192.168.25.10**, ответ должен быть положительным.
(Если добавить маску, например **[root@localhost/root]# ipchains -b -A input –j REJECT -s 192.168.25.10/255.255.255.0 -d 192.168.25.8** то мы видим, что отправка и приём пакетов запрещены всем станциям). При выполнение команды ping с удалённых ПЭВМ выдаётся сообщение, что заданный порт не доступен.

4.3.7. Настройка межсетевого экрана через графический интерфейс ОС МСВС.

Для того чтобы настроить межсетевой экран, необходимо на панели управления вызвать <***К>,*** <***Система***>,<***Настройка сети***>,<***Настройка firewall***>. По умолчанию в окне МЭ никаких правил нет.

- Запустить команду **ping 192.168.25.8**, ответ должен быть положительным.
- На компьютере приёмнике с IP- адресом 192.168.25.8 (или любого другого компьютера сети) запустить команду **ping 192.168.25.10**, ответ должен быть положительным.

4.3.8. Уничтожение пакетов переданных с IP-адреса 192.168.25.10 на IP- адрес 192.168.25.8.

Нажать кнопку <***Добавить***>, появится окно настройки, выбрать необходимую цепочку нажав на кнопку <***Цепочка***>**.** Выбрать ***<Input>* .**
В окне адрес источника написать адрес компьютера с ОС МСВС - 192.168.25.10 .
В окне адрес приёмника написать адрес компьютера (например arm- 8 – 192.168.25.8) .
В окне <***Действие***> выбрать “уничтожить” (**DENY**).
Для вступления изменений в силу нажать кнопку <***Есть***>.
Мы видим, что в окне <***Настройка firewall***> появилось новое правило.

- Запустить команду **ping 192.168.25.8**, ответ должен быть отрцательным.
- На компьютере приёмнике с IP- адресом 192.168.25.8 запустить команду **ping 192.168.25.10**, ответ должен быть отрицательным.

4.3.9. Запрет в пересылке пакетов от одного компьютера (например, arm- 8 с IP- адресом 192.168.25.8) к arm- 10 (с IP- адресом 192.168.25.10).

Нажать кнопку <***Добавить***>, появится окно настройки, выбрать необходимую цепочку нажав на кнопку <***Цепочка***>. Выбрать <***input>* .**

В окне адрес источника написать адрес компьютера с (например arm- 8 – 192.168.25.3) .

В окне адрес приёмника написать адрес компьютера ОС МСВС - 192.168.25.10 .

В окне <***Действие***> выбрать “запретить” (**REJECT**).
Для вступления изменений в силу нажать кнопку <***Есть***>.
Мы видим, что в окне <***Настройка firewall***> появилось новое правило.

-Запустить команду **ping 192.168.25.3**, ответ должен быть отрицательным.
- Запустить команду **ping 192.168.25.9**, ответ должен быть положительным.
- На компьютере приёмнике с IP- адресом 192.168.25.8 запустить команду **ping 192.168.25.10**, ответ должен быть отрицательным.
- На компьютере приёмнике с IP- адресом 192.168.25.9 запустить команду **ping 192.168.25.10**, ответ должен быть положительным.
(Если добавить маску, например, в IP – адресе источника **192.168.25.8/255.255.255.0 и соответственно приёмника 192.168.25.10** то мы видим, что отправка и приём пакетов запрещены всем станциям). При выполнение команды ping с удалённых ПЭВМ выдаётся сообщение, что заданный порт не доступен.

4.4. Дополнительное задание:

Создать скрипт, выполняющий автоматическую смену **1** на **0** в файле ip-forward **(**/proc/sys/net/ipv4/ip-forward**),** каждый раз при загрузке ОС МСВС, для работы фильтра пакетов.

5.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
- Знать назначение межсетевого экрана, основные определения и понятия.
- Уметь включать фильтр пакетов.
- Уметь формировать правила фильтрации.
- Знать действия с правилами, которые можно задавать в правилах.

– 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.

6.Заключительная часть

Товарищи курсанты, на сегодняшнем занятии вы практически отработали вопросы, связанные с настройкой МЭ и формированием правил фильтрации пакетов МЭ.

На занятии активно и правильно выполняли задания курсанты:___им выставлены оценки.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Во вступительной части преподавателю объявить тему занятия, его цели, учебные вопросы, порядок его проведения, отметить практическую значимость МЭ, используемую литературу.

Проверку готовности слушателей к занятию осуществить проверкой наличия у них рабочих тетрадей, а также постановкой контрольных вопросов по знанию материала предыдущего группового занятия.

Отработку учебных вопросов осуществлять путем выполнения заданий, выдаваемых всей группе.

При отработке первого вопроса основное внимание обратить на приобретение слушателями практических навыков составления правил фильтрации пакетов межсетевым экраном. Показать на конкретных примерах.

При отработке второго вопроса прививать практические навыки в самостоятельной работе по настройке межсетевого экрана для МСВС 3.0

В заключительной части занятия оценить работу учебной группы в целом, подвести итоги занятия, выставить оценки слушателям, ответить на возникшие вопросы. Сформулировать задание на самоподготовку и объявить тему следующего занятия.

Задание и методические указания курсантам на самостоятельную подготовку

1. Повторить материалы лекции «Комплексное обеспечение информационной безопасности АС».
2. Продолжить работу над курсовым проектированием и быть готовым доложить полученные результаты.

IV. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

Доцент 27 кафедры
к.т.н.
подполковник

С. Краснов

«___»_____20__г.