Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики»

(СибГУТИ)

Кафедра ИКСС

Контрольная работа

по дисциплине: «Операционные системы»

Вариант 19

Выполнил: студент

группы *NN*

*ФИО*

Проверил:

*ФИО*

**Теория:**

**Межсетевой экран** (МЭ, брандмауэр или Firewall) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение. В фильтрации трафика брандмауэр опирается на установленные параметры — чаще всего их называют правилами МЭ. Современные межсетевые экраны располагаются на периферии сети, ограничивают транзит трафика, установку нежелательных соединений и подобные действия за счет средств фильтрации и аутентификации.

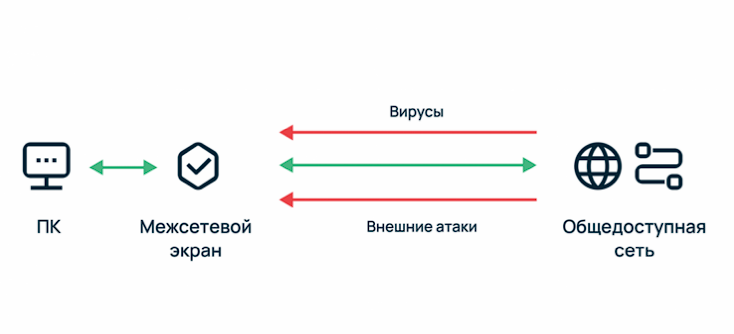


Рис.1 - Пример работы межсетевого экрана.

**Главная задача МЭ** – это фильтрация трафика между зонами сети. Он может использоваться для разграничения прав доступа в сеть, защиты от сканирования сети компании, проведения сетевых атак. Проще говоря, межсетевой экран – это одно из устройств, при помощи которого обеспечивается сетевая безопасность компании.

**Функции межсетевого экрана**

Брандмауэр может:

1. Остановить подмену трафика. Представим, что ваша компания обменивается данными с одним их своих подразделений, при этом ваши IP-адреса известны. Злоумышленник может попытаться замаскировать свой трафик под данные офиса, но отправить его с другого IP. Брандмауэр обнаружит подмену и не даст ему попасть внутрь вашей сети.
2. Защитить корпоративную сеть от DDoS-атак. То есть ситуаций, когда злоумышленники пытаются вывести из строя ресурсы компании, отправляя им множество запросов с зараженных устройств. Если система умеет распознавать такие атаки, она формирует определенную закономерность и передает ее брандмауэру для дальнейшей фильтрации злонамеренного трафика.
3. Заблокировать передачу данных на неизвестный IP-адрес. Допустим, сотрудник фирмы скачал вредоносный файл и заразил свой компьютер, что привело к утечке корпоративной информации. При попытке вируса передать информацию на неизвестный IP-адрес брандмауэр автоматически остановит это.

**Типы межсетевых экранов**

МЭ делятся на два основных типа: аппаратные и программные.

1. Аппаратный межсетевой экран

Аппаратный МЭ – это, как правило, специальное оборудование, составляющие которого (процессоры, платы и т. п.) спроектированы специально для обработки трафика.

Работает они на специальном ПО — это необходимо для увеличения производительности оборудования. Примерами аппаратного межсетевого экрана выступают такие устройства, как Cisco ASA, FortiGate, Cisco FirePower, UserGate и другие.

Аппаратные МЭ более мощные по сравнению с программными, однако это влияет на стоимость решений. Нередко она в разы выше, чем у программных аналогов.

1. Программный межсетевой экран

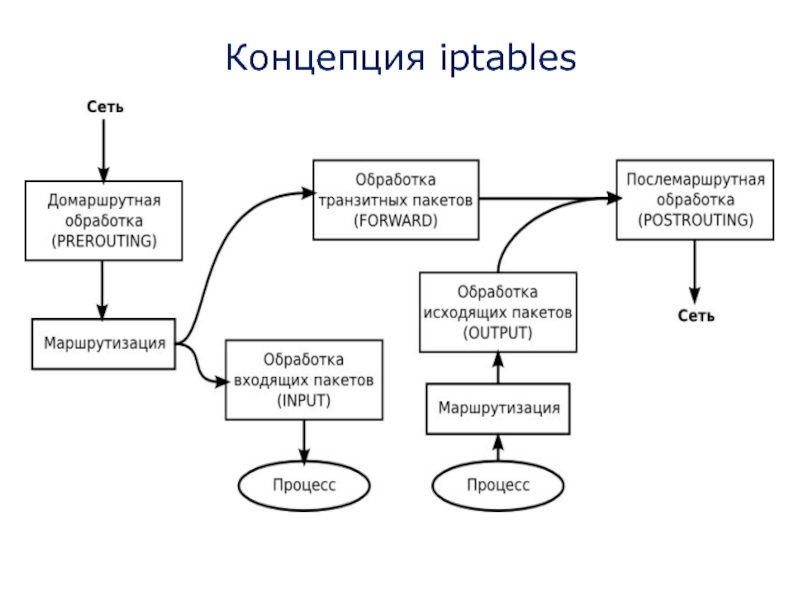
Программный МЭ – это программное обеспечение, которое устанавливается на устройствах, реальное или виртуальное.

Через такой межсетевой экран перенаправляется весь трафик внутрь рабочей сети. К программным относятся брандмауэр в Windows и iptables в Linux.

Программные МЭ, как правило, дешевле и могут устанавливаться не только на границах сети, но и на рабочих станциях пользователей. Из основных недостатков — более низкая пропускная способность и сложность настройки в ряде случаев.

**Концепция iptables**

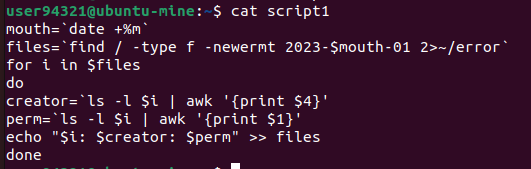
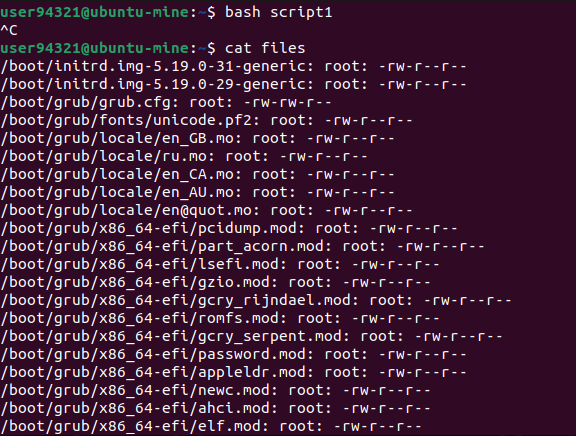
Iptables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter для ядер Linux. Она позволяет управлять входящими и исходящими сетевыми пакетами, применяя правила к их фильтрации. Это может включать в себя блокировку определенных портов, разрешение доступа только для определенных IP-адресов или различные другие ограничения для управления доступом к сети. В общем, iptables является мощным инструментом для управления сетевыми пакетами и защиты системы от внешних угроз.

  
Рис.1 – Концепция iptables.

**Источники**

1. *Selectel «Межсетевой экран: что такое и как работает – Блог компании Селектел»* [электронный ресурс] // <https://selectel.ru/blog/firewall/>
2. *K-max «Как работает iptables в Linux | Блог любителя экспериментов»* [электронный ресурс] // <https://www.k-max.name/linux/netfilter-iptables-v-linux/>
3. *Wikipedia «Iptables»* [электронный ресурс] // <https://ru.wikipedia.org/wiki/Iptables>

Задание 1.

mouth=`date +%m` # из команды date берётся числовое значение текущего месяца

files=`find / -type f -newermt 2023-$mouth-01 2>~/error` # поиск всех файлов, созданных с начала текущего месяца (-newermt)

for i in $files # цикл по файлам

do

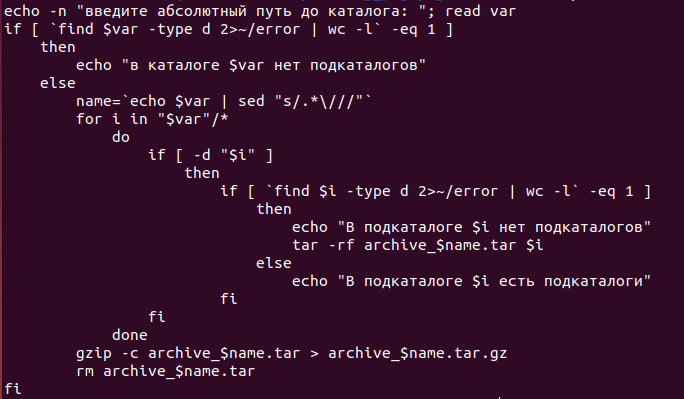
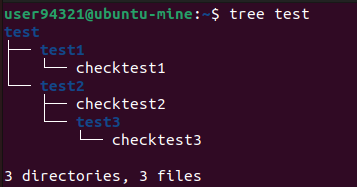
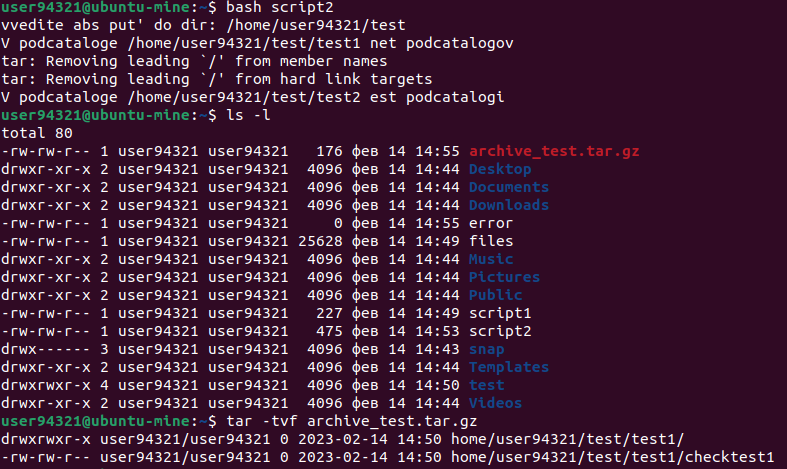
creator=`ls -l $i | awk '{print $4}'` # имя создателя из 4 столбца вывода команды ls -l

perm=`ls -l $i | awk '{print $1}' # права из 1 столбца вывода команды ls -l

echo "$i: $creator: $perm" >> files # вывод названия\_файла: имя\_создателя : права в файл files

done

Задание 2.

echo -n "введите абсолютный путь до каталога: "; read var # вводится абсолютный путь до каталога

if [ `find $var -type d 2>~/error | wc -l` -eq 1 ] # если (вывод из команды find содержимого введённого каталога равен 1(нет подкаталогов ключ -d)

then # то

echo "в каталоге $var нет подкаталогов"

else # иначе

name=`echo $var | sed "s/.\*\///"` # абсолютный путь форматируется, чтобы убрать все символы до названия каталога (относительный путь), про sed - ищет совпадения с регулярным выражением .\*/, которое означает "любые символы, повторенные любое количество раз, за которыми следует слэш", и заменяет его на пустую строку, т.е. удаляет их.

for i in "$var"/\* # цикл по содержимому введённого каталога

do

if [ -d "$i" ] # если содержимое каталог

then

if [ `find $i -type d 2>~/error | wc -l` -eq 1 ] # если в этом подкаталоге нет подкаталогов

then

echo "В подкаталоге $i нет подкаталогов"

tar -rf archive\_$name.tar $i # в архив с названием изначального каталога добавляется (ключ -r) этот подкаталог

else # иначе

echo "В подкаталоге $i есть подкаталоги"

fi

fi

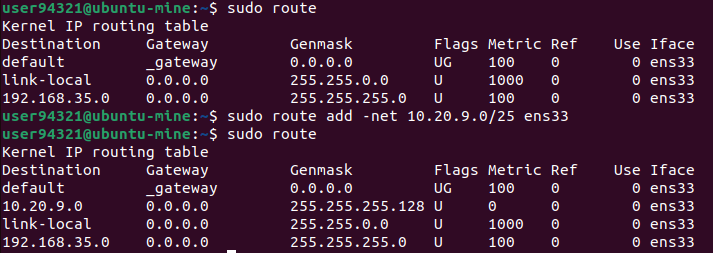
done

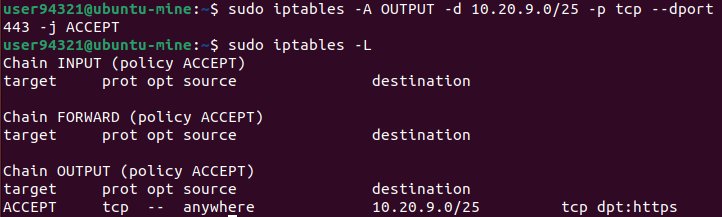
gzip -c archive\_$name.tar > archive\_$name.tar.gz # полученный каталог сжимается с помощью сжатия gz

rm archive\_$name.tar # изначальный каталог удаляется

fi

Задание 3.

* 1. route add -net 10.20.9.0/25 ens33
  2. Изображение выглядит как текст

     Автоматически созданное описание  
       
     output – исходящие (-d) с хостов к которым настроена маршрутизация в пункте 3.1, протокол tcp (-p tcp) –dport (порт назначения 443) -j ACCEPT (если правило подошло разрешить)