

Оглавление

Тема и цель работы	3
Оборудование, ПО	3
Ход лабораторной работы	4
Вывод.....	7
Контрольные вопросы	7

Тема и цель работы

Тема лабораторной работы: «Организация доступа в сеть интернет через NAT

Цель работы: Научиться устанавливать, проводить базовые настройки и проверять работоспособность NAT.

Вариант №25

Оборудование, ПО

Таблица 1 - Оборудование, ПО

Устройство	Операционная система	IP адрес/Маска	Шлюз	DNS
CLI_A1	Astra Linux SE 1.8.x	10.0.25.10/24	-	au- 1.au.team.lab
CLI_A2	Astra Linux SE 1.8.x	10.0.25.20/24	-	au- 2.au.team.lab
CLI_A3	Astra Linux SE 1.8.x	10.0.25.30/24	-	au- 3.au.team.lab

Ход лабораторной работы

- ## 1. Установить и настроить брандмауэр firewalld для настройки

Для установки `firewalld` необходимо установить командой данный пакет командой **`apt-get install firewalld`** (см. рис. 1).

```
root@usoltsev:/home/astra# apt-get install firewallld
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не т
  libgdk-pixbuf-xlib-2.0-0 libgdk-pixbuf2.0-0 python-cairo
  python-pkg-resources
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  gir1.2-nm-1.0 ipset libcap-ng0 libipset13 python3-attr pyt
```

Рисунок 1 – установка пакета

2. Проверить текущие активные зоны с помощью команды **firewall-**

cmd -get-active-zones и установить типы интерфейсов на внутренние (trusted) и внешние (external) командами:

```
firewall-cmd --zone=external --add-interface=enp0s8 --
permanent
```

```
firewall-cmd --zone=trusted --add-interface=enp0s3 --
permanent
```

(см. рис. 2)

```
root@usoltsev:/home/astra# firewall-cmd --zone=external --add-interface=enp0s8 --permanent
success
root@usoltsev:/home/astra# firewall-cmd --get-active-zones
public
    interfaces: enp0s3
root@usoltsev:/home/astra# firewall-cmd --zone=trusted --add-interface=enp0s3 --permanent
The interface is under control of NetworkManager, setting zone to 'trusted'.
success
root@usoltsev:/home/astra#
```

Рисунок 2 – проверка активных зон и настройка интерфейсов

- ### 3. Проверить правильность настройки интерфейсов.

Ввести команду **systemctl restart firewalld** для перезагрузки службы брандмауэра и команду **firewall-cmd --get-active-zones** (см. рис. 3).

```

root@usoltsev:/home/astra# systemctl restart firewalld
root@usoltsev:/home/astra# firewall-cmd --get-active-zones
external
    interfaces: enp0s8
trusted
    interfaces: enp0s3
root@usoltsev:/home/astra#

```

Рисунок 3 – перезагрузка службы и проверка настроек

4. Изменить настройки файла **/etc/sysctl.conf** (см. рис. 4).

```

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

#Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

```

Рисунок 4 – настройка файла /etc/sysctl.conf

Внести изменения без перезагрузки устройства можно командой **sysctl -p** (см. рис. 5).

```

root@usoltsev:/# vim /etc/sysctl.conf
root@usoltsev:/# sysctl -p
net.ipv4.ip_forward = 1
root@usoltsev:/#

```

Рисунок 5 – вывод команды

Проверить доступ в Интернет на второй машине командой **ping 8.8.8.8**

```

root@usoltsev-2:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=105 time=17.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=17.1 ms

```

Рисунок 6 – доступ в Интернет присутствует

Аналогично с третьей машиной (см. рис. 7).

```
root@usoltsev-3:/# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=105 time=19.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=19.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=19.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=105 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=105 time=19.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=105 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=105 time=19.2 ms
```

Рисунок 7 – доступ в Интернет присутствует

Вывод

В процессе настройки брандмауэра `firewalld` была выполнена установка пакета и настройка интерфейсов для различных зон безопасности. С помощью команд **`firewall-cmd`** были определены внешние и внутренние интерфейсы, что позволяет управлять доступом к сети. После перезагрузки службы `firewalld` была проверена корректность настроек активных зон. Также были внесены изменения в файл конфигурации `/etc/sysctl.conf` для оптимизации сетевых параметров. Проверка доступа в Интернет на нескольких машинах с помощью команды **`ping`** подтвердила успешное подключение. В целом, процесс настройки `firewalld` обеспечил надежную защиту и корректное функционирование сетевых интерфейсов.

Контрольные вопросы

1. Что такое NAT?

NAT (Network Address Translation) — это метод, используемый для преобразования IP-адресов в пакетах данных, проходящих через маршрутизатор или брандмауэр. Он позволяет нескольким устройствам в частной сети использовать один внешний IP-адрес для доступа в Интернет, что помогает экономить адресное пространство и повышает безопасность.

2. Что такое `firewalld`?

`Firewalld` — это динамическая система управления брандмауэром для Linux, которая предоставляет интерфейс для настройки правил фильтрации трафика. Она использует концепцию зон для управления доступом и позволяет администратору легко изменять правила без необходимости перезагрузки службы.

3. Что такое статический NAT?

Статический NAT представляет собой тип NAT, при котором один внутренний IP-адрес всегда сопоставляется с одним внешним IP-адресом. Это позволяет устройствам внутри частной сети иметь постоянный адрес в

Интернете, что полезно для серверов и других ресурсов, требующих стабильного доступа.

4. Что такое динамический NAT?

Динамический NAT — это метод, при котором внутренние IP-адреса сопоставляются с пулом внешних IP-адресов на временной основе. Когда устройство из внутренней сети инициирует соединение с Интернетом, оно получает временный внешний адрес, который освобождается после завершения сессии, что позволяет более эффективно использовать доступные IP-адреса.