

Администрирование сетевых подсистем

Расширенные настройки межсетевого экрана (Лабораторная работа №7)

Суннатилло Махмудов

4 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Получить навыки настройки межсетевого экрана **firewalld** в Linux:
перенаправление портов, настройка маскарadingа и создание пользовательских служб.

1. Создать пользовательскую службу **ssh-custom** на основе стандартной SSH.
2. Настроить переадресацию порта **2022 → 22**.
3. Активировать **маскарадинг (Masquerading)**.
4. Проверить доступность подключения и выхода в Интернет.
5. Подготовить конфигурацию для автоматического развертывания через Vagrant.

Теоретическая часть

- **firewalld** — динамически управляемый брандмауэр Linux.
- Работает с понятиями:
 - **Зона** — уровень доверия к сети.
 - **Служба** — набор правил доступа по портам и протоколам.
- Конфигурационные файлы:
 - `/usr/lib/firewalld/services/` — системные службы.
 - `/etc/firewalld/services/` — пользовательские службы.

- **Port Forwarding** — перенаправление сетевых пакетов с одного порта на другой.
- **Masquerading** — подмена исходного IP-адреса при выходе во внешнюю сеть (частный случай NAT).
- **Преимущества firewalld:**
 - изменение правил без перезапуска;
 - централизованное управление зонами;
 - поддержка IPv4 и IPv6.

Ход выполнения лабораторной работы


```
[snahmudov@server.snahmudov.net ~]$ sudo -i
[sudo] password for snahmudov:
[root@server.snahmudov.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.snahmudov.net ~]# cd /etc/firewalld/services/
[root@server.snahmudov.net services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.snahmudov.net services]#
```

Рис. 1: Создание пользовательского файла службы

```
[root@server.smahmudov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.smahmudov.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.smahmudov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.smahmudov.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.smahmudov.net services]# firewall-cmd --reload
success
[root@server.smahmudov.net services]#
[root@server.smahmudov.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
success
[root@server.smahmudov.net services]#
```

Рис. 2: Появление службы ssh-custom после перезагрузки правил

Перенаправление портов



```
smahmudov@server:~ – ssh -p 2022 smahmudov@server.smah...  
[smahmudov@client.smahmudov.net ~]$ ssh -p 2022 smahmudov@server.smahmudov.net  
The authenticity of host '[server.smahmudov.net]:2022 ([192.168.1.1]:2022)' can't  
be established.  
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[server.smahmudov.net]:2022' (ED25519) to the list o  
f known hosts.  
smahmudov@server.smahmudov.net's password:  
Web console: https://server.smahmudov.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Mon Sep 29 09:45:50 2025  
[smahmudov@server.smahmudov.net ~]$
```

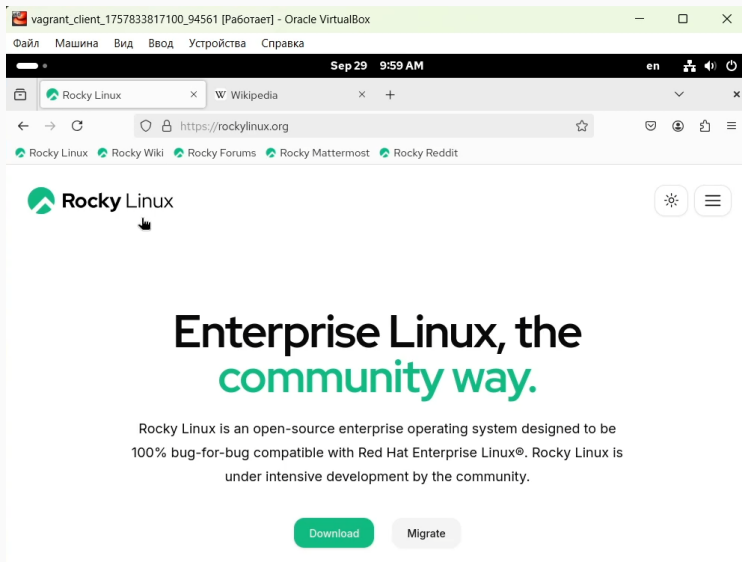
Рис. 3: Подключение по SSH через перенаправленный порт

Настройка Masquerading

```
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server.smahmudov.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.smahmudov.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.smahmudov.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.smahmudov.net services]# firewall-cmd --reload
success
[root@server.smahmudov.net services]#
```

Рис. 4: Включение пересылки пакетов и маскардинга

Проверка выхода в Интернет



```
[root@server.smahmudov.net services]#  
[root@server.smahmudov.net services]# cd /vagrant/provision/server/  
[root@server.smahmudov.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services  
[root@server.smahmudov.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d  
[root@server.smahmudov.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/  
[root@server.smahmudov.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/  
[root@server.smahmudov.net server]# touch firewall.sh  
[root@server.smahmudov.net server]# chmod +x firewall.sh  
[root@server.smahmudov.net server]#
```

Рис. 6: Создание каталогов и скрипта firewall.sh для сохранения конфигурации

Вывод

В ходе лабораторной работы была освоена настройка **firewalld**:
создана пользовательская служба, реализовано перенаправление портов и маскардинг.
Результатом стало формирование безопасной сетевой конфигурации и автоматизация её
развертывания.