

Лабораторная работа №7

Расширенные настройки межсетевого экрана (FirewallD)

Элсаиед Адел

3 января 2026

Цели и ожидаемый результат

Цель работы

Получить навыки настройки межсетевого экрана в Linux: - переадресация (port forwarding); - маскарадинг (masquerading / NAT).

Выполнение работы

Создание пользовательской службы FirewallD (ssh-custom)

- скопирован файл `/usr/lib/firewalld/services/ssh.xml`;
- создан пользовательский файл `/etc/firewalld/services/ssh-custom.xml`;
- изучена структура XML-описания службы.

```
[root@server.elsaiedadel.net server]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.elsaiedadel.net server]# cd /etc/firewalld/services/
[root@server.elsaiedadel.net services]# cat 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.elsaiedadel.net services]#
```

Рис. 1: Просмотр содержимого ssh-custom.xml

Редактирование ssh-custom: порт и описание

Изменения в `/etc/firewalld/services/ssh-custom.xml`: - порт SSH изменён со стандартного 22 на 2022; - описание уточнено как пользовательская модификация.



The screenshot shows a text editor window with the title bar "ssh-custom.xml" and the path "/etc/firewalld/services". The editor has standard controls for "Open", "Save", and "New". The XML code is displayed in the main pane:

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <service>
3   <short>SSH</short>
4   <description>Secure Shell (SSH) custom</description>
5   <port protocol="tcp" port="2022"/>
6 </service>
```

Рис. 2: Редактирование порта и описания службы

Активация службы ssh-custom

Служба добавлена в правила FirewallD:

```
[root@server.elsaiedadel.net services]#  
[root@server.elsaiedadel.net services]# firewall-cmd --list-services  
cockpit dhcp dhcpcv6-client dns http https ssh  
[root@server.elsaiedadel.net services]# firewall-cmd --add-service=ssh-custom  
success  
[root@server.elsaiedadel.net services]# firewall-cmd --list-services  
cockpit dhcp dhcpcv6-client dns http https ssh ssh-custom  
[root@server.elsaiedadel.net services]# firewall-cmd --add-service=ssh-custom --permanent  
success  
[root@server.elsaiedadel.net services]# firewall-cmd --reload  
success  
[root@server.elsaiedadel.net services]#
```

Рис. 3: Добавление ssh-custom и перезагрузка FirewallD

Перенаправление портов 2022 → 22 на сервере

Настройка позволяет: - принимать подключения на внешнем порту 2022, - при этом обслуживать их локальной SSH-службой на 22.

```
[root@server.elsaiedadel.net services]#  
[root@server.elsaiedadel.net services]# firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22  
success  
[root@server.elsaiedadel.net services]#
```

Рис. 4: Настройка port forward 2022 -> 22

Проверка SSH-подключения с клиента

На **client** выполнено подключение по SSH к **server** через порт 2022.

```
[elsaiedadel@client.elsaiedadel.net ~]$ ssh -p 2022 elsaiedadel@server.elsaiedadel.net
The authenticity of host '[server.elsaiedadel.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.elsaiedadel.net]:2022' (ED25519) to the list of known hosts.
elsaiedadel@server.elsaiedadel.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Jan  3 08:19:09 2026
[elsaiedadel@server.elsaiedadel.net ~]$
logout
Connection to server.elsaiedadel.net closed.
[elsaiedadel@client.elsaiedadel.net ~]$ █
```

Рис. 5: Проверка SSH-подключения через порт 2022

Включение IPv4 forwarding + masquerading (NAT)

- создан /etc/sysctl.d/90-forward.conf с net.ipv4.ip_forward = 1;
- применены sysctl-настройки;
- включён masquerading (NAT) для зоны public;
- перезагружен FirewallD для применения конфигурации.

```
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.elsaiedadel.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.elsaiedadel.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.elsaiedadel.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.elsaiedadel.net services]# firewall-cmd --reload
success
[root@server.elsaiedadel.net services]#
```

Проверка выхода клиента в Интернет

На client проверен доступ во внешнюю сеть.

The screenshot shows a Firefox browser window with the following details:

- Title Bar:** rudn - Поиск в Google
- Address Bar:** https://www.google.com/search?client=firefox-b-e&channel=...
- Toolbar:** Back, Forward, Stop, Refresh, Home, Bookmarks, History, Downloads, Tabs.
- Page Header:** Rocky Linux, Rocky Wiki, Rocky Forums, Rocky Mattermost, Rocky Reddit.
- Search Bar:**rudn
- Search Results:**
 - Russian University of Friendship of Peoples**
https://www.rudn.ru
Russian University of Friendship of Peoples
 - RUDN University**
Admissions - Educational Programs - Education - Contacts
- Language Context Menu (highlighted in yellow):** Looking for results in English?
 - Change to English
 - Оставить русский
 - Изменить язык
- Page Footer:** 9/12

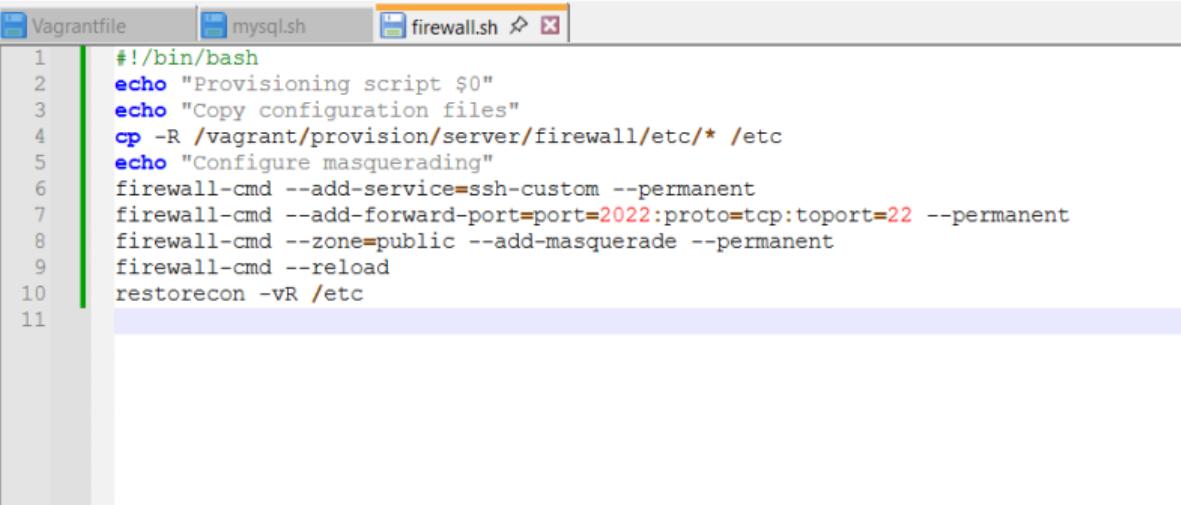
Подготовка файлов в provision-структуре

Для воспроизведимости окружения подготовлены файлы в
`/vagrant/provision/server/`: - `ssh-custom.xml` (служба FirewallD); -
`90-forward.conf` (sysctl-настройка forwarding).

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

Рис. 8: Подготовка каталогов и копирование конфигураций

Скрипт firewall.sh для автоматической настройки



```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc
echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
restorecon -vR /etc
```

Рис. 9: Содержимое скрипта firewall.sh

Итоги

Выводы по работе

В ходе лабораторной работы:

- создана пользовательская служба FirewallD для SSH с портом 2022;
- настроено перенаправление 2022 → 22 и подтверждено успешным SSH-подключением;
- включены IPv4 forwarding и masquerading для маршрутизации трафика клиента;
- подготовлена автоматизация через provisioning для повторяемого развёртывания.