

# Администрирование системных подсистем

## Настройка FirewallD, Port Forwarding и Masquerading

---

Сейдалиев Тагьетдин Ровшенович

26 ноября 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Получить практические навыки:

- создания пользовательских служб FirewallD;
- настройки перенаправления портов;
- включения masquerading;
- интеграции сетевых конфигураций в систему провижининга Vagrant.

## Создание пользовательской службы FirewallD

---

Создана копия стандартного файла `ssh.xml` → `ssh-custom.xml`.

Проанализирована структура XML-файла службы.

```
[root@server.trseidaliyev.net server]#  
[root@server.trseidaliyev.net server]#  
[root@server.trseidaliyev.net server]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml  
[root@server.trseidaliyev.net server]# cd /etc/firewalld/services/  
[root@server.trseidaliyev.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 provide  
s 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.trseidaliyev.net services]# █
```

Рис. 1: `ssh-custom.xml`

Изменён порт с 22 на 2022, обновлено описание службы.



```
ssh-custom.xml
/etc/firewalld/services

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

Рис. 2: Изменение порта

После reload служба появилась в списке доступных, но не активированных.

```
iver zabox-trapper zabox-web-service zero-k zerotier
[root@server.trseidaliev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.trseidaliev.net services]# firewall-cmd --add-service=ssh-custom
success
[root@server.trseidaliev.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.trseidaliev.net services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.trseidaliev.net services]# firewall-cmd --reload
success
[root@server.trseidaliev.net services]# █
```

Рис. 3: Добавление службы

`ssh-custom` добавлена в активные службы и сохранена в постоянной конфигурации.



## Перенаправление портов

---

Реализовано перенаправление порта 2022 на стандартный порт SSH.

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

Рис. 4: Forward-port

Успешное подключение по SSH через порт 2022.

```
[trseidaliev@client.trseidaliev.net ~]$ ssh -p 2022 trseidaliev@server.trseidaliev.net
The authenticity of host '[server.trseidaliev.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxmw0XTU.
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.trseidaliev.net]:2022' (ED25519) to the list of known hosts.
trseidaliev@server.trseidaliev.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Nov 26 16:46:11 2025
[trseidaliev@server.trseidaliev.net ~]$
[trseidaliev@server.trseidaliev.net ~]$
logout
Connection to server.trseidaliev.net closed.
[trseidaliev@client.trseidaliev.net ~]$
```

## Настройка forwarding и masquerading

---

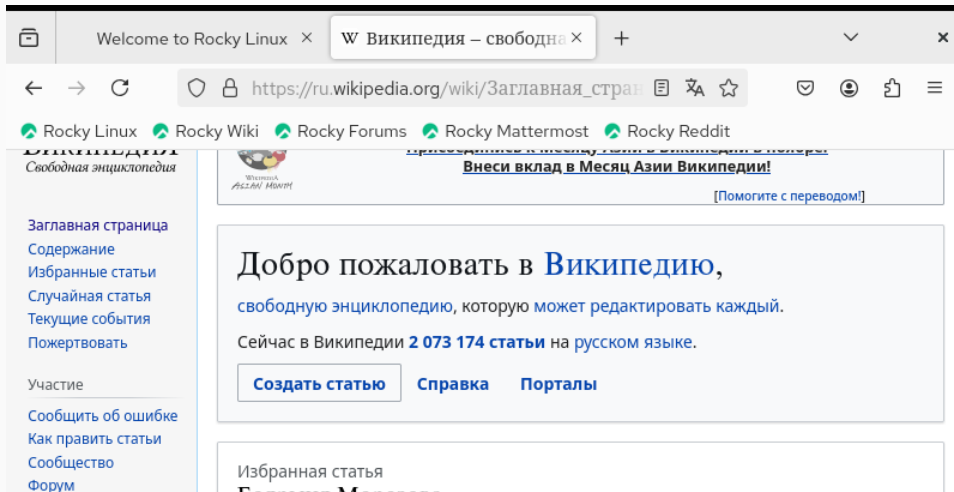
Включена поддержка перенаправления IPv4-пакетов через конфигурацию sysctl.

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

# Masquerading

В зоне **public** активирован masquerading.

После reload проверен доступ в Интернет с клиентской машины.



## Итоги работы

---

- создана пользовательская служба firewall с портом 2022;
- настроено перенаправление портов и masquerading;
- обеспечена корректная работа SSH через новый порт;
- выполнена интеграция сетевых правил в Vagrant-провижининг.