Лабораторная работа №13

Настройка пакетного фильтра (firewalld)

Тукаев Тимур

07 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Основная цель

Получить практический опыт настройки межсетевого экрана Linux с помощью инструментов **firewall-cmd** и **firewall-config**.

Ход выполнения

Определение зоны и доступных служб

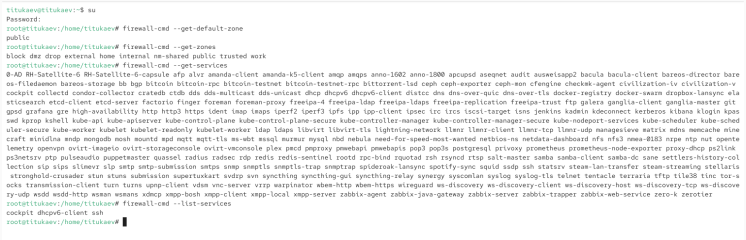

Рис. 1: Определение зоны и списка служб

Переход в режим суперпользователя и проверка активной зоны (`public`) и доступных служб/зон в системе.

Просмотр конфигурации зоны

```
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Добавление службы VNC (временное)

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# firewall-cmd --add-service=vnc-server
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev# systemctl restart firewalld.service
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Добавление службы VNC (постоянно)

```
root@titukaev:/home/titukaev# firewall-cmd --add-service=vnc-server  --permanent
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Добавление порта 2022/tcp

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# firewall-cmd --add-port=2022/tcp --permanent
success
root@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Рис. 5: Добавление порта TCP

Включение служб через GUI

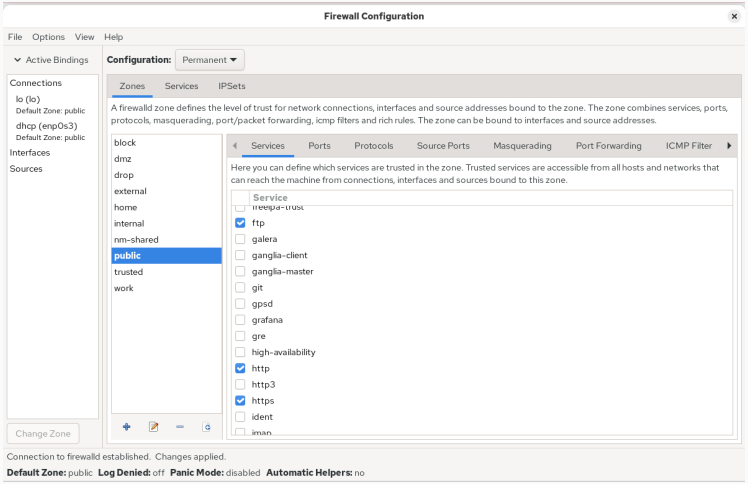

Рис. 6: Включение служб

Добавление порта через firewall-config

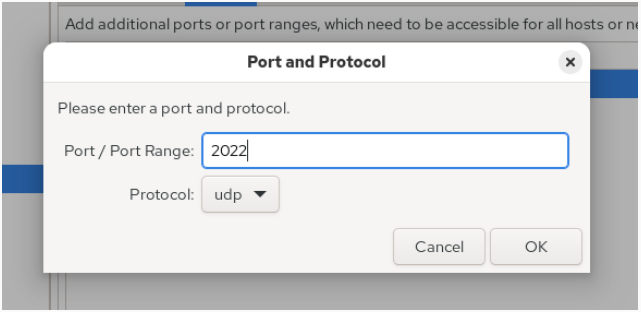

Рис. 7: Добавление порта UDP

Добавление порта 2022/udp через графический интерфейс.

Применение конфигурации GUI

```
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Настройка доступа к службам

```
root@titukaev:/home/titukaev# firewall-cmd --reload
success
root@titukaev:/home/titukaev# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https imap pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@titukaev:/home/titukaev#
```

Рис. 9: Конфигурация telnet, imap, pop3, smtp

- telnet — добавлен через терминал
- imap, pop3, smtp — добавлены через GUI

Итоги работы

Вывод

В ходе лабораторной работы освоены:

- настройка межсетевого экрана с помощью `firewall-cmd` и `firewall-config`;
- отличие runtime и permanent конфигураций;
- включение служб и открытие портов;
- управление зонами безопасности.

Полученные навыки позволяют управлять сетевым доступом и обеспечивать безопасность системы.