

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

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev# firewall-cmd --get-default-zone
public
root@titukaev:/home/titukaev# firewall-cmd --get-zones
block dmz drop external home internal m-shared public trusted work
root@titukaev:/home/titukaev# firewall-cmd --get-services
@AD RH-Satellite-6 RH-Satellite-6-capsule afp alvz amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage b2b bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lad ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-lv civilization-v cockpit collectd condor-collector cratedb ctdb dde dde-multicast ddns-unicast dhcp dhcpc6 dhcpcv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server Factorio Finger Foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpd grafana gretz high-availability http http3 https iotent imaps sponerf3 sponerf3_gpgs tpp tpp-client 1psync trc trc-iscsi-target tsns jenkins kademli kdeconnect kerberos kibana klogin kpas sed kprop kshell kube-apt kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-readonly kubelet kubelet-worker ldap libvirt libvirt-tls lightning-network l1anz l1anz-client llmnr-tcp llmnr-tcp 1lmmr manageviews matrix mdns memcache mine craft minidns mnode mongodb mosh mountd epiphany mgmt mgmt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ms netdata-dashboard nfcs nf3 nmap ntp nut opentelephony openvpn ovirt-imageio ovirt-storageconsole ovirt-vcosnsole plex pacd pmemproxy pmewebapi pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd zcp-blnd zoquodad zsh rsyncd rtsp salt-master samba samba-client samba-dc same settlers-history-collection sip sips slinevr sipp sntp smtp smtp-submission smtps snmp snmptrap snmptrap spiderOak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission superluxkart svdp svn syncthing syncthing-gui syncthing-relay synergy sysconlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-a ocks transmission-client turn turns upnp-client vdsm vnc-server vrzip warpinator abem-https abem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-https wdd wddi wwan wwanan xmpp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
root@titukaev:/home/titukaev# firewall-cmd --list-services
cockpit dhcpc6-client ssh
root@titukaev:/home/titukaev#
```

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 dhcpcv6-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 dhcpcv6-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# 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 dhcpcv6-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 dhcpcv6-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 dhcpcv6-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 dhcpcv6-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 dhcpcv6-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 службы через GUI

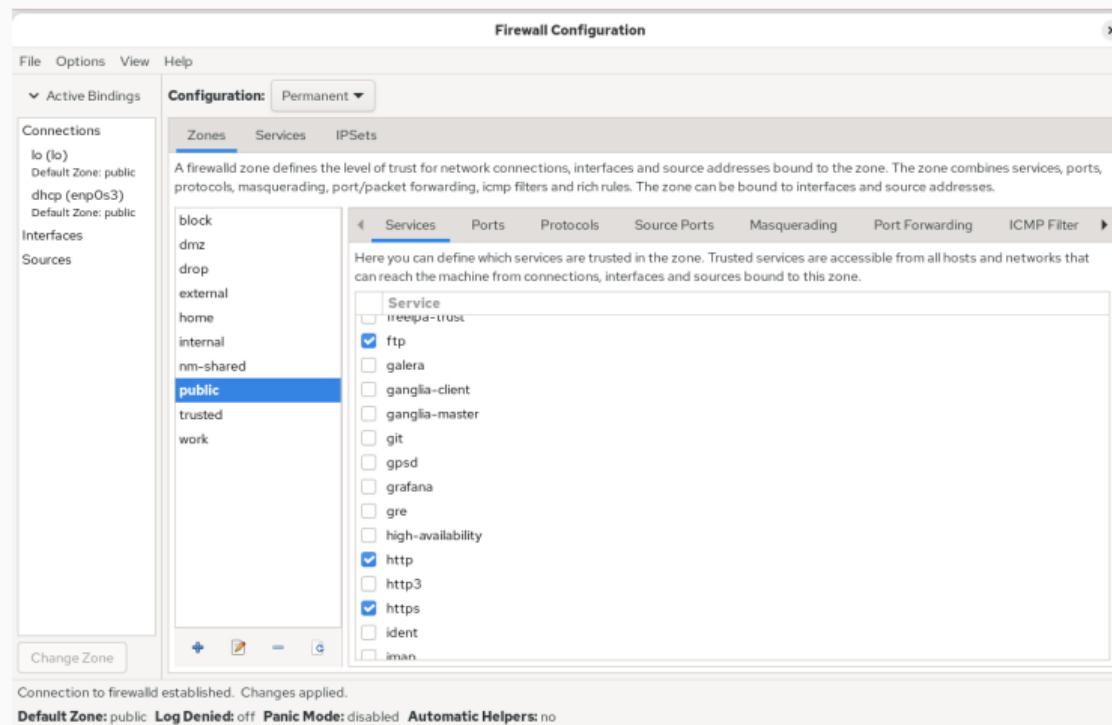


Рис. 6: Включение служб

Добавление порта через firewall-config

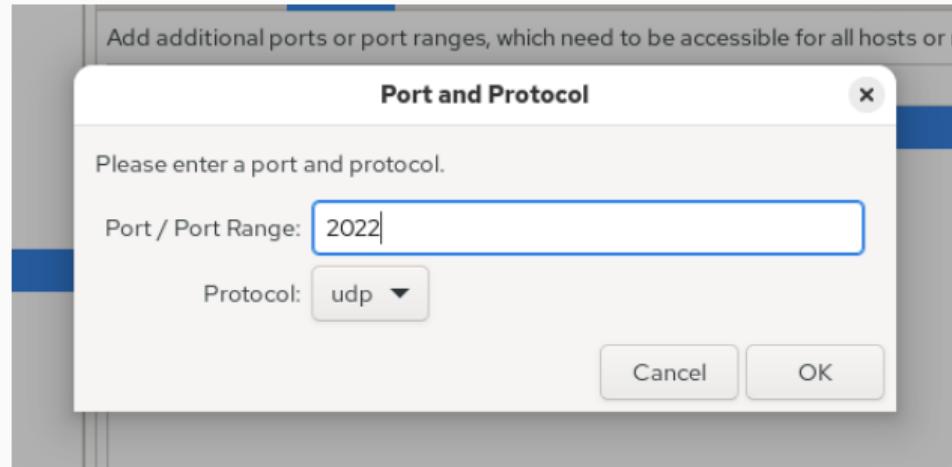


Рис. 7: Добавление порта UDP

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 dhcpcv6-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 dhcpcv6-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 dhcpcv6-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

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.