

Презентация по лабораторной работе №13

Управление брандмауэром в Linux (firewalld)

Амина Аджигалиева

5 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель

Изучить управление фильтрацией пакетов в Linux с использованием **firewalld**, освоить работу с режимами **runtime** и **permanent**, добавлением служб и портов через командную строку и графическую утилиту **firewall-config**.

Ход выполнения работы

Определение параметров брандмауэра

```
+ aradzhigalieva@aradzhigalieva:/home/aradzhigalieva x
aradzhigalieva@aradzhigalieva:~$ su
Password:
root@aradzhigalieva:/home/aradzhigalieva#
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --get-default-zone
public
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd a
seqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc b
itcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civili
zation-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpcv6 dhcpcv6-client distcc dns
dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio fing
er foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client g
anglia-master git gpgsql grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ip
sec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserve
r kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-service
s kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls l
ightning-network llmntr llmntr-client llmntr-tcp llmntr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mo
sh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nf
s nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pm
webapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseau
dio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba sa
mba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtpts snmp snmptls snmptls-t
rap snmptrap spiderOak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-
crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog sysl
og-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp
warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-
udp wsdd wsdd-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-
server zabbix-trapper zabbix-web-service zero-k zerotier
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --list-services
cockpit dhcpcv6-client ssh
root@aradzhigalieva:/home/aradzhigalieva#
```

Анализ активной конфигурации

```
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva# 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:
```

Добавление службы VNC (runtime)

```
root@aradzhigalieva:/home/aradzhigalieva#  
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --add-service=vnc-server  
success  
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva#
```

Рис. 3: Добавление vnc runtime

Добавление VNC в permanent конфигурацию

```
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --add-service=vnc-server --permanent
success
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva#
```

Рис. 4: Сохранение и применение настроек

Добавление пользовательского порта

```
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --add-port=2022/tcp --permanent
success
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --reload
success
root@aradzhigalieva:/home/aradzhigalieva# 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@aradzhigalieva:/home/aradzhigalieva#
```

Рис. 5: Добавление порта

Включение служб через графический интерфейс

Firewall Configuration

File Options View Help

▼ Active Bindings

Configuration: Permanent

Connections

- lo (lo)
Default Zone: public
- dhcp (enp0s3)
Default Zone: public

Interfaces

Sources

Zones Services IPSets

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

Services Ports Protocols Source Ports Masquerading Port Forwarding

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

Service
<input checked="" type="checkbox"/> http
<input type="checkbox"/> galera
<input type="checkbox"/> ganglia-client
<input type="checkbox"/> ganglia-master
<input type="checkbox"/> git
<input type="checkbox"/> gpsd
<input type="checkbox"/> grafana
<input type="checkbox"/> gre
<input type="checkbox"/> high-availability
<input checked="" type="checkbox"/> https
<input type="checkbox"/> http3
<input checked="" type="checkbox"/> https
<input type="checkbox"/> ident

Change Zone + - C

Connection to firewalld established. Changes applied.

Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

Добавление UDP-порта 2022

Firewall Configuration

File Options View Help

Configuration: Permanent

Active Bindings

Connections

- lo (lo)
Default Zone: public
- dhcp (enp0s3)
Default Zone: public

Interfaces

Sources

Zones Services IPSets

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

Services Ports Protocols Source Ports Masquerading Port Forwarding

Add additional ports or port ranges, which need to be accessible for all hosts or networks that can connect to the machine.

Port	Protocol
2022	tcp
2022	udp

Change Zone    

Add Edit Remove

Connection to firewalld established. Changes applied.

Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

9/12

Настройка доступа к службам telnet, imap, pop3, smtp

Firewall Configuration

File Options View Help

▼ Active Bindings

Configuration: Permanent

Zones Services IPSets

A firewalld zone defines the level of trust for network connections, interfaces and source addresses bound to the zone. The zone combines services, ports, protocols, masquerading, port/packet forwarding, icmp filters and rich rules. The zone can be bound to interfaces and source addresses.

block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

Services Ports Protocols Source Ports Masquerading Port Forwarding

Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone.

Service
<input type="checkbox"/> slimevr
<input type="checkbox"/> slp
<input type="checkbox"/> smtp
<input checked="" type="checkbox"/> smtps
<input type="checkbox"/> smtp-submission
<input type="checkbox"/> snmp
<input type="checkbox"/> snmpvls
<input type="checkbox"/> snmpvls-trap
<input type="checkbox"/> snmptrap
<input type="checkbox"/> spideroak-lansync
<input type="checkbox"/> spotify-sync
<input type="checkbox"/> squid

Change Zone + - C

Connection to firewalld established. Changes applied.

Default Zone: public **Log Denied:** off **Panic Mode:** disabled **Automatic Helpers:** no

Проверка итоговой конфигурации

```
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --add-service=telnet --permanent
success
root@aradzhigalieva:/home/aradzhigalieva# firewall-cmd --reload
success
root@aradzhigalieva:/home/aradzhigalieva# 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 smtps ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@aradzhigalieva:/home/aradzhigalieva#
```

Рис. 9: GUI: службы добавлены

Заключение

В ходе работы я:

- изучила управление брандмауэром `firewalld`;
- научилась добавлять и удалять службы и порты;
- разобралась в различии `runtime` и `permanent` настроек;
- освоила как работу через CLI, так и через GUI (`firewall-config`).

Полученные навыки помогут в администрировании серверов и обеспечении сетевой безопасности.