Отчёт по лабораторной работе №13

Фильтр пакетов

Щемелев Илья Владимирович

Российский университет дружбы народов, Москва, Россия

Цель работы

Формулировка цели

Получить навыки настройки пакетного фильтра в Linux.

Ход выполнения работы

Определение зоны по умолчанию и доступных служб

```
root@ivschemelev:~# firewall-cmd --get-default-zone
public
root@ivschemelev:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ivschemelev:~# 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 ase
qnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitco
in-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization
-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-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-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-maste
r git gpsd grafana gre high-availability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs i
scsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-p
lane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler k
ube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llm
nr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqt
t-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe nt
p nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3
s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel rad
ius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settl
ers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync s
potify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission sup
ertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp
 tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wiregu
ard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xm
pp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service z
ero-k zerotier
root@ivschemelev:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ivschemelev:~#
```

Рис. 1: Определение зоны и просмотр служб/сервисов

Просмотр конфигурации активной зоны

```
root@ivschemelev:~# 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@ivschemelev:~#
```

Сравнение list-all и list-all для зоны public

```
root@ivschemelev:~# 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@ivschemelev:~#
```

Добавление сервиса vnc-server (runtime)

```
root@ivschemelev:~# firewall-cmd --add-service=vnc-server
success
root@ivschemelev:~# 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@ivschemelev:~#
```

Перезапуск firewalld и сброс runtime-конфигурации

```
root@ivschemelev:~#
root@ivschemelev:~# systemctl restart firewalld.service
root@ivschemelev:~# 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@ivschemelev:~#
```

Добавление vnc-server в permanent

```
root@ivschemelev:~# firewall-cmd --add-service=vnc-server --permanent
success
root@ivschemelev:~# 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@ivschemelev:~#
```

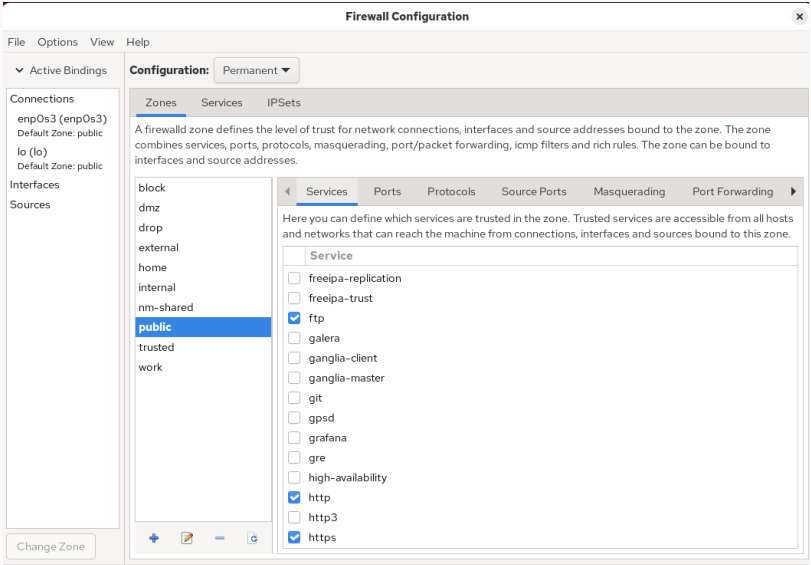
Применение permanent-настроек через reload

```
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# 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@ivschemelev:~#
```

Добавление порта 2022/tcp в permanent

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

Запуск GUI и выбор режима Permanent



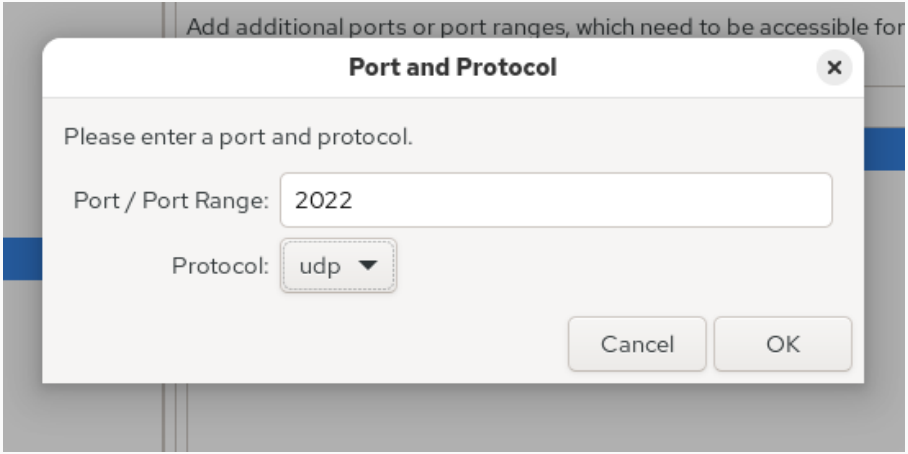
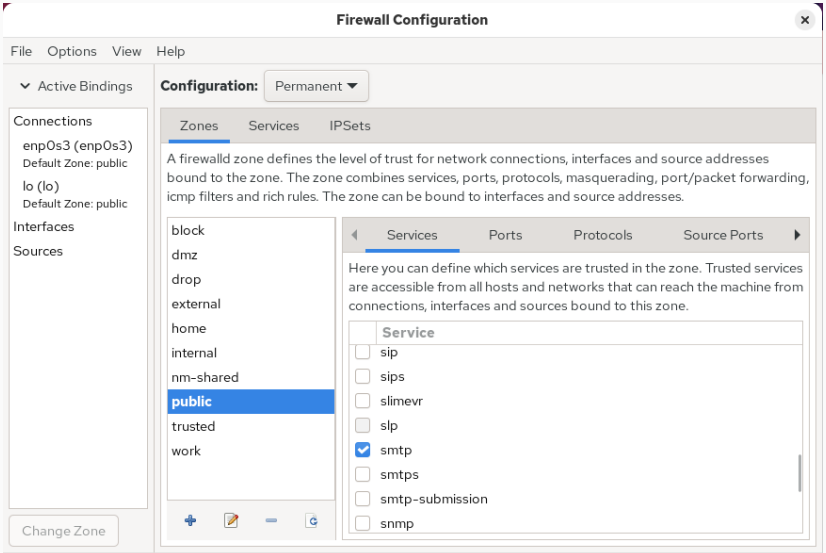


Рис. 10: Добавление порта 2022/udp в GUI

Применение изменений в runtime через reload

```
root@ivschemelev:~#
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# 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@ivschemelev:~#
```

Добавление служб imap, pop3, smtp через GUI



Добавление telnet и итоговая проверка конфигурации

```
root@ivschemelev:~#
root@ivschemelev:~# firewall-cmd --add-service=telnet --permanent
success
root@ivschemelev:~# firewall-cmd --reload
success
root@ivschemelev:~# 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 ident 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@ivschemelev:~#
```

Рис. 13: Итоговая конфигурация с telnet и другими службами

Итоги работы

Заключение

Отработаны способы управления firewalld через firewall-cmd и firewall-config. Проверено различие между runtime и permanent-конфигурациями и порядок применения изменений (reload). Настроен доступ к службам и портам, обеспечена постоянная активация конфигурации после перезагрузки системы.