

Отчёт о лабораторной работе

Лабораторная работа 13. Фильтр пакетов

Баранов Никита Дмитриевич

Содержание

1. Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2. Задание

1. Используя `firewall-cmd`: – определить текущую зону по умолчанию; – определить доступные для настройки зоны; – определить службы, включённые в текущую зону; – добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`: – добавьте службы `http` и `ssh` в зону `public`; – добавьте порт 2022 протокола UDP в зону `public`; – добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

3. Выполнение лабораторной работы

3.1 Работа с `firewalld` через командную строку

Получаем полномочия администратора и определяем текущую зону по умолчанию (рис. [fig:001?]).

```
root@ndbaranov:~# firewall-cmd --get-default-zone
public
root@ndbaranov:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ndbaranov:~# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule app amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl
ent bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-
lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-uni
cast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client e
tcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera gangl
ia-client ganglia-master git gssd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-cont
rol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-schedule
r kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network ll
nmr llmr-client llmr-top llmr-udp managesieve matrix mdns memcache minidlna mongod mosh mounted ngtt ngtt-tls ns-wot mysql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
torageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps3netshr ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquodad r
sh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap s
nmptrap spiderOak-lansync spotify-sync squid sddp ssh steam-streaming svdrp svn synching synching-gui synching-relay synergy
syslog syslog-tls telnet tentacle tftp tftp38 tinc tor-socks transmission-client upnp-client vdm vnc-server warpinator wbm-h
tftp wbm-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman xdmp xmp-bosh xmp-c
lient xmp-local xmp-server zabbox-agent zabbox-server zerotier
root@ndbaranov:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ndbaranov:~# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov:~# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
```

Определение зоны по умолчанию

Текущая зона по умолчанию: public

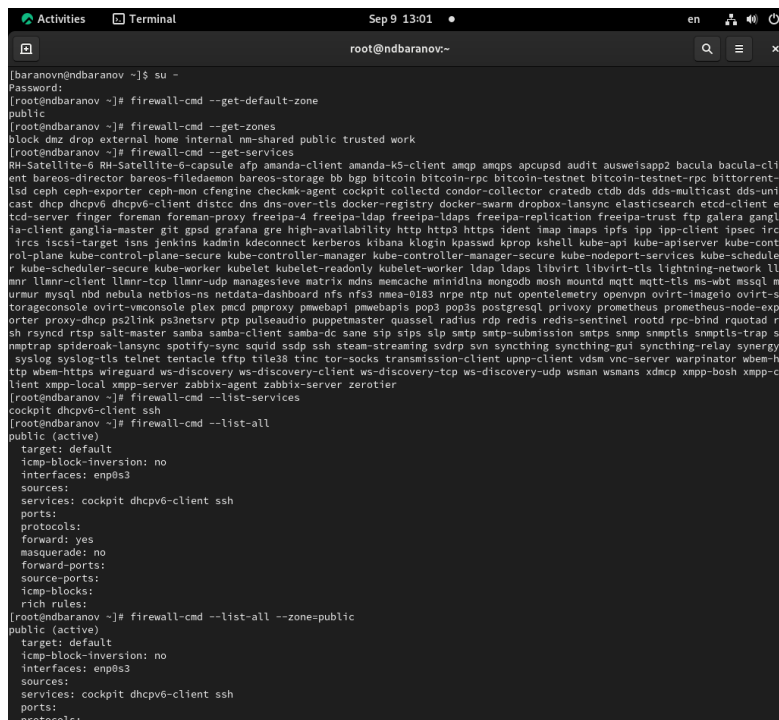
Просматриваем доступные зоны безопасности (рис. [fig:001?]).

```
root@ndbaranov:~# firewall-cmd --get-default-zone
public
root@ndbaranov:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ndbaranov:~# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule app amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl
ent bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-
lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-uni
cast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client e
tcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera gangl
ia-client ganglia-master git gssd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-cont
rol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-schedule
r kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network ll
nmr llmr-client llmr-top llmr-udp managesieve matrix mdns memcache minidlna mongod mosh mounted ngtt ngtt-tls ns-wot mysql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
torageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps3netshr ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquodad r
sh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap s
nmptrap spiderOak-lansync spotify-sync squid sddp ssh steam-streaming svdrp svn synching synching-gui synching-relay synergy
syslog syslog-tls telnet tentacle tftp tftp38 tinc tor-socks transmission-client upnp-client vdm vnc-server warpinator wbm-h
tftp wbm-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman xdmp xmp-bosh xmp-c
lient xmp-local xmp-server zabbox-agent zabbox-server zerotier
root@ndbaranov:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ndbaranov:~# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov:~# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
```

Доступные зоны безопасности

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

Просматриваем доступные службы (рис. [fig:001?]).



```
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# firewall-cmd --get-default-zone
public
[root@ndbaranov ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@ndbaranov ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afd amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl
ent bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent
lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-uni
cast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client e
tcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera gangl
ia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-cont
rol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-schedule
r kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network ll
nmr llmn-client llmn-tcp llmn-udp managesieve matrix ndns memcache minidlna mongod mosh mountd mqtt mqtt-tls ms-mot ssl m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
torageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquotad r
sh rsyncd rtsp salt-master samba samba-client samba-dc sane sip slps sip smtp smtp-submission smtps snmp snmptls snmptls-trap s
nmptrap spiderOak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp sun syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbem-h
ttp wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman xdmpc xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbox-agent zabbox-server zerotier
[root@ndbaranov ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
rich rules:
[root@ndbaranov ~]# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
```

Доступные службы

Количество доступных служб: более 200 сетевых служб

Просматриваем активные службы в текущей зоне (рис. [fig:001?]).

```
root@ndbaranov:~# firewall-cmd --get-default-zone
public
root@ndbaranov:~# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@ndbaranov:~# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule app amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula bacula-cl
ent bareos-director bareos-filedemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-
lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-uni
cast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client e
tcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera gangl
ia-client ganglia-master git gssd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc
ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-cont
rol-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-schedule
r kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network ll
nmr llmn-client llmn-top llmn-udp managelive matrix mdns memcache minidbm mongodb mosh mounted ngtt ngtt-tls ns-wot mysql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
torageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps3netdrv ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rootd rpc-bind rquodad r
sh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap s
nmptrap spiderOak-lansync spotify-sync squid sddp ssh steam-streaming svdrp svn synching synching-gui synching-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdm vnc-server warpinator wbeam-h
tftp wbeam-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsman xdmp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbox-agent zabbox-server zerotier
root@ndbaranov:~# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@ndbaranov:~# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov:~# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
```

Активные службы в зоне public

Активные службы: cockpit dhcpv6-client ssh

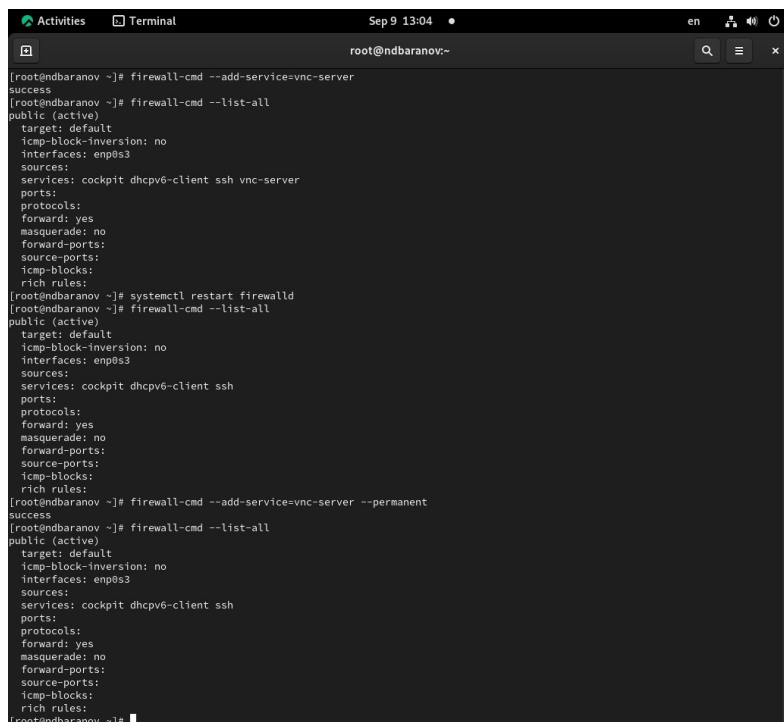
Сравниваем вывод информации о текущей зоне (рис. [fig.001?]).

```
root@ndbaranov:~# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov:~# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
```

Сравнение вывода информации

Результат сравнения: Обе команды выводят идентичную информацию о зоне public

Добавляем службу VNC-server в конфигурацию (рис. [fig:002?]).

A terminal window titled 'Terminal' with a timestamp of 'Sep 9 13:04'. The user is root@ndbaranov. The terminal shows the following commands and output:

```
[root@ndbaranov ~]# firewall-cmd --add-service=vnc-server
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# systemctl restart firewalld
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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:
```

Добавление службы VNC-server

Проверяем добавление службы (рис. [fig:002?]).

```
Activities Terminal Sep 9 13:04 en root@ndbaranov:~
[root@ndbaranov ~]# firewall-cmd --add-service=vnc-server
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# systemctl restart firewalld
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Проверка добавления VNC-server

Результат: Служба vnc-server успешно добавлена в активные службы

Перезапускаем службу firewalld и проверяем конфигурацию (рис. [fig:002?]).

```
Activities Terminal Sep 9 13:04 en root@ndbaranov:~
[root@ndbaranov ~]# firewall-cmd --add-service=vnc-server
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# systemctl restart firewalld
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Проверка после перезапуска

Результат: Служба vnc-server отсутствует, так как была добавлена только для времени выполнения, а не постоянно

Добавляем службу vnc-server с параметром `--permanent` (рис. [fig:002?]).

```
Activities Terminal Sep 9 13:04 en root@ndbaranov:~
[root@ndbaranov ~]# firewall-cmd --add-service=vnc-server
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# systemctl restart firewalld
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-service=vnc-server --permanent
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Добавление постоянной службы

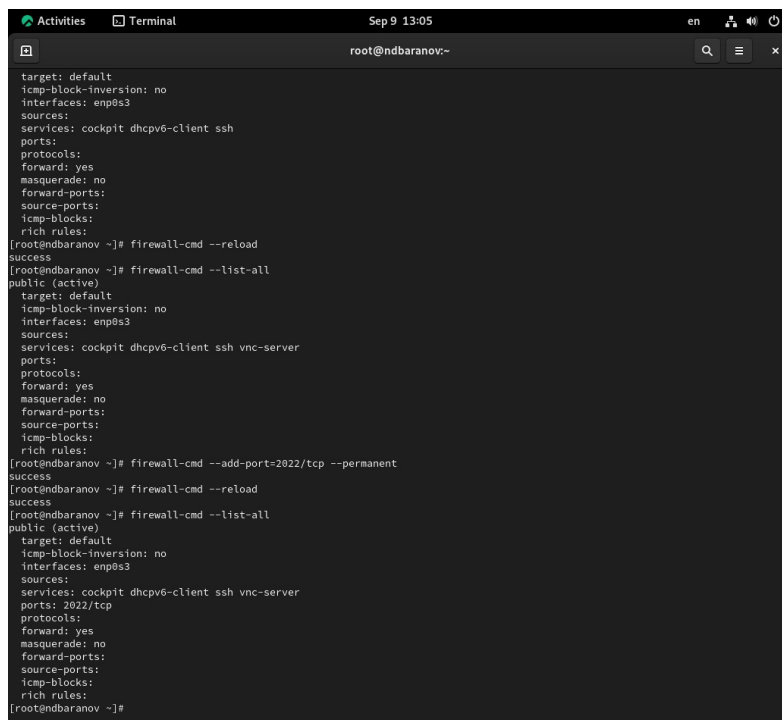
Перезагружаем конфигурацию и проверяем (рис. [fig:003?]).

```
Activities Terminal Sep 9 13:05 en root@ndbaranov:~
target: default
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@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Перезагрузка конфигурации

Результат: Служба vnc-server теперь постоянно присутствует в конфигурации

Добавляем порт 2022/tcp в конфигурацию (рис. [fig:003?]).



```
target: default
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@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Добавление порта 2022/tcp

Проверяем добавление порта (рис. [fig:003?]).

```
Activities Terminal Sep 9 13:05 en
root@ndbaranov:~
target: default
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@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]# firewall-cmd --list-all
public (active)
target: default
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@ndbaranov ~]#
```

Проверка добавленного порта

Результат: Порт 2022/tcp успешно добавлен в конфигурацию

3.2 Работа с графическим интерфейсом firewall-config

Устанавливаем и запускаем графический интерфейс (рис. [fig:006?]).

```
Activities Terminal Sep 9 13:17 en
baranovn@ndbaranov~

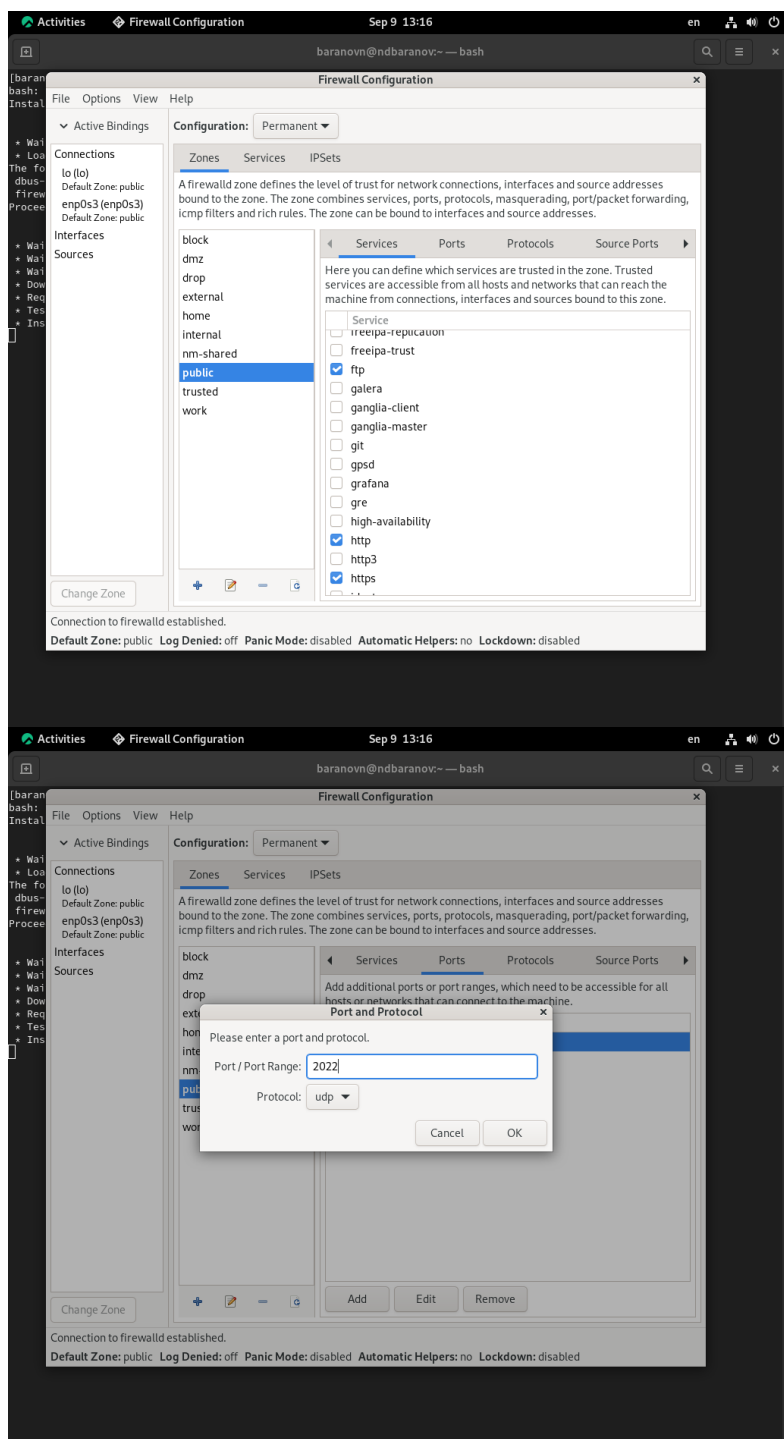
* Waiting in queue...
* Loading list of packages....
The following packages have to be installed:
dbus-x11-1:1.12.20-8.el9.x86_64      X11-requiring add-ons for D-BUS
Firewall-config-1.3.4-9.el9_5.noarch Firewall configuration application
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[baranovn@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranovn@ndbaranov ~]$ firewall-cmd --reload
success
[baranovn@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranovn@ndbaranov ~]$
```

Установка *firewall-config*

Работаем с графическим интерфейсом (рис. [fig:004?], [fig:005?]).



Выполненные действия в графическом интерфейсе: - Установка режима "Permanent" для постоянных изменений - Добавление служб: http, https, ftp - Добавление порта 2022/udp

Проверяем изменения после перезагрузки конфигурации (рис. [fig:006?]).

```
Activities Terminal Sep 9 13:17 en
baranov@ndbaranov~$

* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
dbus-x11-1:1.12.20-8.el9.x86_64      X11-requiring add-ons for D-BUS
firewall-config-1.3.4-9.el9_5.noarch Firewall configuration application
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[baranov@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranov@ndbaranov ~]$ firewall-cmd --reload
success
[baranov@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranov@ndbaranov ~]$
```

Проверка изменений после GUI

Результат: Все изменения из графического интерфейса применены: -
Службы: cockpit dhcpv6-client ftp http https ssh vnc-server - Порты:
2022/tcp 2022/udp

3.3 Настройка доступа к сетевым службам

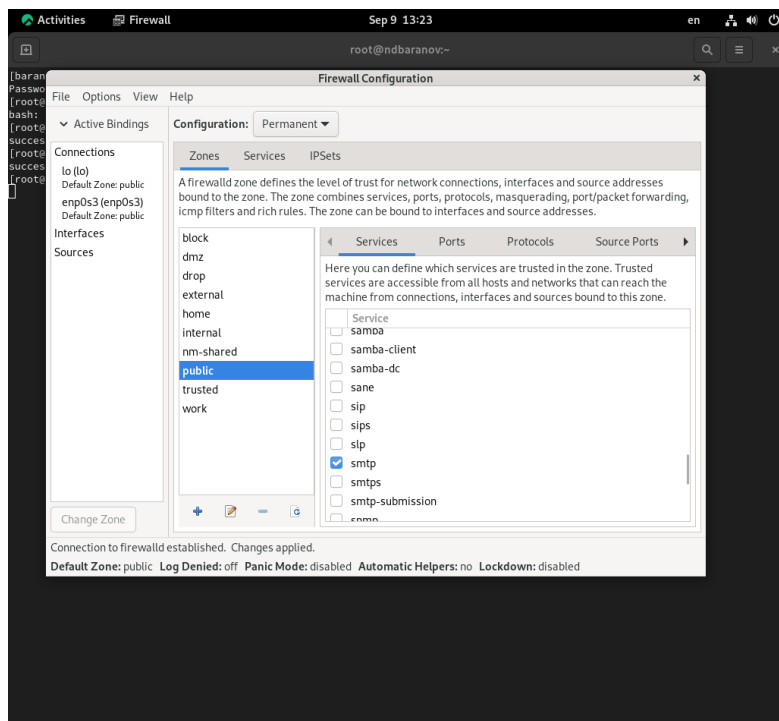
Добавляем службу telnet через командную строку (рис. [fig:007?]).

```
Activities Terminal Sep 9 13:22 en
root@ndbaranov:~
[baranov@ndbaranov ~]$ su -
Password:
[root@ndbaranov ~]# firewall-cmd --permanent --add-service=telnet
bash: firewall-cmd: command not found...
[root@ndbaranov ~]# firewall-cmd --permanent --add-service=telnet
success
[root@ndbaranov ~]# firewall-cmd --reload
success
[root@ndbaranov ~]#
```

Добавление службы telnet

Выполненная команда: `firewall-cmd --permanent --add-service=telnet`

Добавляем службы imap, pop3, smtp через графический интерфейс (рис. [fig:008?]).



Добавление почтовых служб

Добавленные службы: - imap - протокол доступа к электронной почте -
pop3 - протокол получения почты - smtp - протокол отправки почты

Проверяем окончательную конфигурацию (рис. [fig:006?]).

```
Activities Terminal Sep 9 13:17 en
baranov@ndbaranov~$

* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
dbus-x11-1:1.12.20-8.el9.x86_64      X11-requiring add-ons for D-BUS
firewall-config-1.3.4-9.el9.noarch   Firewall configuration application
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[baranov@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranov@ndbaranov ~]$ firewall-cmd --reload
success
[baranov@ndbaranov ~]$ firewall-cmd --list-all
public (active)
target: default
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:
[baranov@ndbaranov ~]$
```

Финальная проверка конфигурации

4. Выводы

Мы получили навыки настройки пакетного фильтра в Linux.

Список литературы