

Лабораторная работа 13

Фильтр пакетов

Баранов Никита Дмитриевич

- Баранов Никита Дмитриевич
- студент группы НПИбд-02-24
- Российский университет дружбы народов
- 1132242977@pfur.ru



Цель работы

Получить навыки настройки пакетного фильтра в Linux.

1. Используя **firewall-cmd**:
 - определить текущую зону по умолчанию;
 - определить доступные зоны;
 - определить службы в текущей зоне;
 - добавить vnc-server.
2. Используя **firewall-config**:
 - добавить службы http, ssh, ftp;
 - добавить порт 2022/udp.
3. Выполнить задание для самостоятельной работы (раздел 13.5).

Определение зоны по умолчанию

```
Activities Terminal Sep 9 13:01 en root@ndbaranov:~

[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 afp 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 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
nvr llmn-client llmn-tcp llmn-udp managesieve matrix adns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-
storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps2netary 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 sipps slp smtp smtp-submission smtps snmp snmp-tls snmp-tls-trap s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbm-h
ttp wdem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbix-agent zabbix-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:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Доступные зоны безопасности

```
Activities Terminal Sep 9 13:01 en root@ndbaranov:~

[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 afp 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 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
nvr llmnr-client llmnr-tcp llmnr-udp managesieve matrix adns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql 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 pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps2netary 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 sipps slp smtp smtp-submission smtps snmp snmp-tls snmp-tls-trap s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbm-h
ttp wdem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbix-agent zabbix-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 службы

```
Activities Terminal Sep 9 13:01 en root@ndbaranov:~

[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 afp 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 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
nvr llmnr-client llmnr-tcp llmnr-udp managiesieve matrix adns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmedbapi pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps2netary 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 sipps slp smtp smtp-submission smtps snmp snmp-tls snmp-tls-trap s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbm-h
ttp wdem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbix-agent zabbix-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:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

Активные службы в зоне

```
Activities Terminal Sep 9 13:01 en root@ndbaranov:~

[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 afp 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 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
nvr llmnr-client llmnr-tcp llmnr-udp managiesieve matrix adns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql m
urmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap nmap-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-s
torageconsole ovirt-vmconsole plex pmcd pmproxy pmmebapi pmmebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps2netary 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 sipd smtp smtp-submission smtps snmp snmp-tls snmp-tls-trap s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbm-h
ttp wdem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbix-agent zabbix-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:
```


Сравнение вывода информации о зоне

```
Activities Terminal Sep 9 13:01 en root@ndbaranov:~

[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 afp 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 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
nvr llmnr-client llmnr-tcp llmnr-udp managesieve matrix adns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql 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 pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exp
orter proxy-dhcp ps2link ps2netary 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 sipps slp smtp smtp-submission smtps snmp snmp-tls snmp-tls-trap s
nmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy
syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client vdsim vnc-server warpinator wbm-h
ttp wdem-https wireguard ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-c
lient xmpp-local xmpp-server zabbix-agent zabbix-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:
```

Добавление VNC-server

```
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

```
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 VNC-server permanent

```
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 ~]#
```

Перезагрузка конфигурации

```
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 ~]#
```

Добавление порта 2022/tcp

```
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 ~]#
```

Установка firewall-config

```
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

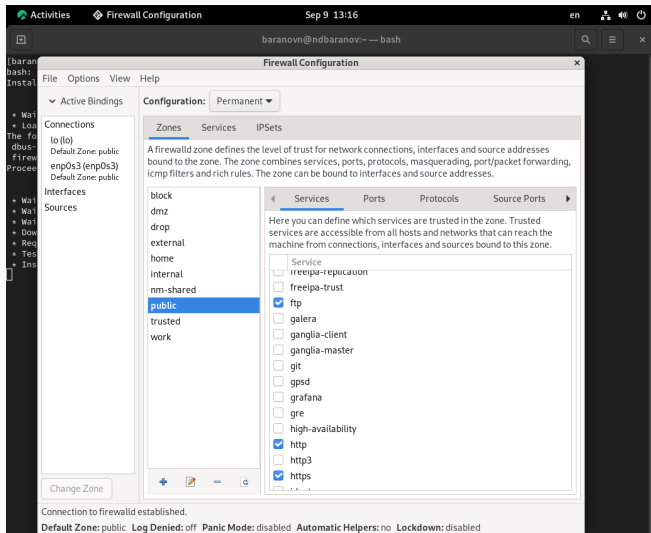
* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[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 ~]$
```

Работа с firewall-config



Проверка после GUI

```
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

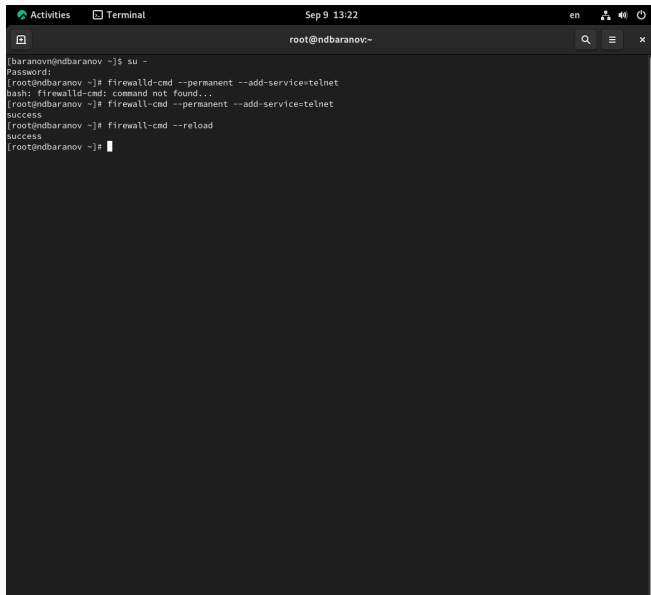
* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...

[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 ~]$
```

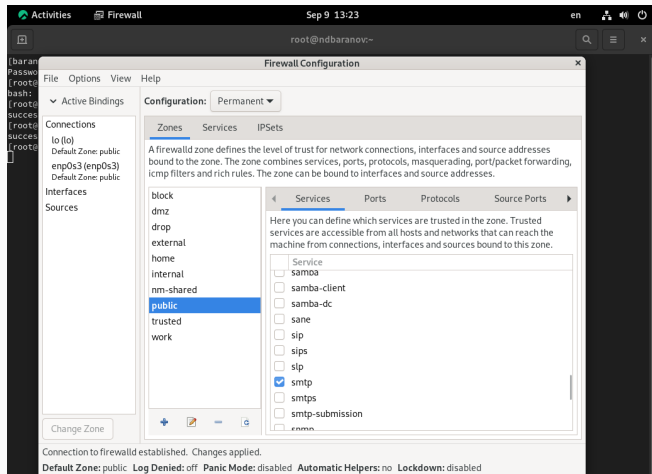
Добавление telnet (CLI)



A terminal window titled "Terminal" with a date and time of "Sep 9 13:22". The window shows a user switching to root and configuring the firewall to allow telnet connections. The commands and their outputs are as follows:

```
(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 почтовых служб (GUI)



Финальная проверка конфигурации

```
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...

(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 ~)$
```

- Получены навыки настройки пакетного фильтра в Linux
- Освоена работа с **firewall-cmd** и **firewall-config**
- Настроены зоны, службы и порты
- Изучена разница между временными и постоянными настройками