

Лабораторная работа №13

Презентация

Устинова В. В.

28 ноября 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Устинова Виктория Вадимовна
- студент НПИбд-01-24
- Российский университет дружбы народов

Получить навыки настройки пакетного фильтра в Linux.

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).

Определите текущую зону по умолчанию, введя, определите доступные зоны, введя

```
[vvustinova@vvustinova ~]$ su -
Пароль:
[root@vvustinova ~]#
[root@vvustinova ~]# firewall-cmd --get-default-zone
public
[root@vvustinova ~]# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[root@vvustinova ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisap
cula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-test
net bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd cond
lector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-
try docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa
freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gps
fana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-targe
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control
plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services
scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libv
ls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongo
db mountd mott mott-tls ms-smbt mssql mysql mongodb nebula netbios-ns netdata-dashboard nfs nfs3 nfs4-01
```

Рис. 1: Текущая public, и смотрим остальные доступные

Управление брандмауэром с помощью firewall-cmd

Определите доступные службы в текущей зоне, Сравните результаты вывода информации при использовании команды

```
[root@vvustinova ~]# firewall-cmd --list-services
cockpit dhcpv6-client ssh
[root@vvustinova ~]# 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@vvustinova ~]# 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
```

Добавьте сервер VNC в конфигурацию брандмауэра, Проверьте, добавился ли vnc-server в конфигурацию

```
[root@vvustinova ~]# firewall-cmd --add-service=vnc-server
success
[root@vvustinova ~]# 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:
```

Управление брандмауэром с помощью firewall-cmd

Перезапустите службу firewalld, проверьте, есть ли vnc-server в конфигурации, Добавьте службу vnc-server ещё раз, но на этот раз сделайте её постоянной, используя команду

```
[root@vvustinova ~]# systemctl restart firewalld
[root@vvustinova ~]# 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@vvustinova ~]# firewall-cmd --add-service=vnc-server --permanent
success
```

Рис. 4: VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения

Управление брандмауэром с помощью firewall-cmd

Проверьте наличие vnc-server в конфигурации, Перезагрузите конфигурацию firewalld и просмотрите конфигурацию времени выполнения

```
success
[root@vvustinova ~]# 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@vvustinova ~]# firewall-cmd --reload
success
[root@vvustinova ~]# 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
```



Управление брандмауэром с помощью firewall-cmd

Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP, Затем перезагрузите конфигурацию firewalld, проверьте что добавлен

```

[root@vvustinova ~]# firewall-cmd --add-port=2022/tcp --permanent
success
[root@vvustinova ~]# firewall-cmd --reload
success
[root@vvustinova ~]# 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@vvustinova ~]#
```

Рис. 6: после перезагрузки все есть

Нажмите выпадающее меню рядом с параметром Configuration . Откройте раскрывающийся список и выберите Permanent Выберите зону public и отметьте службы http, https и ftp, чтобы ВКЛЮЧИТЬ ИХ

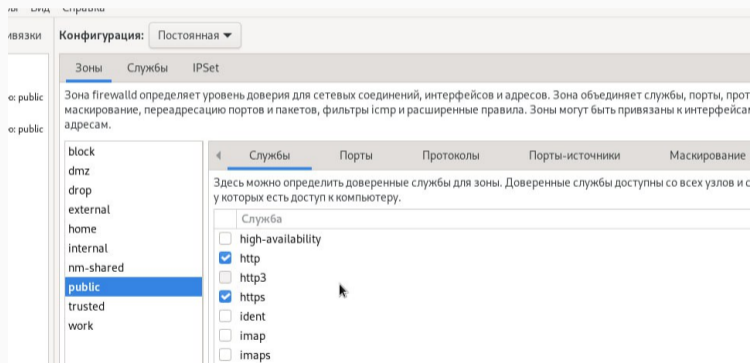


Рис. 7: Выполняем

Выберите вкладку Ports и на этой вкладке нажмите Add . Введите порт 2022 и протокол udp, нажмите OK

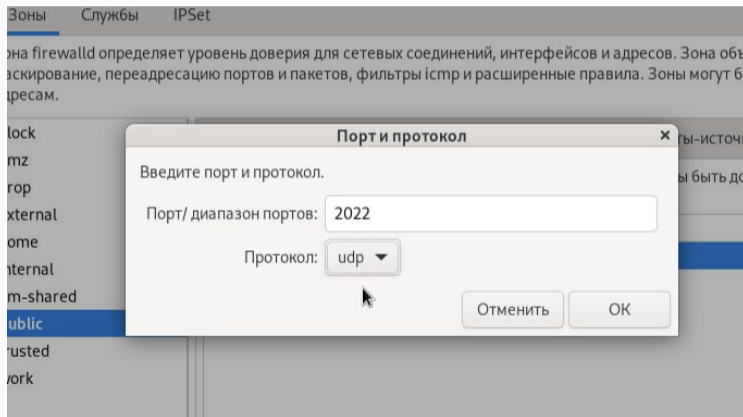
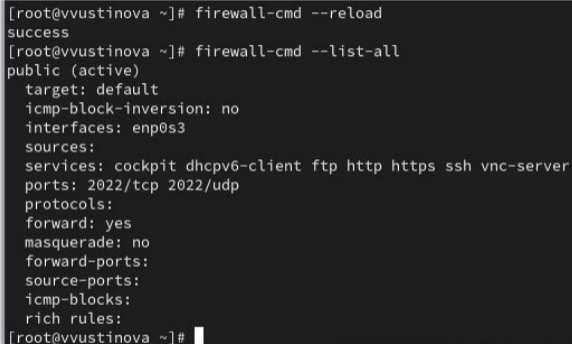


Рис. 8: Выполняем

Перегрузите конфигурацию firewall-cmd, и список доступных сервисов

A terminal window with a dark background. The prompt is [root@vvustinova ~]#. The first command is firewall-cmd --reload, which returns success. The second command is firewall-cmd --list-all, which returns a detailed configuration for the 'public' zone. The configuration includes target: default, icmp-block-inversion: no, interfaces: enp0s3, sources: (empty), services: cockpit dhcpv6-client ftp http https ssh vnc-server, ports: 2022/tcp 2022/udp, protocols: (empty), forward: yes, masquerade: no, forward-ports: (empty), source-ports: (empty), icmp-blocks: (empty), and rich rules: (empty). The prompt returns to [root@vvustinova ~]#.

```
[root@vvustinova ~]# firewall-cmd --reload
success
[root@vvustinova ~]# 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:
[root@vvustinova ~]#
```

Рис. 9: теперь видны изменения все добавилось

Самостоятельная работа

Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:– telnet;– imap;– pop3;– smtp

Конфигурация: Постоянная ▼

Зоны Службы IPSet

Зона firewalld определяет уровень доверия для сетевых соединений, интерфейсов и адресов. Зона маскирование, переадресацию портов и пакетов, фильтры iptables и расширенные правила. Зоны могут применяться к сетевым интерфейсам, IP-адресам или сетевым зонам.

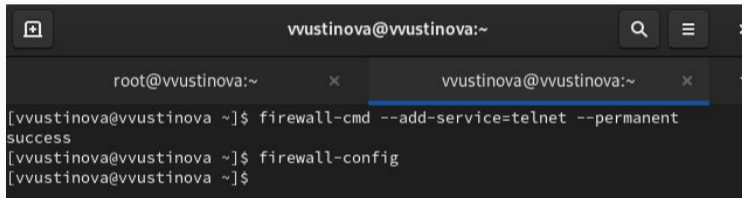
block
dmz
drop
external
home
internal
nm-shared
public
trusted
work

Службы Порты Протоколы Порты-исключения

Здесь можно определить доверенные службы для зоны. Доверенные службы – это службы, у которых есть доступ к компьютеру.

Служба
<input type="checkbox"/> plex
<input type="checkbox"/> pmcd
<input type="checkbox"/> pmproxy
<input type="checkbox"/> pmwebapi
<input type="checkbox"/> pmwebapis
<input checked="" type="checkbox"/> pop3
<input type="checkbox"/> pop3s

Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:– telnet;– imap;– pop3;– smtp



```
vvustinova@vvustinova:~  
root@vvustinova:~  
[vvustinova@vvustinova ~]$ firewall-cmd --add-service=telnet --permanent  
success  
[vvustinova@vvustinova ~]$ firewall-config  
[vvustinova@vvustinova ~]$
```

Рис. 11: Добавляем telnet через командную строку

Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера

```
[vvustinova@vvustinova ~]$ firewall-cmd --reload
success
[vvustinova@vvustinova ~]$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-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:
[vvustinova@vvustinova ~]$
```

Рис. 12: Мы проверили и у нас все добавилось!

Мы успешно получили навыки настройки пакетного фильтра в Linux.