Администрирование сетевых подсистем

Настройка и расширенные возможности firewalld

Метвалли Ахмед Фарг Набеех

6 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получить навыки настройки межсетевого экрана **firewalld** в Linux, включая создание пользовательских служб, переадресацию портов и настройку маскарадинга.

Выполнение лабораторной работы

Создание пользовательской службы firewalld

Рис. 1: Создание и редактирование ssh-custom.xml

Проверка и активация службы

```
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# firewall-cmd --reload
success
[root@server.ahmedfarg.net services]# 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 aseqnet audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bit
coin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-a
gent civilization-iv civilization-v cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast d
hcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasti
csearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa
-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http ht
tp3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeco
nnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-se
cure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-s
ecure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr l
lmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd m
qtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3
 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy
 pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv
 ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp
 salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submissio
n smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh ssh-custom statsrv steam-
lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing
syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-so
cks transmission-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-d
iscovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http 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@server.ahmedfarg.net services]#
```

Рис. 2: Добавление пользовательской службы и проверка списка

Перенаправление портов

Рис. 3: Настройка переадресации порта 2022 на 22

Проверка подключения по новому порту

Рис. 4: SSH-подключение через порт 2022

Настройка Port Forwarding и Masquerading

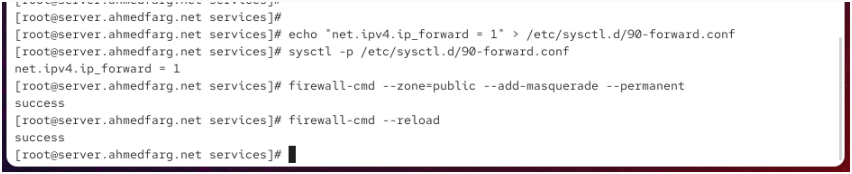
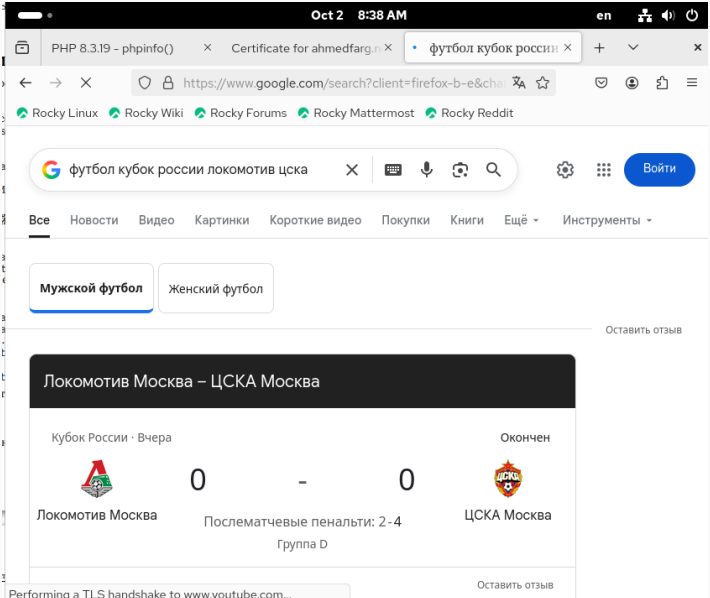
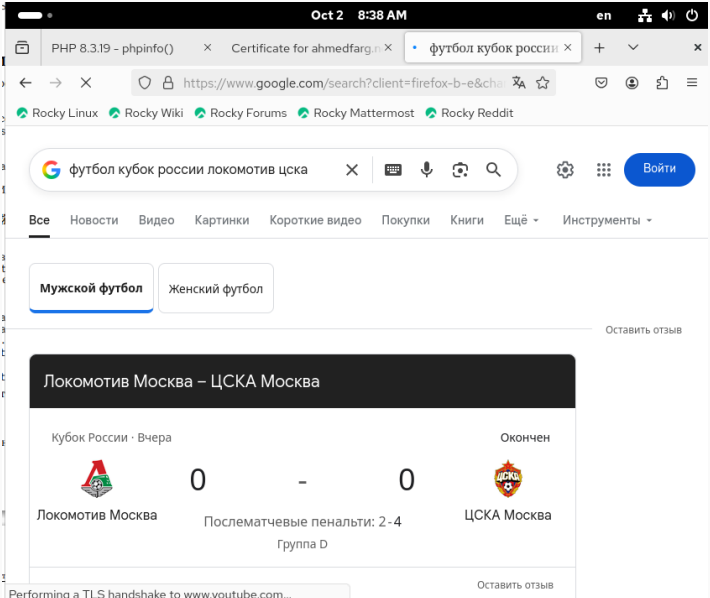


Рис. 5: Проверка и включение ip_forward

Включение маскарадинга



Проверка доступа в Интернет



Создание структуры конфигурационных файлов

```
success
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# cd /vagrant/provision/server/
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.ahmedfarg.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewal
l/etc/firewalld/services/
[root@server.ahmedfarg.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sys
ctl.d/
[root@server.ahmedfarg.net server]# touch firewall.sh
[root@server.ahmedfarg.net server]#
```

Рис. 8: Создание каталогов и скрипта firewall.sh

Контрольные вопросы

Выводы по проделанной работе

Итог

Были выполнены:

- создание пользовательской службы **firewalld**;
- настройка переадресации портов и маскарадинга;
- проверка работы межсетевого экрана;
- автоматизация конфигурации с помощью скрипта **firewall.sh**.