

Администрирование сетевых подсистем

Настройка и расширенные возможности firewalld

Метвалли Ахмед Фарг Набеев

6 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

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

Выполнение лабораторной работы

Создание пользовательской службы firewalld

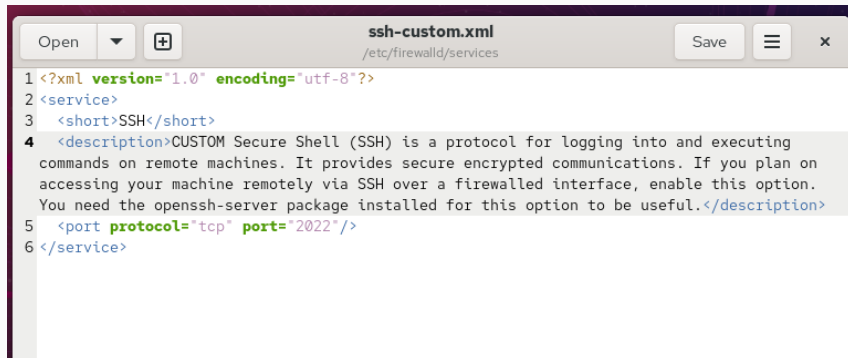


Рис. 1: Создание и редактирование ssh-custom.xml

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 dhcpcv6 dhcpcv6-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 kdec  
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 mounthd 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 ps3net  
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 synching  
synching-gui synching-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-so  
cks transmission-client turn turns upnp-client vdsms 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



```
ahmedfarg@server:~ – ssh -p 2022 ahmedfarg@server.ahmedf...  
[ahmedfarg@client.ahmedfarg.net ~]$ ssh -p 2022 ahmedfarg@server.ahmedfarg.net  
The authenticity of host '[server.ahmedfarg.net]:2022 ([192.168.1.1]:2022)' can't be established.  
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[server.ahmedfarg.net]:2022' (ED25519) to the list of known hosts.  
ahmedfarg@server.ahmedfarg.net's password:  
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/  
  
Last login: Thu Oct 2 08:17:56 2025  
[ahmedfarg@server.ahmedfarg.net ~]$  
[ahmedfarg@server.ahmedfarg.net ~]$
```

Рис. 3: Настройка переадресации порта 2022 на 22

Проверка подключения по новому порту

A terminal window titled 'ahmedfarg@server:~ - ssh -p 2022 ahmedfarg@server.ahmedfarg...' with standard window controls. The terminal shows a user at a client machine running an SSH command to connect to a server on port 2022. The connection is initially refused, and the user is prompted to confirm the host's fingerprint. The user confirms, and the connection is established. The terminal then displays the server's password prompt, a web console URL, and the last login time.

```
ahmedfarg@client.ahmedfarg.net ~]$ ssh -p 2022 ahmedfarg@server.ahmedfarg.net
The authenticity of host '[server.ahmedfarg.net]:2022 ([192.168.1.1]:2022)' can't
be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.ahmedfarg.net]:2022' (ED25519) to the list o
f known hosts.
ahmedfarg@server.ahmedfarg.net's password:
Web console: https://server.ahmedfarg.net:9090/ or https://192.168.1.1:9090/

Last login: Thu Oct  2 08:17:56 2025
ahmedfarg@server.ahmedfarg.net ~]$
ahmedfarg@server.ahmedfarg.net ~]$
```

Рис. 4: SSH-подключение через порт 2022


```
[root@server.ahmedfarg.net ~]# systemctl restart services
[root@server.ahmedfarg.net services]#
[root@server.ahmedfarg.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.ahmedfarg.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.ahmedfarg.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.ahmedfarg.net services]# firewall-cmd --reload
success
[root@server.ahmedfarg.net services]#
```

Рис. 5: Проверка и включение ip_forward

Включение маскардинга

Oct 2 8:38 AM en

PHP 8.3.19 - phpinfo() x Certificate for ahmedfarg.n x футбол кубок россия x

← → × https://www.google.com/search?client=firefox-b-e&cha

Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit

футбол кубок россия локомотив цска × Войти

Все Новости Видео Картинки Короткие видео Покупки Книги Ещё ▾ Инструменты ▾

Мужской футбол Женский футбол

Оставить отзыв

Локомотив Москва – ЦСКА Москва

Кубок России · Вчера Окончен

0 - 0

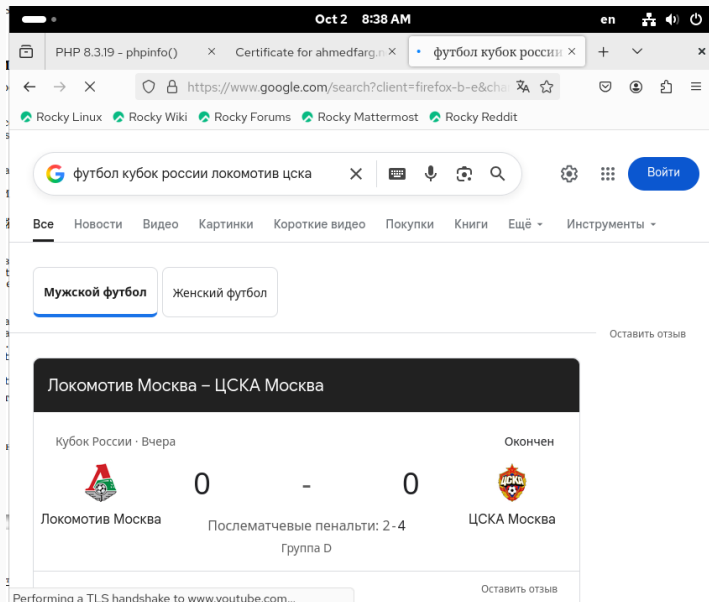
Локомотив Москва ЦСКА Москва

Послематчевые пенальти: 2-4
Группа D

Оставить отзыв

Performing a TLS handshake to www.youtube.com...

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

Были выполнены:

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