

# Презентация по лабораторной работе №7

Расширенные настройки межсетевого экрана

---

Галацан Николай

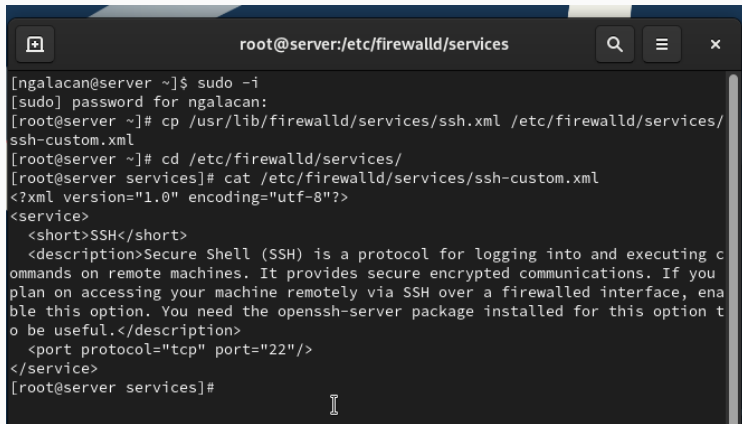
Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

## Создание пользовательской службы firewalld

---



```
root@server:/etc/firewalld/services

[ngalacan@server ~]$ sudo -i
[sudo] password for ngalacan:
[root@server ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server ~]# cd /etc/firewalld/services/
[root@server services]# cat /etc/firewalld/services/ssh-custom.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing c
ommands on remote machines. It provides secure encrypted communications. If you
plan on accessing your machine remotely via SSH over a firewalled interface, ena
ble this option. You need the openssh-server package installed for this option t
o be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server services]#
```

Рис. 1: Создание собственного файла описания службы и просмотр

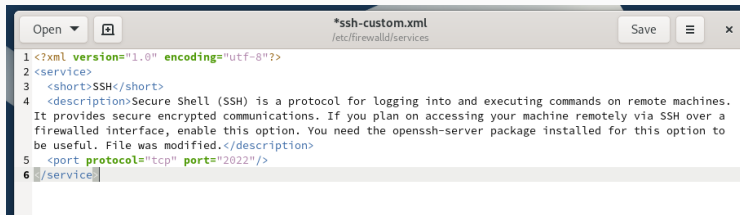
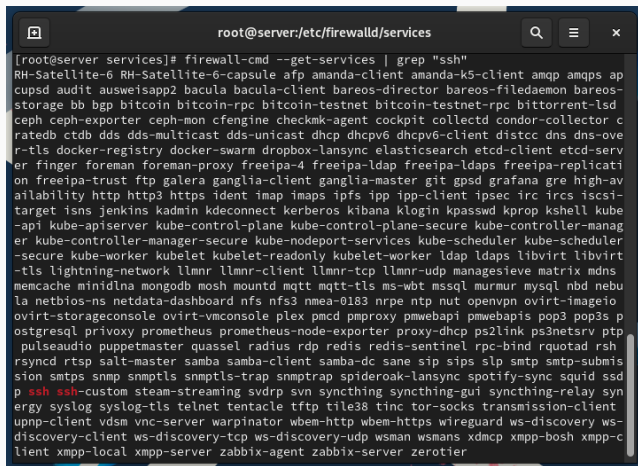


Рис. 2: Редактирование файла описания службы

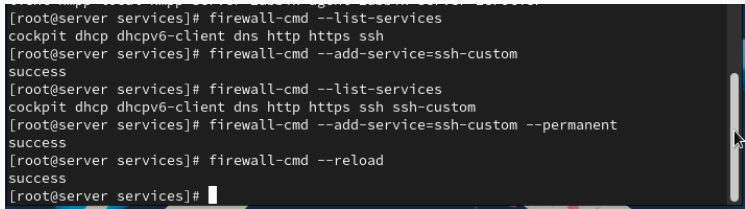
# Выполнение лабораторной работы



```
root@server:/etc/firewalld/services

[root@server services]# firewall-cmd --get-services | grep "ssh"
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps ap
cupsd audit ausweisapp2 bacula bacula-client 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 c
ratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-ove
r-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-serv
er finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replicati
on freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-av
ailability 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-control-plane kube-control-plane-secure kube-controller-manag
er kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler
-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt
-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns
memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebu
la netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio
ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s p
ostgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp
pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh
rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submis
sion smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssd
p ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui syncthing-relay syn
ergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client
upnp-client vdsml vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-
discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-cl
ient xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
```

Рис. 3: Новая служба в списке доступных служб



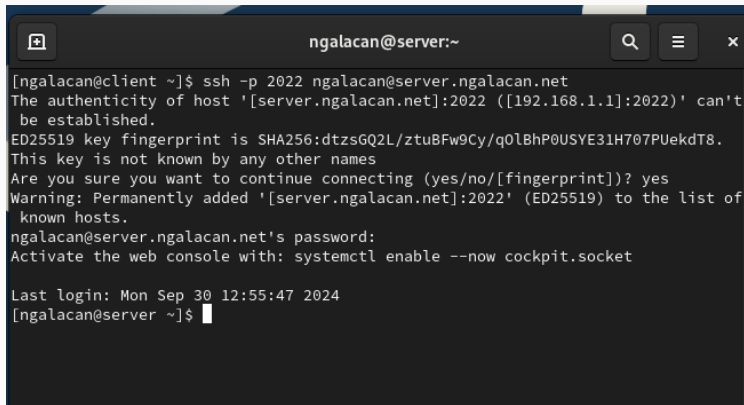
```
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]# firewall-cmd --add-service=ssh-custom
success
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server services]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 4: Добавление новой службы и просмотр списка активных служб, сохранение информации о состоянии



## Перенаправление портов

---



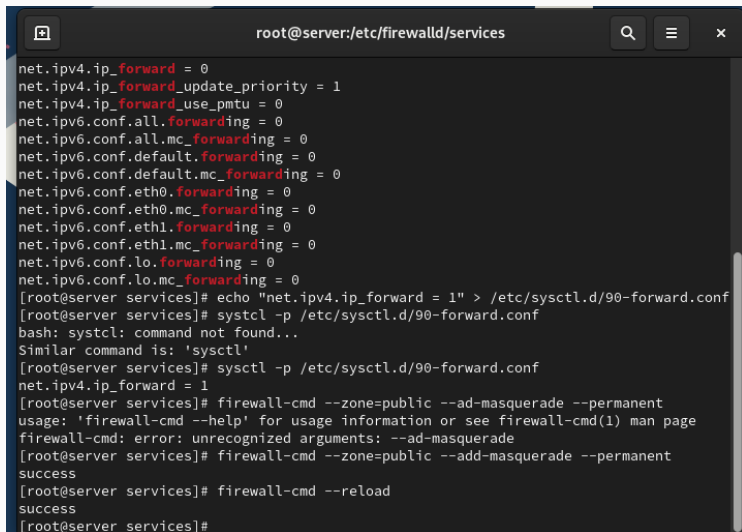
The image shows a terminal window titled 'ngalacan@server:~'. The terminal output shows a user at a client machine running the command 'ssh -p 2022 ngalacan@server.ngalacan.net'. The terminal displays a warning about the host's authenticity, showing the host key fingerprint 'SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8'. The user responds 'yes' to continue. The terminal then shows the user's password and the command 'systemctl enable --now cockpit.socket'. Finally, it shows the last login time 'Mon Sep 30 12:55:47 2024' and the prompt 'ngalacan@server ~\$'.

```
ngalacan@server:~  
[ngalacan@client ~]$ ssh -p 2022 ngalacan@server.ngalacan.net  
The authenticity of host '[server.ngalacan.net]:2022 ([192.168.1.1]:2022)' can't  
be established.  
ED25519 key fingerprint is SHA256:dtzsGQ2L/ztuBFw9Cy/q0lBhP0USYE31H707PUekdT8.  
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.ngalacan.net]:2022' (ED25519) to the list of  
known hosts.  
ngalacan@server.ngalacan.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Mon Sep 30 12:55:47 2024  
ngalacan@server ~$
```

Рис. 5: Доступ по SSH к серверу через порт 2022 на клиенте

## Настройка Port Forwarding и Masquerading

---

A terminal window titled 'root@server:/etc/firewalld/services' with search, menu, and close icons. It displays a series of commands and their outputs for configuring packet forwarding and masquerading in firewalld. The configuration is applied to the 'public' zone.

```
net.ipv4.ip_forward = 0
net.ipv4.ip_forward_update_priority = 1
net.ipv4.ip_forward_use_pmtu = 0
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.all.mc_forwarding = 0
net.ipv6.conf.default.forwarding = 0
net.ipv6.conf.default.mc_forwarding = 0
net.ipv6.conf.eth0.forwarding = 0
net.ipv6.conf.eth0.mc_forwarding = 0
net.ipv6.conf.eth1.forwarding = 0
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
[root@server services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
bash: sysctl: command not found...
Similar command is: 'sysctl'
[root@server services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --add-masquerade
[root@server services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server services]# firewall-cmd --reload
success
[root@server services]#
```

Рис. 6: Включение перенаправления пакетов и включение маскарadingа

Внесение изменений в настройки  
внутреннего окружения  
виртуальной машины

---

```
[root@server services]# cd /vagrant/provision/server
[root@server server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/
server/firewall/etc/firewalld/services/
[root@server server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/fi
rewall/etc/sysctl.d/
[root@server server]# cd /vagrant/provision/server
[root@server server]# touch firewall.sh
[root@server server]# chmod +x firewall.sh
[root@server server]#
```

Рис. 7: Создание каталогов и копирование конфигурационных файлов, создание скрипта firewall.sh



```
1 #!/bin/bash
2
3 echo "Provisioning script $0"
4
5 echo "Copy configuration files"
6 cp -R /vagrant/provision/server/firewall/etc/* /etc
7
8 echo "Configure masquerading"
9 firewall-cmd --add-service=ssh-custom --permanent
10 firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
11 firewall-cmd --zone=public --add-masquerade --permanent
12 firewall-cmd --reload
13
14 restorecon -vR /etc
```

Рис. 8: Редактирование firewall.sh

```
server.vm.provision "server firewall",  
  type: "shell",  
  preserve_order: true,  
  path: "provision/server/firewall.sh"
```



В результате выполнения работы получены навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.