

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ПРЕЗЕНТАЦИЯ

### ВЫПОЛНЕННОЙ ЛАБОРАТОРНОЙ РАБОТЫ № 7

*дисциплина: Администрирование сетевых подсистем*

### Расширенные настройки межсетевого экрана

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

## Цель работы

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

## Ход работы

### Создание пользовательской службы firewalld

- Создание файла с собственным описанием службы ssh на основе существующего

```
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.etanribergenov.net ~]# cd /etc/firewalld/services/
[root@server.etanribergenov.net services]# ls
ssh-custom.xml
```

*Рис. 1. Копирование и переименование файла описания службы ssh*

```
[root@server.etanribergenov.net 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 commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
```

*Рис. 2. Просмотр содержимого файла службы ssh*

```
mc [root@server.etanribergenov.net]:/etc/firewalld/services
ssh-custom.xml [----] 0 L:[ 1+ 6 7/ 7] *(486 / 486b) <EOF>
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH custom</short>
  <description>SSH customed. Secure Shell (SSH) is a protocol for logg
  <port protocol="tcp" port="2022"/>
</service>
```

Рис. 3. Редактирование файла описание службы

- Добавление созданной службы ssh-custom в работу межсетевого экрана

```
[root@server.etanribergenov.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcup
sd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
net-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb
dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbo
x-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-
4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-cli
ent ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-cl
ient ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogi
n kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-man
ager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network l
lmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel ra
dius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samb
a-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroa
k-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-g
ui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-
client upnp-client vdsm vnc-server wbem-http wbem-https wireguard wsman wsmans xdmcp
xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
```

Рис. 4. Список доступных FirewallD служб

Примечание: Новой службы ещё нет в списке.

```
[root@server.etanribergenov.net services]# firewall-cmd --reload
success
[root@server.etanribergenov.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcup
sd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-test
net-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb
dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbo
x-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-
4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-cli
ent ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-cl
ient ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogi
n kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-controller-man
ager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network l
lmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-w
bt mssql murmur mysql nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-im
ageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel ra
dius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samb
a-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroa
k-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing
syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks tr
ansmission-client upnp-client vdsms vnc-server wbem-http wbem-https wireguard wsman ws
mans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
[root@server.etanribergenov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.etanribergenov.net services]#
```

*Рис. 5. Перезагрузка правил firewallD и доступные службы*

```
[root@server.etanribergenov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.etanribergenov.net services]#
```

*Рис. 6. Вывод активных служб*

```
[root@server.etanribergenov.net services]# firewall-cmd --add-service=ssh-custom
success
```

*Рис. 7. Добавление новой службы*

```
[root@server.etanribergenov.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.etanribergenov.net services]#
```

*Рис. 8. Активные службы*

## Перенаправление портов

- Организация переадресации порта на сервере

```
[root@server.etanribergenov.net ~]#  
[root@server.etanribergenov.net ~]# firewall-cmd --add-forward-port=port=2022:  
proto=tcp:toport=22  
success  
[root@server.etanribergenov.net ~]#
```

*Рис. 9. Переадресация порта на сервере*

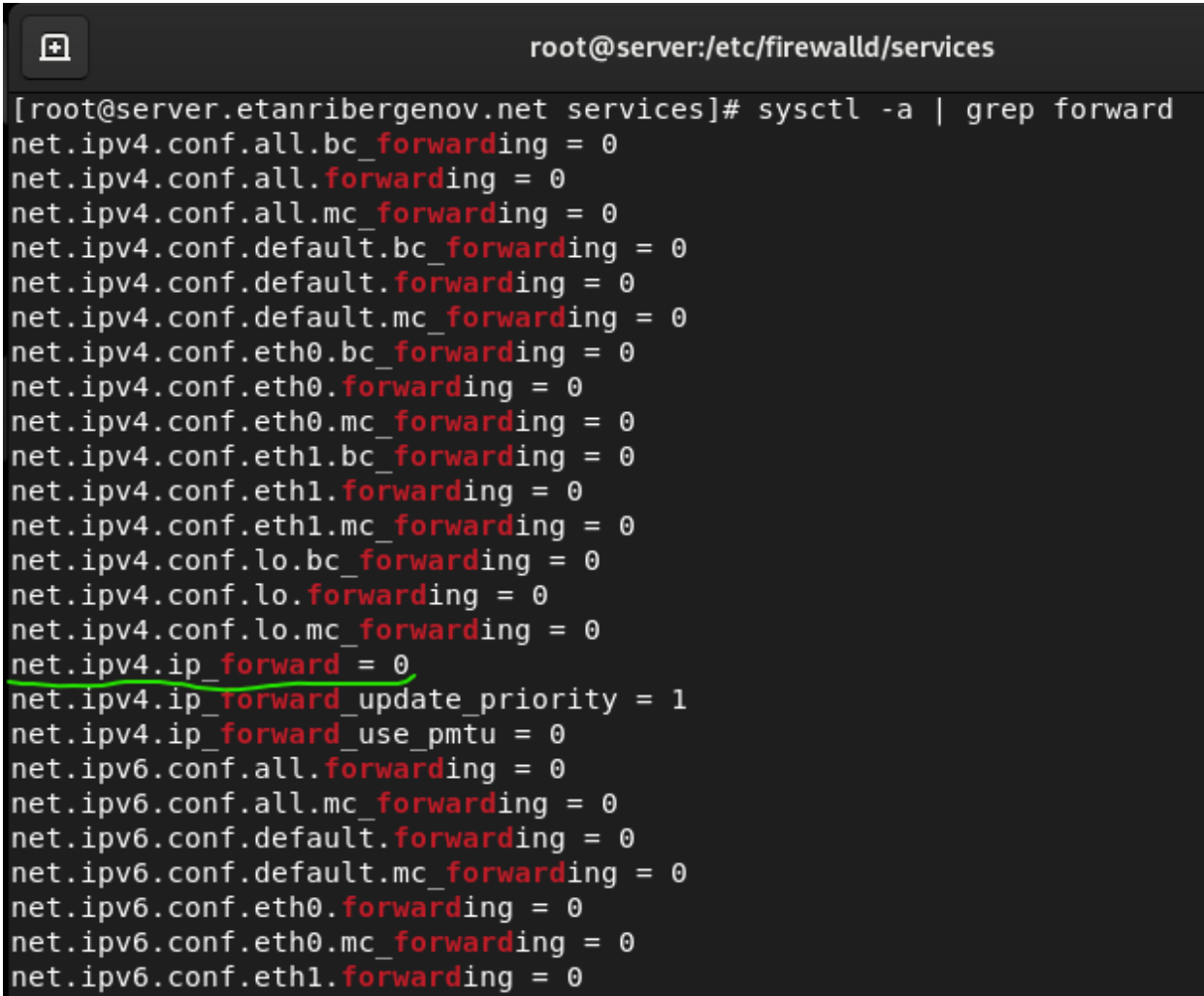
- Подключение клиента к серверу по SSH через порт 2022

```
etanribergenov@server:~  
[etanribergenov@client.etanribergenov.net ~]$ ssh -p 2022 etanribergenov@server.  
etanribergenov.net  
The authenticity of host '[server.etanribergenov.net]:2022 ([192.168.1.1]:2022)'  
can't be established.  
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.  
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.etanribergenov.net]:2022' (ED25519) to the l  
ist of known hosts.  
etanribergenov@server.etanribergenov.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Wed Apr  5 19:58:02 2023  
[etanribergenov@server.etanribergenov.net ~]$
```

*Рис. 10. Получение на клиенте доступа к серверу по SSH через порт 2022*

## Настройка Port Forwarding и Masquerading

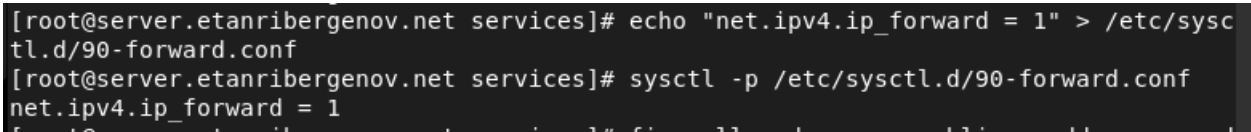
- Организация перенаправления IPv4-пакетов



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

[root@server.etanribergenov.net services]# sysctl -a | grep forward
net.ipv4.conf.all.bc_forwarding = 0
net.ipv4.conf.all.forwarding = 0
net.ipv4.conf.all.mc_forwarding = 0
net.ipv4.conf.default.bc_forwarding = 0
net.ipv4.conf.default.forwarding = 0
net.ipv4.conf.default.mc_forwarding = 0
net.ipv4.conf.eth0.bc_forwarding = 0
net.ipv4.conf.eth0.forwarding = 0
net.ipv4.conf.eth0.mc_forwarding = 0
net.ipv4.conf.eth1.bc_forwarding = 0
net.ipv4.conf.eth1.forwarding = 0
net.ipv4.conf.eth1.mc_forwarding = 0
net.ipv4.conf.lo.bc_forwarding = 0
net.ipv4.conf.lo.forwarding = 0
net.ipv4.conf.lo.mc_forwarding = 0
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
```

Рис. 11. Проверка состояния перенаправления IPv4-пакетов в ядре системы сервера



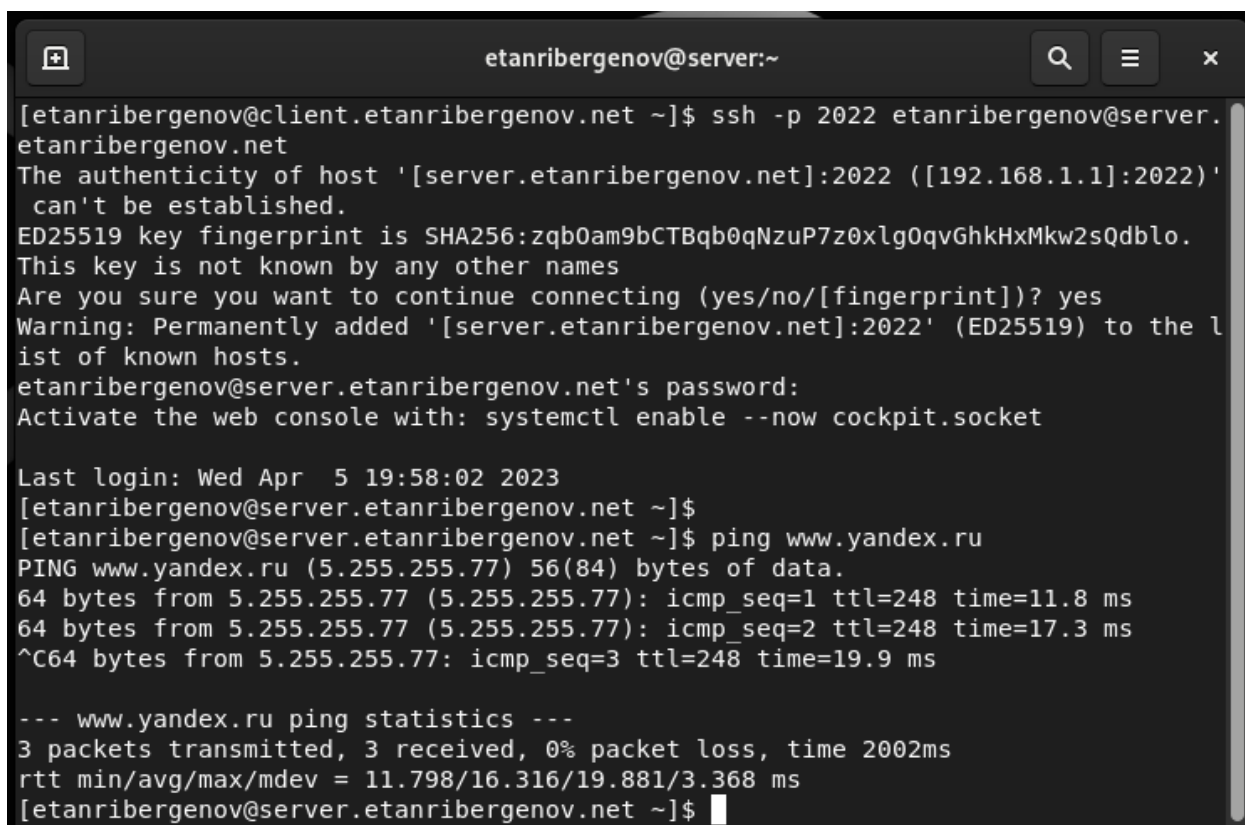
```
[root@server.etanribergenov.net services]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.etanribergenov.net services]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
```

Рис. 12. Включение перенаправления IPv4-пакетов

- Включение маскарадинга и проверка доступности выхода в Интернет на клиенте

```
[root@server.etanribergenov.net services]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.etanribergenov.net services]# firewall-cmd --reload
success
```

*Рис. 13. Включение маскарадинга*



The screenshot shows a terminal window titled 'etanribergenov@server:~'. The user has executed an SSH command to connect to 'etanribergenov@server.etanribergenov.net' with port 2022. The terminal displays a warning about the host's authenticity, which the user accepts. After entering the password, the user runs 'ping www.yandex.ru'. The output shows three successful ping packets with varying response times. Finally, the user runs 'ping statistics', which shows 3 packets transmitted, 3 received, and 0% packet loss.

```
etanribergenov@server:~
[etanribergenov@client.etanribergenov.net ~]$ ssh -p 2022 etanribergenov@server.
etanribergenov.net
The authenticity of host '[server.etanribergenov.net]:2022 ([192.168.1.1]:2022)'
can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
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.etanribergenov.net]:2022' (ED25519) to the l
ist of known hosts.
etanribergenov@server.etanribergenov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Apr  5 19:58:02 2023
[etanribergenov@server.etanribergenov.net ~]$
[etanribergenov@server.etanribergenov.net ~]$ ping www.yandex.ru
PING www.yandex.ru (5.255.255.77) 56(84) bytes of data.
64 bytes from 5.255.255.77 (5.255.255.77): icmp_seq=1 ttl=248 time=11.8 ms
64 bytes from 5.255.255.77 (5.255.255.77): icmp_seq=2 ttl=248 time=17.3 ms
^C64 bytes from 5.255.255.77: icmp_seq=3 ttl=248 time=19.9 ms

--- www.yandex.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 11.798/16.316/19.881/3.368 ms
[etanribergenov@server.etanribergenov.net ~]$
```

*Рис. 14. Проверка доступности Интернета на клиенте*

## Внесение изменений в настройки внутреннего окружения виртуальной машины

- Копирование конфигурационных файлов

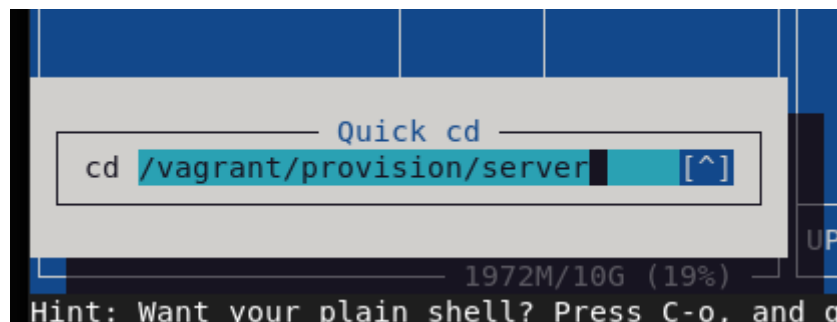


Рис. 15. Переход в каталог для внесения изменений в настройки внутреннего окружения

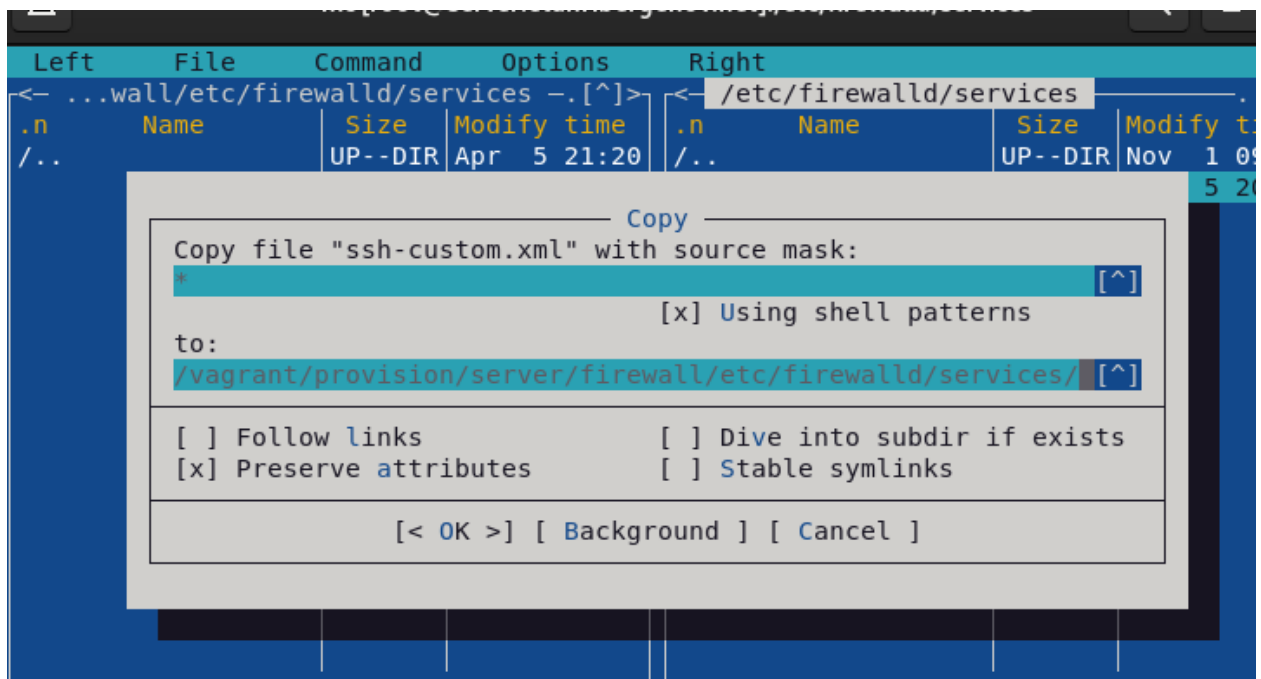
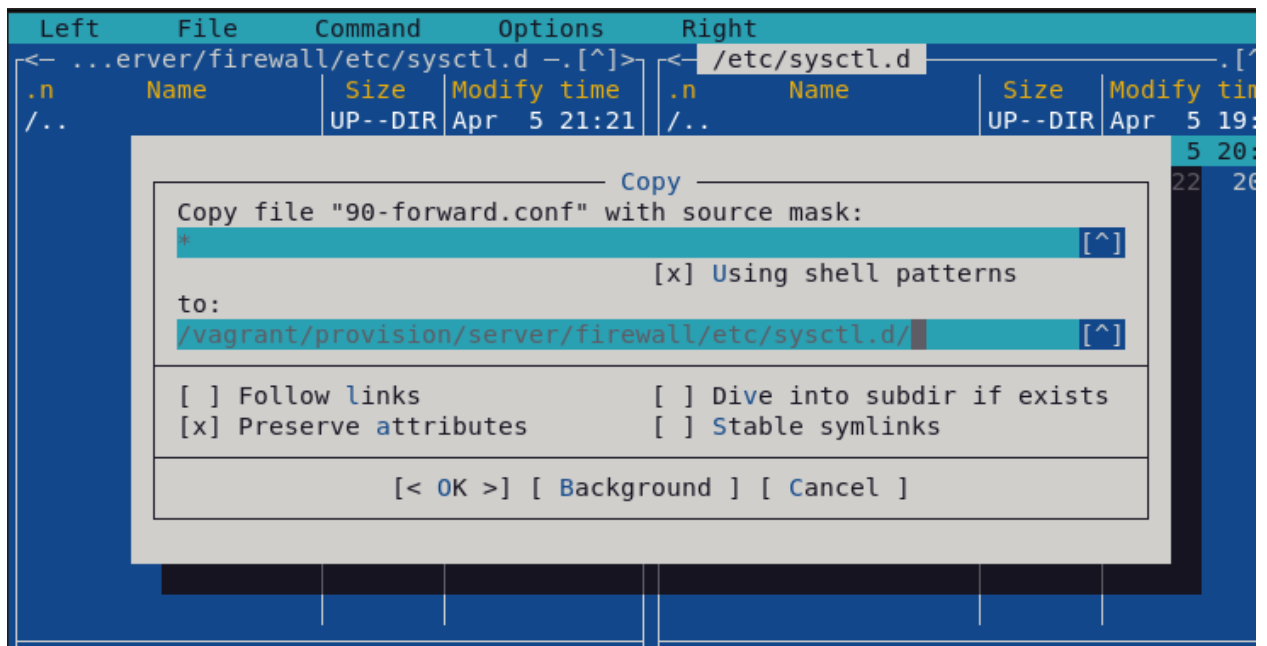


Рис. 16. Копирование конф. файла FirewallD ssh-custom.xml





*Рис. 17. Копирование конф. файла FirewallD перенаправления пакетов*

- Создание скрипта, повторяющего произведённые действия

```
[root@server.etanribergenov.net server]# touch firewall.sh
[root@server.etanribergenov.net server]# chmod +x firewall.sh
[root@server.etanribergenov.net server]#
```

*Рис. 18. Создание исполняемого файла*

```
firewall.sh [----] 21 L:[ 1+11 12/ 14] *(360 / 381b) 0010 0x00A
#!/bin/bash

echo "Provisioning script $0"

echo "Copy configuration files"
cp -R /vagrant/provision/server/firewall/etc/* /etc

echo "Configure masquerading"
firewall-cmd --add-service=ssh-custom --permanent
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload

restorecon -vR /etc
```

*Рис. 19. Скрипт в исполняемом файле*

```
/vagrant/Vagrantfile
server.vm.provision "server dhcp",
  type: "shell",
  preserve_order: true,
  path: "provision/server/dhcp.sh"

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

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

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

*Рис. 20. Добавление записи для скрипта в конф. файле Vagrantfile*