

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 7

дисциплина: Администрирование сетевых подсистем

Расширенные настройки межсетевого экрана

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы

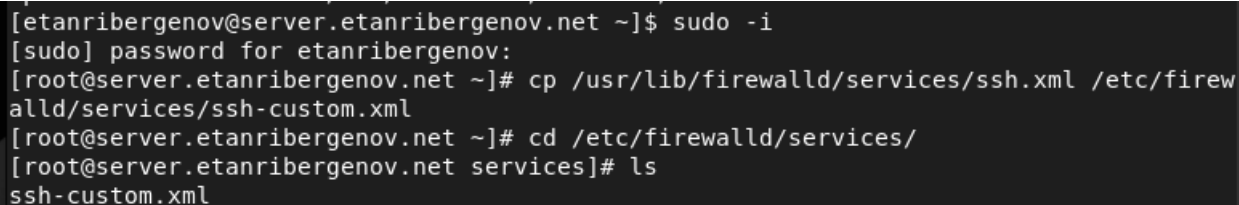
Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Ход работы

1. Создание пользовательской службы firewalld

1. На основе существующего файла описания службы ssh создайте файл с собственным описанием

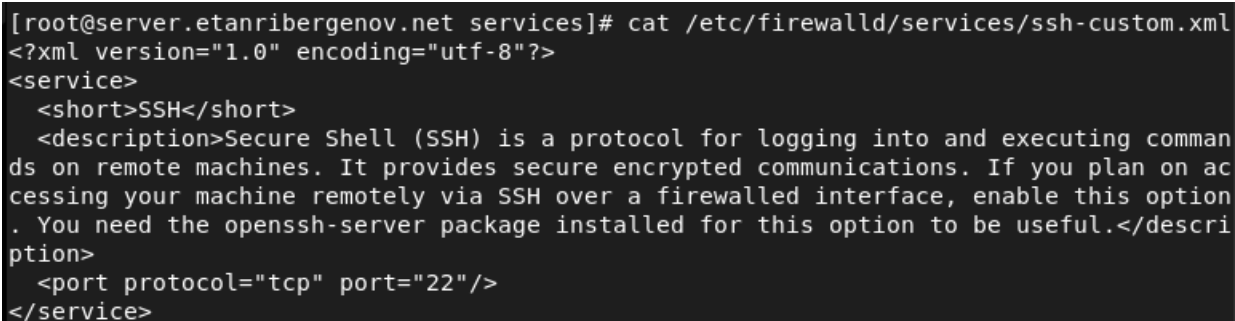
```
cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
```



```
[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. Создание файла с собственным описанием службы ssh на основе существующего

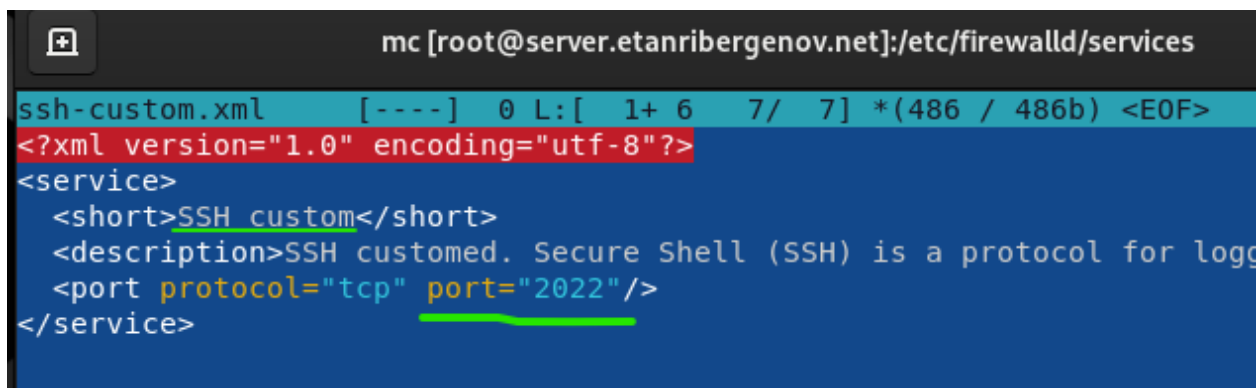
2. Посмотрите содержимое файла службы



```
[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

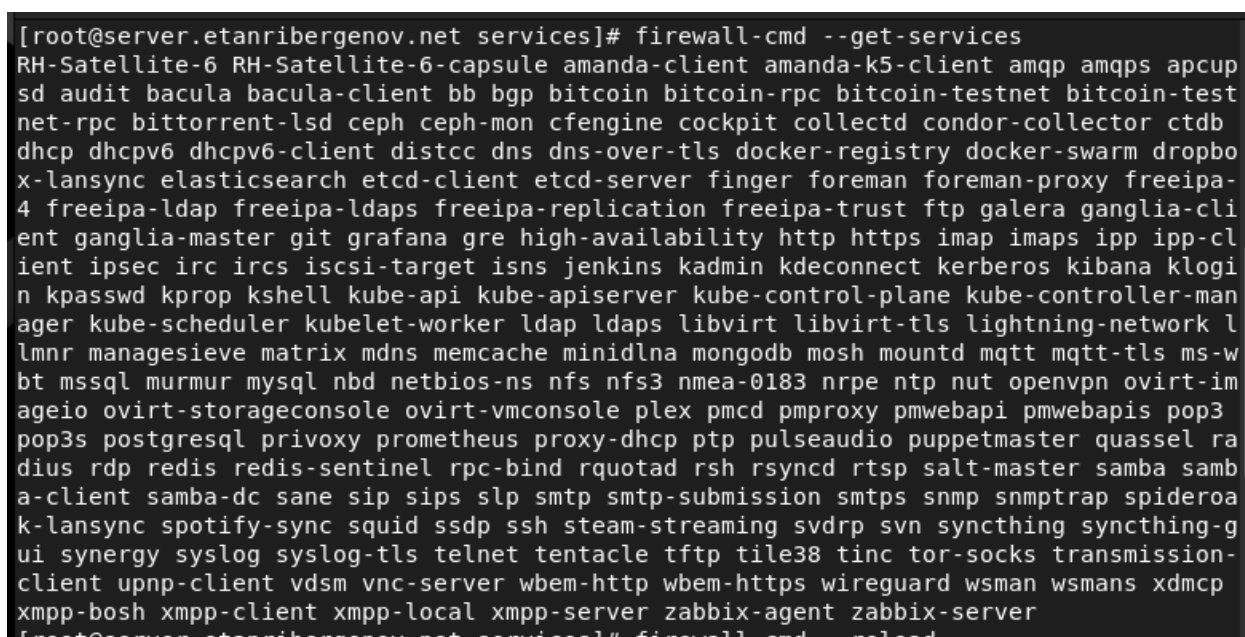
3. Откройте файл описания службы на редактирование и замените порт 22 на новый порт (2022)



```
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

4. Просмотрите список доступных FirewallD служб



```
[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 pmpcd 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 vds vnc-server wbem-http wbem-https wireguard wsmans xdmcp
xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
```

Рис. 4. Список доступных FirewallD служб

Новой службы ещё нет в списке.

5. Перегрузите правила межсетевого экрана с сохранением информации о состоянии и вновь выведите на экран список служб, а также список активных служб

```
[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

В списке доступных появилась служба ssh-custom.

```
[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

Среди них, разумеется, нет нашей созданной службы ssh-custom.

6. Добавьте новую службу в FirewallD и выведите на экран список 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

Новая служба успешно добавлена.

2. Перенаправление портов

1. Организуйте на сервере переадресацию с порта 2022 на порт 22

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

Рис. 9. Организация переадресации порта на сервере

2. На клиенте попробуйте получить доступ по SSH к серверу через порт 2022



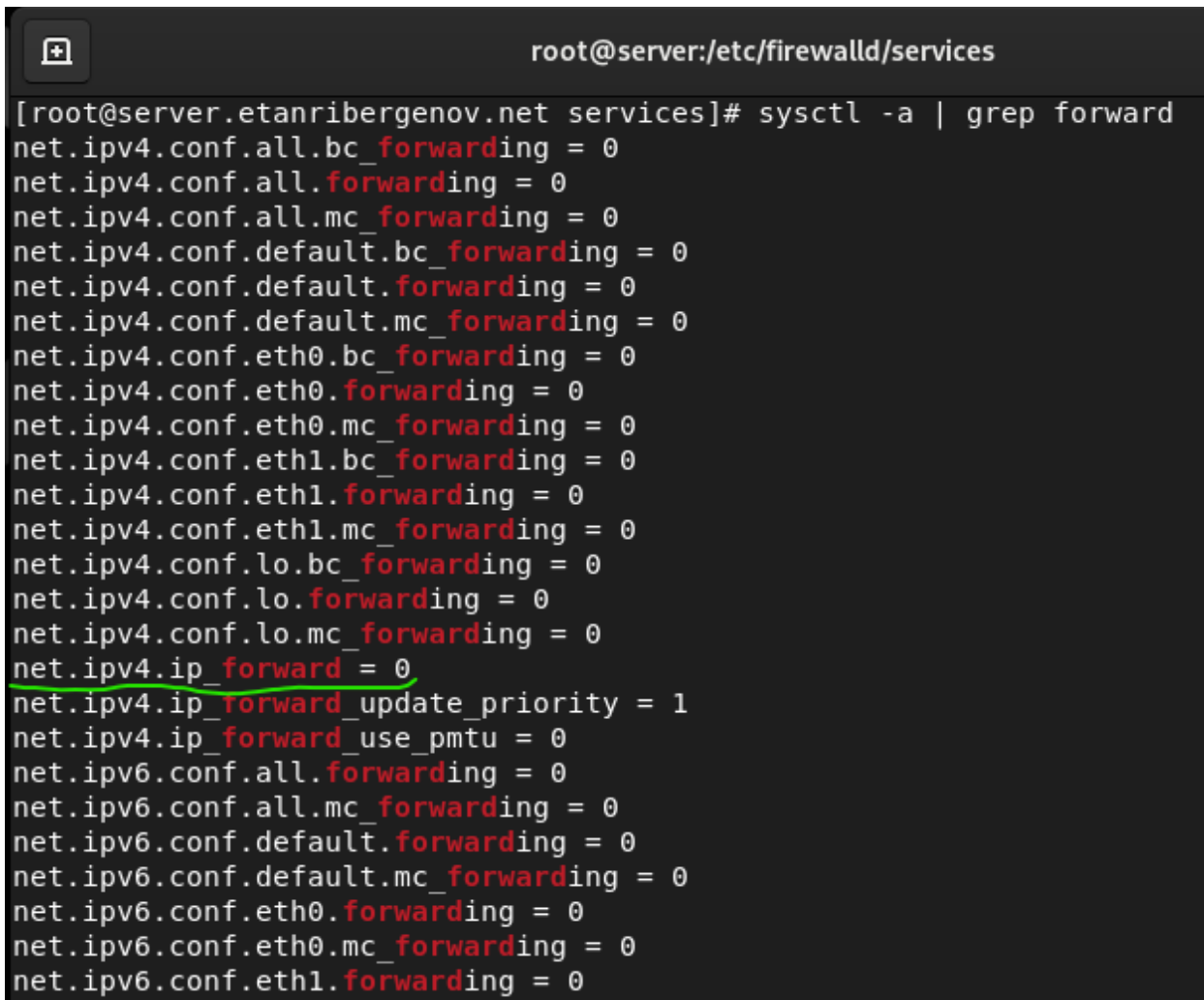
The screenshot shows a terminal window titled 'etanribergenov@server:~'. The user is at a client machine and runs the command 'ssh -p 2022 etanribergenov@server.etanribergenov.net'. The terminal output shows the SSH connection process: it identifies the host, displays the ED25519 key fingerprint (SHA256:zqb0am9bCTBqb0qNzuP7z0xlq0qvGhkHxMkw2sQdblo), asks for confirmation to continue, and receives a 'yes' response. It then prompts for the password, which is entered. The terminal shows the last login time as 'Wed Apr 5 19:58:02 2023' and the user is now logged in as 'etanribergenov@server.etanribergenov.net'.

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

Перед подключением система уведомила о том, что SSH-ключ неизвестен, и спросила уверен ли я, что хочу подключиться. Ввёл yes – доступ был получен.

3. Настройка Port Forwarding и Masquerading

1. На сервере посмотрите, активирована ли в ядре системы возможность 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

Перенаправление IPv4-пакетов не активировано.

2. Включите перенаправление IPv4-пакетов на сервере

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
sysctl -p /etc/sysctl.d/90-forward.conf
```

```
[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

3. Включите маскарадинг на сервере

```
firewall-cmd --zone=public --add-masquerade --permanent
```

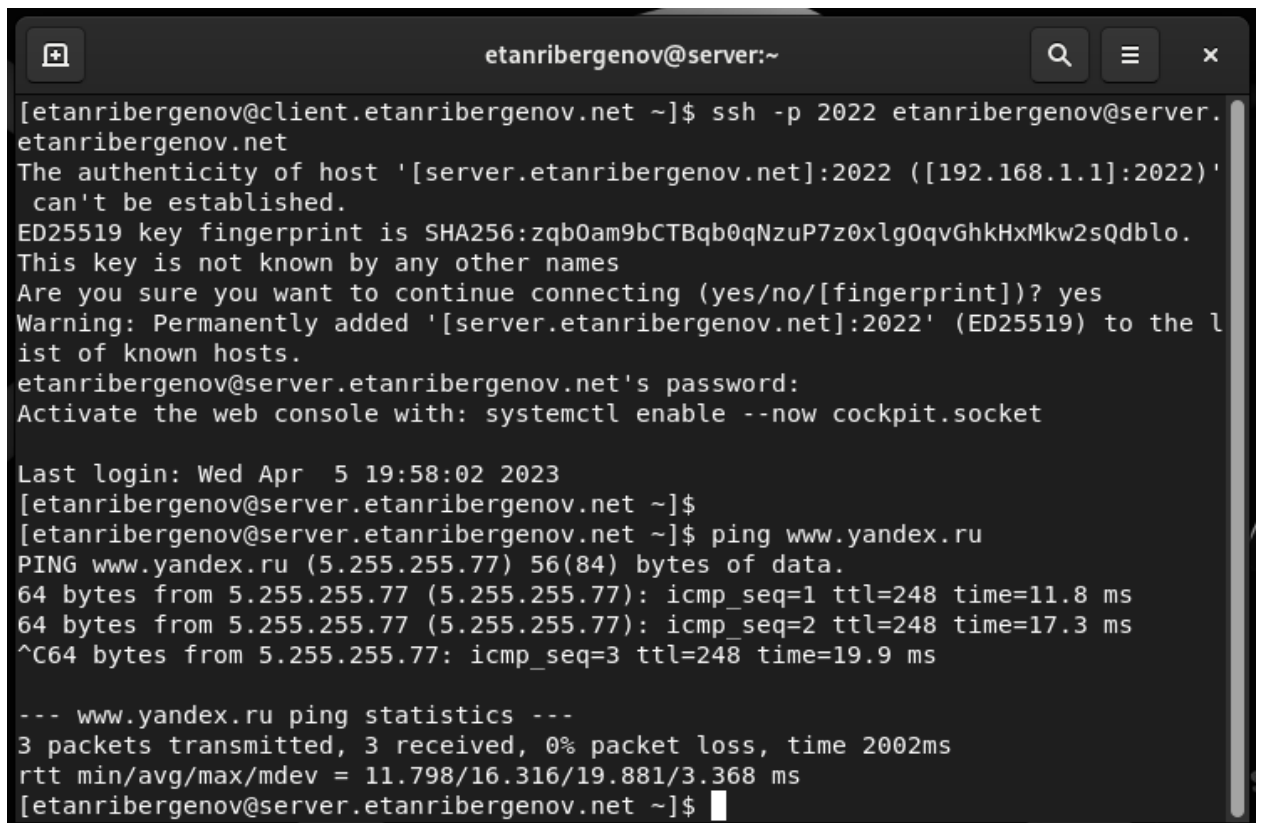
```
firewall-cmd --reload
```

```
[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

4. На клиенте проверьте доступность выхода в Интернет.

Я сделал это при помощи команды ping. Пакеты успешно отправились – Интернет работает.

A terminal window titled 'etanribergenov@server:~' showing a sequence of commands and their outputs. The user connects via SSH to 'server.etanribergenov.net' on port 2022. After a warning about a new host key, the user enters 'yes'. Then, they run 'ping www.yandex.ru', which shows three successful pings with decreasing times. Finally, they run 'ping -c 3 www.yandex.ru' to get summary statistics.

```
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

4. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создайте в нём каталог `firewall`, в который поместите в соответствующие подкаталоги конфигурационные файлы

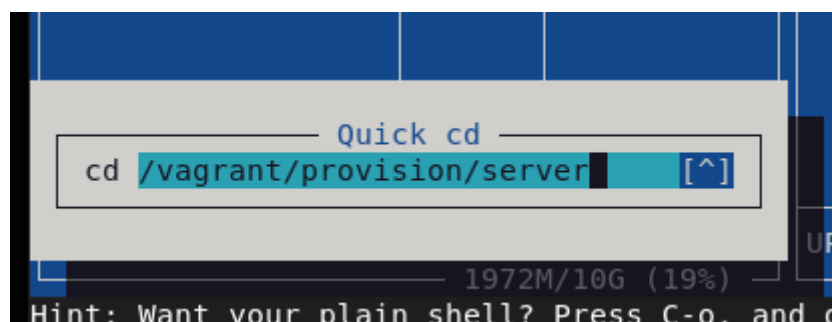


Рис. 15. Переход в каталог для внесения изменений в настройки внутреннего окружения

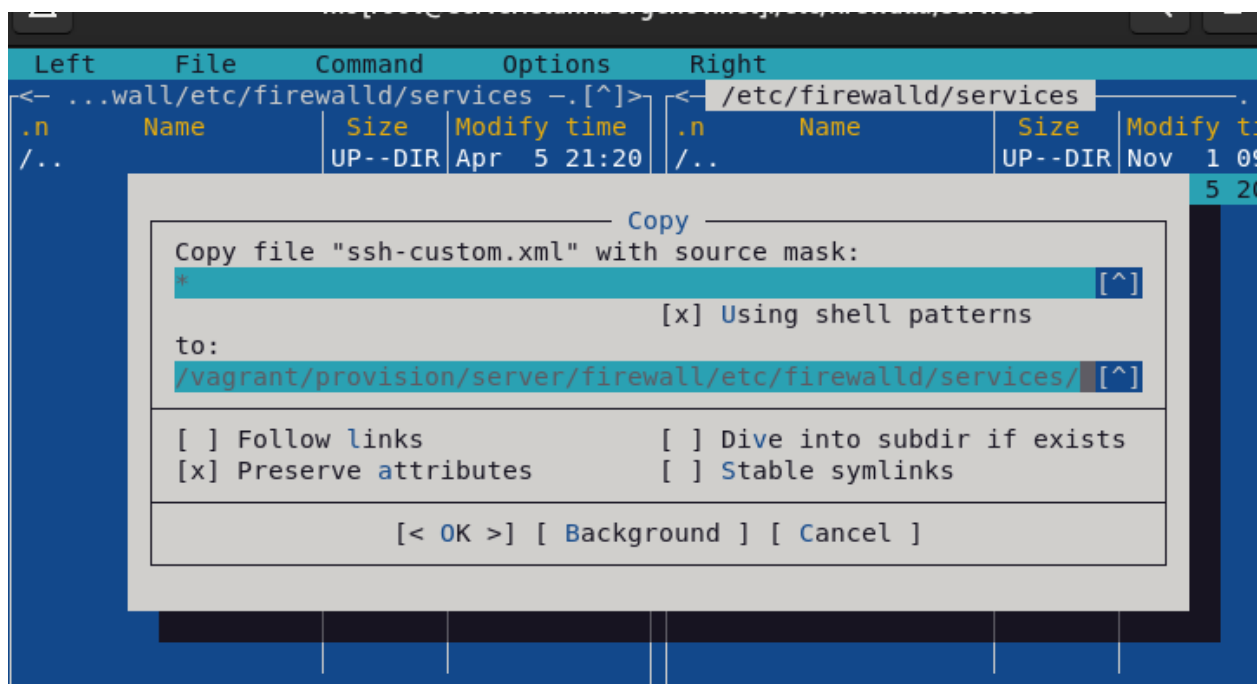


Рис. 16. Копирование конф. файла FirewallD `ssh-custom.xml`

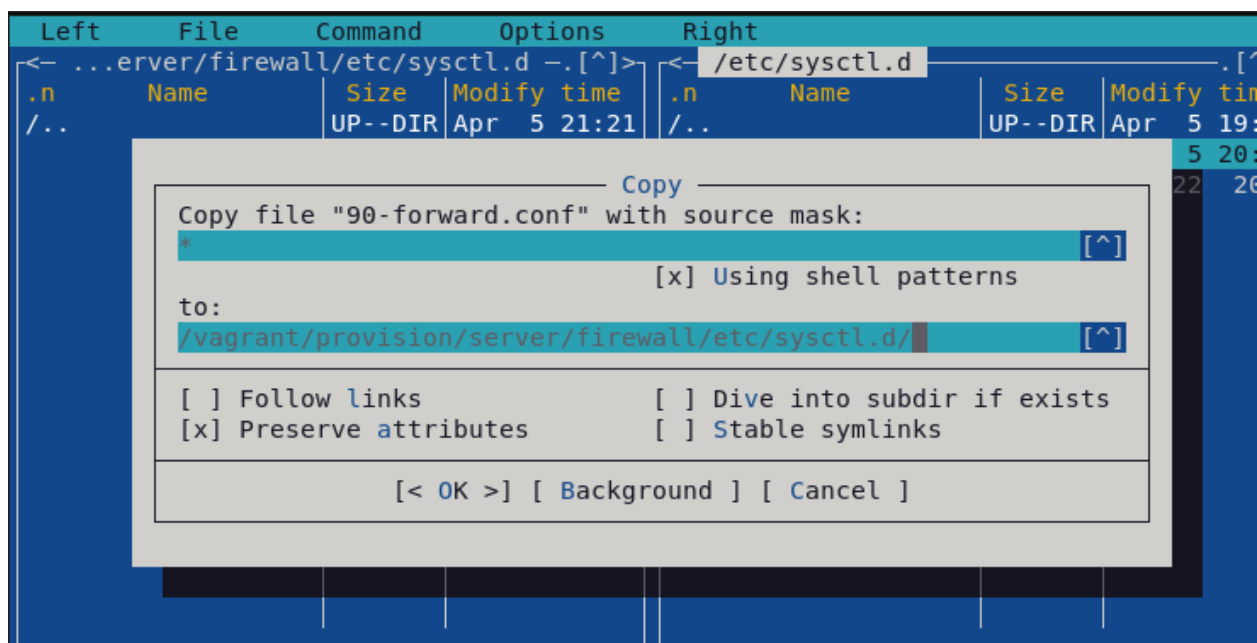


Рис. 17. Копирование конф. файла FirewallD перенаправления пакетов

2. В каталоге /vagrant/provision/server создайте файл firewall.sh

```
[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

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить запись в разделе конфигурации для сервера.

```
/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

Вывод

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

Ответы на контрольные вопросы

1. `/usr/lib/firewalld`
2. `<port protocol="tcp" port="2022"/>`
3. `firewall-cmd --get-services`
4. Маскарад - замена адреса на адрес машины, выполняющей маскарад.
Трансляция адресов - замена адреса на любой указанный.
5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10
6. `firewall-cmd --zone=public --add-masquerade`