

Лабораторная работа №7

Расширенные настройки межсетевого экрана

Студент: БАНСИМБА КЛОДЕЛИ ДЬЕГРА

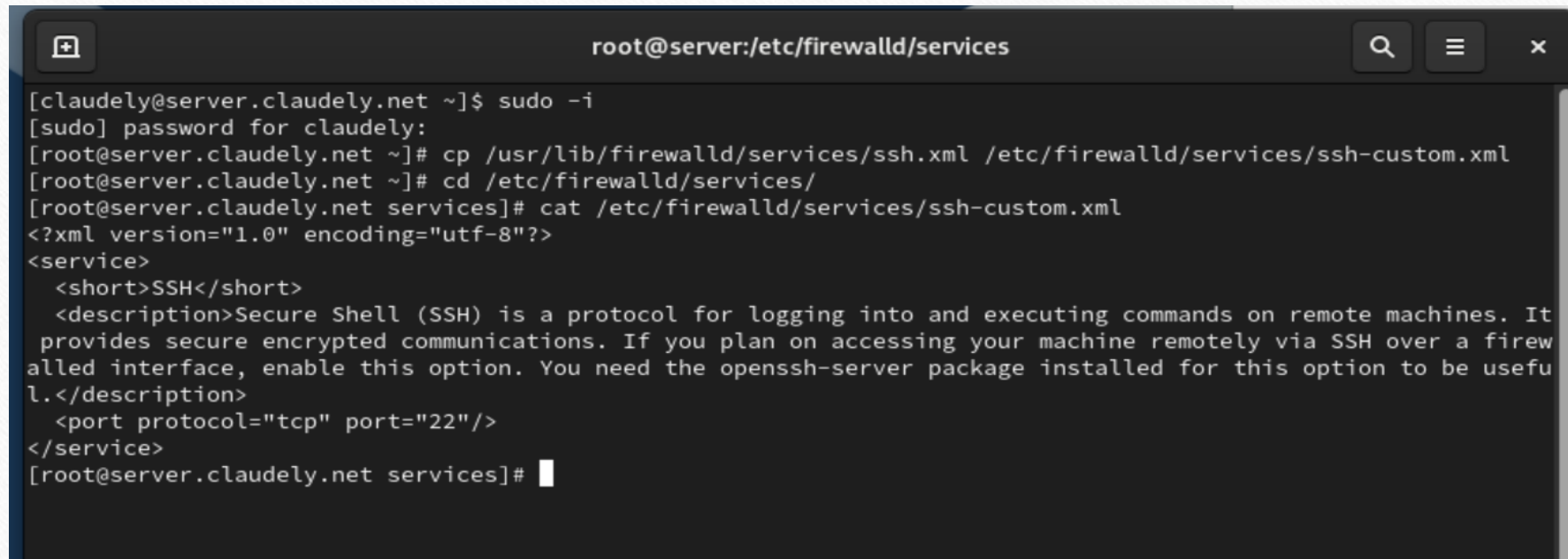
Группа: НПИбд 02–22

дисциплина: Администрирование сетевых подсистем (Lab 7)

Цель работы

Целью данной работы является получение навыков настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

Создание пользовательской службы firewalld

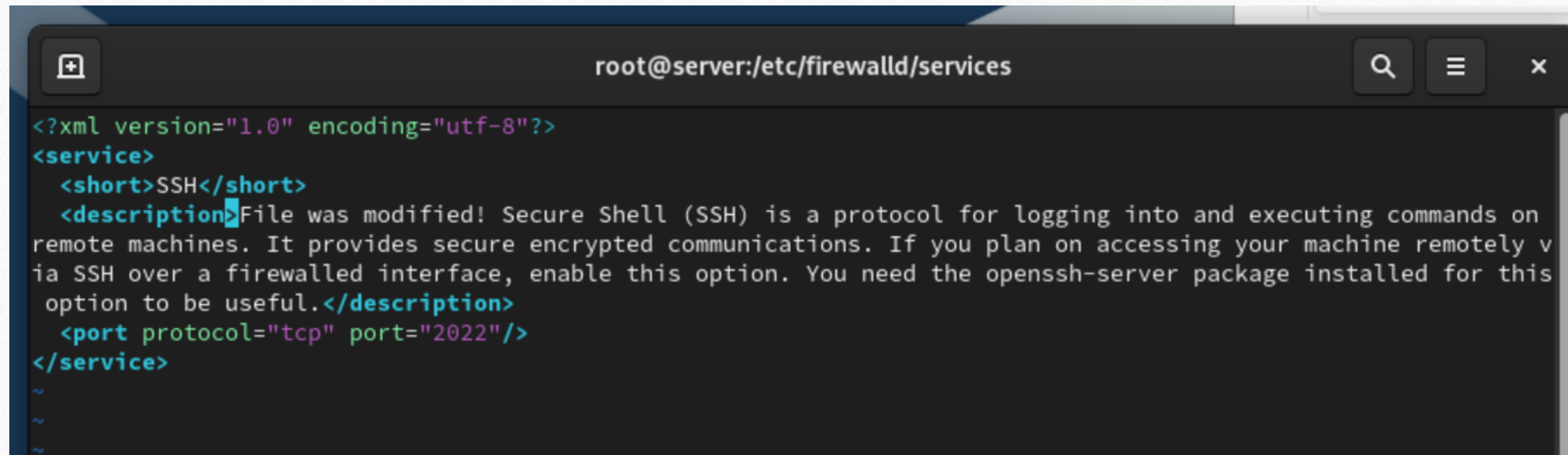


```
root@server:/etc/firewalld/services

[claudely@server.claudely.net ~]$ sudo -i
[sudo] password for claudely:
[root@server.claudely.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.claudely.net ~]# cd /etc/firewalld/services/
[root@server.claudely.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 firew
  alled interface, enable this option. You need the openssh-server package installed for this option to be usefu
  l.</description>
  <port protocol="tcp" port="22"/>
</service>
[root@server.claudely.net services]#
```

Рис. 1.1. Создание файла с собственным описанием на основе существующего файла описания службы ssh.
Просмотр содержимого файла службы.

Создание пользовательской службы firewalld



The screenshot shows a terminal window with the title bar "root@server:/etc/firewalld/services". The terminal content displays an XML configuration for the SSH service. The configuration includes a short name, a description, and a port change from 22 to 2022. The description text includes a notice that the file was modified. The terminal uses a dark theme with syntax highlighting.

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>File was modified! 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 v
ia 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="2022"/>
</service>
~
~
~
```

Рис. 1.2. Открытие файла описания службы на редактирование и замена порта 22 на новый порт (2022), корректирование описания службы для демонстрации, что это модифицированный файл службы.

Создание пользовательской службы firewalld

```
[root@server.claudely.net services]#  
[root@server.claudely.net services]# firewall-cmd --get-services  
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2  
bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testn  
et bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd cond  
or-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls dock  
er-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy fr  
eeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master  
git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs is  
csi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver  
kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep  
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap lda  
ps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcac  
he minidlina mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboar  
d nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy  
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3ne  
tsrv 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-submission smtps snmp snmptls snmptls-trap snm  
ptrap spideroak-lansync spotify-sync squid sssd ssh steam-streaming svdrp svn syncthing syncthing-gui syncthin  
g-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-client v  
dsm 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-client xmpp-local xmpp-server zabbix-agent zabbix-server zerot  
ier  
[root@server.claudely.net services]#
```

Рис. 1.3. Просмотр списка доступных Firewalld служб.

Создание пользовательской службы firewalld

```
[root@server.claudely.net services]# firewall-cmd --reload
success
[root@server.claudely.net services]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2
bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testn
et bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd cond
or-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls dock
er-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy fr
eeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master
git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs is
csi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver
kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodep
ort-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap lda
ps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcac
he minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboar
d nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy
pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3ne
tsrv 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-submission smtps snmp snmptls snmptls-trap snm
ptrap spideroak-lansync spotify-sync squid sssd ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-g
ui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client up
np-client vdsml vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discov
ery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-s
erver zerotier
[root@server.claudely.net services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.claudely.net services]#
```

Рис. 1.4. Перегрузка правил межсетевого экрана с сохранением информации о состоянии, вывод на экран списка служб, а также списка активных служб.

Создание пользовательской службы firewalld

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

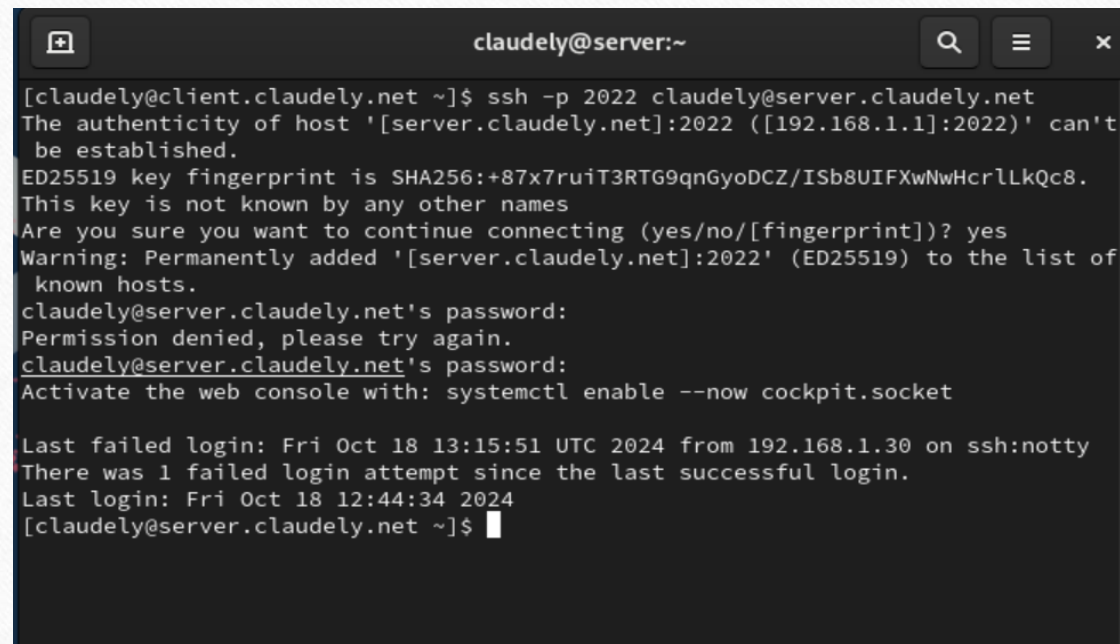
Рис. 1.5. Добавление новой службы в FirewallD и вывод на экран списка активных служб.

Перенаправление портов

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

Рис. 2.1. Организация переадресации на сервере с порта 2022 на порт 22.

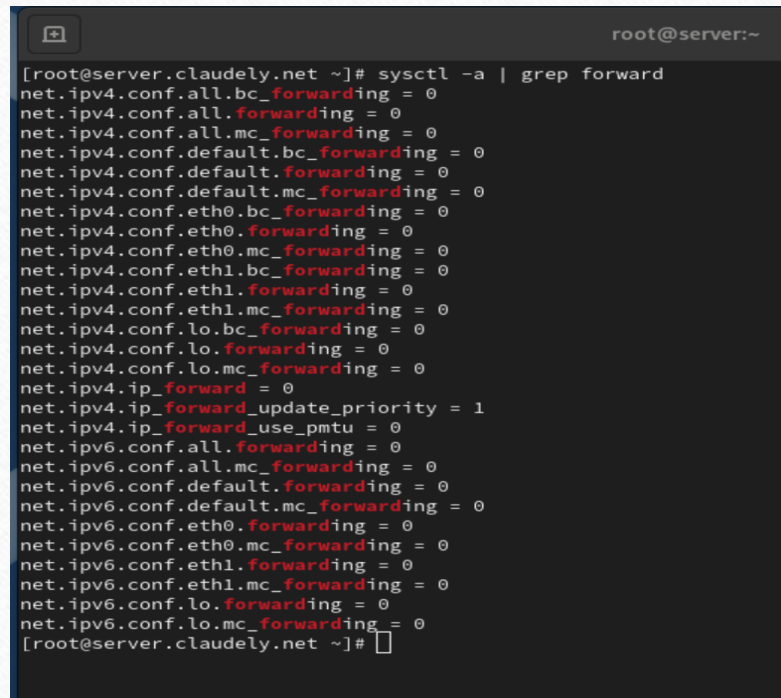
Перенаправление портов

A terminal window titled 'claudely@server:~' with search, menu, and close icons. It shows a user running 'ssh -p 2022 claudely@server.claudely.net' from a client. The terminal displays a warning about host authenticity, a fingerprint, and a confirmation prompt. After entering the password, it shows a 'Permission denied' message and a command to enable Cockpit. It also displays login history for the user 'notty' on the 'ssh' shell.

```
claudely@server:~  
[claudely@client.claudely.net ~]$ ssh -p 2022 claudely@server.claudely.net  
The authenticity of host '[server.claudely.net]:2022 ([192.168.1.1]:2022)' can't  
be established.  
ED25519 key fingerprint is SHA256:+87x7ruiT3RTG9qnGyoDCZ/ISb8UIFXwNwHcrLLkQc8.  
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.claudely.net]:2022' (ED25519) to the list of  
known hosts.  
claudely@server.claudely.net's password:  
Permission denied, please try again.  
claudely@server.claudely.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last failed login: Fri Oct 18 13:15:51 UTC 2024 from 192.168.1.30 on ssh:notty  
There was 1 failed login attempt since the last successful login.  
Last login: Fri Oct 18 12:44:34 2024  
[claudely@server.claudely.net ~]$
```

Рис. 2.2. Попытка получить на клиенте доступ по SSH к серверу через порт 2022.

Настройка Port Forwarding и Masquerading



```
root@server:~  
[root@server.claudely.net ~]# 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  
net.ipv6.conf.eth1.mc_forwarding = 0  
net.ipv6.conf.lo.forwarding = 0  
net.ipv6.conf.lo.mc_forwarding = 0  
[root@server.claudely.net ~]#
```

Рис. 3.1. Просмотр на сервере, активирована ли в ядре системы возможность перенаправления IPv4-пакетов.

Настройка Port Forwarding и Masquerading

```
net.ipv4.conf.eth0.forwarding = 1
[root@server.claudely.net ~]# echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf
[root@server.claudely.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.claudely.net ~]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.claudely.net ~]# firewall-cmd --reload
success
[root@server.claudely.net ~]#
```

Рис. 3.2. Включение перенаправления IPv4-пакетов на сервере и маскардинга на сервере.

Настройка Port Forwarding и Masquerading

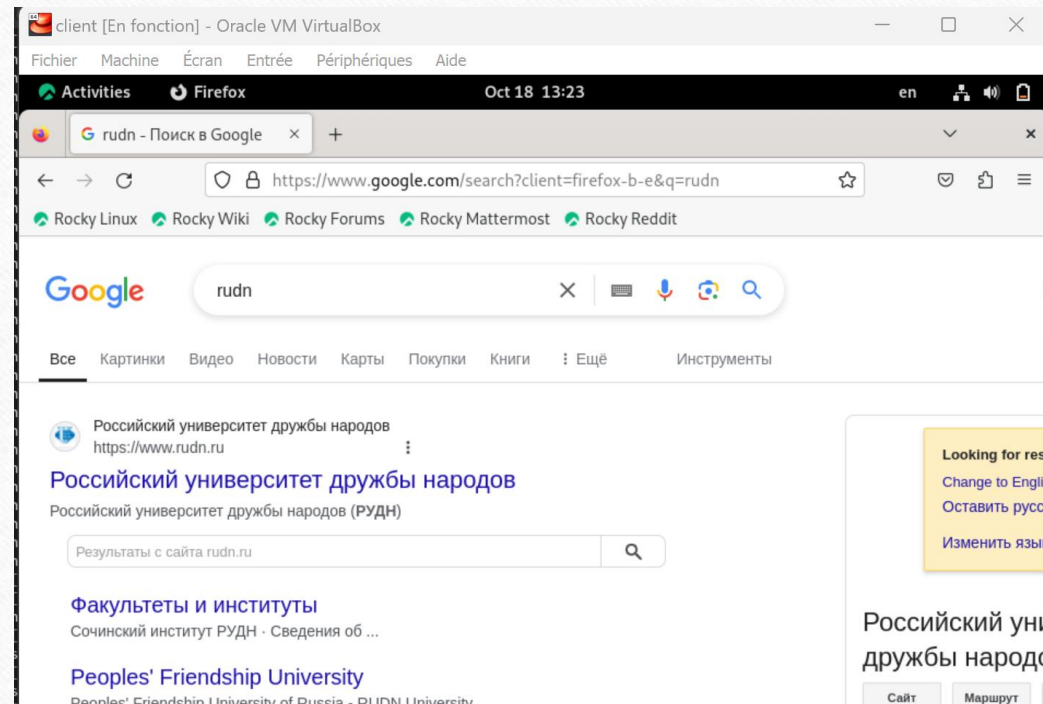


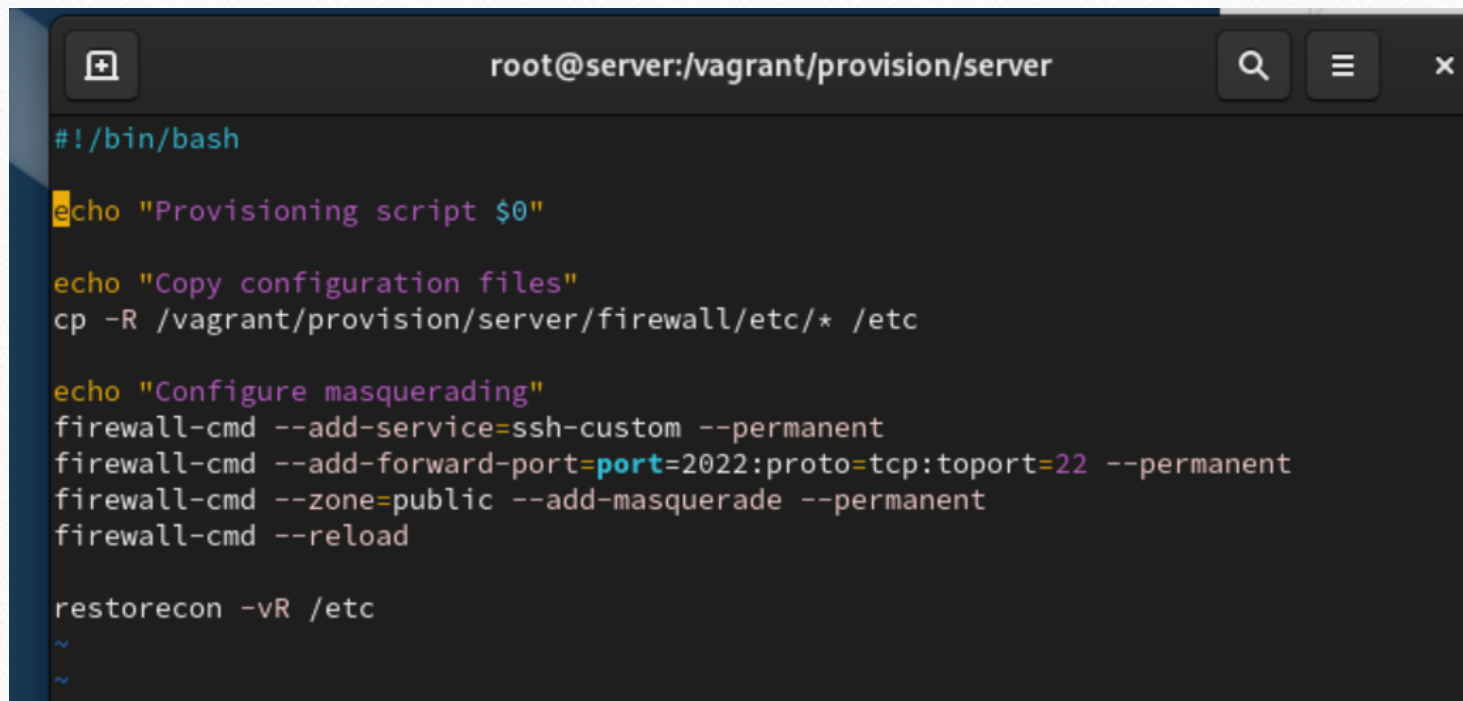
Рис. 3.3. Проверка доступности выхода в Интернет на клиенте.

Внесение изменений в настройки внутреннего окружения виртуальной машины

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

Рис. 4.1. Открытие каталога для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога firewall, в который помещаем в соответствующие подкаталоги конфигурационные файлы FirewallD. Создание в каталоге /vagrant/provision/server файла firewall.sh.

Внесение изменений в настройки внутреннего окружения виртуальной машины

A screenshot of a terminal window with a dark background. The title bar at the top shows 'root@server:/vagrant/provision/server' and standard window controls (search, menu, close). The terminal content shows a series of commands being executed, including 'echo' statements for logging and 'firewall-cmd' commands for configuring SSH access and masquerading. The prompt is '#!/bin/bash'.

```
#!/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. 4.2. Открытие файла на редактирование и прописывание в нём скрипта из лабораторной работы.

Внесение изменений в настройки внутреннего окружения виртуальной машины

Fichier	Modifier	Affichage
		<pre>preserve_order: true, path: "provision/server/dns.sh"</pre>
<u>server.vm.provision</u>		<pre>"server dhcp", type: "shell", preserve_order: true, path: "provision/server/dhcp.sh"</pre>
<u>server.vm.provision</u>		<pre>"server http", type: "shell", preserve_order: true, path: "provision/server/http.sh"</pre>
<u>server.vm.provision</u>		<pre>"server mysql", type: "shell", preserve_order: true, path: "provision/server/mysql.sh"</pre>
<u>server.vm.provision</u>		<pre>"server firewall", type: "shell", preserve_order: true, path: "provision/server/firewall.sh"</pre>

Рис. 4.3. Добавление записи в конфигурационном файле Vagrantfile.

Вывод

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

Спасибо за внимание!