Лабораторная работа № 7. Расширенные настройки межсетевого экрана

Данила Стариков
НПИбд-02-22

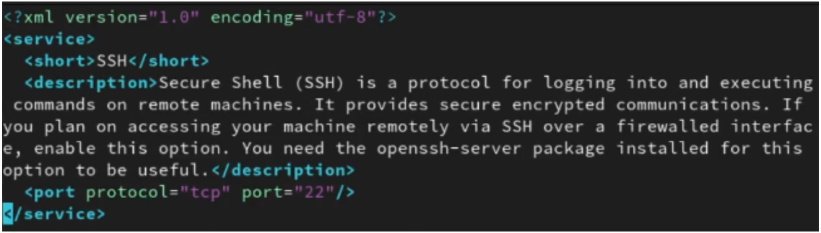
Российский университет дружбы народов имени Патриса Лумумбы

2024

Цель работы

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

Создание пользовательской службы firewalld



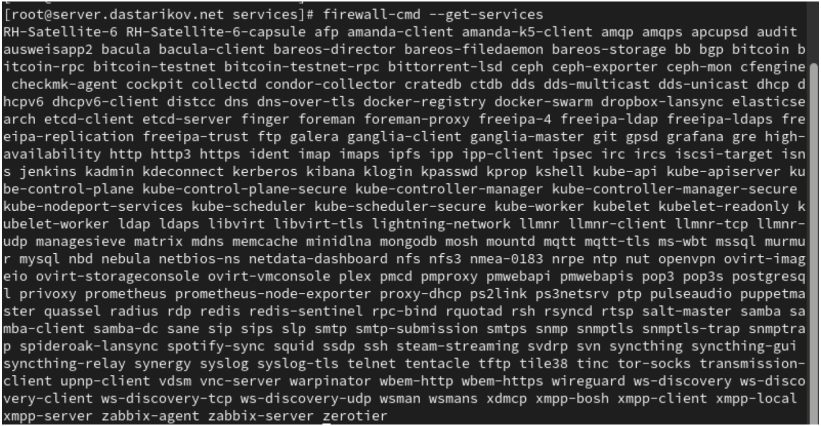
```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing
 commands on remote machines. It provides secure encrypted communications. If
you plan on accessing your machine remotely via SSH over a firewalled interfac
e, enable this option. You need the openssh-server package installed for this
option to be useful.</description>
  <port protocol="tcp" port="22"/>
</service>
```

Рис.: Содержимое файла ssh.xml по умолчанию

Создание пользовательской службы firewalld

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Modified SSH with port 2022.</description>
  <port protocol="tcp" port="2022"/>
</service>
```

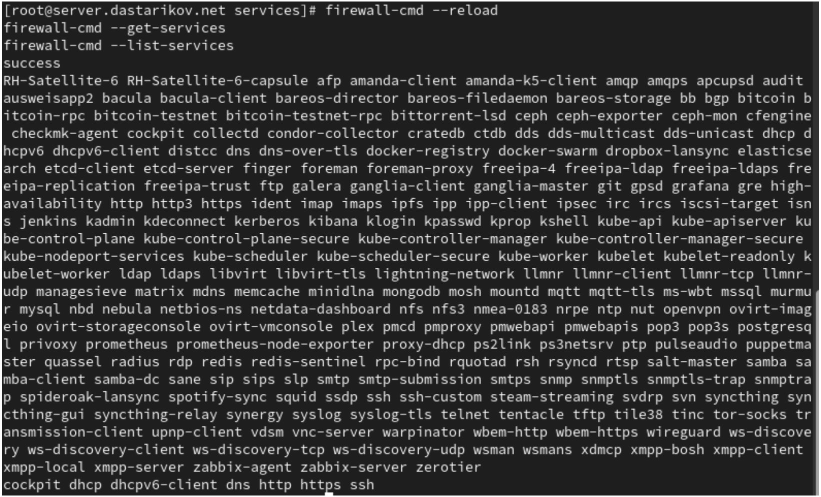
Создание пользовательской службы firewalld



```
[root@server.dastarikov.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 b
itcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine
 checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp d
hcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticse
arch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps fre
eipa-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 iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku
be-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly k
ubelet-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 murmu
r mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imag
eio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresq
l privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetma
ster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba sa
mba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptra
p spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui
syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-
client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discovery ws-disco
very-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local
xmpp-server zabbix-agent zabbix-server zerotier
```

Рис.: Список доступных служб.

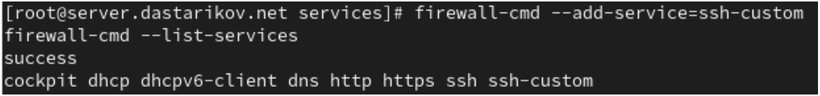
Создание пользовательской службы firewalld



```
[root@server.dastarikov.net services]# firewall-cmd --reload
firewall-cmd --get-services
firewall-cmd --list-services
success
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 b
itcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine
 checkmk-agent cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp d
hcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticse
arch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps fre
eipa-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 iscsi-target isn
s jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver ku
be-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-secure
kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly k
ubelet-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 murmu
r mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imag
eio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresq
l privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetma
ster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba sa
mba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptra
p spideroak-lansync spotify-sync squid ssdp ssh ssh-custom steam-streaming svdrp svn syncthing syn
cthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks tr
ansmission-client upnp-client vdsm vnc-server warpinator wbem-http wbem-https wireguard ws-discove
ry ws-discovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client
xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
cockpit dhcp dhcpv6-client dns http https ssh
```

Рис.: Список доступных и активных служб после обновления.

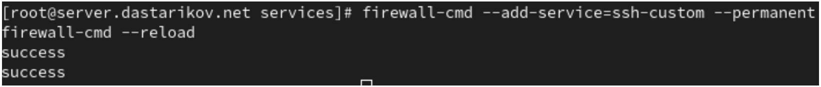
Создание пользовательской службы firewalld



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

Рис.: Список активных служб после добавления ssh-custom.

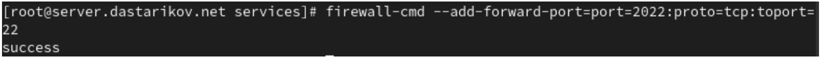
Создание пользовательской службы firewalld



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

Рис.: Сохранение информации о состоянии и перезагрузка службы firewalld.

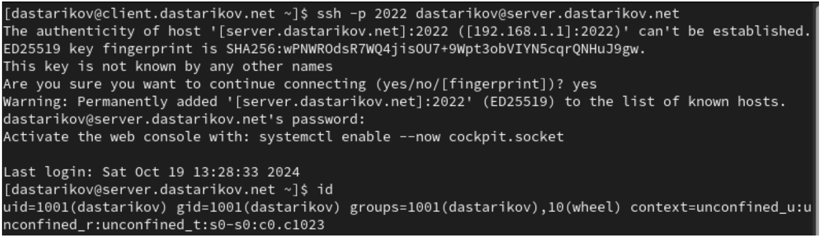
Перенаправление портов



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

Рис.: Успешное добавление переадресации с порта 2022 на порт 22.

Перенаправление портов

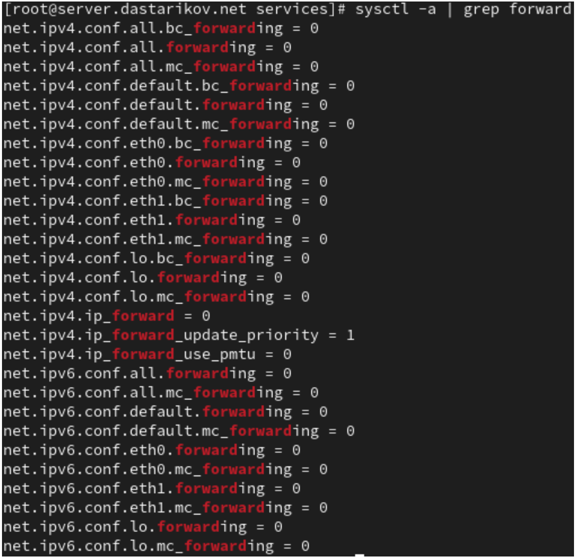


```
[dastarikov@client.dastarikov.net ~]$ ssh -p 2022 dastarikov@server.dastarikov.net
The authenticity of host '[server.dastarikov.net]:2022 ([192.168.1.1]:2022)' can't be established.
ED25519 key fingerprint is SHA256:wPNWROdsR7WQ4jisOU7+9Wpt3obVIYN5cqrQNHuJ9gw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[server.dastarikov.net]:2022' (ED25519) to the list of known hosts.
dastarikov@server.dastarikov.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Oct 19 13:28:33 2024
[dastarikov@server.dastarikov.net ~]$ id
uid=1001(dastarikov) gid=1001(dastarikov) groups=1001(dastarikov),10(wheel) context=unconfined_u:u
nconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис.: Получение доступа по SSH на клиенте.

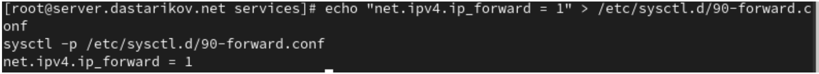
Настройка Port Forwarding и Masquerading



```
[root@server.dastarikov.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
net.ipv6.conf.eth1.mc_forwarding = 0
net.ipv6.conf.lo.forwarding = 0
net.ipv6.conf.lo.mc_forwarding = 0
```

Рис.: Список параметров, связанных с перенарпавлением пакетов.

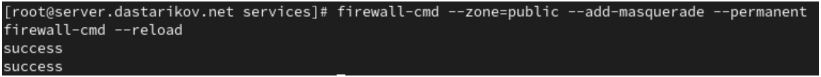
Настройка Port Forwarding и Masquerading



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

Рис.: Включение перенапрвления IPv4пакетов на сервере.

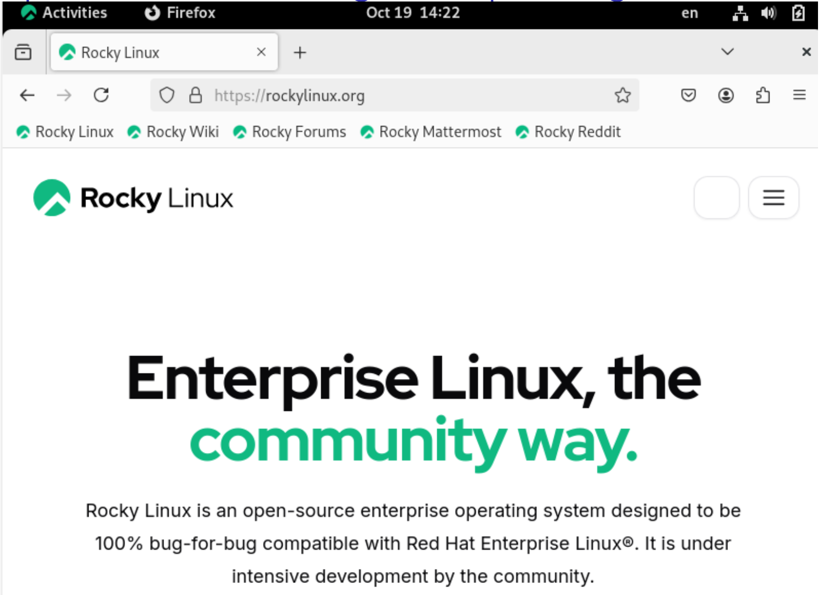
Настройка Port Forwarding и Masquerading



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

Рис.: Включение маскарадинга на сервере.

Настройка Port Forwarding и Masquerading

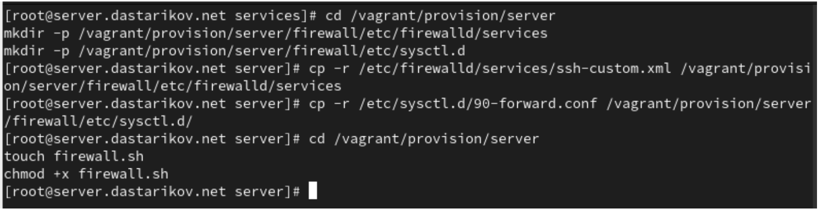


Enterprise Linux, the community way.

Rocky Linux is an open-source enterprise operating system designed to be 100% bug-for-bug compatible with Red Hat Enterprise Linux®. It is under intensive development by the community.

Рис.: Проверка доступности Интернета на клиенте.

Внесение изменений в настройки внутреннего окружения виртуальной машины



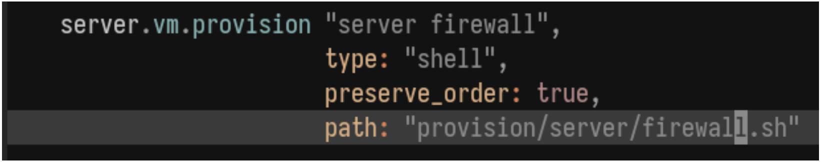
```
[root@server.dastarikov.net services]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.dastarikov.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provisi
on/server/firewall/etc/firewalld/services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

Рис.: Создание каталога с конфигурацией firewalld.

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
#!/bin/shell
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
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



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

Рис.: Изменение Vagrantfile.

Выводы

- В результате выполнения лабораторной работы продолжили изучать настройки межсетевого экрана в Linux, настроили переадресацию портов и Masquerading.