Администрирование сетевых подсистем

Расширенные настройки межсетевого экрана (Лабораторная работа №7)

Заур Мустафаев

16 декабрь 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Получение практических навыков настройки межсетевого экрана в Linux, включая создание пользовательских служб firewalld, перенаправление портов, настройку Port Forwarding и Masquerading.

Выполнение лабораторной работы

Создание файла службы

```
[root@server.zmustafaev.net ~]# cp /usr/lib/firewalld/services/ssh.xml /etc/firewalld/services/ssh-custom.xml
[root@server.zmustafaev.net ~]# cd /etc/firewalld/services/
[root@server.zmustafaev.net services]# cat 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 encrypte
d 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>
[root@server.zmustafaev.net services]#
```

Рис. 1: Просмотр содержимого ssh-custom.xml

Анализ структуры файла службы

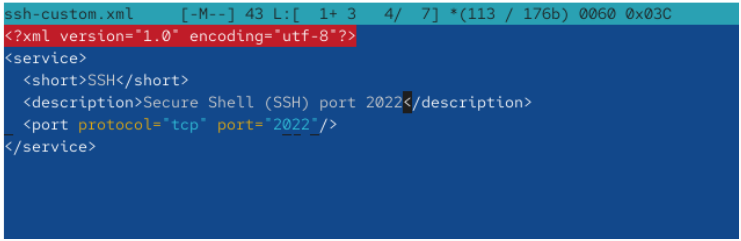

Рис. 2: Редактирование файла ssh-custom.xml

Модификация параметров службы

```
s freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https id
ent imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpas
swd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-s
ecure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvir
t libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp manageseive matrix mdns memcache minecraft minidlna mndp mongodb
 mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nm
ea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius r
adsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-col
lection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ss
h statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing synct
hing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client tu
rn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host
 ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-ja
va-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
[root@server.zmustafaev.net services]# firewall-cmd --reload
success
[root@server.zmustafaev.net services]# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet audit
 auswelsapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-t
estnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit collectd condor-col
lector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls docker-registry docke
r-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldap
s freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https id
ent imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpas
swd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-controller-manager kube-controller-manager-s
ecure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvir
t libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp manageseive matrix mdns memcache minecraft minidlna mndp mongodb
 mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nm
ea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3
 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius r
adsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane settlers-history-col
lection sip sips slimevr slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ss
h ssh-custom statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn sync
thing syncthing-gui syncthing-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmissio
n-client turn turns upnp-client vdsm vnc-server vrrp warpinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-disc
overy-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agen
t zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
[root@server.zmustafaev.net services]#
```

Рис. 3: Список доступных служб firewalld

Активация пользовательской службы

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

Рис. 4: Добавление и активация службы ssh-custom

Настройка Port Forwarding

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

Рис. 5: Настройка перенаправления портов

Проверка SSH-подключения

```
[zmustafaev@client.zmustafaev.net ~]$ ssh -p 2022 zmustafaev@server.zmustafaev.n
et
The authenticity of host '[server.zmustafaev.net]:2022 ([192.168.1.1]:2022)' can
't be established.
ED25519 key fingerprint is SHA256:n0w0vphoobfpKiXoFhmCpcTAKAVt01RYFK5Kxnw0XTU.
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.zmustafaev.net]:2022' (ED25519) to the list
of known hosts.
zmustafaev@server.zmustafaev.net's password:
Web console: https://server.zmustafaev.net:9090/ or https://10.0.2.15:9090/

Last login: Tue Dec 16 14:09:29 2025
[zmustafaev@server.zmustafaev.net ~]$
[zmustafaev@server.zmustafaev.net ~]$
logout
Connection to server.zmustafaev.net closed.
[zmustafaev@client.zmustafaev.net ~]$
```

Рис. 6: Подключение по SSH через порт 2022

Настройка Masquerading

Включение Masquerading

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

Проверка выхода в Интернет

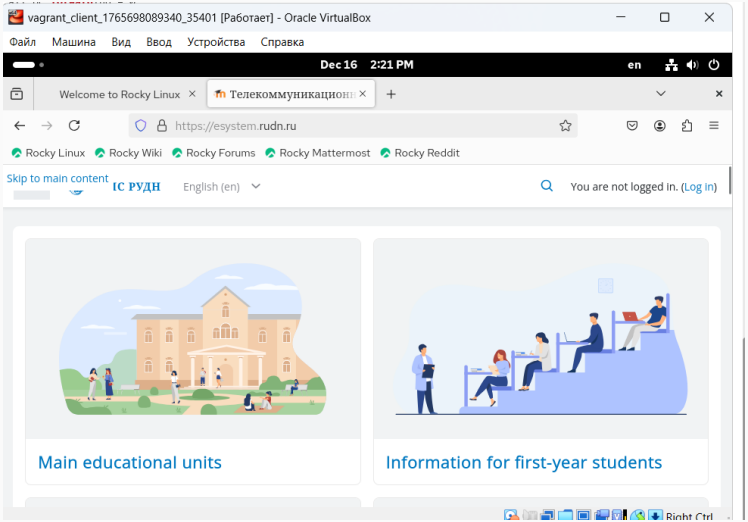

Рис. 8: Проверка выхода в Интернет

Скрипт автоматизации

Vagrantfile | mysql.sh | firewall.sh

```
#!/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. 9: Скрипт firewall.sh

Выводы по проделанной работе

Вывод

В ходе лабораторной работы была выполнена расширенная настройка межсетевого экрана firewalld. Создана пользовательская служба SSH с изменённым портом, реализовано перенаправление портов, включены механизмы Port Forwarding и Masquerading. Настройки успешно проверены и автоматизированы для повторного развёртывания в среде Vagrant.