

Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Заур Мустафеев

Содержание

1	Цель работы	5
2	Выполнение работы	6
2.1	Создание пользовательской службы firewalld	6
2.2	Перенаправление портов	9
2.3	Настройка Port Forwarding и Masquerading	9
2.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	11
3	Вывод	13
4	Контрольные вопросы	14
5	Список литературы	16

Список иллюстраций

2.1	Просмотр содержимого ssh-custom.xml	7
2.2	Редактирование файла ssh-custom.xml	7
2.3	Список доступных служб firewalld	8
2.4	Перезагрузка firewalld и проверка служб	8
2.5	Настройка перенаправления портов	9
2.6	Подключение к серверу по SSH через порт 2022	9
2.7	Включение IP forwarding и masquerading	10
2.8	Выход в сеть Интернет	11
2.9	firewall.sh	12

Список таблиц

1 Цель работы

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

2 Выполнение работы

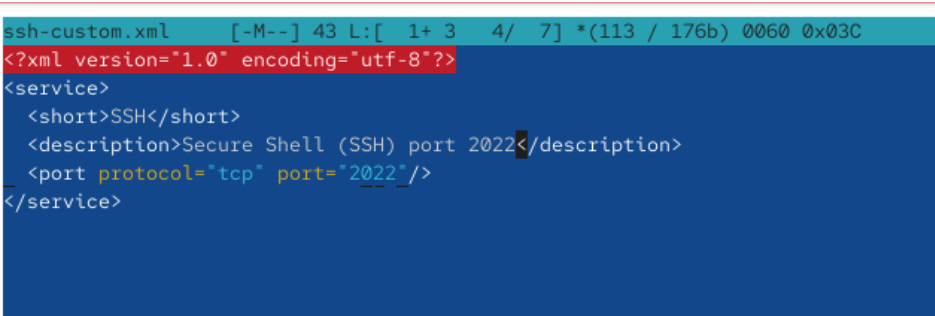
2.1 Создание пользовательской службы firewalld

1. Выполнен вход в рабочий каталог проекта и запущена виртуальная машина **server**. После загрузки системы выполнен переход в режим суперпользователя для выполнения административных операций.
2. На основе стандартного файла описания службы **ssh** создан пользовательский файл службы **ssh-custom.xml**. Файл был скопирован из системного каталога `/usr/lib/firewalld/services/` в каталог пользовательских служб `/etc/firewalld/services/`.
3. Просмотрено содержимое файла `ssh-custom.xml`. Файл представляет собой XML-описание службы `firewalld` и включает:
 - декларацию версии XML;
 - корневой элемент `<service>`;
 - элемент `<short>`, содержащий краткое имя службы;
 - элемент `<description>`, описывающий назначение службы;
 - элемент `<port>`, задающий протокол и номер порта, разрешённого для данной 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 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>
[root@server.zmustafaev.net services]#
```

Рис. 2.1: Просмотр содержимого ssh-custom.xml

4. Файл службы был открыт для редактирования. В нём изменён номер порта с **22** на **2022**, а описание службы скорректировано для указания, что используется модифицированная версия службы SSH.



```
ssh-custom.xml [-M--] 43 L:[ 1+ 3 4/ 7] *(113 / 176b) 0060 0x03C
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) port 2022</description>
  <port protocol="tcp" port="2022"/>
</service>
```

Рис. 2.2: Редактирование файла ssh-custom.xml

5. Получен список доступных служб firewalld. Установлено, что созданная пользовательская служба на данном этапе ещё не активна.

```

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 managesieve matrix ndns memcache minecraft minidlna mnpd mongod
mosh mountd mpd mqtqt mqtqt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboards nfs nfs3 nm
ea-0183 nrpe ntp ntp ntp opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmpd pmpoxy pwebapi pwebapis 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 vdsu vnc-server vrrp warpinator wben-http wben-https wireguard ws-discovery ws-discovery-client ws-discovery-host
ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsmn 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
ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoi
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-qtcp 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 managesieve matrix ndns memcache minecraft minidlna mnpd mongod
mosh mountd mpd mqtqt mqtqt-tls ms-wbt mssql murmur mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboards nfs nfs3 nm
ea-0183 nrpe ntp ntp ntp opentelemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmpd pmpoxy pwebapi pwebapis 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 vdsu vnc-server vrrp warpinator wben-http wben-https wireguard ws-discovery ws-discovery-client ws-disc
overy-host ws-discovery-tcp ws-discovery-udp wsdd wsdd-http wsmn 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. 2.3: Список доступных служб firewalld

6. Выполнена перезагрузка правил межсетевого экрана с сохранением теку-щего состояния. После перезагрузки повторно выведен список служб, в котором появилась служба **ssh-custom**, однако она не была активирована.

```

[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. 2.4: Перезагрузка firewalld и проверка служб

7. Пользовательская служба **ssh-custom** добавлена в активные службы теку-щей зоны. После этого выполнено постоянное добавление службы с сохра-нением конфигурации и повторная перезагрузка firewalld.

2.2 Перенаправление портов

1. На сервере настроено перенаправление входящих TCP-соединений с порта **2022** на стандартный порт службы SSH **22**.

```
[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. 2.5: Настройка перенаправления портов

2. На клиентской виртуальной машине выполнена попытка подключения к серверу по SSH через порт **2022**. Подключение прошло успешно, что подтверждает корректность настройки перенаправления портов.

```
[zmustafaev@client.zmustafaev.net ~]$ ssh -p 2022 zmustafaev@server.zmustafaev.net  
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. 2.6: Подключение к серверу по SSH через порт 2022

2.3 Настройка Port Forwarding и Masquerading

1. Проверено состояние параметров ядра, отвечающих за пересылку IPv4-пакетов. Установлено, что перенаправление пакетов по умолчанию отключено.

2. Включена поддержка перенаправления IPv4-пакетов путём добавления соответствующей настройки в файл `/etc/sysctl.d/90-forward.conf` и применения параметров ядра.
3. Для внешнего сетевого интерфейса включён режим маскарadingа, обеспечивающий трансляцию сетевых адресов. После внесения изменений выполнена перезагрузка правил межсетевого экрана.

```
[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]#
```

Рис. 2.7: Включение IP forwarding и masquerading

4. На клиентской виртуальной машине проверена доступность выхода в сеть Интернет. Доступ подтверждён, что свидетельствует о корректной работе настроек Port Forwarding и Masquerading.

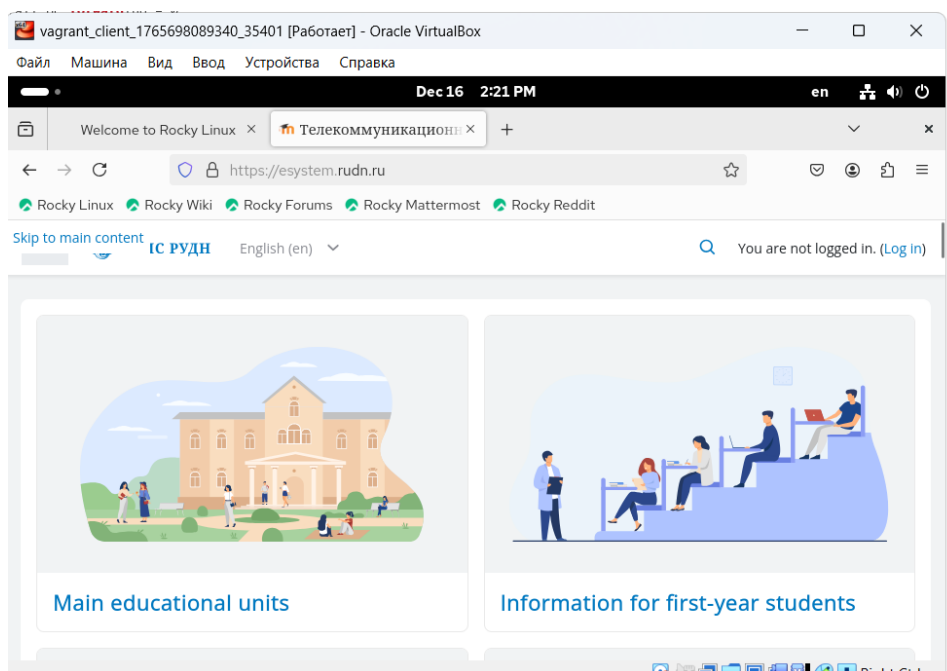


Рис. 2.8: Выход в сеть Интернет

2.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. В каталоге `/vagrant/provision/server` создана структура каталогов для хранения конфигурационных файлов FirewallD и параметров ядра.
2. В соответствующие подкаталоги помещены конфигурационные файлы пользовательской службы `ssh-custom.xml` и файл настроек ядра `90-forward.conf`.
3. В каталоге `/vagrant/provision/server` создан исполняемый файл `firewall.sh`, предназначенный для автоматизации настройки межсетевого экрана, применения перенаправления портов и маскарadingа при развёртывании виртуальной машины.



The image shows a terminal window with three tabs: 'Vagrantfile', 'mysql.sh', and 'firewall.sh'. The 'firewall.sh' tab is active, displaying a shell script. The script starts with a shebang line, followed by echo statements for provisioning and copying files. It then uses 'cp' to copy files from a specific path to '/etc'. Another echo statement precedes a series of 'firewall-cmd' commands: adding a custom service, adding a forward port (2022 to 22), adding masquerade, and reloading. The script ends with a 'restorecon' command.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Copy configuration files"
4  cp -R /vagrant/provision/server/firewall/etc/* /etc
5  echo "Configure masquerading"
6  firewall-cmd --add-service=ssh-custom --permanent
7  firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22 --permanent
8  firewall-cmd --zone=public --add-masquerade --permanent
9  firewall-cmd --reload
10 restorecon -vR /etc
```

Рис. 2.9: firewall.sh

3 Вывод

В ходе работы была создана и настроена пользовательская служба **firewalld** на основе стандартной службы SSH. Выполнена модификация конфигурации с изменением порта, произведена активация службы и проверка её работы. Реализовано перенаправление портов, включены механизмы **Port Forwarding** и **Masquerading**, что обеспечило корректную маршрутизацию и доступ клиентов к внешней сети. Дополнительно подготовлены файлы и скрипт автоматизации для применения настроек в среде Vagrant.

4 Контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

Пользовательские файлы firewalld хранятся в каталоге `/etc/firewalld/`, в частности описания служб размещаются в `/etc/firewalld/services/`.

2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

Для указания порта необходимо добавить строку
`<port protocol="tcp" port="2022"/>`.

3. Какая команда позволяет перечислить все службы, доступные в настоящее время на вашем сервере?

Для вывода списка всех доступных служб используется команда `firewall-cmd --get-services`.

4. В чем разница между трансляцией сетевых адресов (NAT) и маскарadingом (masquerading)?

NAT предполагает статическое сопоставление внутренних и внешних IP-адресов, тогда как маскарading является динамической формой NAT и автоматически подставляет внешний IP-адрес интерфейса, что удобно при использовании изменяемых адресов.

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

Для этого используется команда перенаправления портов с указанием целевого адреса и порта службы SSH.

6. Какая команда используется для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public?

Маскарадинг для зоны public включается с помощью команды `firewall-cmd --zone=public --add-masquerade --permanent`.

5 Список литературы

1. NAT: вопросы и ответы. — URL: https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html (дата обр. 13.09.2021).
2. Динамический брандмауэр с использованием FirewallD. — URL: <https://fedoraproject.org/wiki/> (дата обр. 13.09.2021).
3. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. — М.: Вильямс, 2017. — 912 с. — (Cisco Press Core Series).
4. Часто задаваемые вопросы по технологии NAT / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/c/ru_ru/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html (дата обр. 13.09.2021).