

Лабораторная работа №7

Расширенные настройки межсетевого экрана

Андреева С.В.

Группа НПИбд-01-23

Российский университет дружбы народов, Москва, Россия

Информация

- Андреева Софья Владимировна
- Группа НПИбд-01-23
- Российский университет дружбы народов

Вводная часть

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

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом: Затем запустим виртуальную машину `server`:

На основе существующего файла описания службы `ssh` создадим файл с собственным описанием, посмотрим его содержимое

```
[root@server svandreeva:~]# cp /usr/lib/iptables/services/ssh.xml /etc/iptables/services/ssh-custom.xml
[root@server svandreeva:~]# cat /etc/iptables/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>
[root@server svandreeva:~]#
```

Рис. 1: Содержание файла службы ssh

В первой строчке этого файла указана версия xml и используемая кодировка - utf8. Затем указаны тег service, а внутри его тег-потомок short, внутри которого указано SSH. Также внутри указан тег description, внутри которого написано описание протокола ssh, и указан протокол передачи порта tcp и номер порта 22.

Откроем файл описания службы на редактирование и заменим порт 22 на новый порт (2022) и скорректируем описание службы



A terminal window with a pink header bar. The header bar contains a small icon on the left and the text "root@server:~ - sudo -i" on the right. The terminal displays XML code for an SSH service file. The code is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>This is a modified SSH service file.</description>
  <port protocol="tcp" port="2022"/>
</service>
~
~
~
```

Рис. 2: Редактирование файла службы SSH

Просмотрим список доступных FirewallD служб

```
[root@server.svandreeva.net ~]# firewall-cmd --get-services
Q-AD R4-Satellite-6 R4-Satellite-6-capsule afp alvr amanda-client amanda-k5-client anap anaps anno-1602 anno-1608 apcupsd aseqnet audit ausweisapp2 bacula bacula-clien
t barcos-director barcos-filedaemon barcos-storage bb bqp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bitterrent-lsd ceph ceph-exporter ceph-mon cfsengine c
heckmk-agent civilization-iv civilization-v cockpit collectd conder-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-
quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freei
pa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gnsd grafana gre high-availability http http3 https ident inap inaps iperf2 ipe
rf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogind kpassd kprop kshell kube-api kube-apiserver kube-control-pla
ne kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kub
elet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesteve matrix mds memcache minecraft minidln
a mmpd mongod mosh mountd mpd mqtt mqtt-tls ns-abt mssql msumr mysql nbd nebula need-for-speed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nnea-0183 nrip ntp n
ut opentelemetry openvpn ovirt-imagelo ovirt-storageconsole ovirt-vnconsole plex pncd papproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-no
de-exporter proxy-dhcp ps2link ps3netstv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd rtsp salt-master
samba samba-client samba-dc sane settlers-history-collection sip slp slmerv slp smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spoti
fy-sync squid ssdp ssh statshv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn synching synching-gui sy
nching-relay synergy sysconlan syslog syslog-tls tgtnet tentacle terraria tfftp tile38 tinc tor-sacks transmission-client turn turns upnp-client vdm vnc-server vrrp w
arminator wben-http wben-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-top ws-discovery-udp wsd wsd-http wsmn wsmns xdmcp xmpp-bo
sh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-trapper zabbix-web-service zero-k zerotier
```

Рис. 3: Список доступным FirewallD служб

В этом списке нет новой службы. Теперь перезагрузим правила межметевого экрана с сохранением информации о состоянии и вновь выведем на экран список служб, а также список активных служб. Новая служба отображается в списке доступных служб, но не активирована. Затем активируем новую службу в FirewallD и выведем на экран список активных служб. Новая служба активирована

Выполнение работы

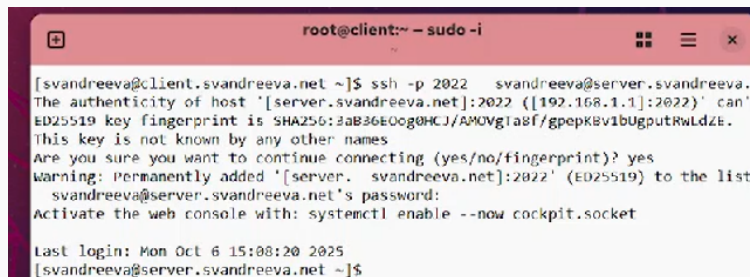
```
sn xhrrp-client xhrrp-local xhrrp-server zabbox-agent zabbox-java-gateway zabbox-server zabbox-trapper zabbox-web-service zero-k zerotier
[root@server.svandreeva.net ~]# firewall-cmd --reload
success
[root@server.svandreeva.net ~]# firewall-cmd --get-services
0-AD-R4-Satellite-6 R4-Satellite-6 capsule afp alvr amanda-client amanda-k5-client amqp anops anno-1602 anno-1800 apcupsd aseqnet audit ausweisapp2 bacula bacula-client
bareos-dircator bareos-filedemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine c
heckmk-agent civilization-iv civilization-v cockpit collected conder-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-
quic dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-lldap freei
pa-lldap freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gssd grafana gre high-availability http http3 https ident inap inaps iperf2 ipe
rf3 ipfs ipp ipp-client ipsec irc ircs lscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasrad kprop kshell kube-api kube-api-server kube-control-pla
ne kube-control-plane-secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kub
elet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llennr llennr-client llennr-tcp llennr-udp managesieve matrix mDNS memcache minecraft minidln
a mnpd mongod nosh noundd npd netd netd-tls ns-abt nssql nurnur mysql nbd nebula need-for-speed-host-wanted netbios-ns netdata-dashboard nfs nfs3 nnea-0183 nripe ntp n
ut openletenetry openvpn ovirt-inageio ovirt-storageconsole ovirt-vnconsole plex pncd papproxy pwebapi pwebapis pop3 pop3s postgresql privoxy prometheus prometheus-no
de-exporter proxy-dhcp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rostd rpc-bind rquotad rsh rsyncd rtsp salt-master
samba samba-client samba-dc sane settlers-history-collection sip sipd slmever sip snmp snmp-subelusion snmps snmp snmptls snmptls-trap snmptrap spideroak-lansync spoti
fy-sync squid ssdp ssh ssh-custom statsrv steam-lan-transfer steam-streaming stellaris stronghold-crusader stun stuns submission supertuxkart svdrp svn synching syncr
ing-gui synching-relay synergy syscomlan syslog syslog-tls telnet tentacle terraria rftp rife38 rline tor-socks transmission-client turn turns upnp-client vdsn vnc-se
rver vrrp warpinguard xbox-http xbox-https xloguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsd wsd-http wsmn wsmns xd
wp xmpg-bosh xmpg-client xmpg-local xmpg-server zabbox-agent zabbox-java-gateway zabbox-server zabbox-trapper zabbox-web-service zero-k zerotier
[root@server.svandreeva.net ~]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server.svandreeva.net ~]# firewall-cmd --add-service=ssh-custom
success
[root@server.svandreeva.net ~]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server.svandreeva.net ~]# firewall-cmd --add-service=ssh-custom --permanent
success
[root@server.svandreeva.net ~]# firewall-cmd --reload
success
[root@server.svandreeva.net ~]#
```

Рис. 4: Добавление новой службы и её активация

Организуем на сервере переадресацию с порта 2022 на порт 22 с помощью команды:

```
firewall-cmd --add-forward-port=port=2022:proto=tcp:toport=22
```

На клиенте попробуем получить доступ по SSH к серверу через порт 2022



```
root@client:~ - sudo -i

[svandreeva@client.svandreeva.net ~]$ ssh -p 2022 svandreeva@server.svandreeva.net
The authenticity of host '[server.svandreeva.net]:2022 ([192.168.1.1]:2022)' can't
be established; ED25519 key fingerprint is SHA256:3aB36EOog0HCJ/AM0VgTa8f/gpepKBv1bugputRWLDZE.
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.svandreeva.net]:2022' (ED25519) to the list
svandreeva@server.svandreeva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Oct 6 15:08:20 2025
[svandreeva@server.svandreeva.net ~]$
```

Рис. 5: Получение клиентом удаленного доступа по SSH к серверу через порт 2022

Настройка Port Forwarding и Masquerading

На сервере посмотрим, активирована ли в ядре системы возможность перенаправления IPv4-пакетов, затем включим пренаправление IPv4-пакетов на сервере и включим маскарадинг на сервере

Выполнение работы

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


Теперь проверим доступность выхода в Интернет на клиенте.

Выполнение работы

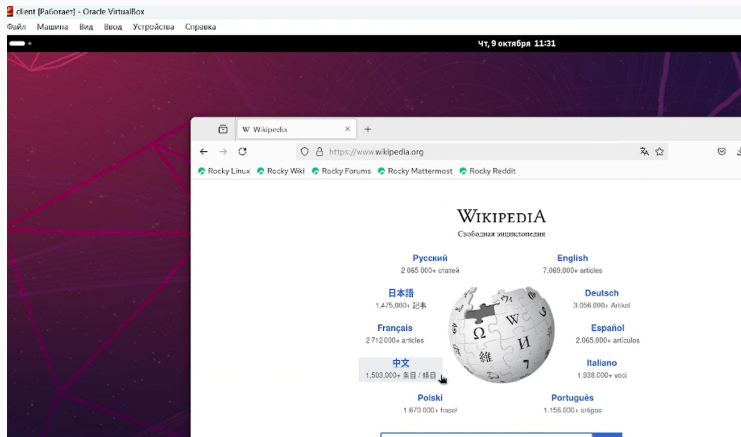


Рис. 7: Доступность выхода в Интернет на клиенте.

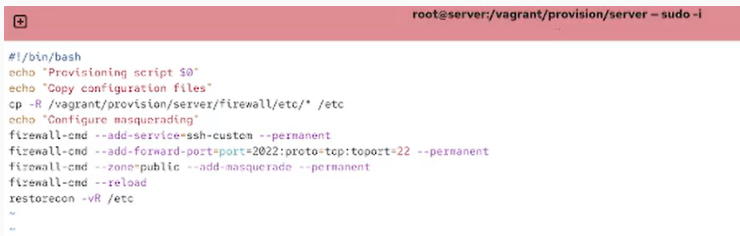
Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине `server` перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `firewall`, в который поместим в соответствующие подкаталоги конфигурационные файлы `FirewallD` и создадим исполняемый файл `firewall.sh`

```
[root@server.svandreeva.net ~]# echo 'net.ipv4.ip_forward = 1' > /etc/sysctl.d/90-forward.conf
[root@server.svandreeva.net ~]# sysctl -p /etc/sysctl.d/90-forward.conf
net.ipv4.ip_forward = 1
[root@server.svandreeva.net ~]# firewall-cmd --zone=public --add-masquerade --permanent
success
[root@server.svandreeva.net ~]# firewall-cmd --reload
success
[root@server.svandreeva.net ~]# cd /vagrant/provision/server
[root@server.svandreeva.net server]# mkdir -p /vagrant/provision/server/firewall/etc/firewalld/services
[root@server.svandreeva.net server]# mkdir -p /vagrant/provision/server/firewall/etc/sysctl.d
[root@server.svandreeva.net server]# cp -r /etc/firewalld/services/ssh-custom.xml /vagrant/provision/server/firewall/etc/firewalld/services/
[root@server.svandreeva.net server]# cp -r /etc/sysctl.d/90-forward.conf /vagrant/provision/server/firewall/etc/sysctl.d/
[root@server.svandreeva.net server]# cd /vagrant/provision/server
[root@server.svandreeva.net server]# touch firewall.sh
[root@server.svandreeva.net server]# chmod +x firewall.sh
```

Рис. 8: Создание окружения для внесения изменений в настройки окружающей среды

Открыв firewall.sh на редактирование, пропишем в нём следующий скрипт



```
root@server:/vagrant/provision/server - sudo -i

#!/bin/bash
echo "Provisioning script $@"
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: Содержание firewall.sh

Для отработки созданного скрипта во время загрузки виртуальной машины `server` в конфигурационном файле `Vagrantfile` добавим в разделе конфигурации для сервера

Выполнение работы

```
C: > work > svandreeva > vagrant > Vagrantfile
 4  Vagrant.configure("2") do |config|
24    config.vm.define "server", autostart: false do |server|
33
34      server.vm.network :private_network,
35                        ip: "192.168.1.1",
36                        virtualbox__intnet: true
37
38      server.vm.provision "server dummy",
39                        type: "shell",
40                        preserve_order: true,
41                        path: "provision/server/01-dummy.sh"
42
43      server.vm.provision "server dns",
44                        type: "shell",
45                        preserve_order: true,
46                        path: "provision/server/dns.sh"
47
48      server.vm.provision "server dhcp",
49                        type: "shell",
50                        preserve_order: true,
51                        path: "provision/server/dhcp.sh"
52      server.vm.provision "server http",
53                        type: "shell",
54                        preserve_order: true,
55                        path: "provision/server/http.sh"
56
57      server.vm.provision "server mysql",
58                        type: "shell",
59                        preserve_order: true,
60                        path: "provision/server/mysql.sh"
61      server.vm.provision "server firewall",
62                        type: "shell",
63                        preserve_order: true,
64                        path: "provision/server/firewall.sh"
65
```

В результате выполнения данной работы были приобретены практические навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.