

Отчёт по лабораторной работе 7

Расширенные настройки межсетевого экрана

Цвелев С.А. НПИбд-02-22

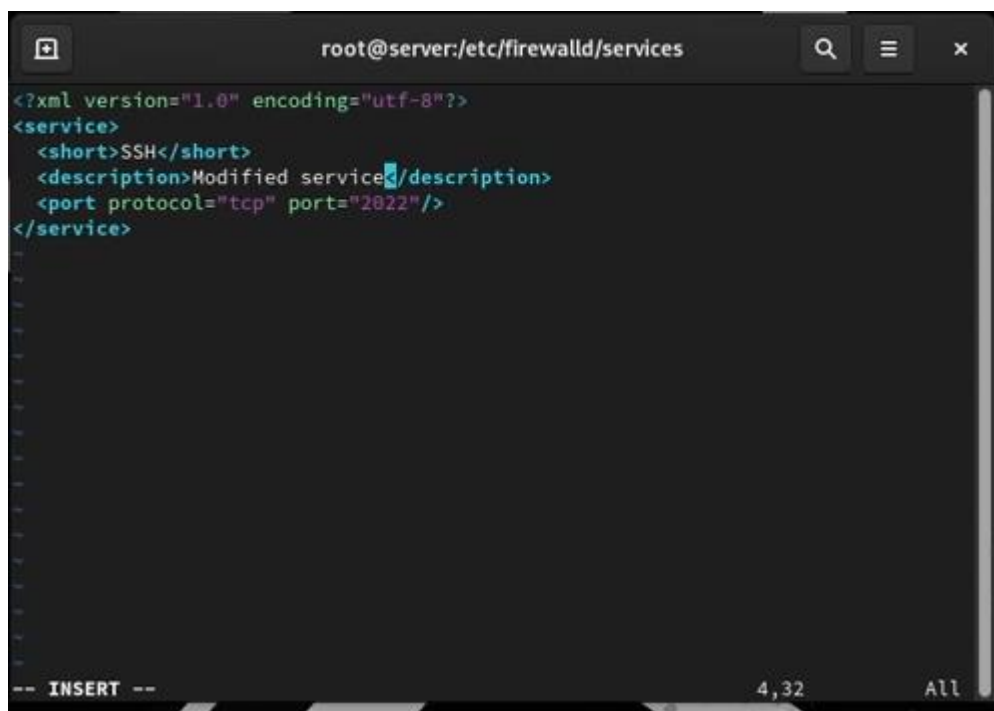
Содержание

1 Цель работы

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

2 Ход работы

Запускаем машину server и включаем режим суперпользователя. На основе существующего файла описания службы ssh создаем файл с собственным описанием. Открываем файл описания службы и меняем порт 22 на новый - 2022. Также меняем описание для себя.



The screenshot shows a terminal window with the title bar 'root@server:/etc/firewalld/services'. The terminal content displays an XML configuration for a service named 'SSH'. The configuration is as follows:

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

At the bottom of the terminal, there is a status bar showing '-- INSERT --' on the left, '4,32' in the center, and 'All' on the right.

Проверяем список доступных FirewallD служб. Нашей пока нет, для этого мы перегружаем правила межсетевого экрана. Проверяем еще раз и убеждаемся, что служба появилась.

```
root@server:/etc/firewalld/services
kube-control-plane kube-control-plane-secure kube-controller-manager kube-control-
ller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure
kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-t
ls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve matrix m
dns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysq
l nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opente
lemetry openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmpd pmp
roxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node
-exporter proxy-dhcp ps2link ps3netdrv ptp pulseaudio puppetmaster quassel radiu
s 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 sn
mp-tls-trap snmptrap spideroak-lansync spotify-sync squid sssd ssh ssh-custom ste
am-streaming svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog sy
slog-tls telnet tentacle tftp tile38 tinc tor-socks transmission-client upnp-cli
ent vdsms vnc-server warpinator wbm-http wbm-https wireguard ws-discovery ws-di
scovery-client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xm
pp-client xmpp-local xmpp-server zabbix-agent zabbix-server zerotier
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh
[root@server services]# firewall-cmd --add-service=ssh-custom
success
[root@server services]# firewall-cmd --list-services
cockpit dhcp dhcpv6-client dns http https ssh ssh-custom
[root@server services]#
```

Проверяем возможность перенаправления пакетов. На сервере включаем перенаправление IPv4-пакетов и включаем маскарading.

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

3 Вывод

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