

# Расширенные настройки межсетевого экрана

---

Абд эль хай мохамад

03.01.2024

РУДН, Москва, Российская Федерация

# Введение

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

# Создание пользовательской службы firewalld

Открываю файл описания службы на редактирование и заменяю порт 22 на новый порт (2022): `<port protocol="tcp" port="2022"/>`

Изменяю поля `<short>` и `<description>` добавляя описание для демонстрации, что это модифицированный файл службы.

Просматриваю список доступных FirewallD служб:

```
firewall-cmd --get-services
```

Новая служба ещё не отображается в списке.

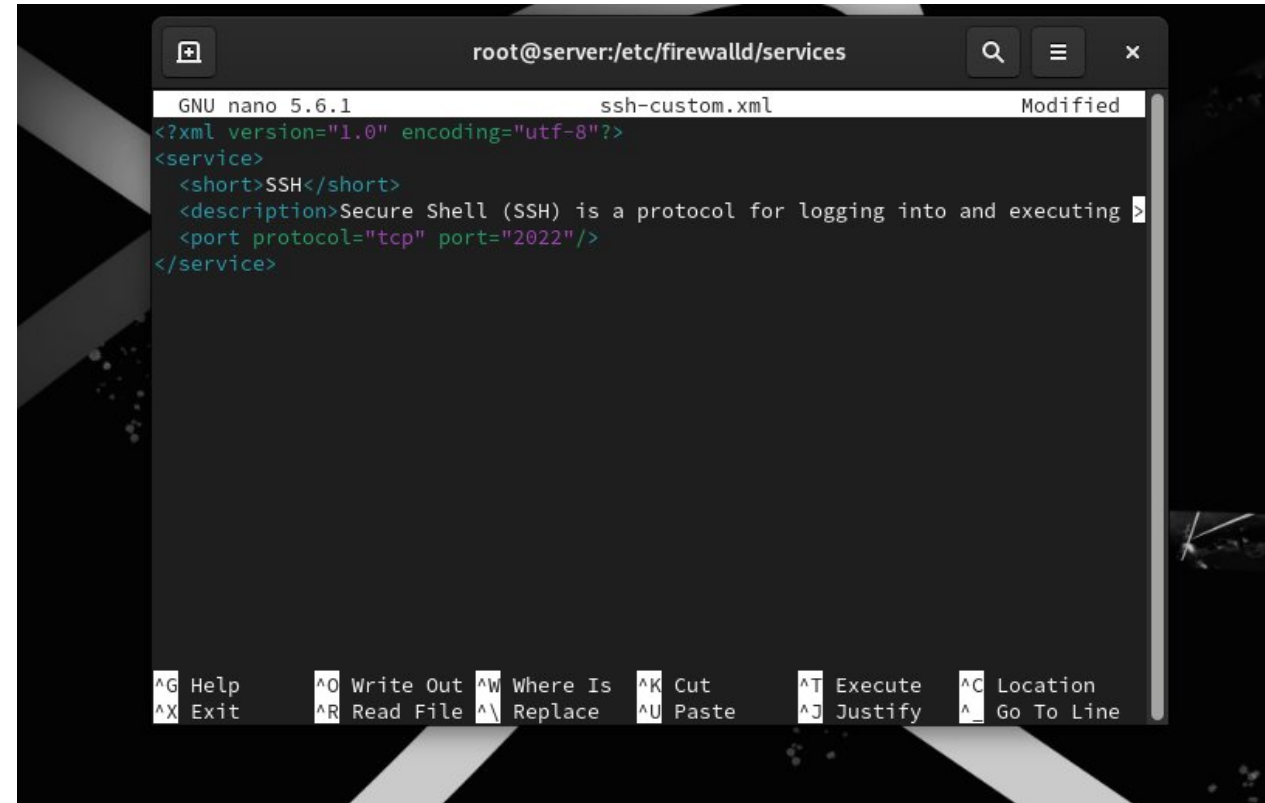
Перегрузите правила межсетевого экрана с сохранением информации о состоянии и вновь выведите на экран список служб, а также список активных служб:

```
firewall-cmd -reload
```

```
firewall-cmd --get-services
```

```
firewall-cmd --list-services
```

Созданная служба отображается в списке доступных для FirewallD служб, но не активирована.



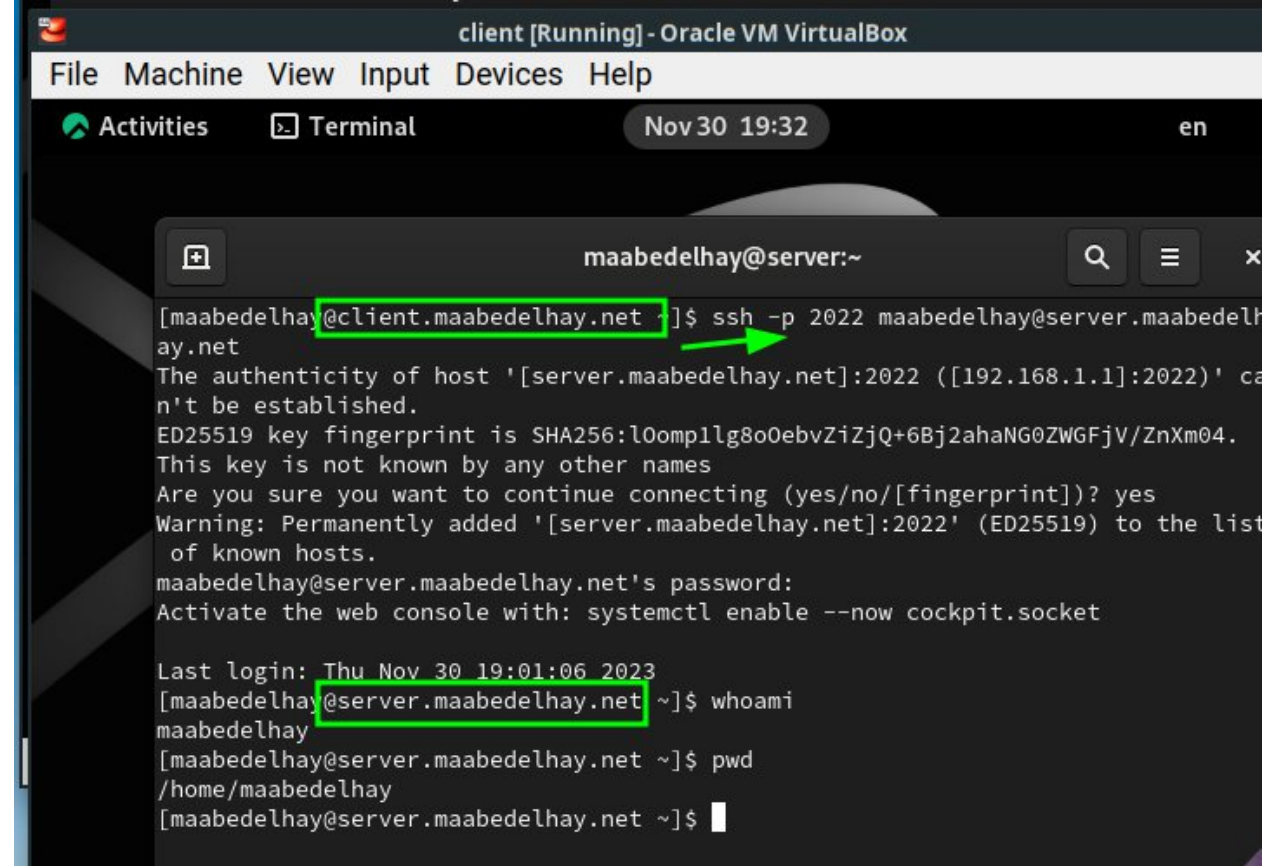
```
root@server:/etc/firewalld/services
GNU nano 5.6.1 ssh-custom.xml Modified
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SSH</short>
  <description>Secure Shell (SSH) is a protocol for logging into and executing
  <port protocol="tcp" port="2022"/>
</service>
```

# Перенаправление портов

Организовываю на сервере переадресацию с порта 2022 на порт 22:

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

На клиенте получаю доступ по SSH к серверу через порт 2022:



The screenshot shows a terminal window titled "client [Running] - Oracle VM VirtualBox". The terminal displays the command `ssh -p 2022 maabedelhay@server.maabedelhay.net` being executed. The output shows the SSH connection process, including the host key fingerprint and the user's password. The terminal prompt changes from `[maabedelhay@client.maabedelhay.net ~]$` to `[maabedelhay@server.maabedelhay.net ~]$`, indicating a successful connection. The user then runs `whoami` and `pwd`, confirming they are on the server.

```
client [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Activities Terminal Nov 30 19:32 en  
maabedelhay@server:~  
[maabedelhay@client.maabedelhay.net ~]$ ssh -p 2022 maabedelhay@server.maabedelhay.net  
The authenticity of host '[server.maabedelhay.net]:2022 ([192.168.1.1]:2022)' can't be established.  
ED25519 key fingerprint is SHA256:l0omp1lg8o0ebvZiZjQ+6Bj2ahaNG0ZWGFjV/ZnXm04.  
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.maabedelhay.net]:2022' (ED25519) to the list of known hosts.  
maabedelhay@server.maabedelhay.net's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Thu Nov 30 19:01:06 2023  
[maabedelhay@server.maabedelhay.net ~]$ whoami  
maabedelhay  
[maabedelhay@server.maabedelhay.net ~]$ pwd  
/home/maabedelhay  
[maabedelhay@server.maabedelhay.net ~]$
```

# Настройка Port Forwarding и Masquerading

На сервере просматриваю, активирована ли в ядре системы возможность перенаправления IPv4-пакетов:

```
sysctl -a | grep forward
```

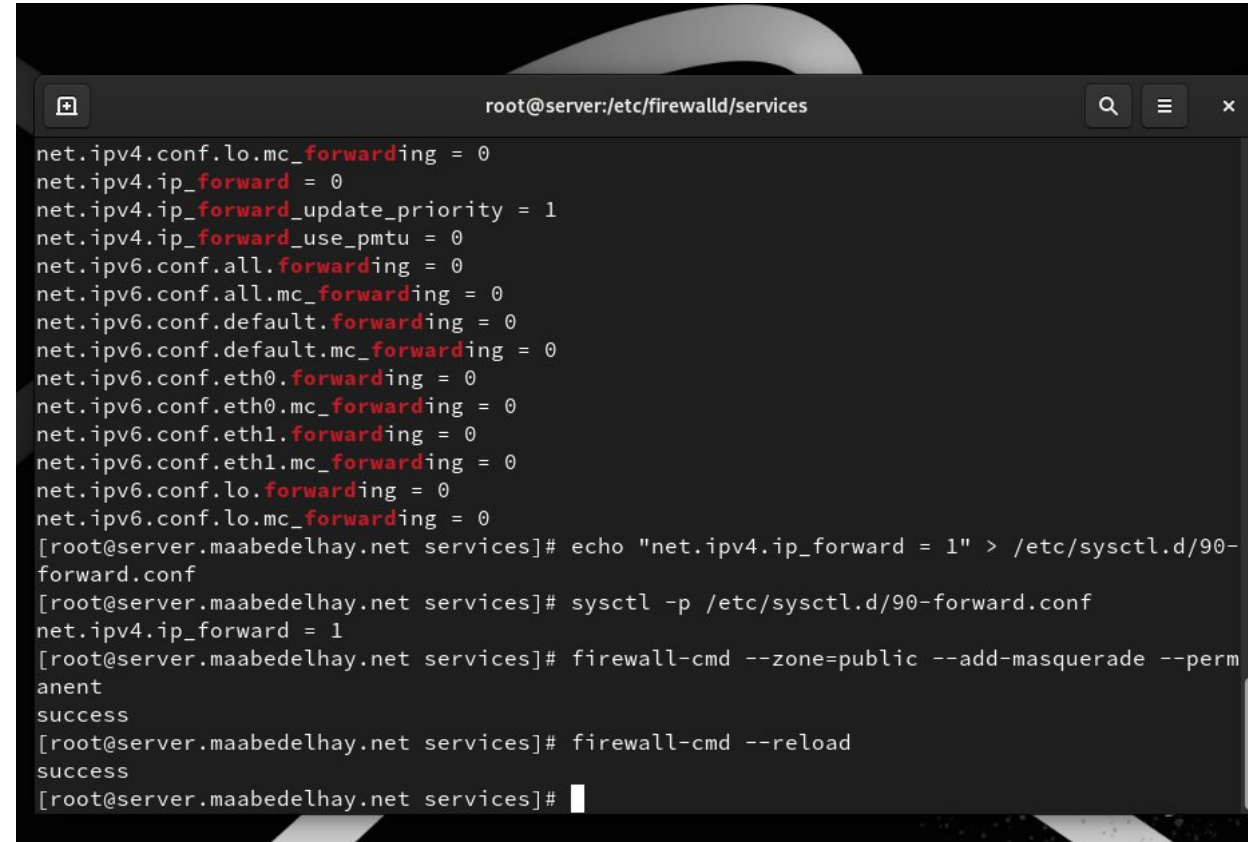
Включаю перенаправление IPv4-пакетов на сервере:

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/90-forward.conf  
sysctl -p /etc/sysctl.d/90-forward.conf
```

Включаю маскарадинг на сервере:

```
firewall-cmd --zone=public --add-masquerade --permanent  
firewall-cmd --reload
```

На клиенте проверяю доступность выхода в Интернет.



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

# Вывод

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

Спасибо За Внимание