

Main Homework

1 Настройка сети и SSH

Настройка сети

Т.к. при установке ubuntu server 22.04.2 LTS мы не устанавливали никаких дополнительных утилит и программ, установим необходимое.

```
hw_tms_ub_srv
anex13@anextmshwsrv:~$ ifconfig
Command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools
anex13@anextmshwsrv:~$ sudo apt install net-tools -y_
```

Проверим настройки сети при помощи ifconfig

```
hw_tms_ub_srv
anex13@anextmshwsrv:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.50.20.60 netmask 255.255.255.0 broadcast 10.50.20.255
    inet6 fe80::20c:29ff:fe81:57be prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:81:57:be txqueuelen 1000 (Ethernet)
    RX packets 34575 bytes 57873930 (57.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6093 bytes 434831 (434.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 206 bytes 20466 (20.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 206 bytes 20466 (20.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

anex13@anextmshwsrv:~$
```

Проверим netplan файл открыв его при помощи nano командой

`sudo nano /etc/netplan/00-installer-config.yaml`

```
hw_tms_ub_srv
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      dhcp4: true
  version: 2
```

Изменим нетплан чтобы сохранить ип адрес (плохая практика)

```
hw_tms_ub_srv
GNU nano 6.2 /etc/netplan/00-installer-config.yaml *
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      dhcp4: false
      addresses: [10.50.20.60/24]
      gateway4: 10.50.20.1
      nameservers:
        addresses: [10.50.20.1, 8.8.8.8]
      version: 2
```

Проверяем и видим что опция gateway4 нежелательна и лучше использовать default route

```
anex13@anextmshwsrv:~$ sudo netplan try

** (process:18553): WARNING **: 05:57:49.927: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.
```

Сделаем как надо

```
hw_tms_ub_srv
GNU nano 6.2 /etc/netplan/00-installer-config.yaml *
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      dhcp4: false
      addresses: [10.50.20.60/24]
      nameservers:
        addresses: [10.50.20.1, 8.8.8.8]
      routes:
        - to: default
          via: 10.50.20.1
      version: 2
```

Видим что теперь всё как надо

```
anex13@anextmshwsrv:~$ sudo netplan try
WARNING:root:Cannot call Open vSwitch: ovssdb-server.service is not running.
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 113 seconds
Configuration accepted.
anex13@anextmshwsrv:~$ _
```

Проверим

```
hw_tms_ub_srv
anex13@anextmshwsrv:~$ ping google.com
PING google.com (172.217.16.46) 56(84) bytes of data.
64 bytes from waw02s14-in-f14.1e100.net (172.217.16.46): icmp_seq=1 ttl=115 time=29.3 ms
64 bytes from muc03s08-in-f46.1e100.net (172.217.16.46): icmp_seq=2 ttl=115 time=29.1 ms
64 bytes from muc03s08-in-f46.1e100.net (172.217.16.46): icmp_seq=3 ttl=115 time=29.1 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 29.067/29.153/29.250/0.075 ms
anex13@anextmshwsrv:~$ _
```

```
hw_tms_ub_srv
anex13@anextmshwsrv:~$ nslookup ya.ru
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   ya.ru
Address: 5.255.255.242
Name:   ya.ru
Address: 77.88.55.242
Name:   ya.ru
Address: 2a02:6b8::2:242
anex13@anextmshwsrv:~$
```

Всё работает.

(Я не очень понял зачем нам менять resolve.conf, systemd-resolve (переименованный в resolvectl) это локальный кэширующий днс сервер который ускоряет ответы (тк они кэшируются) и снижает количество запросов к внешнему серверу.)

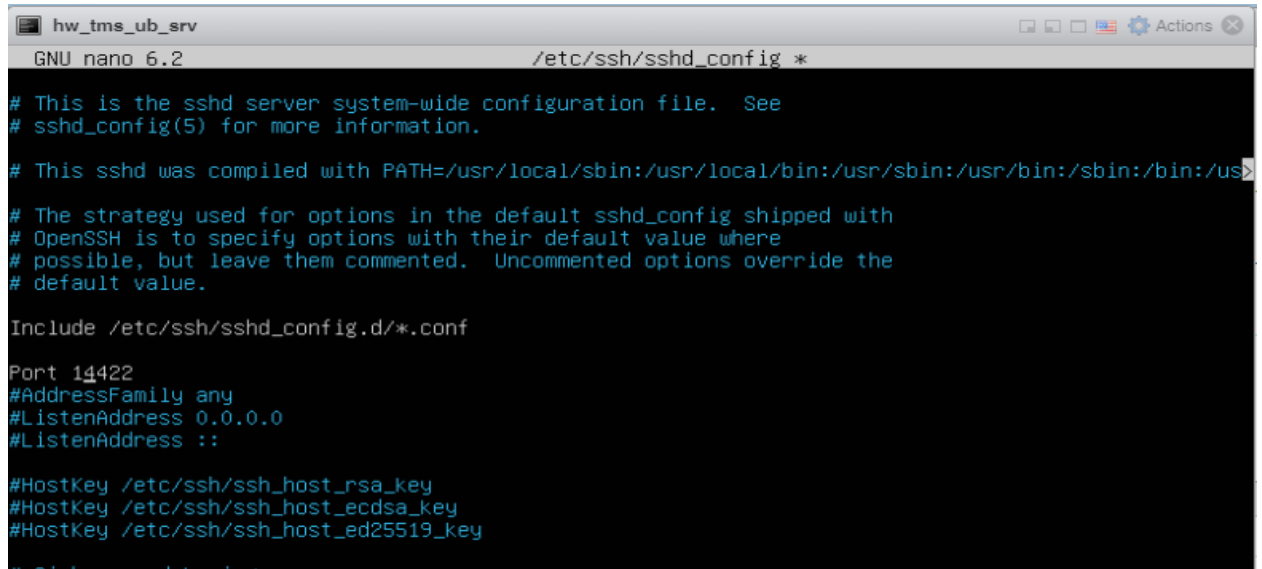
Настройка SSH.

Судя по всему , даже со снятой галкой install ssh при установке Ubuntu server 22.04.2 SSH сервер все равно устанавливается.

```
anex13@anextmshwsrv:~$ sudo service ssh status
• ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2024-04-05 05:38:21 UTC; 1h 1min ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 18437 (sshd)
    Tasks: 1 (limit: 9389)
  Memory: 1.7M
    CPU: 29ms
  CGroup: /system.slice/ssh.service
          └─18437 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 05 05:38:21 anextmshwsrv systemd[1]: Starting OpenBSD Secure Shell server...
Apr 05 05:38:21 anextmshwsrv sshd[18437]: Server listening on 0.0.0.0 port 22.
Apr 05 05:38:21 anextmshwsrv sshd[18437]: Server listening on :: port 22.
Apr 05 05:38:21 anextmshwsrv systemd[1]: Started OpenBSD Secure Shell server.
```

Для первичной защиты от быстрого сканирования well known портов сменим порт подключения SSH



```
hw_tms_ub_srv
GNU nano 6.2 /etc/ssh/sshd_config *
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/sbin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 14422
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# GSSAPI and Kerberos
```

Перезапустим сервис и проверим

```
anex13@anextmshwsrv:~$ sudo service ssh restart
anex13@anextmshwsrv:~$ sudo service ssh status
• ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2024-04-05 06:57:01 UTC; 7s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 19148 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 19149 (sshd)
    Tasks: 1 (limit: 9389)
  Memory: 1.7M
    CPU: 34ms
  CGroup: /system.slice/ssh.service
          └─19149 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 05 06:57:01 anextmshwsrv systemd[1]: Starting OpenBSD Secure Shell server...
Apr 05 06:57:01 anextmshwsrv sshd[19149]: Server listening on 0.0.0.0 port 14422.
Apr 05 06:57:01 anextmshwsrv sshd[19149]: Server listening on :: port 14422.
Apr 05 06:57:01 anextmshwsrv systemd[1]: Started OpenBSD Secure Shell server.
anex13@anextmshwsrv:~$ _
```

Bonus Homework

Настройка SSH с доступом по ключам

Сгенерируем ключ командой ssh-keygen

```
anexl3@anextmshwsrv:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/anexl3/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/anexl3/.ssh/id_rsa
Your public key has been saved in /home/anexl3/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:RQbih8rgSItqwFyyXEOQHINvxHte4uYEijKNvtflo+g anexl3@anextmshwsrv
The key's randomart image is:
+---[RSA 3072]-----+
|o=+. . .o      |
|.o= . o o      |
|=. = o . .     |
|*o@o+... .     |
|=@.=oo  S      |
|O . = .        |
|+o +. o        |
|.. .o. o       |
| .+E .. .      |
+---[SHA256]-----+
anexl3@anextmshwsrv:~$
```

Отредактируем настройки SSH

```
Port 14422
```

```
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
```

```
HostbasedAuthentication no
```

```
PasswordAuthentication no
PermitEmptyPasswords no
```

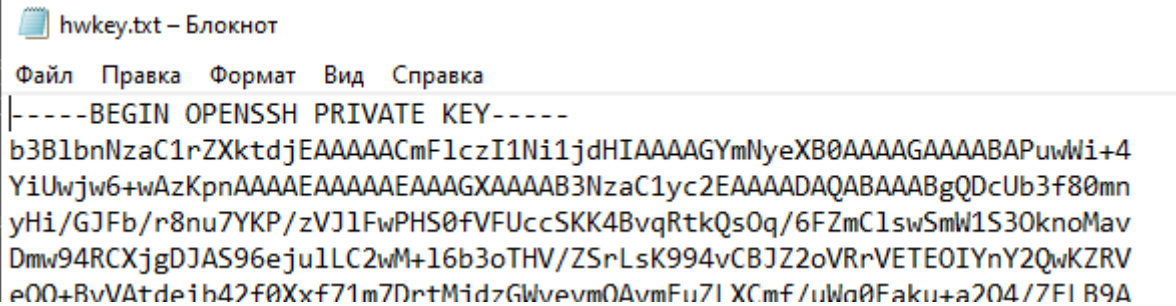
Добавим ключ в авторизованные

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

Сохраним себе на компьютер привэйт ключ

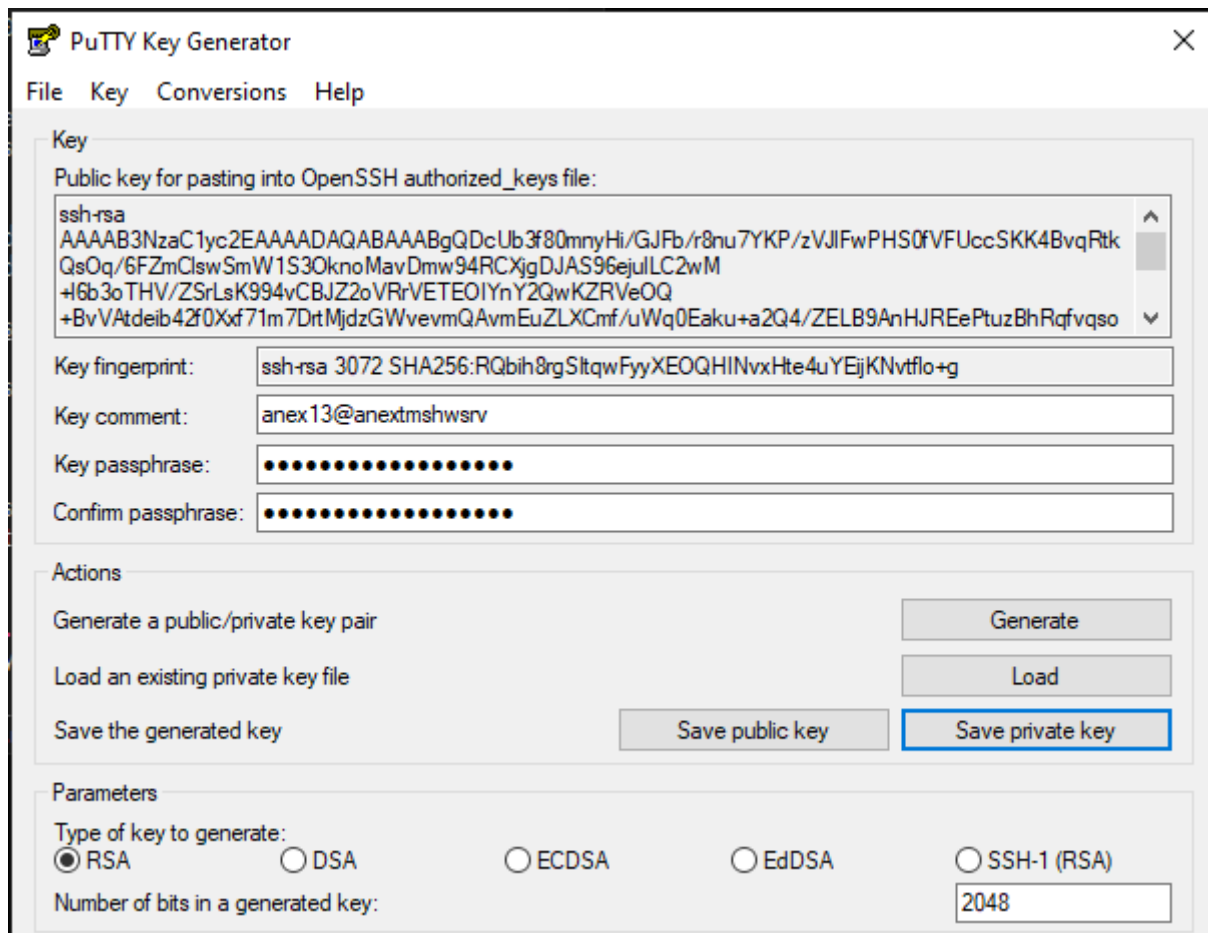
Откроем для просмотра и скопируем содержимое в текстовый файл

```
anex13@anextmshwsrv:~$ cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAPuwWi+4
YiUwjw6+wAzKpnaAAAAEAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQDcUb3f80mn
yHi/GJFb/r8nu7YKP/zVJlFwPHS0fVFUccSKK4BvqRtkQs0q/6FZmClswSmW1S30knoMav
Dmw94RCXjgDJAS96ejulLC2wM+l6b3oTHV/ZSrLsK994vCBJZ2oVRrVETE0IYnY2QwKZRV
e0Q+BvVAtdeib42f0Xxf71m7DrtMjdzGWvevmQAvmEuZLXCmf/uWq0Eaku+a2Q4/ZELB9A
nHJREePtuzBhRqfvqso+oDeEu/H9WaILPhSAG6QoUh073jLG0fa5xFGkl/P0zRjHBCctE3
```



Ключ должен начинаться на -----BEGIN OPENSSH PRIVATE KEY----- и заканчиваться на -----END OPENSSH PRIVATE KEY-----

Для работы с PuTTY необходимо преобразовать ключ в формат путти отурыв и сохранив ключ



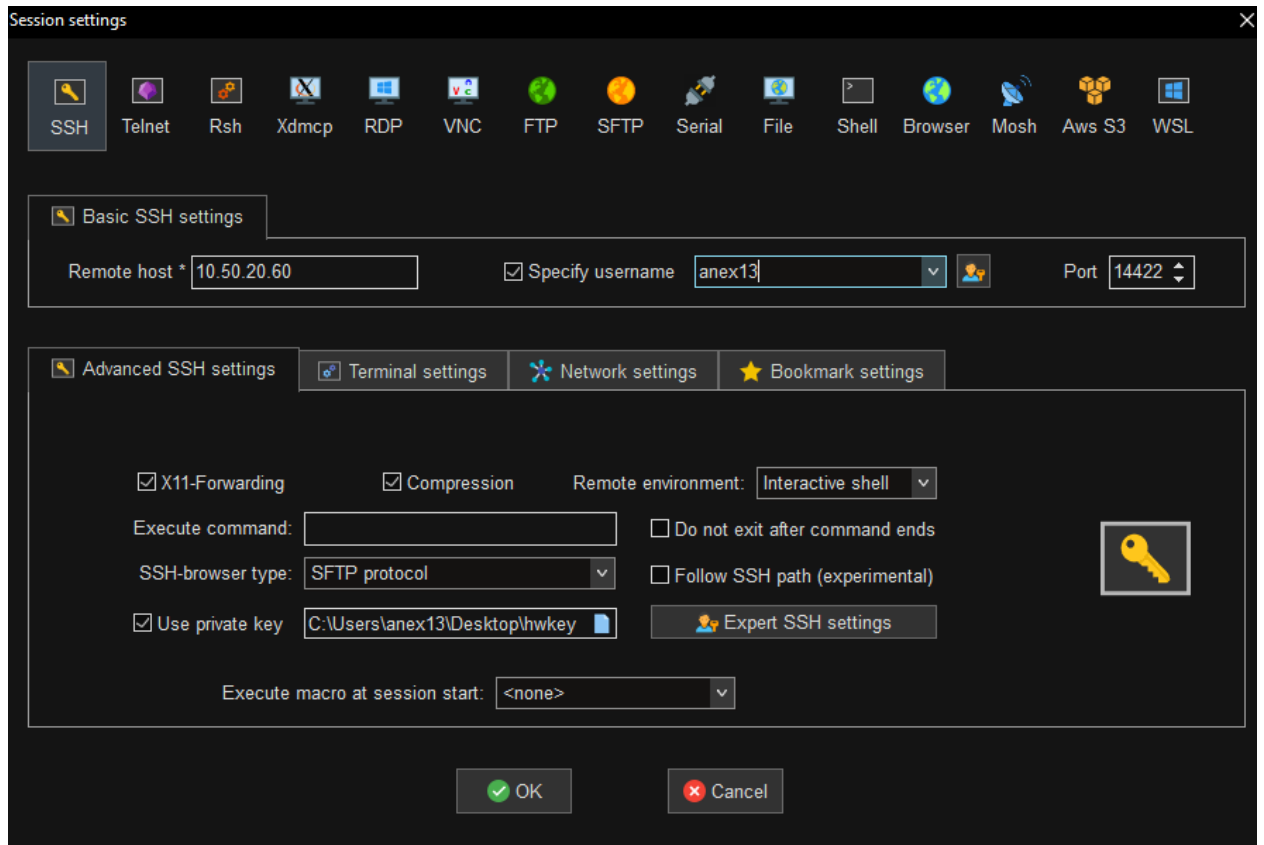
Ключ для путти указывается в Connection-SSH-Auth-Credential в поле Private key file...

Проверяем

```
login as: anex13
Authenticating with public key "anex13@anextmshwsrv"
Passphrase for key "anex13@anextmshwsrv":
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro
```

Для Моба xTerm ключ можно указывать в изначальном формате без преобразований



Проверяем

🚩 Authenticating with public key "anex13@anextmshwsrv"

• MobaXterm Personal Edition v24.0 •
(SSH client, X server and network tools)

- ▶ SSH session to **anex13@10.50.20.60**
 - Direct SSH : ✓
 - SSH compression : ✓
 - SSH-browser : ✓
 - X11-forwarding : ✓ (remote display is forwarded through SSH)
- ▶ For more [info](#), ctrl+click on [help](#) or visit our [website](#).

Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/pro>

System **information** as of Fri Apr 5 08:23:56 AM UTC 2024

System load:	0.01220703125	Processes:	236
Usage of /:	18.3% of 38.09GB	Users logged in:	1
Memory usage:	4%	IPv4 address for ens160:	10.50.20.60
Swap usage:	0%		

- * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

<https://ubuntu.com/engage/secure-kubernetes-at-the-edge>

Expanded Security Maintenance for Applications is not **enabled**.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See <https://ubuntu.com/esm> or run: `sudo pro status`

Last login: Fri Apr 5 08:22:11 2024 from **192.168.198.249**

Настройка iptables

Проверим состояние

```
anex13@anextmshsrv:~$ sudo iptables -vnL
[sudo] password for anex13:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
```

Добавим правила доступа и закроем остальное.

```
anex13@anextmshsrv:~$ sudo iptables -A INPUT -s localhost -j ACCEPT
anex13@anextmshsrv:~$ sudo iptables -A INPUT -s 192.168.198.249 -j ACCEPT
anex13@anextmshsrv:~$ sudo iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT
anex13@anextmshsrv:~$ sudo iptables --policy INPUT DROP
```

Проверим работу

```
anex13@anextmshsrv:~$ ping google.com
PING google.com (216.58.215.78) 56(84) bytes of data.
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=1 ttl=115 time=29.2 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=2 ttl=115 time=29.0 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=3 ttl=115 time=29.0 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 28.985/29.069/29.215/0.103 ms
^Canex13@anextmshsrv:~$
```

Доступ со стороннего компьютера

```
Обмен пакетами с 10.50.20.60 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
```

С доверенного

```
Обмен пакетами с 10.50.20.60 по с 32 байтами данных:
Ответ от 10.50.20.60: число байт=32 время<1мс TTL=63
Ответ от 10.50.20.60: число байт=32 время<1мс TTL=63
Ответ от 10.50.20.60: число байт=32 время<1мс TTL=63
Ответ от 10.50.20.60: число байт=32 время<1мс TTL=63

Статистика Ping для 10.50.20.60:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Сохраним

```
anex13@anextmshsrv:~$ sudo mkdir /etc/iptables-conf/
anex13@anextmshsrv:~$ sudo iptables-save -f /etc/iptables-conf/iptables_rules.ipv4
```

И создадим скрипт восстановления при загрузке

```
anex13@anextmshsrv:~$ sudo nano /etc/network/if-pre-up.d/iptables
```

```
GNU nano 6.2 /etc/network
#!/bin/sh
/sbin/iptables-restore < /etc/iptables_rules.ipv4
```

Сохраняем и меняем атрибут чтобы сделать файл исполняемым

```
anex13@anextmshwsrv:~$ sudo chmod +x /etc/network/if-pre-up.d/iptables
```

Перезагружаем , проверяем

```
anex13@anextmshwsrv:~$ sudo iptables -L
[sudo] password for anex13:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Ничего не работает ((

Обнаруживаем что в мануале где мы смотрели не правильный путь к файлу , правим пробуем опять.

```
GNU nano 6.2 /etc/network/if-pre-up.
#!/bin/sh

/sbin/iptables-restore < /etc/iptables-conf/iptables_rules.ipv4
```

Как оказалось скрипты пре-ап работают только на интерфейсах управляемых ifupdown

Поэтому опять ничего не работает после ребута(

Сдаемся ставим пакет iptables-persistent

```
anex13@anextmshwsrv:~$ sudo apt install iptables-persistent
```

При установке оно спрашивает сохранить ли наши правила отвечаем да предварительно восстановив их командой

```
anex13@anextmshwsrv:~$ sudo /sbin/iptables-restore < /etc/iptables-conf/iptables_rules.ipv4
```

Перезагружаемся опять и проверяем.

```
anex13@anextmshwsrv:~$ sudo iptables -L
[sudo] password for anex13:
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  localhost             anywhere
ACCEPT     all  --  192.168.198.249       anywhere
ACCEPT     all  --  anywhere              anywhere             state ESTABLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
anex13@anextmshwsrv:~$
```

Правила на месте. Ура.

Github

Аккаунт создан

