если кто-то хочет домашку по нетворкингу:

1. создать VM 1 на локальных ресурсах Debian OS

2. создать VM 2 на локальных ресурсах Ubuntu Os

3. создать VM 3 - EC2 линукс интанс on AWS.

сеть между VM 1 и VM 2 - хост онли нетворк. вторая сеть для VM 2 к хосту с гипервизором - NAT сеть.

настроить роутинг: VM 2 - дефаулт гейтвей для VM 1, для VM 2 - дефаулт роутер - хост с гипервизором.

На шлюзе

Раскомментируем в /etc/sysctl.conf

net.ipv4.ip_forward=1

Настраиваем iptables

```
root@ubuntu1804:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 9 packets, 723 bytes)
 pkts bytes target     prot opt in     out     source               destination

  119 24275 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

    1    84 ACCEPT     all  --  enp0s8 *       0.0.0.0/0            0.0.0.0/0

  335 24544 ACCEPT     all  --  enp0s3 *       0.0.0.0/0            0.0.0.0/0
        ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     all  --  enp0s8 *       0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     all  --  enp0s3 *       0.0.0.0/0            0.0.0.0/0
        ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 203 packets, 13430 bytes)
 pkts bytes target     prot opt in     out     source               destination

   71  6135 ACCEPT     all  --  enp0s3 enp0s8  0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
        ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  enp0s3 enp0s8  0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     all  --  enp0s8 enp0s3  0.0.0.0/0            0.0.0.0/0
        ctstate RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 262 packets, 37470 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Убираем «лишние» дефроуты, созданные по dhcp через route delete

На клиенте

Выставить адрес из нужной сети – в моем примере 192.168.56.111/24 шлюз 192.168.56.110

Прописать в /etc/resolv.conf

nameserver 8.8.8.8

продемонстировать трейс с VM 1 до google.com

```
traceroute to google.com (216.58.208.206), 30 hops max, 60 byte packets
 1  _gateway (192.168.56.110)  0.928 ms  0.903 ms  0.889 ms
 2  192.168.254.254 (192.168.254.254)  0.920 ms  0.904 ms  0.892 ms
 3  254.189.87.109.triolan.net (109.87.189.254)  2.235 ms  2.328 ms  2.129 ms
 4  10.65.166.65 (10.65.166.65)  2.398 ms  2.346 ms  2.293 ms
 5  10.161.100.161 (10.161.100.161)  7.711 ms  7.760 ms  7.708 ms
 6  10.81.150.9 (10.81.150.9)  16.144 ms  14.492 ms  14.468 ms
 7  226.3.86.109.triolan.net (109.86.3.226)  14.539 ms  14.524 ms  16.978 ms
 8  108.170.248.147 (108.170.248.147)  15.082 ms  14.523 ms 108.170.248.131 (108
.170.248.131)  15.688 ms
 9  209.85.248.105 (209.85.248.105)  29.838 ms  30.092 ms  30.075 ms
10  142.250.46.55 (142.250.46.55)  29.610 ms  29.690 ms  29.736 ms
11  216.239.35.133 (216.239.35.133)  29.095 ms 72.14.232.136 (72.14.232.136)  28
.837 ms 142.250.37.193 (142.250.37.193)  27.952 ms
12  142.250.224.89 (142.250.224.89)  28.584 ms 142.250.37.209 (142.250.37.209)
28.910 ms  29.168 ms
13  142.250.224.91 (142.250.224.91)  29.006 ms par10s21-in-f14.1e100.net (216.58
.208.206)  29.052 ms  28.251 ms
```

настроить IPSEC VPN с VM 2 до VM3

Устанавливаем пакеты (на обоих сторонах)

apt install strongswan xl2tpd (на обоих сторонах)

настраиваем /etc/ipsec.conf (на обоих сторонах)

настраиваем /etc/ipsec.secrets (на обоих сторонах)

Ура! Туннель поднялся!

```
root@ip-172-31-40-107:~# ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-1065-aws, x86_64):
  uptime: 8 minutes, since May 20 23:13:05 2020
  malloc: sbrk 1622016, mmap 0, used 661536, free 960480
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled:
 9
  loaded plugins: charon aesni aes rc2 sha2 sha1 md4 md5 mgf1 random nonce x509
revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem ope
nssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default
 connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
  172.31.40.107
Connections:
      tunnel:  %any...109.87.189.240  IKEv2, dpddelay=30s
      tunnel:   local:  uses pre-shared key authentication
      tunnel:   remote: uses pre-shared key authentication
      tunnel:   child:  dynamic === dynamic TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
      tunnel[1]: ESTABLISHED 30 seconds ago, 172.31.40.107[172.31.40.107]...109.
87.189.240[192.168.254.106]
      tunnel[1]: IKEv2 SPIs: 91806f10a198b0b4_i* 3f9dd45f86062a8d_r, pre-shared
key reauthentication in 39 minutes
      tunnel[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/M
```

После поднимаем L2tp over IPsec

Uncomment the next line to enable packet forwarding for IPv4 (на обоих сторонах)

net.ipv4.ip_forward=1

Настраиваем /etc/xl2tpd/xl2tpd.conf (на сервере – в моем случае это амазон)

Настраиваем /etc/ppp/chap-secrets (на сервере)

Настраиваем /etc/ppp/options.xl2tp (на сервере)

/etc/init.d/ipsec restart && /etc/init.d/xl2tpd restart (на сервере)

Настраиваем /etc/ppp/options.l2tpd.client (на клиенте)

Настраиваем /etc/xl2tpd/xl2tpd.conf (на клиенте)

Перезапускаем службу

/etc/init.d/ipsec restart && /etc/init.d/xl2tpd restart (на клиенте)
Ура! работает

```
4: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1000 qdisc fq_codel stat
 UNKNOWN group default qlen 3
    link/ppp
    inet 192.168.100.2 peer 192.168.100.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
root@ubuntu1804:~# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=142 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=142 ms
^C
--- 192.168.100.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 142.069/142.530/142.992/0.596 ms
```

добавить на VM 1-3 правила фаервола, которые запретят все, но позволять работать ссш и трейсроуту.

См fw.sh

Я не нашел как включить ICMP ответ на последние два хопа, есть мысль, что это ограничение амазон фритира
Но мы можем обрезать все ответы и включить ответы для трейсроута, этот конфиг работает на других серверах

Для сохранения **iptables-save > /etc/network/iptables.rules**
И в /etc/network/interfaces.

```
iface eth0 inet static
        pre-up iptables-restore < /etc/network/iptables.rules
```

```
root@ubuntu1804:~# ping 3.23.61.224
PING 3.23.61.224 (3.23.61.224) 56(84) bytes of data.
^C
--- 3.23.61.224 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3060ms

root@ubuntu1804:~# traceroute 3.23.61.224
traceroute to 3.23.61.224 (3.23.61.224), 30 hops max, 60 byte packets
 1  192.168.254.254 (192.168.254.254)  0.419 ms  0.583 ms  0.732 ms
 2  254.189.87.109.triolan.net (109.87.189.254)  2.569 ms  2.716 ms  2.761 ms
 3  10.65.166.65 (10.65.166.65)  2.705 ms  2.684 ms  2.723 ms
 4  v3253.core1.kbp1.he.net (184.104.204.33)  23.553 ms  23.258 ms  23.381 ms
 5  100ge15-1.core1.vie1.he.net (184.104.192.225)  31.556 ms  33.444 ms  33.639
ms
 6  100ge13-1.core1.par2.he.net (184.105.65.5)  48.813 ms  57.343 ms  57.395 ms
 7  100ge14-1.core1.nyc4.he.net (184.105.81.77)  117.759 ms  115.733 ms  115.917
 ms
 8  * paix01-jfk1.amazon.com (198.32.118.102)  123.456 ms  123.554 ms
 9  * * *
10  * * *
11  * * *
12  150.222.242.134 (150.222.242.134)  141.759 ms 150.222.242.114 (150.222.242.1
14)  145.993 ms *
13  * * *
14  * * *
15  * * *
16  * * *
17  150.222.243.201 (150.222.243.201)  137.296 ms 150.222.241.187 (150.222.241.1
87)  136.426 ms 150.222.241.181 (150.222.241.181)  138.971 ms
18  * * *
19  * * *
20  * * *
21  * * *
22  52.93.132.61 (52.93.132.61)  138.111 ms 52.93.134.29 (52.93.134.29)  139.615
 ms 52.93.132.61 (52.93.132.61)  137.213 ms
23  * * *
24  52.95.1.150 (52.95.1.150)  137.375 ms 52.95.2.0 (52.95.2.0)  140.654 ms 52.9
3.239.9 (52.93.239.9)  141.657 ms
25  52.95.1.245 (52.95.1.245)  178.460 ms 52.95.2.17 (52.95.2.17)  178.476 ms 52
.95.1.187 (52.95.1.187)  142.131 ms
26  52.95.1.136 (52.95.1.136)  142.265 ms 52.95.2.42 (52.95.2.42)  141.482 ms 52
.95.2.14 (52.95.2.14)  139.946 ms
27  52.95.1.143 (52.95.1.143)  137.928 ms 52.95.1.255 (52.95.1.255)  144.475 ms
 137.745 ms
28  52.95.1.40 (52.95.1.40)  140.159 ms  139.105 ms 52.95.3.142 (52.95.3.142)  1
38.253 ms
29  * * *
30  * * *
root@ubuntu1804:~#
```

А если прописать маршруты между виртуалками

sudo ip r add 192.168.56.0/24 via 192.168.100.1 (для ВМ3)

sudo ip r add 172.31.32.0/20 via 192.168.100.1 (для вм2)

а лучше - сохранить оные в netplan

То можно сделать вот так

```
PING 192.168.56.111 (192.168.56.111) 56(84) bytes of data.
64 bytes from 192.168.56.111: icmp_seq=1 ttl=63 time=137 ms
64 bytes from 192.168.56.111: icmp_seq=2 ttl=63 time=137 ms
^C
--- 192.168.56.111 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 137.127/137.180/137.234/0.374 ms
ubuntu@ip-172-31-40-107:~/.ssh$ traceroute 192.168.56.111
traceroute to 192.168.56.111 (192.168.56.111), 30 hops max, 60 byte packets
 1  ip-192-168-100-2.us-east-2.compute.internal (192.168.100.2)  136.803 ms  136.687 ms  136.698 ms
 2  ip-192-168-56-111.us-east-2.compute.internal (192.168.56.111)  137.155 ms  137.187 ms  137.643 ms
```

*Стоит обратить внимание, что амазон подставляет везде свои именования хостов, даже к хостам вне его сети

или –в обратную сторону

```
haviras@debian:~$ ping 172.31.40.107
PING 172.31.40.107 (172.31.40.107) 56(84) bytes of data.
64 bytes from 172.31.40.107: icmp_seq=1 ttl=63 time=137 ms
64 bytes from 172.31.40.107: icmp_seq=2 ttl=63 time=137 ms
^C
--- 172.31.40.107 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 137.094/137.141/137.188/0.047 ms
haviras@debian:~$ traceroute 172.31.40.107
traceroute to 172.31.40.107 (172.31.40.107), 30 hops max, 60 byte packets
 1  _gateway (192.168.56.110)  0.448 ms  0.424 ms  0.408 ms
 2  172.31.40.107 (172.31.40.107)  137.304 ms  137.284 ms  137.267 ms
haviras@debian:~$
```

дополнительное задание: построить AWS site-2-site VPN (например по этому гайду

https://aws.amazon.com/premiumsupport/knowledge-center/create-connection-vpc/

)

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario4.html

внимание - сайт2сайт стоит денег (немного - но это не бесплатный тир)

Если использовать лютые костыли

iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o eth0 -j MASQUERADE

(или /24 – если надо только к виртуалкам и из виртуалок доступ) на «шлюзовой» машине амазона

и прописать роуты в сети

то можно получить вот такое, правда только в одну сторону.

В обратную – никак.

Скриншот со «шлюза» виртуалки в домашней сети, который VM2

```
traceroute to 172.31.38.231 (172.31.38.231), 30 hops max, 60 byte packets
 1  192.168.100.1 (192.168.100.1)  144.874 ms  144.841 ms  144.775 ms
 2  172.31.38.231 (172.31.38.231)  145.337 ms  145.222 ms  145.184 ms
haviras@ubuntu1804:~/.ssh$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.254.254 0.0.0.0         UG    100    0        0 enp0s3
172.31.0.0      192.168.100.1   255.255.0.0     UG    0      0        0 ppp666
192.168.100.1   0.0.0.0         255.255.255.255 UH    0      0        0 ppp666
192.168.254.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
192.168.254.254 0.0.0.0         255.255.255.255 UH    100    0        0 enp0s3
```

Правильно использовать site2site

Хорошее видео по теме

https://www.youtube.com/watch?v=kqrWjR2Nn7Q

Но такое решение, в отличии от site 2 site является бесплатным, что позволить может сэкономить денег на проекте, особенно если оффсайт бекапы большие