EPAM University Programs

DevOps external course

Module 5 Networking

TASK 5

**Danylenko Homework**

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.

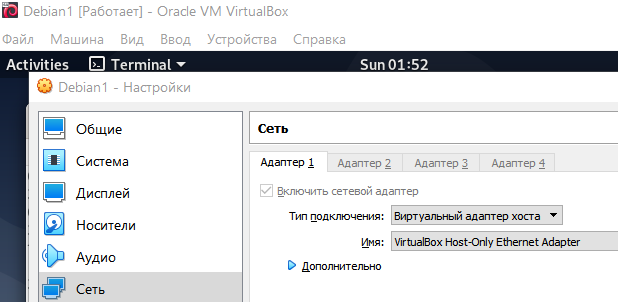
настроить роутинг: VM 2 - дефаулт гейтвей для VM 1, для VM 2 - дефаулт роутер - хост с гипервизором.

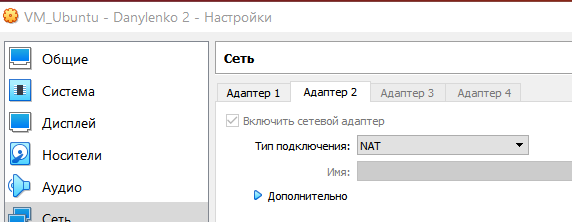
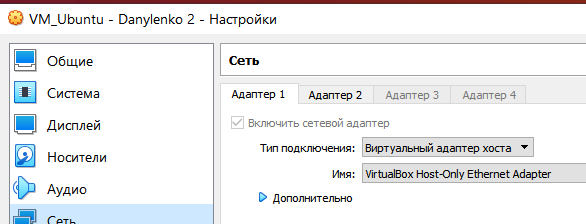
настроить IPSEC VPN с VM 2 до VM3

продемонстировать трейс с VM 1 до google.com

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

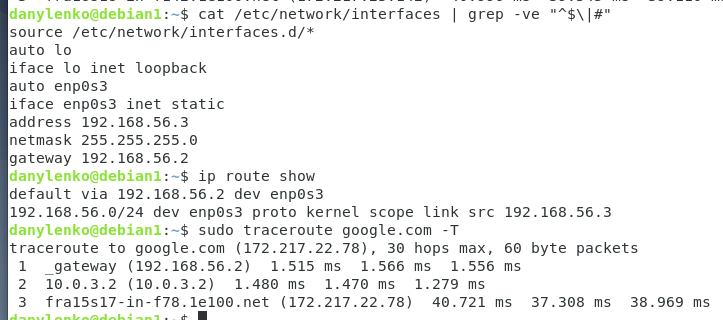
сеть между VM 1 и VM 2 - хост онли нетворк. вторая сеть для VM 2 к хосту с гипервизором - NAT сеть.





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

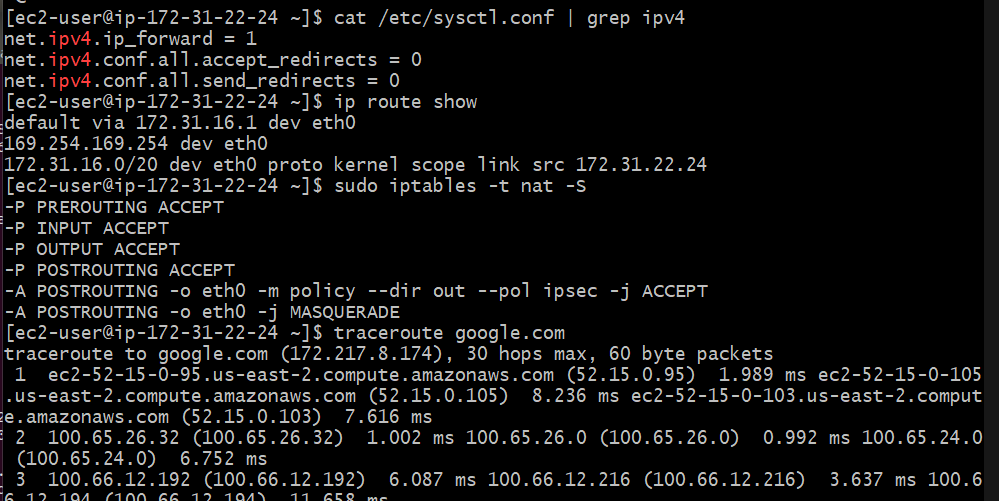
**VM1:**



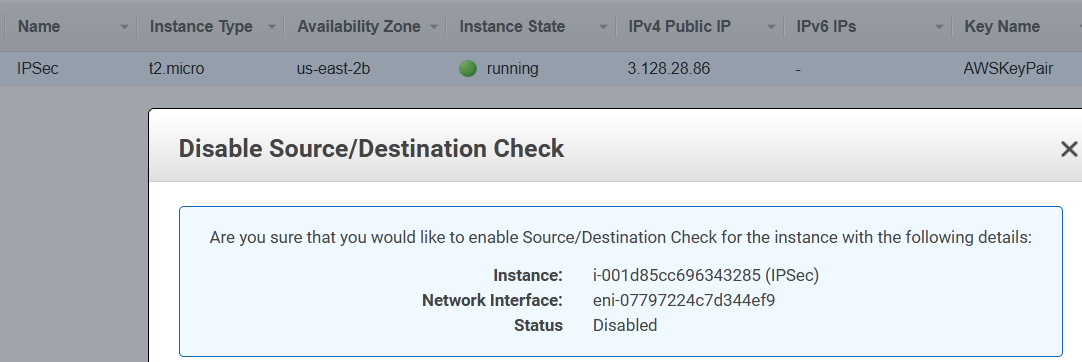
**VM2:**



**VM3 AWS:**



**Disabled Source/Destinations Checks for NAT to work:**

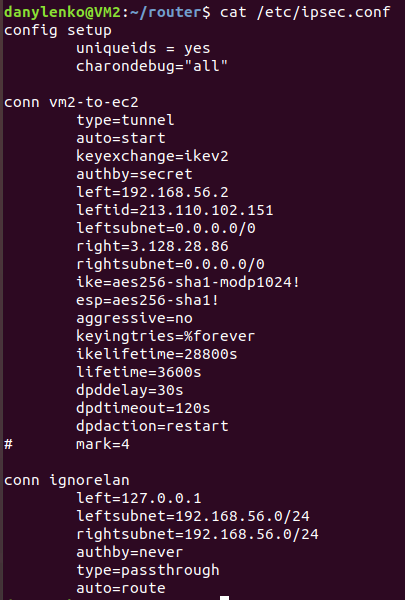
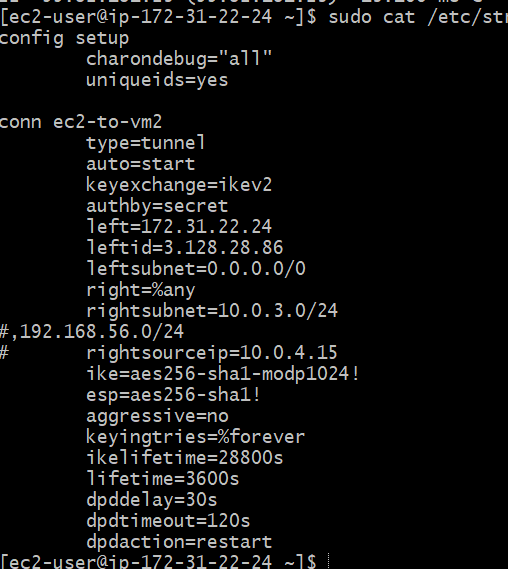


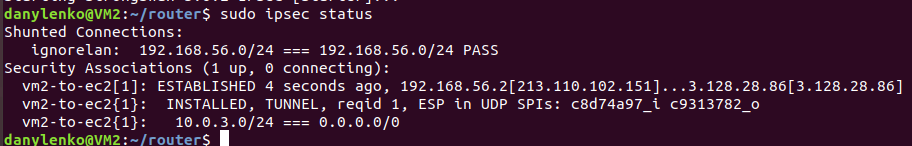
настроить IPSEC VPN с VM 2 до VM3

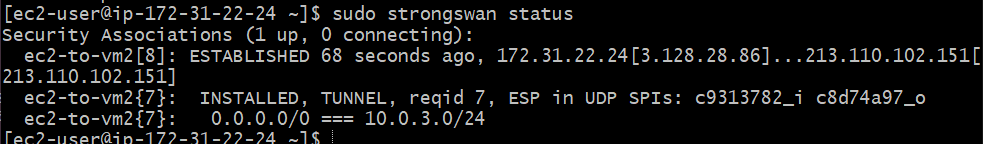
For IPSEC I used strongSwan on both sides with private key,

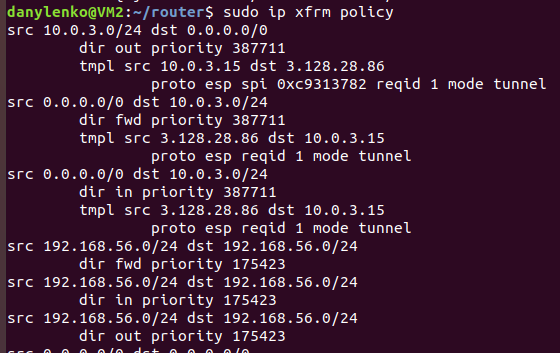
VM2 VM3 AWS:

With enabled policy routing:



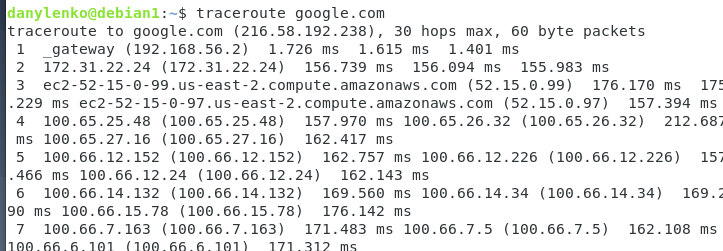




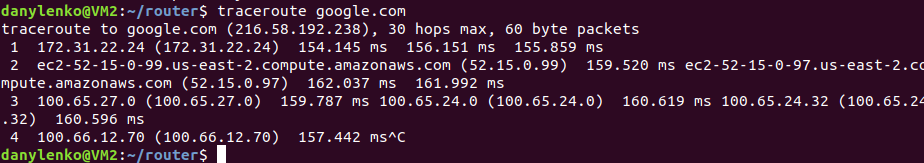


продемонстировать трейс с VM 1 до google.com

**VM1 > google.com**



**VM2 > google.com**



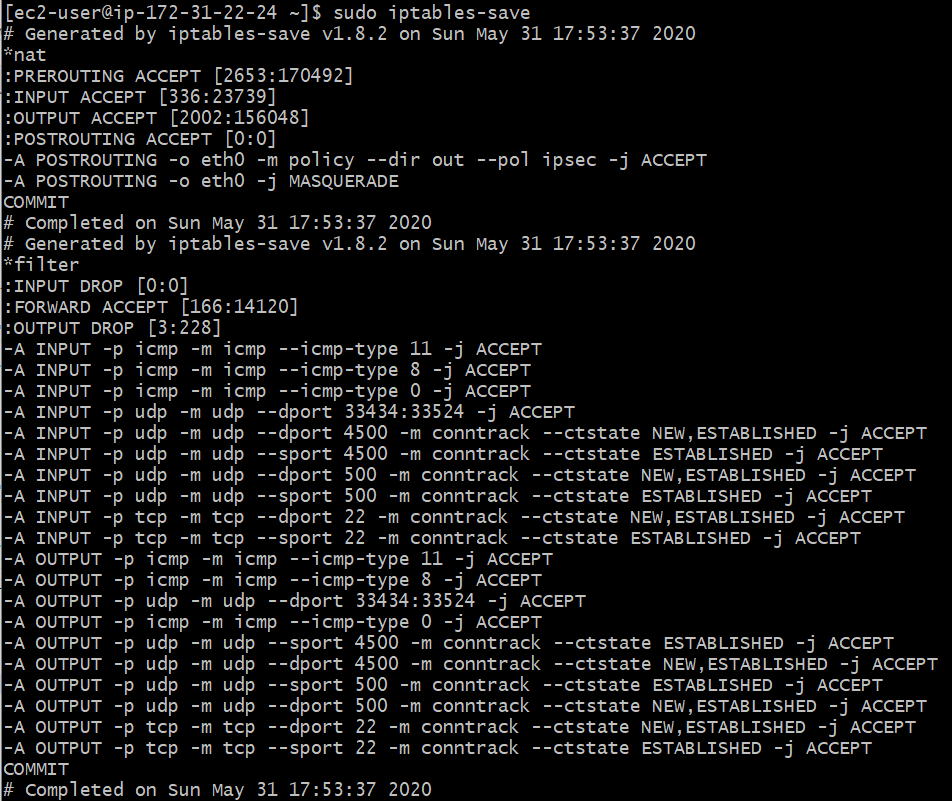
добавить на VM 1-3 правила фаервола, которые запретят все, но позволять работать ссш и трейсроуту.

Since VM1-3 firewall rules were mentioned:

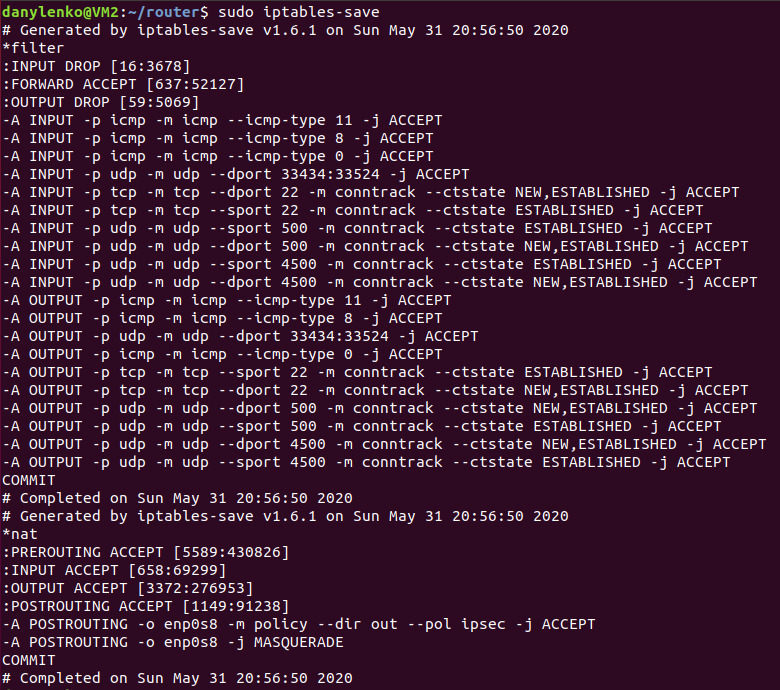
I made rules to ACCEPT FORWARD traffic thorough gateways VM2,VM3,

Only to drop INTUP and OUTPUT traffic on them, and all traffic drops from VM1-debian

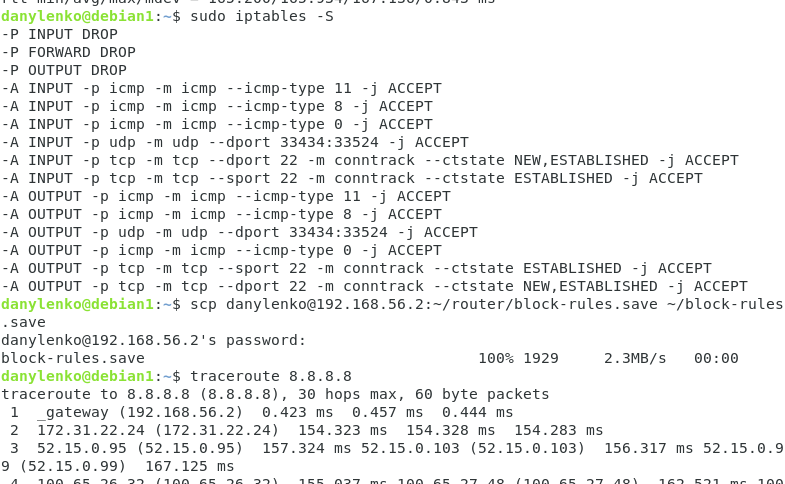
VM3 AWS



VM2 Ubuntu gateway



VM1 client



All Iptable and nat rules saved through iptable-save \ and applied on system restart on each VM with iptable-restore

