Module 6. Thems 5. Routing in Lan

Task 6.5-1. Настройка нескольких локальных сетей Routing

1. Использовать результаты Task-3 и Task-4*.
2. Создать 3 сети. Выбрать такие адреса сети, которые позволили бы разместить:
   - в первой сети, не боле 6 хостов;
   - во второй сети, не более 24 хостов;
   - в третьей сети, не более 50 хостов.

Адреса сети выбрать так чтобы количество записей маршрутизации было минимальным.

Сеть имеет следующую топологию:

net 1: подсоединена к сети net3 (отдельный роутер R13 хост с двумя интерфейсами)

net 2: подсоединена к сети net3 (отдельный роутер R23 хост с двумя интерфейсами)

net 3: имеет **nat** доступ к сети ***epam***

net-dmz: имеет выход в inet (сеть EPAM) через сеть net 3 (отдельный роутер Rdmz3 хост с двумя интерфейсами)

3. Настроить:
   a. один DNS и DHCP†‡;
   b. настроить **nat** для доступа в интернет из локальной сети;
   c. настроить маршрутизацию между сетями net1, net2, net3, net-dmz;
   d. из любой локальной сети (net1, net2, net3) должен быть доступ на ресурсы в сети DMZ;
   e. из Internet (сеть EPAM) доступ на сервера NGINX;
   f. из DNS доступа в локальные сети запрещен.
4. Настроить в сети DMZ два сервера nginx на разных хостах. На серверах nginx развернуть сайт (одна страница, ваше резюме). На DNS настроить Round robin DNS на nginx.
5. Настроить автоматическую регистрацию DHCP клиентов в DNS сервере, для всех клиентов всех сетей.
6. ** Построить большую локальную сеть, объединив все сети (построенные на одном notebook, ***nat*** *отключить*) в одну большую. Разбиться на 2(4) команды (оффиса). Каждый офис компании должен иметь
   a. единственное подключение к internet (NAT)
   b. DNS организации
   c. VPN туннель для связи между офисами
   d. распределить IP адреса в каждом из офисов
   e. настроить маршрутизации

   net 1: подсоединена к сети net3 (отдельный роутер R13 хост с двумя интерфейсами)

   net 2: подсоединена к сети net3 (отдельный роутер R23 хост с двумя интерфейсами)

   net 3: имеет доступ к интересу сети epam (bridge), а wi-fi nat (см. таблицу)

   настроить vpn server

В качестве результата вы должны получить набор скриптов и Vagrantfile, который размещен на gitlab, по истории коммитов должна прослеживаться последовательность решения. Рекомендуется применить Feature branching Workflow, при этом основная ветка в которую происходят слияния должна быть *buildable на каждом коммите*

** Командная работа.

---

* **Использовать Vagrant с провиженом Shell в Vagrantfile**

† **Использовать Ubuntu 20.04, Oracle Linux 8, CentOS Stream 8. Один роутер на Ubuntu 20, другой Oracle Linux 8, CentOS Stream 8. Для DNS и DHCP использовать отдельные VM, но с разними OS: Ubuntu или CentOS.**

‡ Если вычислительные ресурсы не позволяют, то объединить сервера DNS и DHCP на одной VM.

Module 6. Thems 6. Rules on Iptables

Task 6.6-1. Rule of NAT

Написать правила, которые позволяют выполнить пробросить сервис из DMZ в сеть EPAM. Используйте веб сервер NGINX и сервер ssh, но не через vagrant interface.

Для сервиса SSH настроить ограничения на подключения по IP и доменному имени. Как из внутренней сети, так и из сети EPAM.

Task 6.6-2. Проверка открытых портов по протоколам TCP в направлении DMZ->LAN

По умолчанию доступа из DMZ в LAN нет. Для доступа из DMZ в LAN выполняется запрос в Support в котором указывается номер порта, DNS of VM in DMZ и DNS of VM in LAN, после команда Security и Network выполняют настройки. Далее они просят вас проверить доступность порта.
Необходимо написать скрипт, который проверяет открытость порта. На каждую VM имеется доступ по SSH port 22 и SSH ключи.

a) Поддержка протокола TCP.
b) При успешной проверки получаем ответ в следующем формате:
   "DMZ->LAN <DNS_DMZ/IP_DMZ> <DNS_LAN/IP_LAN> <UDP/TCP> <Port> successful"
c) если не получается проверить доступность порта, то попытаться установить причину отказа:
   i. хост недоступен;
   ii. ошибка в маршрутизации;
   iii. превышение времени жизни;
   iv. установлении соединения успешно, данные не передаются;
   v. проверить все вышеперечисленные ошибки, т.е. написать ошибочные настройки маршрутизации и правил firewall.
d) Поддержка протокола UDP
e) Скрипт написать на bash и python

Task 6.6-3. Rule of log and limit

Написать правила, которые позволят ограничить количество одновременных TCP соединений по ssh.
Выполнить логирование IP адресов с который осуществлялись попытки подключения.

Task 6.6-4. Rule of security

Проанализировать основные сетевые атаки, оценить степень их угрозы. Для 3-х наиболее опасных атак прописать правила их перекрытия. Логирование направить в отдельный журнал.