Лабораторная 3. Часть 1

VPN

Задание:

Hастройка VPN подключений Wireguard и IPSec/IKEv2.

Техническое задание:

Для каждого типа VPN подключения необходимо настроить отдельный сервер или виртуальную машину с Ubuntu/CentOS/Fedora. В случае настройки VPN на виртуальной машине, необходимо выделить ей отдельный IP.

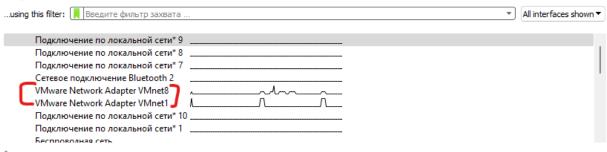
Инструкция по установке сервера Wireguard в упрощенном варианте https://devpew.com/blog/wireguard/

Инструкция по установке и скрипт автоконфига для IPSec https://github.com/hwdsl2/setup-ipsec-vpn. При установке с помощью автоматического скрипта необходимо убедиться, что система полностью обновлена и после его отработки не забыть сохранить stdout консоли, т.к. там записан пароль.

```
## Compiling and installing Libreswan, please wait
 make -j3 -s base
 make -s install-base
## Creating VPN configuration...
## Updating sysctl settings...
## Updating IPTables rules...
## Enabling services on boot...
## Starting services...
IPsec VPN server is now ready for use!
Connect to your new VPN with these details:
Server IP:
IPsec PSK:
Password:
Write these down. You'll need them to connect!
Important notes: https://git.io/vpnnotes
Setup VPN clients: https://git.io/vpnclients
IKEv2 guide:
                  https://git.io/ikev2
.-----
```

ОС, с которой будет происходить подключение с VPN, не имеет значения. Для проверки работоспособности VPN необходимо захватить трафик с включенным VPN с помощью wireshark в течение 1 минуты, при этом зайти в браузере на любые сайты. Захват трафика включать ТОЛЬКО после подключения VPN. Для более удобного перехвата трафика лучше использовать виртуальную машину в VMware и подключаться к VPN в ней

Capture



Отчет выполнить в формате MD. В отчете отразить этапы установки VPN сервера, данные о подключении в виде вывода ifconfig (или аналога для вашей ОС) и к отчету приложить 2 файла перехваченного трафика wireguard.pcap и ipsec.pcap.