MikroTik

Indonetworkers.com
everytime always learn

Setting an OpenVPN on Linux and MikroTik to securely access a web server

Teddy Yuliswar

MikroTik Certified Trainer #TR0442

MUM
MikroTik User Meeting

Indonetworkers.com Training Center (ITC)
Jl. S. Parman No. 189B Ulak Karang Utara
Padang – West Sumatera - Indonesia

Indonetworkers.com/training

MikroTik

Indonetworkers.com
everytime always learn

Case

1. We want to have a web-based application that is on a server that can only be accessed by office employees - our branch offices (not allowed to be accessed publicly) or
2. We want to manage client routers that do not have public ip via a single web based app

Problem

At the Head Office and Branch (both) there is no dedicated internet for example :

1. From ISP Dynamic Internet IP
2. Under the NAT Router / Does not have a public IP

MikroTik

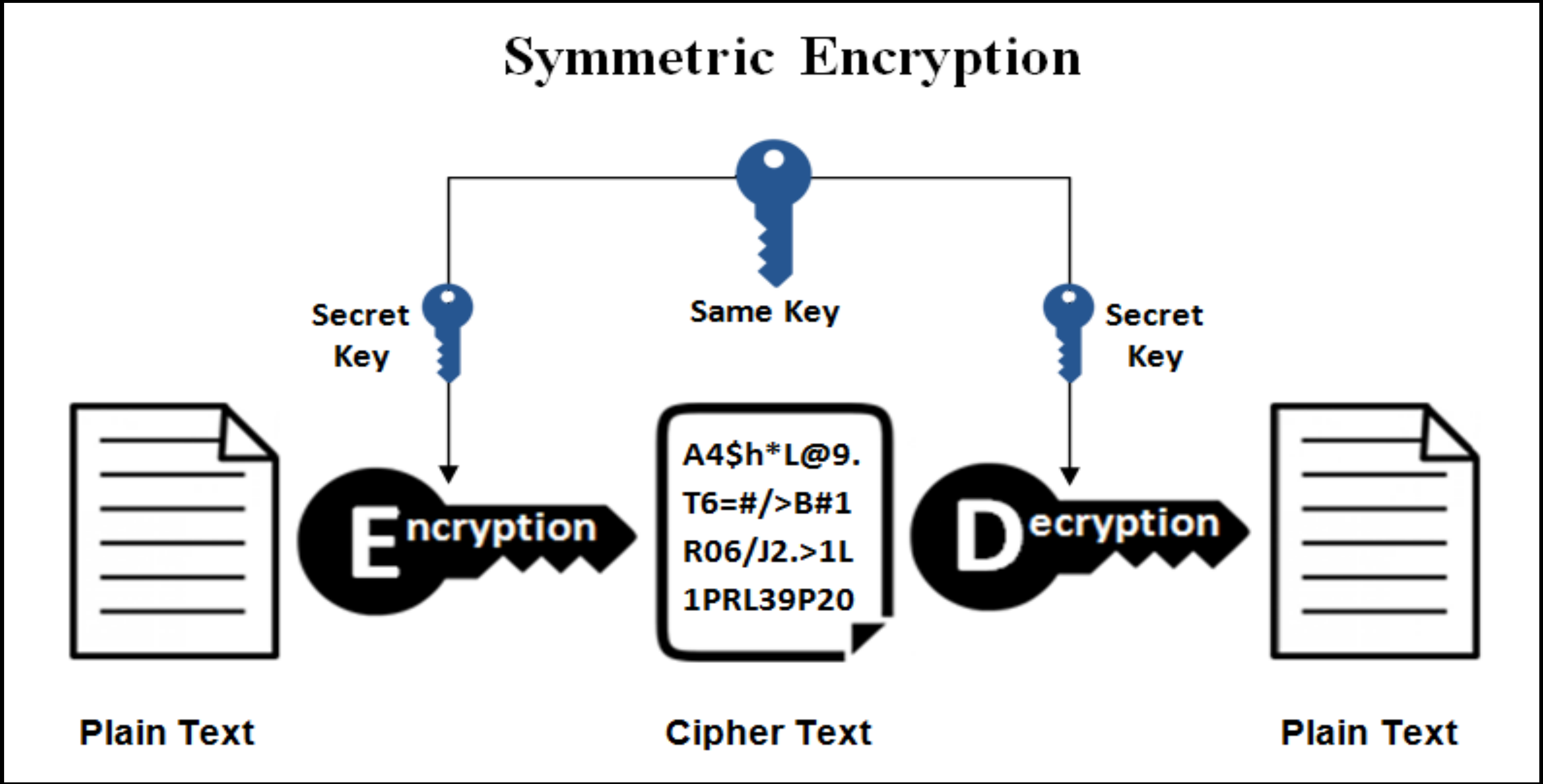
Indonetworkers.com
everytime always learn

What do we need to solved this problem?

What are the steps?

What is OpenVPN?

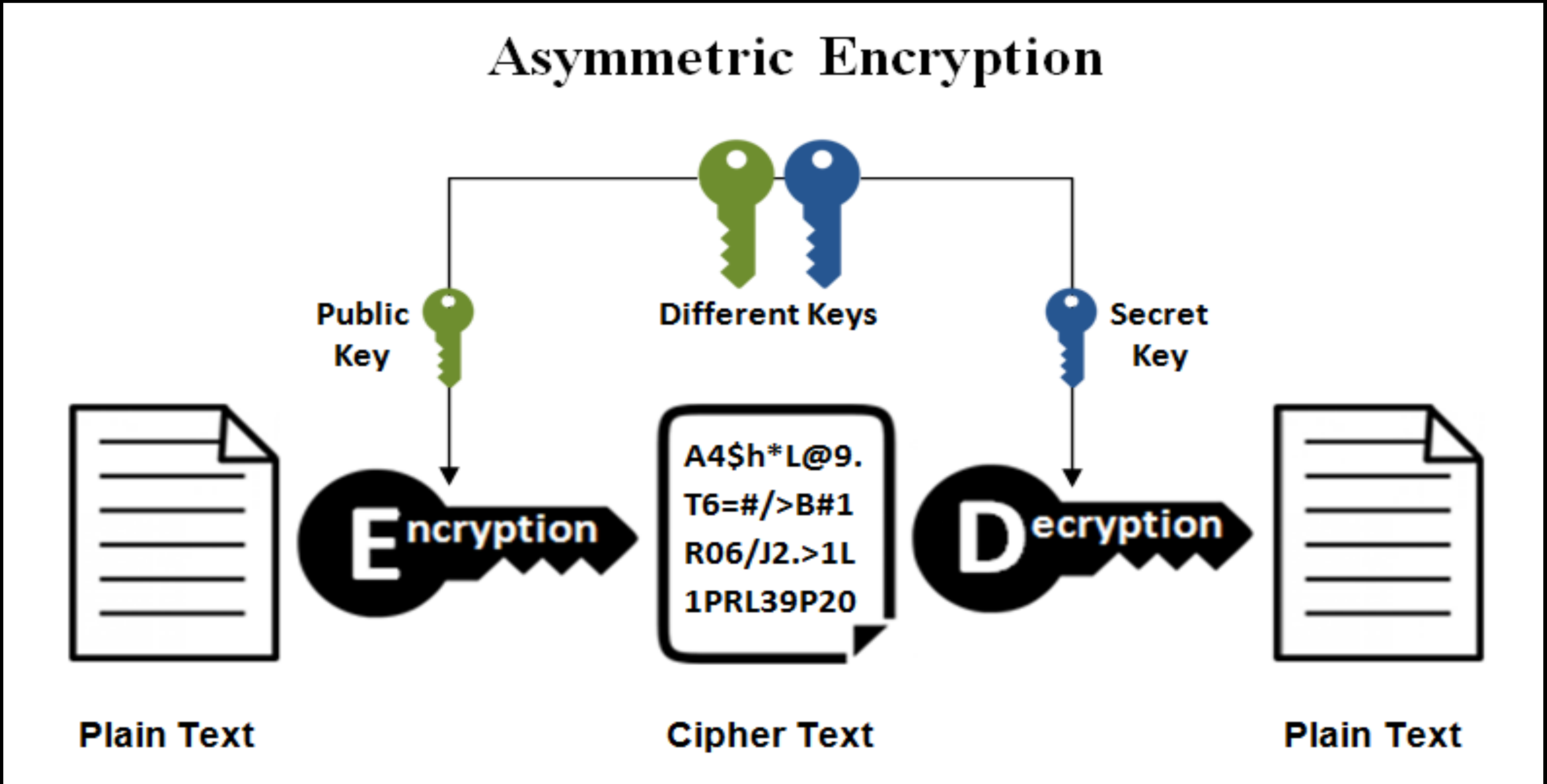
Symmetric Encryption



Example Symmetric Encryption

- Blowfish, AES, RC4, DES, RC5, and RC6
- The most widely used now AES-128, AES-192, and AES-256.

Asymmetric Encryption



Example Asymmetric Encryption

Most are used in everyday communication channels, especially through the Internet.

Popular asymmetric key encryption :

ElGamal, RSA, DSA, Elliptic curve techniques, PKCS

Why OpenVPN?

	OpenVPN	PPTP	L2TP/IPsec	SSTP	IKEv2/IPSec
Encryption	160-bit, 256-bit	128-bit	256-bit	256-bit	256-bit
Security	Very high	Weak	High security (might be weakened by NSA)	High	High
Speed	Fast	Speedy, due to low encryption	Medium, due to double encapsulation	Fast	Very fast
Stability	Very stable	Very stable	Stable	Very stable	Very stable
Compatibility	Strong desktop support, but mobile could be improved. Requires third-party software.	Strong Windows desktop support.	Multiple device and platform support.	Windows-platform, but works on other Linux distributions.	Limited platform support beyond Windows and Blackberry
Final Word	Most recommended choice. Fast and secure.	Native on Windows. Weak security. Useful for geo-restricted content.	Versatile and secure. A decent alternative to OpenVPN.	Faster and more secure alternative to PPTP and L2TP.	Secure, stable, and mobile-oriented.

Source : https://thebestvpn.com/pptp-l2tp-openvpn-sstp-ikev2-protocols/

OpenVPN uses SSL / TLS

SSL and TLS

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) SSL are universally accepted standards for authenticated and encrypted communication between clients and servers.
- SSL / TLS uses a combination of public key and symmetric-key encryption

- OpenVPN uses SSL / TLS for Public Key Infrastructure, then SSL / TLS uses AES to encrypt the public key, then the public key is sent to the client

So the process is,

Server Side:

1. Create public and private keys
2. Public key encryption with AES
3. Encrypt data with a private key
4. Make a hash with sha or md5
5. Send data in encrypted form and also send public AES encrypted keys, as well as fingerprint hashes

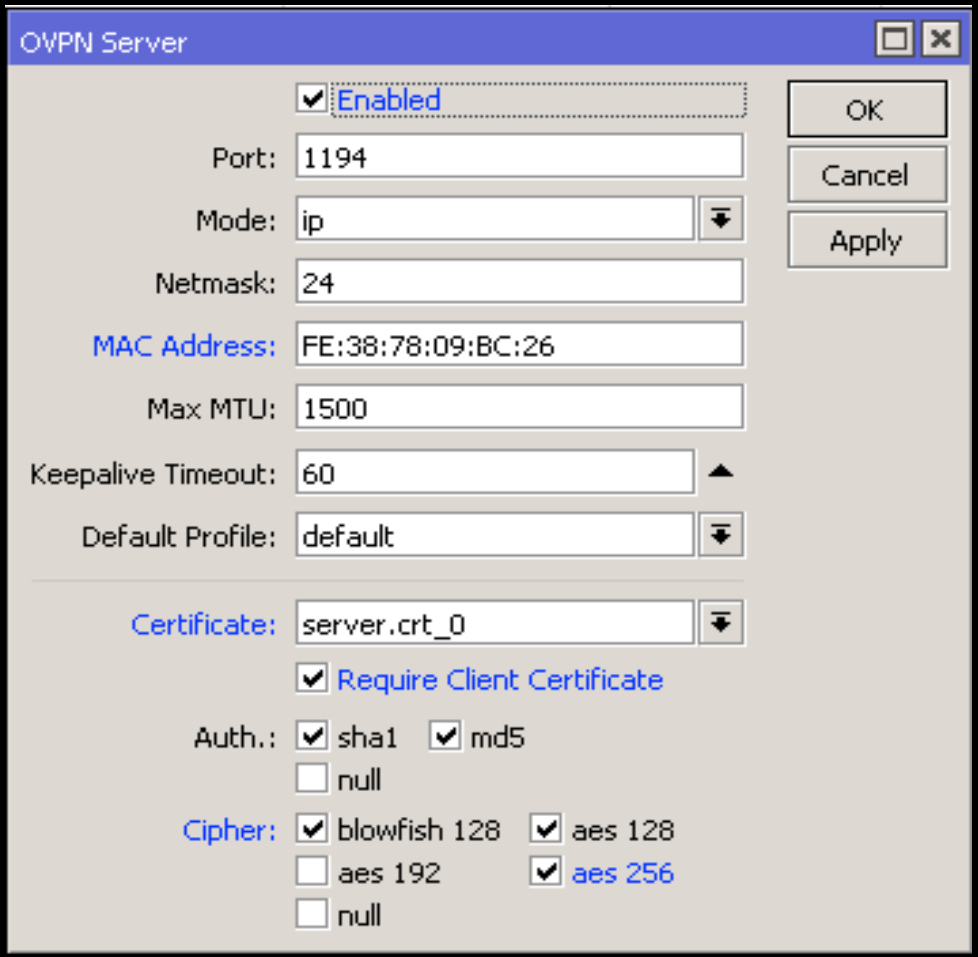
Client Side :

1. Receive data, public key, fingerprint hash
2. Check data integrity with hashes
3. Decryption of the public key
4. Decrypt data with a public key that has been decrypted in point 3
5. Finish

Future Data Communication is almost certain to use:

1. Public Key Infrastructure for data encryption
2. Symmetric Encryption To send a public key
3. Hashing for Data Integrity checking

OpenVPN on MikroTik RouterOS



OVPN Server

☑ Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:38:78:09:BC:26

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: default

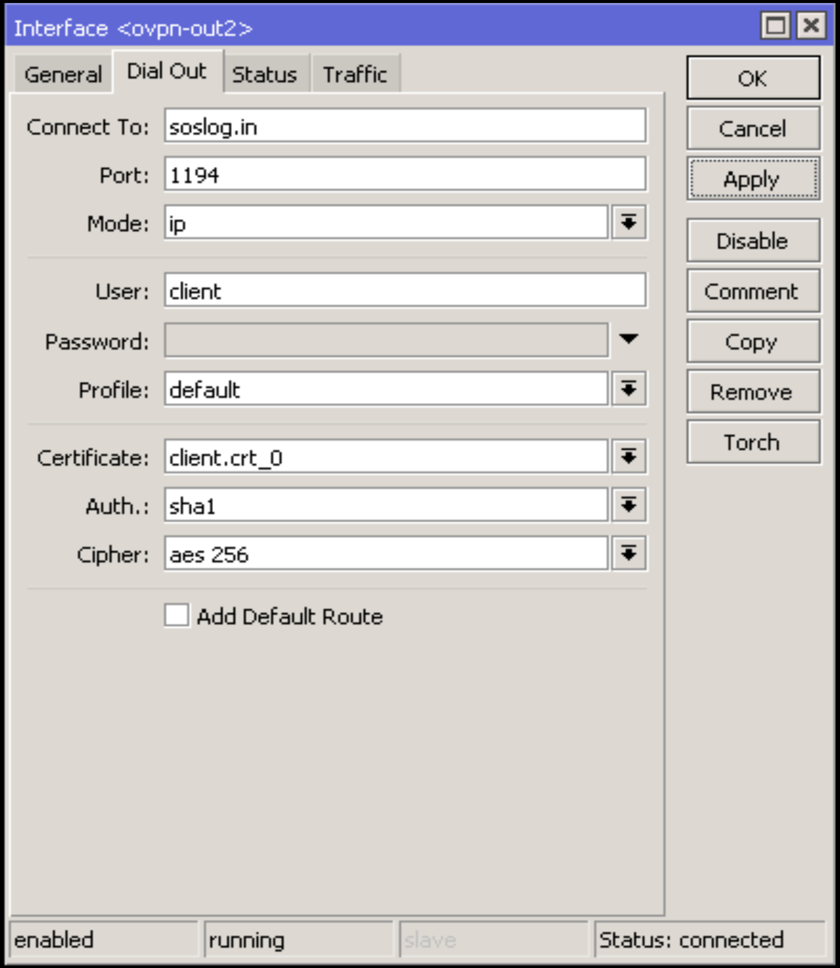
Certificate: server.crt_0

☑ Require Client Certificate

Auth.: ☑ sha1 ☑ md5 ☐ null

Cipher: ☑ blowfish 128 ☑ aes 128 ☐ aes 192 ☑ aes 256 ☐ null

Server



Interface <ovpn-out2>

Connect To: soslog.in

Port: 1194

Mode: ip

User: client

Password:

Profile: default

Certificate: client.crt_0

Auth.: sha1

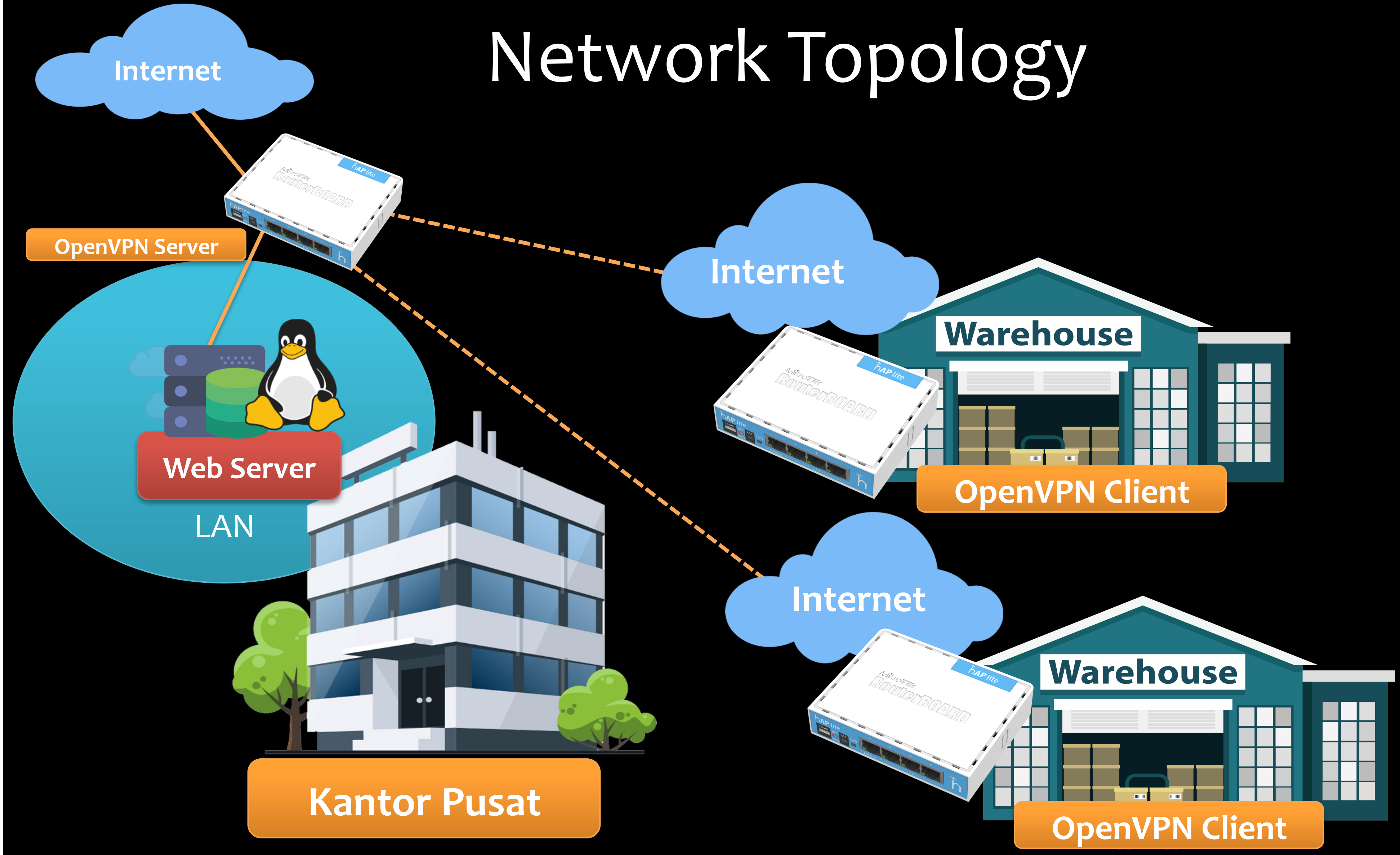
Cipher: aes 256

☐ Add Default Route

enabled | running | slave | Status: connected

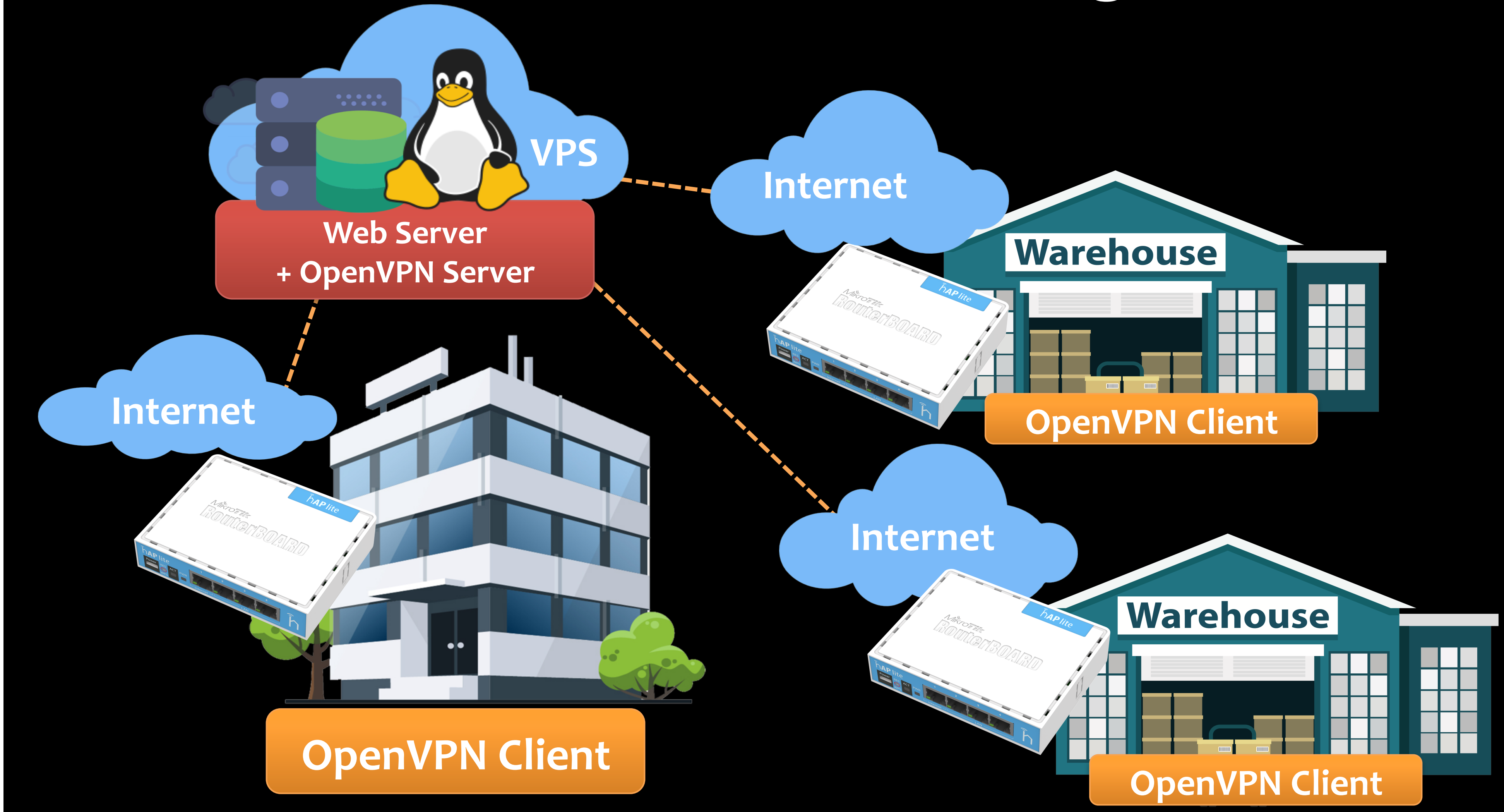
Client

Network Topology

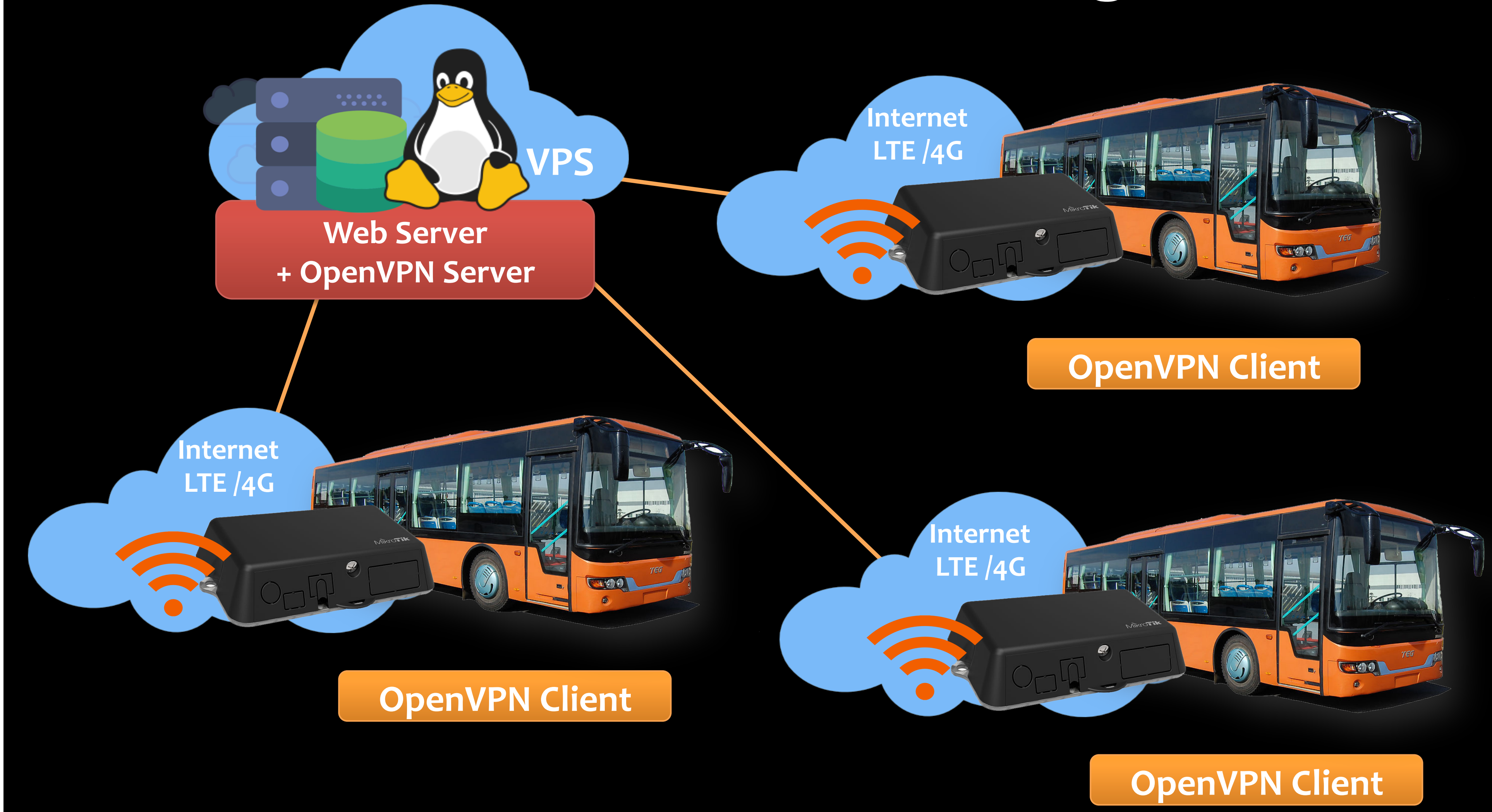


* On the OpenVPN Mikrotik server there must be a Public IP Static or if Dynamic IP Enable Cloud IP

Network Topology



Network Topology



VPS

Web Server
+ OpenVPN Server

Internet
LTE /4G

OpenVPN Client

Internet
LTE /4G

OpenVPN Client

Internet
LTE /4G

OpenVPN Client

VPS

7

configuration

```
yum update -y
wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
rpm -ivh epel-release-latest-7.noarch.rpm
yum install openvpn openssl

openssl dhparam -out /etc/openvpn/dh.pem 2048

openssl genrsa -out /etc/openvpn/ca.key 2048
chmod 600 /etc/openvpn/ca.key
openssl req -new -key /etc/openvpn/ca.key -out /etc/openvpn/ca.csr -subj /
CN=OpenVPN-CA/
openssl x509 -req -in /etc/openvpn/ca.csr -out /etc/openvpn/ca.crt -signkey /etc/
openvpn/ca.key -days 365
echo 01 > /etc/openvpn/ca.srl
```

```
openssl genrsa -out /etc/openvpn/server.key 2048
chmod 600 /etc/openvpn/server.key
openssl req -new -key /etc/openvpn/server.key -out /etc/
openvpn/server.csr -subj /CN=OpenVPN/
openssl x509 -req -in /etc/openvpn/server.csr -out /etc/
openvpn/server.crt -CA /etc/openvpn/ca.crt -CAkey /etc/
openvpn/ca.key -days 365

openssl genrsa -out /etc/openvpn/client.key 2048
chmod 600 /etc/openvpn/client.key
openssl req -new -key /etc/openvpn/client.key -out /etc/
openvpn/client.csr -subj /CN=OpenVPN-Client/
openssl x509 -req -in /etc/openvpn/client.csr -out /etc/
openvpn/client.crt -CA /etc/openvpn/ca.crt -CAkey /etc/
openvpn/ca.key -days 36525
```

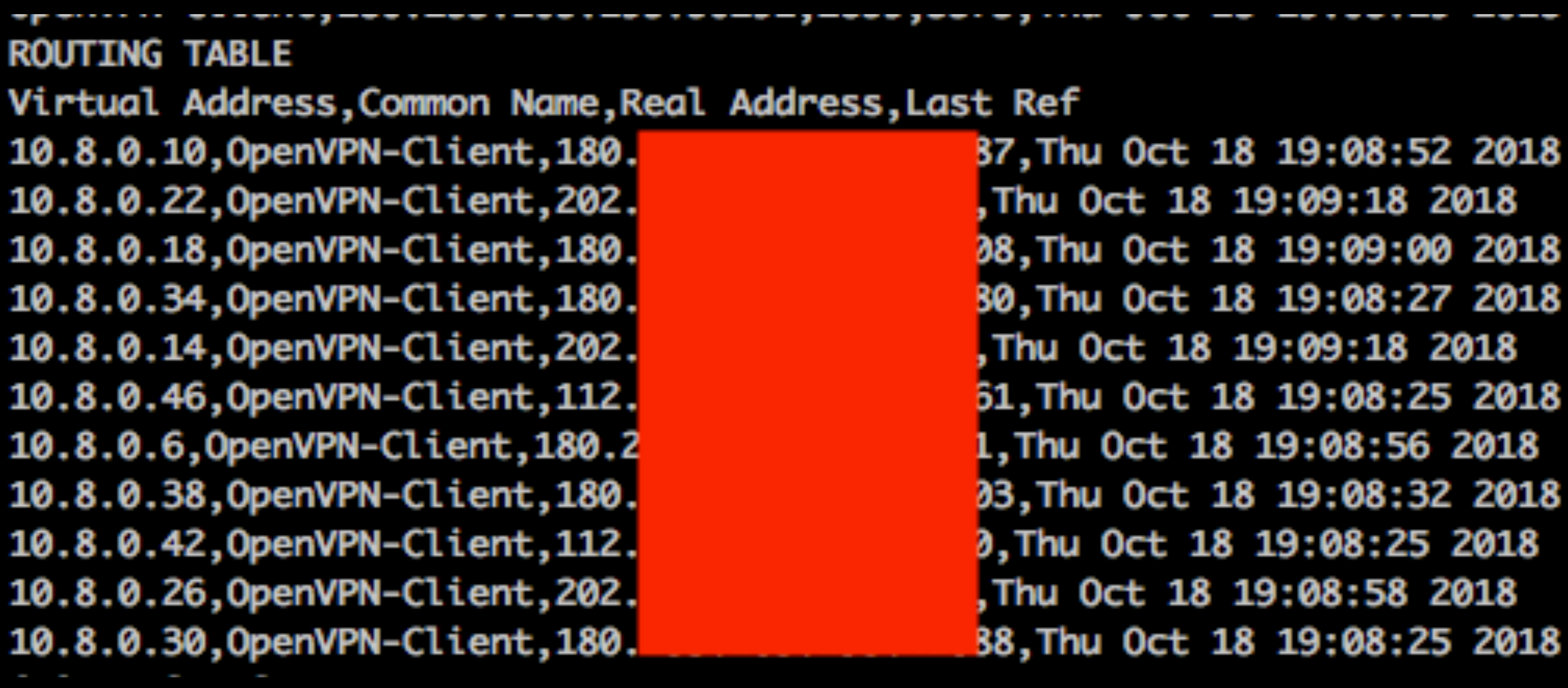
nano /etc/openvpn/server.conf

```
port 1194
proto tcp
dev tun1194
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key  # This file should be kept secret
dh /etc/openvpn/dh.pem
#client-config-dir /etc/openvpn/ccd
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-to-client
push "route 10.8.0.0 255.255.255.0"
push "redirect-gateway def bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
duplicate-cn
keepalive 10 120
cipher AES-256-CBC
;comp-lzo
user nobody
group nobody
persist-tun
status openvpn-status.log
verb 3
```

- systemctl enable openvpn@server
- systemctl start openvpn@server

** don't forget the firewalld or iptables set (according to each taste) ☺

tail -f /etc/openvpn/openvpn-status.log



```
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
10.8.0.10,OpenVPN-Client,180.[redacted]37,Thu Oct 18 19:08:52 2018
10.8.0.22,OpenVPN-Client,202.[redacted],Thu Oct 18 19:09:18 2018
10.8.0.18,OpenVPN-Client,180.[redacted]08,Thu Oct 18 19:09:00 2018
10.8.0.34,OpenVPN-Client,180.[redacted]30,Thu Oct 18 19:08:27 2018
10.8.0.14,OpenVPN-Client,202.[redacted],Thu Oct 18 19:09:18 2018
10.8.0.46,OpenVPN-Client,112.[redacted]61,Thu Oct 18 19:08:25 2018
10.8.0.6,OpenVPN-Client,180.2[redacted]1,Thu Oct 18 19:08:56 2018
10.8.0.38,OpenVPN-Client,180.[redacted]03,Thu Oct 18 19:08:32 2018
10.8.0.42,OpenVPN-Client,112.[redacted]0,Thu Oct 18 19:08:25 2018
10.8.0.26,OpenVPN-Client,202.[redacted],Thu Oct 18 19:08:58 2018
10.8.0.30,OpenVPN-Client,180.[redacted]38,Thu Oct 18 19:08:25 2018
```

Demo

Thank You

Special thanks to Shohibul Amin and Muhammad Riza Nurtam

More Info and discussion : teddy@cit.co.id