Compte rendu VPN

Commande vpn:

--remote : @ip ou fqdn indique l'adresse de serveur VPN
--local @ip indique quelle ip ou interface utiliser localement
--dev indique l'interface virtuelle
--port 1194 par défaut
--proto udp ou tcp
--verb mode verbeux 1à5
--ifconfig permet l'adressage virtuel du tunnel (ip remote)
--genkey génère une clef symétrique
--secret précise le fichier contenant la clef
--push pousse une instruction sur le client depuis le VPN
--server réseau et masque pour distribuer les ips virtuelles, la première est pour le serveur, désigne aussi le serveur TLS
--client désigne un client TLS
--dh précise les fichier concernant la clef de Diffie Hell mans
--ca précise les fichier concernant le certificat d'autorité
--cert précise les fichier concernant le certificat machine
--key précise les fichier concernant la clef privée machine

Installation des machines :

-commencer par installer une vm debian 11 de 30go et de 2go de RAM
-installer un client pour pouvoir faire les routes
-installer au serveur vpn les paquets suivant : apt install openssl && apt install openvpn && apt install ssh && apt install wireshark
-installer au client les paquets suivant : apt install openvpn && apt install ssh && apt install wireshark

Configuration des adresses des machines :

-attribuer des adresses aux deux machines, pour le client nous allons le mettre en dhcp (il aura donc pour adresse 172.17.1.16) et pour le vpn nous allons réserver une adresse dans le serveur dhcp :

```
host vpnjuju {
        hardware ethernet 00:15:5d:13:12:24;
        fixed-address 172.17.1.15;
}
```

Configuration du tunnel et du chiffrement:

- tunnel sur le serveur vpn : sudo openvpn --dev --verb 5 --ifconfig 192.168.0.3 192.168.0.4
-tunnel sur le client : sudo openvpn --dev --verb 5 --ifconfig 192.168.0.4 192.168.0.3 --remote 172.17.1.16
- une fois les deux tunnel fait, les lancer et ouvrir un wireshark le client pour pouvoir voir les trames sur eth0, faire un ping depuis le serveur vers le client : ping 192.168.0.4 ,on peut remarquer que le client ping fonctionne et observer le wireshark
- pour le chiffrement nous allons créer une clef sur le client : sudo openvpn --genkey --secret Fichierclef

- transférer la clef sur le serveur pour cela on va utiliser la commande scp depuis le serveur : scp -p root@172.17.1.16:/root/Fichierclef /etc/
- nous allons modifier le tunnel pour intégrer cette clef, pour le serveur: sudo openvpn --dev --verb 5 --secret /etc/Fichierclef --ifconfig 192.168.0.3 192.168.0.4
-pour le client : sudo openvpn --dev --verb 5 --secret Fichierclef --ifconfig 192.168.0.4 192.168.0.3 --remote 172.17.1.16

Création de certificat :
-créer les fichiers suivants : mkdir -p /apps/openvpn/keys && mkdir -p /apps/openvpn/log && mkdir -p /apps/openvpn/conf && mkdir -p /apps/pki-booktic
-faire une copie du répertoire /easy-rsa dans le dossier /apps/pki-booktic/ : cp -r /urs/share/easy-rsa /apps/pki-booktic pour voir si cela a bien fonctionner faire : ls /apps/pki-booktic
-se placer dans le fichier : cd /apps/pki-booktic/easy-rsa et faire rm vars.example vars pour renommer se fichiers
-faire nano vars et retirer le # des lignes suivantes et les modifier :

```
set_var EASYRSA_REQ_COUNTRY     "Fr"
set_var EASYRSA_REQ_PROVINCE    "France"
set_var EASYRSA_REQ_CITY        "Franconville"
set_var EASYRSA_REQ_ORG         "certif"
set_var EASYRSA_REQ_EMAIL       "vpn@juju"
set_var EASYRSA_REQ_OU          "booktic"
```

(faire les commande suivante sur le serveur vpn : et dans le dossier /apps/pki-booktic/easy-rsa)
- faire la commande ./easyrsa init-pki cela nous donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa init-pki

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /apps/pki-booktic/easy-rsa/pki
```

-
faire le commande ./easyrsa init-pki build-ca nopass cela nous donne :

```
Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating RSA private key, 2048 bit long modulus (2 primes)
............+++++
.....................................+++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CA

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/apps/pki-booktic/easy-rsa/pki/ca.crt
```

-faire le commande ./easyrsa gen-req vpnjuju nopass cela nous donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa gen-req vpnjuju nopass

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating a RSA private key
............+++++
.....................................................................+++++
writing new private key to '/apps/pki-booktic/easy-rsa/pki/easy-rsa-10486.qBc3Ws/tmp.s2pE3U'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

-faire le commande ./easyrsa gen-req clientvpnjuju nopass cela nous donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa gen-req clientvpnjuju nopass

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating a RSA private key
......+++++
.................................+++++
writing new private key to '/apps/pki-booktic/easy-rsa/pki/easy-rsa-10508.oE2yvI/tmp.NdhADx'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [clientvpnjuju]:clientvpnjuju

Keypair and certificate request completed. Your files are:
req: /apps/pki-booktic/easy-rsa/pki/reqs/clientvpnjuju.req
key: /apps/pki-booktic/easy-rsa/pki/private/clientvpnjuju.key
```

-faire la commande : sudo openvpn --genkey --secret /apps/openvpn/keys/bookticsign.key
cela nous donne :

```
root@vpnjuju:~# sudo openvpn --genkey --secret /apps/openvpn/keys/bookticsign.key
2022-10-20 11:57:51 WARNING: Using --genkey --secret filename is DEPRECATED.  Use --genkey secret fil
ename instead.
```

-faire le commande ./easyrsa sign-req server vpnjuju pour signer le certificat cela nous
donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa sign-req server vpnjuju

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
    commonName                = vpnjuju


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /apps/pki-booktic/easy-rsa/pki/easy-rsa-10564.gMzMJS/tmp.INyL2u
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'vpnjuju'
Certificate is to be certified until Jan 22 09:14:18 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /apps/pki-booktic/easy-rsa/pki/issued/vpnjuju.crt
```

--faire le commande ./easyrsa sign-req client clientvpnjuju pour signer le certificat
cela nous donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa sign-req client clientvpnjuju

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 825 days:

subject=
    commonName                = clientvpnjuju


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /apps/pki-booktic/easy-rsa/pki/easy-rsa-10632.X3YL9p/tmp.bL4Xgc
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'clientvpnjuju'
Certificate is to be certified until Jan 22 09:17:16 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /apps/pki-booktic/easy-rsa/pki/issued/clientvpnjuju.crt
```

-faire la commande ./easyrsa gen-dh pour créer une clef de session cela nous donne :

```
root@vpnjuju:/apps/pki-booktic/easy-rsa# ./easyrsa gen-dh

Note: using Easy-RSA configuration from: /apps/pki-booktic/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1n  15 Mar 2022
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....................................................+.................+.........................
.....................+.....................................................+.........
...............+.........................................+.....................................
.....................................................................+.............................
.....................................+.............+.....................................................
.............................+.....................................................................+
...................................................................................................
.....................................................................+........+.....................
.....................................................................................+.....
.....................................................................+.............................
...................................................................................................
...................................................................................................
.....................................................+.............................................
.....................................................+.............................................
...+...............................................................................................+...
...................................................................................................
......+............................................................................................
.............................+.....................................................................
..+.........................++*++*++*++*

DH parameters of size 2048 created at /apps/pki-booktic/easy-rsa/pki/dh.pem
```

-

(sur le client)

-créer le dossier certif dans etc : mkdir /etc/cerfif pour pouvoir mettre les fichier qui vont être transférer
- avec scp – root@172.17.1.15:/apps/pki-booktic/easy-rsa/pki/private/clientvpnjuju.key /etc/certif
cette commande permet de déplacer clientvpnjuju.key du vpn vers le dossier certif du client
- avec scp – root@172.17.1.15:/apps/pki-booktic/easy-rsa/pki/issued/clientvpnjuju.crt /etc/certif
cette commande permet de déplacer clientvpnjuju.crt du vpn vers le dossier certif du client
- avec scp – root@172.17.1.15:/apps/pki-booktic/easy-rsa/pki/ca.crt /etc/certif
cette commande permet de déplacer ca.crt du vpn vers le dossier certif du client
- avec scp – root@172.17.1.15:/apps/openvpn/keys/ bookticsign.key /etc/certif
cette commande permet de déplacer bookticsign.key du vpn vers le dossier certif du client
- faire un ls dans le dossier /etc/certif pour voir si on a bien déplacer les fichiers, c'est sensé donner cela :

```
root@clientvpnjuju:/etc/certif# ls
bookticsign.key  ca.crt  clientvpnjuju.crt  clientvpnjuju.key
```

Configuration du serveur:

- créer dossier: mkdir -p /apps/openvpn/conffiles/
- se placer dans ce fichier: cd /apps/openvpn/conffiles/ et lui créer un fichier : touch bookticVPN.conf
- déplacer les fichiers: dh.pem / vpnjuju.key / vpnjuju.crt /ca.crt / bookticsign.key dans les dossier
-faire nano bookticVPN.conf

```
proto udp
dev tun
ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/vpnjuju.crt
key /apps/openvpn/keys/vpnjuju.key
dh /apps/openvpn/keys/dh.pem
tls-auth /apps/openvpn/keys/bookticsign.key 0

server 192.168.0.0 255.255.0.0
client-to-client
explicit-exit-notify 1
keepalive 10 120
persist-key
persist-tun
cipher AES-256-CBC
compress lz4-v2
status openvpn-status.log
log     /apps/openvpn/log/openvpn.log
log-append      /apps/openvpn/log/openvpn.log
verb 5
```

-faire la commande: ls -n /apps/openvpn/conffiles/bookticVPN.conf /etc/openvpn/bookticVPN.conf
-faire la commande systemctl restart openvpn@bookticVPN

Configuration du client :

-créer le dossier : mkdir -p /apps/openvpn/keys et lui ajouter en copiant les fichier : ca.crt / bookticsign.key /clientvpnjuju.crt / clientvpnjuju.key qui se trouve dans le dossier /etc/certif
-créer un fichier dans /etc/openvpn : touch MonCltVPN.conf et faire cd /etc/openvpn/
-nano MonCltVPN.conf

```
client
dev tun
proto udp
remote 172.17.1.15 1194

resolv-retry infinite
nobind

persist-key
persist-tun
mute-replay-warnings

ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/clientvpnjuju.crt
key /apps/openvpn/keys/clientvpnjuju.key
tls-auth /apps/openvpn/keys/bookticsign.key 1

cipher AES-256-CBC
compress lz4-v2
verb 5
```

-faire la commande: ls -n /apps/openvpn/conffiles/MonCltVPN.conf /etc/openvpn/MonCltVPN.conf

(sur le serveur)
- redémarrer le serveur : systemctl restart openvpn
-pour voir si cela a bien fonctionner il faut aller voir le fichier de log : nano /apps/openvpn/log/openvpn.log et on doit retrouver une ligne avec des WR à la fin de fichier :

```
2022-10-20 15:35:28 us=587403 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit k
2022-10-20 15:35:28 us=587419 SENT CONTROL [clientvpnjuju]: 'PUSH_REPLY,route 192.168.0.0 255.255.0.
WRRRWRWRWRWRWWRRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWRWR
```

<u>Routage sur le serveur et redirection sur le pare-feu :</u>

(sur le client)
-le mettre dans le vlan 60 et faire : systemctl restart networking pour que l'on puisse faire le changement d'adresse et faire la commande ip a pour voir que cela est bien fonctionner

(sur le serveur)
-dans le fichier /etc/sysctl.conf retirer le # de la ligne suivante net.ipv4_ipforward=1
-écrire la commande iptables -t nat -A POSTROURING -o eth0 -j MASQUERADE pour masquer toutes les ips sortant du tunnel vers le réseau
-dans le fichier /etc/openvpn/bookticVPN.conf rajouter la ligne suivant : push "route 172.17.1.15 *<ip de serveur>* 255.255.255.0 *<son masque>*

(sur le pare-feu)
-faire une règles :

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐ ✔ ⇄	WAN	UDP	*	*	WAN address	1194 (OpenVPN)	172.17.1.15	1194 (OpenVPN)		