Zone	Réseau	Masque	Usage
WAN	10.252.3.0/23	255.255.255.0	NAT VirtualBox / Internet
LAN	192.168.129.0/24	255.255.255.0	Services internes, DHCP, postes de test
VPN	10.0.8.0/24	255.255.255.0	Pool d’adresses pour clients OpenVPN

Équipement	Interface	IP	Interface
Firewall	WAN	dhcp	via NAT VirtualBox
	VPN	10.0.8.1	gateway VPN
	LAN	192.168.129.1	gateway LAN
Load-balancer (HAProxy)	–	192.168.129.10	LAN
Web #1	–	192.168.129.10	LAN
Web #2	–	192.168.129.11	LAN
Mail (Postfix/Dovecot)	–	192.168.129.14	LAN
LDAPS	–	192.168.129.12	LAN
NFS	–	192.168.129.13	LAN
DHCP (isc-dhcp-server)	–	192.168.129.2	LAN
DNS (BIND9)	–	192.168.129.2	LAN
Client Linux	–	DHCP	WAN

https://www.canva.com/design/DAGqfjuncUc/NxtaPPxMek61eMke1mdnZg/edit?utm_content=DAGqfjuncUc&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

3. Configuration DHCP (exemple pour 10.0.20.0/24)

CONFIGURATION DHCP:

```
default-lease-time 600;
max-lease-time 7200;
authoritative;

subnet 192.168.129.0 netmask 255.255.255.0 {
  range 192.168.129.100 192.168.129.200;
  option routers 192.168.129.1;
  option domain-name-servers 192.168.129.2;
  option domain-name "kelpeter.fr";
}
```

```
sudo nano /etc/default/isc-dhcp-server
INTERFACESv4="enp0s3"
INTERFACESv6=""
```

Modificationsur les machines statics dans /etc/resolv.conf :

```
nameserver 192.168.129.2
```

OpenVPN:

```
sudo openvpn --config client.ovpn
```

```
<ca>
-----BEGIN CERTIFICATE-----...
-----END CERTIFICATE-----
</ca>

<cert>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
</key>
<tls-auth>
-----BEGIN OpenVPN Static key V1-----
-----END OpenVPN Static key V1-----
</tls-auth>
```

Docker :
sudo apt update
sudo apt install docker.io docker-compose -y
sudo systemctl enable docker
sudo systemctl start docker

/opt/network-services/
docker-compose.yml :

```
version: "3.9"

services:
  dhcp:
    image: networkboot/dhcpd
    container_name: dhcp
    network_mode: host
    volumes:
      - ./dhcp:/data
      - /var/lib/dhcp:/var/lib/dhcp
    environment:
      - INTERFACES=enp0s3
    restart: unless-stopped

  bind9:
    restart: always
    image: ubuntu/bind9:latest
    container_name: bind9
    ports:
      - "53:53/tcp"
      - "53:53/udp"
    volumes:
      - ./bind:/etc/bind
```

docker-compose down && docker-compose up -d

ip link set enp0s8 up
ip addr add 192.168.56.2/24 dev enp0s8

docker run -it --rm --entrypoint /bin/sh internetsystemsconsortium/bind9:9.18

/usr/sbin/named -g -u bind

HaProxy :

```
frontend https_front
    bind *:443 ssl crt /etc/ssl/certs/haproxy/haproxy.pem
    mode http
    default_backend web_servers

backend web_servers
    balance roundrobin
    server srv-web-1 192.168.129.10:80 check
    server srv-web-2 192.168.129.11:80 check
```

```
cat Certificat-WWW.crt Certificat-WWW.key > /etc/ssl/certs/haproxy/www.pem
```

Voici un rappel rapide des différents fichiers LDIF que tu as créés :

- **group.ldif** :
  Sert à créer une branche ou unité organisationnelle (Organizational Unit) `ou=Group` dans l'annuaire, où tu stockeras les groupes.
  Exemple : groupes d'utilisateurs.

- **people.ldif** :
  Sert à créer une branche ou unité organisationnelle `ou=People` dans l'annuaire, où tu stockeras les utilisateurs (les personnes).
  Cette séparation est une bonne pratique pour organiser ton annuaire :

  - `ou=People` pour les utilisateurs
  - `ou=Group` pour les groupes

- **myusers.ldif** :
  Sert à créer un groupe précis dans la branche `ou=Group`. Par exemple, un groupe `cn=myusers`.

- Ensuite, tu peux créer des utilisateurs sous la branche `ou=People` (avec des fichiers LDIF spécifiques à chaque utilisateur).

```
ldapadd -x -D "cn=admin,dc=kelpeter,dc=fr" -W -f people.ldif
ldapadd -x -D "cn=admin,dc=kelpeter,dc=fr" -W -f group.ldif
ldapadd -x -D "cn=admin,dc=kelpeter,dc=fr" -W -f myusers.ldif
ldapadd -x -D "cn=admin,dc=kelpeter,dc=fr" -W -f marius.ldif

ldapsearch -x -b "dc=kelpeter,dc=fr" "(objectClass=*)" | less
ldapsearch -x -b "ou=People,dc=kelpeter,dc=fr"
ldapsearch -x -b "ou=Group,dc=kelpeter,dc=fr"

ldapmodify -x -D "cn=admin,dc=kelpeter,dc=fr" -W -f /root/gecos.ldif

ldapsearch -x -D "cn=admin,dc=kelpeter,dc=fr" -W -b
"uid=marius,ou=People,dc=kelpeter,dc=fr" userPassword
```

ldapsearch -H ldaps://ldaps.kelpeter.fr -D "cn=admin,dc=kelpeter,dc=fr" -W -b "dc=kelpeter,dc=fr" "uid=marius,ou=People,dc=kelpeter,dc=fr"

debug:
LDAPTLS_REQCERT=never ldapsearch -d 256 -H ldaps://ldaps.kelpeter.fr -D "cn=admin,dc=kelpeter,dc=fr" -W -b "dc=kelpeter,dc=fr" "(uid=marius)"

Machine / Service	Certificat à installer	Où stocker la clé privée et le certificat public
PKI / CA (192.168.129.3)	– Certificat racine (CA)	Conserve **toujours** la clé privée du CA ici, ne la copiez nulle part ailleurs.
LDAP (192.168.129.3)	Certificat `ldap.mondomaine.local`	`/etc/ssl/private/ldap.key` + `/etc/ssl/certs/ldap.crt`
OpenVPN (10.10.10.13)	Certificat `vpn.mondomaine.local`	`/etc/openvpn/server/vpn.key` + `/etc/openvpn/server/vpn.crt`
Mail (Postfix/Dovecot) (10.10.10.14)	Certificat `mail.mondomaine.local`	`/etc/ssl/private/mail.key` + `/etc/ssl/certs/mail.crt`
Load-Balancer (HAProxy) (10.10.10.2)	Certificat `www.mondomaine.local`	Si TLS en terminaison ici : `/etc/haproxy/certs/www.pem` (concat clé+certificat)
Web #1 (10.10.10.11) & Web #2 (10.10.10.12)	Certificat `www.mondomaine.local`	`/etc/ssl/private/www.key` + `/etc/ssl/certs/www.crt`
Clients Linux & Windows	Certificat racine (CA)	Importez le fichier `ca.crt` dans le magasin de confiance (OS / OpenVPN / mail).

mount -a
mount nfs.kelpeter.fr:/srv/partagenfs/home /home/

su - marius
marius
touch text.txt
bien sur les deux fichiers

SQUID:
curl -vk --proxy http://localhost:3128 https://www.kelpeter.fr