Infrastructure & Réseaux

I) Mise en place de l’infrastructure du système et réseau

1. Déploiement d'un serveur web

Nginx

- **Installation :**

```
sudo apt update
 sudo apt install nginx
```

Configuration :

Le fichier de configuration principal se trouve dans /etc/nginx/nginx.conf.
Les fichiers de configuration des sites se trouvent dans /etc/nginx/sites-available/ et les liens symboliques dans /etc/nginx/sites-enabled/.
Démarrage et gestion du service :

```
sudo systemctl start nginx
sudo systemctl enable nginx
```

Apache

Installation :

```
sudo apt update
sudo apt install apache2
```

Configuration :

Le fichier de configuration principal se trouve dans /etc/apache2/apache2.conf.
Les fichiers de configuration des sites se trouvent dans /etc/apache2/sites-available/ et

les liens symboliques dans /etc/apache2/sites-enabled/.
Démarrage et gestion du service :

```
sudo systemctl start apache2
sudo systemctl enable apache2
```

2. Déploiement d'un serveur de base de données

PostgreSQL
Installation :

```
sudo apt update
sudo apt install postgresql postgresql-contrib
```

Configuration :

Le fichier de configuration principal se trouve dans **/etc/postgresql/(version)/main/postgresql.conf.**

Configuration de l'accès réseau dans /etc/postgresql/(version)/main/pg_hba.conf.
Démarrage et gestion du service :

```
sudo systemctl start postgresql
sudo systemctl enable postgresql
```

MySQL

Installation :

```
sudo apt update
sudo apt install mysql-server
```

Configuration :

Le fichier de configuration principal se trouve dans /etc/mysql/mysql.conf.d/mysqld.cnf.
Démarrage et gestion du service :

```
sudo systemctl start mysql
sudo systemctl enable mysql
```

3. Déploiement d'un serveur de messagerie

Postfix

Installation :

```
sudo apt update
sudo apt install postfix
```

Configuration :

Le fichier de configuration principal se trouve dans /etc/postfix/main.cf.
Démarrage et gestion du service :

```
sudo systemctl start postfix
sudo systemctl enable postfix
```

4. Déploiement d'un serveur DNS

Bind

Installation :

```
sudo apt update
sudo apt install bind9
```

Configuration :

Les fichiers de configuration se trouvent dans /etc/bind/named.conf et ses inclusions.
Démarrage et gestion du service :

```
sudo systemctl start bind9
sudo systemctl enable bind9
```

II) Mise en place d’un pare-feu

Configuration d'un pare-feu avec iptables
Installation (si nécessaire) :

```
sudo apt update
sudo apt install iptables
```

Configuration de base :

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j
ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -j DROP
```

Sauvegarde des règles :

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

Utilisation d'un outil de gestion de pare-feu (ufw)

Installation :

```
sudo apt update
sudo apt install ufw
```

Configuration :

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw enable
```

III) Maîtrise du routage dynamique (DHCP)

Configuration d'un serveur DHCP
Installation de DHCP server (ISC DHCP Server)

```
sudo apt update
sudo apt install isc-dhcp-server
```

Configuration :

Le fichier de configuration principal se trouve dans /etc/dhcp/dhcpd.conf.
Exemple de configuration :

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.100;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1, 8.8.8.8;
  option domain-name "localdomain";
}
```

Démarrage et gestion du service :

```
sudo systemctl start isc-dhcp-server
sudo systemctl enable isc-dhcp-server
```

IV) Sécurité des serveurs

1. Chiffrement des bases de données

PostgreSQL avec SSL/TLS
Génération des certificats SSL :

```
sudo mkdir /etc/postgresql/ssl
sudo openssl req -new -x509 -days 365 -nodes -out
/etc/postgresql/ssl/server.crt -keyout /etc/postgresql/ssl/server.key
sudo chmod 600 /etc/postgresql/ssl/server.key
```

Configuration de PostgreSQL pour utiliser SSL :

Modifier postgresql.conf :

```
ssl = on
ssl_cert_file = '/etc/postgresql/ssl/server.crt'
ssl_key_file = '/etc/postgresql/ssl/server.key'
```

Redémarrer le service PostgreSQL :

```
sudo systemctl restart postgresql
```

2. Utilisation du protocole HTTPS pour le serveur web

Nginx avec Let's Encrypt
Installation de Certbot :

```
sudo apt update
sudo apt install certbot python3-certbot-nginx
```

Obtention et installation du certificat SSL :

```
sudo certbot --nginx -d example.com -d www.example.com
```

Renouvellement automatique des certificats :

```
sudo certbot renew --dry-run
```

3. Définition de règles d'accès réseau strictes

Configuration des règles dans iptables :

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 5432 -s 192.168.1.0/24 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -j DROP
```

Enregistrer les règles :

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```