

# **Présentation De Quelques Fonctionnalités Du Routeur Mikrotik**

**Sommaire:**

Listes des figures : .....	2
Introduction.....	3
I. Proposons Une Architecture Technique Du Projet .....	4
II. Implémentons Les Techniques : Bridge, DHCP, NAT, DNS; .....	5
1. Bridge.....	5
2. Serveur DHCP .....	6
3. Serveur DNS .....	6
4. NAT.....	7
5. Vérification des configurations.....	8
III. Implémentation De Quelques Fonctionnalités Clés.....	10
a) Firewall .....	11
b) QoS (Quality of Service) .....	14
c) Hotspot.....	15
d) VPN.....	20
IV. Configuration Avancées Du Routeur Mikrotik .....	25
1. Gestion Des Utilisateurs Et Groupes .....	25
2. Sauvegarde Et Restauration Des Configurations De Mikrotik .....	28
a. Sauvegarde et restauration via fichier binaire (.backup) .....	29
b. Export et import de la configuration en fichier texte.....	29
3. Bloquer l'accès certains sites Web.....	31
Conclusion .....	34
Bibliographie.....	35

## **Listes des figures :**

Figure 1: Architecture de notre réseau de test.....	4
Figure 2: Architecture de notre réseau dans le logiciel GNS3 .....	5
Figure 3: Configuration du Serveur DHCP .....	6
Figure 4: Configuration du serveur DNS .....	7
Figure 5: Configuration du NAT .....	8
Figure 6: Test de fonctionnement du DHCP et DNS sur kali.....	9
Figure 7: Test de fonctionnement DHCP et DNS sur PC2.....	9
Figure 8: Navigation sur internet depuis kali .....	10
Figure 9: Autorisation de l'accès SSH de kali vers le serveur Web.....	12
Figure 10: Bloquer l'accès SSH au serveur web pour tous les autres.....	13
Figure 11: Accès au serveur web depuis Kali.....	14
Figure 12: Configuration des bandes passantes download et upload pour Kali .....	14
Figure 13: Création du Hotspot.....	16
Figure 14: Création du profile étudiant .....	17
Figure 15: Liste des profiles créés.....	18
Figure 16: Création d'un utilisateur du hotspot.....	18
Figure 17: Liste des utilisateurs du hotspot .....	19
Figure 18: Portail captif en action .....	19
Figure 19: Connexion d'un utilisateur au portail captif.....	20
Figure 20: Création d'une proposition pour le VPN .....	21
Figure 21: Création d'un peer pour le VPN .....	22
Figure 22: Création de l'identité .....	23
Figure 23: Configuration de la politique du VPN.....	23
Figure 24: Configuration des règles NAT pour le VPN .....	24
Figure 25: VPN site-to-site réussi .....	25
Figure 26: Création d'un compte utilisateur du Mikrotik.....	26
Figure 27: Liste des comptes utilisateurs de Mikrotik.....	26
Figure 28: Création d'un groupe d'utilisateur.....	28
Figure 29: Sauvegarde dans un fichier binaire .....	29
Figure 30: Exportation du fichier de configuration .....	30
Figure 31: Fichiers de restauration exporté .....	30
Figure 32: Importation du fichier de configuration .....	31
Figure 33: Configuration de Walled Garden.....	32
Figure 34: Liste des sites bloqués.....	32
Figure 35: Impossible d'accéder à YouTube .....	33

## Introduction

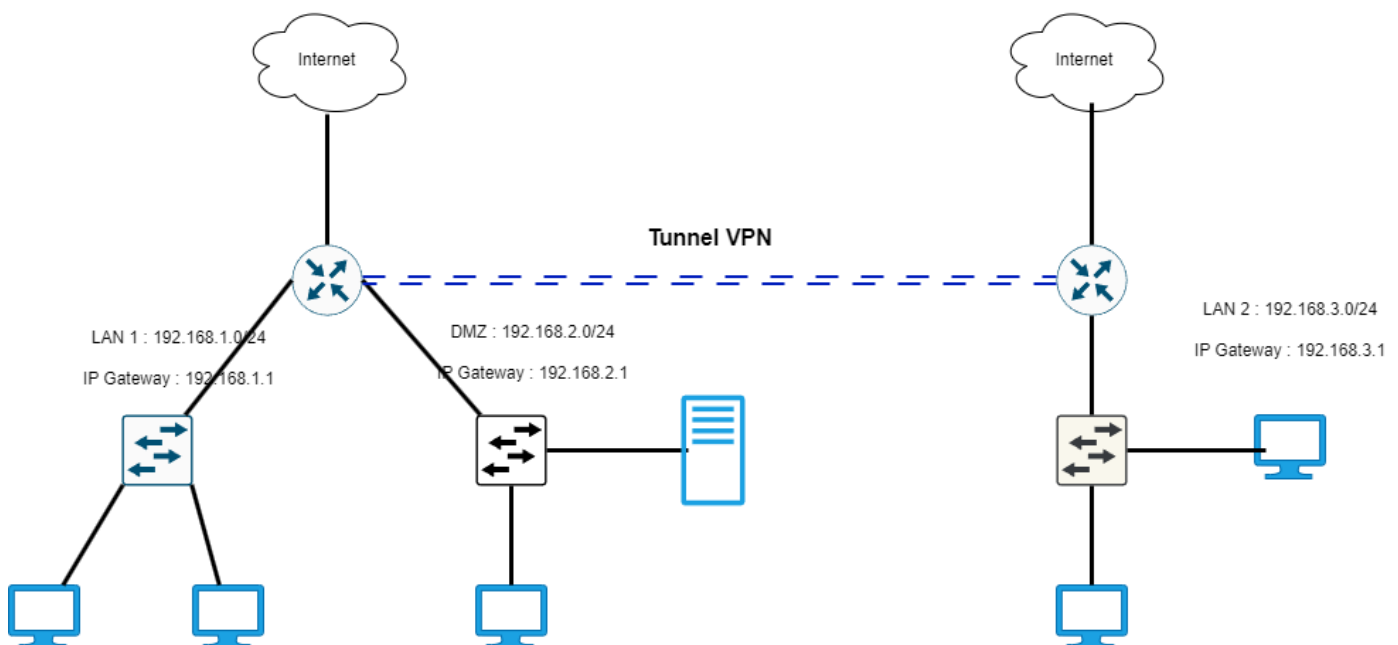
Ce travail pratique explore les fonctionnalités des routeurs **MikroTik**, des équipements reconnus pour leur polyvalence et leur robustesse dans les environnements réseau variés. L'objectif principal est de mettre en œuvre et de tester différentes configurations réseau courantes en entreprise, en tirant parti de l'environnement de simulation **GNS3**. Grâce à **GNS3**, nous pouvons modéliser fidèlement une infrastructure réseau complexe, incluant plusieurs routeurs MikroTik interconnectés, des commutateurs, et des machines virtuelles simulant des clients et des serveurs. Ce TP permettra de manipuler les outils de configuration de MikroTik (Winbox et CLI) et de comprendre les concepts clés tels que le routage, les VPNs site-to-site, les règles de pare-feu et la gestion de la qualité de service (QoS). La topologie réseau utilisée pour ce TP est la suivante : deux sites distants reliés par un VPN, chacun ayant un routeur MikroTik, des clients et des serveurs.

## I. Proposons Une Architecture Technique Du Projet

Pour réaliser notre projet et mettre en évidence les fonctionnalités principales de la technologie Mikrotik, nous avons opté pour l'architecture contenant les éléments suivants :

- ✓ **02 routeurs Mikrotik** : L'objectif est de mettre en évidence la communication sécurisée en utilisant le VPN. Le routeur 1 est relié au site 1 de l'entreprise et située dans la ville de Bafoussam tandis que le routeur 2 se trouve dans le site 2 de l'entreprise et se trouve à Yaoundé.
- ✓ **LAN 1** : qui est vu dans notre architecture comme le réseau interne de l'entreprise dans la succursale 1 ;
- ✓ **DMZ** : qui est la zone contenant les serveurs dans le site 1 ;
- ✓ **LAN 2** : qui est considéré dans notre architecture comme le réseau interne de l'entreprise dans le site 2 ;
- ✓ **02 Cloud** : ils permettent de simuler le Fournisseur d'accès internet dans nos différentes succursales ;

Une représentation de notre architecture réseau est le suivant :



*Figure 1: Architecture de notre réseau de test*

## II. Implémentons Les Techniques : Bridge, DHCP, NAT, DNS;

### 1. Bridge

Le **Bridge** est une fonctionnalité qui permet de faire en sorte que plusieurs ports d'un routeur se trouvent dans le même réseau car les interfaces d'un routeur sont conçues pour être dans des réseaux distincts les uns des autres. Cela est très important lorsque nous n'avons pas de switch à notre portée.

Dans notre cas, nous avons utilisé l'application de simulation réseau **GNS3** qui nous donne la possibilité de simuler, émuler et virtualiser notre réseau d'entreprise. Nous n'avons pas eu besoin de configurer le bridge car nous avons des commutateurs dans notre architecture.

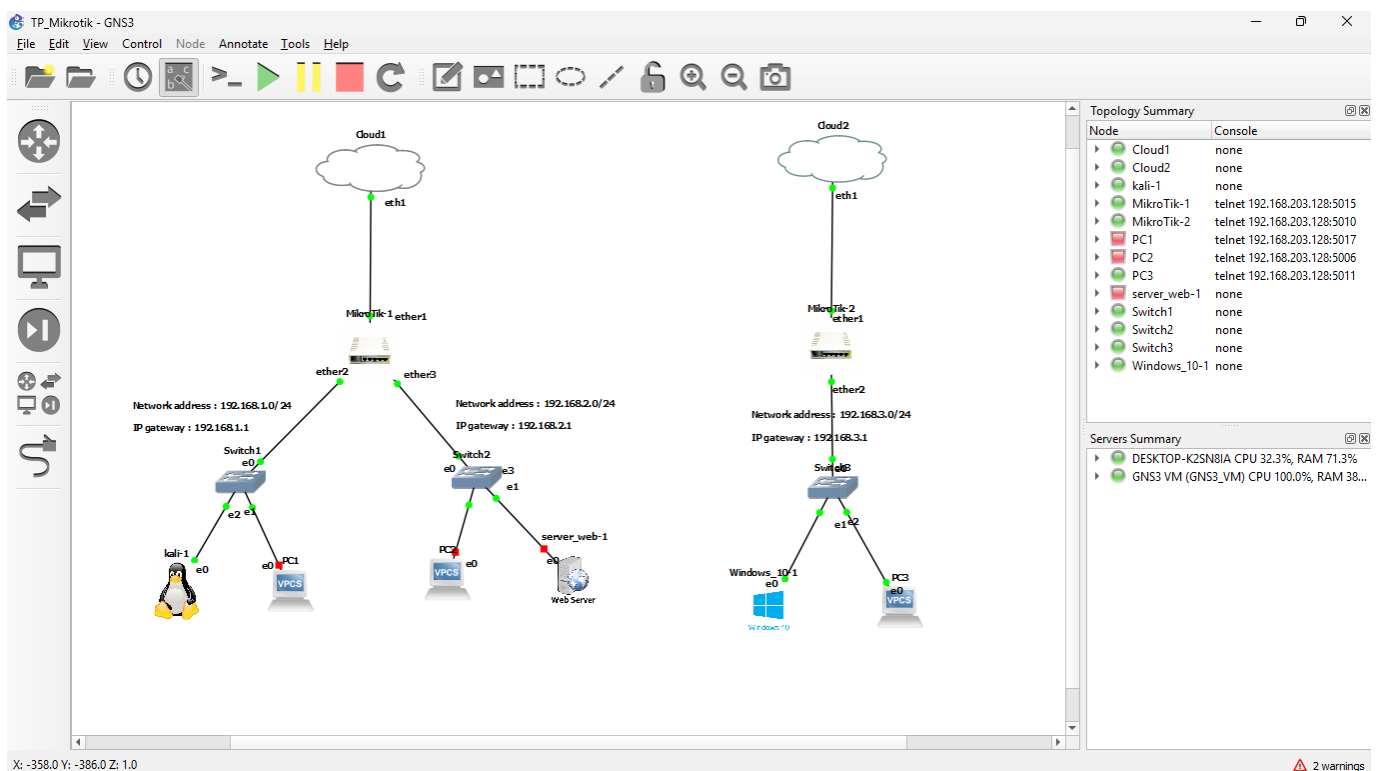
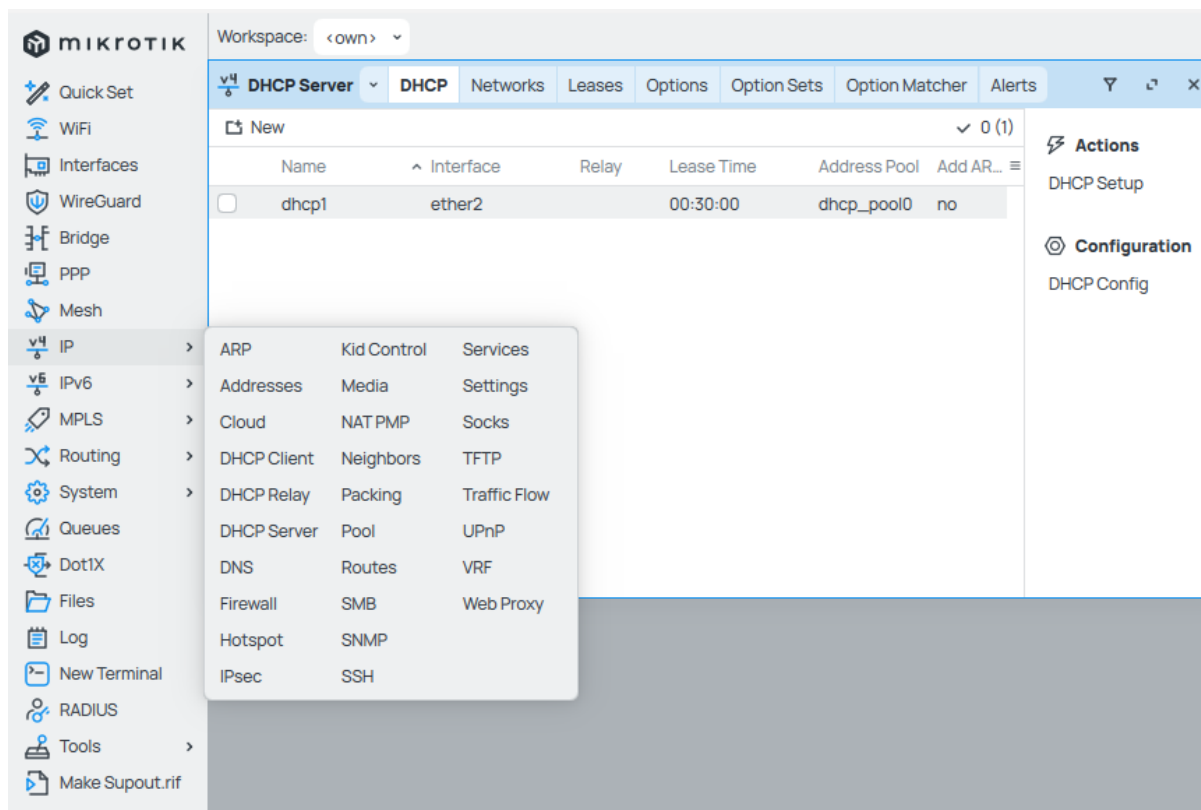


Figure 2: Architecture de notre réseau dans le logiciel GNS3

## 2. Serveur DHCP

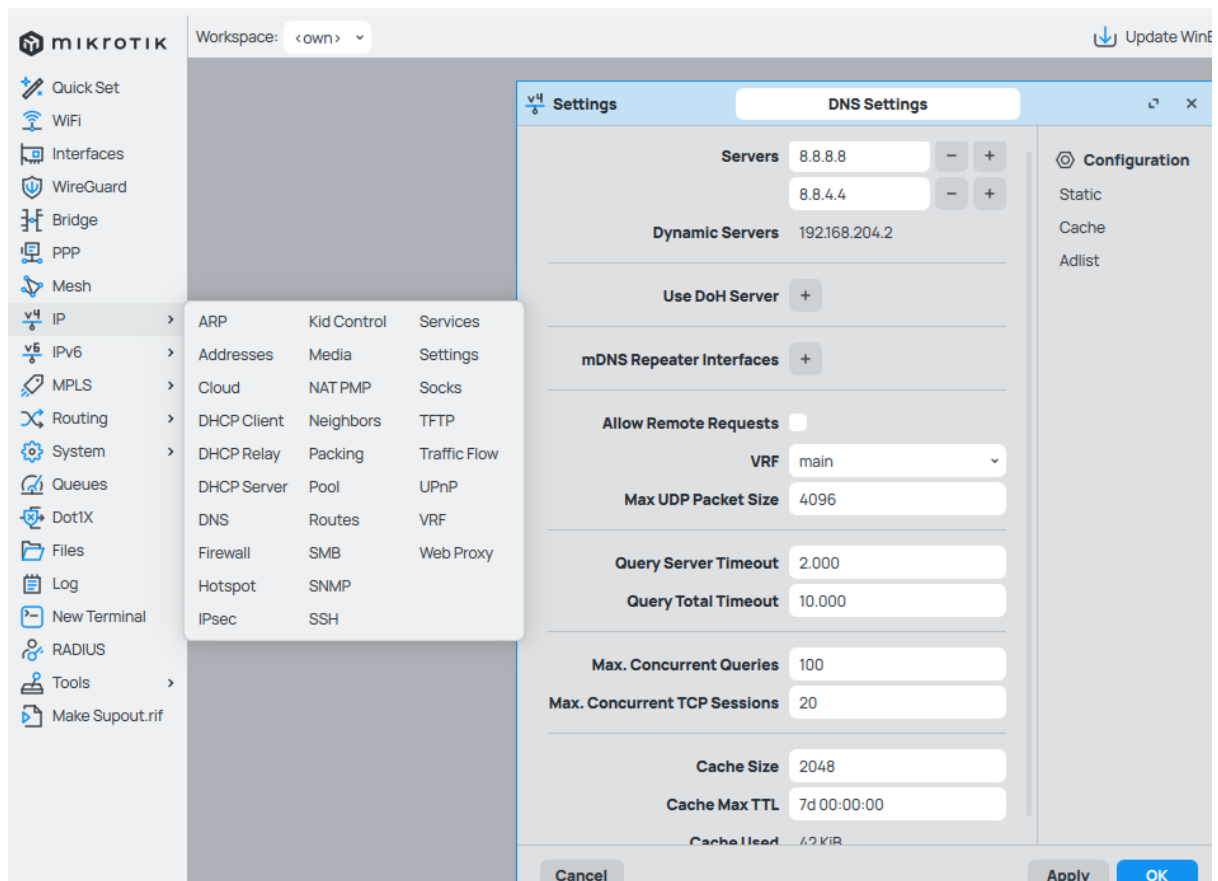
**Le serveur DHCP :** Cette fonctionnalité donne la possibilité au routeur Mikrotik d'adresser dynamiquement les machines qui sont liées à une de ses interfaces. Pour configurer cela, nous allons sur *ip/dhcp server/DHCP setup* et vous renseigner les différents champs.



*Figure 3: Configuration du Serveur DHCP*

## 3. Serveur DNS

**Serveur DNS :** Cette fonctionnalité permet à notre routeur Mikrotik de s'occuper de la résolution de nom de domaine en adresse IP. Dans notre cas, nous avons décidé d'utiliser le serveur DNS de notre fournisseur d'accès internet, car nous activons le client DHCP sur notre interface qui est reliée à internet. Si vous souhaitez configurer le DNS, il faut cliquer sur **IP**, ensuite sur **DNS**, renseigner les informations demandées et en fin valider.

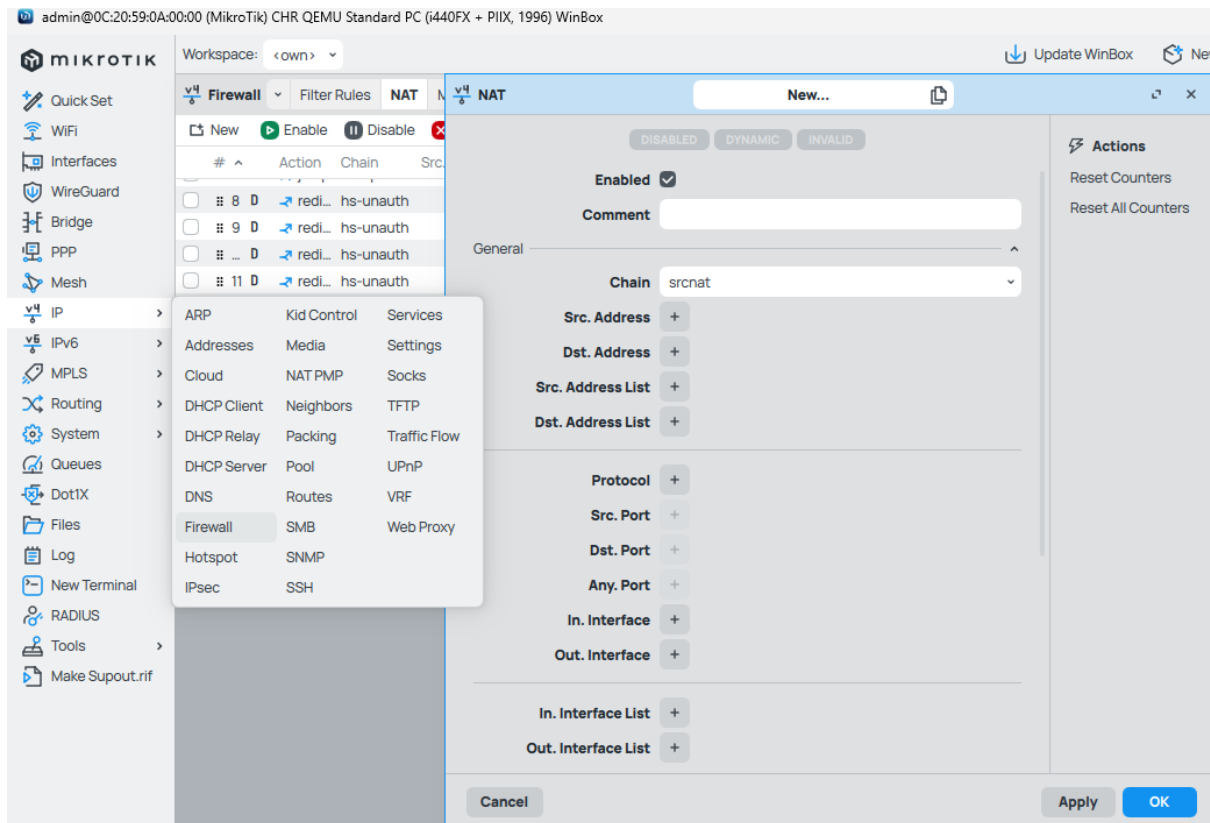


*Figure 4: Configuration du serveur DNS*

#### 4. NAT

Le NAT pour **Network Address Translation**, est une fonctionnalité qui permet la traduction d'adresse privée en adresse publique ceci dans le but de permettre aux ordinateurs du réseaux privé d'accéder à internet car il est impossible d'accéder à internet avec les adresses privées. Pour le configurer, nous cliquons sur **IP**, ensuite **Firewall**, puis **NAT** nous renseignons les informations nécessaires et enfin nous cliquons sur **apply**.





*Figure 5: Configuration du NAT*

## 5. Vérification des configurations

Après l'implémentation de ces services, une phase de validation a été menée :

- Les clients PC1, PC2, kali ont tous reçu une adresse IP automatiquement via DHCP;
- Ils sont capables de résoudre des noms de domaine grâce à la configuration DNS;
- Une connexion Internet fonctionnelle a été vérifiée via des tests de ping;
- Navigation Web, Ouvrir un navigateur Web sur chaque PC et accéder à différents sites Web pour vérifier la connectivité HTTP/HTTPS.

```

kali@kali: ~
File Actions Edit View Help
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:94:0f:0a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global dynamic noprefixroute
        eth0
        valid_lft 1743sec preferred_lft 1743sec
    inet6 fe80::29b3:860b:9bf8:f256/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=53.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=37.0 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1105ms
rtt min/avg/max/mdev = 36.990/45.163/53.337/8.173 ms

(kali@kali)-[~]
$ ping google.com
PING google.com (216.58.223.228) 56(84) bytes of data:
64 bytes from los02s04-in-f14.1e100.net (216.58.223.228): icmp_seq=1 ttl=127
time=51.9 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.228): icmp_seq=2 ttl=127
time=38.2 ms
  
```

Figure 6: Test de fonctionnement du DHCP et DNS sur kali

```

PC2 - PuTTY

PC2> show

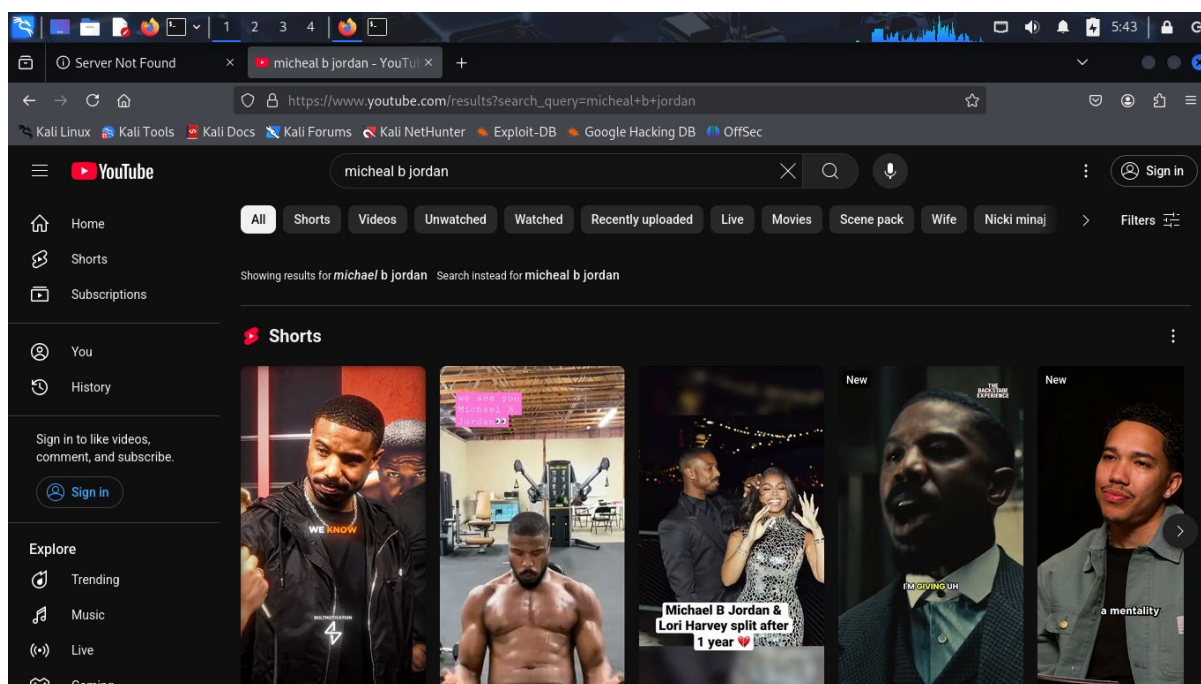
NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
PC2       192.168.2.2/24  192.168.2.1  00:50:79:66:68:01  20037  127.0.0.1:20038
192.168.2.250:791f1e66:6801/64

PC2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=40.522 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=127 time=37.408 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=41.893 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=127 time=38.458 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=127 time=45.186 ms

PC2> ping gooogole.com
goooogle.com resolved to 216.58.223.228
84 bytes from 216.58.223.228 icmp_seq=1 ttl=127 time=43.591 ms
84 bytes from 216.58.223.228 icmp_seq=2 ttl=127 time=40.726 ms
84 bytes from 216.58.223.228 icmp_seq=3 ttl=127 time=40.375 ms
84 bytes from 216.58.223.228 icmp_seq=4 ttl=127 time=41.184 ms
84 bytes from 216.58.223.228 icmp_seq=5 ttl=127 time=44.394 ms

PC2>
  
```

Figure 7: Test de fonctionnement DHCP et DNS sur PC2



*Figure 8: Navigation sur internet depuis kali*

Ces tests confirment que les machines sont bien configurées, connectées et obéissent aux règles établies dans les étapes précédentes.

### **III. Implémentation De Quelques Fonctionnalités Clés**

Compte tenu de notre architecture réseau, voici une brève description des fonctionnalités clés que nous avons implémentées :

- **Firewall** : Le pare-feu protège le réseau en filtrant le trafic entrant et sortant en fonction de règles définies, assurant ainsi la sécurité et le contrôle d'accès ;
- **Simple Queues (QoS)** : Les Simple Queues permettent de gérer la bande passante en définissant des limites de débit maximales et minimales pour chaque poste, assurant ainsi une qualité de service (QoS) en priorisant certains types de trafic ;
- **Hotspot** : Un hotspot sur un routeur MikroTik est une fonctionnalité qui permet de fournir un accès Internet aux utilisateurs via une page d'authentification ;
- **IPsec (VPN Site-to-Site)** : IPsec est un protocole VPN utilisé pour créer une connexion sécurisée et chiffrée entre deux sites distants, permettant ainsi aux réseaux locaux de communiquer de manière sécurisée sur Internet.

### a) **Firewall**

**Le pare-feu (Firewall)** est une fonctionnalité essentielle de sécurité qui permet de filtrer les communications réseau en fonction de règles prédéfinies. Il peut autoriser ou bloquer le trafic entrant ou sortant en se basant sur l'adresse IP, le port, le protocole ou le contenu.

Dans notre cas, il est utilisé pour :

- Bloquer l'accès à distances au serveur web aux ordinateurs du réseau LAN du site 1, sauf l'ordinateur **Kali**.
- Protéger le réseau contre les connexions non autorisées.

Nous devons attention lors de la configuration des règles de pare-feu car la lecture se fait de manière séquentielle.

The screenshot shows the Mikrotik WinBox interface for configuring a new firewall rule. The window is titled "Filter Rules" and has a "New..." button. The rule is configured as follows:

- Enabled:** ☒
- Comment:** (empty field)
- General:**
  - Chain:** forward
  - Src. Address:** 192.168.1.101
  - Dst. Address:** 192.168.2.252
  - Src. Address List:** +
  - Dst. Address List:** +
- Protocol:** 6 (tcp)
- Src. Port:** +
- Dst. Port:** 22
- Any. Port:** +
- In. Interface:** +
- Out. Interface:** +
- In. Interface List:** +
- Out. Interface List:** +

The **Actions** panel on the right shows the following options:

- Reset Counters
- Reset All Counters

At the bottom of the window, there are buttons for **Cancel**, **Apply**, and **OK**.

*Figure 9: Autorisation de l'accès SSH de kali vers le serveur Web*

**Filter Rules** 192.168.2.252:22

DISABLED DYNAMIC INVALID

Enabled ☒

Comment

General

Chain forward

Src. Address +

Dst. Address 192.168.2.252 -

Src. Address List +

Dst. Address List +

Protocol 6 (tcp) -

Src. Port +

Dst. Port 22 -

Any. Port +

In. Interface +

Out. Interface +

In. Interface List +

Out. Interface List +

Actions

Reset Counters

Reset All Counters

Cancel Apply OK

*Figure 10: Bloquer l'accès SSH au serveur web pour tous les autres*

```

(kali@kali)-[~]
└─$ ssh lion-security@192.168.2.252
The authenticity of host '192.168.2.252 (192.168.2.252)' can't be established.
ED25519 key fingerprint is SHA256:73qJmIOcWp/o819DFFiaIandkhAucrar+T5qtIC+WXM
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.252' (ED25519) to the list of known hos
ts.
lion-security@192.168.2.252's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Apr 17 01:25:15 AM UTC 2025

System load:  0.08          Processes:    221
Usage of /:   43.0% of 9.75GB Users logged in: 1
Memory usage: 11%          IPv4 address for ens33: 192.168.2.252
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
ur Internet connection or proxy settings

lion-security@server:~$

```

*Figure 11: Accès au serveur web depuis Kali*

### **b) QoS (Quality of Service)**

La QoS permet de gérer et prioriser la bande passante disponible sur le réseau. Grâce à cette fonctionnalité, il est possible de :

- Limiter la bande passante par poste ;
- Prioriser certains types de trafic ;
- Garantir une meilleure répartition des ressources réseau pour éviter la saturation.

Cela assure une expérience utilisateur plus fluide et un réseau plus stable. Pour le configurer, nous allons configurer le Simple Queue de Mikrotik.

The screenshot shows the 'Simple Queues' configuration window in Mikrotik WinBox. The window title is 'Simple Queues' and the specific queue is named 'kaliBandePassante'. The status is 'DISABLED'. The 'Enabled' checkbox is checked. The 'Comment' field is empty. The 'General' tab is selected, showing the 'Name' as 'kaliBandePassante' and the 'Target' IP as '192.168.1.101'. The 'Dst.' field has a '+' button. Below this, there are two columns for 'Target Upload' and 'Target Download'. The 'Max Limit' is set to '1M' for upload and '3M' for download. The 'Burst' is set to '^'. The 'Burst Limit', 'Burst Threshold', and 'Burst Time' are all set to '0'. The 'Time' dropdown is set to 'v'. The 'Advanced', 'Statistics', 'Traffic', and 'Total' tabs are collapsed. On the right, the 'Actions' panel shows 'Reset Counters', 'Reset All Counters', and 'Torch'. At the bottom, there are 'Cancel', 'Apply', and 'OK' buttons.

*Figure 12: Configuration des bandes passantes download et upload pour Kali*

**c) Hotspot**

Le **Hotspot** est un service qui oblige les utilisateurs à s'authentifier via une page de connexion web avant d'accéder à Internet. Il est principalement utilisé dans les environnements publics ou semi-publics (entreprises, écoles, hôtels, hôpitaux ...).

Les principales fonctionnalités offertes sont :

- ✓ Redirection automatique vers une page de login;
- ✓ Gestion des utilisateurs (avec mots de passe ou tickets);
- ✓ Contrôle du temps de session et du volume de données;

Pour configurer cela, nous allons:

- Aller dans IP > Hotspot > Setup
- Choisir l'interface (dans notre cas l'interface reliée au réseau LAN)



- Définir le pool DHCP, DNS...

*Figure 13: Création du Hotspot*

A présent, nous devons créer les utilisateurs qui devront se connecter au hotspot. Pour cela, nous devons créer des profiles d'utilisateurs qui devront nous servir de modèle pour les différents utilisateurs dans notre cas nous avons créé deux profiles :

- ✓ Profile étudiant
- ✓ Profile enseignant.

La procédure pour créer les profiles des utilisateurs dans le routeur Mikrotik est la suivante :

*IP > Hotspot > User profiles*

The screenshot shows the 'User Profiles' configuration window in Mikrotik WinBox. The window title is 'User Profiles' with a 'New...' button and a close button. A 'DEFAULT' tab is selected. The 'General' section is expanded, showing the following fields:

- Name:** etudiant
- Address Pool:** dhcp\_pool0
- Session Timeout:** +
- Idle Timeout:** none (dropdown menu)
- Keepalive Timeout:** 00:02:00
- Status Autorefresh:** 00:01:00
- Shared Users:** 25
- Rate Limit (rx/tx):** 1024k/1024k
- Add MAC Cookie:** ☒
- MAC Cookie Timeout:** 3d 00:00:00
- Address List:** +
- Incoming Filter:** +
- Outgoing Filter:** +

At the bottom, there are three buttons: 'Cancel', 'Apply', and 'OK'.

Figure 14: Création du profile étudiant

Hotspot	Servers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	Cookies			
New												0 (3)		
Name	Session Tim...	Idle Timeout	Shared U...	Rate Limit (rx/bx)										
<input checked="" type="checkbox"/> * • default		none	1											
<input type="checkbox"/> • enseignant		none	10	2M/2M										
<input type="checkbox"/> • etudiant		none	25	1024k/1024k										

*Figure 15: Liste des profiles créés*

Maintenant que les profiles des utilisateurs sont créés, nous devons créer des utilisateurs qui devront appartenir se connecter au hotspot. Pour cela, nous devons suivre le chemin suivant :

**IP > Hotspot > Users**

*Figure 16: Création d'un utilisateur du hotspot*

Hotspot	Servers	Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List	Cookies			
New													0 (4)	
Server	Name	Address	MAC Address	Profile	Uptime									
counters and limits for trial users														
<input type="checkbox"/>	*	•			00:00:00									
<input type="checkbox"/>	• all	LION		default	00:00:46									
<input type="checkbox"/>	• portailCa...	Russel		enseignant	00:00:00									
<input type="checkbox"/>	• portailCa...	Dirane		etudiant	00:00:00									

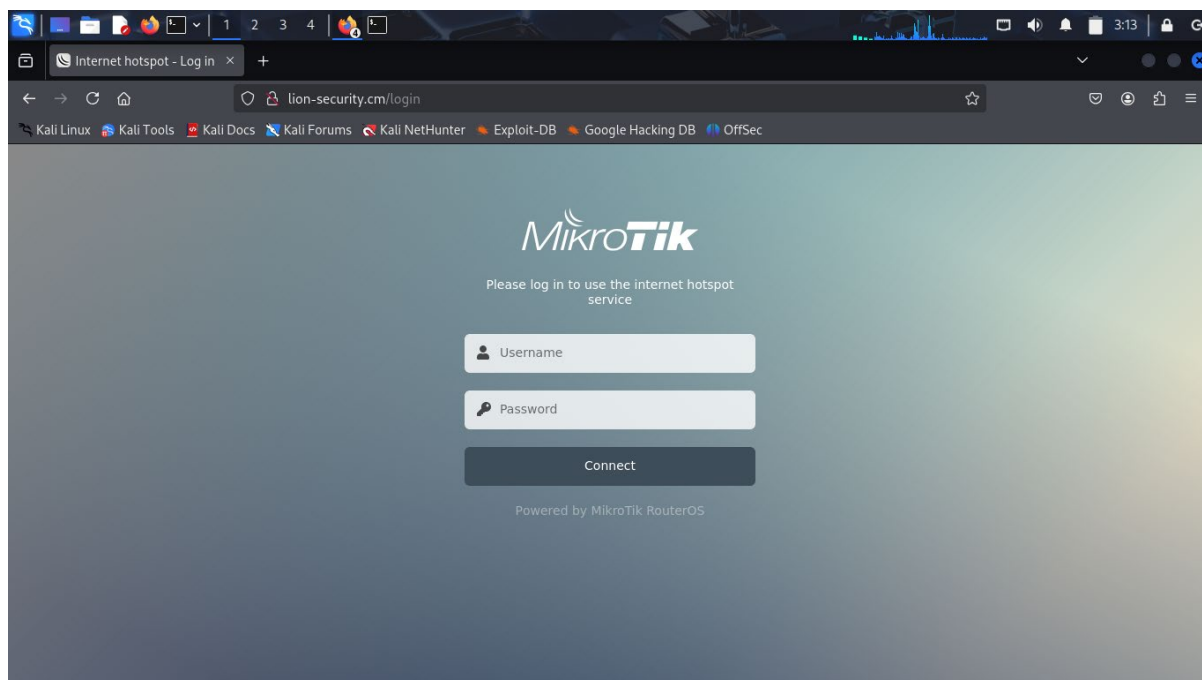
**Actions**

Reset Counters

Reset All Counters

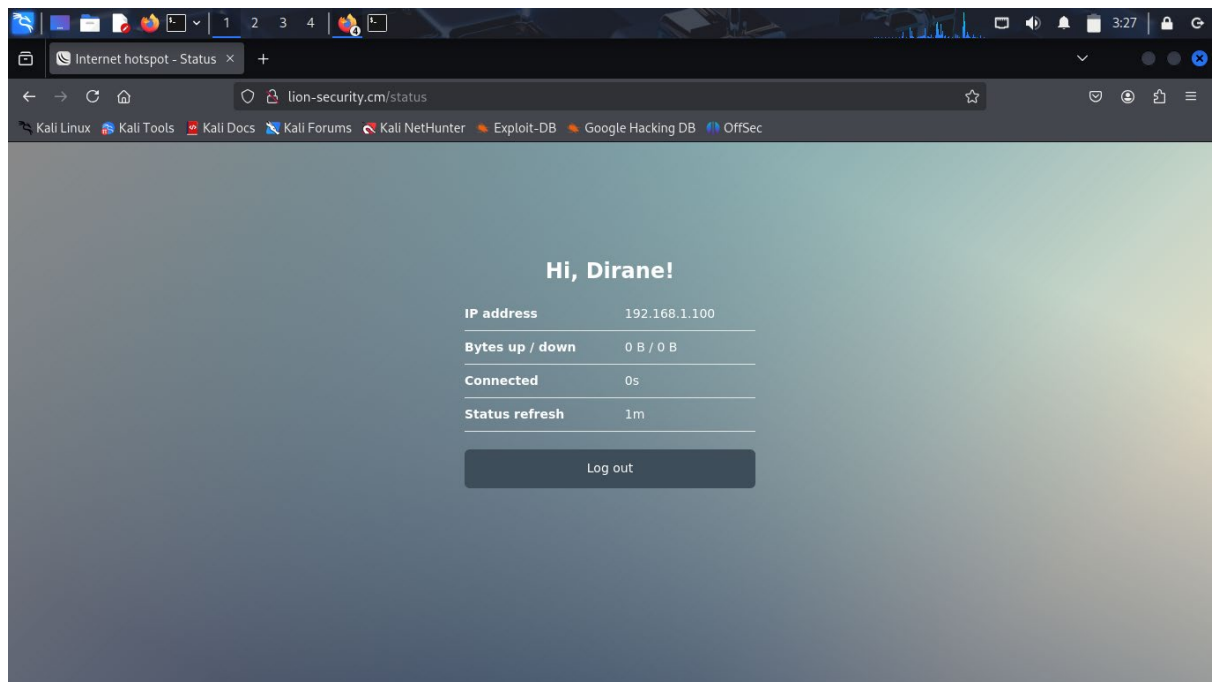
*Figure 17: Liste des utilisateurs du hotspot*

Maintenant que nous avons terminé avec nos configurations, il est temps de tester le fonctionnement de notre hotspot. Pour cela, nous pouvons nous rendre dans le navigateur d'une machine du réseau local et lancer une recherche, notre portail captif s'affiche.



*Figure 18: Portail captif en action*

A présent, nous utilisons l'un des comptes que nous avons créé précédemment pour nous connecter au portail captif.



*Figure 19: Connexion d'un utilisateur au portail captif*

#### d) VPN

Le VPN permet de créer un tunnel sécurisé entre deux points distants via Internet. Les données qui circulent sont chiffrées, ce qui garantit la *confidentialité* et l'*intégrité* des communications.

Il est utilisé pour :

- Accéder à distance aux ressources de l'entreprise
- Interconnecter deux sites géographiques distants
- Protéger la connexion sur les réseaux publics

Dans ce projet, un VPN de type Ipsec (site-to-site) est mis en place. Pour le configurer, nous avons besoin de configurer *la proposition, le peer, l'identité et la politique, ainsi qu'ajuster les règles du NAT.*

- **Création de la proposition :** Allez dans **IP > IPsec > Proposals**, puis ajoutez une nouvelle proposition. La figure suivante illustre cela :

The screenshot shows the 'Proposals' configuration window in Mikrotik WinBox. The window title is 'VPNproposal'. At the top, there are 'DISABLED' and 'DEFAULT' buttons. The 'Enabled' checkbox is checked. The 'Name' field contains 'VPNproposal'. Under 'Auth. Algorithms', 'md5' and 'null' are unchecked, while 'sha1' and 'sha256' are checked. 'sha512' is also present but unchecked. Under 'Encr. Algorithms', 'null', 'des', '3des', 'blowfish', 'camellia-128', 'camellia-256', 'aes-192 ctr', 'aes-128 gcm', and 'aes-256 gcm' are unchecked. 'aes-128 cbc', 'aes-192 cbc', 'aes-256 cbc', 'twofish', 'camellia-192', 'aes-128 ctr', 'aes-256 ctr', 'aes-192 gcm', and 'chacha20 poly1305' are checked. The 'Lifetime' field is set to '00:30:00'. The 'PFS Group' dropdown is set to 'modp1024'. At the bottom, there are 'Cancel', 'Apply', and 'OK' buttons.

*Figure 20: Création d'une proposition pour le VPN*

- **Création du peer :** Allez dans **IP > IPsec > Peer**, puis ajoutez un nouveau peer. La figure suivante illustre cela :

The screenshot shows the 'Peers' configuration window in Mikrotik WinBox. The window title is 'Peers' with a sub-header 'peer1'. There are three tabs: 'DISABLED', 'DYNAMIC', and 'RESPONDER'. The 'DYNAMIC' tab is selected. The configuration includes the following fields and values:

- Enabled:** ☒
- Comment:** (empty text field)
- Name:** peer1
- Address:** 192.168.204.157
- Port:** +
- Local Address:** +
- Profile:** default
- Exchange Mode:** main
- Passive:** ☐
- Send INITIAL\_CONTACT:** ☒

At the bottom, there are three buttons: a trash icon, 'Cancel', and 'Apply'. A blue 'OK' button is also present.

*Figure 21: Création d'un peer pour le VPN*

- **Création de l'identité du peer :** Allez dans **IP > IPsec > identities**, puis ajoutez une nouvelle identité. La figure suivante illustre cela :

The screenshot shows the 'Identities' configuration window in Mikrotik WinBox. The window title is 'Identities' with a sub-header 'peer1'. There are two tabs: 'DYNAMIC' and 'DISABLED'. The 'DYNAMIC' tab is selected. The configuration includes the following fields and values:

- Comment:** (empty text field)
- Enabled:** ☒
- Peer:** peer1
- Auth. Method:** pre shared key
- Secret:** (masked with dots)
- Policy Template Group:** default
- Notrack Chain:** (empty text field)
- My ID Type:** auto
- Remote ID Type:** auto
- Match By:** remote id
- Mode Configuration:** request-only
- Generate Policy:** no

At the bottom, there are three buttons: a trash icon, 'Cancel', and 'Apply'. A blue 'OK' button is also present.

*Figure 22: Création de l'identité*

- **Configuration de la politique du VPN :** Allez dans **IP > IPsec > Politiques**, puis ajoutez une nouvelle politique. La figure suivante illustre cela :

The screenshot shows the 'New...' window for creating a new IPsec policy in Mikrotik WinBox. The window has a title bar with 'v4 Policies', 'New...', and window control buttons. Below the title bar are tabs: 'DISABLED', 'INVALID', 'DYNAMIC', 'DEFAULT', 'TEMPLATE', and 'ACTIVE'. The 'Enabled' checkbox is checked. There is a 'Comment' text field. The 'General' section is expanded, showing 'Peer' set to 'peer1', 'Tunnel' checked, 'Src. Address' as '192.168.1.0/24', 'Src. Port' with a '+' button, 'Dst. Address' as '192.168.3.0/24', 'Dst. Port' with a '+' button, and 'Protocol' set to '255 (all)'. The 'Template' checkbox is unchecked. The 'Action' section is expanded, showing 'Action' set to 'encrypt', 'Level' set to 'require', 'IPsec Protocols' set to 'esp', and 'Proposal' set to 'default'. At the bottom are 'Cancel', 'Apply', and 'OK' buttons.

*Figure 23: Configuration de la politique du VPN*

- **Ajuster les règles NAT :** Allez dans **IP > Firewall > NAT**, puis ajoutez une nouvelle règle NAT. Le but de cette règle NAT est de laisser passer le trafic entre les deux LAN distant sans masquer les adresses. La figure suivante illustre cela :



*Figure 24: Configuration des règles NAT pour le VPN*

- **Vérification des Configurations :** afin de vérifier que le trafic entre les réseaux locaux des deux sites transite correctement à travers le tunnel VPN. Nous avons Lancé une commande ping depuis Mikrotik du Site 1 vers un Mikrotik du Site 2. La capture ci-dessous illustre cela :



The screenshot shows the 'Users' configuration window in Mikrotik WinBox. The 'New...' tab is active. The form includes fields for 'Enabled' (checked), 'Comment', 'Name' (Lion), 'Group' (full), 'Allowed Address' (+), 'Password' (masked), 'Confirm Password' (masked), 'Inactivity Timeout' (00:10:00), and 'Inactivity Policy' (none). There are 'Cancel', 'Apply', and 'OK' buttons at the bottom.

*Figure 26: Création d'un compte utilisateur du Mikrotik*

The screenshot shows the 'User List' window in Mikrotik WinBox. The 'Users' tab is active. The table lists the following users:

Name	Group	Allowed Address	Last Logged In
Lion	full		
Taptue	read		
system default user			
admin	full		2025-04-17 00:43:51

On the right side, there is a 'Configuration' sidebar with 'Settings' and 'AAA' options.

*Figure 27: Liste des comptes utilisateurs de Mikrotik*



MikroTik permet la création de multiples utilisateurs, chacun pouvant se voir attribuer des droits d'accès spécifiques en fonction de son rôle au sein de l'organisation. Pour faciliter la gestion des permissions, il est possible de regrouper ces utilisateurs en groupes de sécurité. Chaque groupe bénéficie alors d'un ensemble de privilèges définis, ce qui permet de limiter les accès aux fonctionnalités sensibles et de réduire les risques d'erreurs ou d'intrusions.

Nous avons décidé de créer le groupe admin-Network avec les privilèges ci-dessous :

*Figure 28: Création d'un groupe d'utilisateur*

## **2. Sauvegarde Et Restauration Des Configurations De Mikrotik**

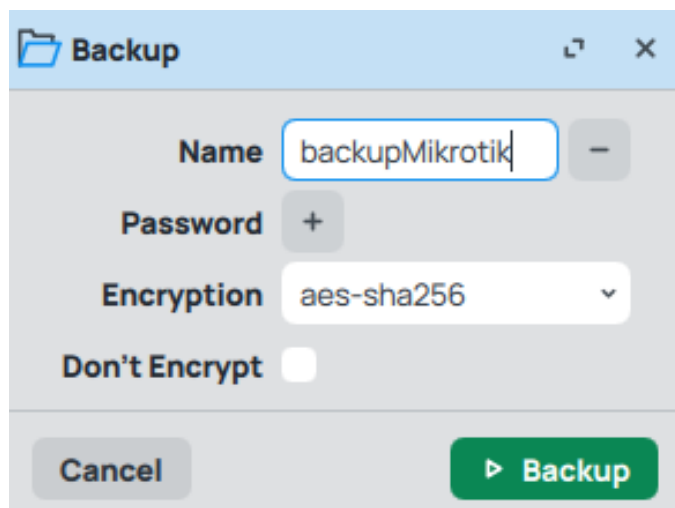
La sauvegarde régulière de la configuration des routeurs Mikrotik est essentielle pour garantir la continuité du service et faciliter la reprise en cas de panne ou de modification non désirée. Deux méthodes principales sont utilisées pour sauvegarder et restaurer la configuration :

### a. Sauvegarde et restauration via fichier binaire (.backup)

Cette méthode consiste à générer un fichier de sauvegarde complet, contenant l'intégralité de la configuration du routeur, incluant les paramètres système, les règles firewall, les configurations VPN, etc. Ce fichier est spécifique à la version de RouterOS et au modèle du matériel.

- **Sauvegarde** : Elle s'effectue facilement via l'interface Winbox en cliquant sur **Files** puis **Backup**, comme illustre dans les figures ci-dessous.
- **Restauration** : Le fichier de sauvegarde est chargé dans le routeur et la restauration s'effectue après un redémarrage toujours dans le même interface.

Cette méthode est rapide et complète, mais le fichier généré n'est pas éditable manuellement, ce qui limite la flexibilité en cas de besoin de modification avant restauration.



*Figure 29: Sauvegarde dans un fichier binaire*

### b. Export et import de la configuration en fichier texte

Cette méthode exporte la configuration sous forme d'un script texte, lisible et modifiable. Elle est particulièrement utile pour migrer la configuration vers un autre routeur, ou pour apporter des modifications avant la restauration.

- **Export** : Réalisé via Winbox ou en CLI avec la commande `/export file=backup17_04_2025.rsc`. Ensuite, nous avons la possibilité de télécharger cela dans l'onglet **Fichier**.
- **Import** : Le fichier texte peut être importé via `/import file= backup17_04_2025.rsc`.

Cette méthode offre une grande flexibilité, mais ne sauvegarde pas certains éléments sensibles comme les mots de passe chiffrés ou certains fichiers système.

```

MMM      MMM      KKK      TTTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR      000000      TTT      III  KKK  K
KK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000  000      TTT      III  KKKKK
MMM      MMM  III  KKK  KKK  RRRRRR      000  000      TTT      III  KKK  KK
K
MMM      MMM  III  KKK  KKK  RRR  RRR  000000      TTT      III  KKK  K
KK

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > /export file=backup17_04_2025.rsc
[admin@MikroTik] >

```

*Figure 30: Exportation du fichier de configuration*

File Name	Type	Size	Last Modified
<input type="checkbox"/> autosupout.rif	.rif file	324.9 KiB	2025-04-14 18:58:30
<input checked="" type="checkbox"/> backup17_04_2025.rsc	script	3608 B	2025-04-17 13:39:59
<input type="checkbox"/> backupMikrotik.backup	backup	28.6 KiB	2025-04-17 09:37:16
<input type="checkbox"/> hotspot	directory		2025-04-12 14:39:29
<input type="checkbox"/> hotspot/login.html	.html file	1094 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/api.json	.json file	311 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/css	directory		2025-04-12 14:39:29
<input type="checkbox"/> hotspot/css/style.css	.css file	4053 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/error.html	.html file	640 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/errors.txt	.txt file	3719 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/favicon.ico	.ico file	903 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/img	directory		2025-04-12 14:39:29
<input type="checkbox"/> hotspot/img/password.svg	.svg file	644 B	2025-04-12 14:39:29
<input type="checkbox"/> hotspot/img/user.svg	.svg file	444 B	2025-04-12 14:39:29

*Figure 31: Fichiers de restauration exporté*

```

Terminal
MMM      MMM      KKK      TTTTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR      000000      TTT      III  KKK  K
KK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000  000      TTT      III  KKKKK
MMM      MMM  III  KKK  KKK  RRRRRR      000  000      TTT      III  KKK  KK
K
MMM      MMM  III  KKK  KKK  RRR  RRR  000000      TTT      III  KKK  K
KK

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > /import file=backup17_04_2025.rsc

```

*Figure 32: Importation du fichier de configuration*

### 3. Bloquer l'accès certains sites Web

Dans notre environnement de test, nous avons déjà un hotspot nous allons l'utilisé pour gérer l'accès Internet des utilisateurs, et restreindre l'accès à certains sites web pour des raisons de productivité ou de conformité. MikroTik offre plusieurs méthodes pour réaliser ce blocage, notamment via des règles de pare-feu basées sur le filtrage du trafic TLS (HTTPS) ou par contrôle DNS.

Pour le test, nous avons décidé de restreindre l'accès à YouTube depuis le LAN, en utilisant notre hotspot. Pour cela, nous allons l'onglet Walled Garden du Hotspot, puis nous renseignons les champs.

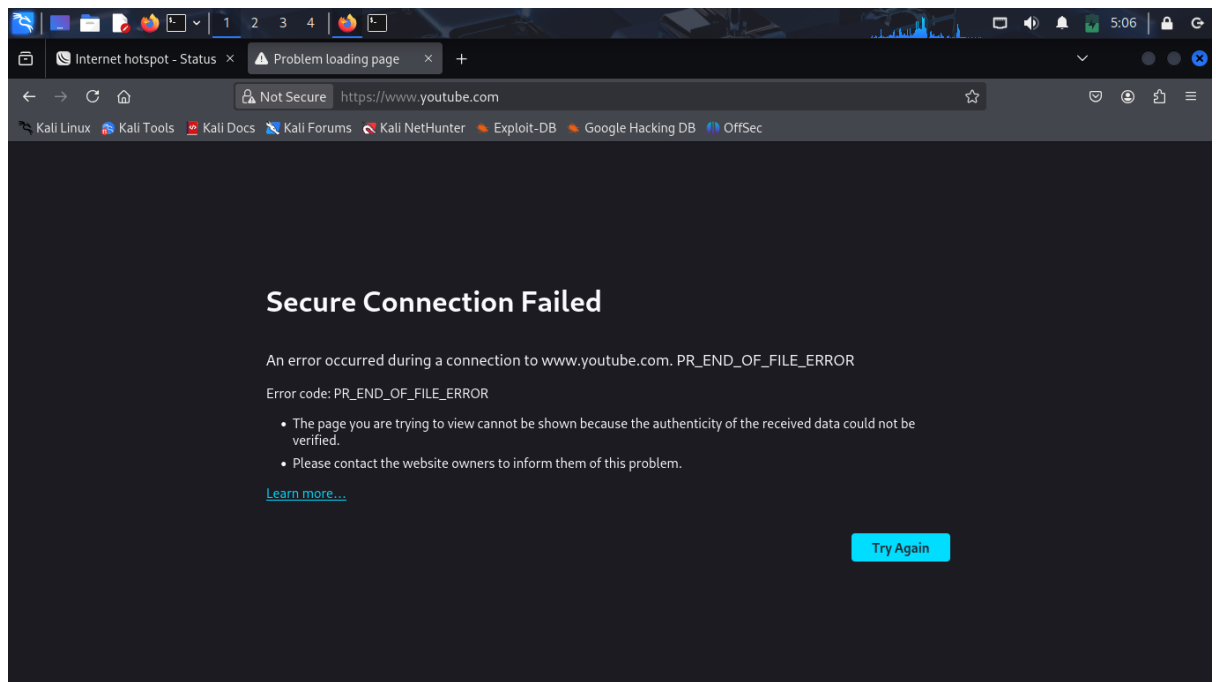


*Figure 33: Configuration de Walled Garden*

#	^	Action	Server	Method	Dst. Host	Dst. Port	Hits
0		deny	portailCaptif		www.youtube.co...	80	0

*Figure 34: Liste des sites bloqués*

Après configuration, nous pouvons voir que l'accès à YouTube est maintenant restreint depuis les machines de réseau LAN.



*Figure 35: Impossible d'accéder à YouTube*

## **Conclusion**

Ce travail pratique a permis de renforcer notre compréhension des routeurs MikroTik et de leurs capacités. En utilisant GNS3, nous avons pu simuler un environnement réseau réaliste et tester diverses configurations dans des conditions contrôlées. Nous avons abordé des aspects essentiels tels que la configuration des interfaces, le routage, la sécurité via pare-feu et la mise en place de VPNs. Les défis rencontrés lors de la résolution des problèmes de connectivité et de performance ont mis en évidence l'importance d'une planification rigoureuse et d'une connaissance approfondie des outils de diagnostic MikroTik. Les compétences acquises au cours de ce TP seront précieuses pour la conception, le déploiement et la gestion de réseaux utilisant des équipements MikroTik.

## **Bibliographie**

- [1] <https://mikrotik.com/> pour la documentation ;
- [2] <https://winbox.en.softonic.com/> pour télécharger l'interface de Mikrotik (Winbox) ;
- [3] TP Mikrotik LIR, Projet Mikrotik.pdf, année académique 2024-2025 présente par nos camarades de classe ;
- [4] IRT\_Portail Captif licence IRT, Non publié par Dr Djimeli