Présentation De Quelques Fonctionnalités Du Routeur Mikrotik

Sommaire:

Listes des figures :

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 relie au site 1 de l'entreprise et situe 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 :

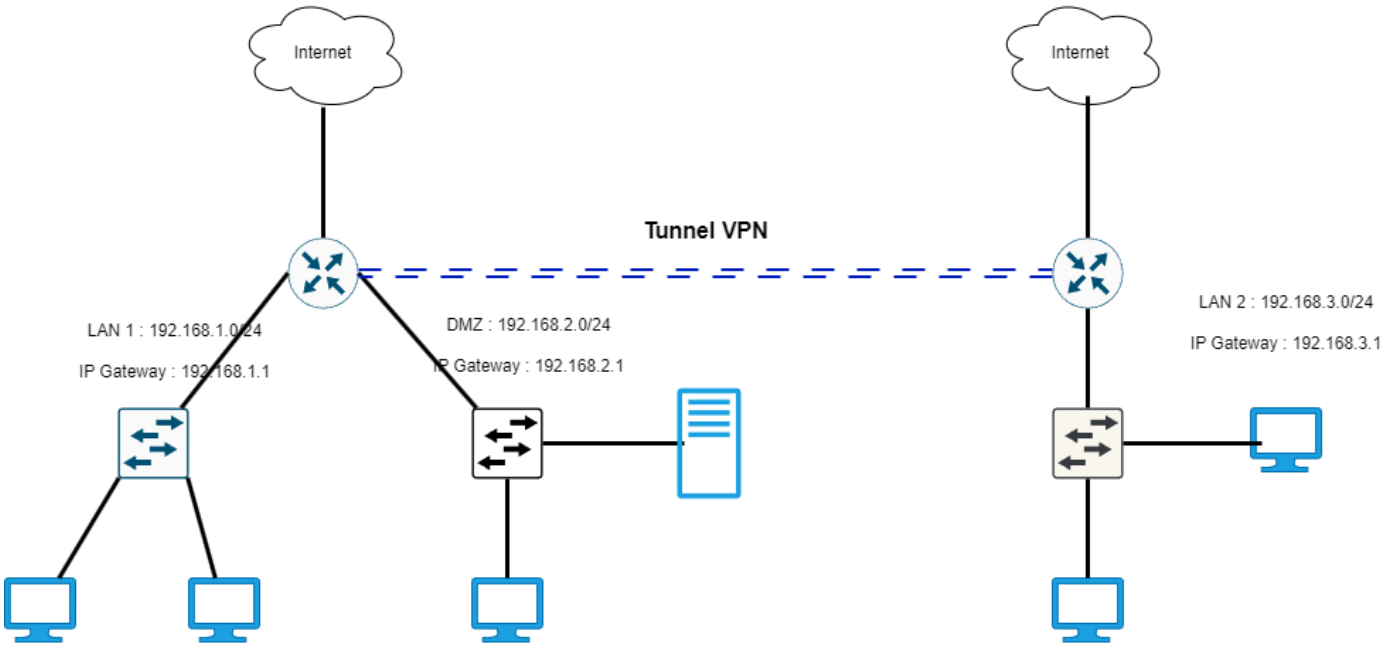

Figure 1: Architecture de notre réseau de test

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 trouve 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 import 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.

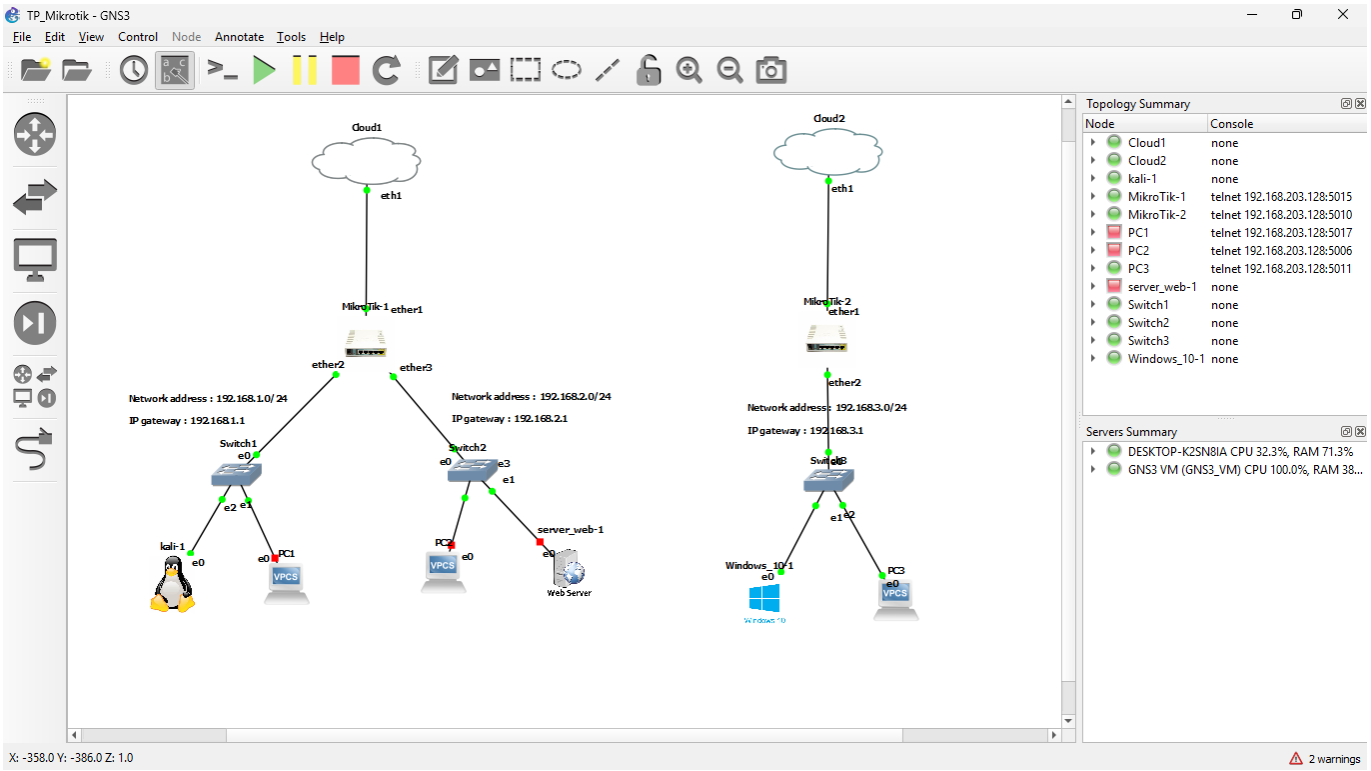

Figure 2: Architecture de notre réseau dans le logiciel GNS3

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.

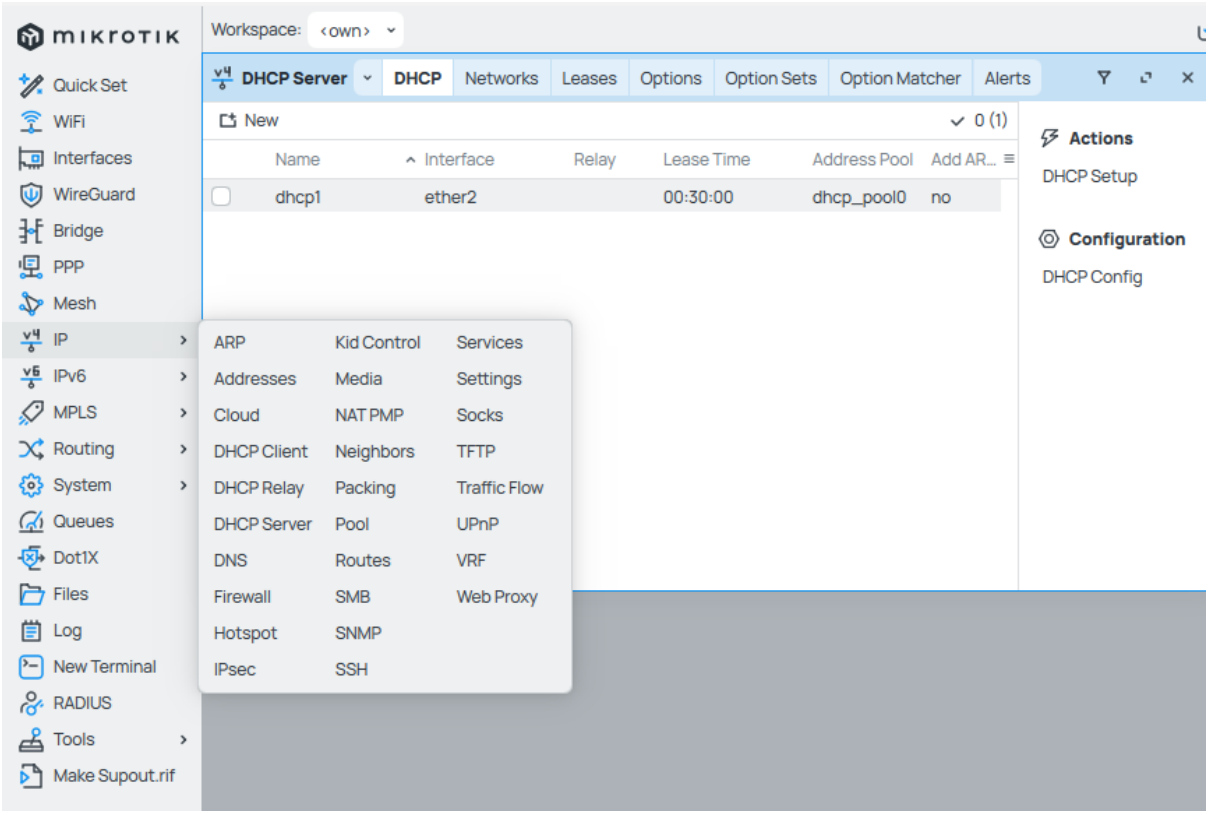

Figure 3: Configuration du Serveur DHCP

3. Serveur DNS

Serveur DNS : Cette fonctionnalité permet à notre routeur Microtik 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 activer le client DHCP sur notre interface qui est relie à internet. Si vous souhaitez configurer le DNS, il faut cliquer sur **IP**, ensuite sur **DNS**, renseigner les informations demandées et en fin valider.

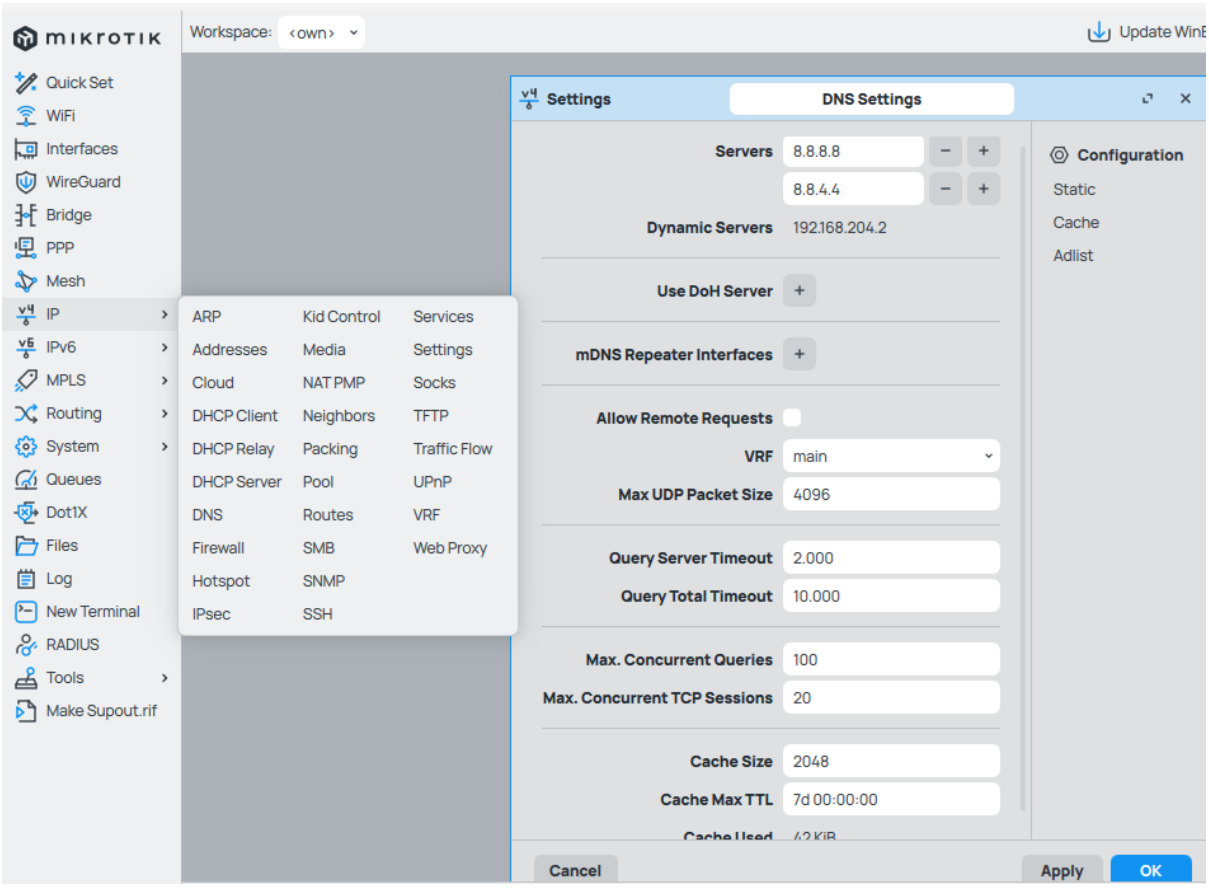

Figure 4: Configuration du serveur DNS

4. NAT

Le NAT pour **Network Address Translation**, est une fonctionnalité qui permet la traduction d'adresse prive 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**.

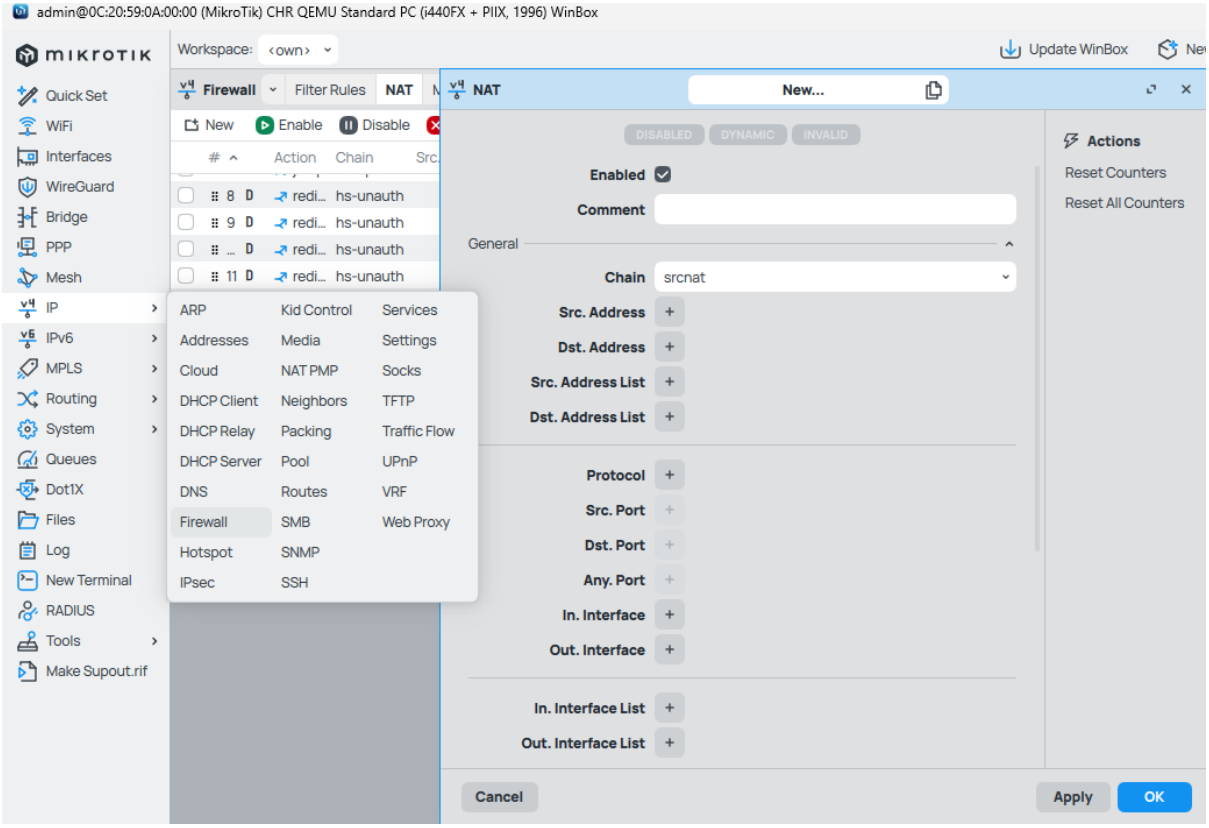

Figure 5: Configuration du NAT

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.

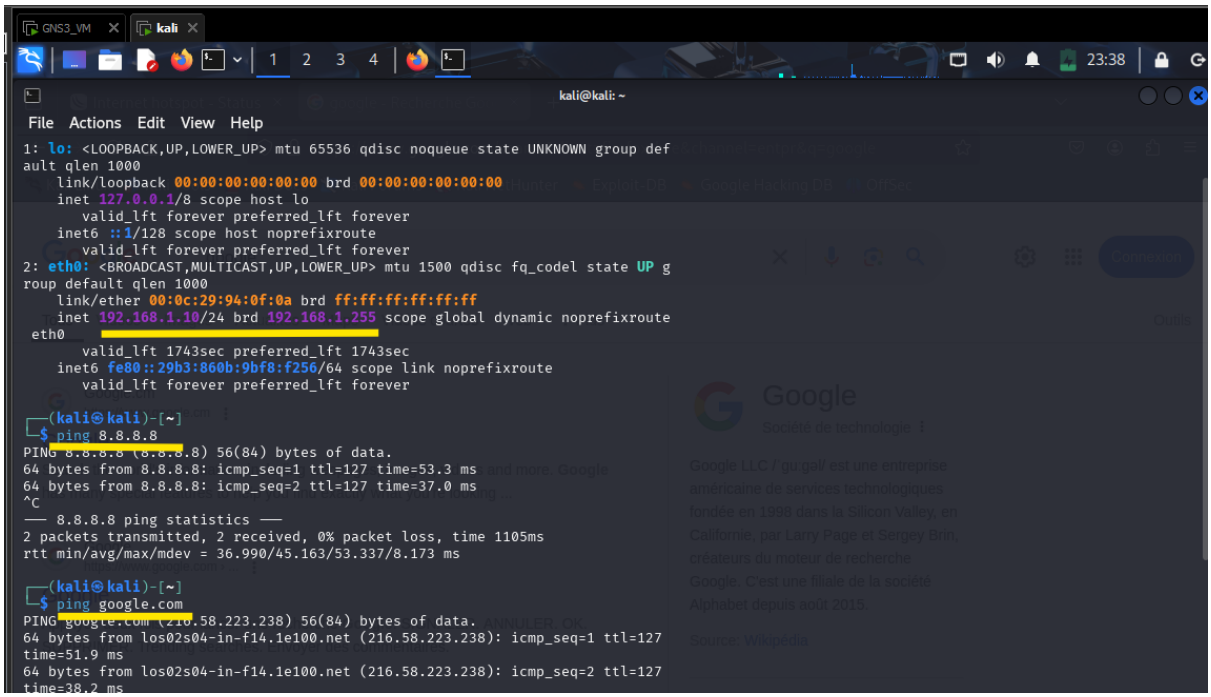

Figure 6: Test de fonctionnement du DHCP et DNS sur kali

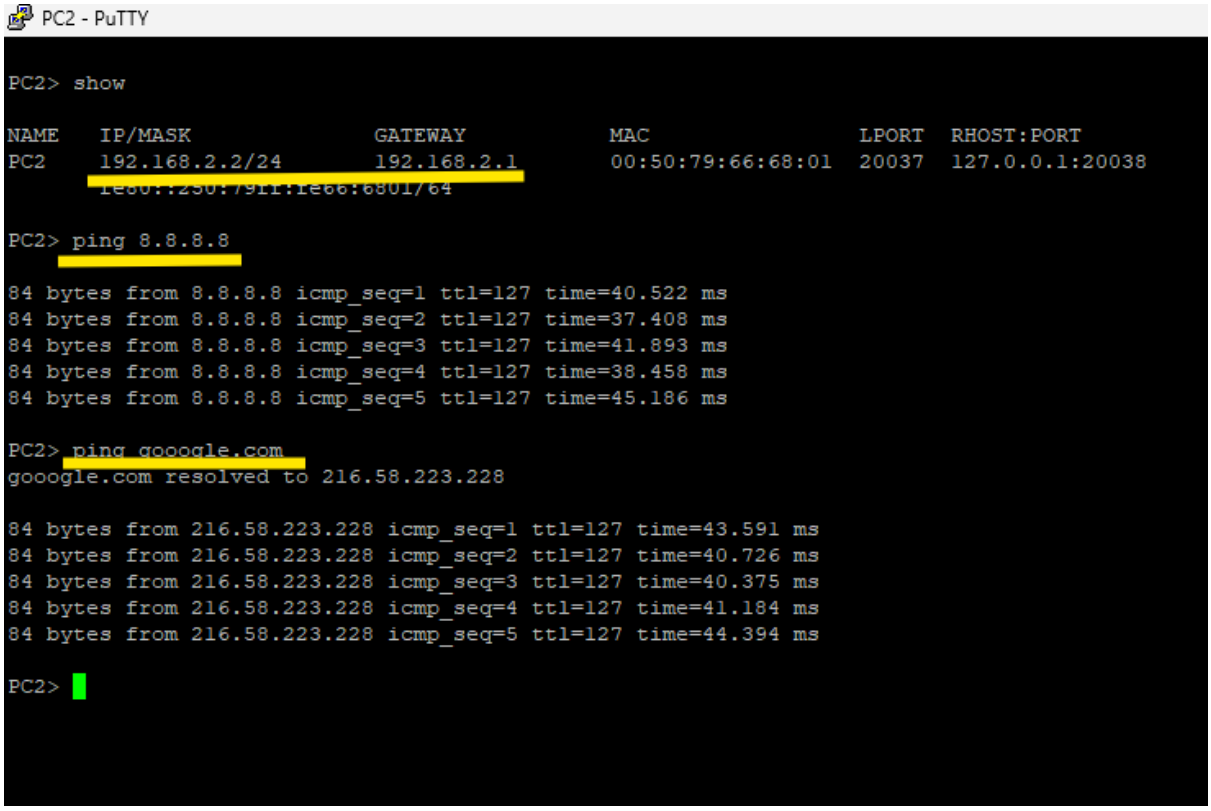

Figure 7: Test de fonctionnement DHCP et DNS sur PC2

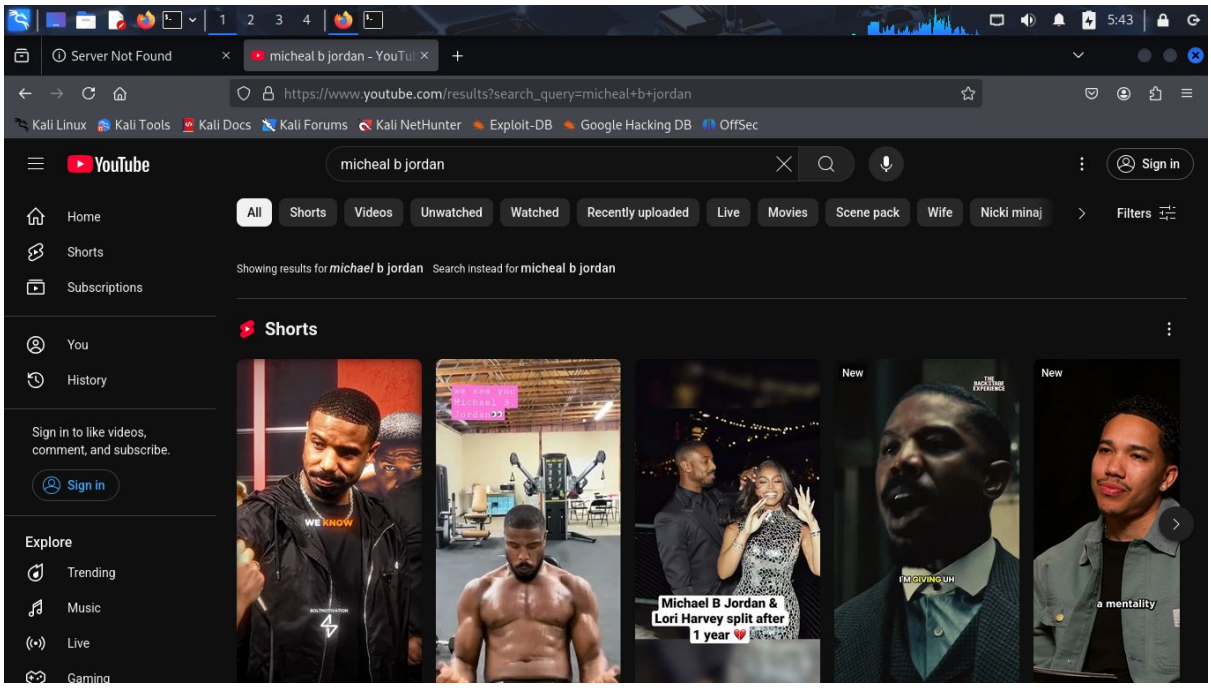

Figure 8: Navigation sur internet depuis kali

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.

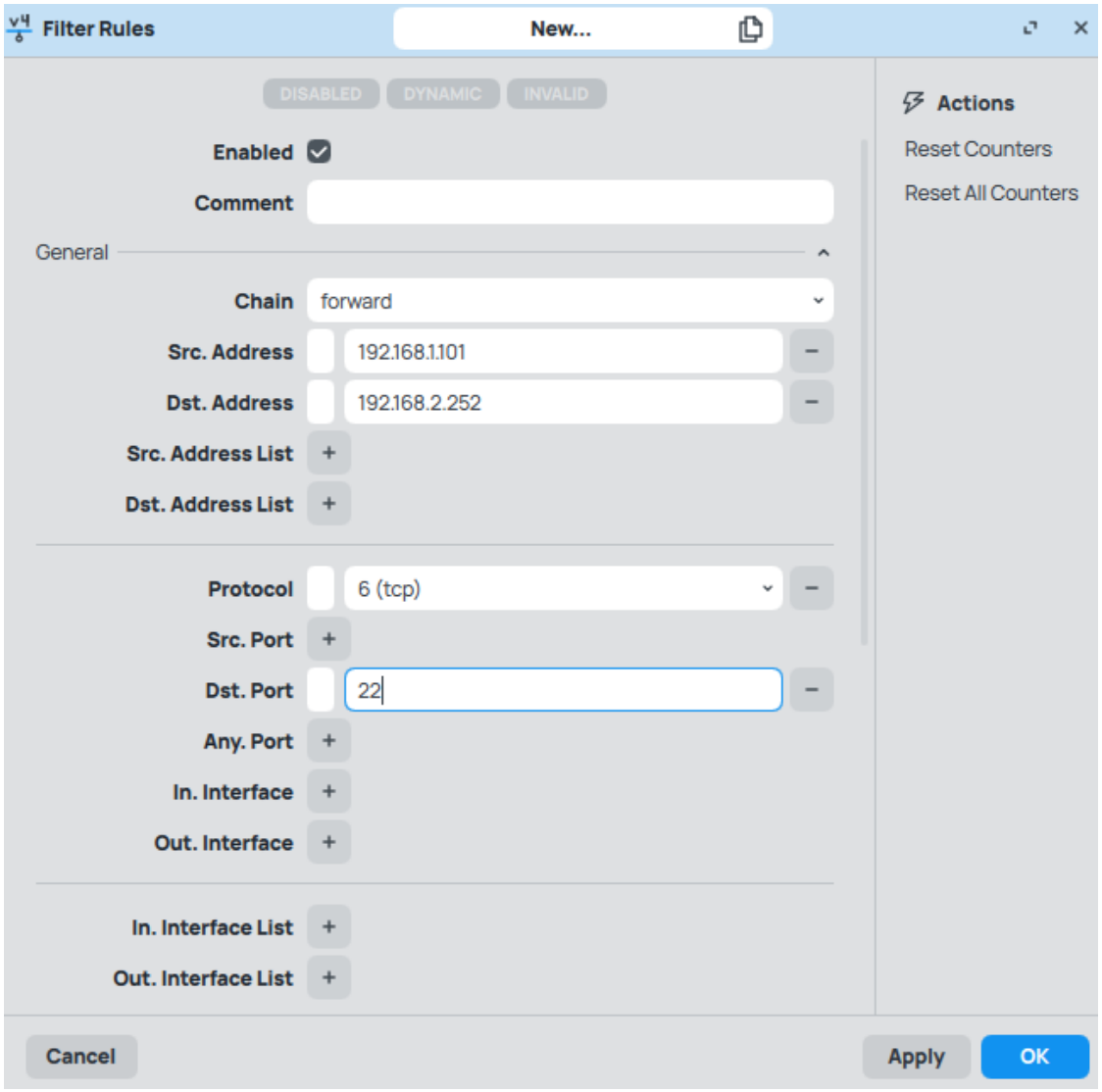

Figure 9: Autorisation de l'accès SSH de kali vers le serveur Web

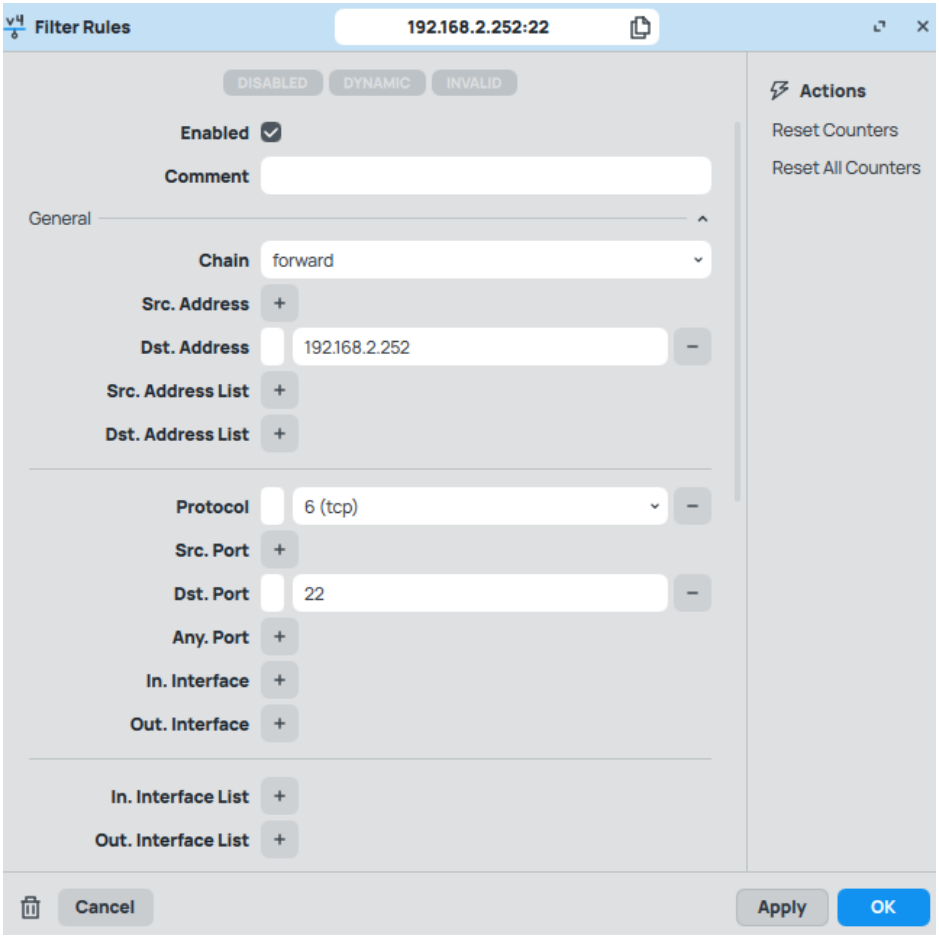

Figure 10: Bloquer l'accès SSH au serveur web pour tous les autres

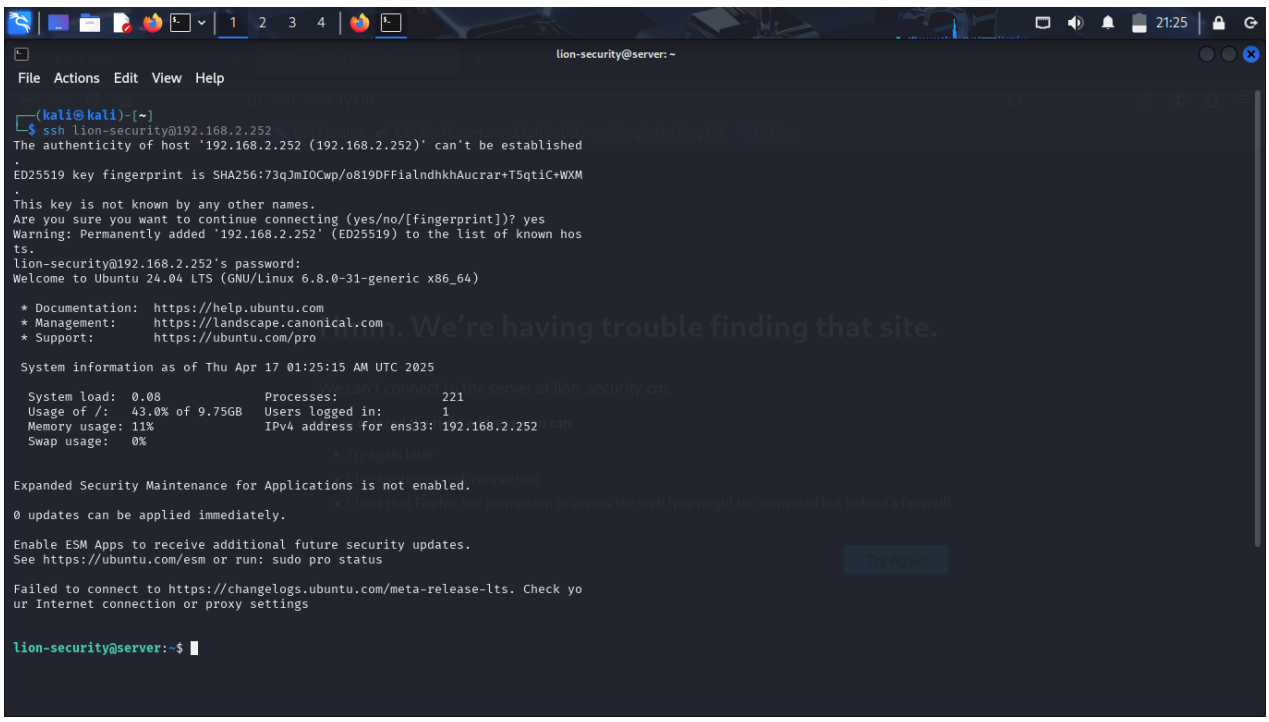

Figure 11: Accès au serveur web depuis Kali

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.

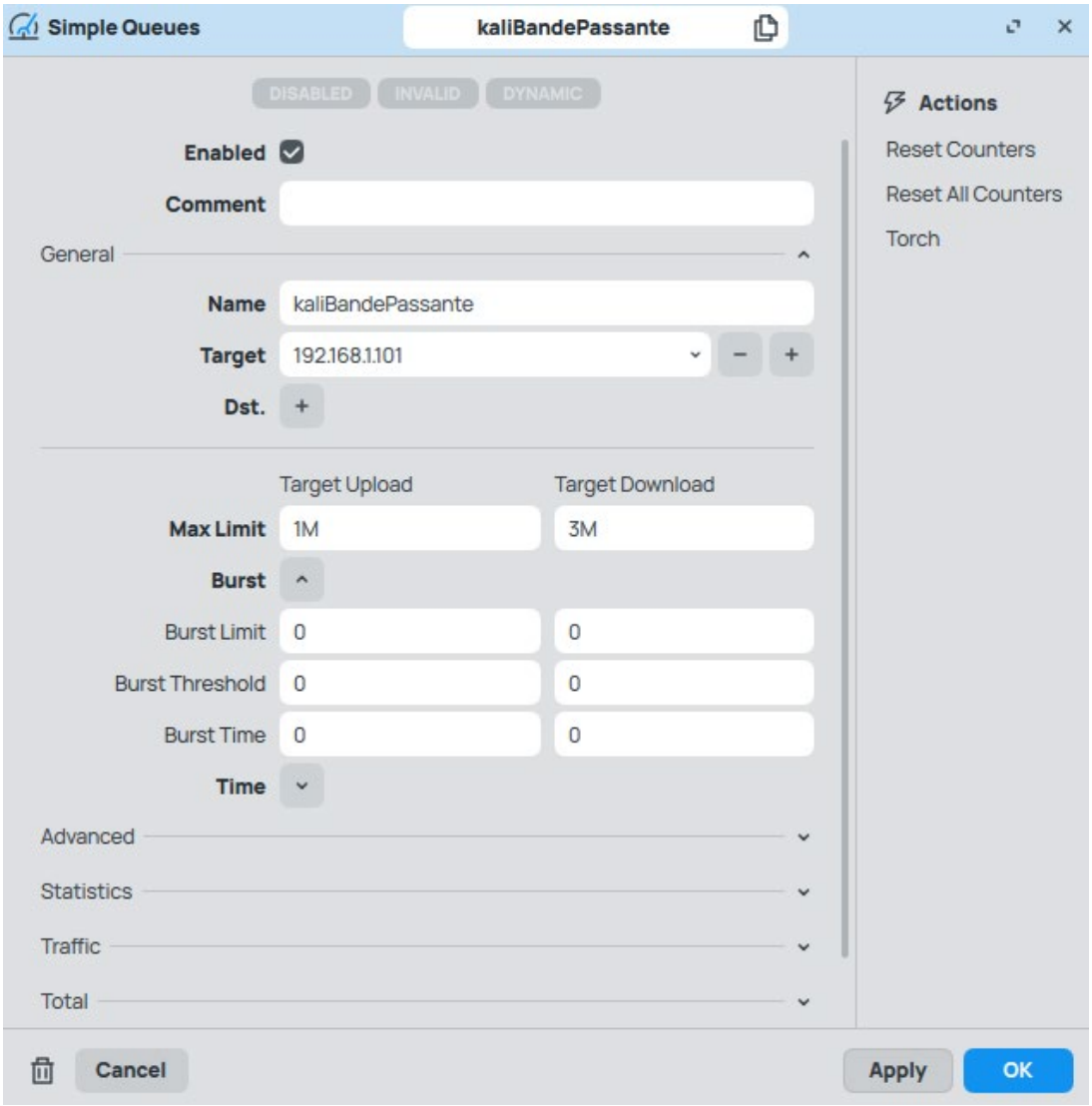

Figure 12: Configuration des bandes passantes download et updload pour Kali

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…

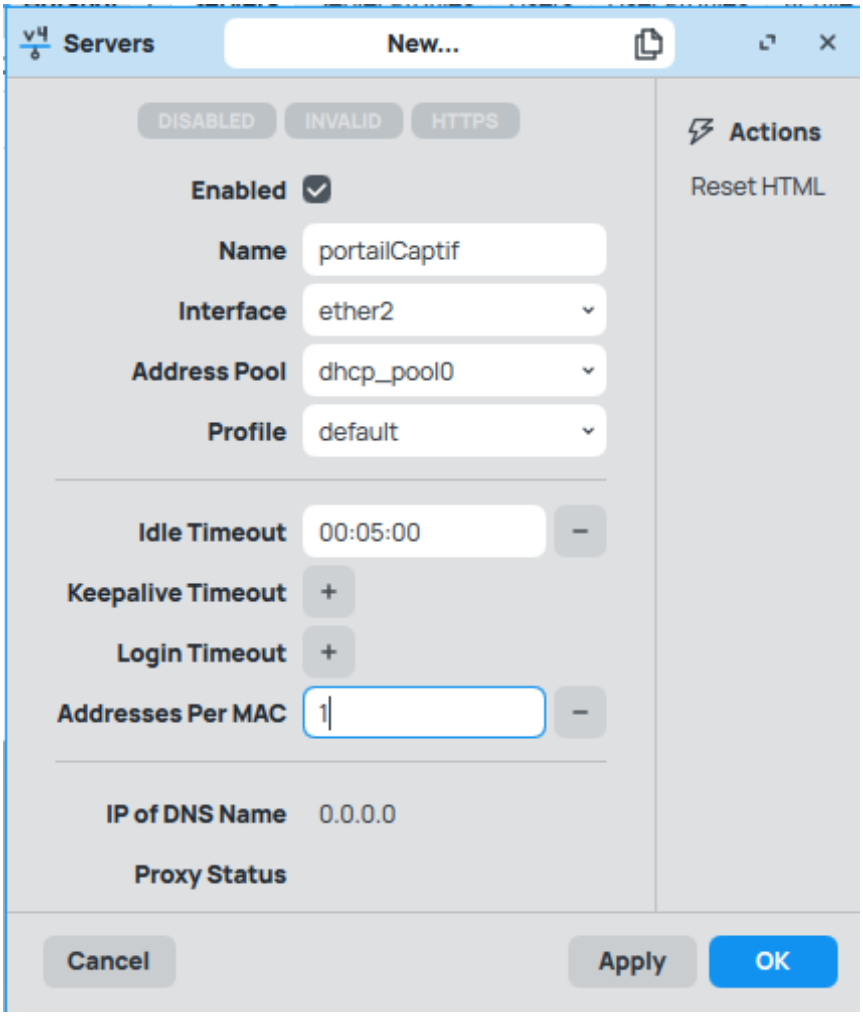

Figure 13: Création du Hotspot

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

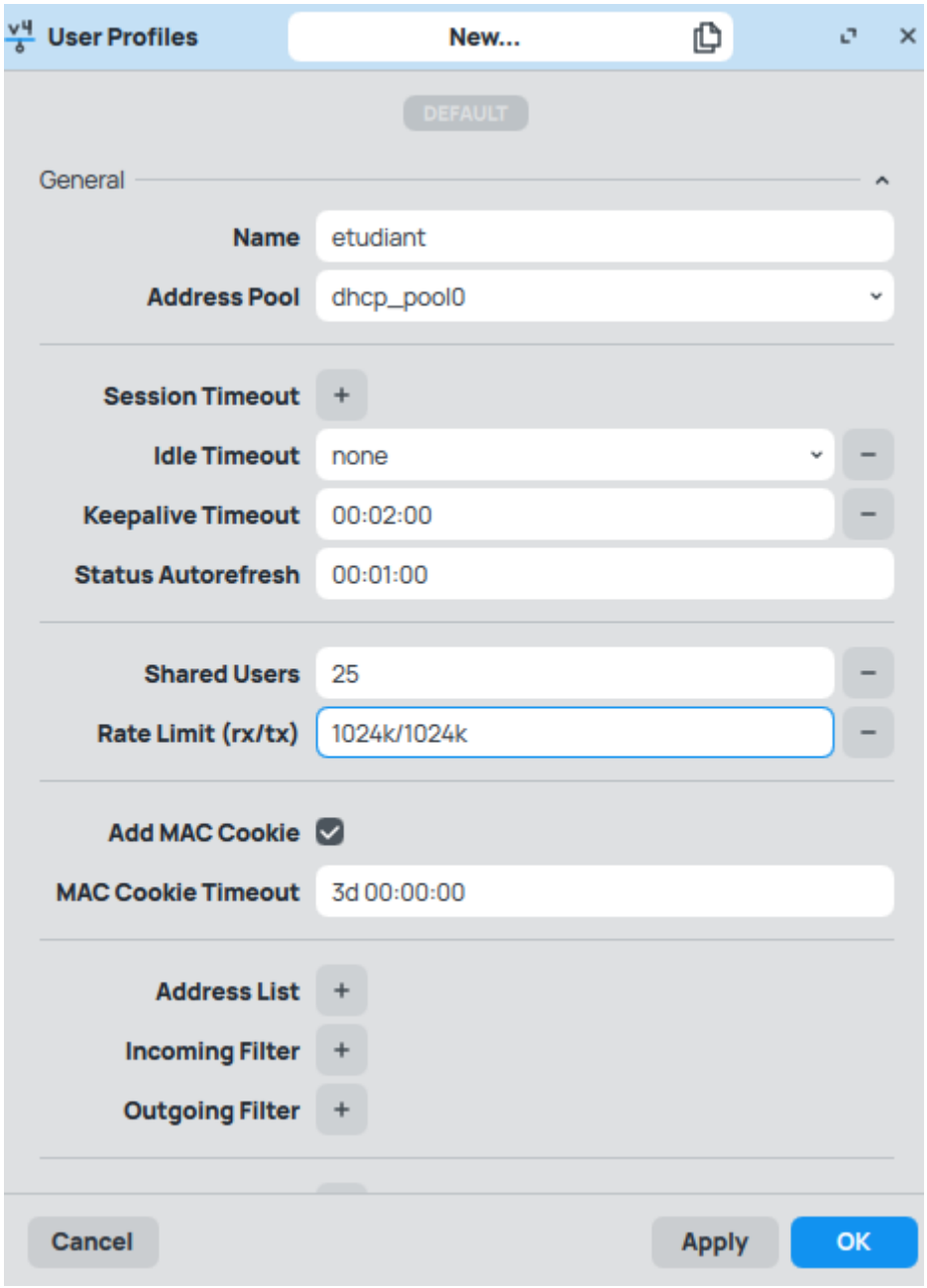

Figure 14: Création du profile étudiant

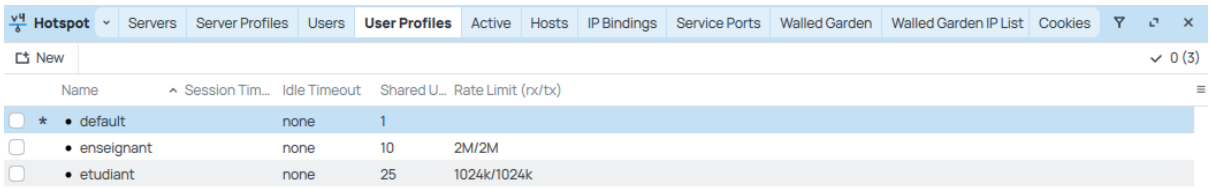

Figure 15: Liste des profiles crées

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***

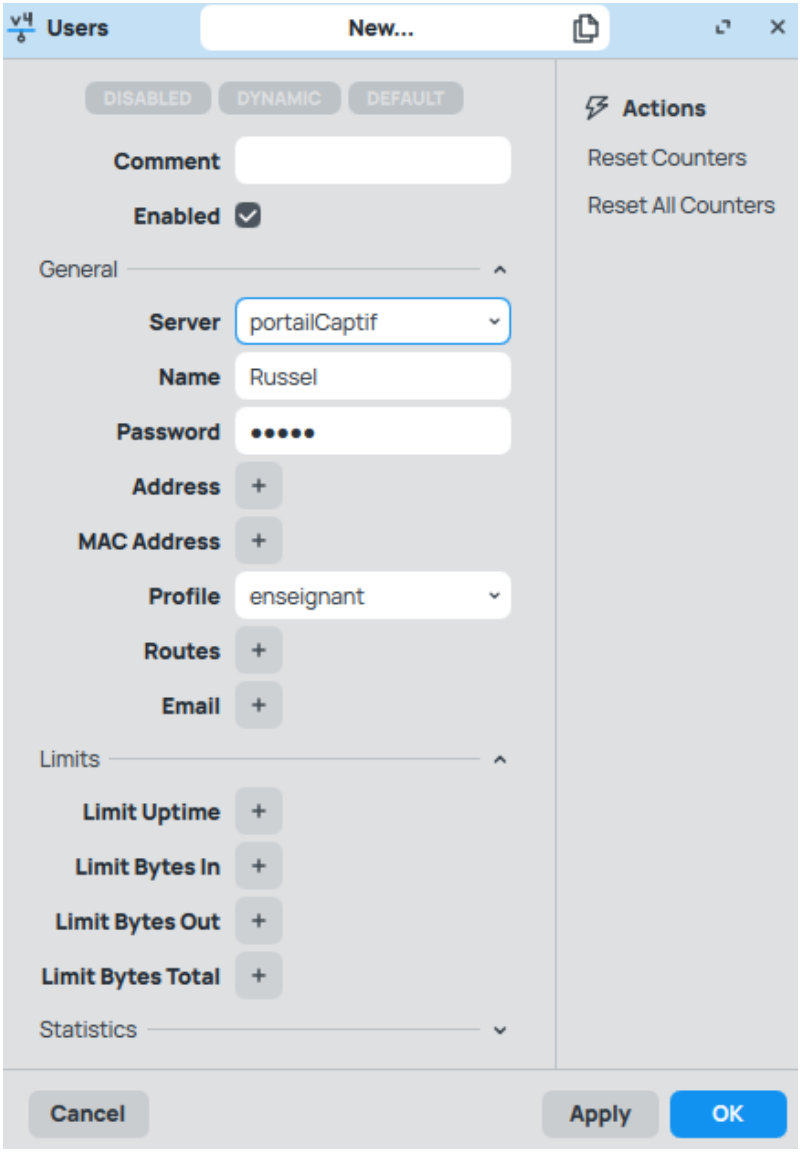

Figure 16: Création d'un utilisateur du hotspot

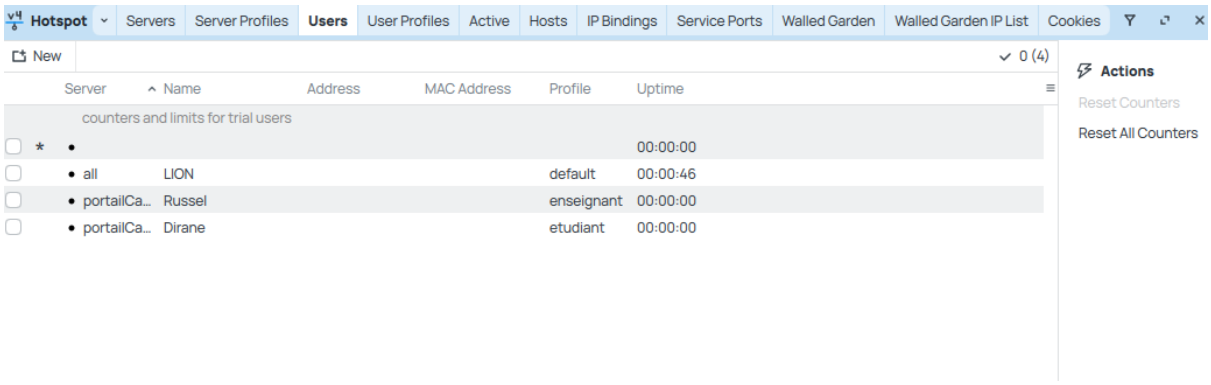

Figure 17: Liste des utilisateurs du hotspot

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.

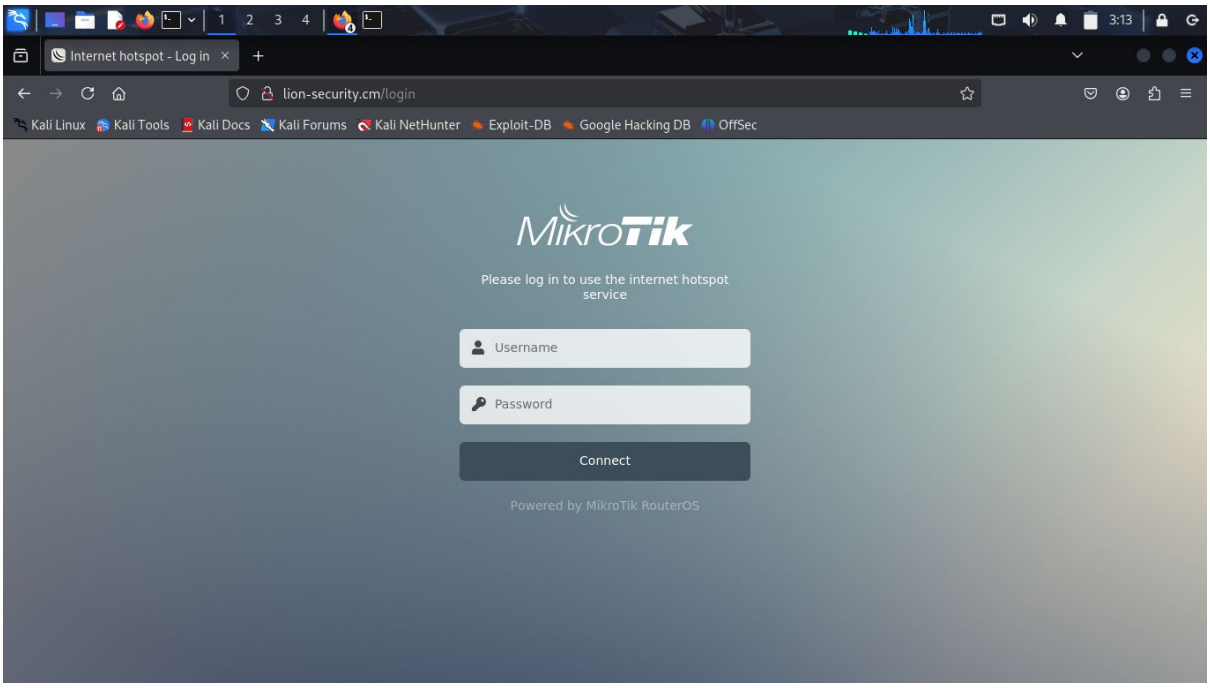

Figure 18: Portail captif en action

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

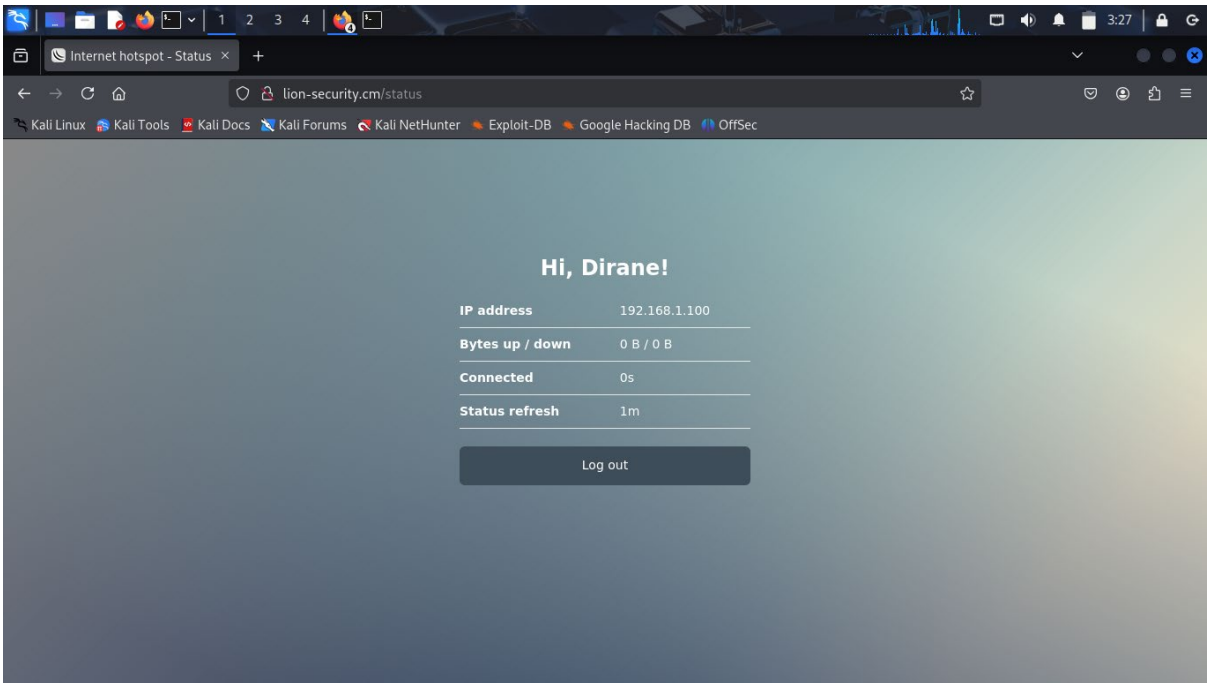

Figure 19: Connexion d'un utilisateur au portail captif

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 :

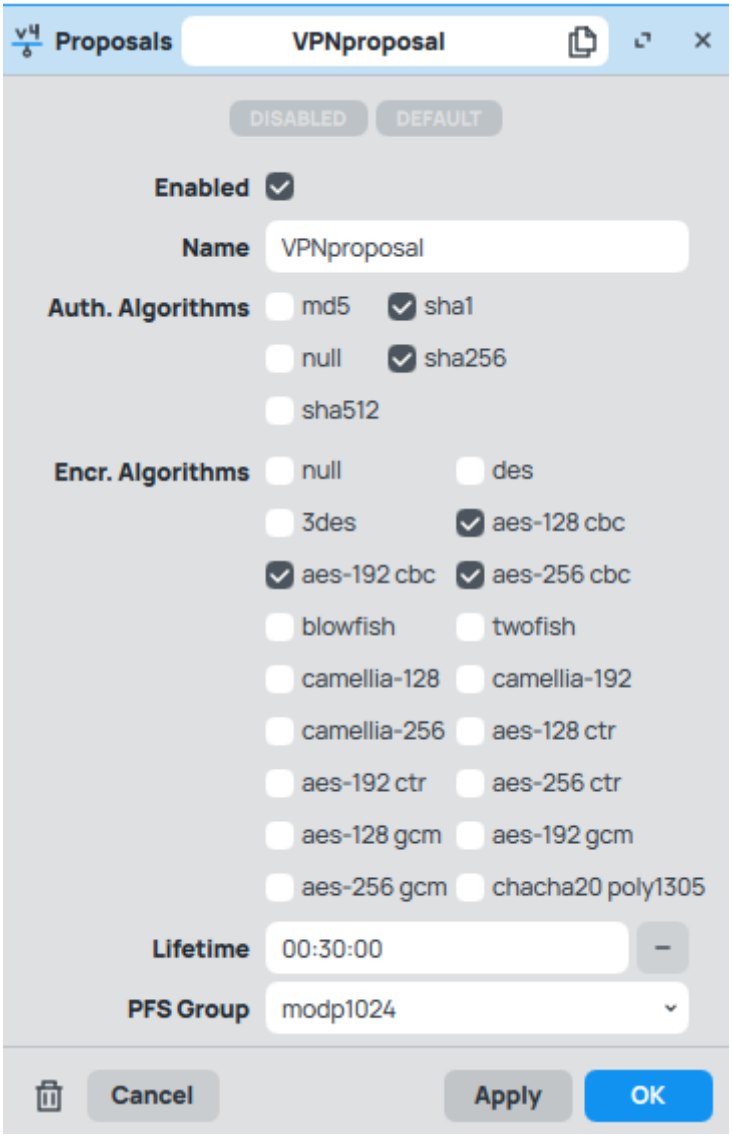

Figure 20: Création d'une proposition pour le VPN

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

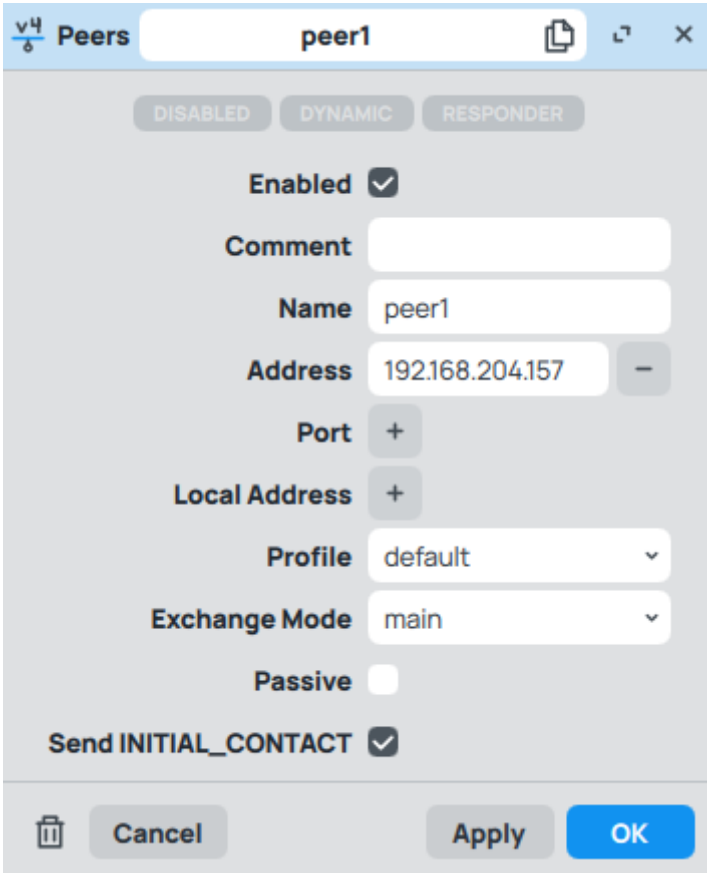

Figure 21: Création d'un peer pour le VPN

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

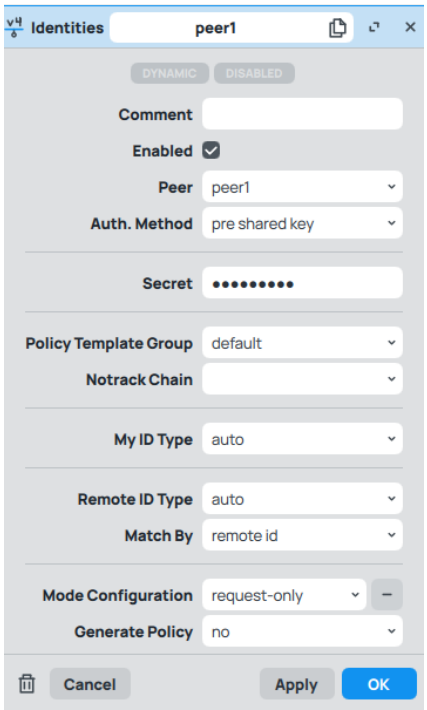

Figure 22: Création de l'identité

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

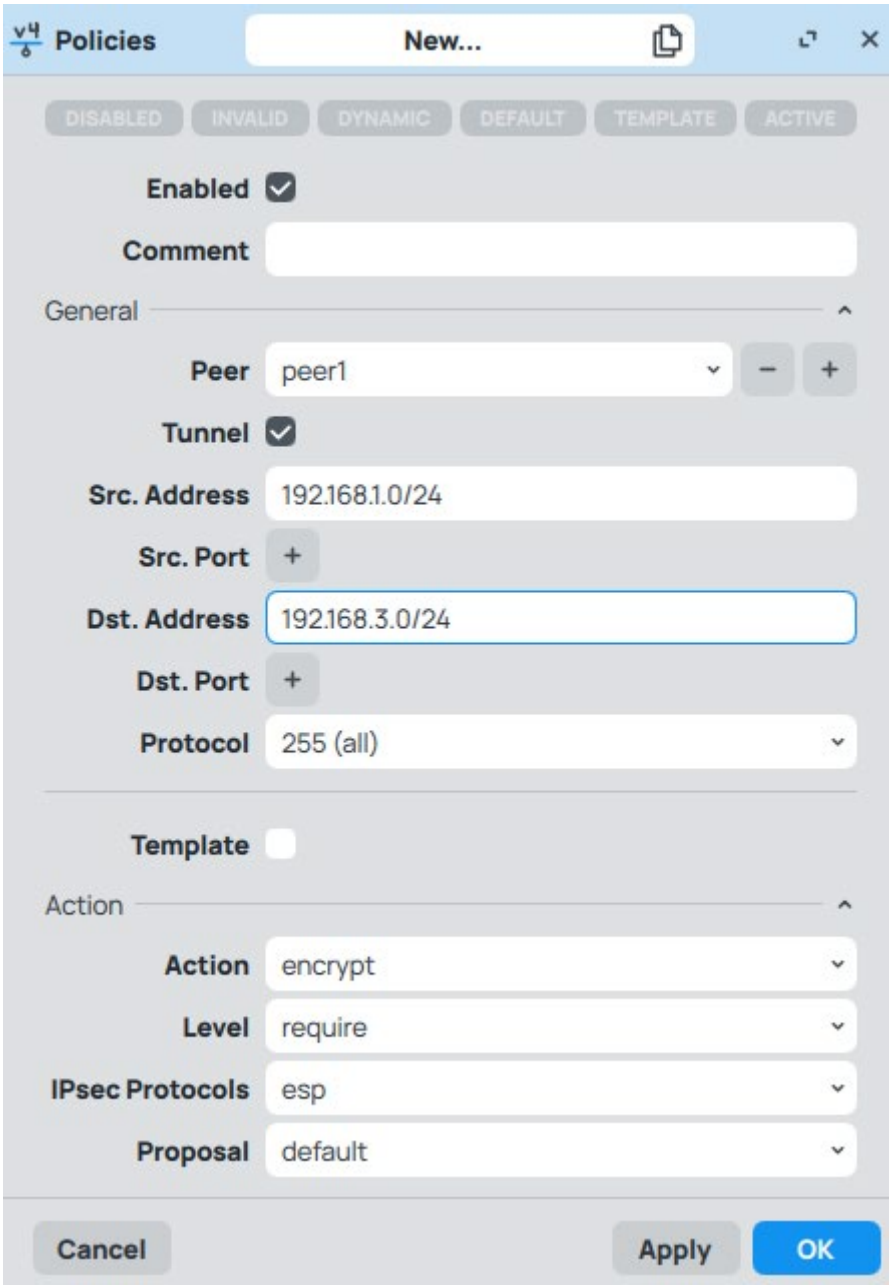

Figure 23: Configuration de la politique du VPN

- **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 :

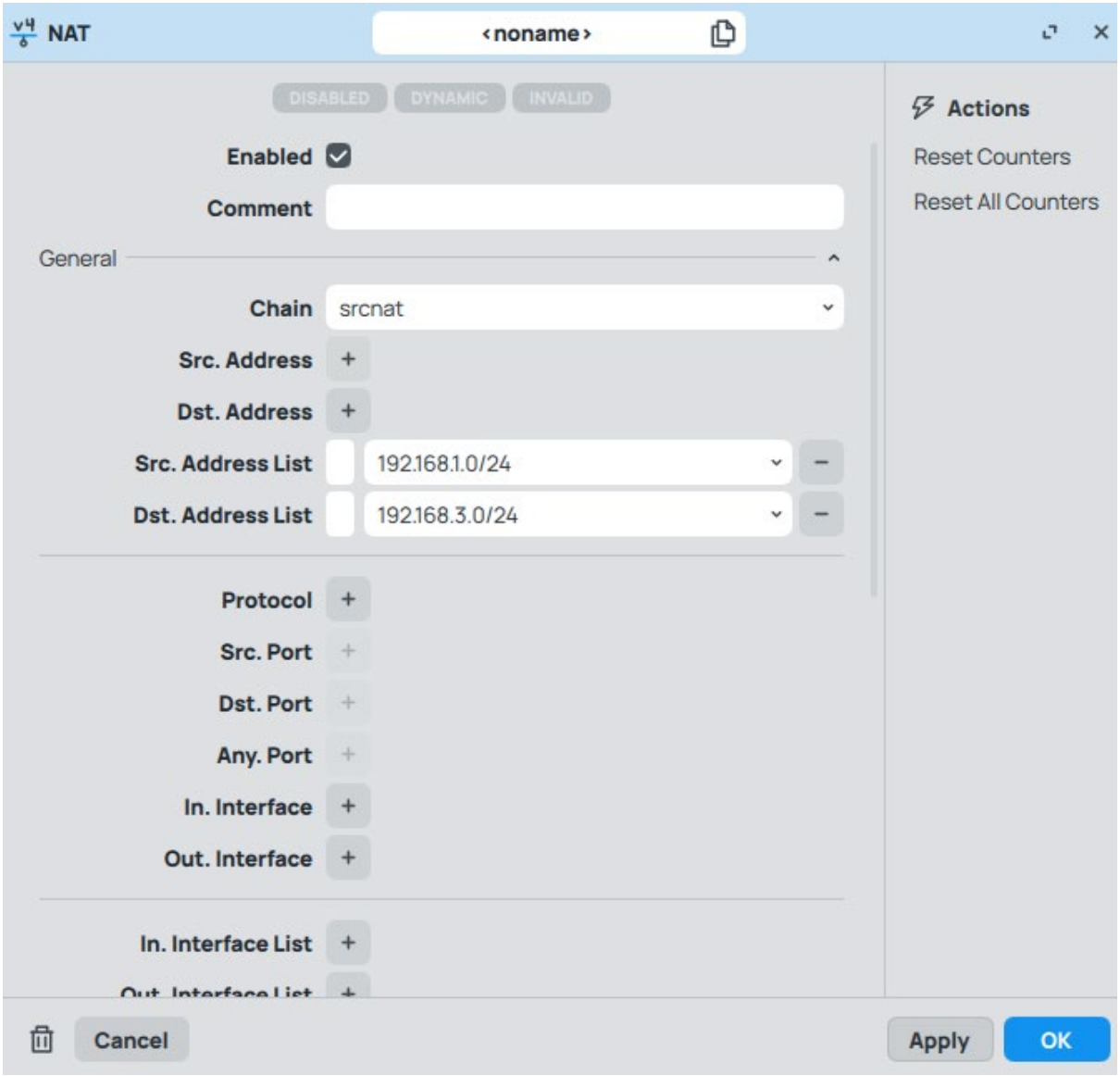

Figure 24: Configuration des règles NAT pour le VPN

- **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 :

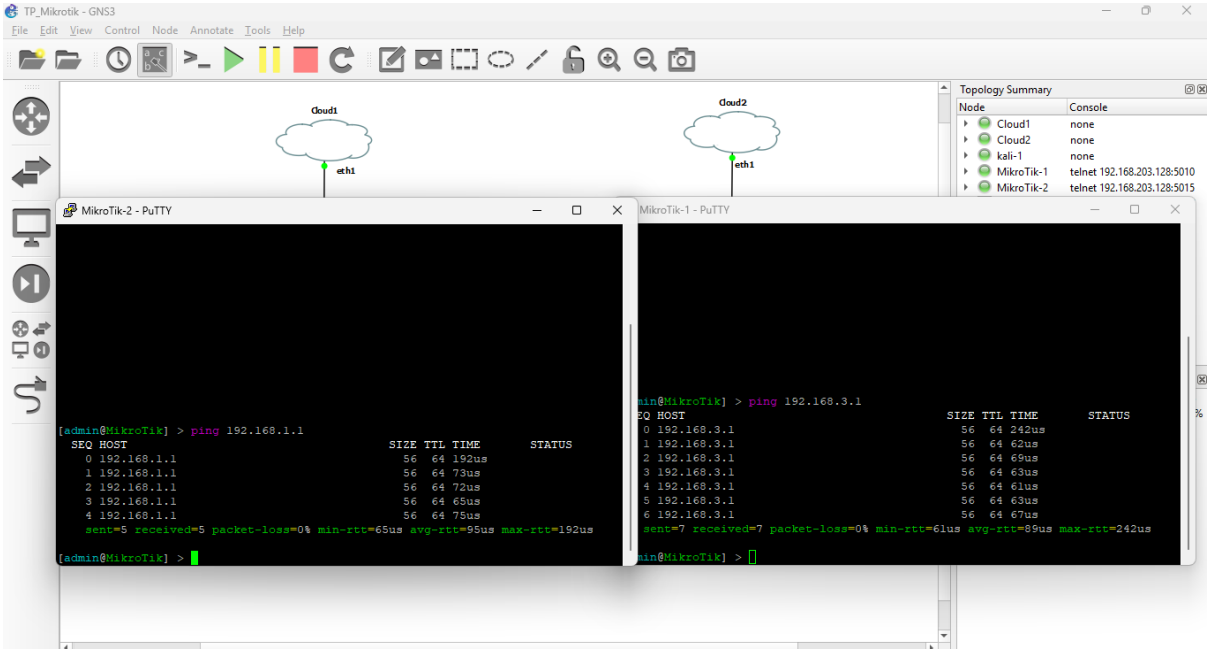

Figure 25: VPN site-to-site réussi

IV. Configuration Avancées Du Routeur Mikrotik

1. Gestion Des Utilisateurs Et Groupes

La gestion des utilisateurs et des groupes de sécurité constitue un élément fondamental pour assurer la sécurité et le contrôle d'accès aux équipements MikroTik. Par défaut, le système RouterOS propose un compte administrateur nommé « **admin** » sans mot de passe, ce qui représente un risque majeur en termes de sécurité. Il est donc impératif, dès la mise en service, de modifier ce compte ou de le supprimer, et de créer des comptes utilisateurs personnalisés dotés de mots de passe robustes.

Pour créer un utilisateur, nous devons-nous rendre sur **system** puis **users** et ensuite cliquer sur **new user**. La figure ci-dessous permet d'illustrer cela :

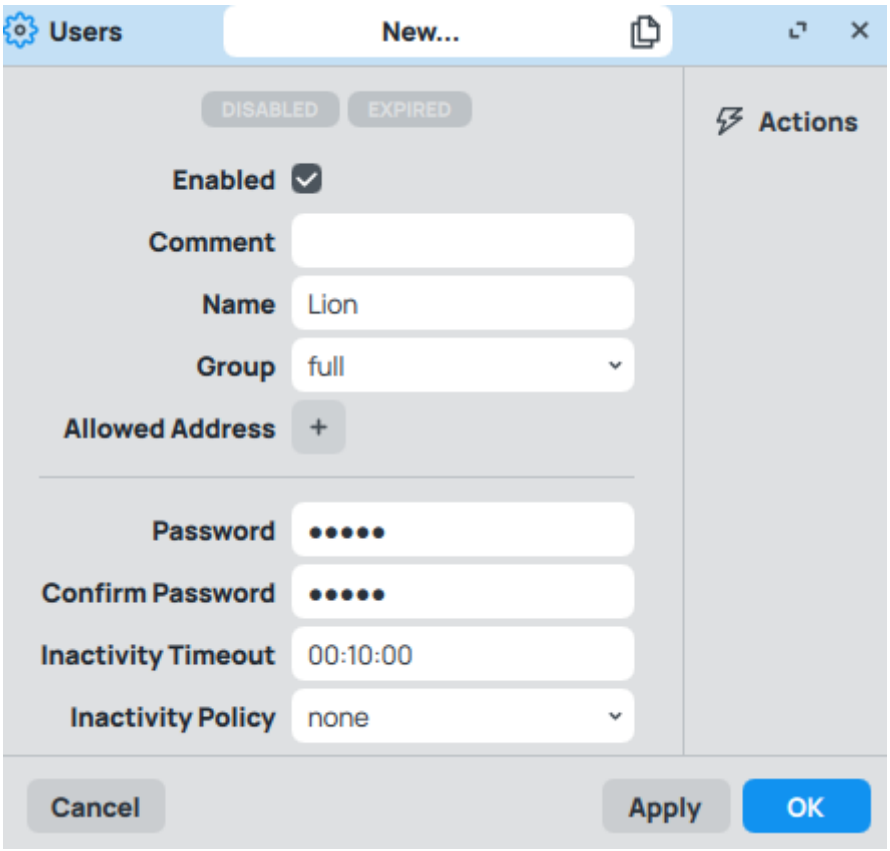

Figure 26: Création d'un compte utilisateur du Mikrotik

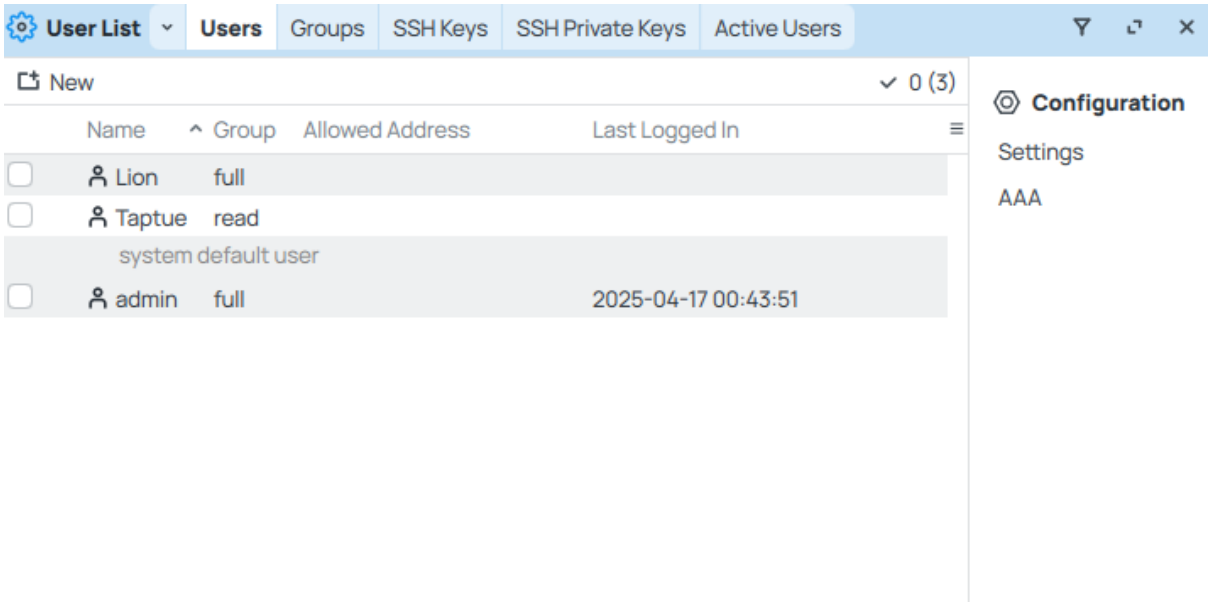

Figure 27: Liste des comptes utilisateurs de Mikrotik

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 Microtik 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.

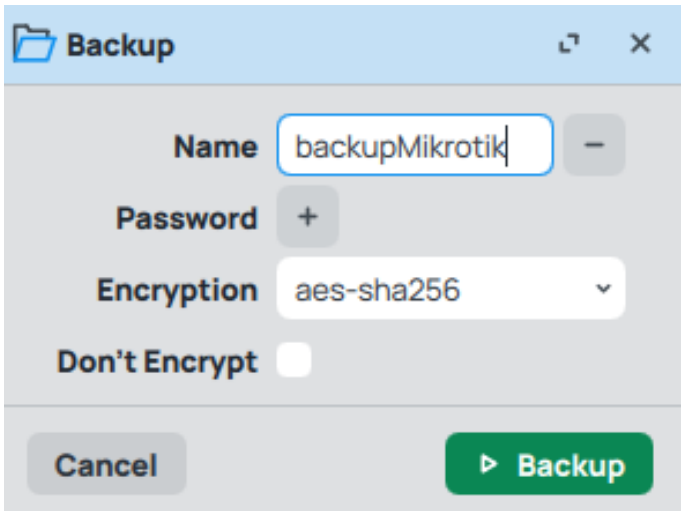

Figure 29: Sauvegarde dans un fichier binaire

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.

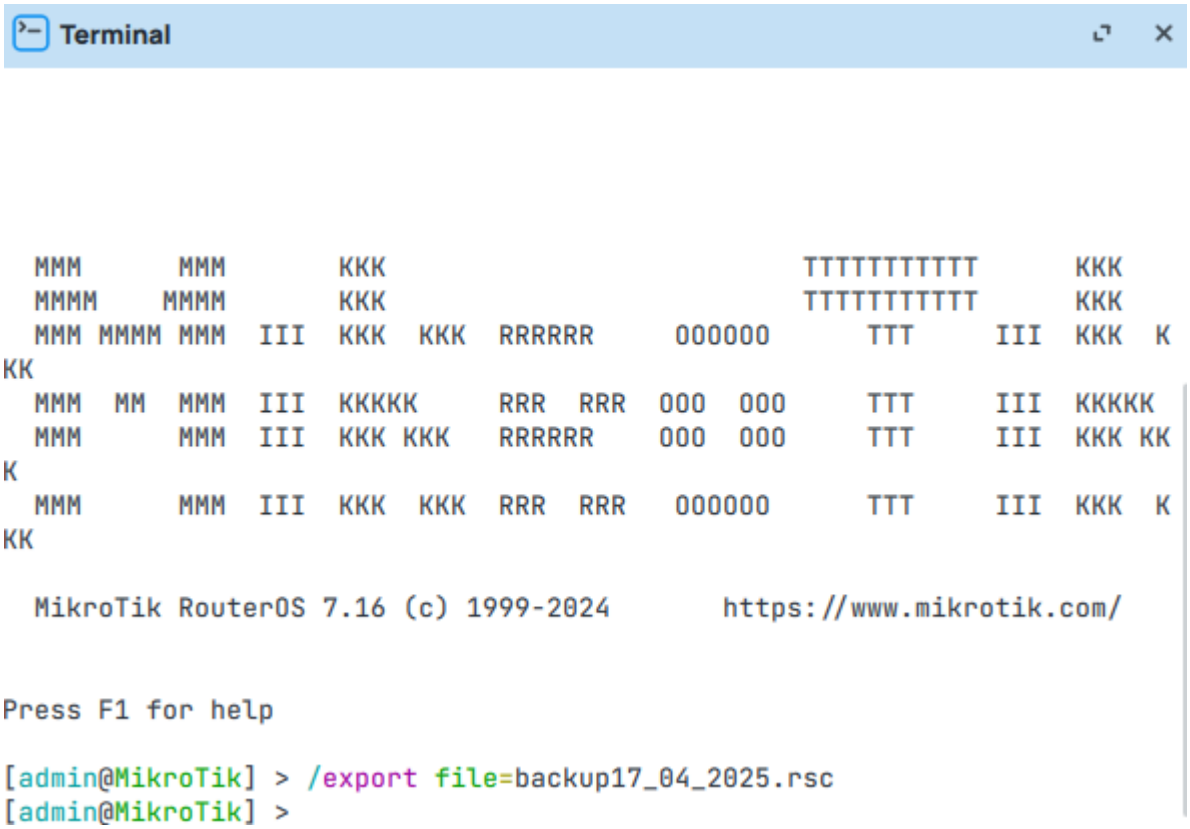

Figure 30: Exportation du fichier de configuration

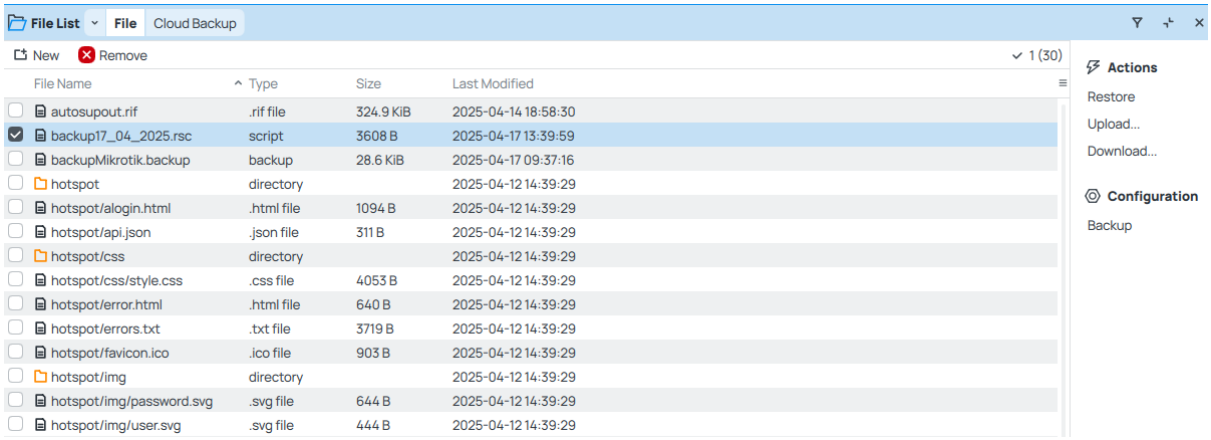

Figure 31: Fichiers de restauration exporté

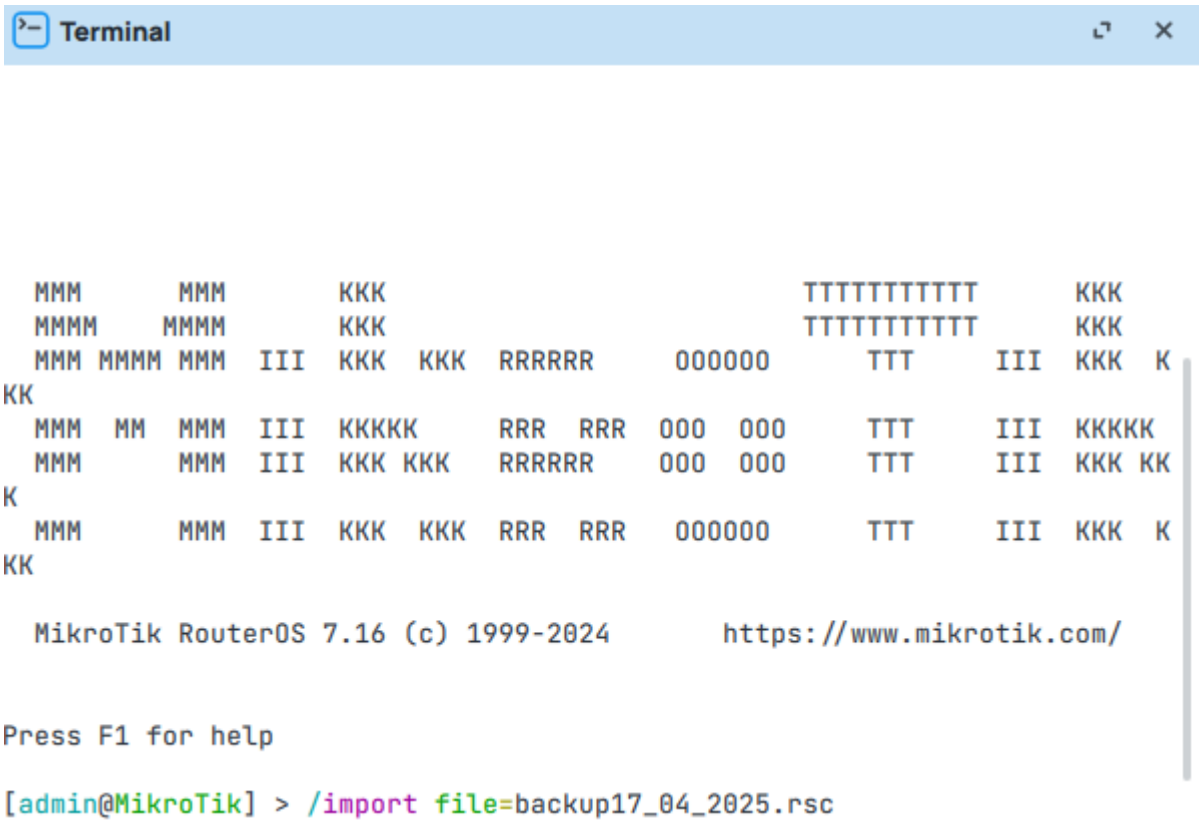

Figure 32: Importation du fichier de configuration

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.

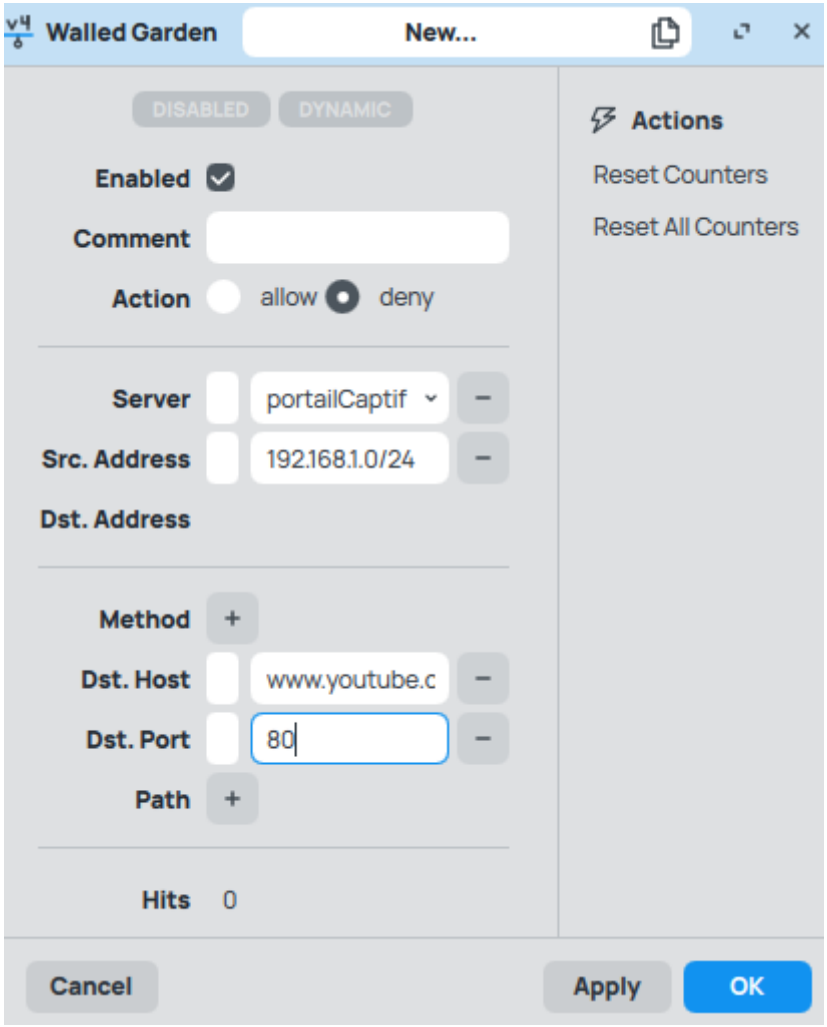

Figure 33: Configuration de Walled Garden

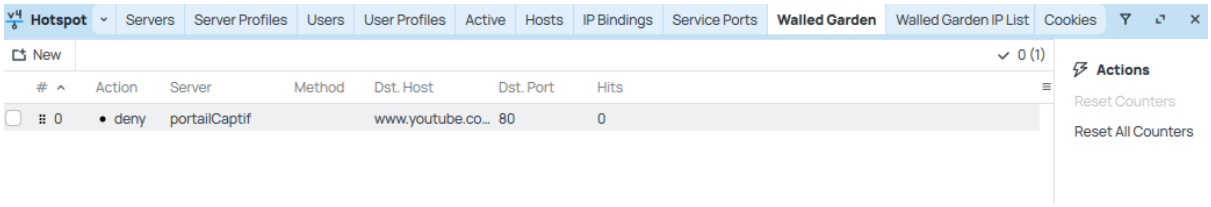

Figure 34: Liste des sites bloqués

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

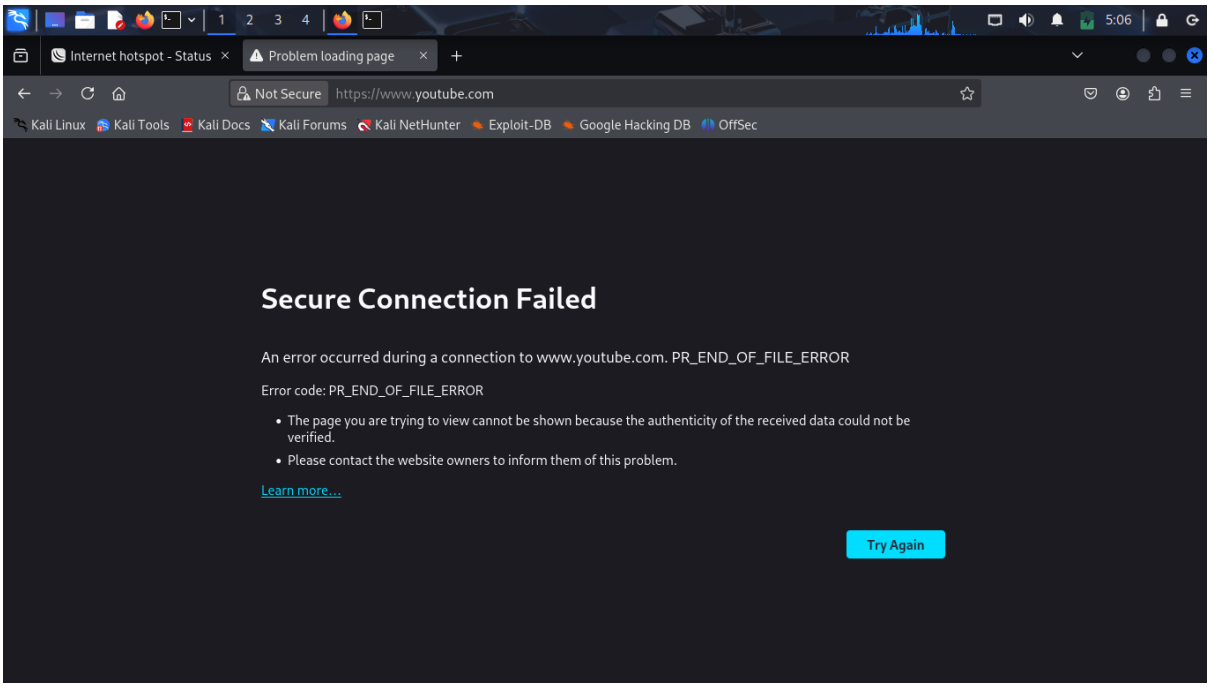

Figure 35: Impossible d'accéder à YouTube

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