

*BTS Services Informatiques aux Organisations
Option - Solutions d'infrastructure, Systèmes et Réseaux*

Épreuve E5 – Administration des systèmes et des Réseaux

Documentation technique



Projet 1 : Mise en place d'un routeur MikroTik
assurant les services DHCP, DNS et VPN
L2TP/IPsec Client-à-site

Sommaire

Introduction.....	Erreur ! Signet non défini.
Test DHCP & DNS.....	Erreur ! Signet non défini.
Test VPN L2TP/IPsec Client-à-site	Erreur ! Signet non défini.
Test de connectivité bidirectionnel (LAN – VPN).....	Erreur ! Signet non défini.
Conclusion	Erreur ! Signet non défini.

1. Introduction

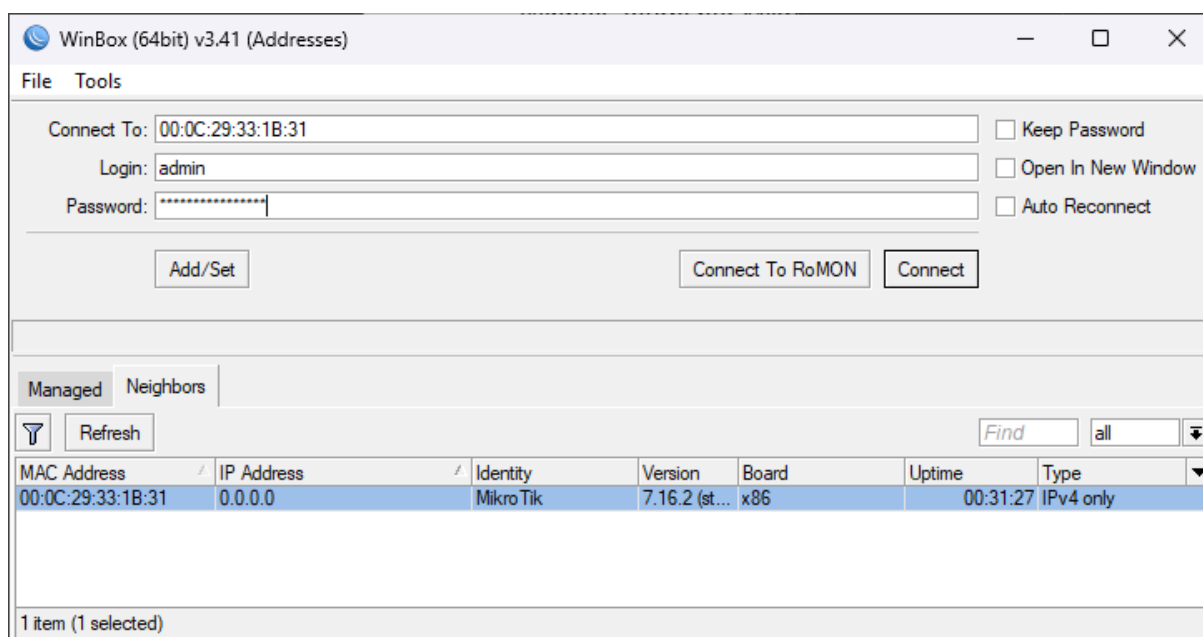
Cette documentation technique présente la mise en place d'une infrastructure réseau basée sur un routeur MikroTik, dans le cadre d'un projet réalisé au sein de l'entreprise Wayscom. L'objectif était de fournir au client Kairos une solution simple, fiable et sécurisée, intégrant un serveur DHCP, un serveur DNS, ainsi qu'un accès distant via VPN L2TP/IPsec (Client-to-Site).

Ce document détaille l'environnement de travail, les différentes étapes de configuration, les paramètres utilisés, ainsi que les outils exploités pour garantir le bon fonctionnement de l'ensemble des services.

2. Connexion au routeur MikroTik

Après avoir connecté physiquement le poste de travail au routeur MikroTik via un câble RJ45, l'accès à l'interface de configuration s'effectue à l'aide du logiciel Winbox, fourni par MikroTik.

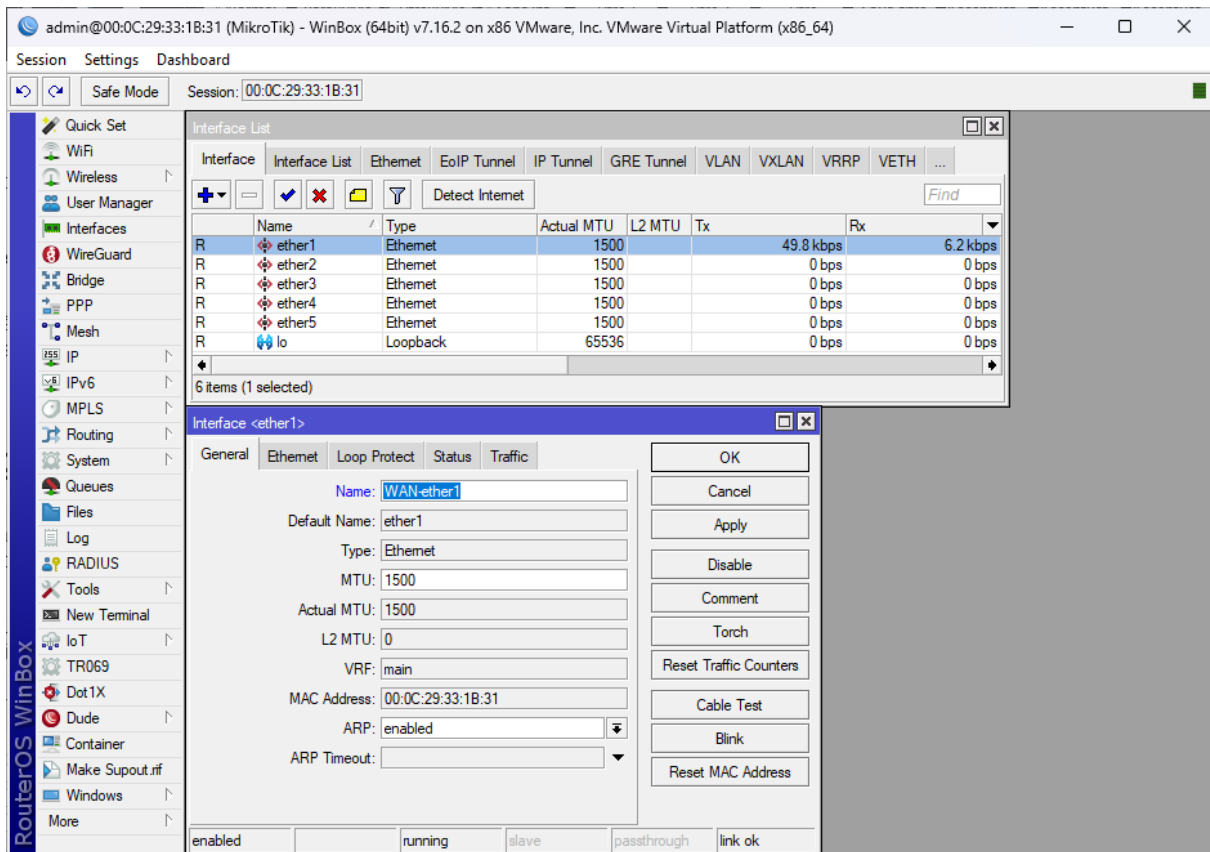
Par défaut, le routeur ne dispose d'aucune adresse IP. La connexion initiale se fait donc via son adresse MAC, en renseignant un nom d'utilisateur et un mot de passe. Pour ensuite cliquer sur le bouton "Connect"



Dans un premier temps, il est nécessaire d'identifier le port du routeur MikroTik qui sera utilisé comme port WAN, c'est-à-dire le port relié à Internet ou à la box du fournisseur d'accès.

Ce port permettra d'assurer la sortie vers l'extérieur ainsi que l'établissement du tunnel VPN client-to-site.

Chemin : **/interface**



Je clique sur "ether 1" afin d'ouvrir les paramètres du port pour ensuite le renommer dans la case "Name"

3. Configuration du DHCP & DNS

Je procède à la configuration réseau avec l’outil intégrer par Winbox “QuickSet” qui donne accès à différentes sections de paramétrage en se référant a notre table de routage

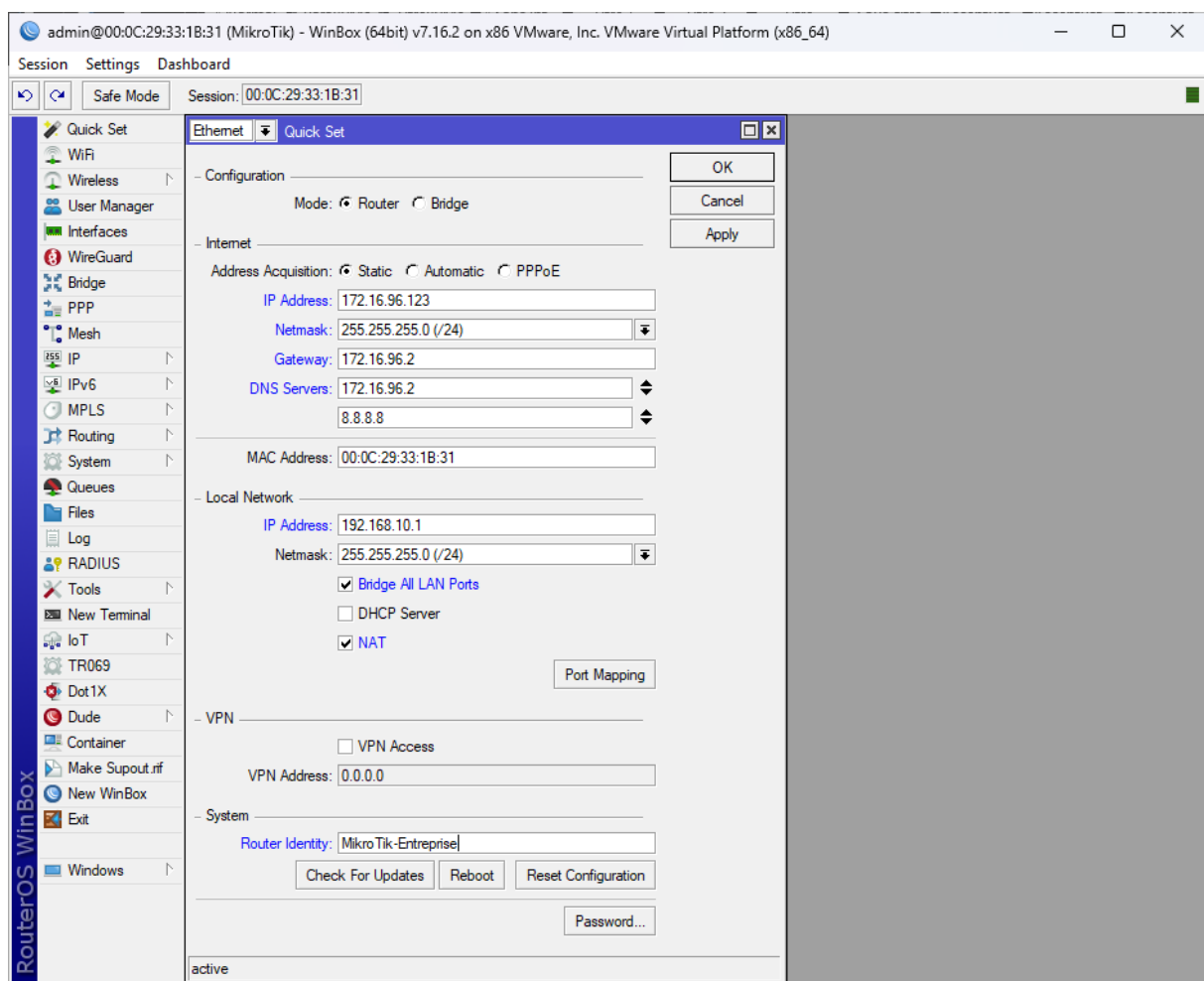
Table de routage :

Destination	Passerelle	Interface	Commentaire
172.16.96.123/24	172.16.96.2	WAN-ether1	Réseau WAN
192.168.10.0/24	192.168.10.1	Bridge1	Réseau LAN
192.168.100.0/24	172.16.96.123/24	L2TP	Réseau VPN

Pools DHCP :

Plage d’adresse
dhcp_pool0 : 192.168.10.2-254
l2tp/ipsec_pool0 : 192.168.100.2-254

Chemin : /Quick Set



Configuration :

- **Mode** : Router

Ce mode permet au MikroTik d'assurer le rôle de routeur, c'est-à-dire de faire transiter les paquets entre le réseau local (LAN) et le réseau externe (WAN). Il permet également d'activer les fonctions NAT, DHCP, etc.

Internet (WAN) :

- **Address Acquisition** : Static

Le routeur utilise une adresse IP fixe (statique) pour se connecter à Internet. Cela évite tout changement d'adresse au redémarrage et assure une meilleure stabilité.

- **IP Address** : 172.16.96.123

Adresse IP du routeur sur le réseau WAN, définie manuellement.

- **Netmask** : 255.255.255.0 (/24)

Masque de sous-réseau pour le réseau WAN, ici un réseau de classe C standard.

- **Gateway** : 172.16.96.2

Passerelle utilisée pour accéder à Internet ou à d'autres réseaux externes.

- **DNS Servers** : 172.16.96.2 et 8.8.8.8

Serveurs DNS utilisés pour la résolution de noms de domaine. Le premier est un DNS interne ou celui du FAI, le second est un DNS public de Google.

Local Network (LAN) :

- **IP Address** : 192.168.10.1

Adresse IP du routeur sur le réseau local. C'est la passerelle par défaut pour les machines du LAN.

- **Netmask** : 255.255.255.0 (/24)

Masque de sous-réseau du réseau local.

- **Bridge all LAN Ports**

Tous les ports Ethernet restants (hors WAN) sont regroupés dans un bridge unique, ce qui permet de les traiter comme un seul réseau.

- **DHCP Server** (décoché)

Il est préférable de procéder ultérieurement à la mise en place du serveur DHCP, de manière plus détaillée et personnalisée.

- **NAT** (coché)

Active la translation d'adresses réseau (NAT) permettant aux clients du LAN d'accéder à Internet en utilisant l'adresse IP publique du routeur.

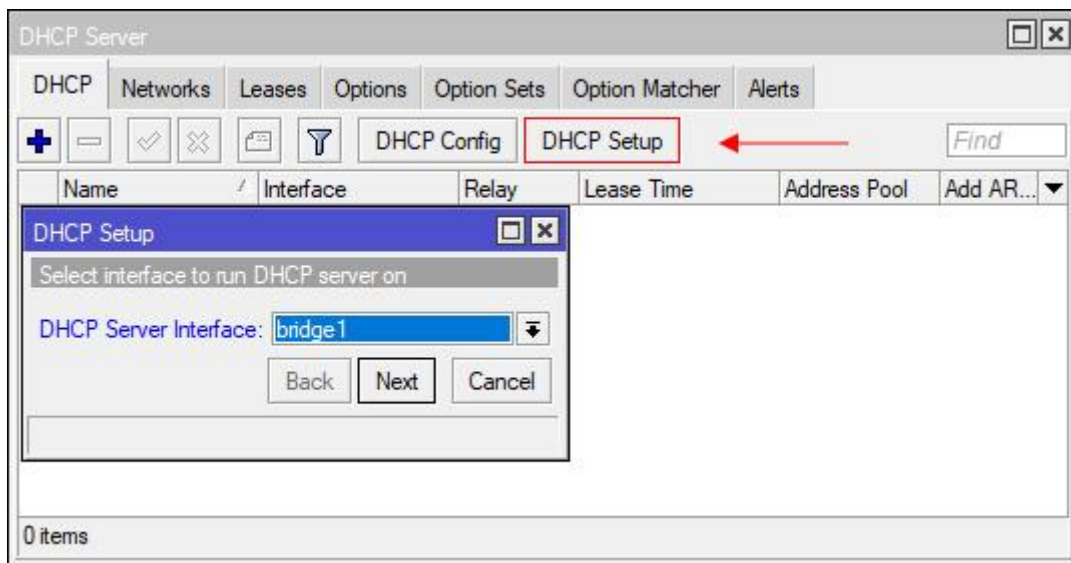
System :

- **Router Identity** : MikroTik-Entreprise
Nom d'identification du routeur dans le réseau. Ce nom est visible dans les outils d'administration et facilite la reconnaissance de l'équipement.

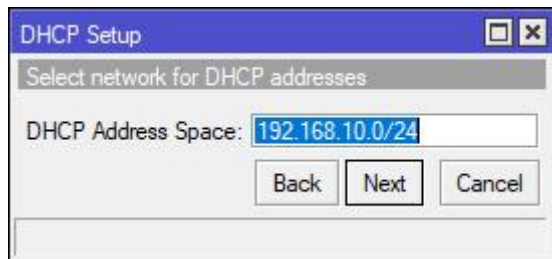
Une fois l'adressage réseau configuré, nous procédons à la mise en place du Serveur DHCP

Chemin : ***/IP/DCHP Server***

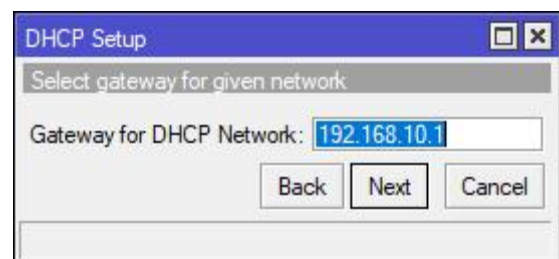
En cliquant sur "DHCP Setup" nous avons l'ouverture de la fenêtre "DHCP Setup"



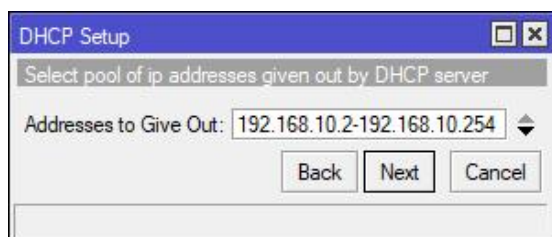
Bridge1 comme choix d'interface du serveur DHCP



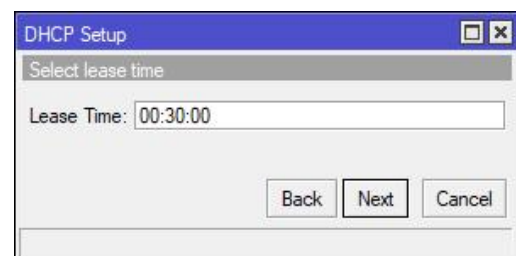
L'adresse réseau



La passerelle

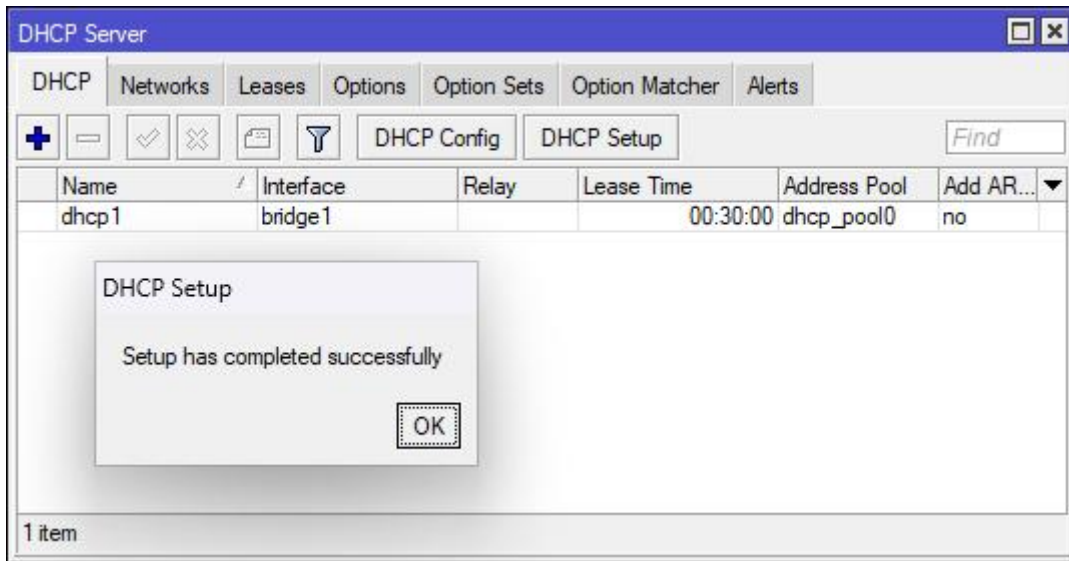


La plage d'adresses IP à distribuer (pool)



La durée de bail accordée à chaque client

Une fois toutes ces étapes effectuées notre serveur DHCP est opérationnelle et fonctionnelle.



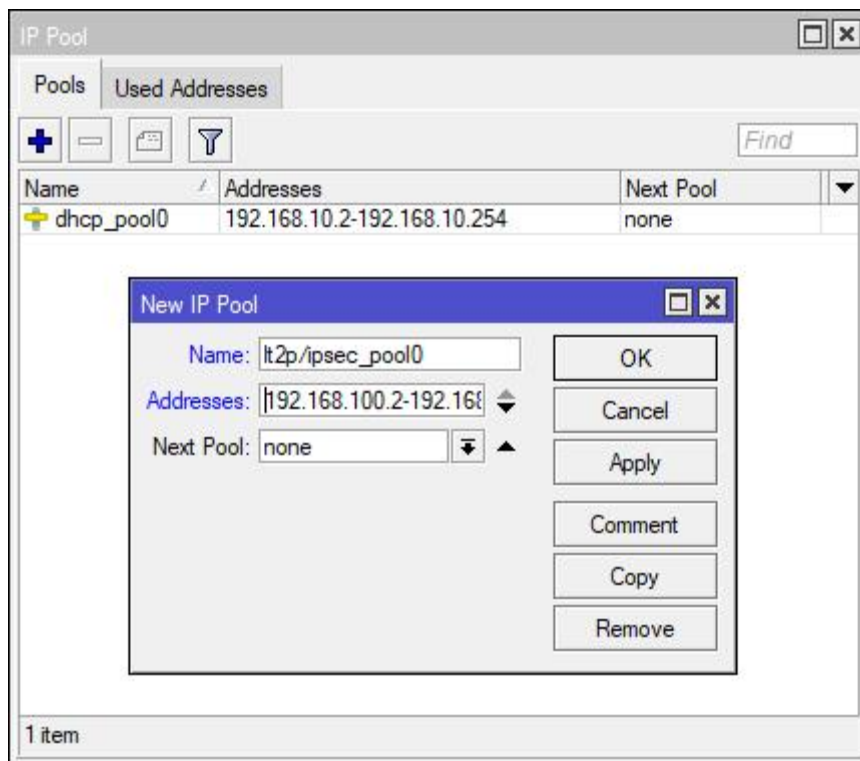
Le routeur MikroTik est désormais en mesure d'attribuer automatiquement les adresses IP et les paramètres réseau nécessaires aux clients du réseau local, assurant ainsi une gestion simplifiée et centralisée de l'adressage IP.

4. Configuration VPN L2TP/IPsec (Client-à-site)

Nous allons à présent procéder à la configuration du VPN L2TP/IPsec en mode client-à-site, permettant aux utilisateurs distants de se connecter en toute sécurité au réseau de l'entreprise.

Avant cela, il est nécessaire de créer un pool d'adresses IP dédié aux clients VPN. Ce pool sera utilisé pour attribuer automatiquement une adresse IP à chaque utilisateur connecté via le tunnel VPN.

Chemin : **/IP/IP Pool**



- **Name** : VPN-Pool
Nom du pool à choisir afin de l'identifier facilement dans la configuration du VPN.
- **Addresses** : 192.168.100.2-192.168.100.254
Plage d'adresse IP qui seront attribuées dynamiquement aux clients VPN.

Ce pool sera utilisé plus tard dans la configuration du profil VPN pour fournir automatiquement une adresse IP à chaque utilisateur connecté.

Création d'un profil VPN personnalisé

Chemin : **/PPP/Profiles**

PPP Profile <profile-VPN-L2TP>

General Protocols Limits Queue Scripts

Name: profile-VPN-L2TP

Local Address: vpn-l2tp/ipsec_pool0

Remote Address: vpn-l2tp/ipsec_pool0

Remote IPv6 Prefix Pool:

DHCPv6 PD Pool:

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Bridge Learning: default

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

Change TCP MSS

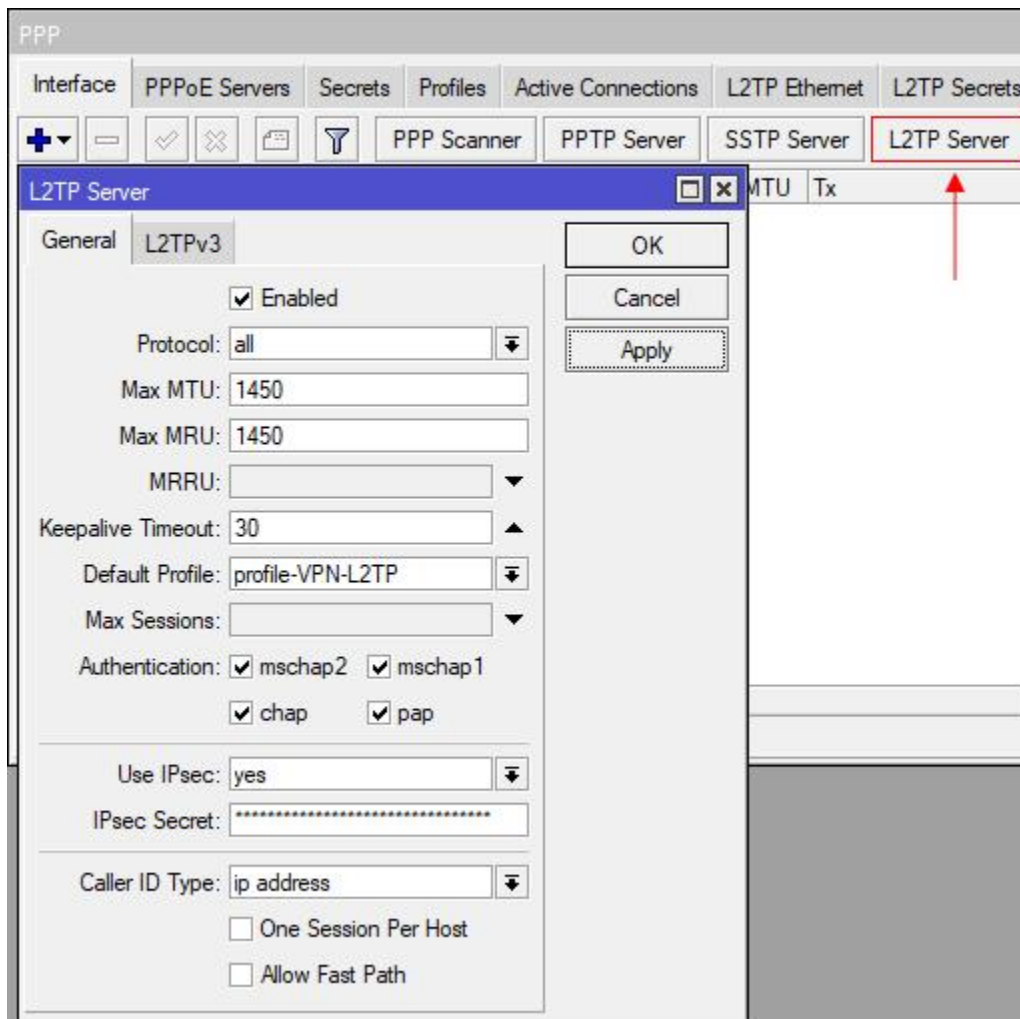
no yes default

OK Cancel Apply Comment Copy Remove

- **Name** : VPN-Pool
Nom du profile à choisir afin de l'identifier facilement dans la sélection de profile VPN.
- **Local Address** : vpn-l2tp/ipsec_pool0
Cette adresse représente l'IP attribuée au routeur MikroTik dans le tunnel VPN. Elle agit comme passerelle pour les clients VPN.

- **Remote Address** : vpn-l2tp/ipsec_pool0
Cette option définit les adresses IP attribuées dynamiquement aux clients VPN lorsqu'ils se connectent.

Configuration Serveur L2TP
Chemin : **/PPP/L2TP Server**



- **Default Profile** : profile-VPN-L2TP
C'est le profil VPN que nous avons créé au préalable, il contient toutes les configurations spécifiques VPN.
- **Authentication** : mschap2, mschap1, chap, pap
Le fait de cocher toutes les sécurités d'authentification permet une compatibilité avec le plus de système possible.
- **Use IPsec** : yes
Active la protection IPsec sur le tunnel L2TP, ajoutant une couche de sécurité via le chiffrement.

- **IPsec Secret** : Pour la clé secrète pré-partagée nous utiliserons l’outil “Google Cloud Generating Pre-Shared-Key” afin de générer une clé suffisamment sécuriser selon la CNIL.

Création d’un utilisateur VPN :

Chemin : **/PPP/Secrets**

The screenshot shows the configuration for a PPP secret. The main window has tabs for Interface, PPPoE Servers, Secrets, Profiles, Active Connections, and L2TP Eth. Below the tabs is a table with columns: Name, Password, Service, Caller ID, Profile, and Local Address. The entry 'Nomade-1' is selected. A dialog box titled 'PPP Secret <Nomade-1>' is open, showing the following fields:

- Name: Nomade-1
- Password: [masked]
- Service: l2tp
- Caller ID: [empty]
- Profile: profile-VPN-L2TP
- Local Address: [empty]
- Remote Address: [empty]
- Remote IPv6 Prefix: [empty]
- Routes: [empty]
- IPv6 Routes: [empty]
- Limit Bytes In: [empty]
- Limit Bytes Out: [empty]
- Last Logged Out: Apr/14/2025 14:45:43
- Last Caller ID: 172.16.96.128
- Last Disconnect Reason: peer request

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status at the bottom is 'enabled'.

- **Name** : Nomade-1
Nous choisissons l’identifiant de connexion qui sera attribuer à l’utilisateur VPN.
- **Password** : Le mot de passe renforcé pour l’utilisateur du VPN est toujours prédéfini que seule l’administrateur système peut modifier.

- **Service** : l2tp
Le choix "L2TP" qui spécifie la technologie VPN choisie pour l'utilisateur.
- **Profile** : profile-VPN-L2TP
C'est le profil VPN que nous avons créé au préalable, il contient toutes les configurations spécifiques VPN.

Le routeur MikroTik est désormais en mesure d'établir des connexions VPN sécurisées en mode client-à-site, permettant aux utilisateurs distants d'accéder aux ressources internes de l'entreprise comme s'ils étaient sur le réseau local. L'infrastructure offre une solution fiable, centralisée et conforme aux bonnes pratiques de sécurité

5. Configuration du Pare-Feu

Afin de sécuriser l'infrastructure réseau, il est essentiel de configurer des règles de pare-feu adaptées. Ces règles permettent de contrôler le trafic entrant et sortant, d'autoriser les connexions VPN, et de protéger le routeur MikroTik contre les accès non autorisés ou les attaques extérieures.

Règle de pare-feu 1

Chemin : ***/IP/Firewall/Filter Rules***

The screenshot shows the Mikrotik Firewall configuration interface. The title bar reads "Firewall Rule <192.168.10.0/24->192.168.100.0/24>". The "General" tab is selected, showing the following configuration:

- Chain: forward
- Src. Address: 192.168.10.0/24
- Dst. Address: 192.168.100.0/24
- Src. Address List: (empty)
- Dst. Address List: (empty)
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: (empty)
- Out. Interface: (empty)
- In. Interface List: (empty)
- Out. Interface List: (empty)
- Packet Mark: (empty)

At the bottom left, the rule is marked as "enabled". On the right side, there are several action buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Cette règle autorise le trafic du réseau local vers le réseau VPN

Règle de pare-feu 2

Chemin : ***/IP/Firewall/Filter Rules***

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists

Firewall Rule <192.168.100.0/24->192.168.10.0/24>

General Advanced Extra Action Statistics

Chain: forward

Src. Address: 192.168.100.0/24

Dst. Address: 192.168.10.0/24

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Cette règle autorise le trafic du réseau VPN vers le réseau LAN

Règle NAT

Chemin : ***/IP/Firewall/NAT***

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address

NAT Rule <192.168.100.0/24>

General Advanced Extra Action ...

Chain: srcnat

Src. Address: 192.168.100.0/24

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: bridge1

In. Interface List:

Out. Interface List:

enabled

2 items (1 selected)

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Cette règle autorise le réseau VPN à accéder à internet via à l'interface **“bridge1”**

Activation du mode Proxy-ARP sur le bridge

Chemin : **/Interfaces/bridge1/ ARP***

The image shows two screenshots from Mikrotik WinBox. The top screenshot is the 'Interface List' window, showing a table of network interfaces. The 'bridge1' interface is selected. The bottom screenshot is the 'Interface <bridge1>' configuration window, showing various settings for the bridge. The 'ARP' dropdown menu is highlighted with a red box and set to 'proxy-arp'.

Interface	Name	Type	Actual MTU	L2 MTU	Tx
R	WAN-ether1	Ethernet	1500		63.6 kb
R	bridge1	Bridge	1500	65535	0 kb
RS	ether2	Ethernet	1500		480 kb
RS	ether3	Ethernet	1500		0 kb
RS	ether4	Ethernet	1500		0 kb
RS	ether5	Ethernet	1500		0 kb

7 items (1 selected)

Interface <bridge1>

General STP VLAN Status Traffic

Name: bridge1

Type: Bridge

MTU: [dropdown]

Actual MTU: 1500

L2 MTU: 65535

MAC Address: 00:0C:29:33:1B:3B

ARP: proxy-arp

ARP Timeout: [dropdown]

Admin. MAC Address: [dropdown]

Ageing Time: 00:05:00

Max Learned Entries: auto

enabled [checkbox] running [checkbox] slave [checkbox] passthrough [checkbox]

OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters

Sur l'interface "bridge1" nous activons dans la section "ARP" l'option "proxy-arp" afin de permettre aux requêtes ARP pour les IP du réseau VPN sur le réseau local

La mise en place de ces règles de pare-feu et de NAT assure une communication fluide et sécurisée entre les clients VPN et le réseau local. Grâce à cette configuration, les utilisateurs distants peuvent accéder aux ressources internes tout en respectant les bonnes pratiques de sécurité réseau.

6. Conclusion

Ce document technique a été réalisé selon les exigences de l'entreprise Wayscom pour le client Kairos, dans le cadre de la mise en place d'une infrastructure réseau fiable, fonctionnelle et sécurisée.

La solution proposée repose sur un routeur MikroTik assurant les services suivants :

- **Un serveur DHCP** pour l'attribution automatique des adresses IP,
- **Un serveur DNS** pour la résolution des noms de domaine,
- **Un VPN L2TP/IPsec** en mode client-à-site permettant aux utilisateurs distants d'accéder aux ressources internes de l'entreprise en toute sécurité.

L'ensemble de la configuration a été testé et validé, répondant pleinement aux objectifs définis par l'entreprise : accessibilité, sécurité et simplicité d'administration. Cette infrastructure constitue une base solide pour les besoins actuels et futurs du client.