

ROUTEROS 7

Cours MikroTik de A à Z

Réseau local, réseau d'entreprise, hotspot, sécurité, VPN et
automatisation : 41 scripts expliqués, prêts à copier

Professeur : Monsieur Stan · Tél. +228 91 53 84 61 · +228 96 18 64 01

Sommaire

1. Les bases du cours
2. Bases
3. Réseau local
4. Entreprise
5. Hotspot
6. Sécurité
7. VPN
8. Automatisation
9. Dépannage

1 Les bases du cours

1. Découvrir MikroTik et RouterOS

MikroTik est un fabricant letton de routeurs, switches et points d'accès très utilisés en Afrique pour leur prix et leur puissance. Tous fonctionnent avec le système RouterOS. Modèles courants : hAP ac² et hAP ax² (maison, petit bureau), hEX (routeur filaire), RB4011 et RB5009 (PME), CCR (gros réseaux, fournisseurs d'accès), cAP et wAP (points d'accès Wi-Fi), LtAP / Chateau (routeurs 4G/5G). Ce cours utilise RouterOS version 7.

2. Se connecter au routeur

Trois façons : Winbox (logiciel Windows, le plus pratique), WebFig (dans le navigateur, adresse <http://192.168.88.1>) et le Terminal (lignes de commande). Sur un routeur neuf : adresse 192.168.88.1, utilisateur admin, et le mot de passe imprimé sur l'étiquette (ou vide sur les anciens modèles). Branchez le PC sur le port 2, jamais sur le port 1 qui sert à Internet (WAN).

3. Comment appliquer un script

1) Faites toujours une sauvegarde d'abord (Files → Backup). 2) Remplacez les valeurs entre guillemets (mots de passe, identifiants, adresses). 3) Dans Winbox, ouvrez New Terminal, collez le script et appuyez sur Entrée. Ou bien : téléchargez le fichier .rsc, glissez-le dans Files, puis tapez `/import file-name=nom.rsc`. 4) Vérifiez le résultat dans le menu concerné. Les lignes qui commencent par `#` sont des commentaires et ne font rien.

4. Les notions à connaître

Interface : un port (ether1, wlan1...). Bridge : regroupe plusieurs ports dans un même réseau local. Liste d'interfaces : groupes WAN (Internet) et LAN (local) utilisés par le pare-feu. DHCP : distribue automatiquement les adresses IP. NAT (masquerade) : partage la connexion Internet. Pare-feu (firewall) : chaîne input = trafic vers le routeur, forward = trafic qui traverse le routeur. VLAN : découpe un réseau en plusieurs réseaux séparés sur les mêmes câbles. Queue : limite le débit.

5. Les trois grands scénarios

Réseau local (maison, boutique, petit bureau) : bridge LAN + DHCP + NAT + pare-feu + Wi-Fi. Réseau d'entreprise : VLAN par service, isolation des invités et des caméras, double connexion Internet (secours ou partage de charge), limitation de débit, VPN pour le télétravail. Hotspot (cyber, hôtel, résidence, quartier) : portail de connexion, forfaits par durée, tickets, sites gratuits et appareils autorisés sans ticket.

Règle d'or

Faites toujours une sauvegarde avant d'appliquer un script, et remplacez les mots de passe et adresses d'exemple par les vôtres.

2 Bases

Nommer le routeur, heure et serveur de temps Débutant

Donne un nom au routeur (visible dans Winbox) et règle l'heure du Togo avec synchronisation automatique, indispensable pour les journaux et les sauvegardes.

```
# Nom du routeur
/system identity set name="GLOBIPNET-R1"
# Fuseau horaire du Togo et heure automatique
/system clock set time-zone-name=Africa/Lome
/system ntp client set enabled=yes
/system ntp client servers add address=pool.ntp.org
```

Créer un administrateur et désactiver « admin » Débutant

Le compte admin par défaut est la première cible des pirates. On crée un compte personnel avec un mot de passe fort, puis on désactive admin.

```
# Remplacez le nom et le mot de passe
/user add name=stan group=full password="MotDePasse-Tres-Fort-2026"
# Reconnectez-vous avec le nouveau compte AVANT de désactiver admin
/user disable admin
```

Important

Testez la connexion avec le nouveau compte avant de désactiver admin, sinon vous risquez de vous bloquer.

Mettre à jour RouterOS et le firmware Débutant

Installe la dernière version stable de RouterOS (corrections de sécurité), puis met à jour le firmware de la carte. Le routeur redémarre.

```
/system package update set channel=stable
/system package update check-for-updates
/system package update install
# Après le redémarrage :
/system routerboard upgrade
/system reboot
```

Remettre le routeur à zéro Intermédiaire

Efface toute la configuration pour repartir sur une base propre. Le routeur redémarre sans aucune configuration : reconnectez-vous ensuite avec Winbox par l'adresse MAC.

```
# ATTENTION : efface toute la configuration
/system reset-configuration no-defaults=yes skip-backup=yes
```

Important

Faites une sauvegarde avant. Après la remise à zéro, ouvrez Winbox, onglet Neighbors, et connectez-vous par l'adresse MAC.

Sauvegarder et restaurer la configuration Débutant

Deux types de sauvegarde : le fichier .backup (copie complète, pour le même routeur) et l'export .rsc (texte lisible, réutilisable sur un autre routeur).

```
# Sauvegarde complète
/system backup save name=sauvegarde-glob dont-encrypt=yes
# Export texte de la configuration
/export file=config-glob
# Restaurer une sauvegarde complète (le routeur redémarre)
# /system backup load name=sauvegarde-glob.backup
```

Important

Téléchargez les fichiers depuis le menu Files vers votre PC et gardez-les en lieu sûr.

3 Réseau local

Configuration complète d'un réseau local (maison / PME)

Débutant

Le script de base : ether1 vers le modem du fournisseur d'accès, ports 2 à 5 regroupés en réseau local 192.168.88.0/24, distribution automatique des adresses (DHCP), DNS et partage de la connexion Internet (NAT).

```
# 1) Bridge du réseau local avec les ports 2 à 5
/interface bridge add name=bridge-lan
/interface bridge port add bridge=bridge-lan interface=ether2
/interface bridge port add bridge=bridge-lan interface=ether3
/interface bridge port add bridge=bridge-lan interface=ether4
/interface bridge port add bridge=bridge-lan interface=ether5
# 2) Listes WAN et LAN (utilisées par le pare-feu)
/interface list add name=WAN
/interface list add name=LAN
/interface list member add list=WAN interface=ether1
/interface list member add list=LAN interface=bridge-lan
# 3) Adresse du routeur et Internet par DHCP sur ether1
/ip address add address=192.168.88.1/24 interface=bridge-lan
/ip dhcp-client add interface=ether1 disabled=no
# 4) Serveur DHCP pour les appareils du réseau
/ip pool add name=pool-lan ranges=192.168.88.10-192.168.88.254
/ip dhcp-server add name=dhcp-lan interface=bridge-lan address-pool=pool-lan disabled=no
/ip dhcp-server network add address=192.168.88.0/24 gateway=192.168.88.1 dns-server=192.168.88.1
# 5) DNS et partage de connexion
/ip dns set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
/ip firewall nat add chain=srcnat out-interface-list=WAN action=masquerade comment="NAT Internet"
```

Important

À appliquer sur un routeur remis à zéro. Ajoutez ensuite le pare-feu de base (catégorie Sécurité).

Internet par PPPoE (fibre, ADSL)

Débutant

Quand le fournisseur d'accès donne un identifiant et un mot de passe de connexion (fibre Togocom, Canalbox, etc. en mode routeur), le MikroTik se connecte lui-même en PPPoE.

```
/interface pppoe-client add name=pppoe-out1 interface=ether1 user="identifiant-FAI" password="motdepasse-FAI" add-default-route=yes use-peer-dns=yes disabled=no
/interface list member add list=WAN interface=pppoe-out1
```

Internet avec adresse IP fixe

Débutant

Pour les liaisons professionnelles avec adresse publique fixe : on renseigne l'adresse, la passerelle et les DNS donnés par le fournisseur.

```
# Remplacez par les valeurs de votre fournisseur
/ip address add address=203.0.113.10/29 interface=ether1
/ip route add dst-address=0.0.0.0/0 gateway=203.0.113.9
/ip dns set servers=8.8.8.8,1.1.1.1
```

Wi-Fi sécurisé (modèles récents, menu WiFi) Débutant

Pour les modèles récents (hAP ax², hAP ax³, cAP ax...) qui utilisent le menu « WiFi » de RouterOS 7. Crée un Wi-Fi protégé WPA2/WPA3 relié au réseau local.

```
/interface wifi set wifi1 configuration.mode=ap configuration.ssid="GLOBIPNET" security.authentication-type
s=wpa2-psk,wpa3-psk security.passphrase="MotDePasseWiFi2026" disabled=no
/interface wifi set wifi2 configuration.mode=ap configuration.ssid="GLOBIPNET-5G" security.authentication-t
ypes=wpa2-psk,wpa3-psk security.passphrase="MotDePasseWiFi2026" disabled=no
/interface bridge port add bridge=bridge-lan interface=wifi1
/interface bridge port add bridge=bridge-lan interface=wifi2
```

Wi-Fi sécurisé (anciens modèles, menu Wireless) Débutant

Pour les modèles plus anciens (hAP ac lite, hAP ac², cAP ac...) qui utilisent le menu « Wireless ».

```
/interface wireless security-profiles add name=wifi-secu mode=dynamic-keys authentication-types=wpa2-psk wp
a2-pre-shared-key="MotDePasseWiFi2026"
/interface wireless set wlan1 mode=ap-bridge ssid="GLOBIPNET" band=2ghz-b/g/n frequency=auto security-profi
le=wifi-secu disabled=no
/interface bridge port add bridge=bridge-lan interface=wlan1
```

Adresse IP fixe pour une imprimante ou un NVR Débutant

Réserve toujours la même adresse à un appareil (imprimante, enregistreur de caméras) grâce à son adresse MAC.

```
/ip dhcp-server lease add address=192.168.88.20 mac-address=AA:BB:CC:DD:EE:FF server=dhcp-lan comment="NVR
cameras"
```

Important

Trouvez l'adresse MAC dans IP → DHCP Server → Leases.

Ouvrir un port (voir ses caméras à distance) Intermédiaire

Redirige un port Internet vers un appareil du réseau, par exemple l'enregistreur de caméras, pour le consulter depuis l'extérieur.

```
/ip firewall nat add chain=dstnat in-interface-list=WAN protocol=tcp dst-port=8000 action=dst-nat to-addres
ses=192.168.88.20 to-ports=8000 comment="NVR cameras"
```

Important

N'ouvrez que les ports nécessaires et protégez l'appareil par un mot de passe fort. Le VPN est plus sûr.

4 Entreprise

VLAN par service (admin, employés, invités, caméras) Avancé

Sépare le réseau de l'entreprise en 4 réseaux indépendants sur les mêmes câbles : 10 Administration, 20 Employés, 30 Invités, 40 Caméras. ether2 va vers un switch administrable (trunk), ether3 est une prise « employés ».

```
/interface bridge add name=br-ent vlan-filtering=no
/interface bridge port add bridge=br-ent interface=ether2 comment="Trunk vers switch"
/interface bridge port add bridge=br-ent interface=ether3 pvid=20 comment="Prise employes"
/interface bridge vlan add bridge=br-ent vlan-ids=20 tagged=br-ent,ether2 untagged=ether3
/interface bridge vlan add bridge=br-ent vlan-ids=10,30,40 tagged=br-ent,ether2
/interface vlan add name=vlan10-admin interface=br-ent vlan-id=10
/interface vlan add name=vlan20-employees interface=br-ent vlan-id=20
/interface vlan add name=vlan30-invites interface=br-ent vlan-id=30
/interface vlan add name=vlan40-cameras interface=br-ent vlan-id=40
/ip address add address=10.10.10.1/24 interface=vlan10-admin
/ip address add address=10.10.20.1/24 interface=vlan20-employees
/ip address add address=10.10.30.1/24 interface=vlan30-invites
/ip address add address=10.10.40.1/24 interface=vlan40-cameras
/ip pool add name=pool10 ranges=10.10.10.10-10.10.10.250
/ip pool add name=pool20 ranges=10.10.20.10-10.10.20.250
/ip pool add name=pool30 ranges=10.10.30.10-10.10.30.250
/ip pool add name=pool40 ranges=10.10.40.10-10.10.40.250
/ip dhcp-server add name=dhcp10 interface=vlan10-admin address-pool=pool10 disabled=no
/ip dhcp-server add name=dhcp20 interface=vlan20-employees address-pool=pool20 disabled=no
/ip dhcp-server add name=dhcp30 interface=vlan30-invites address-pool=pool30 disabled=no
/ip dhcp-server add name=dhcp40 interface=vlan40-cameras address-pool=pool40 disabled=no
/ip dhcp-server network add address=10.10.10.0/24 gateway=10.10.10.1 dns-server=10.10.10.1
/ip dhcp-server network add address=10.10.20.0/24 gateway=10.10.20.1 dns-server=10.10.20.1
/ip dhcp-server network add address=10.10.30.0/24 gateway=10.10.30.1 dns-server=10.10.30.1
/ip dhcp-server network add address=10.10.40.0/24 gateway=10.10.40.1 dns-server=10.10.40.1
/interface list member add list=LAN interface=vlan10-admin
/interface list member add list=LAN interface=vlan20-employees
/interface list member add list=LAN interface=vlan30-invites
/interface list member add list=LAN interface=vlan40-cameras
# A activer en dernier
/interface bridge set br-ent vlan-filtering=yes
```

Important

Gardez un port hors du bridge (par exemple ether5 avec une adresse IP) pour ne pas perdre l'accès au routeur en activant vlan-filtering. Le switch doit être configuré avec les mêmes VLAN.

Isoler les invités et les caméras Intermédiaire

Les invités ont seulement Internet (pas d'accès aux PC de l'entreprise) et les caméras n'ont pas accès à Internet (protection contre le piratage).

```
/ip firewall filter add chain=forward in-interface=vlan30-invites out-interface-list=!WAN action=drop comment="Invites : Internet seulement"
/ip firewall filter add chain=forward in-interface=vlan40-cameras out-interface-list=WAN action=drop comment="Cameras sans Internet"
```

Important

À utiliser avec le script VLAN. L'administration (VLAN 10) peut toujours consulter les caméras.

Double connexion Internet avec bascule automatique Avancé

Deux fournisseurs d'accès : FAI 1 sur ether1, FAI 2 sur ether2. Si FAI 1 tombe (le routeur ne joint plus 8.8.8.8 par FAI 1), tout bascule automatiquement sur FAI 2, puis revient quand FAI 1 est rétabli.

```
/interface list member add list=WAN interface=ether2
# Routes de test : 8.8.8.8 toujours par FAI 1, 1.1.1.1 toujours par FAI 2
/ip route add dst-address=8.8.8.8/32 gateway=192.168.1.1 scope=10 comment="Test FAI1"
/ip route add dst-address=1.1.1.1/32 gateway=192.168.2.1 scope=10 comment="Test FAI2"
# Routes Internet (distance 1 = principale, 2 = secours)
/ip route add dst-address=0.0.0.0/0 gateway=8.8.8.8 target-scope=11 check-gateway=ping distance=1 comment="FAI1 principal"
/ip route add dst-address=0.0.0.0/0 gateway=1.1.1.1 target-scope=11 check-gateway=ping distance=2 comment="FAI2 secours"
```

Important

Remplacez 192.168.1.1 et 192.168.2.1 par les adresses des deux modèmes. ether2 ne doit pas être dans le bridge du réseau local. Supprimez la route par défaut automatique du client DHCP (add-default-route=no).

Partage de charge sur deux connexions (PCC) Avancé

Utilise les deux connexions en même temps : les connexions des utilisateurs sont réparties à moitié sur chaque fournisseur, avec bascule si l'un tombe.

```
/routing table add name=to_WAN1 fib
/routing table add name=to_WAN2 fib
/ip firewall mangle
add chain=prerouting in-interface=ether1 connection-mark=no-mark action=mark-connection new-connection-mark=WAN1_conn passthrough=yes
add chain=prerouting in-interface=ether2 connection-mark=no-mark action=mark-connection new-connection-mark=WAN2_conn passthrough=yes
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/0 action=mark-connection new-connection-mark=WAN1_conn passthrough=yes
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/1 action=mark-connection new-connection-mark=WAN2_conn passthrough=yes
add chain=prerouting in-interface-list=LAN connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=prerouting in-interface-list=LAN connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
add chain=output connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=output connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1 routing-table=to_WAN1 check-gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=192.168.2.1 routing-table=to_WAN2 check-gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1 distance=1 check-gateway=ping
/ip route add dst-address=0.0.0.0/0 gateway=192.168.2.1 distance=2 check-gateway=ping
```

Important

Désactivez la règle fasttrack du pare-feu, sinon le partage ne fonctionne pas. Ajoutez ether2 à la liste WAN.

Limiter le débit par réseau (QoS) Intermédiaire

Réserve la bande passante : les invités ne peuvent pas saturer la connexion de l'entreprise.
Format : envoi/réception (upload/download).

```
/queue simple add name="Employes" target=10.10.20.0/24 max-limit=20M/50M  
/queue simple add name="Invites" target=10.10.30.0/24 max-limit=5M/10M  
/queue simple add name="Cameras" target=10.10.40.0/24 max-limit=10M/5M
```

Important

Les limites ne s'appliquent pas au trafic accéléré : désactivez la règle fasttrack du pare-feu.

Partage équitable entre tous les utilisateurs (PCQ) Intermédiaire

Chaque appareil reçoit automatiquement une part égale du débit, sans créer une règle par utilisateur. Idéal pour bureaux et résidences.

```
/queue type add name=pcq-down kind=pcq pcq-classifier=dst-address pcq-rate=0  
/queue type add name=pcq-up kind=pcq pcq-classifier=src-address pcq-rate=0  
/queue simple add name="Partage-equitable" target=192.168.88.0/24 queue=pcq-up/pcq-down max-limit=20M/50M
```

Important

pcq-rate=0 partage tout le débit à parts égales. Mettez par exemple pcq-rate=2M pour plafonner chaque appareil à 2 Mbit/s.

Bloquer des sites pendant les heures de travail Intermédiaire

Bloque l'accès à certains sites (réseaux sociaux, streaming) pour les employés, du lundi au vendredi de 8 h à 17 h.

```
/ip firewall filter add chain=forward src-address=10.10.20.0/24 protocol=tcp dst-port=443 tls-host=*facebook.com action=reject reject-with=tcp-reset time=8h-17h,mon,tue,wed,thu,fri comment="Bloquer Facebook" place-before=0  
/ip firewall filter add chain=forward src-address=10.10.20.0/24 protocol=tcp dst-port=443 tls-host=*tiktok.com action=reject reject-with=tcp-reset time=8h-17h,mon,tue,wed,thu,fri comment="Bloquer TikTok" place-before=0
```

5 Hotspot

Créer un hotspot avec l'assistant Débutant

La méthode la plus simple : l'assistant pose les questions (interface, adresses, DNS) et crée tout le hotspot. Avant, retirez du bridge le port ou le Wi-Fi destiné au hotspot.

```
/interface bridge port remove [find interface=ether5]
/ip address add address=172.16.0.1/22 interface=ether5 comment="Hotspot"
# Lancez l'assistant puis repondez aux questions (Entree pour accepter)
/ip hotspot setup
```

Important

Questions de l'assistant : interface = ether5, adresse = 172.16.0.1/22, NAT = yes, plage = 172.16.0.10-172.16.3.250, certificat = none, serveur SMTP = 0.0.0.0, DNS = 8.8.8.8, nom DNS = wifi.globipnet-togo.com, utilisateur local = admin.

Créer un hotspot complet par script Intermédiaire

Même résultat que l'assistant, mais en une seule fois : réseau 172.16.0.0/22 (plus de 1 000 appareils), DHCP, portail de connexion et NAT.

```
/interface bridge port remove [find interface=ether5]
/ip address add address=172.16.0.1/22 interface=ether5 comment="Hotspot"
/ip pool add name=pool-hs ranges=172.16.0.10-172.16.3.250
/ip dhcp-server add name=dhcp-hs interface=ether5 address-pool=pool-hs lease-time=1h disabled=no
/ip dhcp-server network add address=172.16.0.0/22 gateway=172.16.0.1 dns-server=172.16.0.1
/ip hotspot profile add name=hsprof-glob hotspot-address=172.16.0.1 dns-name=wifi.globipnet-togo.com login-by=http-chap,cookie
/ip hotspot add name=hotspot-glob interface=ether5 address-pool=pool-hs profile=hsprof-glob disabled=no
/ip firewall nat add chain=srcnat src-address=172.16.0.0/22 out-interface-list=WAN action=masquerade comment="NAT hotspot"
```

Important

Branchez sur ether5 un point d'accès Wi-Fi en mode bridge (cAP, wAP, etc.) pour couvrir la zone.

Forfaits hotspot (1 heure, 1 jour, 1 semaine, 1 mois) Débutant

Crée les forfaits que vous vendez : durée de connexion, débit (envoi/réception) et nombre d'appareils par ticket.

```
/ip hotspot user profile add name="1H" rate-limit=2M/4M shared-users=1 session-timeout=1h
/ip hotspot user profile add name="1JOUR" rate-limit=2M/4M shared-users=1 session-timeout=1d
/ip hotspot user profile add name="1SEMAINE" rate-limit=3M/6M shared-users=1 session-timeout=7d
/ip hotspot user profile add name="1MOIS" rate-limit=4M/8M shared-users=2 session-timeout=30d
```

Important

La durée compte le temps de connexion à chaque session. Pour limiter le temps total d'un ticket, utilisez limit-uptime sur l'utilisateur (script suivant).

Générer des tickets hotspot automatiquement Intermédiaire

Crée d'un coup 20 tickets aléatoires de 6 caractères pour un forfait, avec une durée totale d'utilisation. Imprimez-les depuis IP → Hotspot → Users.

```
:local nombre 20
:local forfait "1H"
:local duree "1h"
:local car "abcdefghijklmnopqrstuvwxyz23456789"
:for i from=1 to=$nombre do={
  :local code ""
  :for j from=1 to=6 do={
    :set code ($code . [:pick $car [:rndnum from=0 to=([:len $car] - 1)])
  }
  /ip hotspot user add name=$code password=$code profile=$forfait limit-uptime=$duree comment="ticket $forfait"
}
:log info "Tickets crees : $nombre ($forfait)"
```

Important

Changez nombre, forfait et durée en haut du script. Le mot de passe est égal au code pour faciliter la saisie.

Créer un client hotspot avec mot de passe Débutant

Crée un compte nominatif pour un client régulier (résident, employé), avec un forfait.

```
/ip hotspot user add name="koffi" password="koffi2026" profile="1MOIS" comment="Chambre 12"
```

Sites accessibles sans ticket (walled garden) Débutant

Permet d'ouvrir certains sites sans être connecté au hotspot : votre site, le paiement Fedapay, WhatsApp pour vous contacter, etc.

```
/ip hotspot walled-garden add dst-host=*globipnet* comment="Site GLOB.IP.NET"
/ip hotspot walled-garden add dst-host=*fedapay.com comment="Paiement Fedapay"
/ip hotspot walled-garden add dst-host=*.whatsapp.net comment="WhatsApp"
```

Appareils autorisés sans ticket Débutant

Laisse passer sans connexion les appareils de l'établissement : imprimante, caméra, PC de la réception, votre téléphone.

```
/ip hotspot ip-binding add mac-address=AA:BB:CC:DD:EE:FF type=bypassed comment="PC reception"
```

Supprimer automatiquement les tickets épuisés

Intermédiaire

Chaque nuit, supprime les tickets dont le temps est terminé, pour garder une liste propre.

```
/system script add name=nettoyage-tickets source={
  :foreach u in[/ip hotspot user find where comment~"ticket"] do={
    :local lim [/ip hotspot user get $u limit-uptime]
    :local up [/ip hotspot user get $u uptime]
    :if ($lim > 0s && $up >= $lim) do={ /ip hotspot user remove $u }
  }
}
/system scheduler add name=nettoyage-nuit start-time=03:00:00 interval=1d on-event=nettoyage-tickets
```

6 Sécurité

Pare-feu de base (indispensable) Débutant

Protège le routeur et le réseau : accepte les connexions déjà établies, autorise l'administration seulement depuis le réseau local et bloque tout ce qui arrive d'Internet sans avoir été demandé.

```
/ip firewall filter
add chain=input action=accept connection-state=established,related,untracked comment="Connexions etablies"
add chain=input action=drop connection-state=invalid comment="Paquets invalides"
add chain=input action=accept protocol=icmp comment="Ping"
add chain=input action=accept in-interface-list=LAN comment="Administration depuis le LAN"
add chain=input action=drop in-interface-list=!LAN comment="Bloquer le reste vers le routeur"
add chain=forward action=fasttrack-connection connection-state=established,related hw-offload=yes comment="Acceleration"
add chain=forward action=accept connection-state=established,related,untracked
add chain=forward action=drop connection-state=invalid
add chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface-list=WAN comment="Bloquer les entrees non demandees"
```

Important

Si vous gérez le routeur à distance par VPN, ajoutez l'interface VPN à la liste LAN.

Désactiver les services inutiles Débutant

Ferme les portes d'entrée inutiles (telnet, ftp, web non sécurisé...) et limite Winbox au réseau local.

```
/ip service disable telnet,ftp,www,api,api-ssl
/ip service set ssh port=2222
/ip service set winbox address=192.168.88.0/24
/tool mac-server set allowed-interface-list=none
/tool mac-server mac-winbox set allowed-interface-list=LAN
/ip neighbor discovery-settings set discover-interface-list=LAN
/ip dns set allow-remote-requests=yes
```

Bloquer les attaques de mots de passe (SSH / Winbox) Intermédiaire

Une adresse qui tente de se connecter trop souvent est mise sur liste noire pendant 1 jour.

```
/ip firewall filter
add chain=input protocol=tcp dst-port=2222,8291 connection-state=new action=add-src-to-address-list address-list=etape1 address-list-timeout=1m place-before=0
add chain=input protocol=tcp dst-port=2222,8291 connection-state=new src-address-list=etape1 action=add-src-to-address-list address-list=etape2 address-list-timeout=1m place-before=0
add chain=input protocol=tcp dst-port=2222,8291 connection-state=new src-address-list=etape2 action=add-src-to-address-list address-list=liste-noire address-list-timeout=1d place-before=0
add chain=input protocol=tcp dst-port=2222,8291 src-address-list=liste-noire action=drop comment="Liste noire" place-before=0
```

Empêcher l'utilisation du DNS depuis Internet Débutant

Évite que votre routeur serve de relais aux attaques DNS venant d'Internet.

```
/ip firewall filter add chain=input in-interface-list=WAN protocol=udp dst-port=53 action=drop comment="DNS
ferme cote Internet" place-before=0
/ip firewall filter add chain=input in-interface-list=WAN protocol=tcp dst-port=53 action=drop place-before
=0
```

7 VPN

VPN WireGuard (télétravail, accès à distance) Intermédiaire

Le VPN moderne et rapide : depuis l'extérieur, un téléphone ou un PC accède au réseau de l'entreprise comme s'il était sur place.

```
/interface wireguard add name=wg-glob listen-port=13231
/ip address add address=10.99.0.1/24 interface=wg-glob
/interface wireguard peers add interface=wg-glob public-key="CLE_PUBLIQUE_DU_TELEPHONE" allowed-address=10.99.0.2/32 comment="Telephone Stan"
/ip firewall filter add chain=input protocol=udp dst-port=13231 action=accept comment="WireGuard" place-before=0
/interface list member add list=LAN interface=wg-glob
# Afficher la cle publique du routeur a mettre dans l'application
/interface wireguard print
```

Important

Sur le téléphone : application WireGuard, créez un tunnel, mettez la clé publique du routeur, l'adresse Internet du routeur et le port 13231.

VPN L2TP/IPsec (Windows, Android, iPhone sans application) Intermédiaire

Utilise le VPN intégré à Windows et aux téléphones, sans installer d'application.

```
/ip pool add name=pool-vpn ranges=10.88.0.10-10.88.0.50
/ppp profile add name=profil-vpn local-address=10.88.0.1 remote-address=pool-vpn dns-server=10.88.0.1
/ppp secret add name=stan password="MotDePasseVPN2026" service=l2tp profile=profil-vpn
/interface l2tp-server server set enabled=yes default-profile=profil-vpn use-ipsec=required ipsec-secret="CleIPsecPartagee2026"
/ip firewall filter add chain=input protocol=udp dst-port=500,1701,4500 action=accept comment="L2TP/IPsec" place-before=0
/ip firewall filter add chain=input protocol=ipsec-esp action=accept place-before=0
```

Relier deux agences (WireGuard site à site) Avancé

Relie le réseau du siège (192.168.88.0/24) et celui d'une agence (192.168.89.0/24) comme un seul réseau. Script à mettre sur le routeur du siège ; faites l'inverse sur l'agence.

```
/interface wireguard add name=wg-agence listen-port=13232
/ip address add address=10.98.0.1/30 interface=wg-agence
/interface wireguard peers add interface=wg-agence public-key="CLE_PUBLIQUE_AGENCE" endpoint-address=IP_PUBLIQUE_AGENCE endpoint-port=13232 allowed-address=10.98.0.2/32,192.168.89.0/24 persistent-keepalive=25s
/ip route add dst-address=192.168.89.0/24 gateway=wg-agence
/ip firewall filter add chain=input protocol=udp dst-port=13232 action=accept comment="WireGuard agence" place-before=0
/interface list member add list=LAN interface=wg-agence
```

8 Automatisation

Sauvegarde automatique chaque nuit Intermédiaire

Crée chaque nuit à 2 h une sauvegarde complète et un export texte datés.

```
/system script add name=sauvegarde source={
  :local d [/system clock get date]
  /system backup save name=("backup-" . $d) dont-encrypt=yes
  /export file=("export-" . $d)
  :log info "Sauvegarde du $d terminée"
}
/system scheduler add name=sauvegarde-nuit start-time=02:00:00 interval=1d on-event=sauvegarde
```

Important

Pensez à supprimer de temps en temps les anciennes sauvegardes dans Files pour libérer la mémoire.

Surveiller Internet (journal en cas de coupure) Débutant

Teste Internet toutes les 30 secondes et note dans le journal l'heure des coupures et des rétablissements.

```
/tool netwatch add host=8.8.8.8 interval=30s down-script=":log warning \"Internet coupe\"" up-script=":log info \"Internet rétabli\"" comment="Surveillance Internet"
```

Redémarrage automatique chaque semaine Débutant

Redémarre le routeur chaque dimanche à 4 h du matin (utile pour les petits modèles très chargés).

```
/system scheduler add name=reboot-hebdo start-time=04:00:00 interval=7d on-event="/system reboot"
```

Important

Le premier redémarrage a lieu 7 jours après la création : créez la tâche un dimanche.

Couper le Wi-Fi la nuit Intermédiaire

Éteint le Wi-Fi à 23 h et le rallume à 6 h (modèles récents, menu WiFi).

```
/system scheduler add name=wifi-off start-time=23:00:00 interval=1d on-event="/interface wifi disable [find]"
/system scheduler add name=wifi-on start-time=06:00:00 interval=1d on-event="/interface wifi enable [find]"
```

Important

Anciens modèles : remplacez « interface wifi » par « interface wireless ».

9 Dépannage

Commandes de diagnostic Débutant

Les commandes à connaître pour trouver une panne rapidement.

```
# Internet repond-il ?
/ping 8.8.8.8 count=4
/ping google.com count=4
# Par ou passent les paquets ?
/tool traceroute 8.8.8.8
# Debit en temps reel sur le port Internet
/interface monitor-traffic ether1
# Qui consomme le debit ?
/tool torch interface=bridge-lan
# Appareils connectes au reseau
/ip dhcp-server lease print
# Erreurs recentes dans le journal
/log print where topics~"error|critical"
```

Vérifier l'état du routeur Débutant

Processeur, mémoire, température, version et ports actifs.

```
/system resource print
/system health print
/system routerboard print
/interface print stats
/ip address print
/ip route print
```

Pannes fréquentes et solutions Débutant

Pas d'Internet : vérifiez /ip route print (une route 0.0.0.0/0 active), le client DHCP ou PPPoE, puis le NAT masquerade. Les appareils n'ont pas d'adresse : vérifiez le serveur DHCP et que le port est bien dans le bridge. Débit faible : /tool torch pour trouver l'appareil qui consomme, et vérifiez les limites (queues). Winbox ne trouve pas le routeur : câble sur ether2 à ether5, ou connexion par l'adresse MAC dans l'onglet Neighbors.

```
# Verifications rapides dans l'ordre
/ip route print where dst-address=0.0.0.0/0
/ip dhcp-client print
/interface pppoe-client print
/ip firewall nat print
/ip dhcp-server print
/interface bridge port print
```