USER MEETING CAMEROON

YAOUNDE 26 JANVIER 2018

Sécurisez votre routeur MIKROTIK

Presented by :

Aurelien D TCHUMTCHOUA

About Aurelien D TCHUMTCHOUA

CEO of TAD-IT & SERVICES

tad@tadit-services.com

+237 674 369 401 | +237 242 065 143

G Suite Administrator and integrator

Network & Systeme administrator

MCP, MTCNA, Solutions Integrator

"Se réunir est un début ;

rester ensemble est un progrès ;

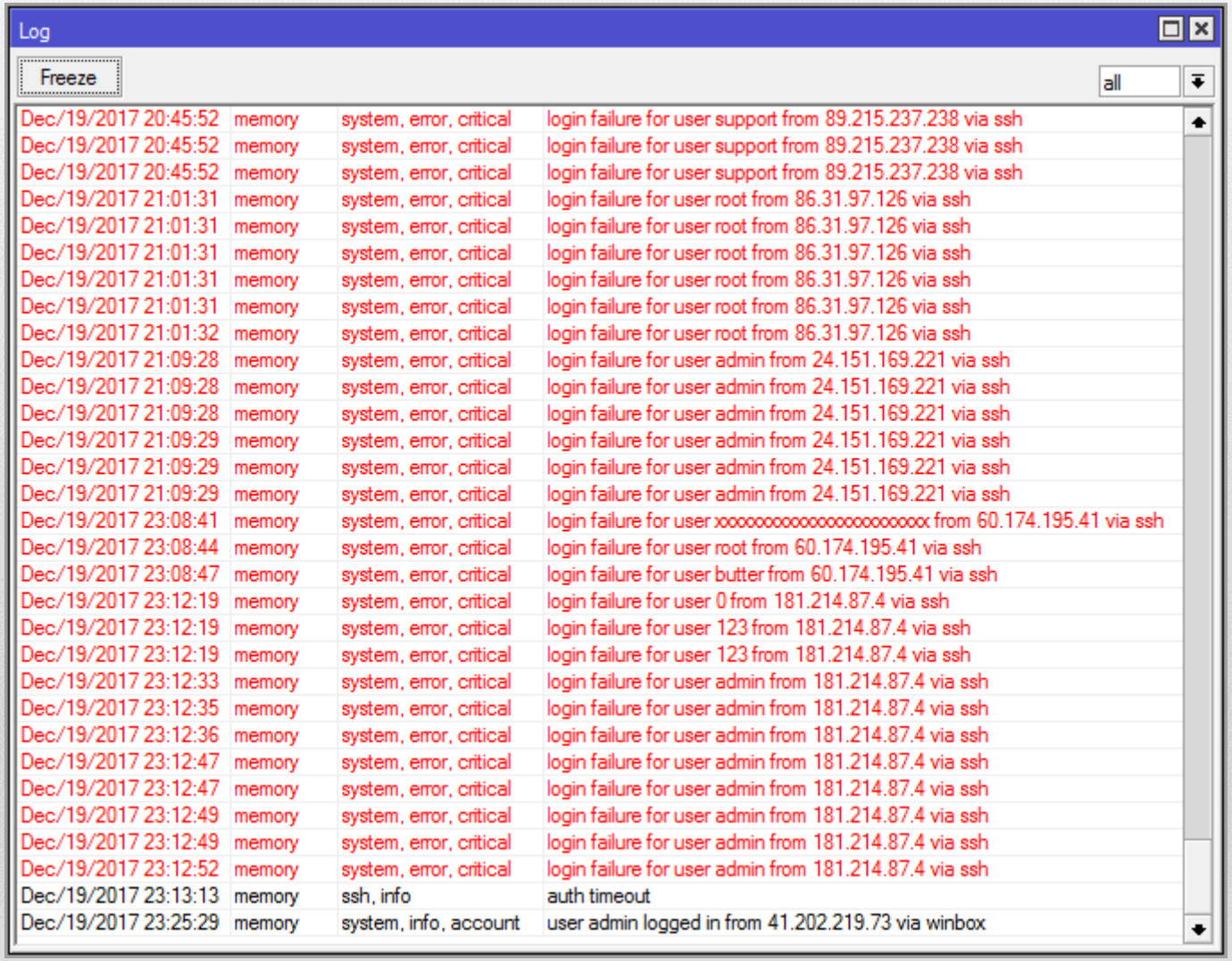
travailler ensemble est la réussite."

Henry Ford

Pourquoi ?

- ✓ Empêcher les personnes non autorisées d'accéder au système
- ✓ L'intrus peut vous voler des informations ou même vous refuser l'accès à vos ressources
- ✓ L'intrus peut utiliser vos ressources pour accéder à d'autre système

Pourquoi ?


Log
Freeze
all
Dec/19/2017 20:45:52 memory system, error, critical login failure for user support from 89.215.237.238 via ssh
Dec/19/2017 20:45:52 memory system, error, critical login failure for user support from 89.215.237.238 via ssh
Dec/19/2017 20:45:52 memory system, error, critical login failure for user support from 89.215.237.238 via ssh
Dec/19/2017 21:01:31 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:01:31 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:01:31 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:01:31 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:01:31 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:01:32 memory system, error, critical login failure for user root from 86.31.97.126 via ssh
Dec/19/2017 21:09:28 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 21:09:28 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 21:09:28 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 21:09:29 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 21:09:29 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 21:09:29 memory system, error, critical login failure for user admin from 24.151.169.221 via ssh
Dec/19/2017 23:08:41 memory system, error, critical login failure for user xxxxxxxxxxxxxxxxxxxxxxxx from 60.174.195.41 via ssh
Dec/19/2017 23:08:44 memory system, error, critical login failure for user root from 60.174.195.41 via ssh
Dec/19/2017 23:08:47 memory system, error, critical login failure for user butter from 60.174.195.41 via ssh
Dec/19/2017 23:12:19 memory system, error, critical login failure for user 0 from 181.214.87.4 via ssh
Dec/19/2017 23:12:19 memory system, error, critical login failure for user 123 from 181.214.87.4 via ssh
Dec/19/2017 23:12:19 memory system, error, critical login failure for user 123 from 181.214.87.4 via ssh
Dec/19/2017 23:12:33 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:35 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:36 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:47 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:47 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:49 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:49 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:12:52 memory system, error, critical login failure for user admin from 181.214.87.4 via ssh
Dec/19/2017 23:13:13 memory ssh, info auth timeout
Dec/19/2017 23:25:29 memory system, info, account user admin logged in from 41.202.219.73 via winbox

Comment ?

- ✓ Garder le routeur à jour
- ✓ Sécuriser l'utilisateur et le mot de passe
- ✓ Sécuriser l'accès physique
- ✓ Configurer les paquets
- ✓ Renforcement des services
- ✓ Paramétrer le pare-feu
- ✓ Journalisation
- ✓ NTP Sync
- ✓ Divers

Garder le routeur à jour

MikroTik

Home About Buy Jobs Hardware Software Support Training Account

Software

Downloads Changelogs Download archive RouterOS The Dude

Upgrading RouterOS

Choose **Bugfix only** version to download the most stable release without new features, just most important fixes. Choose **Current** to have the same fixes including improvements and new features, or choose **Release candidate** for testing the absolute latest builds in test environments.

If you are already running RouterOS, upgrading to the latest version can be done by clicking on "Check For Updates" in QuickSet or System > Packages menu in WebFig or WinBox.

You can find more information about version changes in Changelogs page.

RouterOS

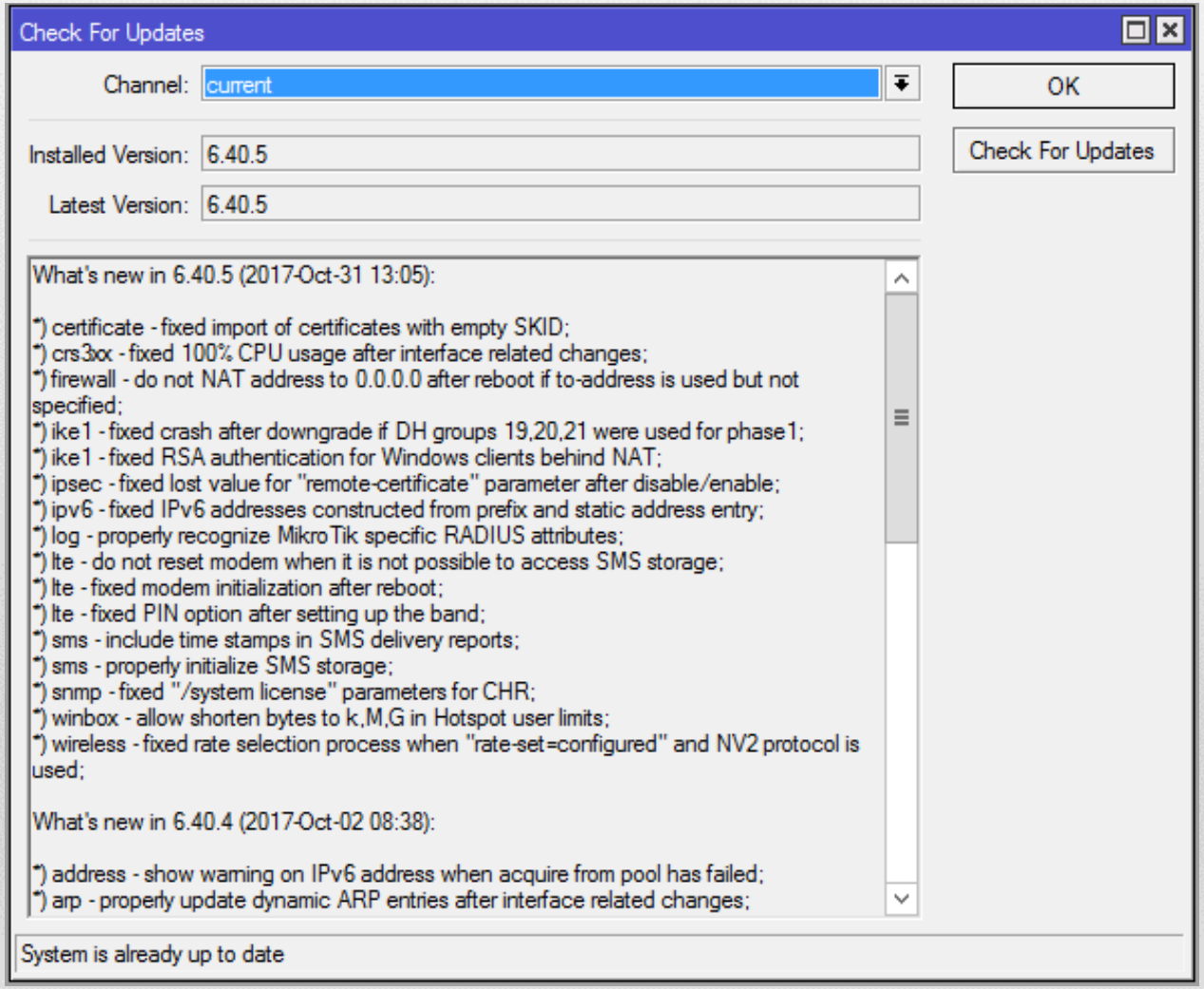
	6.39.3 (Bugfix only)	6.40.5 (Current)	5.26 (Legacy)	6.41rc66 (Release candidate)
MIPSBE	CRS1xx, CRS2xx, DISC, LDF, LHG, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package				
Extra packages				
SMIPS	hAP lite			
Main package			-	
Extra packages			-	

Garder le routeur à jour

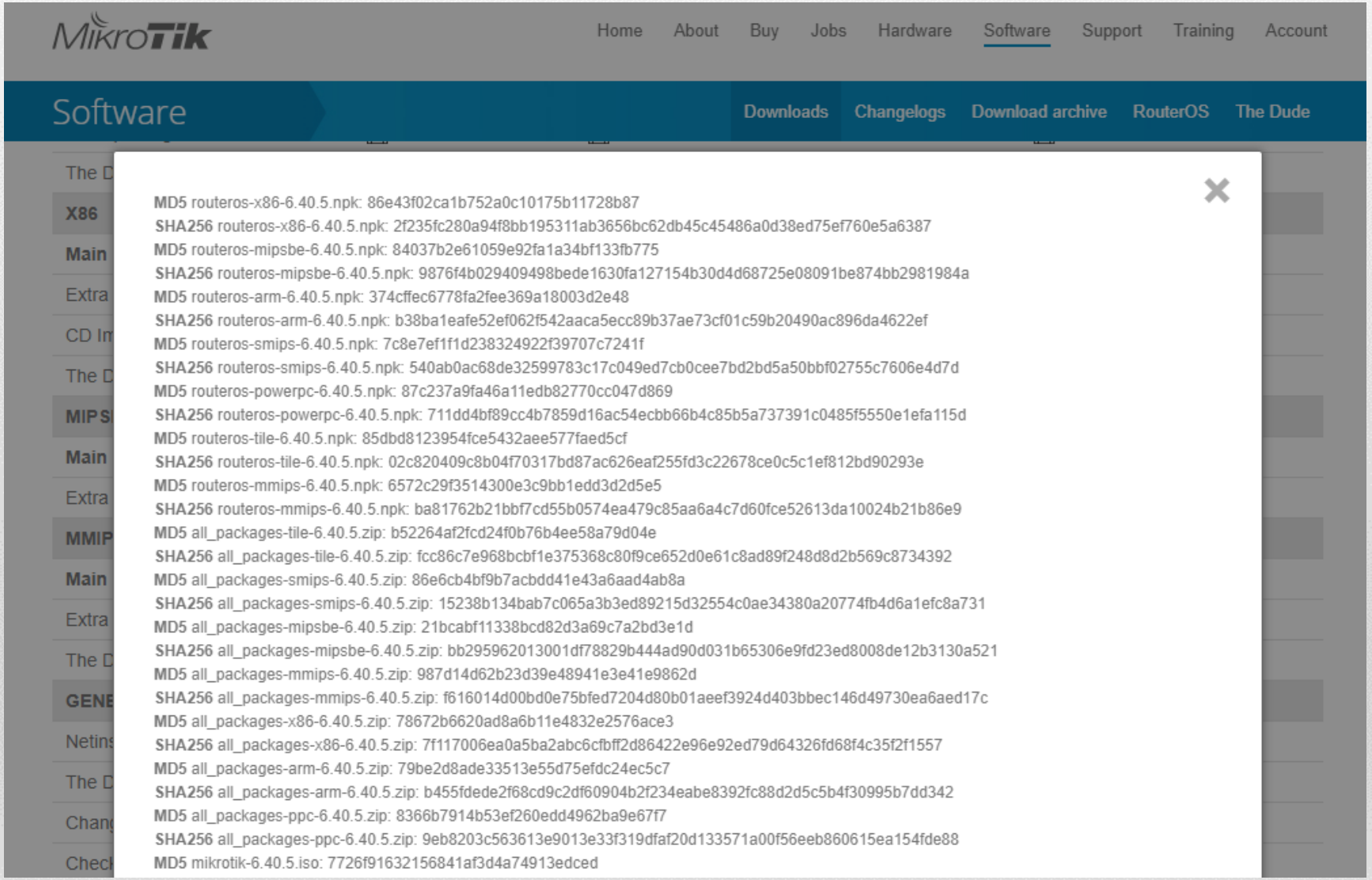
	6.39.3 (Bugfix only)	6.40.5 (Current)	5.26 (Legacy)	6.41rc66 (Release candidate)
MIPSBE	CRS1xx, CRS2xx, DISC, LDF, LHG, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main package	💾	💾	💾	💾
Extra packages	💾	💾	💾	💾
SMIPS	hAP lite			

- ✓ Utiliser la version actuelle
- ✓ Vérifiez le journal des modifications avant la mise à niveau vers une version plus récente
- ✓ Télécharger depuis une source fiable
- ✓ Vérifier le fichier (MD5) lors du téléchargement depuis un site tiers

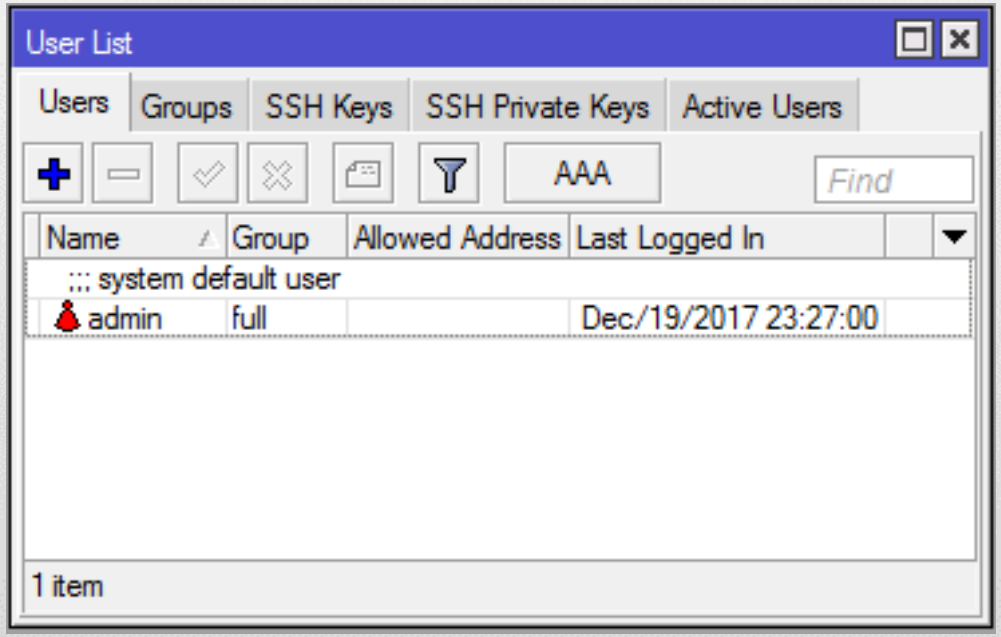
Garder le routeur à jour



Garder le routeur à jour



Sécuriser user ID & password

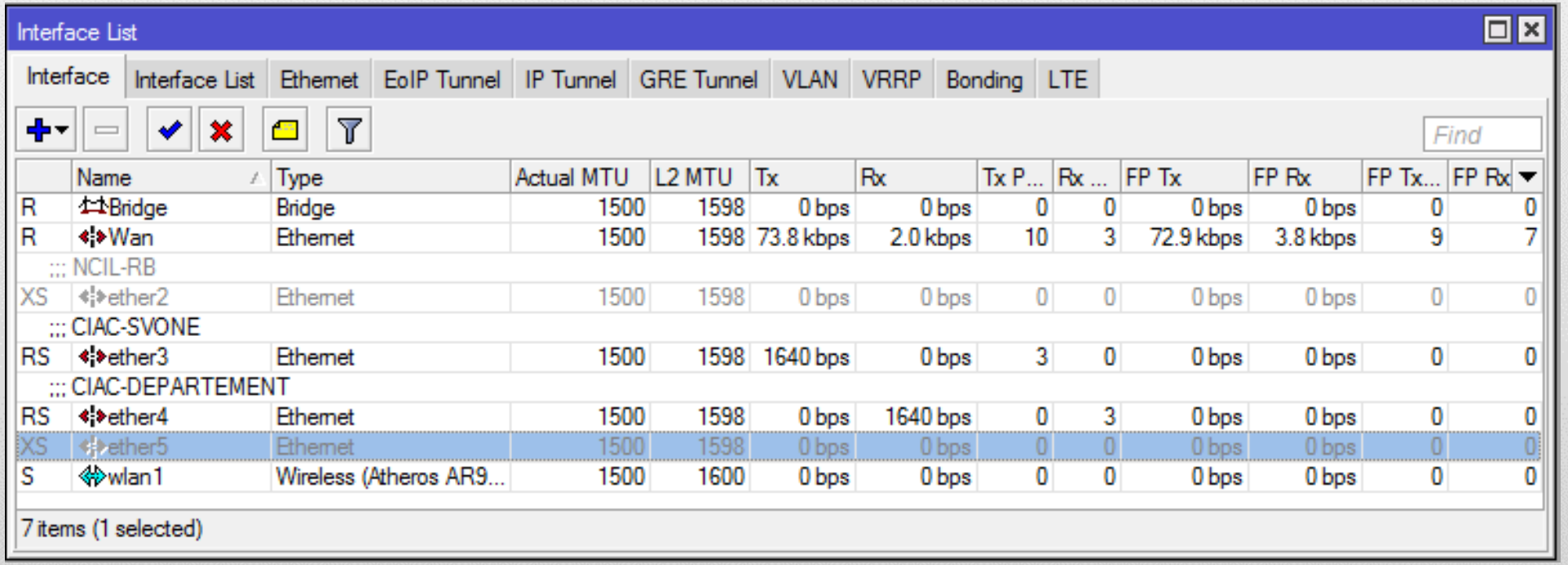


- ✓ Modifier le nom du compte administrateur
- ✓ Définir un mot de passe complexe
- ✓ Créer un compte séparé pour chaque utilisateur
- ✓ Définir l'adresse autorisée
- ✓ Placer un utilisateur en lecture seule dans le groupe "lire"

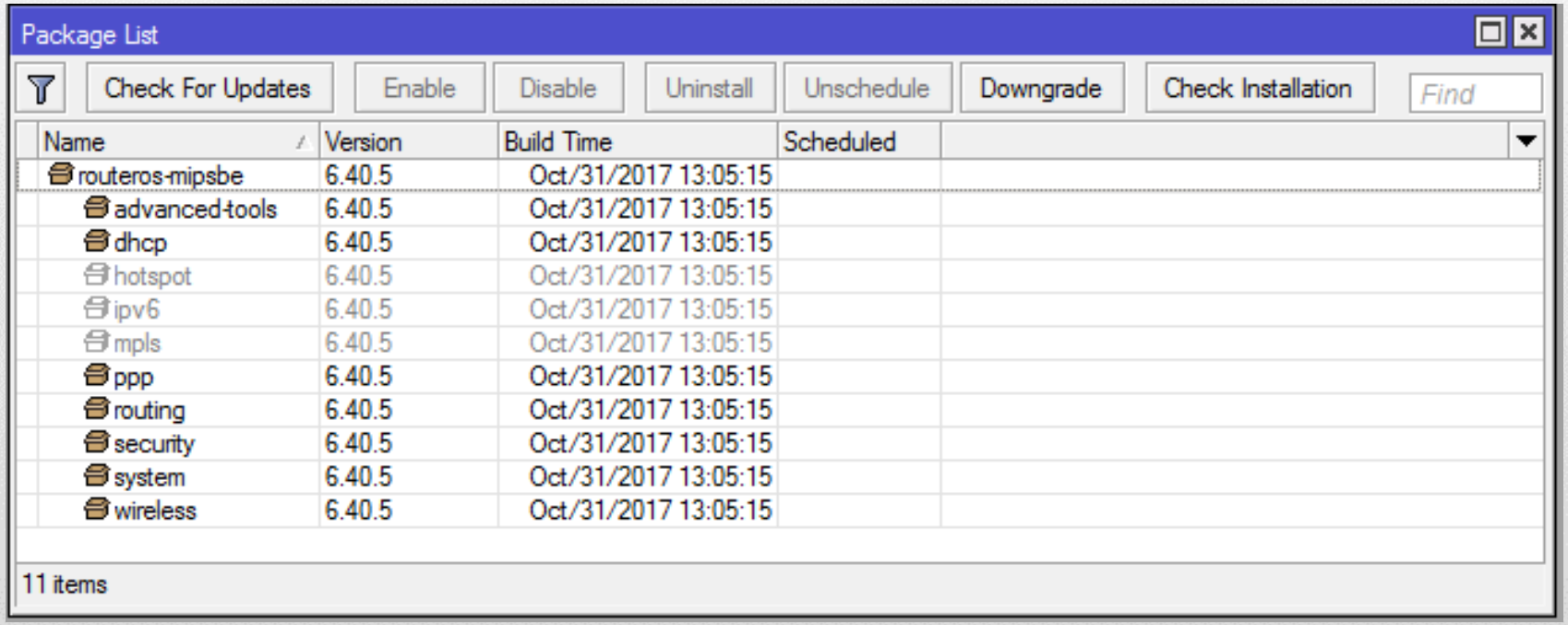
Sécuriser l'accès physique

- ✓ En cas de présente d’un port console, s’il n’est pas utilisé bien vouloir le désactiver (facultatif)
- ✓ Toujours déconnecter sa session console
- ✓ Désactiver les interfaces inutilisées
- ✓ Ne pas configurer les interfaces inutilisées (facultatif)

Sécuriser l'accès physique

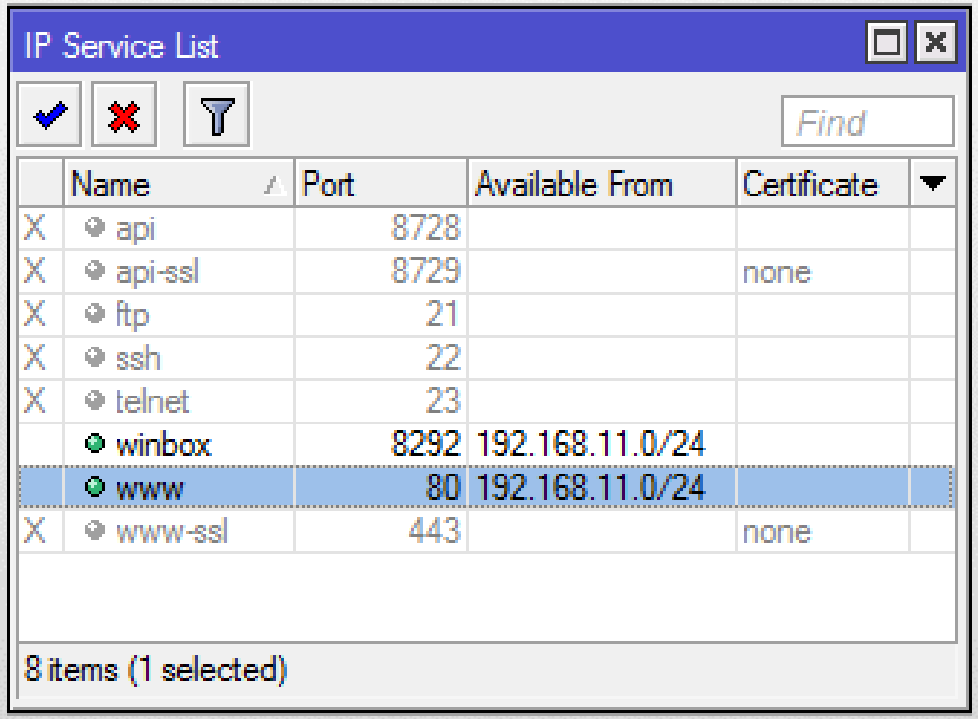


Configuration des paquets



- ✓ Désactiver les packages inutilisés
- ✓ Vérifier les paquets installés
- ✓ Vérifier la version de chaque paquet

Sécurisation des services

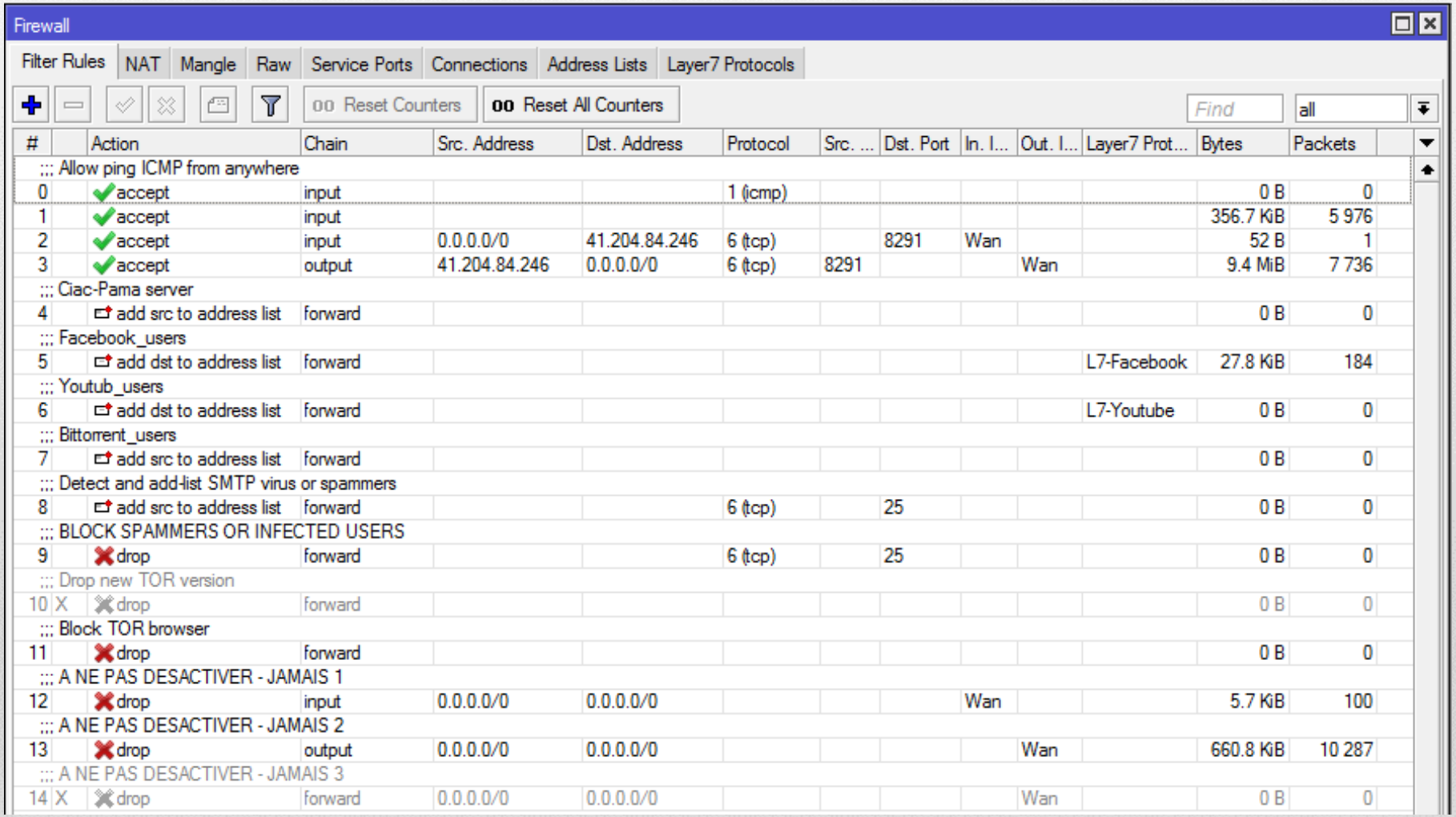


- ✓ Désactiver le service non sécurisé (Ex. Telnet)
- ✓ Changer le port de service (facultatif)
- ✓ Désactiver le service inutilisé
- ✓ Définir des listes d'accès pour chaque service

Paramétrage du pare-feu

- ✓ Le paramétrage du pare-feu ajoute une couche de sécurité
- ✓ Configurer le port knocking (facultatif)

Paramétrage du pare-feu



#		Action	Chain	Src. Address	Dst. Address	Protocol	Src. ...	Dst. Port	In. I...	Out. I...	Layer7 Prot...	Bytes	Packets
;;; Allow ping ICMP from anywhere													
0		accept	input			1 (icmp)						0 B	0
1		accept	input									356.7 KiB	5 976
2		accept	input	0.0.0.0/0	41.204.84.246	6 (tcp)		8291	Wan			52 B	1
3		accept	output	41.204.84.246	0.0.0.0/0	6 (tcp)	8291			Wan		9.4 MiB	7 736
;;; Ciac-Pama server													
4		add src to address list	forward									0 B	0
;;; Facebook_users													
5		add dst to address list	forward								L7-Facebook	27.8 KiB	184
;;; Youtub_users													
6		add dst to address list	forward								L7-Youtube	0 B	0
;;; Bittorrent_users													
7		add src to address list	forward									0 B	0
;;; Detect and add-list SMTP virus or spammers													
8		add src to address list	forward			6 (tcp)		25				0 B	0
;;; BLOCK SPAMMERS OR INFECTED USERS													
9		drop	forward			6 (tcp)		25				0 B	0
;;; Drop new TOR version													
10	X	drop	forward									0 B	0
;;; Block TOR browser													
11		drop	forward									0 B	0
;;; A NE PAS DESACTIVER - JAMAIS 1													
12		drop	input	0.0.0.0/0	0.0.0.0/0				Wan			5.7 KiB	100
;;; A NE PAS DESACTIVER - JAMAIS 2													
13		drop	output	0.0.0.0/0	0.0.0.0/0					Wan		660.8 KiB	10 287
;;; A NE PAS DESACTIVER - JAMAIS 3													
14	X	drop	forward	0.0.0.0/0	0.0.0.0/0					Wan		0 B	0

Paramétrage du pare-feu

Port Knockin process

Hote

Tentative de connexion au routeur avec Wimbox ou telnet ou ssh

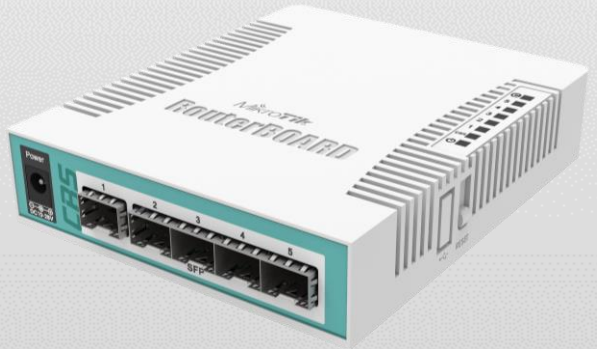
Tentative de connexion rejetée / drop

Knock: tentative de connexion au port prédéfini

Règles de pare-feu modifiées dynamiquement pour autoriser l'accès depuis l'hôte

Tentative de connexion au routeur avec Winbox ou Telnet ou SSH

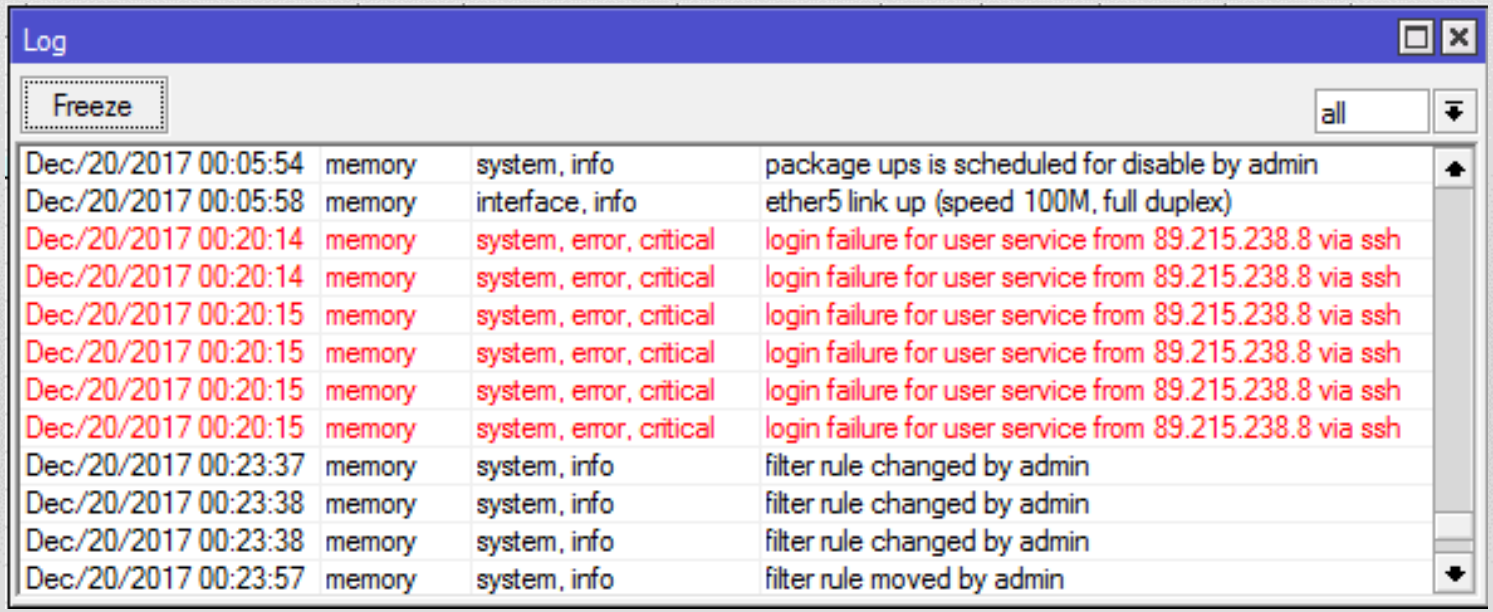
Connexion accordée



Routeur avec parfeu

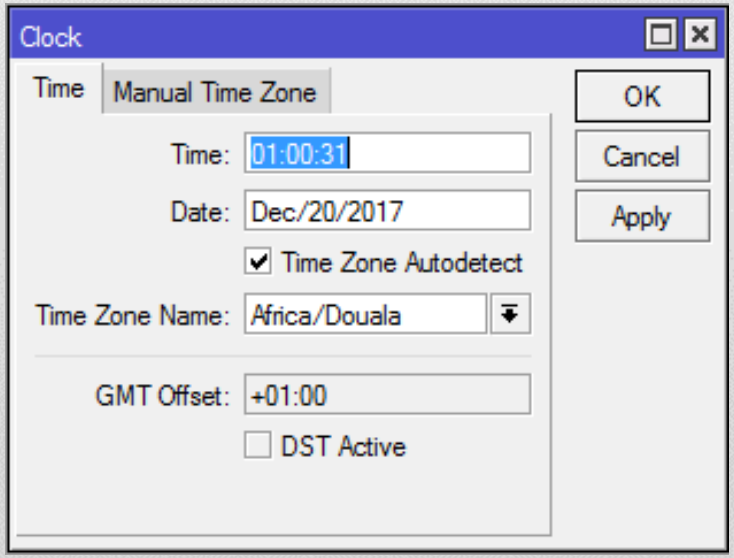
Journalisation

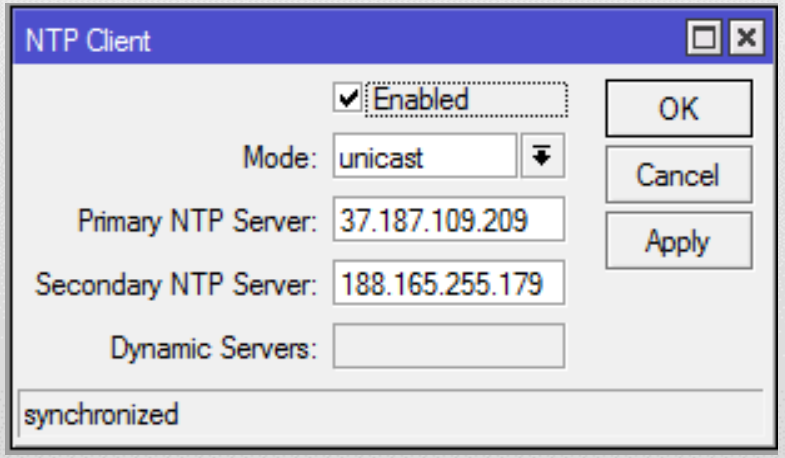
- ✓ Journalisation de la surveillance
- ✓ Sauvegarder sur le disque (journal RouterOS par défaut en mémoire)
- ✓ Transféré le journal vers un serveur syslog

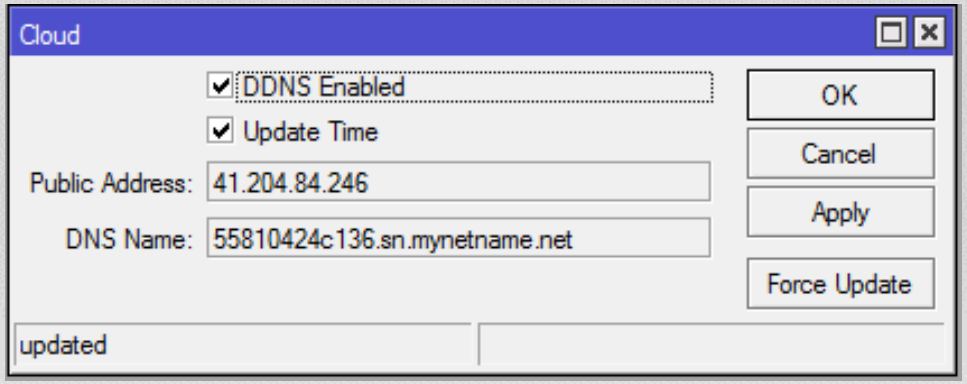


NTP Sync

- ✓ Définir le fuseau horaire
- ✓ Synchroniser l'heure avec un serveur NTP ou le service de IP cloud







Autres

- ✓ Bail DHCP statique
- ✓ Sécurité Wi-Fi
- ✓ Sauvegardé la configuration avec un mot de passe crypté
- ✓ Bloquer la découverte Winbox
- ✓ Désactiver la découverte du voisinage de réseau


?
Questions

L'Entreprise

TAD-IT & SERVICES est une entreprise de conseils et de services dédiée aux nouvelles technologies de l'information. Notre objectif est de satisfaire les clients que nous accompagnions et d'établir avec eux un partenariat à long terme.

Nous intervenons principalement sur tous les secteurs d'activité de l'économie et nous œuvrons dans l'accompagnement de nos clients sur les axes suivants :

- ✓ Infrastructure réseau et systèmes
- ✓ Intégration des solutions d'entreprise
- ✓ Métiers du digital
- ✓ Infogérance

Merci !

TAD-IT & SERVICES

info@tadit-services.com

+237 242 065 143

+237 677 217 368

Facebook/taditservices

Linkedin.com/company/tad-it-&-services

plus.google.com/+Tadit-services