



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





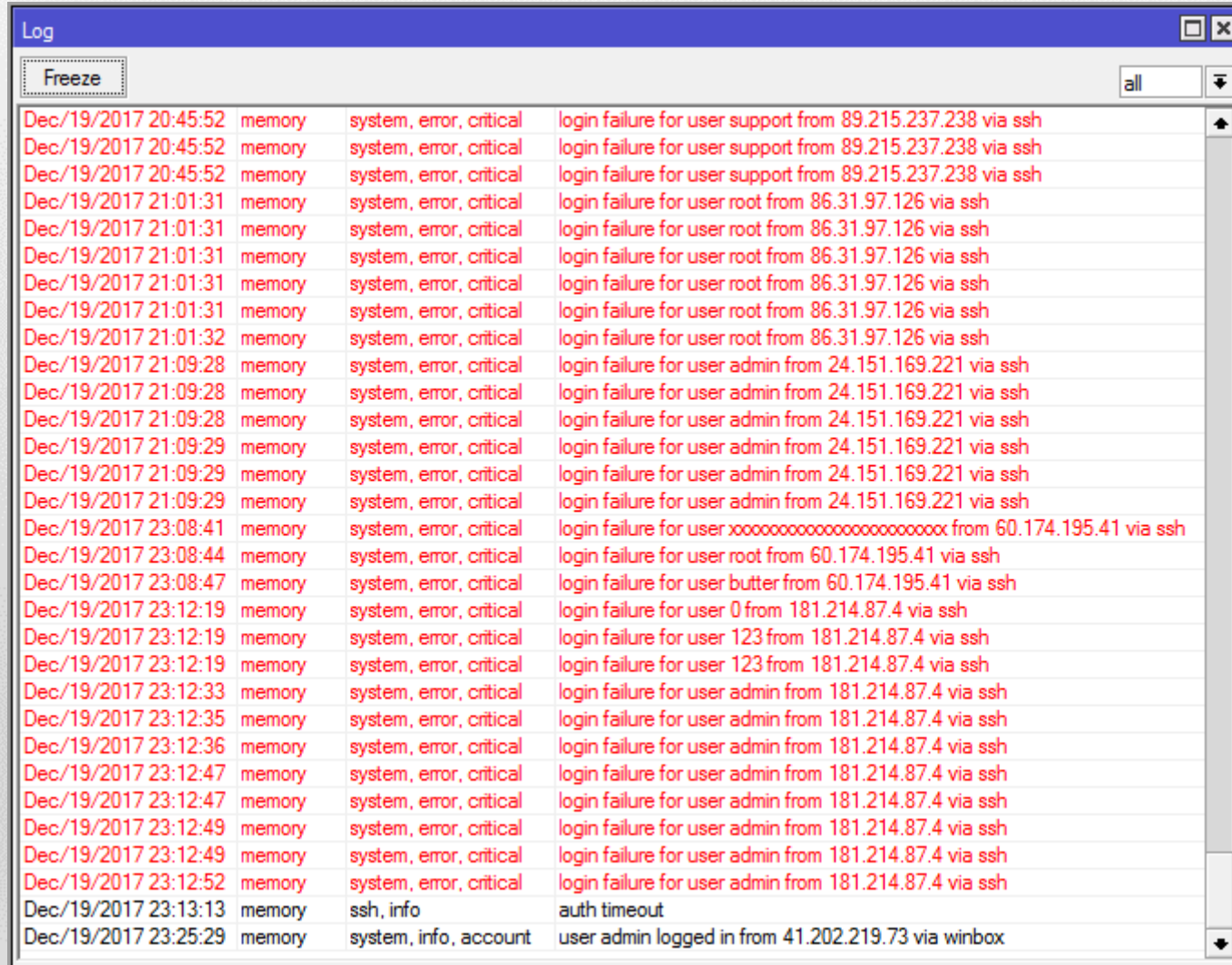
"Se réunir est un début ;
rester ensemble est un progrès ;
travailler ensemble est la réussite."

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 ?



The screenshot shows a Windows Log window titled "Log" with a "Freeze" button and a filter set to "all". The log entries are as follows:

Time	Source	Category	Message
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 21:01:31	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

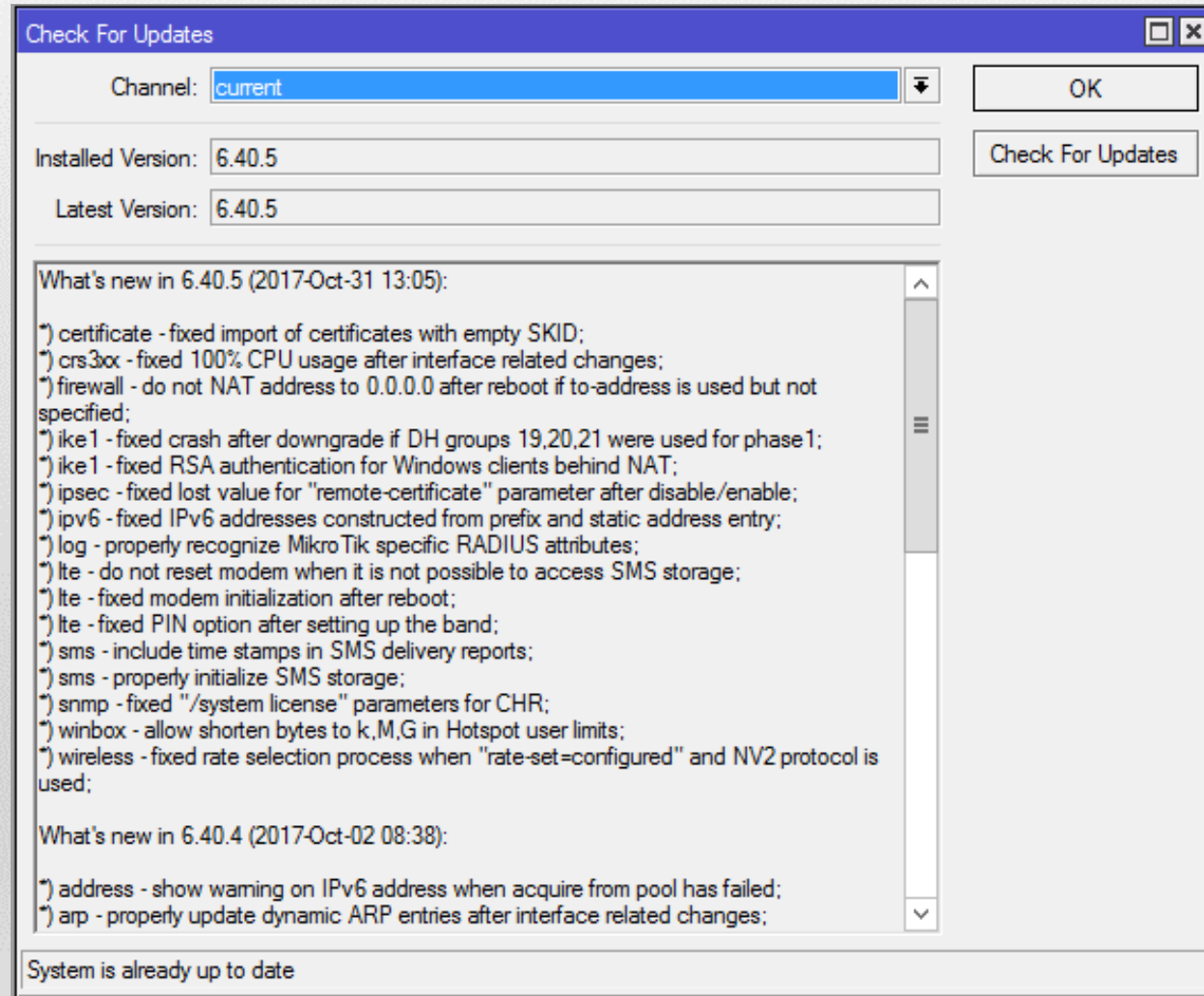
	6.39.3 (Bugfix only)	6.40.5 (Current)	5.26 (Legacy)	6.41rc66 (Release candidate)
MIPSBE	CRS1xx, CRS2xx, DISC, LDF, LHG, NetBox, NetMetal, PowerBox, QRT, RB9xx, hAP, hAP ac, hAP ac lite, mANTBox, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx			
Main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

The screenshot shows the MikroTik website's 'Software' section. A modal window is open, displaying a list of download links for various MikroTik router models and architectures. The links are organized by architecture (X86, MIPS, MMIP) and then by specific model or package type (MD5, SHA256). The list includes links for routers like x86, mipsbe, arm, smips, powerpc, tile, mmips, and all_packages, along with their respective MD5 and SHA256 hashes.

MikroTik Home About Buy Jobs Hardware Software Support Training Account

Software Downloads Changelogs Download archive RouterOS The Dude

The D X86 MD5 routers-x86-6.40.5.npk: 86e43f02ca1b752a0c10175b11728b87
SHA256 routers-x86-6.40.5.npk: 2f235fc280a94f8bb195311ab3656bc62db45c45486a0d38ed75ef760e5a6387

Main MD5 routers-mipsbe-6.40.5.npk: 84037b2e61059e92fa1a34bf133fb775
SHA256 routers-mipsbe-6.40.5.npk: 9876f4b029409498bede1630fa127154b30d4d68725e08091be874bb2981984a

Extra MD5 routers-arm-6.40.5.npk: 374cffe6778fa2fee369a18003d2e48
SHA256 routers-arm-6.40.5.npk: b38ba1eafe52ef062f542aaca5ecc89b37ae73cf01c59b20490ac896da4622ef

CD Im MD5 routers-smips-6.40.5.npk: 7c8e7ef1f1d238324922f39707c7241f
SHA256 routers-smips-6.40.5.npk: 540ab0ac68de32599783c17c049ed7cb0cee7bd2bd5a50bbf02755c7606e4d7d

The D MD5 routers-powerpc-6.40.5.npk: 87c237a9fa46a11edb82770cc047d869
SHA256 routers-powerpc-6.40.5.npk: 711dd4bf89cc4b7859d16ac54ecbb66b4c85b5a737391c0485f5550e1efa115d

MIPS MD5 routers-tile-6.40.5.npk: 85dbd8123954fce5432aee577faed5cf
SHA256 routers-tile-6.40.5.npk: 02c820409c8b04f70317bd87ac626eaf255fd3c22678ce0c5c1ef812bd90293e

Main MD5 routers-mmips-6.40.5.npk: 6572c29f3514300e3c9bb1edd3d2d5e5
SHA256 routers-mmips-6.40.5.npk: ba81762b21bbf7cd55b0574ea479c85aa6a4c7d60fce52613da10024b21b86e9

Extra MD5 all_packages-tile-6.40.5.zip: b52264af2fcd24f0b76b4ee58a79d04e
SHA256 all_packages-tile-6.40.5.zip: fcc86c7e968bcfb1e375368c80f9ce652d0e61c8ad89f248d8d2b569c8734392

MMIP MD5 all_packages-smips-6.40.5.zip: 86e6cb4bf9b7acb41e43a6aad4ab8a
SHA256 all_packages-smips-6.40.5.zip: 15238b134bab7c065a3b3ed89215d32554c0ae34380a20774fb4d6a1efc8a731

Main MD5 all_packages-mipsbe-6.40.5.zip: 21bcabf11338bcd82d3a69c7a2bd3e1d
SHA256 all_packages-mipsbe-6.40.5.zip: bb295962013001df78829b444ad90d031b65306e9fd23ed8008de12b3130a521

Extra MD5 all_packages-mmips-6.40.5.zip: 987d14d62b23d39e48941e3e41e9862d
SHA256 all_packages-mmips-6.40.5.zip: f616014d00bd0e75bfed7204d80b01aee3924d403bbec146d49730ea6aed17c

The D MD5 all_packages-x86-6.40.5.zip: 78672b6620ad8a6b11e4832e2576ace3
SHA256 all_packages-x86-6.40.5.zip: 7f117006ea0a5ba2abc6cbbf2d86422e96e92ed79d64326fd68f4c35f2f11557

GENE MD5 all_packages-arm-6.40.5.zip: 79be2d8ade33513e55d75efdc24ec5c7
SHA256 all_packages-arm-6.40.5.zip: b455fdede2f68cd9c2df60904b2f234eabe8392fc88d2d5c5b4f30995b7dd342

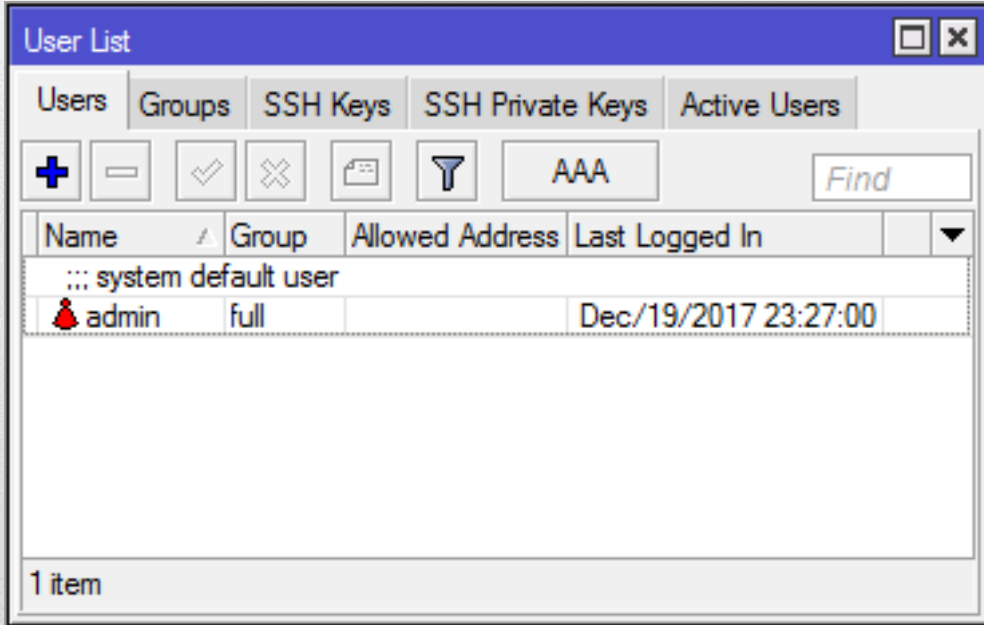
Netins MD5 all_packages-ppc-6.40.5.zip: 8366b7914b53ef260edd4962ba9e67f7
SHA256 all_packages-ppc-6.40.5.zip: 9eb8203c563613e9013e33f319dfaf20d133571a00f56eeb860615ea154fde88

The D MD5 mikrotik-6.40.5.iso: 7726f91632156841af3d4a74913edced

Chang MD5 mikrotik-6.40.5.iso: 7726f91632156841af3d4a74913edced

Check MD5 mikrotik-6.40.5.iso: 7726f91632156841af3d4a74913edced

Sécuriser user ID & password

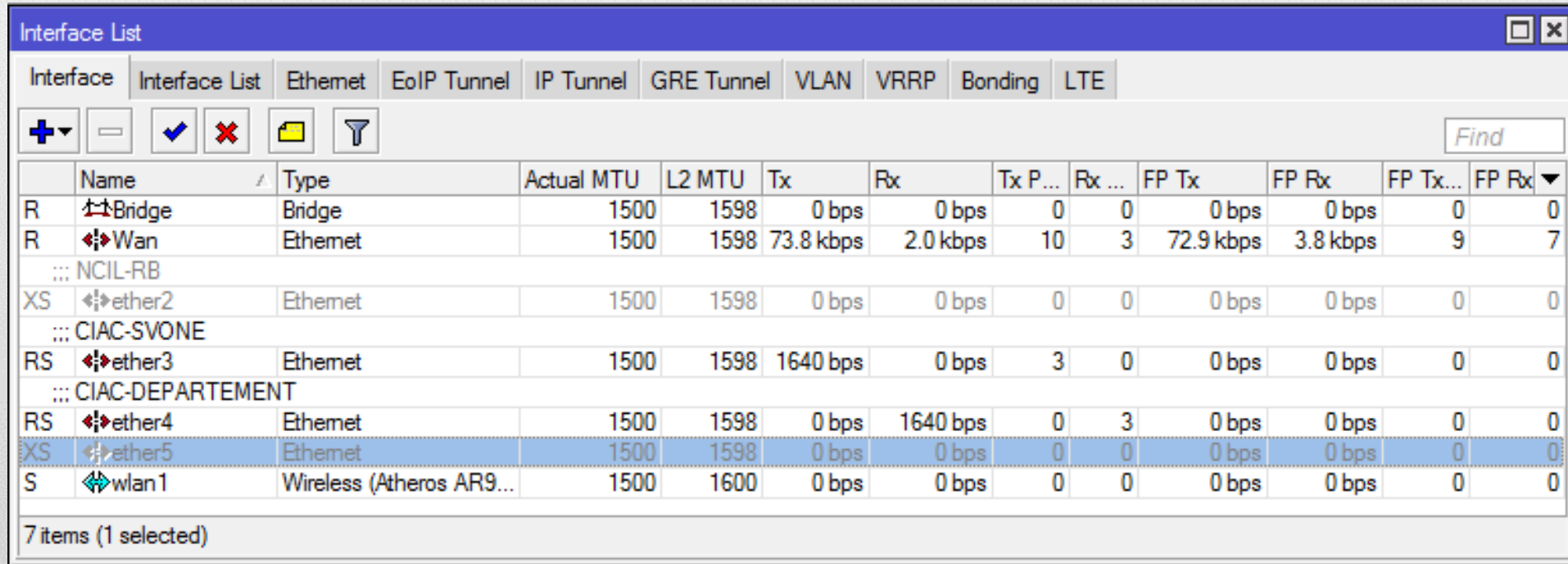


- ✓ Modifier le nom du compte administrateur
- ✓ Définir un mot de passe complexe
- ✓ Créer un compte séparé pour chaque utilisateur
- ✓ Définir l'adresse autorisée
- ✓ Placer un utilisateur en lecture seule dans le groupe "lire"

Sécuriser l'accès physique

- ✓ En cas de présence 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)

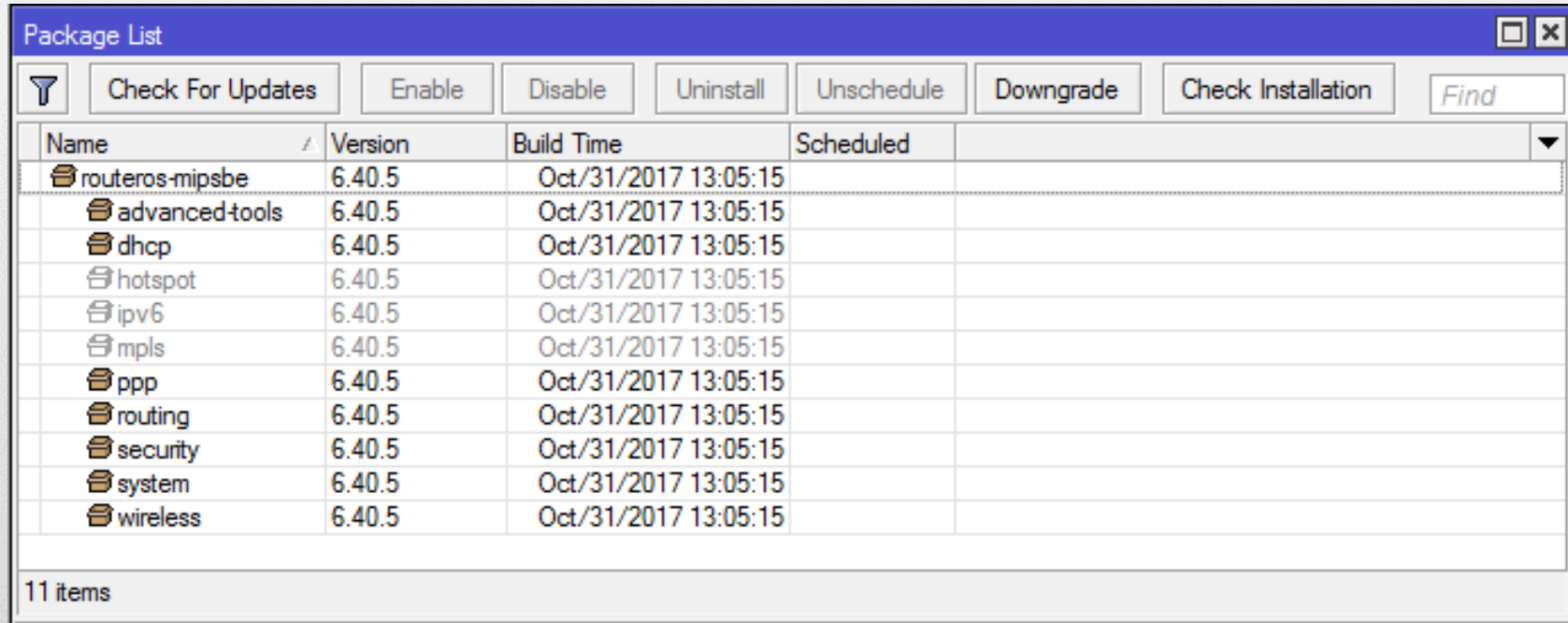
Sécuriser l'accès physique



The screenshot shows the 'Interface List' window in Mikrotik WinBox. The window has a blue title bar and a menu bar with options: Interface, Interface List, Ethernet, EoIP Tunnel, IP Tunnel, GRE Tunnel, VLAN, VRRP, Bonding, and LTE. Below the menu bar are several icons: a plus sign, a minus sign, a checkmark, a red X, a yellow folder, and a funnel. A search box labeled 'Find' is on the right. The main area contains a table with the following columns: Name, Type, Actual MTU, L2 MTU, Tx, Rx, Tx P..., Rx ..., FP Tx, FP Rx, FP Tx..., and FP Rx. The table lists several interfaces, with 'ether5' selected (highlighted in blue). At the bottom, it says '7 items (1 selected)'.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx P...	Rx ...	FP Tx	FP Rx	FP Tx...	FP Rx
R	Bridge	Bridge	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
R	Wan	Ethernet	1500	1598	73.8 kbps	2.0 kbps	10	3	72.9 kbps	3.8 kbps	9	7
::: NCIL-RB												
XS	ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
::: CIAC-SVONE												
RS	ether3	Ethernet	1500	1598	1640 bps	0 bps	3	0	0 bps	0 bps	0	0
::: CIAC-DEPARTEMENT												
RS	ether4	Ethernet	1500	1598	0 bps	1640 bps	0	3	0 bps	0 bps	0	0
XS	ether5	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
S	wlan1	Wireless (Atheros AR9...	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0

Configuration des paquets



The screenshot shows a window titled "Package List" with a toolbar containing buttons for "Check For Updates", "Enable", "Disable", "Uninstall", "Unschedule", "Downgrade", "Check Installation", and a "Find" search box. Below the toolbar is a table with the following columns: Name, Version, Build Time, and Scheduled. The table lists 11 packages, all with version 6.40.5 and build time Oct/31/2017 13:05:15. The packages are: routeros-mipsbe, advanced-tools, dhcp, hotspot, ipv6, mpls, ppp, routing, security, system, and wireless. A status bar at the bottom left indicates "11 items".

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.40.5	Oct/31/2017 13:05:15	
advanced-tools	6.40.5	Oct/31/2017 13:05:15	
dhcp	6.40.5	Oct/31/2017 13:05:15	
hotspot	6.40.5	Oct/31/2017 13:05:15	
ipv6	6.40.5	Oct/31/2017 13:05:15	
mpls	6.40.5	Oct/31/2017 13:05:15	
ppp	6.40.5	Oct/31/2017 13:05:15	
routing	6.40.5	Oct/31/2017 13:05:15	
security	6.40.5	Oct/31/2017 13:05:15	
system	6.40.5	Oct/31/2017 13:05:15	
wireless	6.40.5	Oct/31/2017 13:05:15	

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

Sécurisation des services

	Name	Port	Available From	Certificate	
X	api	8728			
X	api-ssl	8729		none	
X	ftp	21			
X	ssh	22			
X	telnet	23			
	winbox	8292	192.168.11.0/24		
	www	80	192.168.11.0/24		
X	www-ssl	443		none	

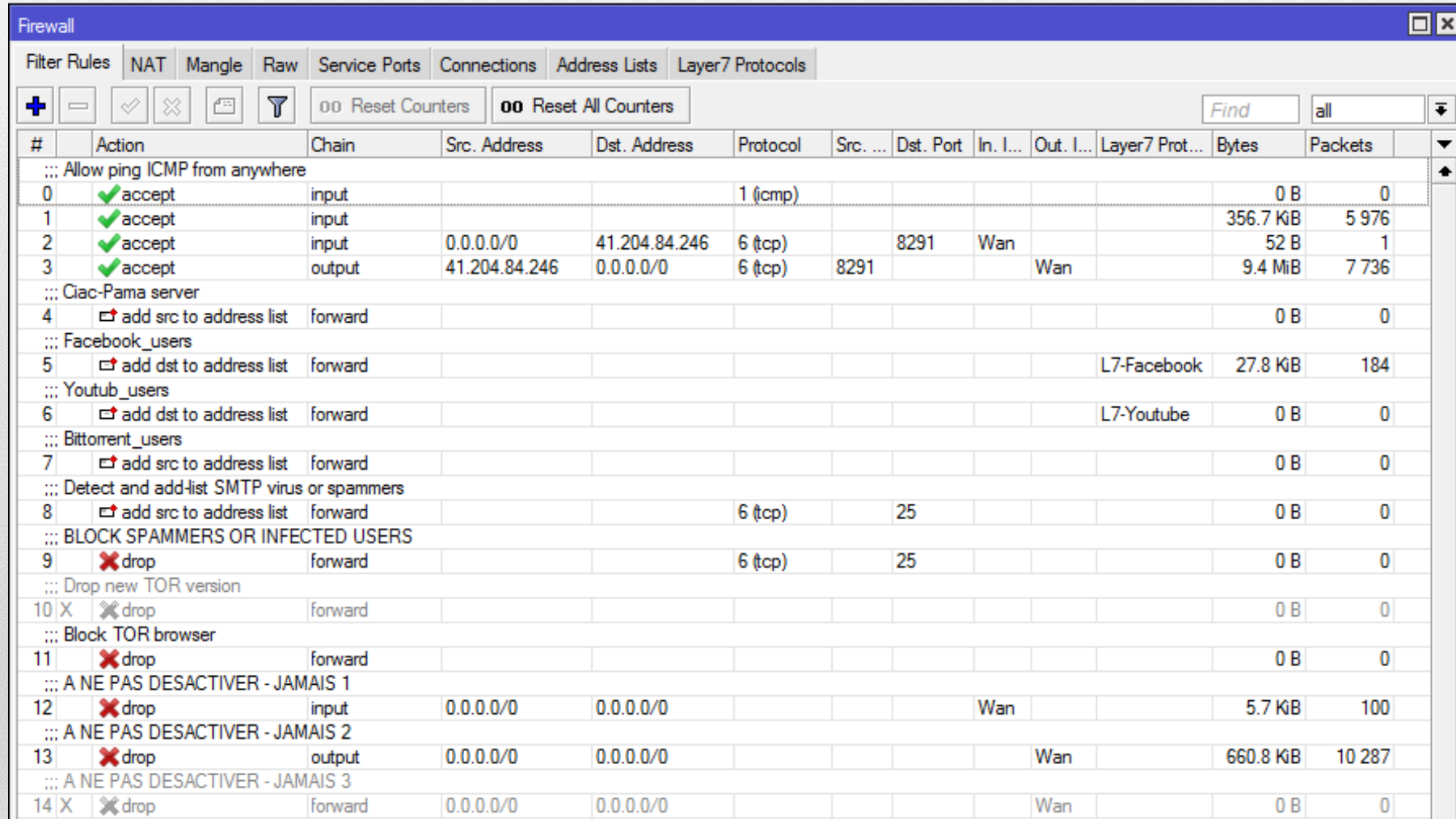
8 items (1 selected)

- ✓ 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



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The window title is "Firewall". The tabs at the top are "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Filter Rules" tab is active. Below the tabs, there are icons for adding, deleting, enabling, disabling, and refreshing rules, along with "Reset Counters" and "Reset All Counters" buttons. A search bar contains the text "Find" and "all".

#	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 KB	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 KB	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 KB	100
::: A NE PAS DESACTIVER - JAMAIS 2												
13	✗ drop	output	0.0.0.0/0	0.0.0.0/0					Wan		660.8 KB	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



Hôte

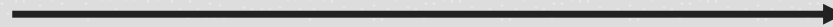
Tentative de connexion au routeur avec
Winbox ou telnet ou ssh



Tentative de connexion rejetée / drop



Knock: tentative de connexion au port prédéfini

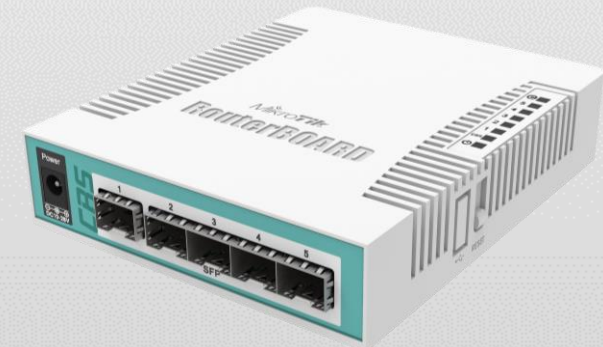


Règles de pare-feu modifiées dynamiquement
pour autoriser l'accès depuis l'hôte

Tentative de connexion au routeur avec Winbox
ou Telnet ou SSH



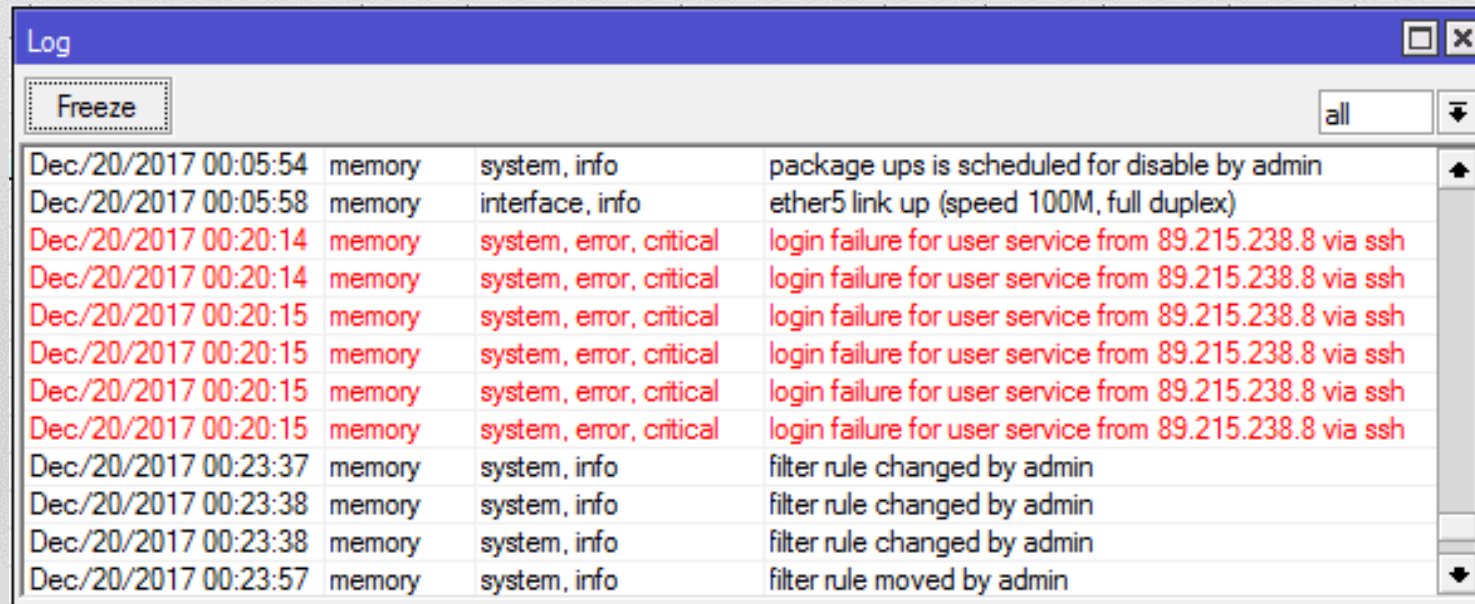
Connexion accordée



Routeur avec
pare-feu

Journalisation

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

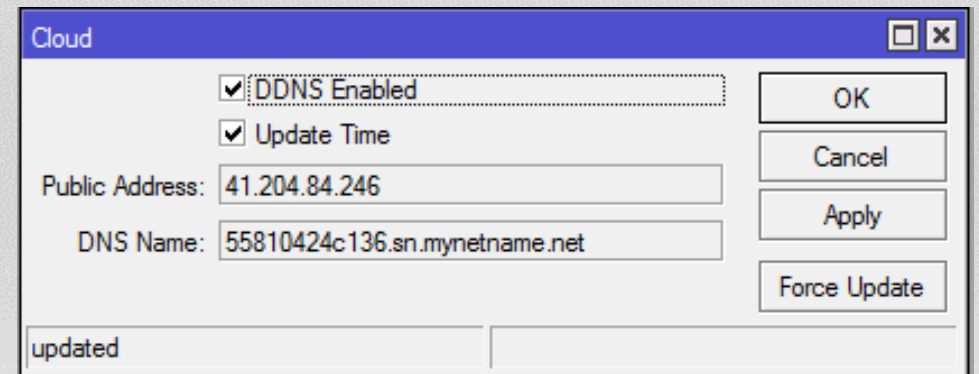
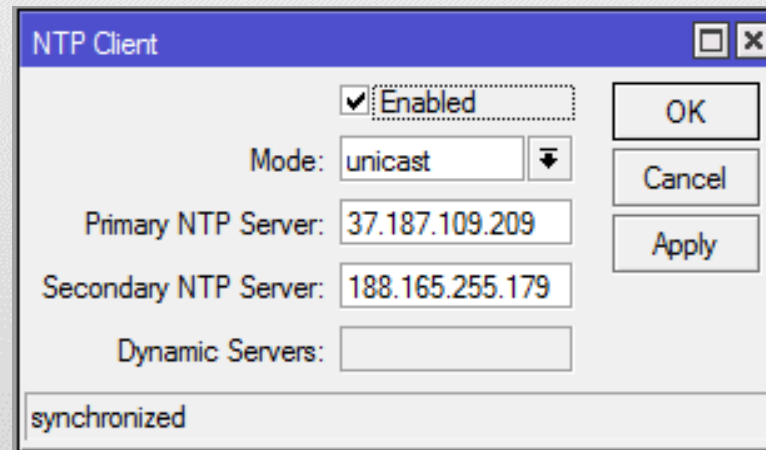
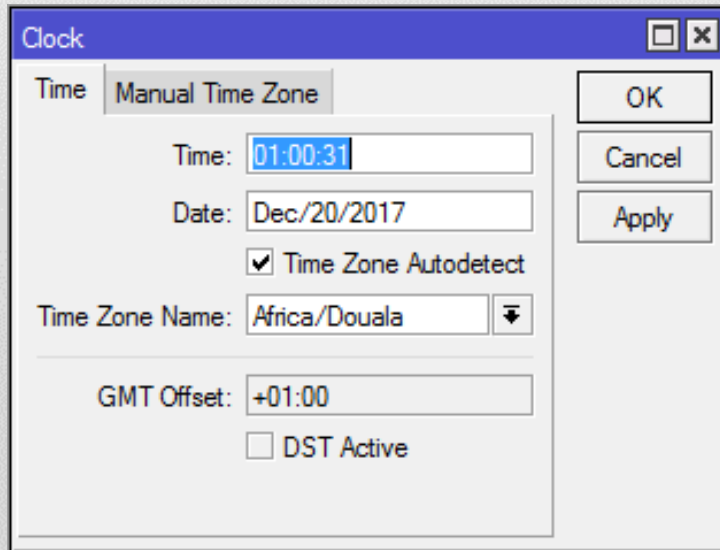


The screenshot shows a 'Log' window with a 'Freeze' button and a filter set to 'all'. The log entries are as follows:

Timestamp	Component	Severity	Message
Dec/20/2017 00:05:54	memory	system, info	package ups is scheduled for disable by admin
Dec/20/2017 00:05:58	memory	interface, info	ether5 link up (speed 100M, full duplex)
Dec/20/2017 00:20:14	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:20:14	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:20:15	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:20:15	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:20:15	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:20:15	memory	system, error, critical	login failure for user service from 89.215.238.8 via ssh
Dec/20/2017 00:23:37	memory	system, info	filter rule changed by admin
Dec/20/2017 00:23:38	memory	system, info	filter rule changed by admin
Dec/20/2017 00:23:38	memory	system, info	filter rule changed by admin
Dec/20/2017 00:23:57	memory	system, info	filter rule moved by admin

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



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 accompagnons 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](https://www.facebook.com/taditservices)

[Linkedin.com/company/tad-it-&-services](https://www.linkedin.com/company/tad-it-&-services)

plus.google.com/+Tadit-services