

Laboratoare Administarea Retelelor de Calculatoare

Securizarea routerului.



Securizarea SSH-ului pentru userul local

- In laboratorul anterior cand am facut serverul de Radius am activat conectarea userului la router, dar ramane un user care nu poate fi sters sau dezactivat (userul admin).
- Pentru acesta si in cazul altor useri locali vom face conexiunea prin ssh doar pe baza certificatelor digitale.
- Incepem prin generarea acestora cu comanda: ssh-keygen
- Recomand in productie sa se paroleze cheia pentru a nu putea fi citita de persoane terte.
- Dupa ce am generat cheia publica o vom importa in router fie prin winbox file manager fie prin ftp.
- Accesand System→Users → SSH Keys o vom imprta.
- Putem incerca conexiunea prin ssh specificand argumentul “-i” si calea catre cheia privata.
- Incercand sa ne conectam cu parola putem observa ca nu putem.

```
abaddon@abaddon in ~/.ssh took 4s
λ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/abaddon/.ssh/id_rsa): admin_mikrotik
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in admin_mikrotik
Your public key has been saved in admin_mikrotik.pub
The key fingerprint is:
SHA256:rRFzFrXK5HgoXs27cmcBucxNw0qcgfq0/B176ijbF+U abaddon@abaddon-82ey
The key's randomart image is:
```

```
+--[RSA 3072]--+
|
|  .  .
|  +  ..
|  . 0ooo.
|  o * O*+
|  o = BSX.
|  . o + BoE
|  + . oo .
|  =..o+o+
|  .++==
+--[SHA256]--+
```

User List		
Users Groups SSH Keys SSH Private Keys Active Users		
Import SSH Key Find		
User	Key Owner	
admin	abaddon@abaddon-82ey	

```
abaddon@abaddon in ~/.ssh took 1ms
λ ssh -i admin_mikrotik admin@192.168.122.60
```

```
MMM      MMM      KKK      TTTTTT
MMMM     MMMM     KKK      TTTTTT
MMM MMMM MMM III  KKK KKK  RRRRRR  000000  TTT
MMM MM  MMM III  KKKKK  RRR  RRR  000 000  TTT
MMM     MMM III  KKK KKK  RRRRRR  000 000  TTT
MMM     MMM III  KKK KKK  RRR  RRR  000000  TTT
```

MikroTik RouterOS 7.8 (c) 1999-2023 <https://www.mikrotik.com>

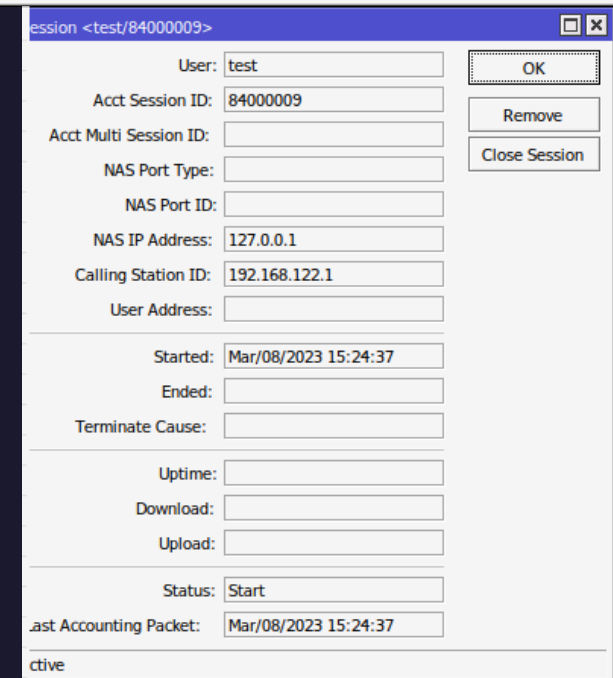
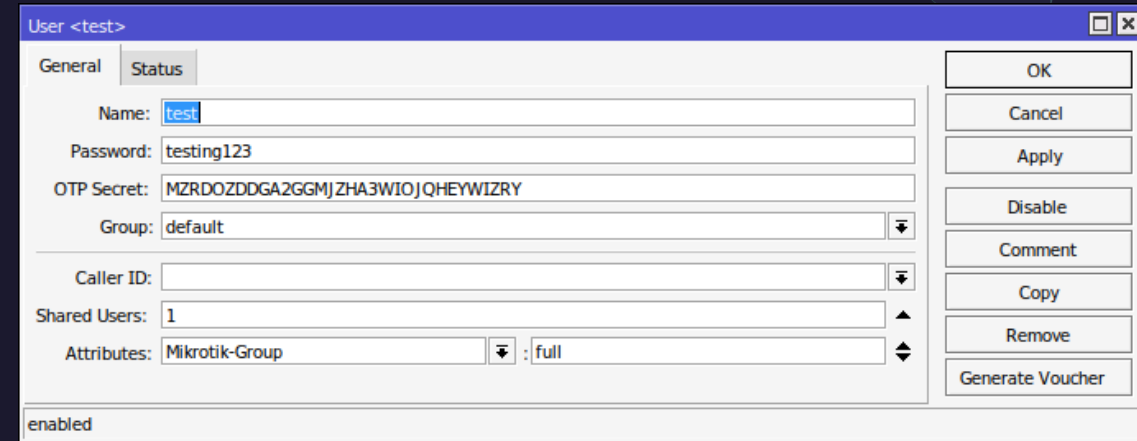
press F1 for help

```
abaddon@abaddon in ~/.ssh took 1m57s
λ ssh admin@192.168.122.60
admin@192.168.122.60's password:
Permission denied, please try again.
admin@192.168.122.60's password:
Permission denied, please try again.
admin@192.168.122.60's password:
admin@192.168.122.60: Permission denied (password).
```

Securizarea utilizatorilor de radius cu TOTP

- Acum ca am migrat spre administrarea routerului/routerelor pe radius.
- Pentru a activa functionalitatea de TOTP pe un user trebuie sa mergem in User Manager→User si pe userul la care vrem sa activam.
- Trebuie sa generam un secret OTP in base32 folosind comanda:

```
bash -c 'a=`date +%s` | sha256sum | base32 | head -c 32` ; echo ${a^^}'
```
- Dupa care adaugam secretul in aplicatia totp fie ca vorbim de Google Authenticator sau alta aplicatie. Petru testare vom folosi: totp.app
- Iar pentru a ne conecta la Winbox spre exemplu vom introduce userul test si parola+codultotp.



Securizarea accesului utilizatorilor locali

- Pentru a bloca accesul utilizatorilor locali la retele putem permite accesul doar din anumite retele.
- Pentru a face asta vom merge la System→Users apoi la userul la care vrem sa setam restrictiile.
- In cazul acesta vom permite accesul doar din retele LAN (192.168.10.0/24)

User <admin>

Name: admin

Group: full

Allowed Address: 192.168.10.0/24

Last Logged In: Mar/08/2023 16:18:15

enabled

WinBox (64bit) v3.37 (Addresses) <2>

Connect To: 192.168.122.60

Login: admin

Password: *****

Session: <own>

Note: MikroTik

Group:

RoMON Agent:

ERROR: wrong username or password

MAC Address	IP Address	Identity	Version	Board	Uptime
18:FD:74:...	192.168.88.1	MikroTik-LTE	7.7 (stab...	S53UG+5Hax02...	43d 03:00:27
4C:5E:0C:...	0.0.0.0	MikroTik-Switch	7.7rc3 (t...	RB2011UIAS-2HnD	47d 03:14:50
50:00:00:...	192.168.122.60	MikroTik	7.8 (stab...	CHR	01:31:54

```
root@Docker:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.253 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::5200:ff:fe03:0 prefixlen 64 scopeid 0x20<link>
    ether 50:00:00:03:00:00 txqueuelen 1000 (Ethernet)
    RX packets 417 bytes 309046 (309.0 KB)
    RX errors 0 dropped 6 overruns 0 frame 0
    TX packets 303 bytes 28207 (28.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Docker:~# ssh -l admin_mikrotik admin@192.168.10.1

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK KKK RRRRRR  000000  TTT  III KKK KKK
MMM MM  MMM III  KKKKK  RRR RRR  000 000  TTT  III KKKKK
MMM     MMM III  KKK KKK RRRRRR  000 000  TTT  III KKK KKK
MMM     MMM III  KKK KKK RRR RRR  000000  TTT  III KKK KKK

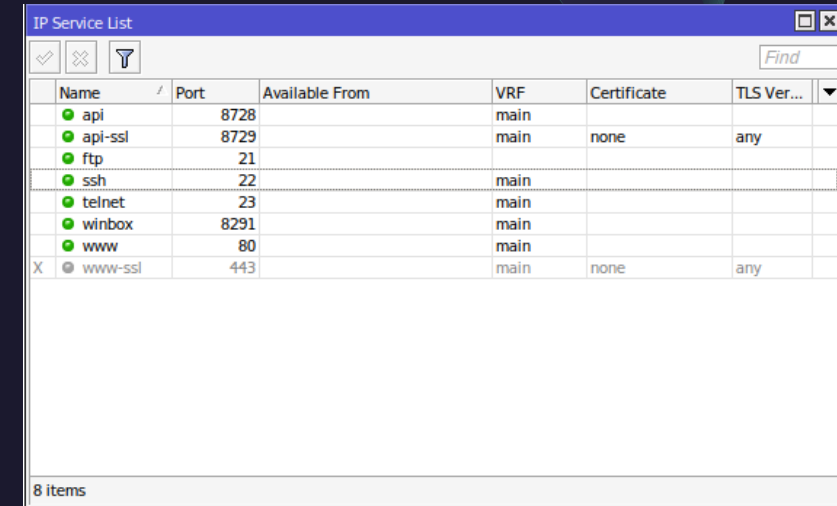
MikroTik RouterOS 7.8 (c) 1999-2023      https://www.mikrotik.com/

Press F1 for help
(2 messages not shown)
mar/08/2023 16:21:19 system,error,critical login failure for user admin from 192.168.122.60 via winbox
mar/08/2023 16:22:47 system,error,critical login failure for user admin from 192.168.122.1 via winbox
mar/08/2023 16:22:48 system,error,critical login failure for user admin from 192.168.122.1 via winbox
mar/08/2023 16:22:48 system,error,critical login failure for user admin from 192.168.122.60 via winbox
mar/08/2023 16:22:48 system,error,critical login failure for user admin from 192.168.122.1 via winbox
mar/08/2023 16:22:49 system,error,critical login failure for user admin from 192.168.122.1 via winbox
mar/08/2023 16:22:49 system,error,critical login failure for user admin from 192.168.122.1 via winbox
mar/08/2023 16:22:52 system,error,critical login failure for user admin from 192.168.122.1 via winbox

[admin@MikroTik] >
16:23:49 echo: system,error,critical login failure for user admin from 192.168.122.60 via winbox
[admin@MikroTik] >
```

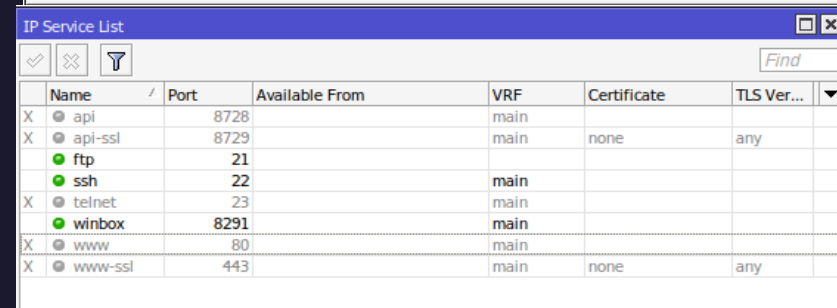

Limitarea accesului la serviciile routerului

- Pentru a limita accesul la serviciile sale trebuie sa intram in IP→Services unde putem vedea o lista de servicii.
- Avand optiunea sa le oprim, sa le limitam accesul si sa le punem un certificat.
- Serviciile api ar trebui oprite daca nu le folosim, de fapt cam orice serviciu pe care nu il folosim ar trebui oprit si pastrate doar cele folosite (de preferat pentru management doar ssh cu certificate sau radius).

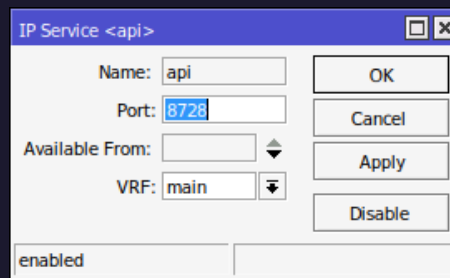


	Name	Port	Available From	VRF	Certificate	TLS Ver...
	api	8728		main		
	api-ssl	8729		main	none	any
	ftp	21				
	ssh	22		main		
	telnet	23		main		
	winbox	8291		main		
	www	80		main		
X	www-ssl	443		main	none	any

8 items



	Name	Port	Available From	VRF	Certificate	TLS Ver...
X	api	8728		main		
X	api-ssl	8729		main	none	any
	ftp	21				
	ssh	22		main		
X	telnet	23		main		
	winbox	8291		main		
X	www	80		main		
X	www-ssl	443		main	none	any



IP Service <api>

Name: api

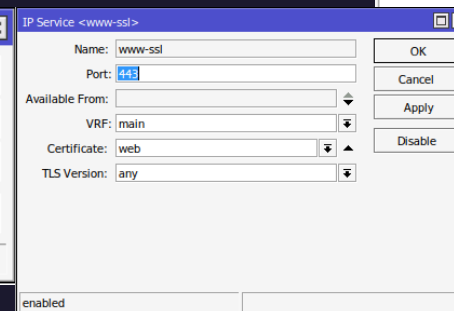
Port: 8728

Available From:

VRF: main

enabled

OK Cancel Apply Disable



IP Service <www-ssl>

Name: www-ssl

Port: 443

Available From:

VRF: main

Certificate: web

TLS Version: any

enabled

OK Cancel Apply Disable