

MIKROTIK zapoznanie ze środowiskiem

WPROWADZENIE

Mikrotik – łotewska firma produkująca sprzęt sieciowy pracujący na jądrze Linuxa. Wykorzystuje autorski system RouterOS (również oparty na Linuxie). Posiada jasny system licencjonowania oprogramowania który posiada odpowiednią licencję „out of the box”. Zarządzanie urządzeniem odbywać się może na kilka sposobów:

- **WWW (Webfig)** – przez przeglądarkę internetową
- **WinBox IP** – dedykowana aplikacja (połączenie szyfrowane)
- **WinBox MAC-Winbox** – j.w.
- **SSH** – połączenie szyfrowane

Występuje jeszcze kilka możliwości połączenia jednak nie zostaną one opisane ponieważ dotyczą sprecyzowanej potrzeby (np. możliwość wykorzystania API) bądź są niezabezpieczone (np. Telnet).

Przy pomocy WWW oraz WinBox praca może odbywać się w systemie „okienkowym” (aplikacja wykorzystuje GUI które po dłuższej współpracy okazuje się bardzo logiczne). W przypadku korzystania z terminala który występuje w powyższych rozwiązaniach ALE jest jedynym możliwym sposobem komunikacji przy pomocy SSH oraz Telnet należy zapamiętać 3 komunikaty:

- **tab** – dopełnia komendę, podpowiada
- **strzałka w górę** – przeszukiwanie historii komend (jak w powershellu, cmd czy terminalu)
- **?** – wyświetla komendy oraz opis ich działania, w ramach danej gałęzi

ŁĄCZENIE Z URZĄDZANIEM

Poleca się każdorazowo podczas wykonywania ćwiczeń przywrócić urządzeniu ustawienia fabryczne. W przypadku pierwszego uruchomienia Mikrotik posiada preinstalowaną konfigurację która m. in. posiada zdefiniowane podstawowe reguły firewalla ale również ma przypisany port WAN (nr.1) – wniosek komputer winniśmy wpiąć w kolejne gniazda.

WAŻNE !

Istnieje kilka sposobów na przywrócenie ustawień fabrycznych. Jeżeli nie mamy dostępu do urządzenia należy (dla HEX S):

- podpiąć zasilanie
- wcisnąć przycisk *reset*
- odpiąć zasilanie trzymając przycisk *reset*
- podpiąć zasilanie trzymając przycisk *reset*
- po 5 sekundach należy zwolnić przycisk

Jeżeli mamy dostęp do urządzenia należy przejść do **System → Reset Configuration** wybrać pożądane parametry i zatwierdzić.

W obu przypadkach konto admin nie posiada hasła.

WWW (port 80)

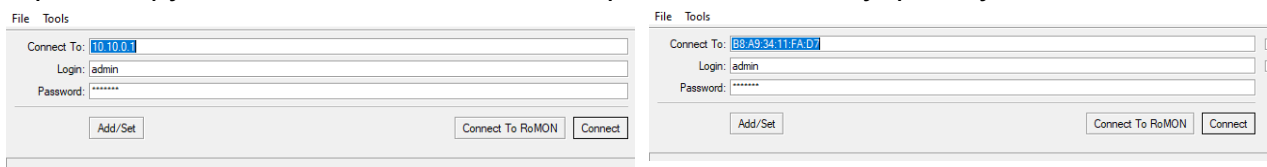
Połączenie przez przeglądarkę nie odbiega od norm stosowanych przez innych producentów urządzeń sieciowych. Należy odnaleźć adres routera i z nim się połączyć. W przypadku urządzeń Mikrotik w 90% przypadków adres domyślny to **192.168.88.1/24**

Logowanie przez przeglądarkę nie należy do złych jednak zgodnie ze sztuką należy pobrać apkę WinBox i z niej korzystać.

WinBox IP oraz MAC (port 8291)

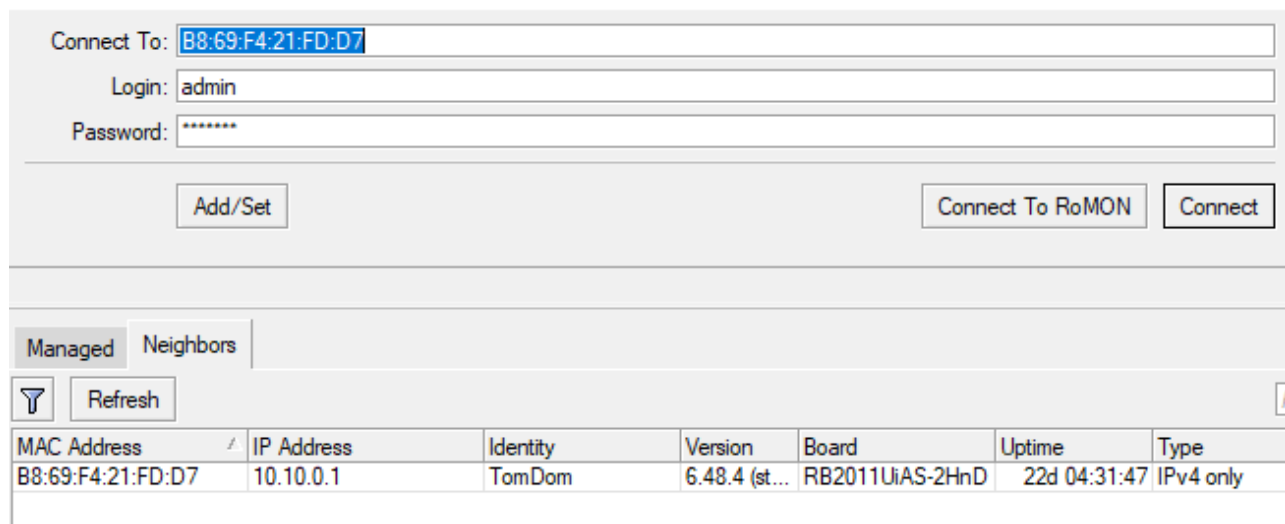
Domyślny sposób pracy z urządzeniami łotewskiego producenta. Program należy pobrać w najnowszej wersji ze strony producenta tj. www.mikrotik.com/download

W stosunku do połączenia główną przewagą jest szybkość oraz możliwość łączenia przez wspomniany już MAC adres. Wizualnie różnica prezentowana zostaje poniżej



Łączenie z wykorzystaniem adresu MAC pozwala dostać się do urządzenia bez konfiguracji domyślnej. **Dodatkowo MAC obsługiwany jest w 2 warstwie modelu OSI.**

Neighbors (port 5678)



MAC Address	IP Address	Identity	Version	Board	Uptime	Type
B8:69:F4:21:FD:D7	10.10.0.1	TomDom	6.48.4 (st...	RB2011UiAS-2HnD	22d 04:31:47	IPv4 only

Automatycznie wykrywa urządzenia firmy Mikrotik które znajdują się w tym samym segmencie sieci co komputer który się z nim łączy. Wspomniane wyżej połączenie MAC działa tylko w powyższym przypadku tj. gdy komputer znajduje się w tej samej sieci co router.

USTAWIENIA PODSTAWOWE

USER i HASŁO

Powinno się zmienić domyślny login administratora na coś innego (utrudnia ew. ataki siłowe które najczęściej dotyczą *admin* 'a) dodając jednocześnie nowe konto do grupy full.

System → Users

Logując się ponownie (na nowe konto) można zdegradować admina do roli read.

IDENTITY

To nazwa naszego urządzenia która w przypadku zarządzania większym gronem sprzętu sieciowego ułatwi identyfikację. Zauważalne jest to również w zakładce Neighbors podczas logowania.

System → Identity

NEIGHBORS

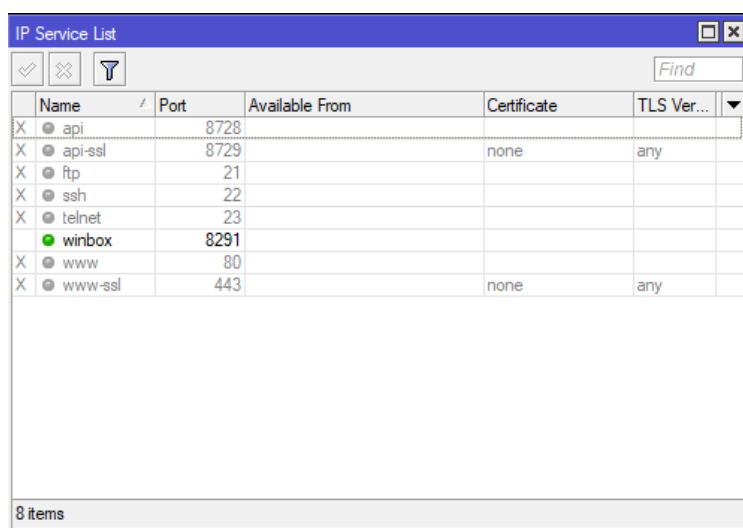
Miecz obosieczny, jeżeli chcemy wiedzieć musimy być takie widziani (protokół MNDP). Bardzo przydatny jednak w przypadku konkretnych sytuacji. Domyślnie powinien zostać wyłączony.

IP → Neighbors

OGRANICZENIE DOSTĘPU

Posiadamy kilka możliwości łączenia z urządzeniem. Te z których nie korzystamy powinny zostać wyłączone co nie jest domyślnie oczywiste.

IP → Services



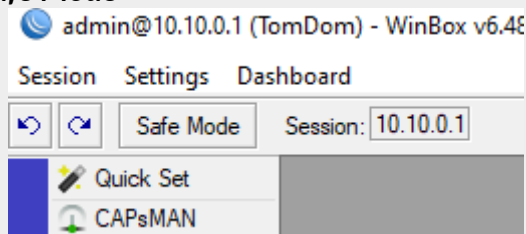
	Name	Port	Available From	Certificate	TLS Ver...
X	api	8728			
X	api-ssl	8729		none	any
X	ftp	21			
X	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	any

8 items

WAŻNE !

Wszelkie ustawienia kliknięte w WinBox są wprowadzane natychmiastowo.

Aby uniknąć ew. nieodwracalnych błędów można wykorzystać narzędzie **Safe Mode**



Po wciśnięciu, wszystkie modyfikacje jakie wprowadzimy wymagają „odhaczenia” tj. ponownego wciśnięcia które wprowadza zmiany „na stałe”.

Gdybyśmy doprowadzili do zerwania połączenia podczas wciśniętego przycisku krytyczne zmiany zostały by cofnięte do momentu sprzed wciśnięcia buttona.

UPDATE

System RouterOS dość często otrzymuje poprawki łatające błędy, poprawiające wydajność czy dodające nowe funkcjonalności. Wyróżniamy 3 możliwe wersje:

- **Long-term** – najbardziej stabilna
- **Stable** – stabilna z dodatkowymi funkcjonalnościami których nie posiada Long-term
- **Testing** – testowa, posiadająca najnowszy kod

System → Packages → Check For Updates

POLECENIA

1. Podepnij router do sieci szkolnej.
2. Nadaj Identity „imie_nazwisko” – nie wyłączaj protokołu MNDP
3. Stwórz nowego usera przypisz mu hasło. Wyłącz konto admin.
4. Przywróć urządzenie do ustawień fabrycznych z parametrem „No Default Configuration”, połącz się przez Webfig.
5. Przywróć ustawienia fabryczne bez parametru „No Default.....”
6. Połącz się z routerem z wykorzystaniem adresu IP.
 - (a) W IP → Services zmień port winbox na 22334
 - (b) połącz się ponownie z routerem przez IP
 - (c) wciśnij funkcję *Safe Mode*
 - (d) ponownie zmień port – na 33445
7. Połącz się z routerem z wykorzystaniem adresu MAC.
 - (a) W IP → Services zmień port winbox na 44556
8. Czym różni się IP i MAC mode.

PARA

1. Wykorzystując protokół MNDP zaloguj się do routera partnera, pośrednio przez Twoje urządzenie.

O CO MOGĘ PYTAĆ ?

ftp
mndp
ssh
telnet
mac
port
szyfrowanie
terminal
nat
brama
maska
rozgłoszeniowy