

Wygodna i łatwa w implementacji koncentracja VPN

Na przykładzie firmy outsourcingowej

MikroTik Warsaw Training Center



Michał Filipek

Network Architect
Zabbix Trainer
MikroTik Trainer



/in/michalfilipek



michal@mwtc.pl

Certyfikowane
Szkolenia
MikroTik



Sieci IP
Konsultacje,
Projektowanie i
Wdrożenia

Systemy
Monitoringu
Szkolenia



Dla kogo ?

- firma świadcząca obsługę informatyczną IT
- ponad 40 klientów abonamentowych
- każdy klient posiada router, wewnętrzną sieć LAN, serwer Windows, Access Point
- potrzebny bezpieczny dostęp do sieci każdego z klientów w celach serwisowych
- potrzebny dostęp dla pracowników wdzwanianych
- nie każdy klient posiada stały/publiczny adres IP

Wymagania

01 Koncentrator VPN

Routery z oddziałów
Pracownicy IT

02 Serwer Radius

Uwierzytelnienie VPN
Uwierzytelnienie pracowników IT

03 Mapowanie adresacji

Rozwiązanie problemów
pokrywającej się adresacji
lokalnej klientów

04 Firewall

Izolacja klientów
Nadawanie uprawnień na
podstawie
przynależności do
grup/profilu

05 Optymalnie kosztowo

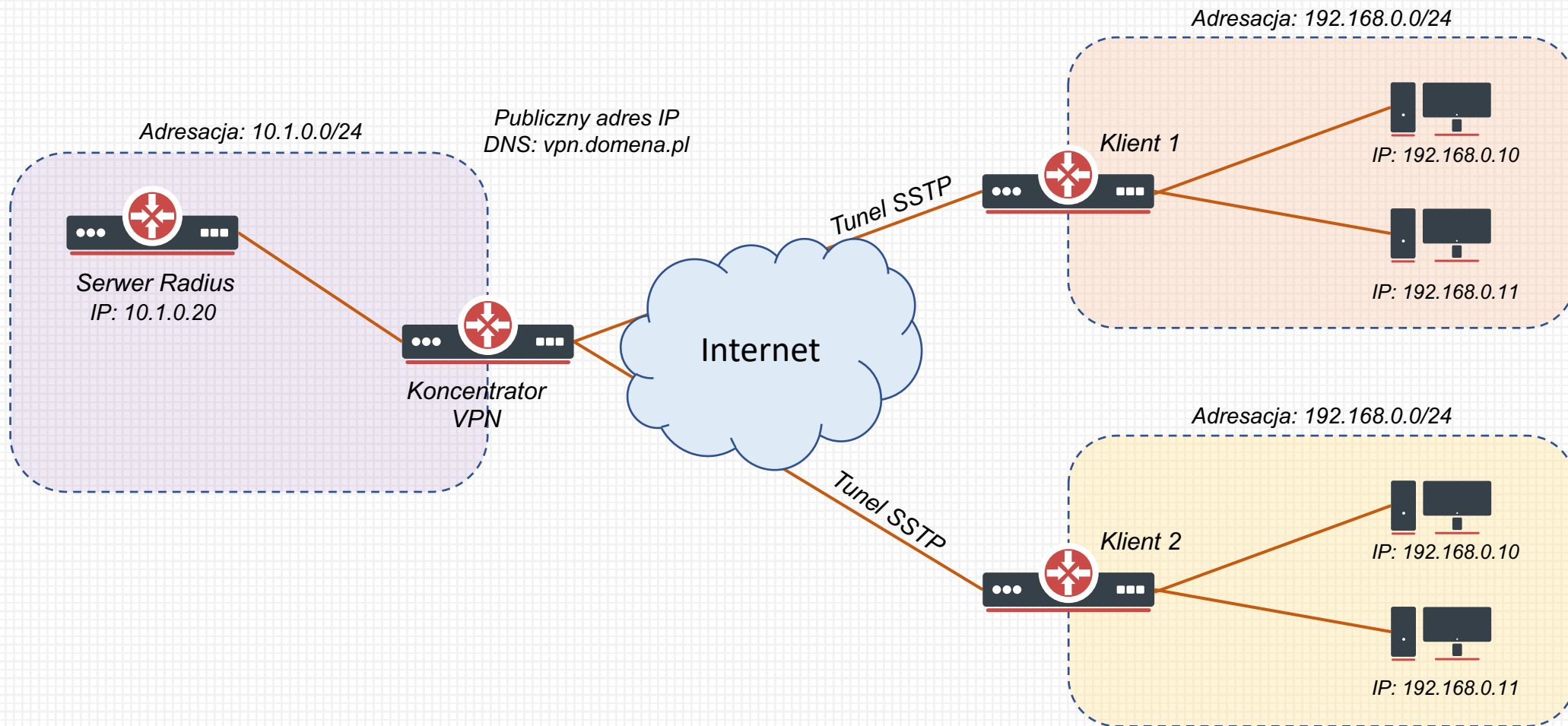
Szybka instalacja
Brak dodatkowych opłat licencyjnych

Koncentrator VPN

Wymagania:

- posiada stały publiczny adres IP
- technologia VPN SSTP (mało wydajny ale łatwy w konfiguracji)
- klienci VPN łączą się podając nazwę DNS vpn.domena.pl zamiast adresu IP
- urządzenie jest klientem serwera RADIUS

Koncentrator VPN



Schemat

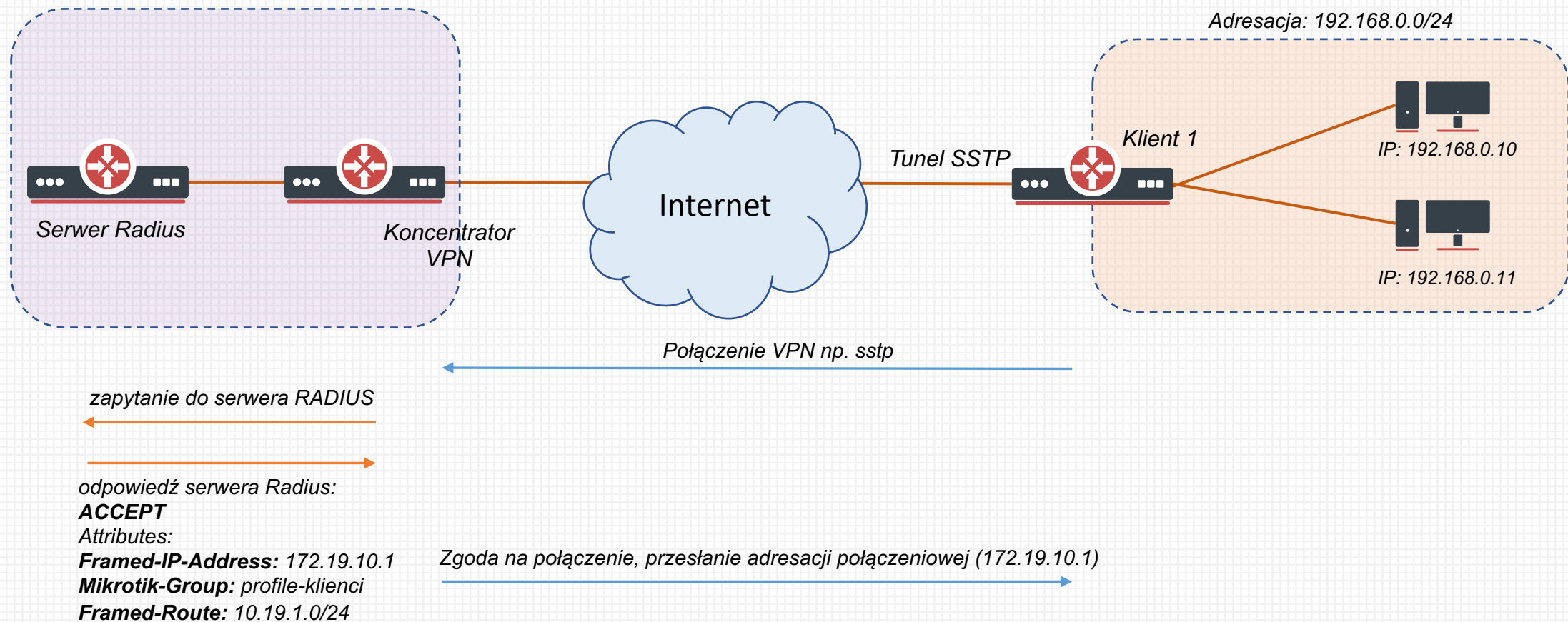
Serwer Radius (user-manager)

RouterOS 7 (w pełni funkcjonalna implementacja Radius):

- uwierzytelnia konta VPN routerów klienckich
- uwierzytelnia dostęp wdzwaniany dla pracowników IT (VPN)
- uwierzytelnia konta dostępu do urządzeń sieciowych
- uwierzytelnianie klientów podłączonych do przełącznika (dot1x)
- uwierzytelnienie klientów sieci bezprzewodowej (wireless)
- centralny punkt nadawania/odbierania dostępu
- poza uwierzytelnieniem użytkownika przesyła dodatkowe atrybuty (np grupa)

Serwer Radius (user-manager)

RouterOS 7 –VPN

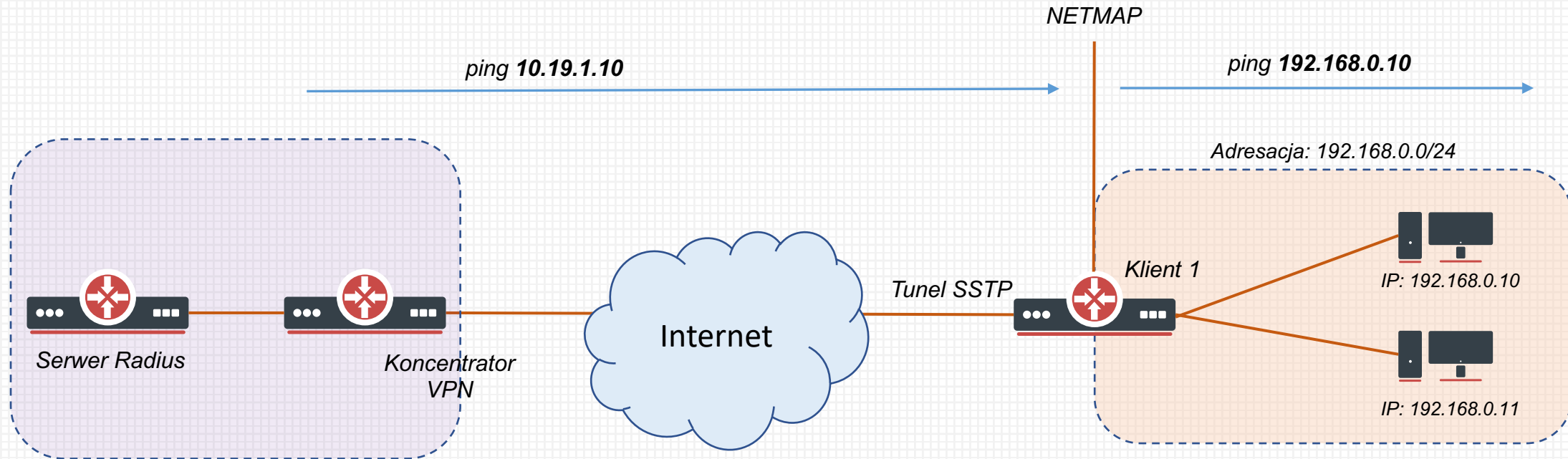


Mapowanie adresacji

- Realizowane jest bezpośrednio na routerach klienckich (nie na koncentratorze)
- Konieczne ze względu na pokrywającą się adresację klientów np. 192.168.0.0/24
- Osobna reguła **netmap** dla łańcucha **src-nat**
- Osobna reguła **netmap** dla łańcucha **dst-nat**

Mapowanie adresacji

- `/ip firewall nat add action=netmap chain=srcnat dst-address=10.1.0.0/24 src-address=192.168.0.0/24 to-addresses=10.19.1.0/24`
- `/ip firewall nat add action=netmap chain=dstnat dst-address=10.19.1.0/24 src-address=10.1.0.0/24 to-addresses=192.168.0.0/24`




Firewall

Koncentrator VPN

- izolacja komunikacji pomiędzy klientami
- zapewnienie ruchu z sieci wewnętrznej 10.1.0.0/24 do sieci LAN klientów
- reguły dla użytkowników z dostępem wdzwanianym
- połączenia VPN posiadają dedykowane profile na potrzeby firewall

Instalacja RADIUS (user-manager)

<https://mikrotik.com/download>











HomeAboutBuyJobsHardwareSoftwareSupportTrainingAccount












Software

DownloadsChangelogsDownload archiveRouterOSThe DudeMobile apps

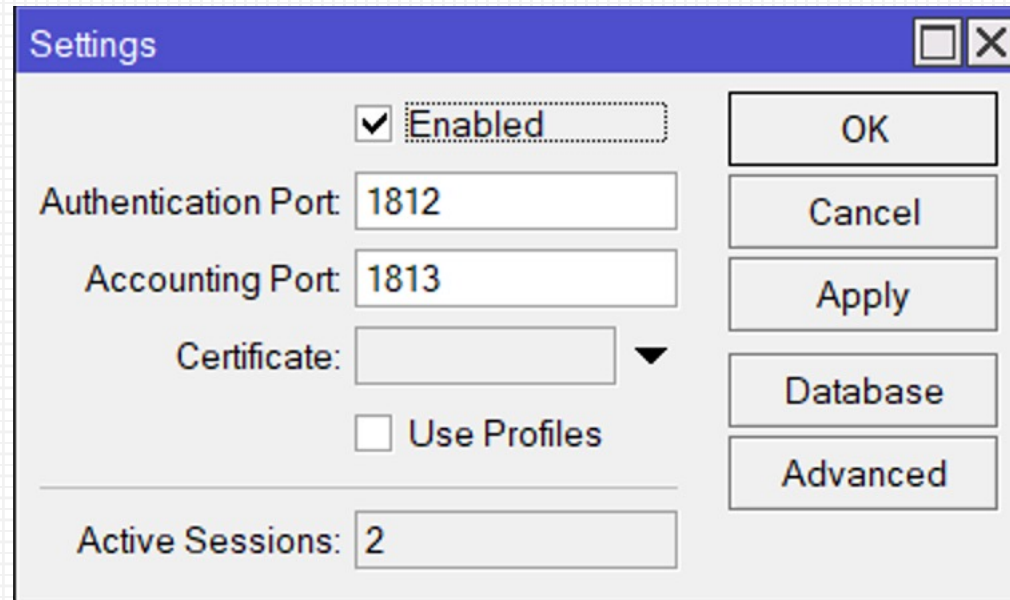
X86

Main package		
Extra packages		
CD Image		
Install image		

< > all_packages-x86-7.11.2

Name	Date Modified	Size	Kind
 calea-7.11.2.npk	1 Sep 2023 at 09:42	25 KB	Document
 container-7.11.2.npk	1 Sep 2023 at 09:42	107 KB	Document
 dude-7.11.2.npk	1 Sep 2023 at 09:42	1,4 MB	Document
 gps-7.11.2.npk	1 Sep 2023 at 09:42	25 KB	Document
 iot-7.11.2.npk	1 Sep 2023 at 09:42	336 KB	Document
 lora-7.11.2.npk	1 Sep 2023 at 09:42	17 KB	Document
 rose-storage-7.11.2.npk	1 Sep 2023 at 09:42	4,1 MB	Document
 tr069-client-7.11.2.npk	1 Sep 2023 at 09:42	152 KB	Document
 ups-7.11.2.npk	1 Sep 2023 at 09:42	41 KB	Document
 user-manager-7.11.2.npk	1 Sep 2023 at 09:42	422 KB	Document
 wifiwave2-7.11.2.npk	1 Sep 2023 at 09:42	307 KB	Document

Instalacja RADIUS (user-manager)



The image shows a 'Settings' dialog box for a RADIUS server configuration. The dialog has a blue title bar with the text 'Settings' and standard window control buttons (minimize, maximize, close). The main area is light gray and contains several configuration options. At the top, there is a checked checkbox followed by a text box containing the word 'Enabled'. Below this, there are two text boxes: 'Authentication Port' with the value '1812' and 'Accounting Port' with the value '1813'. To the right of these is a 'Certificate' label followed by an empty text box and a downward-pointing arrow. Below the certificate field is an unchecked checkbox labeled 'Use Profiles'. At the bottom, there is a text box labeled 'Active Sessions' with the value '2'. On the right side of the dialog, there is a vertical stack of five buttons: 'OK', 'Cancel', 'Apply', 'Database', and 'Advanced'.

<input checked="" type="checkbox"/> Enabled	OK
Authentication Port: 1812	Cancel
Accounting Port: 1813	Apply
Certificate: <input type="text"/> ▼	Database
<input type="checkbox"/> Use Profiles	Advanced
Active Sessions: 2	

Uruchomienie usługi radius serwer

RADIUS (user-manager)

User Manager					
Routers Users User Groups Sessions Profiles User Profiles Limitations Profile Limitations Attributes Payment					
+ - ✓ ✗ ⚙ Settings Generate Report Find					
Name	Address	CoA Port	Access Requ...	Access Failures	
router-VPN	10.1.0.1	3799	5	0	
router1	172.19.10.1	3799	0	0	
router2	172.19.10.2	3799	2	0	

Dodanie koncentratorVPN

RADIUS (user-manager)

The screenshot shows the 'User Manager' web interface. The 'Users' tab is selected. A modal window titled 'User <klient1>' is open, showing the configuration for a user named 'klient1'. The 'General' tab is active, and the 'Status' tab is also visible. The configuration fields are as follows:

- Name: klient1
- Password: ****
- OTP Secret: (empty)
- Group: default
- Caller ID: (empty)
- Shared Users: 1
- Attributes:
 - Framed-IP-Address: 172.19.10.1
 - Mikrotik-Group: profile-klienci
 - Framed-Route: 10.19.1.0/24

At the bottom of the modal, there is a checkbox labeled 'enabled' which is checked. To the right of the modal, there is a list of users with columns for 'S.' and '1'. The first row shows '1' in both columns. Below the list, there are buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Generate Voucher.

Dodanie użytkownika PPP

RADIUS - client

RADIUS Server <10.1.0.20>

General Status

Service: ☒ ppp ☒ login
☐ hotspot ☐ wireless
☐ dhcp ☐ ipsec
☐ dot1x

Called ID:

Domain:

Address: 10.1.0.20

Protocol: udp

Secret: ****

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

☐ Accounting Backup

Realm:

Certificate: none

Src. Address: 0.0.0.0

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

Dodanie użytkownika PPP

RADIUS - client

PPP

Interface | **PPPoE Servers** | Secrets | Profiles | Active Connections | L2TP Ethernet | L2TP Secrets

+ - ✓ ✗ [icon] [icon] PPP Authentication&Accounting

	Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Routes
X	● klient2	*****	any		default	2.2.2.2	3.3.3.3	

PPP Authentication&Accounting

☒ Use Radius

☒ Accounting

☐ Use Circuit ID in NAS Port ID

Interim Update: ▼

OK

Cancel

Apply

1 item

Ustawienie ppp

Dziękujemy za uwagę

<https://mwtc.pl>
[email: info@mwtc.pl](mailto:info@mwtc.pl)
facebook.com/mwtcPL

