MBUM #11

PPP VPN z TOTP w MikroTik RouterOS

SSTP, PPP AAA i User Manager

Bartosz Kowalczyk

Architektura, mechanizm uwierzytelniania i demonstracja

Co właściwie dzieje się podczas połączenia VPN?

Trzy warstwy, które łatwo pomylić: ochrona kanału, sesja użytkownika i dostęp do zasobów.

1

Bezpieczny kanał

TLS + SSTP

Windows sprawdza certyfikat serwera, a TLS szyfruje i chroni integralność komunikacji.

Windows — **MikroTik**

TLS / SSTP

2

Sesja i tożsamość użytkownika

PPP tworzy sesję punkt–punkt i prowadzi uwierzytelnienie. RADIUS przekazuje decyzję do User Managera.

PPP — **MS-CHAPv2** — **RADIUS** — **User Manager** — **TOTP**

3

Dostęp do zasobów

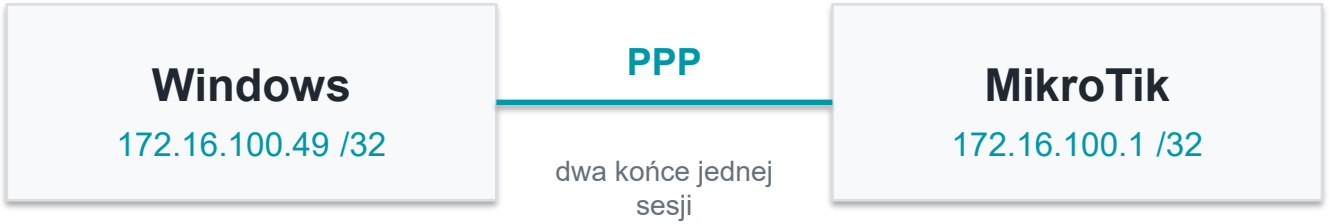
Adresacja + routing + firewall + NAT

Po zestawieniu sesji dopiero te mechanizmy decydują, dokąd może trafić ruch użytkownika.

PPP to więcej niż logowanie

PPP zestawia sesję punkt–punkt, negocjuje jej parametry i dopiero w jednym z etapów uwierzytelnia użytkownika.

Połączenie punkt–punkt



Co to oznacza?

PPP łączy dwa konkretne końce połączenia. Adres /32 na końcu tunelu nie oznacza wspólnego segmentu Ethernet ani wspólnej domeny broadcastowej.

Cykl zestawienia sesji PPP



Najważniejsze: uwierzytelnienie jest częścią PPP, ale PPP nie kończy się na loginie i haśle.

Usługi RouterOS a mechanizmy PPP

PPP pojawia się w kilku usługach RouterOS, ale jego rola nie zawsze jest taka sama.

PPP W PROTOKOLE **SSTP, L2TP i PPPoE faktycznie przenoszą ramki PPP.**

Usługa	Warstwy / zależność	Co z tego wynika?
SSTP	TLS — SSTP — PPP	PPP działa wewnątrz SSTP. To główny wariant tej prezentacji.
L2TP/IPsec	IPsec — L2TP — PPP	L2TP przenosi PPP, a IPsec odpowiada za ochronę transportu.
PPPoE	Ethernet — PPPoE — PPP	PPP działa nad Ethernetem — to nie jest klasyczny VPN przez Internet.

PPP AAA W ROUTEROS **OpenVPN korzysta z infrastruktury PPP AAA, ale sam protokół OpenVPN nie jest PPP.**

OpenVPN	OpenVPN	PPP AAA	W RouterOS może używać /ppp secret, profili i zewnętrznego AAA.
POZA PPP AAA	**WireGuard**	peer + klucze	Inny model uwierzytelniania — bez PPP AAA i bez loginu/hasła.

SSTP: PPP przenoszone przez TLS

Pakiet użytkownika jest opakowywany warstwa po warstwie — każda z nich ma inne zadanie.



TLS
chroni kanał i weryfikuje serwer

SSTP
przenosi PPP przez tunel

PPP
uwierzytelnia użytkownika i zestawia sesję

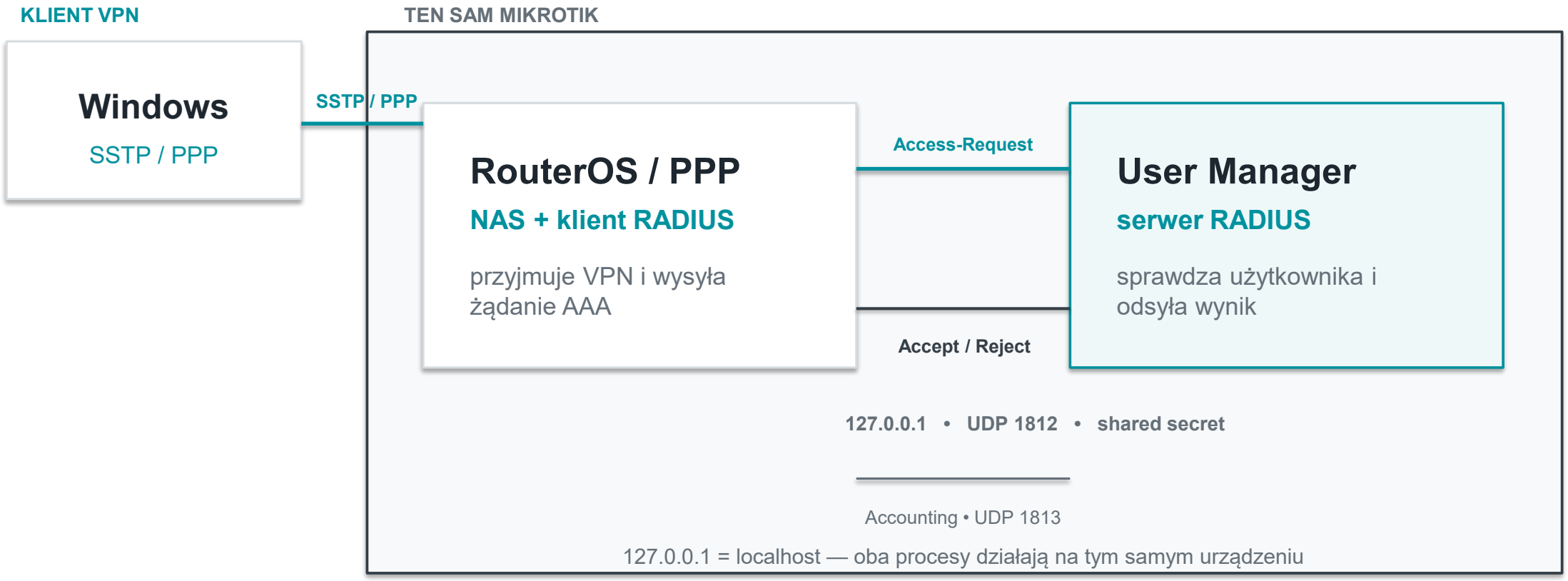
AAA rozdziela trzy zadania

Funkcja	Pytanie	Przykład dla VPN
Authentication	Czy uwierzytelnienie jest poprawne?	Nazwa użytkownika, hasło i kod TOTP
Authorization	Jakie parametry otrzyma sesja?	Adres IP, profil PPP, ograniczenie czasu
Accounting	Co wiemy o przebiegu sesji?	Początek, koniec, transfer, przyczyna rozłączenia

Weryfikacja hasła jest tylko jedną częścią obsługi dostępu.

RADIUS i User Manager: dwie różne role

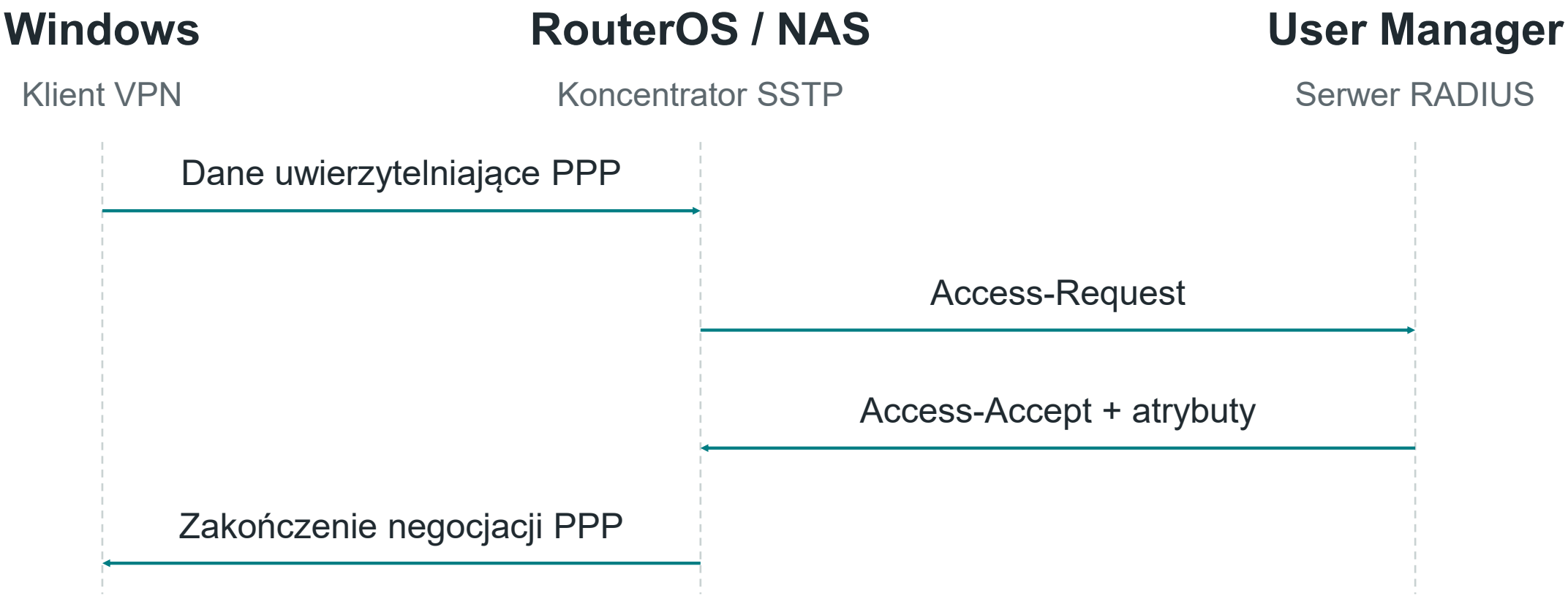
RouterOS wysyła żądanie AAA. User Manager je sprawdza i odsyła decyzję.



/radius = klient RADIUS • User Manager = serwer RADIUS

Shared secret łączy klienta RADIUS z serwerem — nie jest hasłem użytkownika VPN.

Jak przebiega decyzja RADIUS?



Access-Reject kończy próbę uwierzytelnienia bez przyznania sesji.

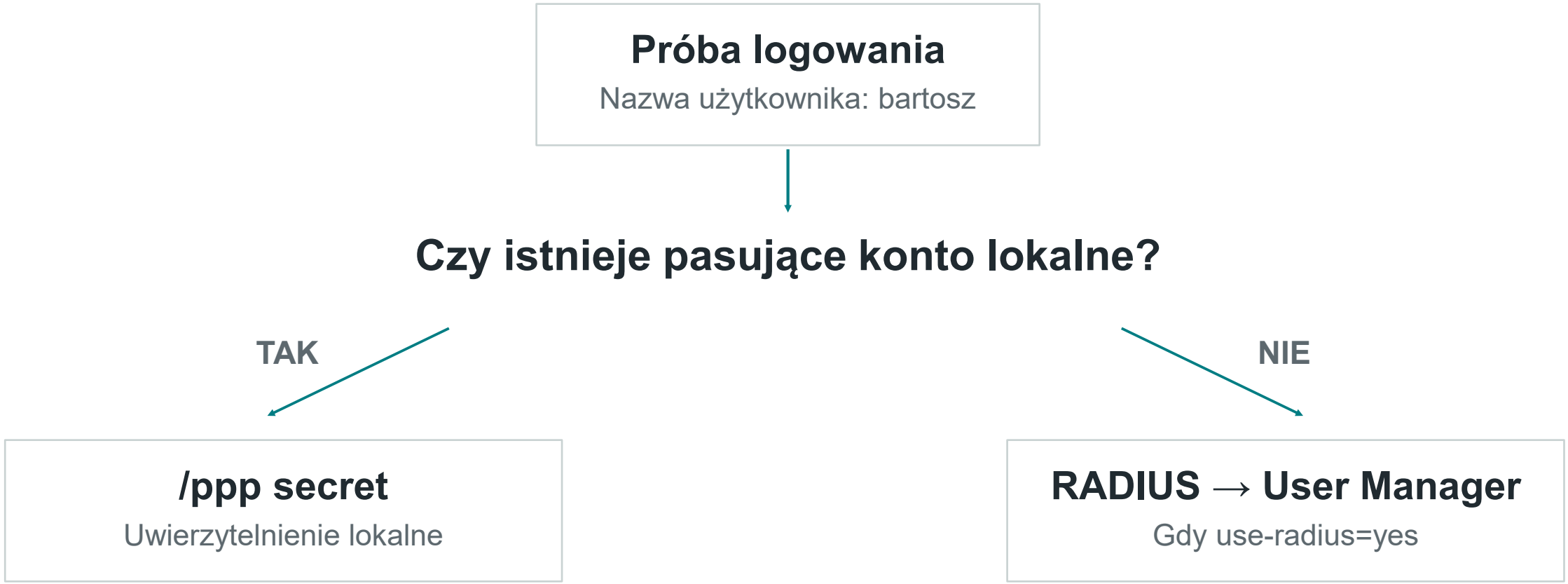
Autoryzacja: parametry sesji i dostęp do sieci

Serwer AAA może zwrócić ustawienia. RouterOS stosuje je do sesji.

Atrybut RADIUS	Znaczenie
`Framed-IP-Address`	Adres IPv4 przydzielany użytkownikowi
`Framed-Pool`	Nazwa puli adresów na koncentratorze
`Mikrotik-Group`	Profil PPP używany dla tej sesji
`Session-Timeout`	Maksymalny czas trwania sesji

Dostęp do konkretnych zasobów nadal wynika z routingu, firewalla i polityk usług.

Lokalny PPP Secret ma pierwszeństwo



Samo włączenie RADIUS nie wymusza TOTP dla kont obsłużonych lokalnie.

MFA w modelu hasło + TOTP

Co użytkownik wie

Użytkownik zna stałe hasło przypisane do swojego konta.

Co użytkownik ma

Użytkownik ma dostęp do generatora zawierającego jego sekret TOTP.

Hasło stałe + **Kod z generatora**

User Manager sprawdza połączoną wartość podczas nowego logowania PPP.

Jak powstaje kod TOTP

```
T = floor((UnixTime - T0) / 30)
```

```
TOTP = HOTP(K, T)
```

K: wspólny sekret

Zapisany w generatorze i w systemie weryfikującym.

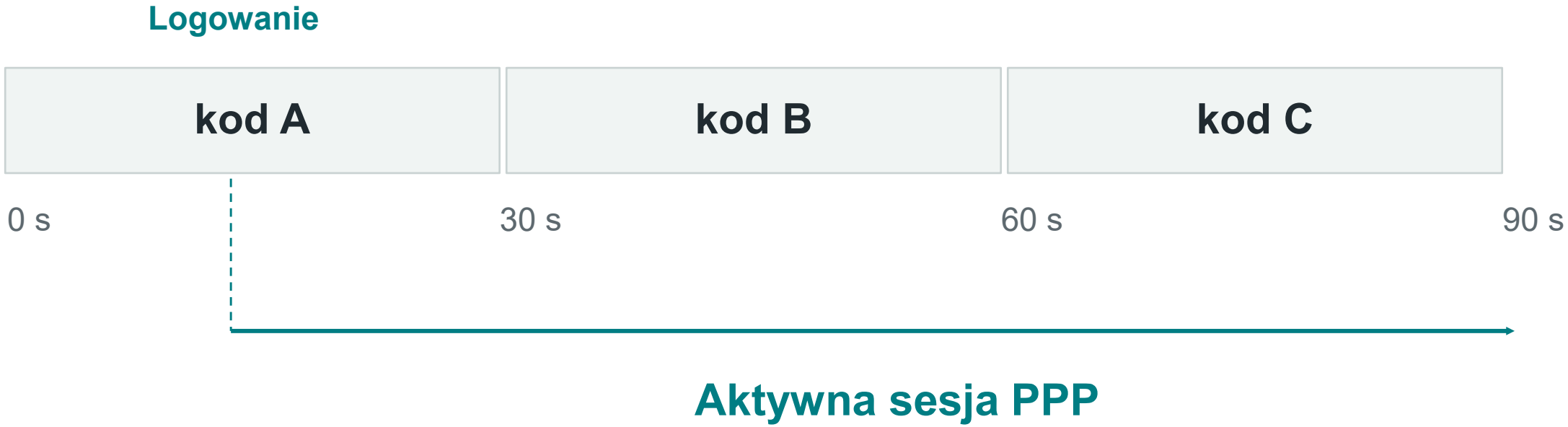
T: licznik przedziałów

Wyznaczony na podstawie czasu Unix. W naszym wariancie zmienia się co 30 sekund.

Generator i User Manager obliczają kod niezależnie. Nie wymieniają go między sobą.

Ważność kodu nie określa długości sesji

Kod jest sprawdzany przy uwierzytelnieniu. Sesja może trwać znacznie dłużej.



Okno tolerancji i ponowne użycie OTP trzeba zweryfikować dla konkretnej implementacji.

Zegar systemowy a strefa czasowa

14:10	16:10	19:40
UTC	Warszawa · UTC+02:00	Indie · UTC+05:30

Zmiana strefy

Zmienia wyświetlaną godzinę. TOTP pozostaje zgodne, jeśli czas absolutny jest poprawny.

Błędny zegar

Zmienia przedział użyty do obliczenia TOTP. Dlatego weryfikator wymaga synchronizacji czasu.

```
NTP Client → synchronized
```

Trzy sekrety, trzy różne zastosowania

Wartość	Kto ją zna?	Do czego służy?
Hasło użytkownika	Użytkownik i system uwierzytelniający	Stały składnik danych logowania
Sekret TOTP	Generator i User Manager	Wyliczanie kodów zmiennych w czasie
RADIUS shared secret	Klient RADIUS i serwer RADIUS	Ochrona wymiany RADIUS i sprawdzanie odpowiedzi

Base32 jest sposobem zapisu sekretu TOTP, a nie jego szyfrowaniem.

Granice ochrony TOTP

Przejęte hasło

Dodatkowy kod utrudnia utworzenie nowej sesji osobie, która zna wyłącznie stałe hasło.

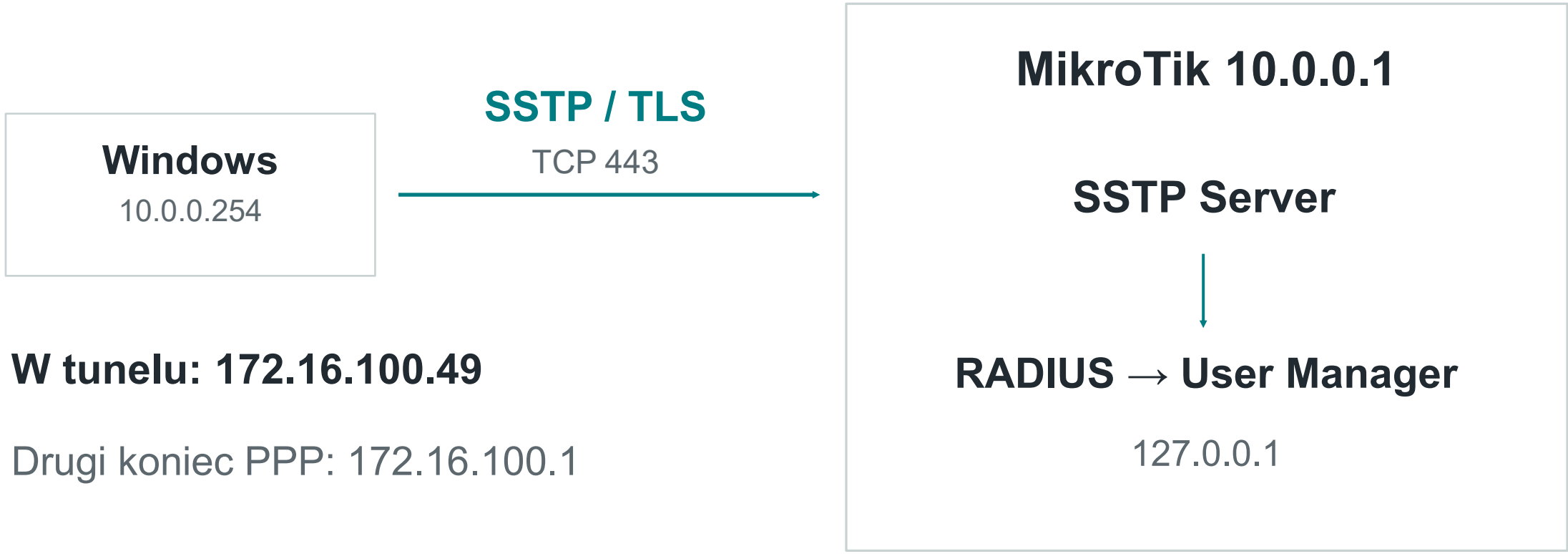
Przekazany na bieżąco kod

TOTP nie jest odporne na phishing. Aktualny kod może zostać przechwycony i użyty w czasie jego ważności.

Przejęty sekret

Sekret umożliwia generowanie kolejnych kodów. Trzeba chronić jego przechowywanie, provisioning i odzyskiwanie konta.

Windows i jeden MikroTik

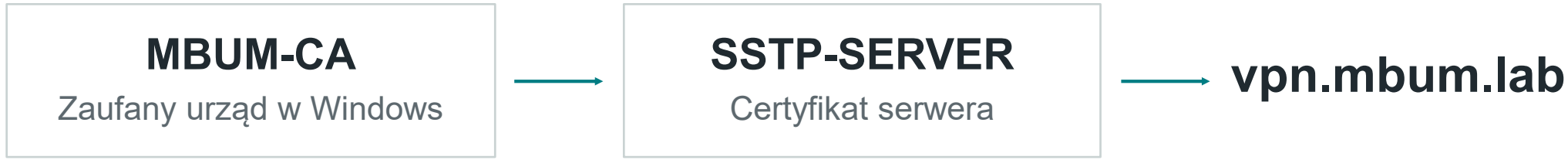


W tunelu: 172.16.100.49

Drugi koniec PPP: 172.16.100.1

RouterOS + User Manager

Zaufanie do serwera przed logowaniem PPP



Właściwość certyfikatu	Wartość z laboratorium
Common Name	vpn.mbum.lab
Subject Alternative Name	DNS:vpn.mbum.lab
Klucz i podpis	RSA 2048 / SHA-256
Przeznaczenie	digital-signature, key-encipherment, tls-server

```
10.0.0.1  vpn.mbum.lab
```

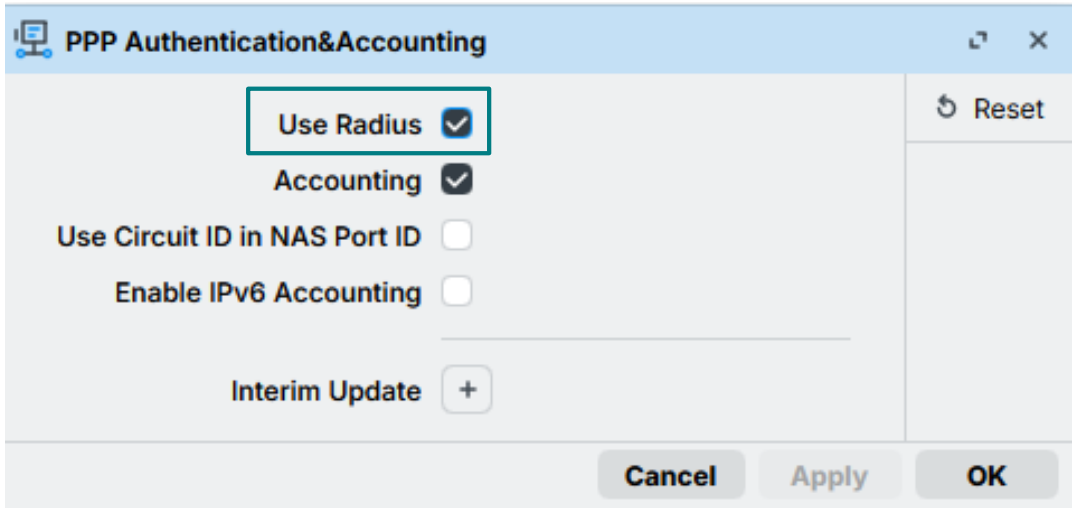
Połączenie PPP z lokalnym User Managerem

Miejsce w RouterOS	Ustawienie w labie	Rola
`/ppp aaa`	`use-radius=yes` `accounting=yes`	Włączenie zewnętrznego AAA dla PPP
`/radius`	`service=ppp` `address=127.0.0.1`	Wskazanie serwera RADIUS
`/user-manager router`	`name=localhost` `address=127.0.0.1`	Zaufany klient / NAS po stronie serwera
`/user-manager user`	`name=bartosz` `password + otp-secret`	Dane uwierzytelniające użytkownika

PPP: włączenie zewnętrznego AAA

Włączenie RADIUS i raportowanie sesji to dwa osobne ustawienia.

PPP → AAA



Use RADIUS

Korzystanie z serwera RADIUS przy uwierzytelnianiu PPP.

Accounting

Raportowanie przebiegu sesji.
Nie jest weryfikacją kodu TOTP.

Odpowiednik w terminalu

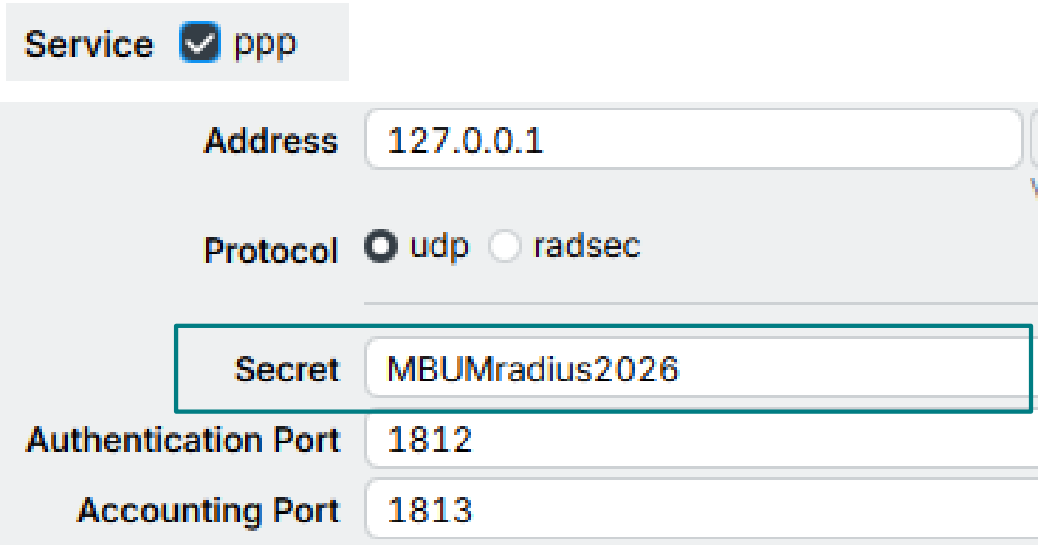
```
/ppp aaa set use-radius=yes accounting=yes
```

Adres serwera i usługę PPP wskazujemy osobno w menu RADIUS.

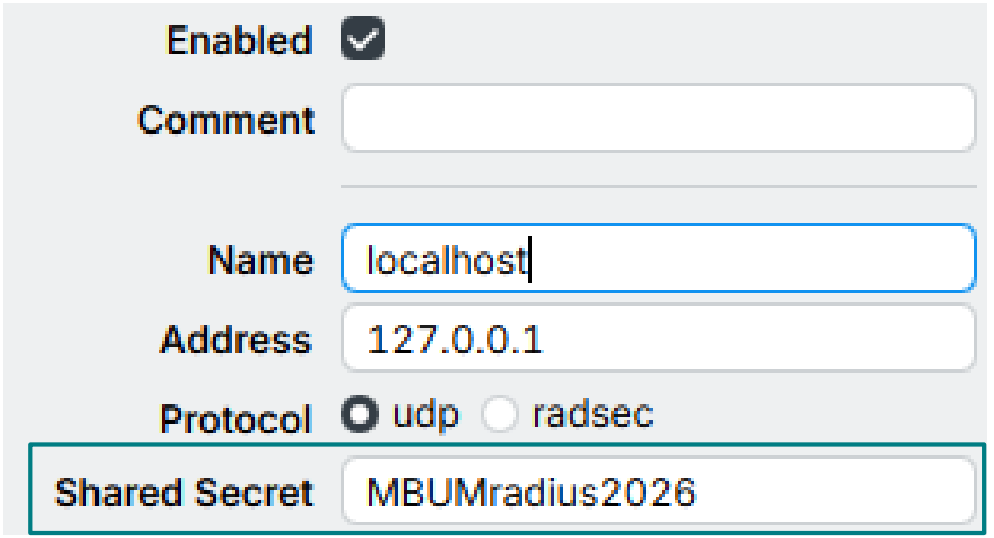
RADIUS: dwa końce tej samej wymiany

Po stronie klienta wskazujemy serwer; po stronie User Managera dopuszczamy NAS.

RADIUS → 127.0.0.1



User Manager → Routers → localhost



Secret i Shared Secret muszą mieć tę samą wartość.

1812: uwierzytelnianie i autoryzacja
1813: Accounting

Włączenie usługi User Manager:

```
/user-manager set enabled=yes
```

TOTP: wspólny sekret dla obu stron

Usługa **MWTC**

Konto **bartosz**

Sekret w formacie Base32

`MZSWS4DGMVQXKZTPNFSWC2TPOQ======`

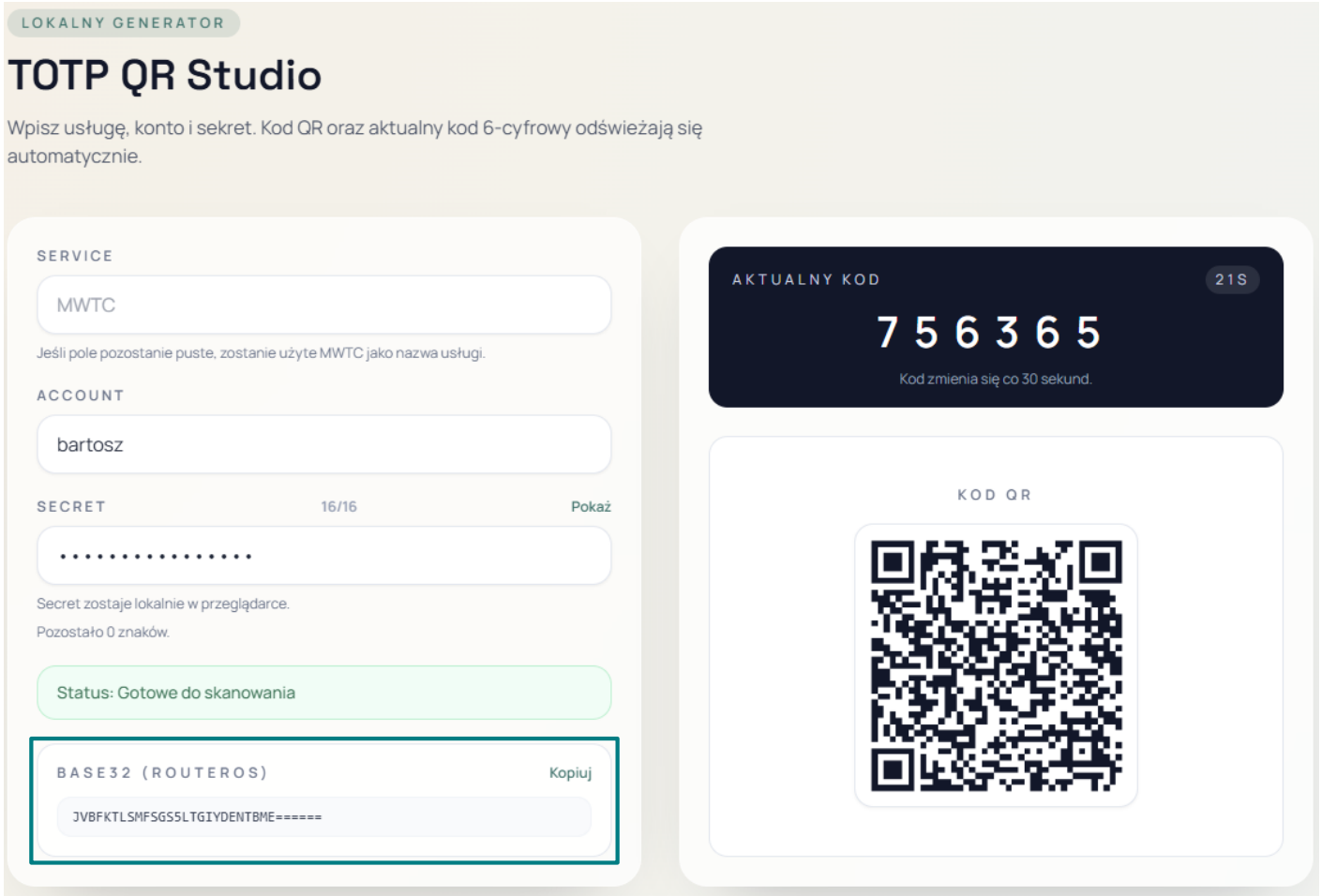
Ta sama wartość trafia do aplikacji generującej kody i do pola otp-secret użytkownika w User Managerze.

QR rejestruje generator. Nie jest kodem jednorazowym.

MWTC / bartosz

TOTP: sekret, QR i aktualny kod

Rejestracja generatora i logowanie używają różnych wartości.



BASE32 (ROUTEROS)

Sekret do skopiowania do pola OTP Secret.

Kod QR

Rejestruje generator z tym samym sekretem.

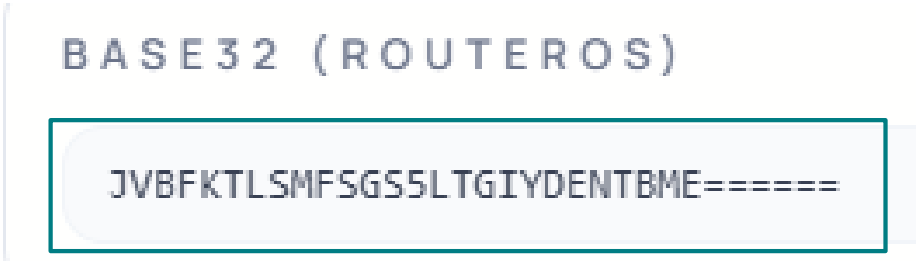
Aktualny kod

Do logowania: hasło + sześć cyfr.

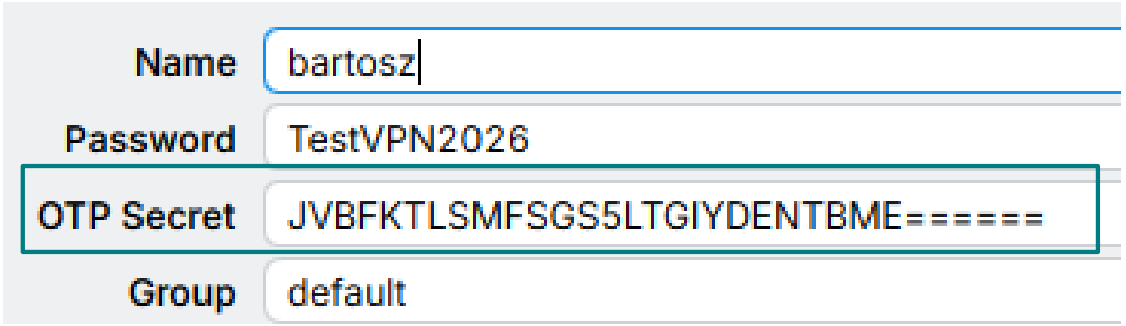
BASE32 (ROUTEROS) → OTP Secret

Kopiujemy cały tekst Base32 — bez ponownego kodowania.

TOTP QR Studio



User Manager → Users → bartosz



Ten sam sekret w obu miejscach

`JVBFKTLSMFSGS5LTGIYDENTBME======`

Odpowiednik dla istniejącego konta

```
/user-manager user set [find name="bartosz"] \
    otp-secret="JVBFKTLSMFSGS5LTGIYDENTBME======"
```

Password pozostaje bez zmian; do OTP Secret nie wpisujemy sześciocyfrowego kodu.

Profil Windows i sposób logowania

```
Name                    : MBUM SSTP
ServerAddress           : vpn.mbum.lab
TunnelType              : Sstp
AuthenticationMethod    : {MsChapv2}
RememberCredential      : False
```

Przy nowym połączeniu: stałe hasło + bieżący sześciocyfrowy TOTP.

Od logowania do aktywnej sesji

Hasło i aktualny kod TOTP tworzą jedną wartość używaną przy logowaniu.

Windows → **RouterOS** → **User Manager**

Odpowiedź MS-CHAPv2 z hasła z kodem.

Żądanie RADIUS do User Managera.

Weryfikacja konta. Access-Accept / Reject.

Aktualny kod w generatorze



Status po zestawieniu PPP



Po Access-Accept RouterOS kończy negocjację PPP i uruchamia sesję.

Wynik uwierzytelnienia w logach

Message
: user bartosz authentication failed
bartosz logged in, 172.16.100.49 from 10.30.1.119
<sstp-bartosz>: authenticated
<sstp-bartosz>: connected

Odrzucenie

Uwierzytelnienie nie zostało zaakceptowane.

Zestawienie sesji

Logowanie, uwierzytelnienie i połączenie PPP.

„Authentication failed” wskazuje etap błędu, ale nie jego dokładną przyczynę.

Sesja PPP i odpowiedź RADIUS

```
[admin@MWTC] > /ppp active/print
Flags: R - RADIUS
Columns: NAME, SERVICE, CALLER-ID, ADDRESS, UPTIME, ENCODING
#   NAME     SERVICE  CALLER-ID    ADDRESS         UPTIME  ENCODING
0 R bartosz  sstp     10.30.1.119  172.16.100.49   7m37s   AES256-GCM
```

RADIUS monitor

```
          pending: 0
         requests: 17
          accepts: 15
          rejects: 2
          resends: 0
         timeouts: 0
      bad-replies: 0
last-request-rtt: 20ms
```

Co potwierdzają te dane?

R Sesja obsłużona przez RADIUS.

CALLER-ID Adres klienta przed tunelem.

ADDRESS Adres przydzielony w PPP.

Liczniki są kumulacyjne. Sama flaga R nie potwierdza wymuszenia TOTP.

Accounting: historia sesji VPN

Raportowane są parametry i przebieg połączenia, nie zawartość pakietów.

Adresy sesji

NAS IP Address	127.0.0.1
NAS Identifier	MWTC
Calling Station ID	10.30.1.119
User Address	172.16.100.50

Ten sam klient: adres przed tunelem
i adres przydzielony w PPP.

Przebieg i transfer

Started	2026-09-18 15:41:59
Ended	2026-09-18 15:55:24
Terminate Cause	User Request
Uptime	00:13:25
Download	5.6 MiB
Upload	3906.5 KiB

Start

Rozpoczęcie sesji.

Interim Update

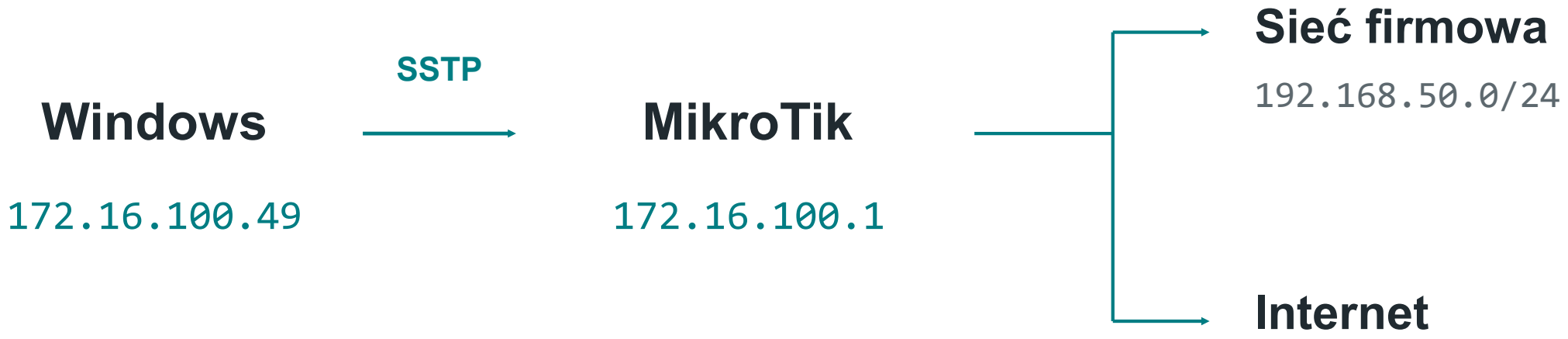
Opcjonalny raport w trakcie.

Stop

Zakończenie sesji.

Po uwierzytelnieniu: dokąd trafia ruch?

Aktywna sesja PPP nie gwarantuje jeszcze dostępu do zasobu.



Routing

Wybiera drogę do sieci docelowej.

Firewall

Dopuszcza albo blokuje ruch użytkownika.

Droga zwrotna

Odpowiedź musi wrócić do klienta PPP.

Uwierzytelnienie i poprawna ścieżka danych to dwa odrębne warunki.

Co składa się na działający VPN z TOTP

TLS / SSTP	Chroniony kanał i weryfikacja serwera.
PPP	Sesja punkt–punkt i konfiguracja IP.
MS-CHAPv2 + TOTP	Uwierzytelnienie z dodatkowym kodem.
RADIUS / User Manager	Wymiana AAA i weryfikacja użytkownika.
Accounting	Zapis przebiegu sesji.
Routing i firewall	Droga do zasobów i dopuszczenie ruchu.

TOTP wzmacnia logowanie. Nie zastępuje ochrony kanału ani polityki dostępu.