

VPN razem z 2FA

RouterOS 7



Ihor Hreskiv



Trener MikroTik

6+ lat doświadczenia

Autor kanału YouTube

MikroTik Polska

Administrator i architekt

20+ lat praktyki

Praktyk

*w zakresie wirtualizacji, sieci,
systemów wysokiej dostępności
VPN, BGP, systemy rozproszone*

Jaki stosować?



Jaki protokół stosować?

SSTP

ZeroTier

IPSec IKEv2

PPTP

WireGuard

L2TP+IPsec

OpenVPN

Jaki protokół stosować?

Protokół	Zalety (Pros)	Wady (Cons)	Security
PPTP	Bardzo prosta konfiguracja Wbudowany w starsze systemy	Bardzo słabe szyfrowanie (MS-CHAPv2 złamany) Łatwy do przechwycenia Niezalecany do produkcji	✗ Niebezpieczny, przestarzały
SSTP	Działa przez TCP/443 (łatwo przechodzi przez firewalle) Wsparcie w Windows	Zamknięty protokół Microsoft Mniejsza przenośność Ograniczone wsparcie w innych OS	⚠ Średni – zależy od implementacji i certyfikatów
L2TP+IPsec	Szerokie wsparcie systemowe (Windows, macOS, iOS, Android) Łączy tunelowanie z szyfrowaniem	Wolniejszy (podwójna enkapsulacja) Problemy z NAT Łatwe do blokowania porty UDP	✓ Bezpieczny, jeśli używa silnych algorytmów
OpenVPN	Open source, audytowany Bardzo elastyczny (TCP/UDP, dowolny port) Duże wsparcie społeczności	Wolniejszy niż IKEv2/WireGuard Trudniejsza konfiguracja Wymaga dodatkowego klienta	✓ Bardzo bezpieczny, przy AES-256 + TLS 1.2/1.3

Jaki protokół stosować?

Protokół	Zalety (Pros)	Wady (Cons)	Security
ZeroTier	Bardzo prosta konfiguracja (ID sieci) Działa przez NAT bez dodatkowych ustawień Multi-platformowy (Windows, macOS, Linux, iOS, Android, routery)	Zależność od centralnego kontrolera Rozwiązanie zamknięte, brak standaryzacji IETF Mniejsza wydajność niż natywny WireGuard/IPSec	✅ Szyfrowanie end-to-end (AES-256, Curve25519) ⚠️ Zależy od zaufania do kontrolera
WireGuard	Bardzo wydajny i szybki Minimalistyczny kod (łatwy do audytu) Dobrze działa za NAT	Brak natywnego wsparcia w starszych systemach Brak integracji z EAP/RADIUS Mniej dojrzały w enterprise	✅ Nowoczesny i bezpieczny (ChaCha20, Poly1305), ale młodszy standard
IPsec IKEv2	Standard IETF, rekomendowany przez NSA/NIST Wsparcie natywne w Windows, macOS, iOS, Android Integracja z RADIUS/MFA	Bardziej złożona konfiguracja Wymaga certyfikatów Problemy interoperacyjności między producentami	✅✅ Bardzo bezpieczny; spełnia NIST/CNSA wymagania

Dlaczego IKEv2

- spełnia aktualne wymagania kryptograficzne (CNSSP 15, NIST)
- mniej podatny na ataki
- prostszy w konfiguracji
- wspierany natywnie przez wszystkie główne systemy
- wykorzystuje RADIUS w połączeniu z mechanizmami MFA

NIST SP 800-77 Rev. 1 – *Guide to IPsec VPNs*

Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology — zalecenia dotyczące konfiguracji VPN-ów IPsec, w tym IKE.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf>

RFC 9206 – *Commercial National Security Algorithm (CNSA) Suite and Usage*

Dokument od NSA, który w sekcji dotyczącej IPsec/i IKEv2 określa wymagania co do algorytmów, grup Diffie-Hellmana, długości kluczy, itp.

<https://www.rfc-editor.org/rfc/rfc9206.txt>

Rekomendacje

Element	Rekomendacja NIST (SP 800-77r1)	Wymagania CNSA Suite (RFC 9206)
Protokół IKE	IKEv2 (RFC 7296) — preferowany IKEv1 — przestarzały	Wymagane IKEv2
Szyfrowanie	AES-128/192/256 (zalecany AES-256)	AES-256 w trybie GCM (AEAD) lub CBC
Integralność	SHA-256, SHA-384, SHA-512	SHA-384 (minimum), SHA-512 dopuszczalne
Grupy DH/ECDH	≥ 2048-bit MODP (DH Group 14) lub lepsze, P-256/384	MODP 3072+, preferowane P-384 (ECDH)
PRF (IKE)	HMAC-SHA-256 lub mocniejsze	HMAC-SHA-384
Klucze sym.	Minimum 128 bitów, preferowane 256 bitów	256 bitów (AES-256)
Uwierzytelnianie	Certyfikaty X.509, EAP z silnym hashem	Certyfikaty X.509 z SHA-384+

IPSec IKEv2 w RouterOS 7



IKEv2 w RouterOS 7

Pula adresów – definiujemy zakres adresów IP, które będą automatycznie przydzielane klientom VPN po nawiązaniu połączenia.

The screenshot shows the 'Pools' configuration window for 'pool-ikev2'. The 'Comment' field is empty. The 'Name' field is 'pool-ikev2'. The 'Addresses' field contains the range '172.16.1.2-172.16.1.254'. The 'Next Pool' dropdown is set to 'none'. The 'Total' is 253, 'Used' is 0, and 'Available' is 253. On the right, there are 'Copy' and 'Remove' buttons. At the bottom are 'Cancel', 'Apply', and 'OK' buttons.

Mode-Config – definiuje pulę adresów, trasy (***Split Include***) oraz opcjonalnie adres serwera DNS, które będą przekazywane klientowi po zestawieniu tunelu.

The screenshot shows the 'Mode Configs' configuration window for 'cfg-ikev2'. The 'Name' field is 'cfg-ikev2'. The 'Responder' checkbox is checked. The 'Address Pool' dropdown is set to 'pool-ikev2'. The 'Address' field has a '+' button. The 'Address Prefix Length' is 32. The 'Split Include' field contains '0.0.0.0/0'. The 'Split DNS' field has a '+' button. The 'System DNS' checkbox is unchecked. The 'Static DNS' field contains '8.8.8.8'. On the right, there are 'Copy' and 'Remove' buttons. At the bottom are 'Cancel', 'Apply', and 'OK' buttons.

IKEv2 w RouterOS 7

The 'Profiles' window shows the configuration for 'profile-ikev2'. It includes fields for Name, Hash Algorithms (sha256), PRF Algorithms (auto), Encryption Algorithm (aes-128, aes-256, 3des), DH Group (modp1024, modp1536, modp2048, ecp256), Proposal Check (obey), Lifetime (1d 00:00:00), Lifebytes (+), NAT Traversal (checked), DPD Interval (120), and DPD Maximum Failures (5). Buttons for Copy, Remove, Cancel, Apply, and OK are visible.

Profile IPsec – to zestaw parametrów używanych w **fazie 1 (IKE)** podczas negocjacji tunelu. Określają m.in. algorytmy szyfrowania, uwierzytelniania i wymiany kluczy

The 'Proposals' window shows the configuration for 'proposal-ikev2'. It includes fields for Enabled (checked), Name (proposal-ikev2), Auth. Algorithms (sha1, sha256), Encr. Algorithms (3des, aes-128 cbc, aes-256 cbc), Lifetime (00:30:00), and PFS Group (none). Buttons for Copy, Remove, Cancel, Apply, and OK are visible.

Proposal IPsec – to ustawienia dla **fazy 2**, które definiują sposób szyfrowania i uwierzytelniania ruchu danych w tunelu. Określają algorytmy używane do ochrony faktycznej transmisji po zestawieniu sesji IKE.

IKEv2 w RouterOS 7

The screenshot shows the 'Policies' configuration window in RouterOS 7. The title bar indicates the path 'Policies > 0.0.0.0/0->172.16.1.0/24'. The 'General' tab is active. The 'Enabled' checkbox is checked. The 'Comment' field is empty. The 'Src. Address' is '0.0.0.0/0' and the 'Dst. Address' is '172.16.1.0/24'. The 'Protocol' is set to '255 (all)'. The 'Template' checkbox is checked, and the 'Group' is set to 'group-ikev2'. On the right, there are 'Copy' and 'Remove' buttons. At the bottom, there is a green 'TEMPLATE' button and 'Cancel', 'Apply', and 'OK' buttons.

Ustawienia IPsec template policy z wyżej dodaną fazą 2

Jako Dst. Address podajemy podsieć, w której będą się znajdować nasze klienci.

The screenshot shows the 'Policies' configuration window in RouterOS 7, with the 'Action' tab active. The 'Action' is set to 'encrypt', 'IPsec Protocols' is 'esp', and 'Proposal' is 'proposal-ikev2'. On the right, there are 'Copy' and 'Remove' buttons. At the bottom, there is a green 'TEMPLATE' button and 'Cancel', 'Apply', and 'OK' buttons.

The screenshot shows the 'Groups' configuration window in RouterOS 7. The title bar indicates the path 'Groups > group-ikev2'. The 'Name' field is 'group-ikev2'. On the right, there are 'Copy' and 'Remove' buttons. At the bottom, there are 'Cancel', 'Apply', and 'OK' buttons.

Dodanie PFS group – Perfect Forward Secrecy (PFS) zapewnia, że każda sesja VPN ma swój unikalny klucz wymiany, niezależny od poprzednich.

Dzięki temu nawet w przypadku kompromitacji jednego klucza nie można odszyfrować wcześniejszej ani przyszłej komunikacji.

IKEv2 w RouterOS 7

The screenshot shows the 'Certificates' configuration window in RouterOS 7. The window has a title bar with a gear icon, the text 'Certificates > vpn.mbum-gdn.online', and window control buttons. Below the title bar are three tabs: 'General' (selected), 'Key Usage', and 'Status'. The 'General' tab contains the following fields: 'Name' (vpn.mbum-gdn.online), 'Issuer' (C=US, O=Let's Encrypt, CN=R12), 'Country', 'State', 'Locality', 'Organization', 'Unit', 'Common Name' (vpn.mbum-gdn.online), 'Subject Alt. Name' (DNS : vpn.mbum-gdn.onlii), 'Key Type' (RSA), 'Key Size' (2048), 'Days Valid' (89), and 'Trusted' (checkbox). To the right of these fields is an 'Actions' panel with buttons: 'Copy', 'Remove', 'Sign', 'Sign via SCEP', 'Create Cert. Request', 'Import', 'Card Reinstall', 'Card Verify', 'Export', and 'Revoke'. At the bottom of the window are three buttons: 'PRIVATE KEY' (green), 'Cancel' (grey), and 'Apply' (blue). The 'OK' button is also blue.

Za pomocą polecenia uruchamiamy proces uzyskania certyfikatu z Let's Encrypt dla wskazanej domeny.

```
/certificate/enable-ssl-certificate\  
  dns-name=vpn.mbum-gdn.online
```

Wymagana jest dostępna i poprawnie skonfigurowana nazwa domenowa dla danego hosta (record A lub AAAA).

Rekomendowaną praktyką jest zmiana domyślnej nazwy certyfikatu na bardziej czytelną — np. zgodną z nazwą domenową routera.

IKEv2 w RouterOS 7

The screenshot shows the 'Peers' configuration window for 'peer-ikev2'. The window has a title bar with a menu icon, 'Peers > peer-ikev2', and window control buttons. The main area contains the following fields and controls:

- Enabled:** A checked checkbox.
- Comment:** An empty text input field.
- Name:** A text input field containing 'peer-ikev2'.
- Address:** A text input field containing '::/0' with a minus button to its right.
- Port:** A text input field with a plus button to its right.
- Local Address:** A text input field with a plus button to its right.
- Profile:** A dropdown menu showing 'profile-ikev2'.
- Exchange Mode:** A dropdown menu showing 'IKE2'.
- Passive:** A checked checkbox.
- Send INITIAL_CONTACT:** A checked checkbox.
- Buttons:** 'Copy' (with a document icon), 'Remove' (with an 'x' icon), 'RESPONDER' (green), 'Cancel' (grey), 'Apply' (blue), and 'OK' (blue).

Peer definiuje parametry połączenia (adres, profil kryptograficzny, tryb IKE2).

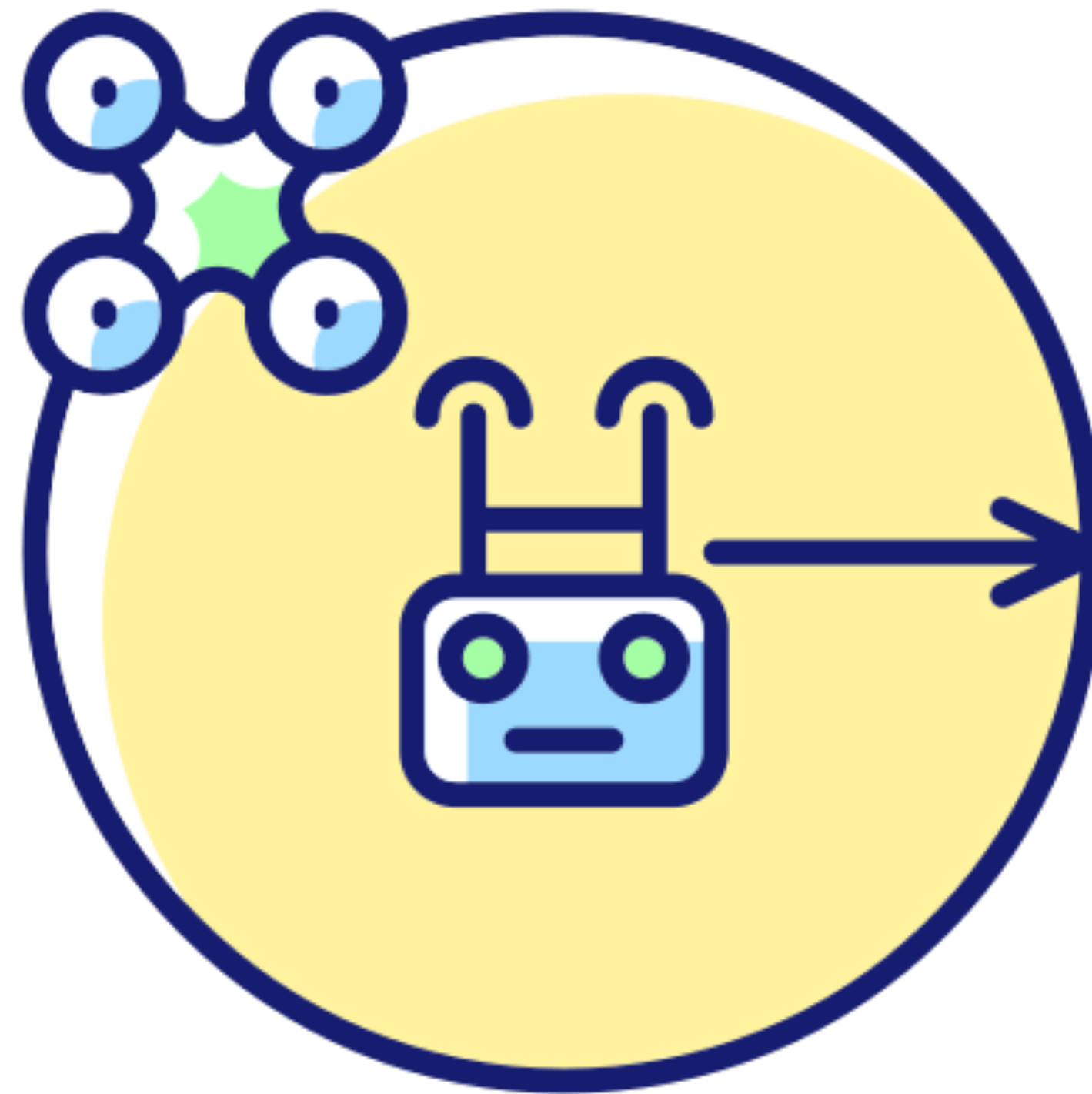
Identity określa metodę uwierzytelniania (EAP RADIUS) oraz certyfikat serwera (np. Let's Encrypt).

Dzięki temu klient rozpoznaje i ufa serwerowi, a logowanie odbywa się z wykorzystaniem RADIUS

The screenshot shows the 'Identities' configuration window for 'peer-ikev2'. The window has a title bar with a menu icon, 'Identities > peer-ikev2', and window control buttons. The main area contains the following fields and controls:

- Enabled:** A checked checkbox.
- Comment:** An empty text input field.
- Peer:** A dropdown menu showing 'peer-ikev2'.
- Auth. Method:** A dropdown menu showing 'eap radius'.
- Certificate:** A dropdown menu showing 'vpn.mbum-gdn.online' with minus and plus buttons to its right.
- Policy Template Group:** A dropdown menu showing 'group-ikev2'.
- Notrack Chain:** A dropdown menu.
- My ID Type:** A dropdown menu showing 'auto'.
- Remote ID Type:** A dropdown menu showing 'auto'.
- Match By:** A dropdown menu showing 'remote id'.
- Mode Configuration:** A dropdown menu showing 'cfg-ikev2' with a minus button to its right.
- Generate Policy:** A dropdown menu showing 'port strict'.
- Buttons:** 'Copy' (with a document icon), 'Remove' (with an 'x' icon), 'Cancel' (grey), 'Apply' (blue), and 'OK' (blue).

Remote Authentication Dial In User Service



User-manager w RouterOS 7

Package List

Packages

Local Update Packages

Local Package Sources

Find

Filter

		Name	Installed	Version	Build Time	Scheduled	Size
☐	XA	calea	no				24.1 KiB
☐	XA	container	no				152.1 KiB
☐	XA	dude	no				1396.1 KiB
☐	XA	gps	no				20.1 KiB
☐	XA	iot	no				548.1 KiB
☐	XA	lora	no				8.1 KiB
☐	XA	rose-storage	no				3496.1 KiB
☐		routeros	yes	7.19.4	2025-07-28 10:00:16		18.6 MiB
☐	XA	tr069-client	no				152.1 KiB
☐	XA	ups	no				36.1 KiB
☒	XA	user-manager	no				408.1 KiB
☐	XA	wireless	no				1148.1 KiB

12 1 Live

Actions

Enable

Disable

Uninstall

Unschedule

Apply Changes

Downgrade

Configuration

Check For Updates

Check Installation

Package List

Packages

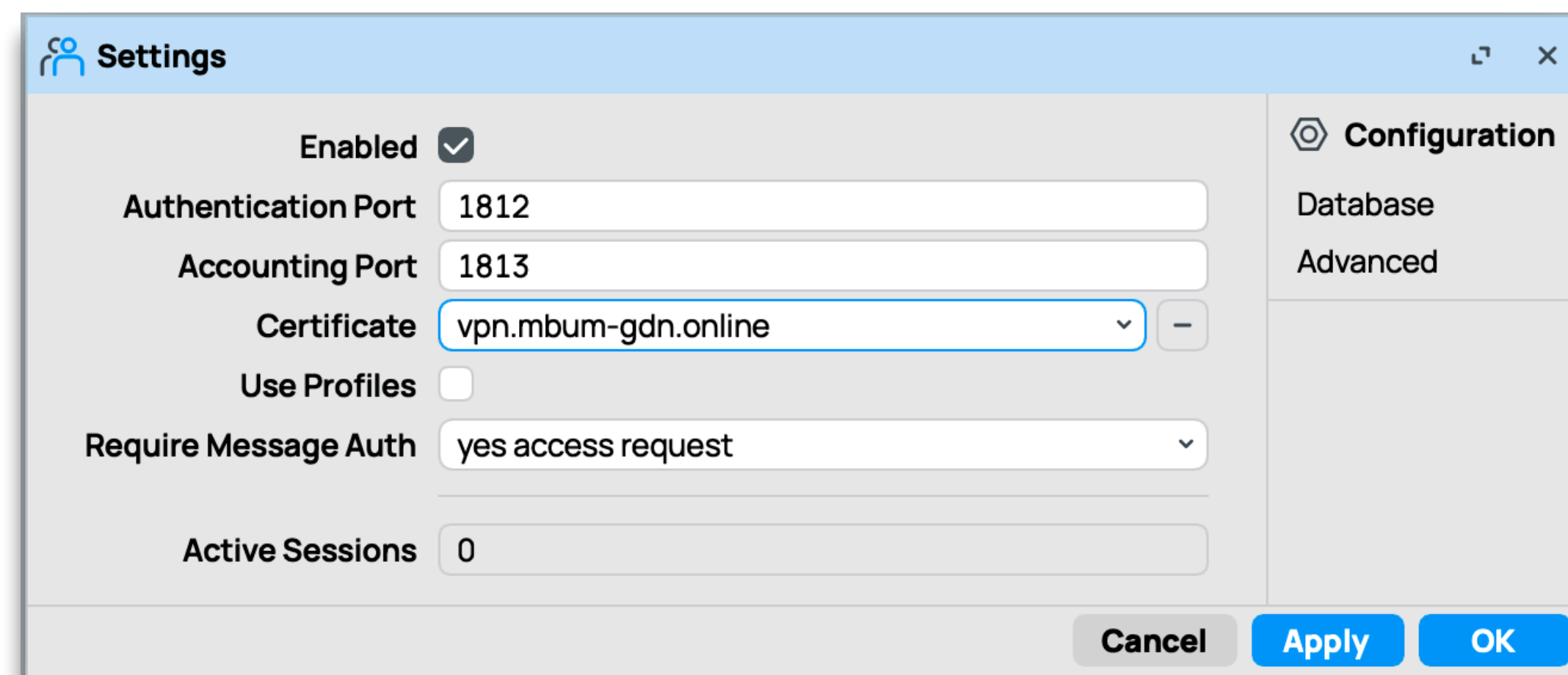
Local Update Packages

Local Package Sources

		Name	Installed	Version	Build Time	Scheduled
☐		routeros	yes	7.19.4	2025-07-28 10:00:16	
☐		user-manager	yes	7.19.4	2025-07-28 10:00:16	

Aby zainstalować pakiet User Manager, należy go aktywować na liście pakietów za pomocą *Enable*, a następnie zatwierdzić wybór poprzez *Apply Changes*.

IKEv2 w RouterOS 7

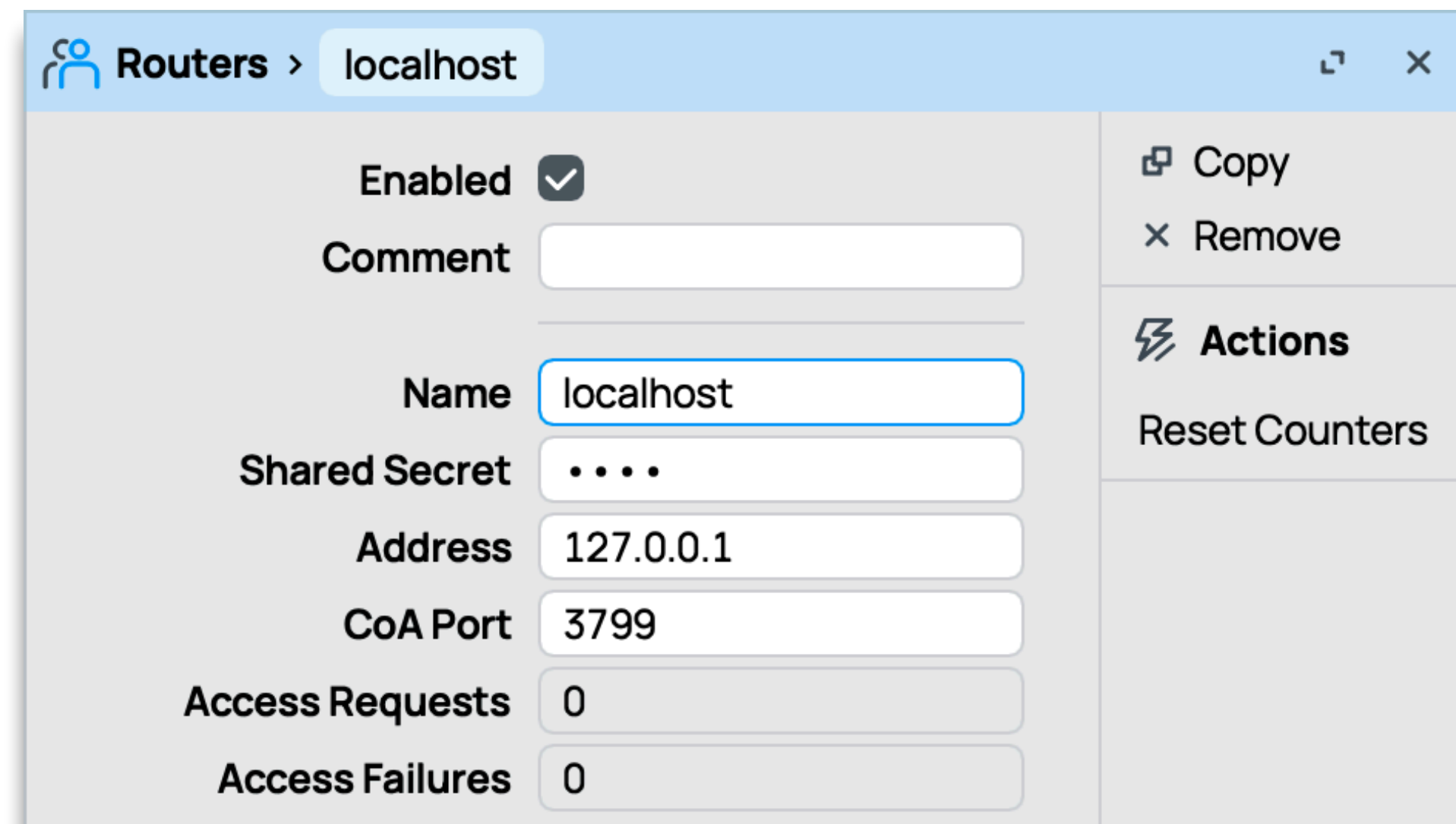


Uruchamiamy serwer RADIUS i przypisujemy do niego wcześniej wygenerowany certyfikat.

Certyfikat jest niezbędny, ponieważ w metodach EAP (np. EAP-MSCHAPv2 w IKEv2) serwer musi potwierdzić swoją tożsamość wobec klienta i zestawić bezpieczny tunel TLS dla przekazania danych logowania.

W skrócie: bez certyfikatu klient nie zaufa serwerowi i autoryzacja EAP nie zadziała.

IPsec w RouterOS 7

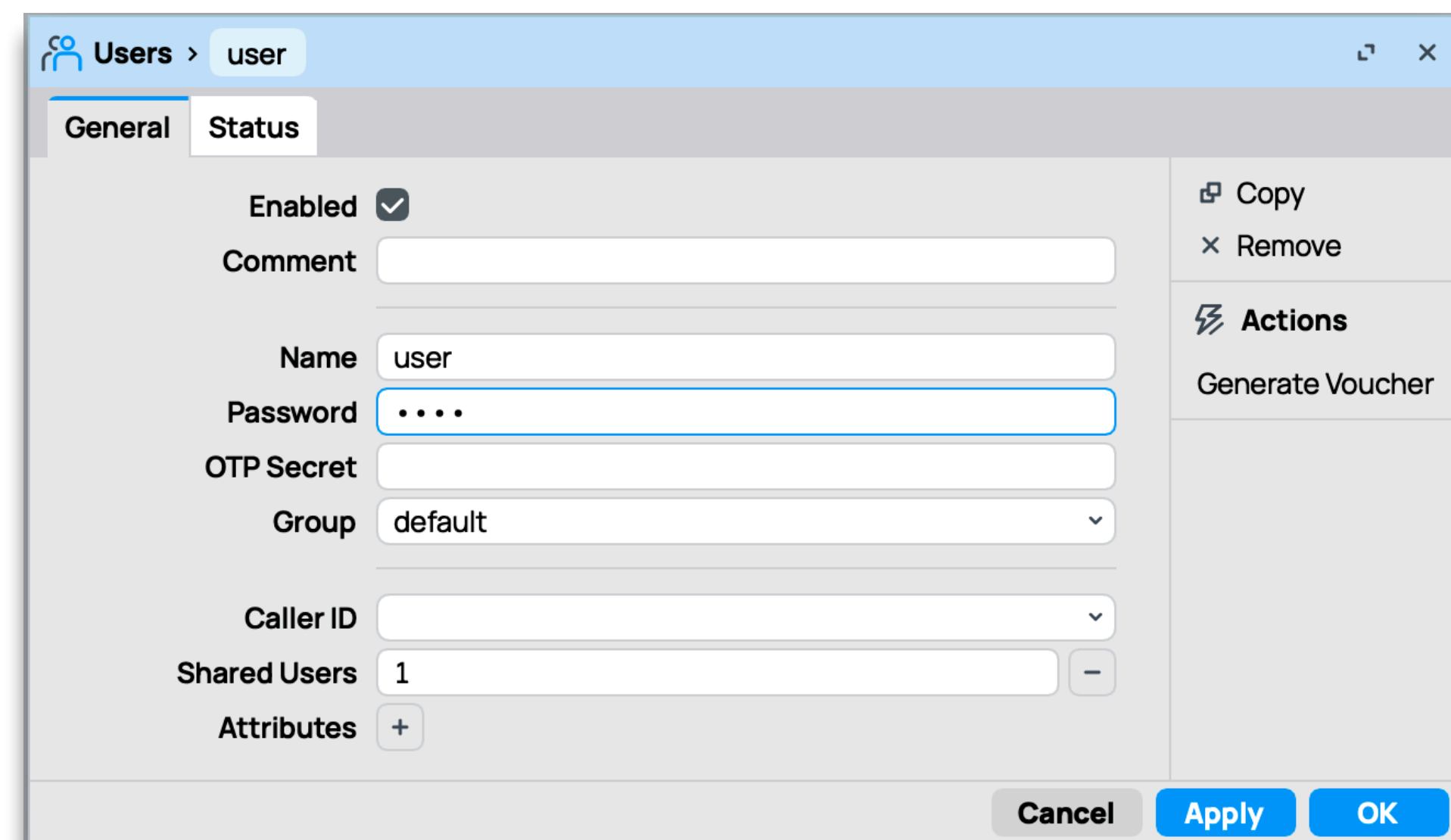


The screenshot shows the 'Routers' configuration window in RouterOS User Manager. The window title is 'Routers > localhost'. The configuration is as follows:

Field	Value
Enabled	☒
Comment	
Name	localhost
Shared Secret	
Address	127.0.0.1
CoA Port	3799
Access Requests	0
Access Failures	0

On the right side, there are buttons for 'Copy' and 'Remove', and an 'Actions' section with a 'Reset Counters' button.

W User Manager dodajemy wpis localhost jako router z adresem (127.0.0.1) ze wspólnym sekretem.



The screenshot shows the 'Users' configuration window in RouterOS User Manager. The window title is 'Users > user'. The 'General' tab is selected. The configuration is as follows:

Field	Value
Enabled	☒
Comment	
Name	user
Password	
OTP Secret	
Group	default
Caller ID	
Shared Users	1
Attributes	+

On the right side, there are buttons for 'Copy' and 'Remove', and an 'Actions' section with a 'Generate Voucher' button. At the bottom, there are 'Cancel', 'Apply', and 'OK' buttons.

Następnie tworzymy użytkownika z hasłem

IKEv2 w RouterOS 7

The screenshot shows the RouterOS 7 configuration window for a RADIUS client with IP 127.0.0.1. The 'General' tab is active. The 'Enabled' checkbox is checked. The 'Service' section has 'ipsec' selected. The 'Address' is set to 127.0.0.1 and the 'Protocol' is set to 'udp'. The 'Authentication Port' is 1812, 'Accounting Port' is 1813, and 'Timeout' is 1100. The 'Secret' field is masked with dots. On the right, there are 'Copy' and 'Remove' buttons, and an 'Actions' section with a 'Reset Status' button.

Field	Value
Enabled	☒
Comment	
Service	☐ ppp ☐ login ☐ hotspot ☐ wireless ☐ dhcp ☒ ipsec ☐ dot1x
Called ID	+
Domain	+
Address	127.0.0.1
Protocol	☒ udp ☐ radsec
Secret	
Authentication Port	1812
Accounting Port	1813
Timeout	1100

W RouterOS dodajemy klienta RADIUS (w tym przypadku `127.0.0.1`) i określamy, do jakich usług będzie używany.

W tym przykładzie wybrano usługę *ipsec*, co oznacza, że logowanie do VPN IKEv2 będzie weryfikowane przez serwer RADIUS (User Manager).

MultiFactor Authentication



Klasyczny VPN / Potencjalne zagrożenia

Single password = single point of failure

- całe bezpieczeństwo opiera się na jednym hasle użytkownika;
- jeśli zostanie odgadnięte, skradzione lub wycieknięte → atakujący ma pełny dostęp.

Brute-force / dictionary attack

- możliwe ataki słownikowe lub siłowe na hasło, szczególnie przy słabych politykach haseł;
- brak dodatkowej warstwy zabezpieczenia.

Wycieki haseł

- użytkownicy często używają tych samych haseł w wielu usługach;
- jeśli hasło wycieknie z innej usługi, automatycznie zagrożony jest też VPN.

MFA (Multi-Factor Authentication)

- **= hasło + coś więcej**
- eliminuje pojedynczy punkt awarii
- zwiększa bezpieczeństwo dostępu do VPN

Najczęściej stosowane MFA

1. **Hasło + SMS** – powszechne, ale podatne na przechwycenie.
2. **Hasło + aplikacja TOTP** (Google/Microsoft Authenticator, FreeOTP) – najpopularniejsze rozwiązanie, dobra równowaga prostoty i bezpieczeństwa.
3. **Hasło + powiadomienie push** (Duo, Microsoft, Google) – wygodne, szybka autoryzacja.
4. **Hasło + biometria** (odcisk palca, Face ID) – często w urządzeniach mobilnych.
5. **Hasło + klucz sprzętowy** (U2F/FIDO2, np. YubiKey) – najwyższy poziom bezpieczeństwa.

TOTP (Time-based One-Time Password, RFC 6238)

- **= 6 cyfr generowanych co 30 sekund**
- kod ważny tylko w krótkim oknie czasowym
- używany np. w Google Authenticator, FreeOTP, RouterOS MFA

Podstawowa idea

- Jest klucz tajny (wspólny dla serwera i klienta)
- Jest czas (podzielony na interwały, zazwyczaj 30 sekund)
- Kod = funkcja (klucz, czas)
- Co 30 sekund → nowy kod

BASE32 encoding / RFC 4668

BASE32 – kodowanie krok po kroku

1. **Wejście:** dane binarne (ciąg bajtów).
2. **Podział na bloki:** dane dzielone są na grupy po **5 bitów**.
3. **Mapowanie:** każda 5-bitowa wartość jest zamieniana na znak z alfabetu:
 - A–Z (26 znaków)
 - 2–7 (6 znaków)
 - razem 32 symbole.
4. **Łączenie:** zakodowane znaki układają się w czytelny ciąg ASCII.
5. **Padding (=):** jeśli długość wejścia nie jest wielokrotnością 40 bitów, dodawane są znaki = aby wynik miał pełne bloki.

Przykład

- Dane wejściowe: HELLO
- Bity: 01001000 01000101 01001100 01001100 01001111
- Podział na 5 bitów → 01001 00001 00010 10100 11000 10011 00100 1111
- Kodowanie: JBSWY3DP

Przykład (z RFC 6238)

- Sekret (ASCII): 12345678901234567890
- Krok czasu: 30 sekund
- Algorytm: HMAC-SHA-1

Dla czasu $T = 59$ sekund (czas UNIX):

- Licznik = $\text{floor}(59 / 30) = 1$
- Obliczenie HMAC $\rightarrow$ wynik = 94287082
- Końcowy kod (6 cyfr) = **287082**

Aplikacje TOTP

TOTP Generator

Generate QR codes for Google Authenticator with live TOTP codes

Service Name:

Account/Email:

Secret/Password:

GDN-VPN

user

••••••••



1234

Live TOTP Code

856222

9 s

QR Code



 BASE32 Secret

GEZDGNBUGMZDC===



 How to use with Google Authenticator:

1. Open Google Authenticator app

2. Tap the "+" button

3. Select "Scan a QR code"

4. Scan the QR code on the left

5. Your TOTP codes will appear in the app!

 Verification:

The live code on the left should match your authenticator app exactly!

<https://mtik.pl/totp.html> — TOTP Generator

Google Authenticator

29

TOTP + RouterOS 7

Users > user

General Status

Enabled ☒

Comment

Name

Password

OTP Secret

Group

Caller ID

Shared Users

Attributes

Copy Remove

Actions

Generate Voucher

Cancel Apply OK

Dodajemy OTP Secret bez ustawiania hasła – w takim przypadku logowanie odbywa się wyłącznie za pomocą kodu TOTP.

Połączenie hasło + OTP zapewnia wyższy poziom bezpieczeństwa, ponieważ uwierzytelnianie składa się z dwóch elementów: części stałej (hasło znane tylko użytkownikowi) oraz części zmiennej (kod TOTP generowany co 30 sekund).

Users > user

General Status

Enabled ☒

Comment

Name

Password

OTP Secret

Group

Caller ID

Shared Users

Attributes

Copy Remove

Actions

Generate Voucher

Cancel Apply OK

Podsumowanie



KEv2 + Let's Encrypt + User Manager + TOTP = proste MFA

- **IKEv2** – nowoczesny, bezpieczny protokół VPN (NSA/NIST compliant)
- **Let's Encrypt** – darmowe certyfikaty X.509, automatyzacja SSL/TLS
- **User Manager (RADIUS)** – centralne uwierzytelnianie użytkowników
- **TOTP** – jednorazowe kody 6-cyfrowe co 30 sekund (RFC 6238)

All-in-one solution

- Całość działa na **RouterOS**
- Bez potrzeby stawiania **zewnętrznych serwerów**
- MFA dostępne natywnie, z prostą konfiguracją

Podsumowanie dla 'spóźnialskich' i nie obecnych



<https://youtu.be/PmiwcX0gtS0>

Dziękuję



mtik.pl



ihor@hreskiv.pl



<https://github.com/hreskiv>



<https://www.youtube.com/@mikrotikpolska>