IPSEC z Mikrotik – zero to hero

Piotr Wasyk
piotr@mwtc.pl

MBUM #3
25/01/2019
Kraków
Mikrotik Beer User Meeting

O mnie

MTCNA MTCRE MTCWE MTCIPv6E MTCINE MTCTCE

piotr@mwtc.pl

W IT od ponad 13 lat. Absolwent Politechniki Warszawskiej oraz studiów podyplomowych z zakresu zarządzania projektami IT.
Na co dzień zajmuje się administracją i zarządzaniem:

- *infrastrukturą serwerową,*
- *centralami VoIP,*
- *sieciami WLAN (Mikrotik i Ubiquiti),*
- *siecią LAN,*
- *tunelami VPN,*
- *QoS,*
- *monitorowaniem usług*

mwtc | MikroTik Warsaw Training Center

Współwłaściciel największego centrum szkoleniowego Mikrotik w Polsce - MikroTik Warsaw Training Center

Największe centrum szkoleniowe Mikrotik w Polsce

Ul. Ogrodowa 58, Warszawa

- Centrum Warszawy
- Bliskość dworca kolejowego

- Komfortowe klimatyzowane sale szkoleniowe

Michał Filipek, Mikrotik Warsaw Training Center

Rating: ★★★★★ 4.9/5 (312 votes)

Average student result: 87%

MTCNA, MTCRE, MTCWE, MTCTCE, MTCINE, MTCIPv6E

Warsaw, Poland

Tel: +48 796 171 971

Agenda

- Czym jest IPSEC, czy naprawdę jest tak skomplikowany?
- IPSEC, a firewall
- Połączenie site-site
  - IPSEC
  - IPIP + IPSEC
- Użytkownicy mobilni
  - L2TP+IPSEC
  - IPSEC XAuth

IPSec

- IPSec – Internet Protocol Security, to **zestaw** protokołów wspierających bezpieczną komunikację w warstwie IP
- W założeniu powstał dla IPv6. W związku z wolną implementacją IPv6, został także zaadoptowany do użycia z IPv4
- Zapewnia szyfrowanie i integralność danych w warstwie IP

Integralność – suma kontrolna zabezpieczona kryptograficznie.

Poufność – poprzez szyfrowanie z wykorzystaniem jednego z algorytmów blokowych np. *DES*, 3DES, AES

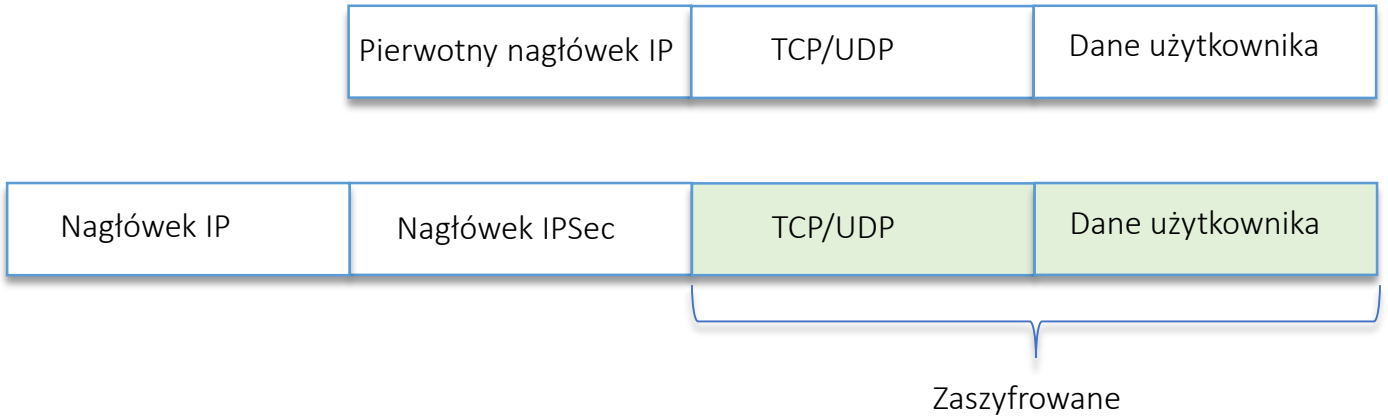
IPSec

- Możliwe jest zastosowanie kilku podejść do wykorzystania IPSec
  - AH – ***Authentication Header***
  - ESP – ***Encapsulating Security Payload***
  - AH + ESP

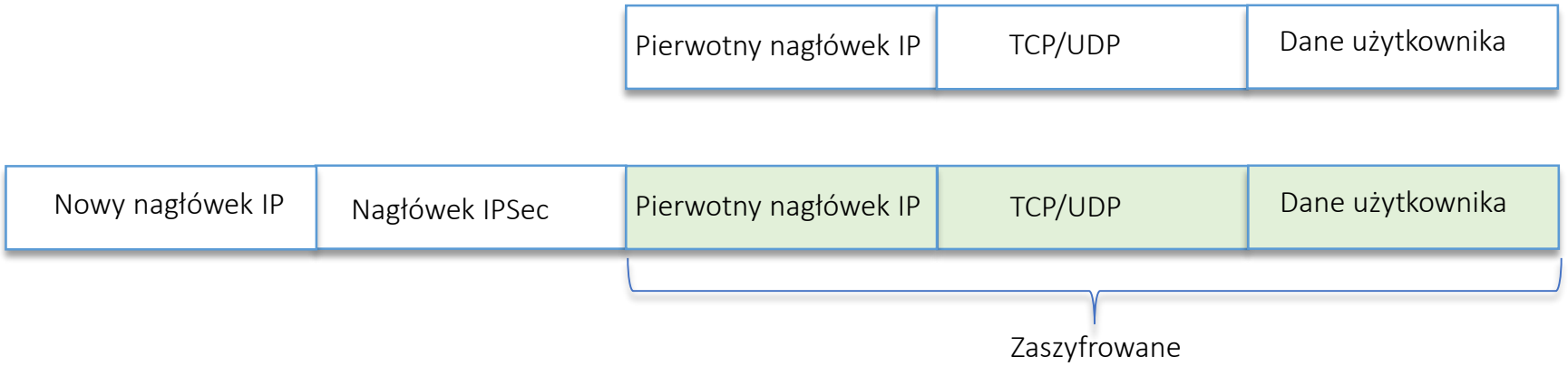
  Obecnie najczęściej stosowanym podejściem jest **ESP**

- Tunele IPSec można ustanowić w dwóch trybach
  - Transport
  - Tunnel

Tryb transportowy – nagłówek IPsec jest wstawiany pomiędzy oryginalny nagłowek IP, a nagłówek warstwy transportowej. Zwykle wykorzystywany do połączenia dwóch hostów z wykorzystaniem IPSec.

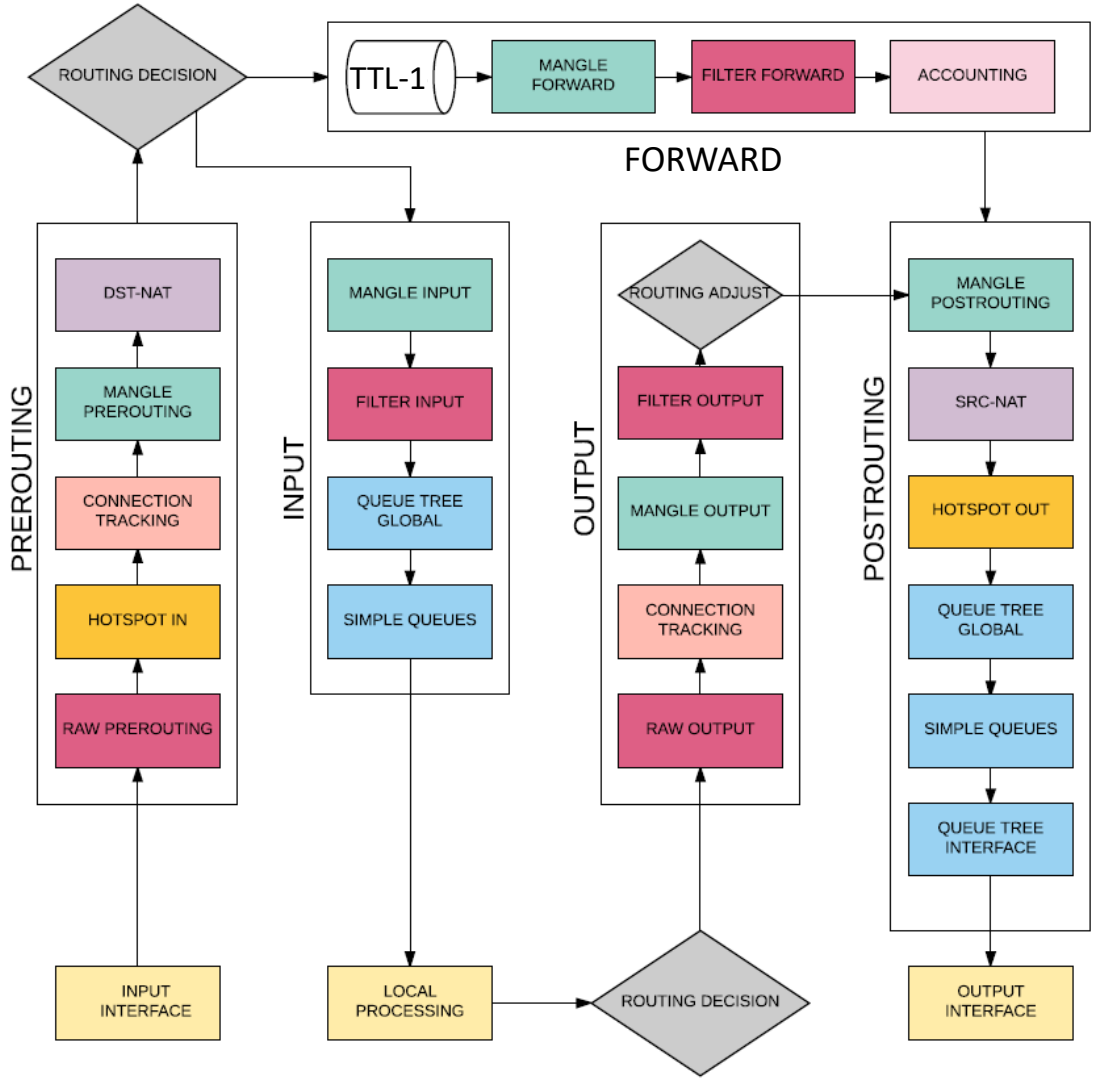


Tryb tunelowy – cały pierwotny pakiet IP jest enkapsulowany wewnątrz nagłówka IPSec. Jest stosowany do połączeń site-site.



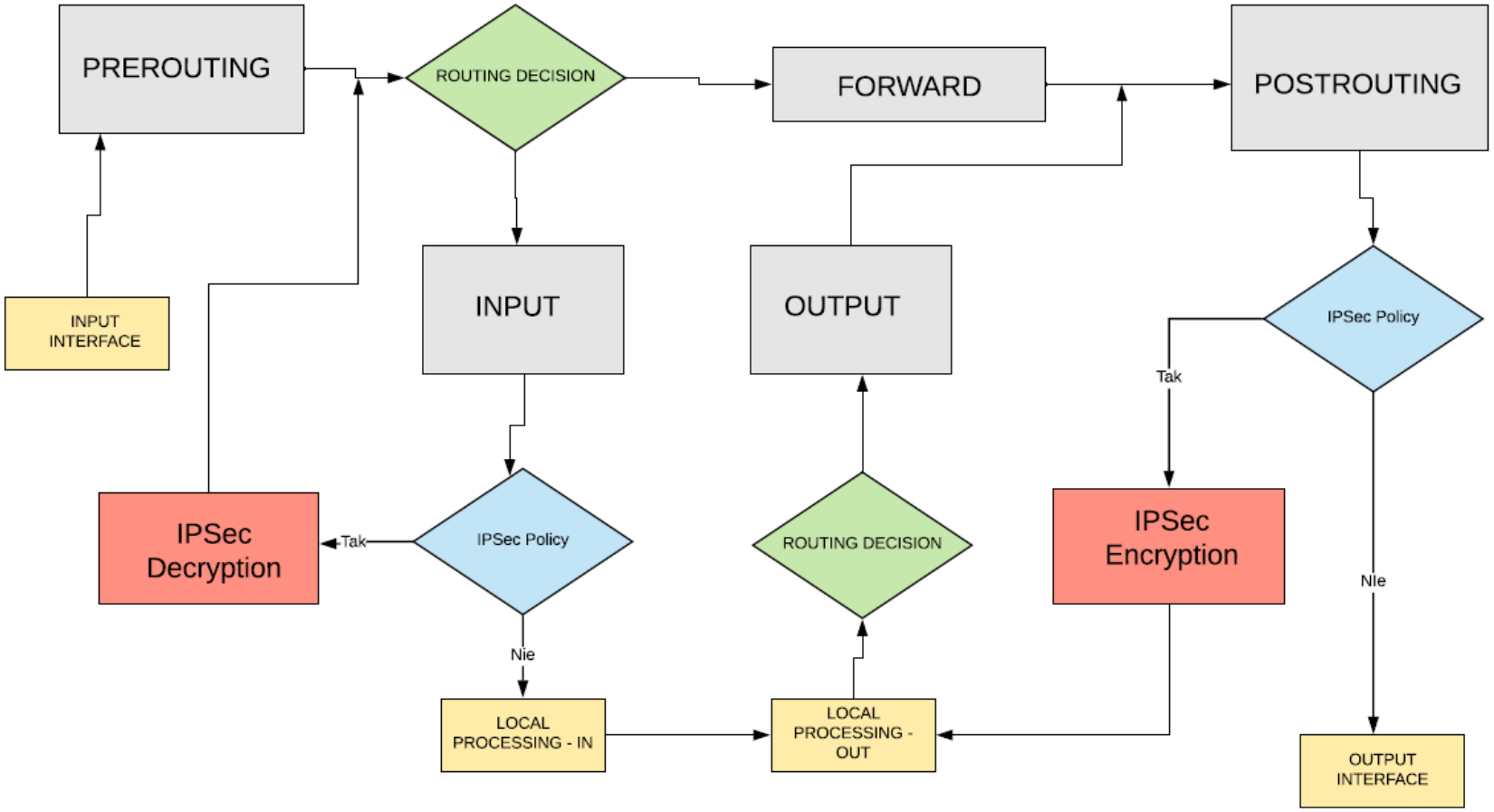
Firewall

Packet Flow



IPSec

Packet flow



IP -> Firewall -> Filter

/ip firewall filter

add action=accept chain=input dst-port=500 protocol=udp
add action=accept chain=input dst-port=4500 protocol=udp
add action=accept chain=input protocol=ipsec-esp

Potrzebne dla IKE

Jeśli korzystamy w NAT-Traversal

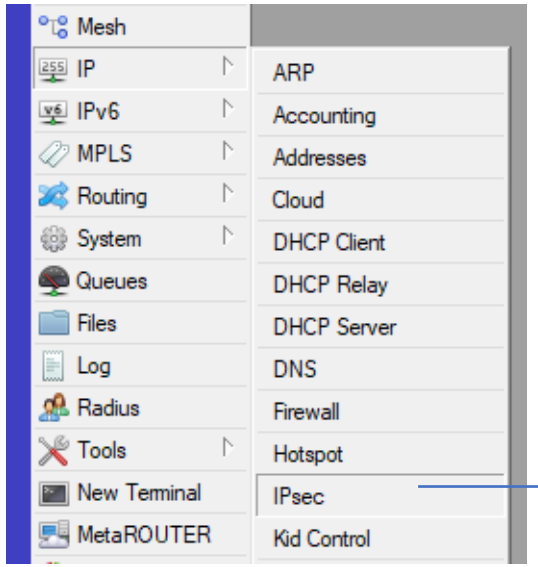
Alternatywnie i/lub AH. Zalecanej jest wykorzystywanie jedynie ESP

IKE - Internet Key Exchange

Odpowiedzialny za automatyczną negocjację parametrów połączenia:

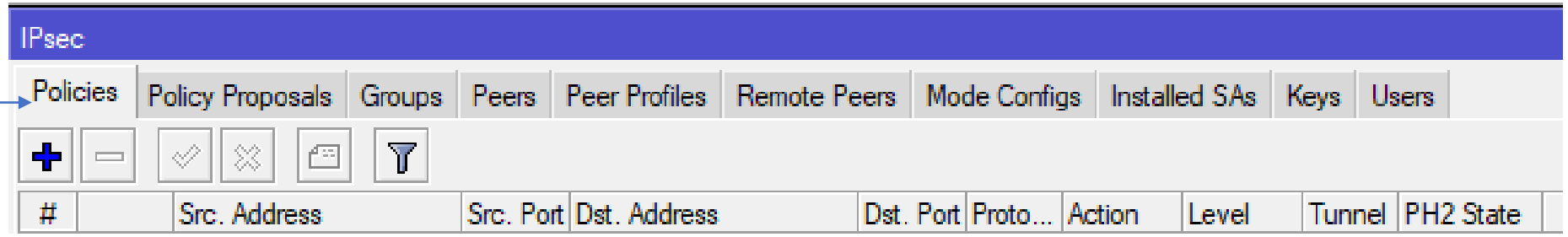
- Uwierzytelnienie
- Utworzenie kanału ISAKMP
- Ustalenie relacji SA
- Uzgadnianie kluczy kryptograficznych

Składa się z dwóch faz:



ISAKMP (Internet Security Association and Key Management Protocol) – odpowiada za uwierzytelnienie, utworzenie kanału ISAKMP (jeden dwukierunkowy kanał), zarządzanie kanałem ISAKMP

Oakley – odpowiedzialna za ustanawianie SA (jednokierunkowe kanały wykorzystywane do transmisji zaszyfrowanych danych. (Security Association). Jest zabezpieczona poprzez wynik działania fazy 1.



ISAKMP – Faza 1

ISAKMP (Internet Security Association and Key Management Protocol) –

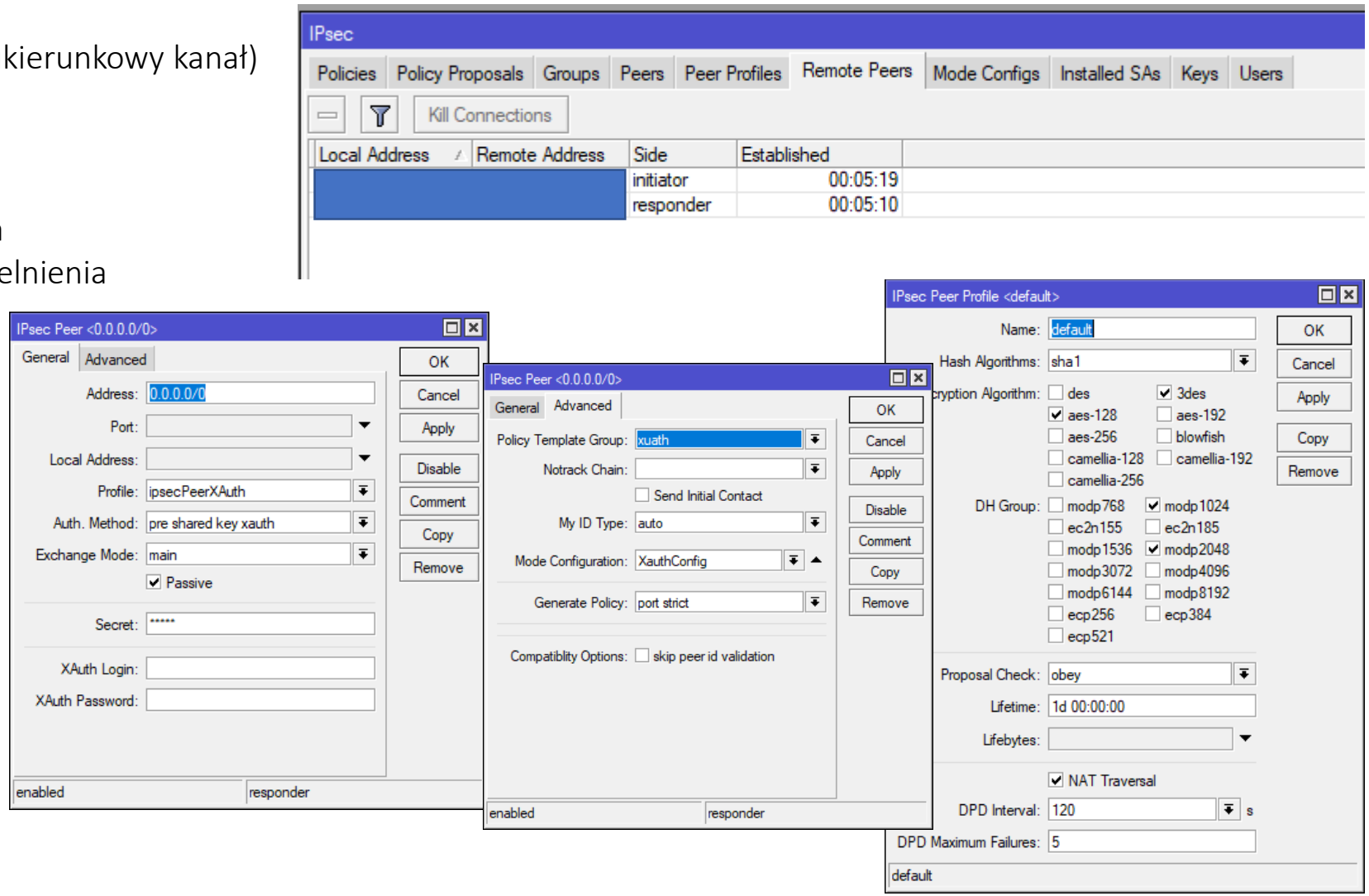
- odpowiada za uwierzytelnienie
- utworzenie kanału ISAKMP(jeden dwukierunkowy kanał)
- zarządzanie kanałem ISAKMP

Peer(y) wymieniają ze sobą informacje o:

- Wspieranych algorytmach szyfrowania
- Wpieranych algorytmach dla uwierzytelnienia
- Wspieranych DH-group
- Współdzielony klucz

Uwierzytelnienie może być realizowane za pomocą:

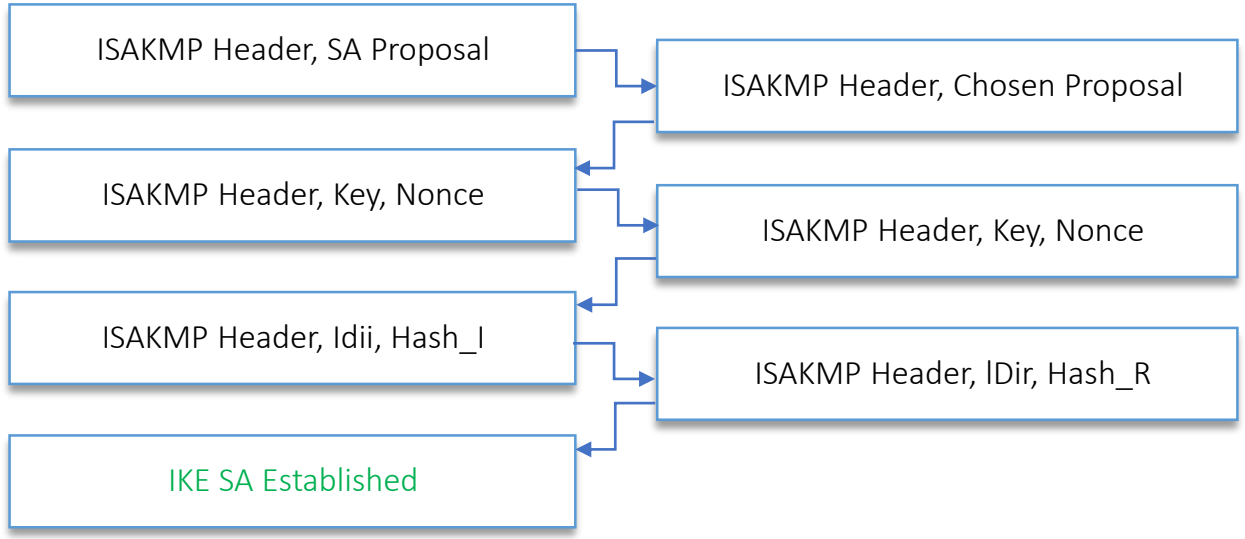
- Współdzielonego hasła
- Podpis RSA
- X.509
- Kerberos



ISAKMP – Faza 1

Tryb normalny (main mode)

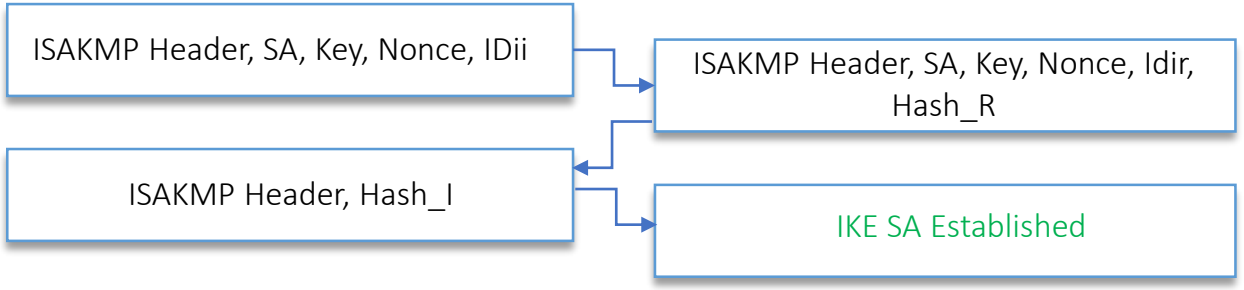
- Wymienianych jest 6 komunikatów
- Wolniejszy
- Bardziej bezpieczny, można stosować bez względu na metodę uwierzytelniania



Tryb agresywny (aggresive mode)

- Wymieniane są 3 komunikaty
- Szybszy

Z racji, że część informacji jest wymieniana zanim ustanowiony zostanie bezpieczny kanał, możliwe jest podsłuchanie skrótu PSK i przeprowadzenie ataku słownikowego. Złamanie PSK pozwoli na podszycie się pod użytkownika.

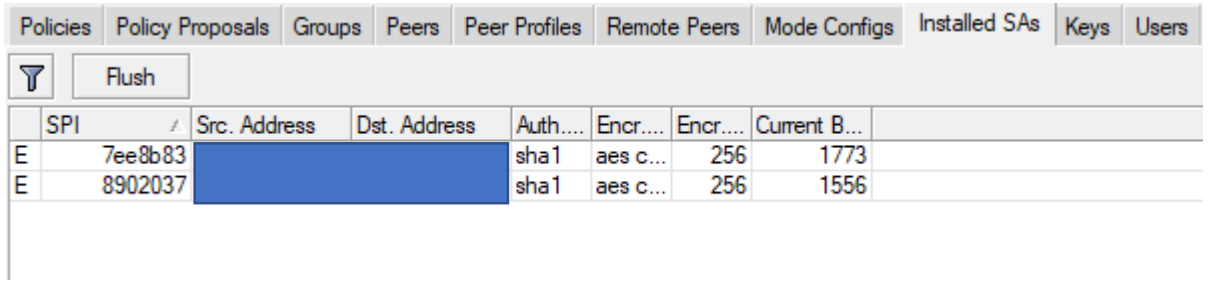


Nie zalecane:

- dla zdalnych połączeń z nieznanych adresów IP
- Przy stosowaniu PSK

Oakley – faza 2

Faza 2 następuje po poprawnym zakończeniu fazy 1 i jest przez nią zabepieczona.
W związku z tym nie ma konieczności przeprowadzenia uwierzytelnienia, a dane przesyłane w jej trakcie są bezpieczne.

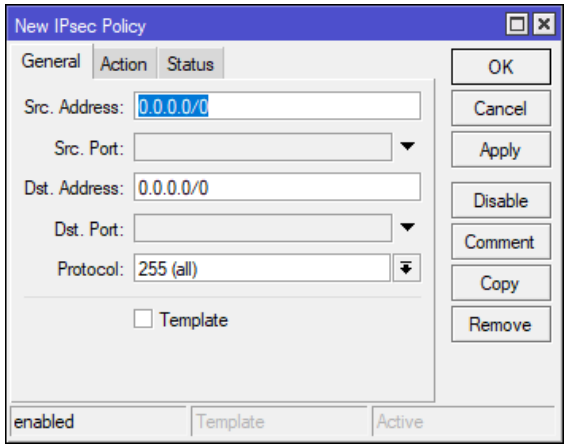


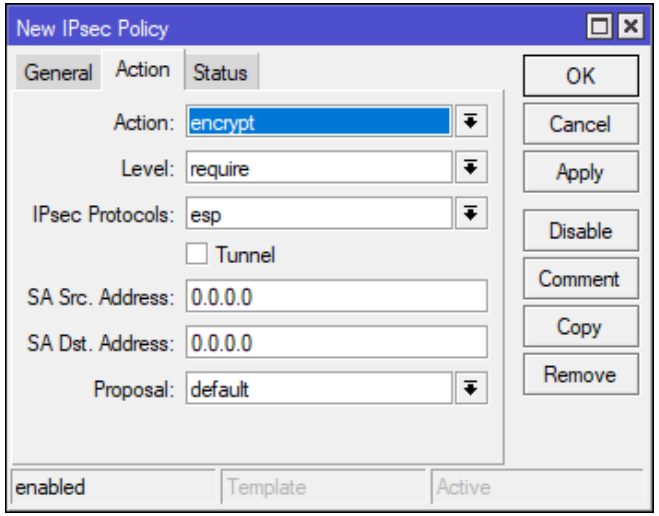
Jej zadaniem jest:

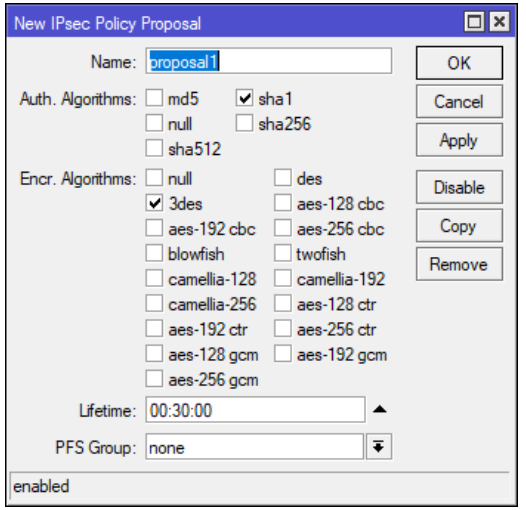
- Uzgadnianie kluczy wg algorytmu DH
- Uzgadnianie IPsec SA

Podczas fazy 2 uczestnicy przesyłają analogicznie jak w fazie 1 informacje dotyczące wymagań bezpieczeństwa dla tworzonych kanałów SA.

AH / ESP / AH+ESP



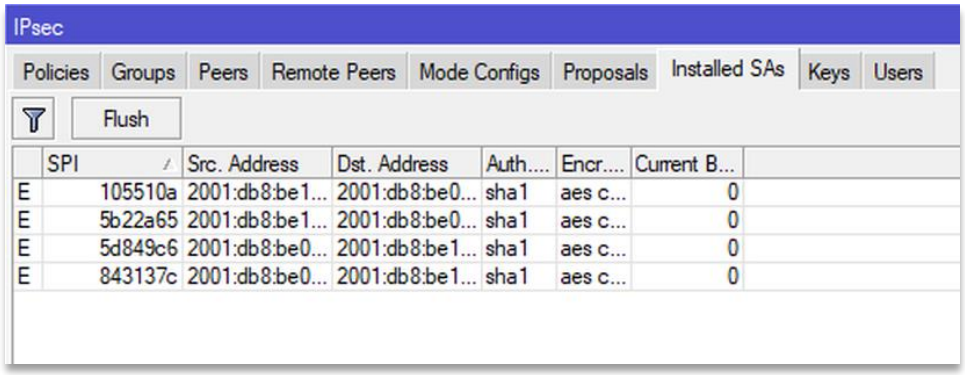




Zawsze przebiega w trybie Aggressive

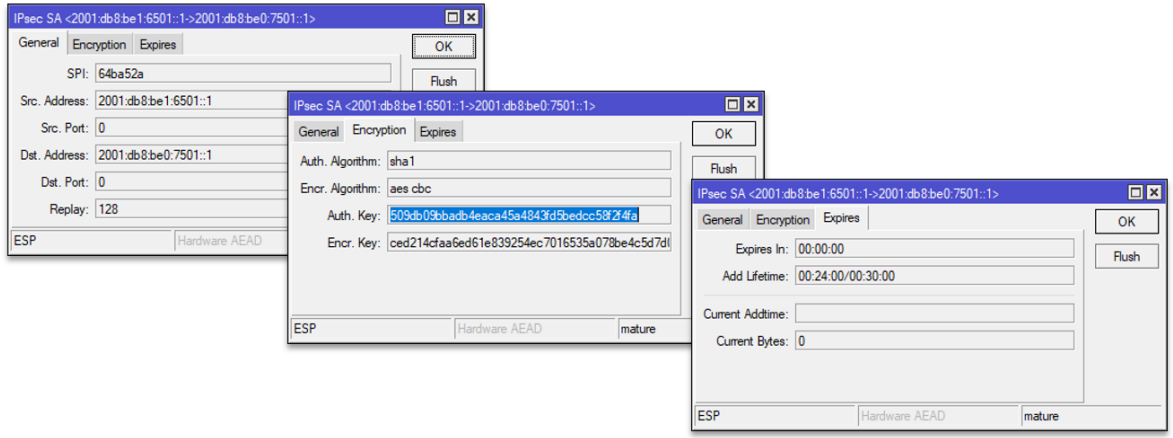
IPsec Security Association (SA)

To **jednokierunkowy** kanał do przesyłania danych pomiędzy nadawcą i odbiorcą.



Baza SAD – Security Association Database

Baza przechowywana przez każdą ze stron o nawiązanych SA. Zawiera informacje o nawiązanych Security Association



Baza SPD - Security Policy Database

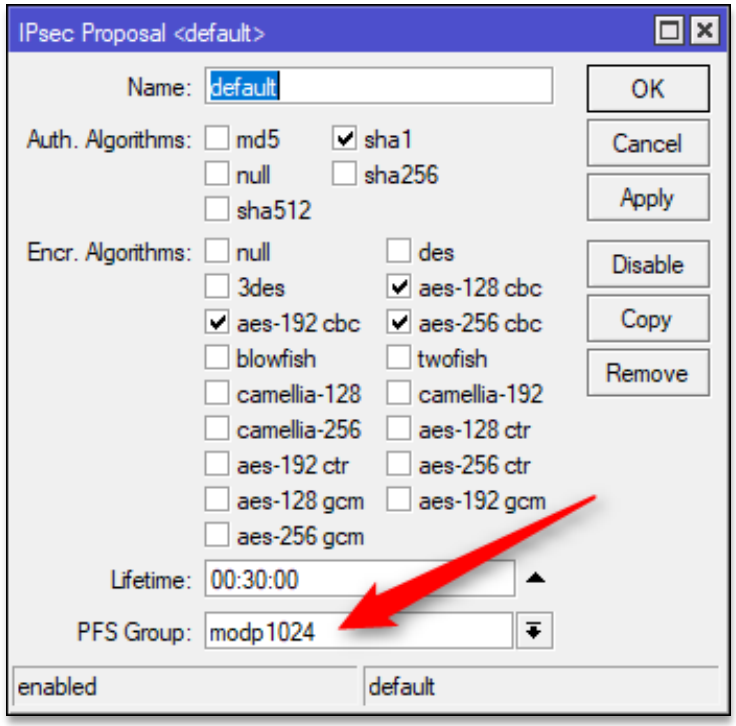
- Jest wykorzystywana do pakietów wychodzących
- System sprawdza, czy dla ruchu do określonego hosta ma korzystać z IPsec

- jeśli tak, to przeglądana jest SAD w poszukiwaniu odpowiedniego SA

PFS – Perfect Forward Secrecy

Mechanizm PFS zapewnia, że materiał klucza głównego jest wykorzystywany tylko raz, do generacji klucza sesji. Za każdym razem, gdy należy wygenerować klucz sesji, przed tym procesem jest przeprowadzana wymiana kluczy (z wykorzystaniem algorytmu Diffiego-Hellmana) celem ustanowienia nowego materiału klucza głównego.

- zwiększa bezpieczeństwo
- podnosi zużycie CPU
- nie każde urządzenie wspiera PFS



IPSEC a NAT

AH

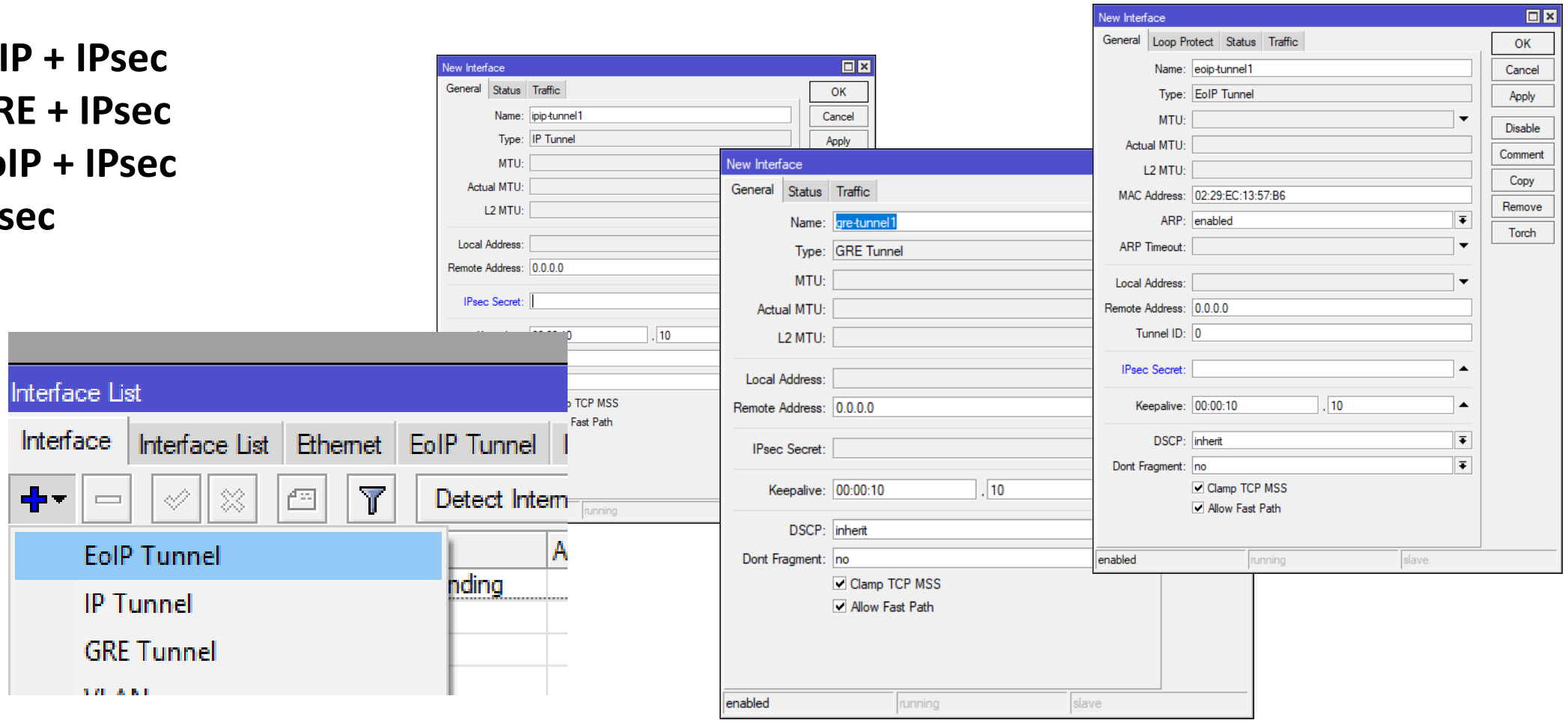
Brak wsparcia dla NAT – cały nagłówek jest zabezpieczony

ESP

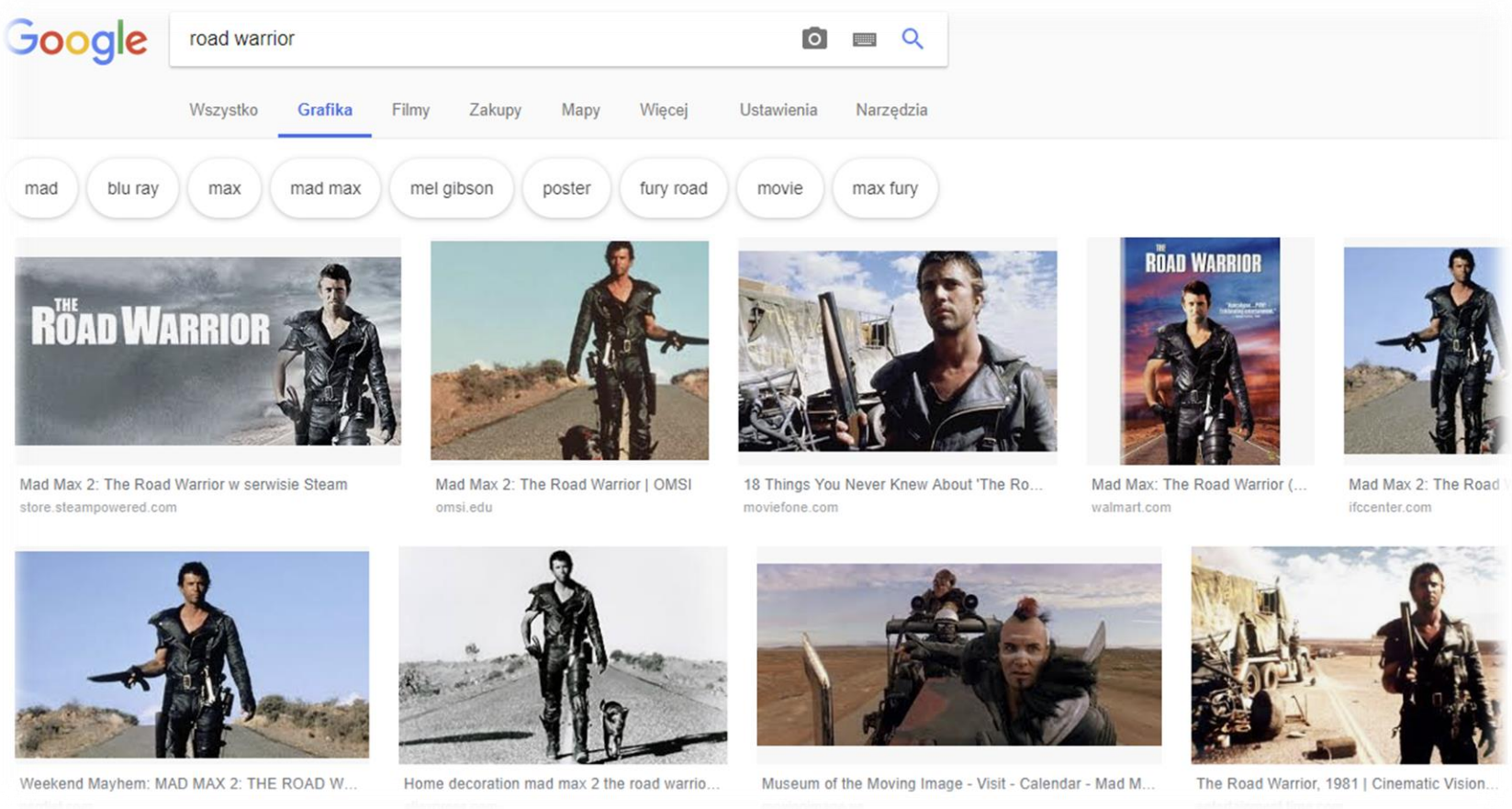
Wsparcie dla NAT jest możliwe. Dopuszczalna jest zmiana źródłowego adresu IP.
Występuje problem, gdy na tym samym NAT połączy się więcej niż jeden klient IPSEC.
Rozwiązaniem jest wykorzystanie NAT-Traversal. Polega on na enkapsulacji ESP w UDP (domyślnie port 4500)

Połączenia site-site

IPIP + IPsec
GRE + IPsec
EoIP + IPsec
IPsec



Zdalni użytkownicy (road – warrior)



Jakie opcje (nie tylko IPSEC)

PPP (Point to Point Protocols)

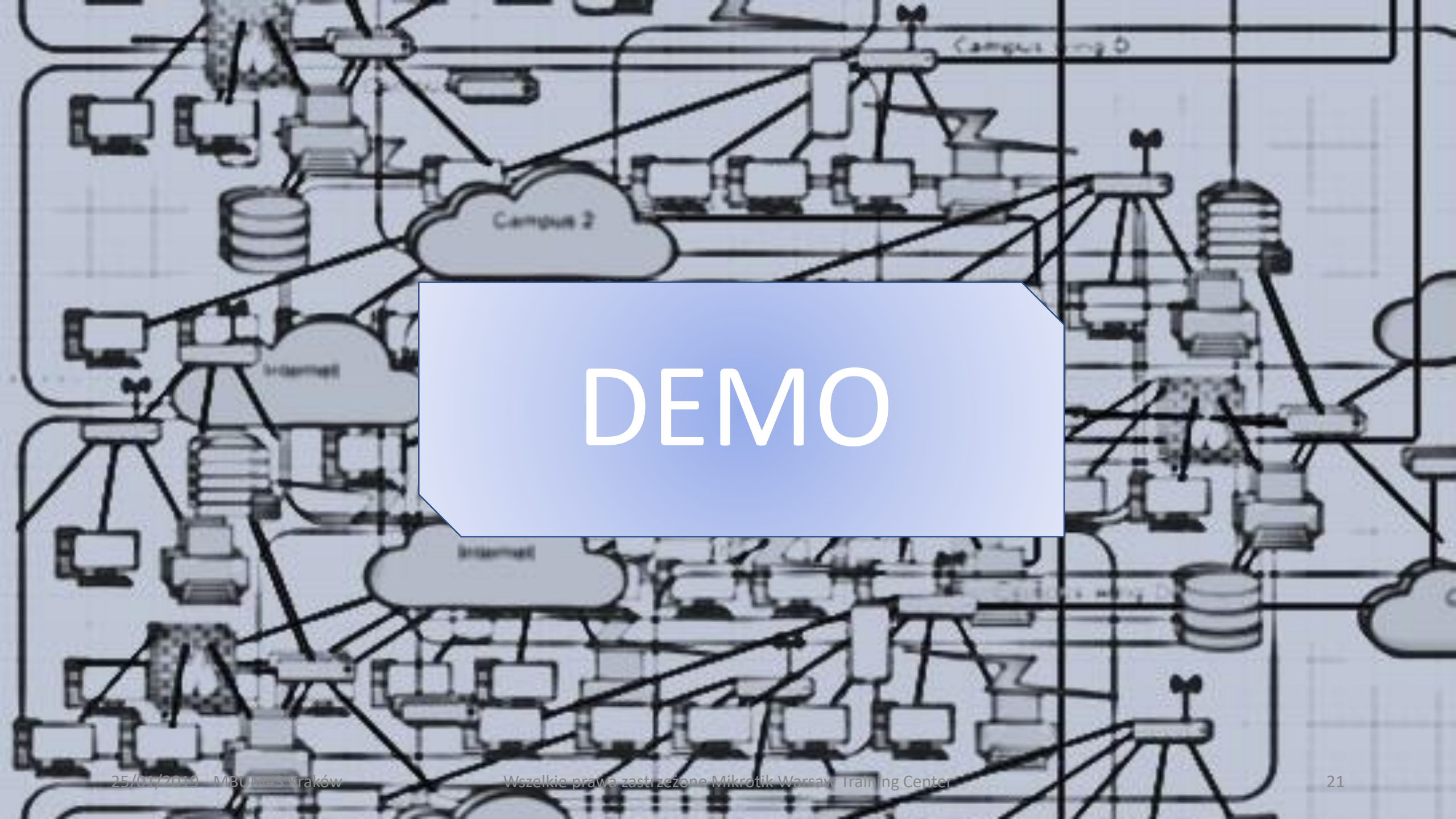
- PPTP (tcp, gre, niezalecane ze względów bezpieczeństwa)
- SSTP (tcp, słabe wspacie natywne poza systemami Microsoft)
- L2TP (udp, szerokie wsparcie na praktycznie wszystkich OS)
- OVPN (upd/tcp, niepełna implementacja serwera na Mikrotik ☹
  - m.in. tylko tcp, brak push config, brak kompresji lzo)

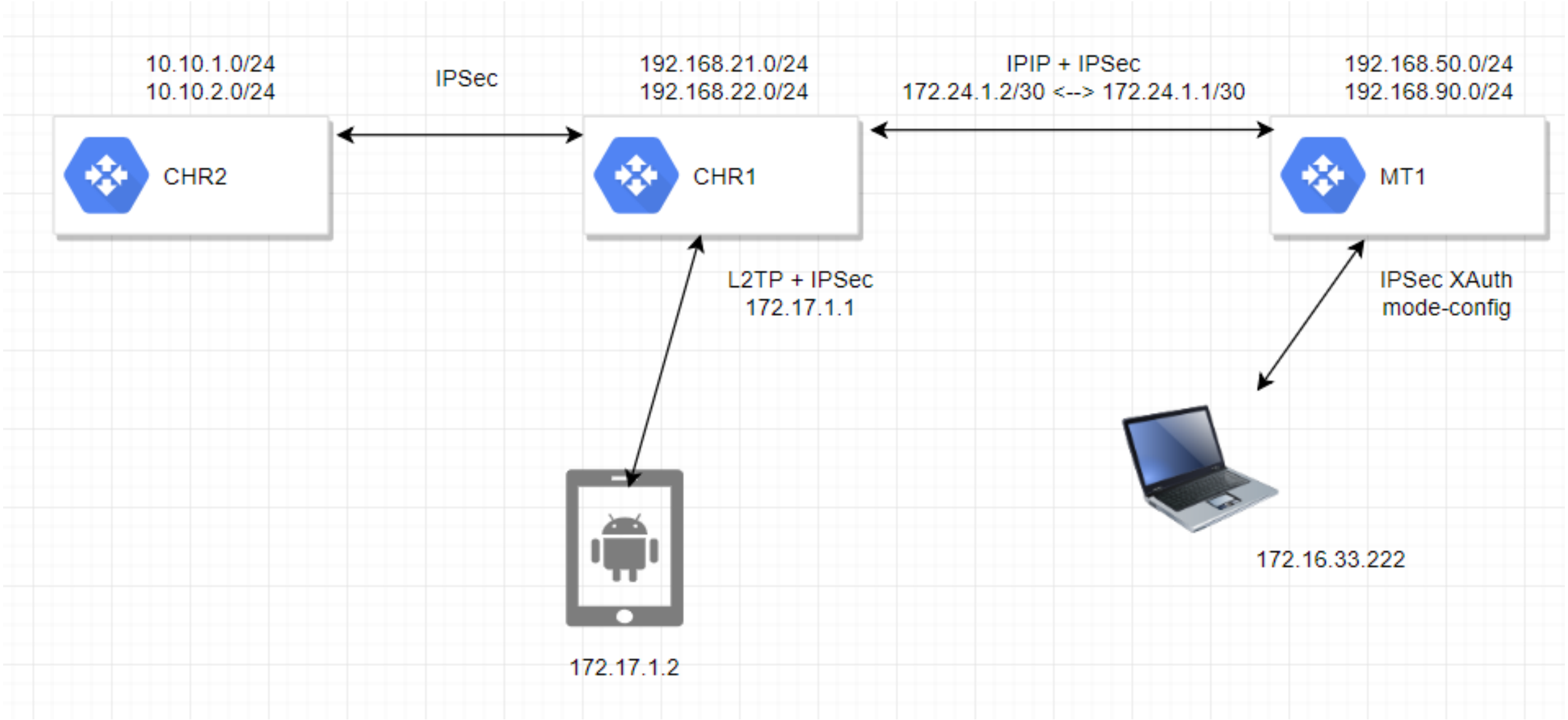
IPSEC Xauth mode-config

szerokie wspacie na OS
nie jest oparty na tcp
częste wsparcie sprzętowe dla IPSEC
PSK, certyfikaty i dwuskładnikowe
push config (DNS, trasy routingu)

IKE2

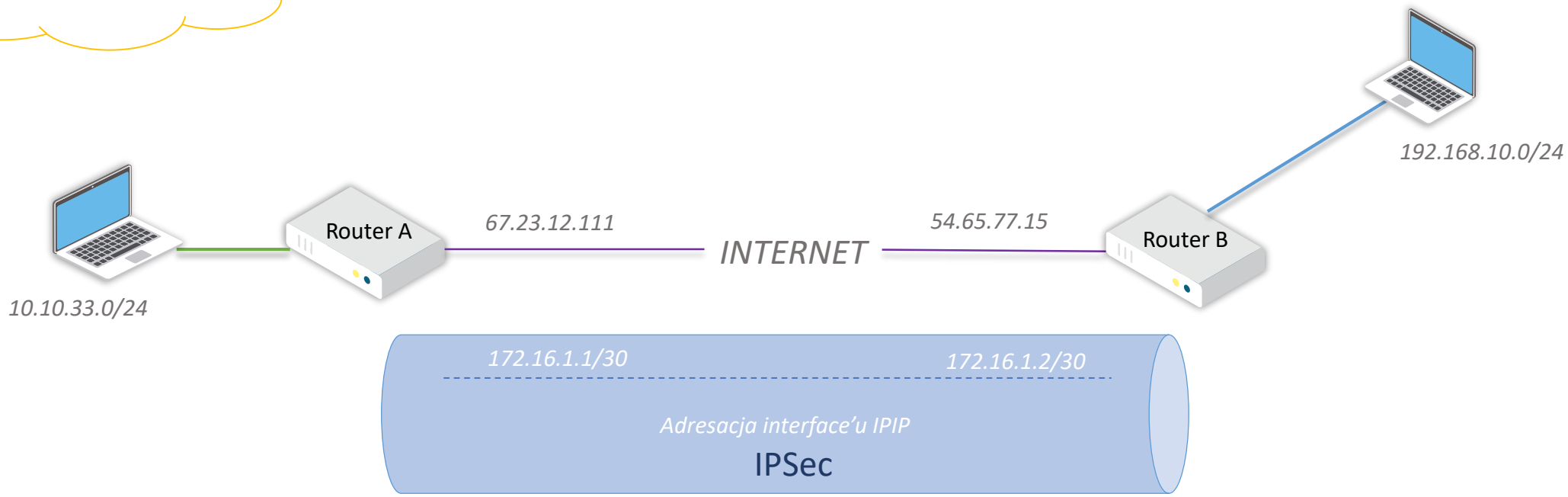
to już nie dziś





Site to site - IPIP+IPSec

Alternatywnie GRE



Pomogą nam „kreatory”

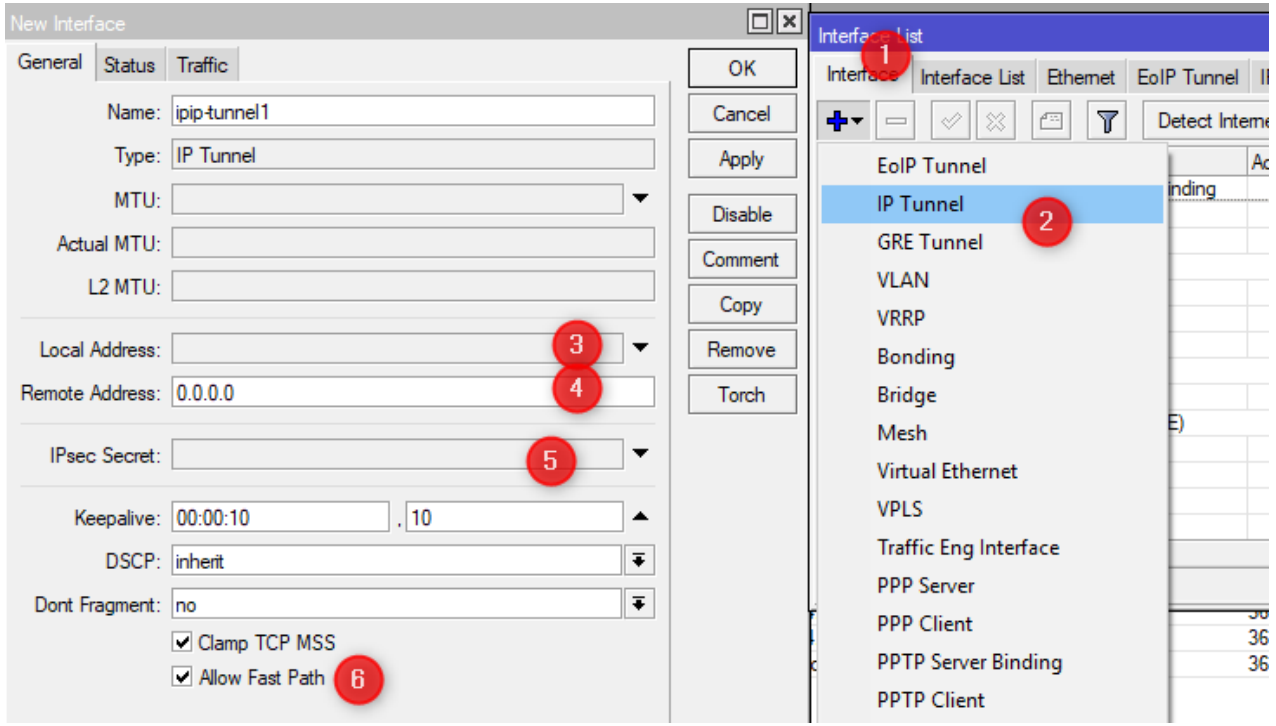
Utworzenie interfejsu dla zakończenia tunelu IPIP

Local Address : publiczny adres naszego koncentratora

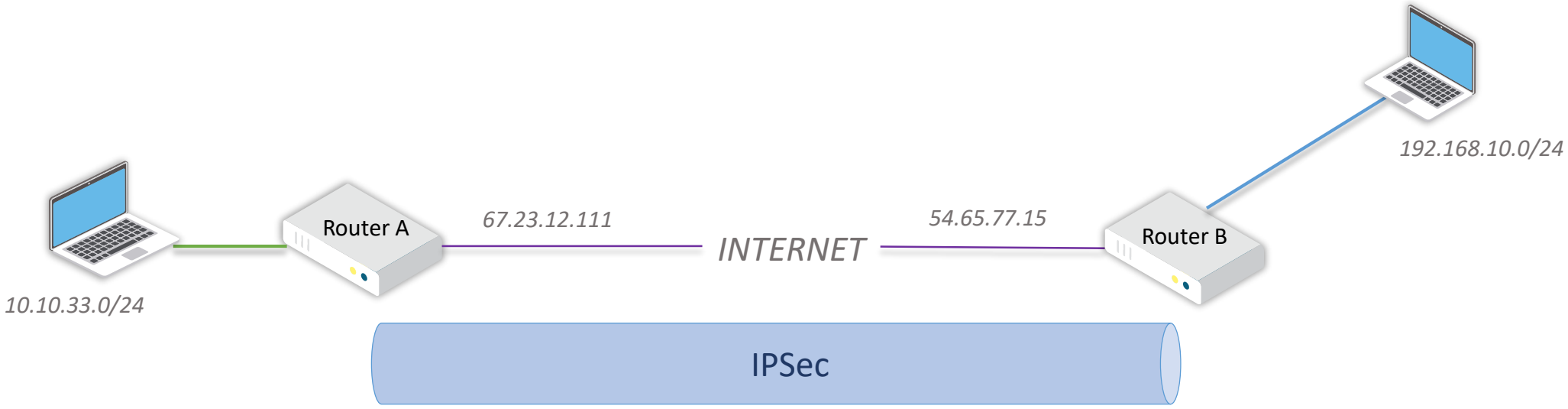
Remote Address : publiczny adres zakończenia tunelu

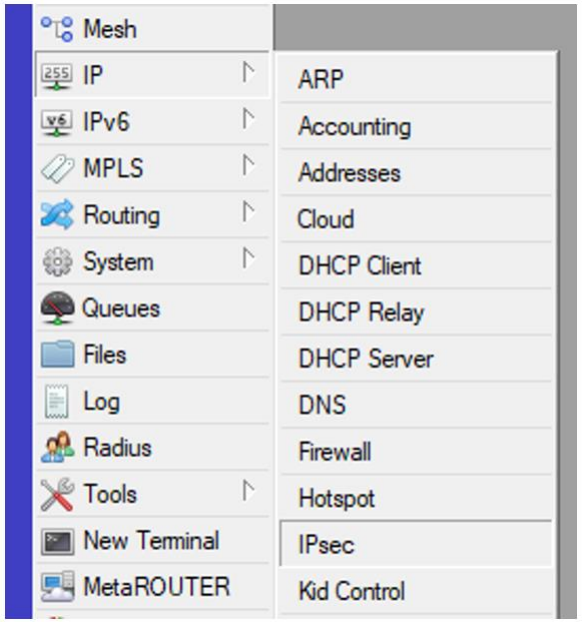
IPsec Secret : PSK dla IPsec (a'la kreator)

Jeśli ruch ma zostać zaszyfrowany konieczne jest odznaczenie **„Allow Fast Path"**



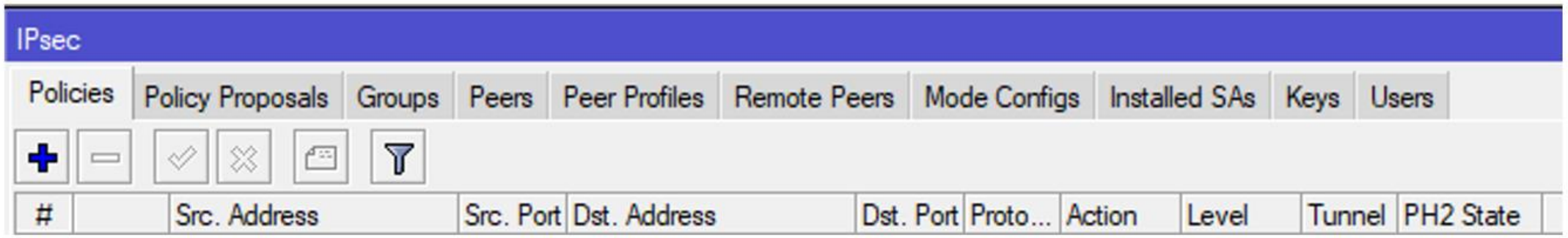
Site to site - IPSec



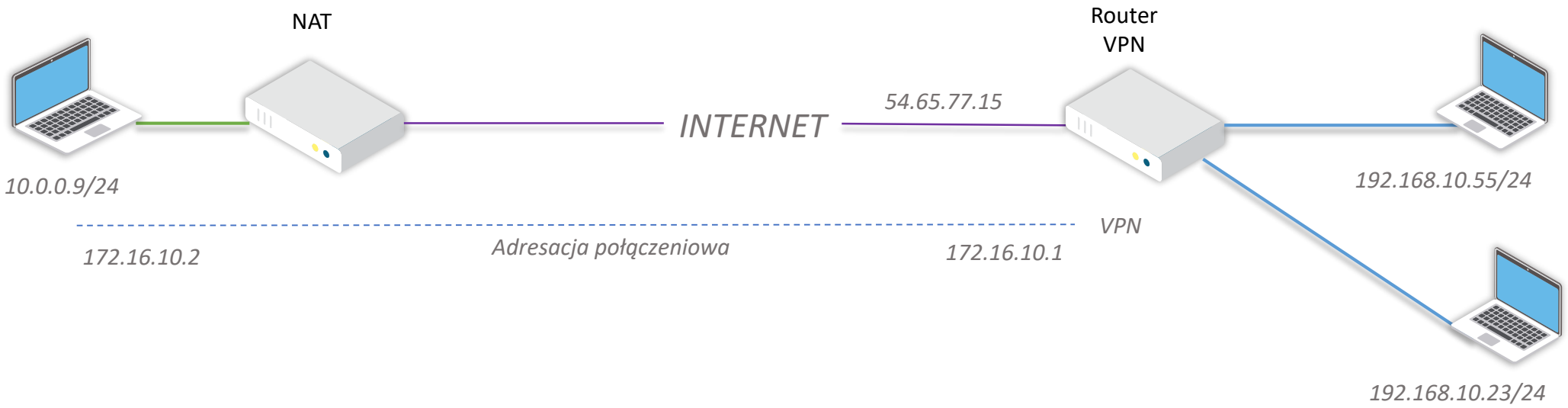


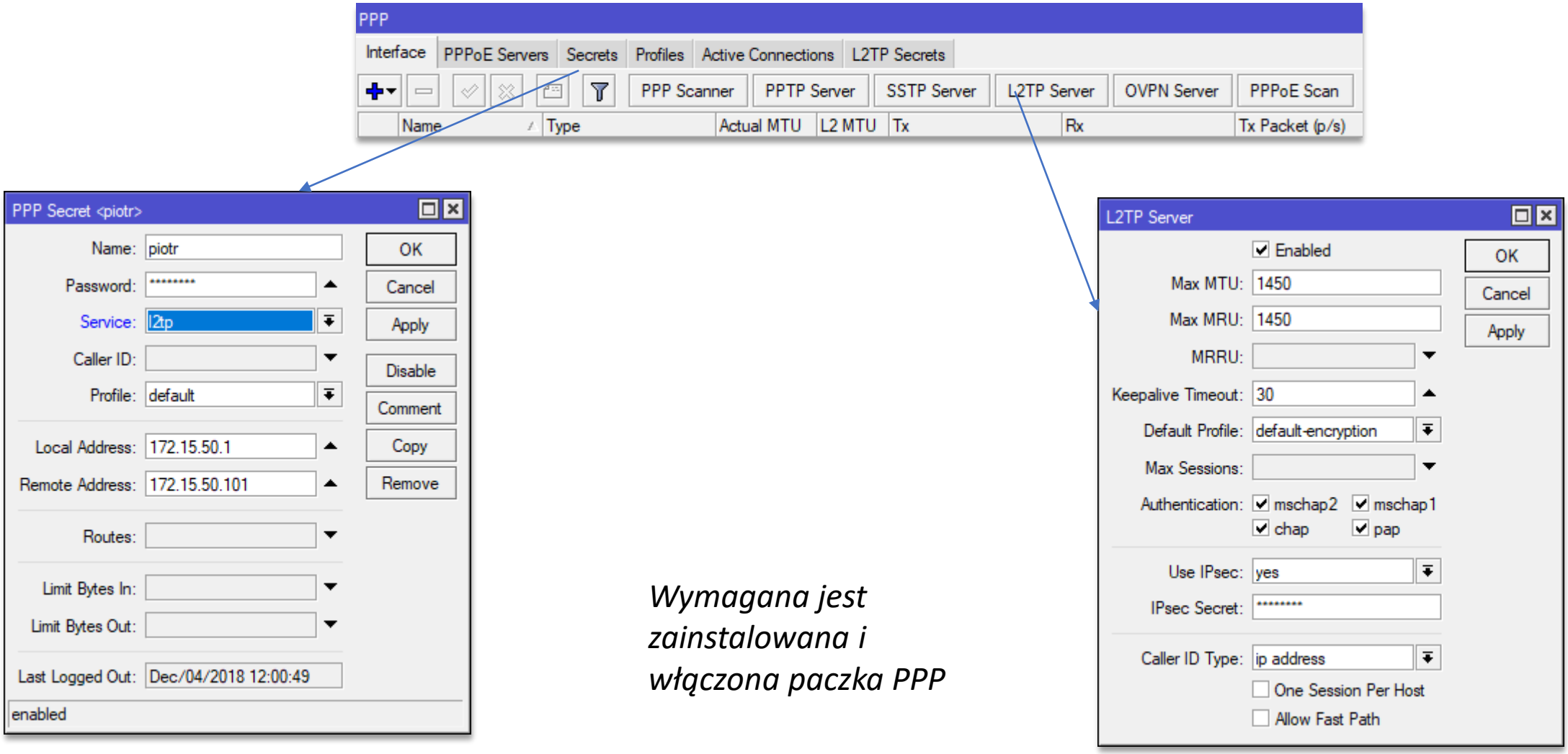
Określa jaki ruch ma zostać obsłużony z IPsec, określa jakie są parametry szyfrowania (faza 2)

Określa zakończenia tunelu oraz parametry dla fazy 1



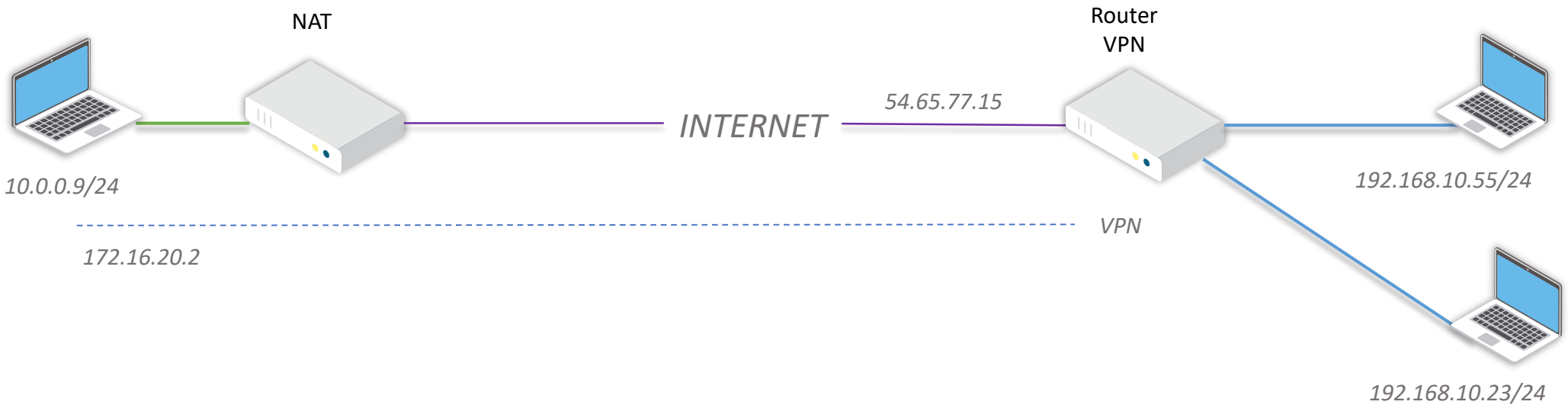
Użytkownicy mobilni – L2TP+IPSec



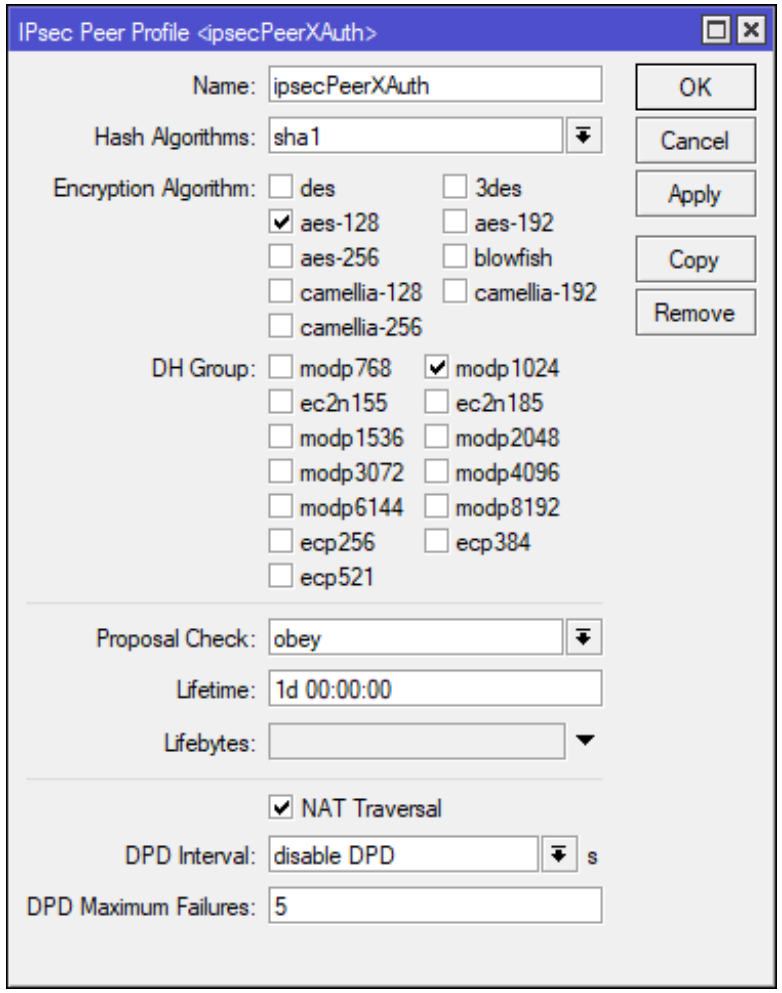


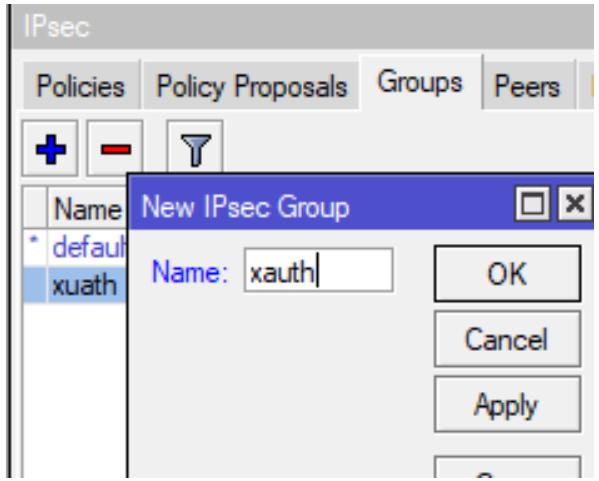
Wymagana jest zainstalowana i włączona paczka PPP

Użytkownicy mobilni – IPSec Xauth mode-config

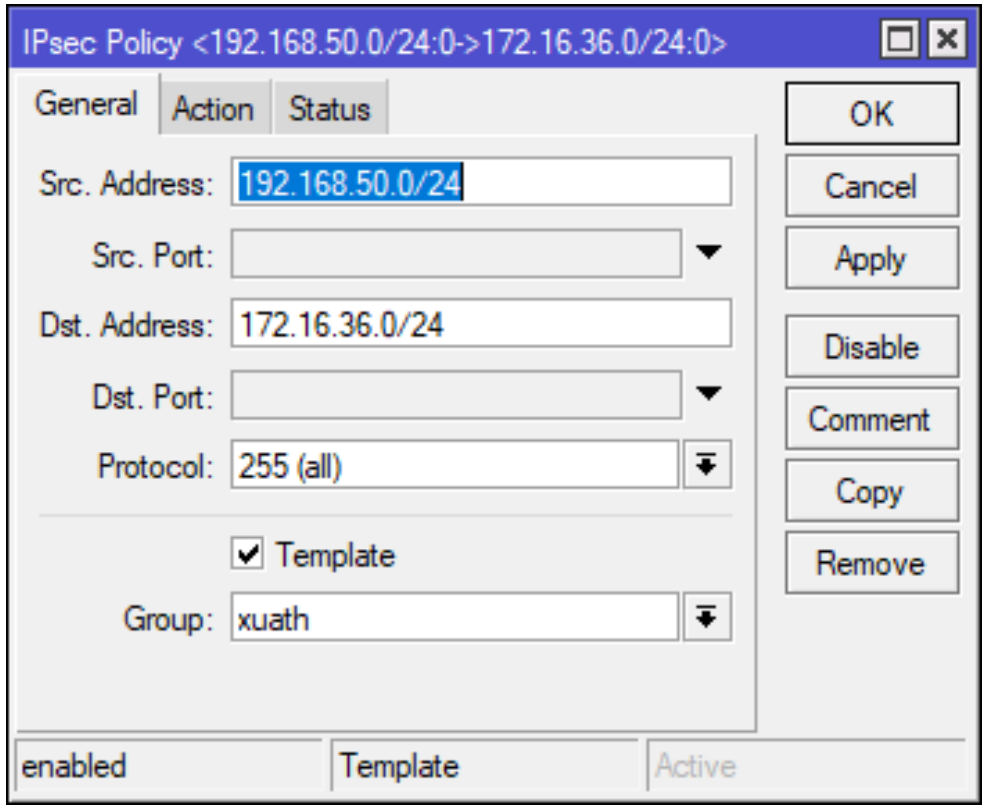


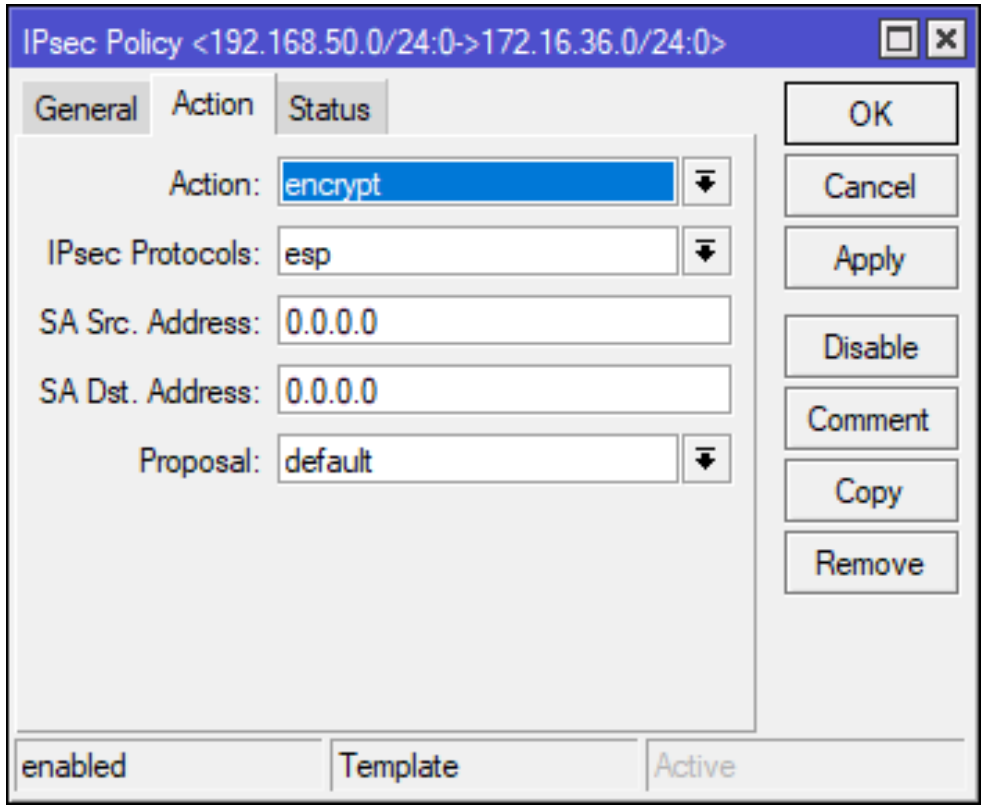
IPSEC Xauth mode-config – peer profile



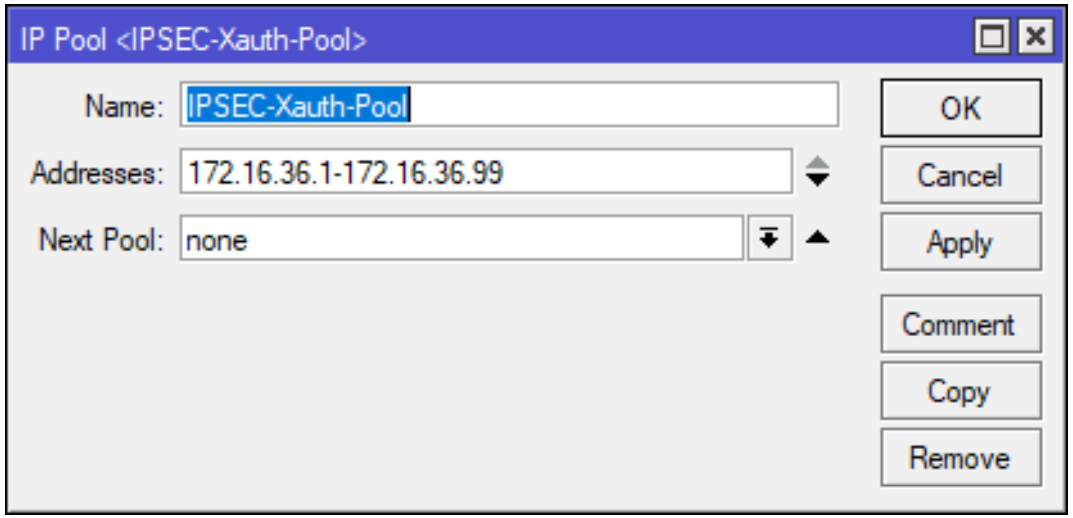


IPSEC Xauth mode-config – szablony Policy

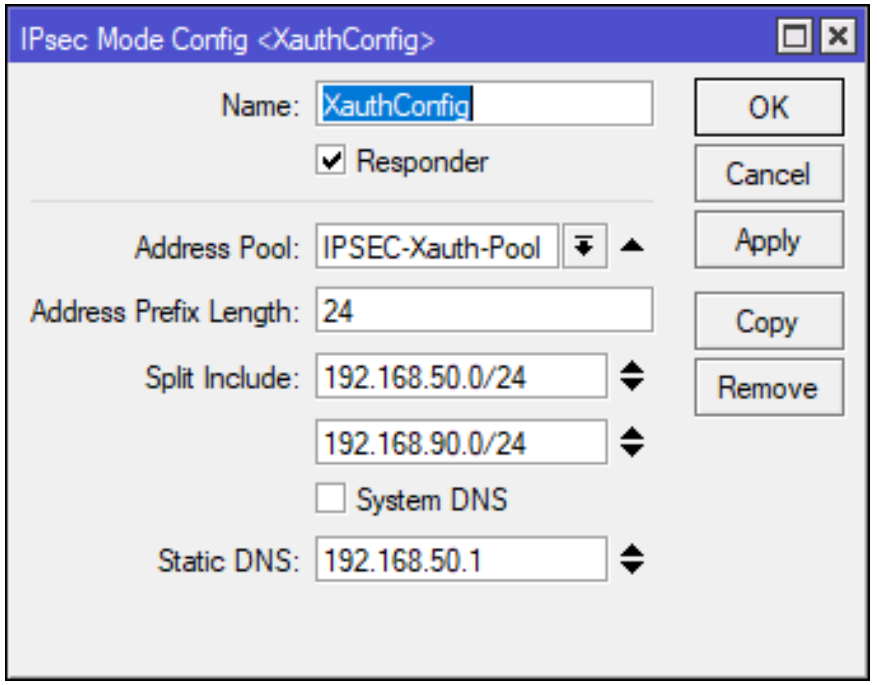




IPSEC Xauth mode-config – push config



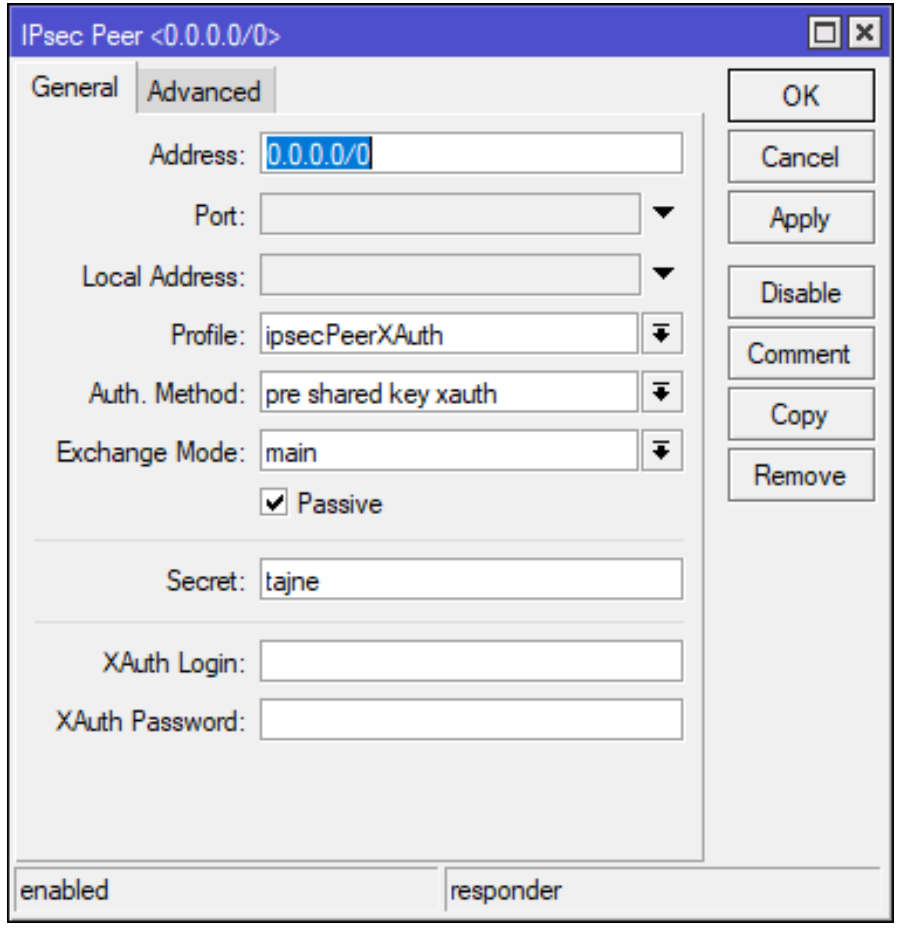
Należy utworzyć pulę dla użytkowników łączących się do naszego koncentratora (analogicznie jak na co dzień robimy na potrzeby DHCP czy profili PPP)

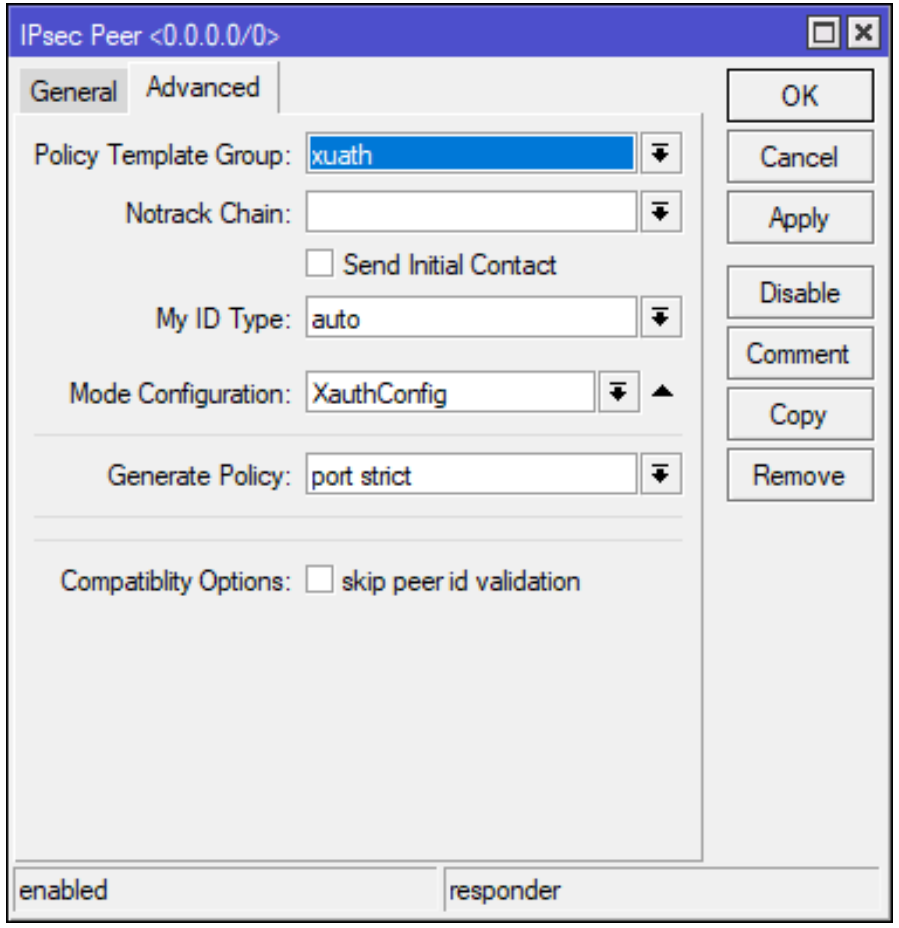


Responder = YES (nasz Mikrotik będzie koncentratorem IPSEC)

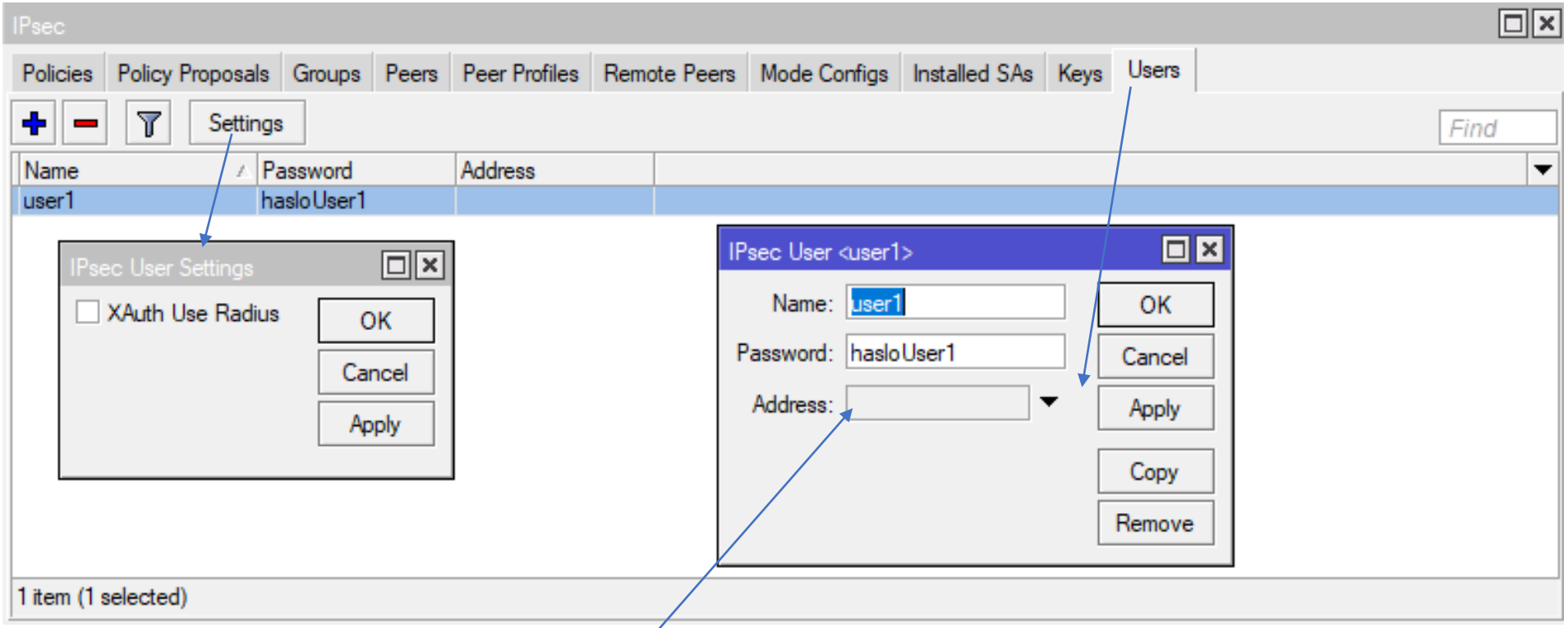
Split Include – trasy przesyłane do Klienta

IPSEC Xauth mode-config – peer config





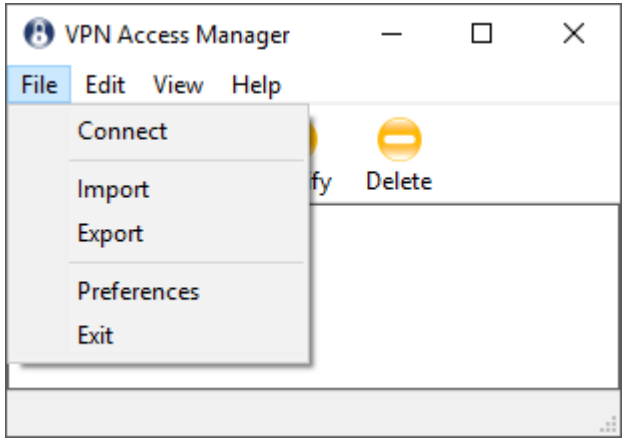
IPSEC Xauth mode-config – użytkownicy

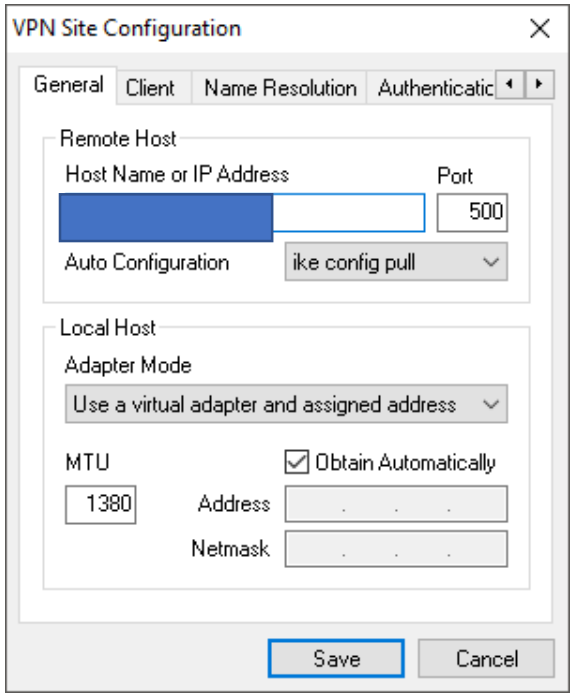


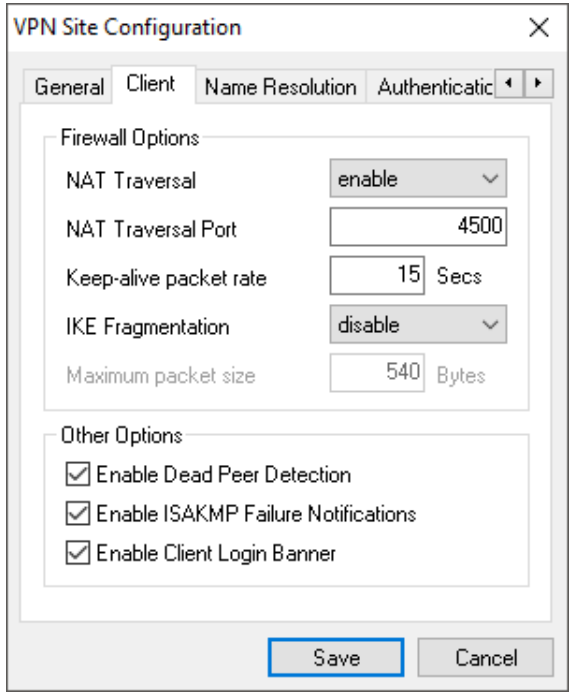
Przypisanie statycznie adresu IP dla Klienta, jeśli puste zostanie wybrany z puli

IPSEC Xauth mode-config – App Client dla MS Windows

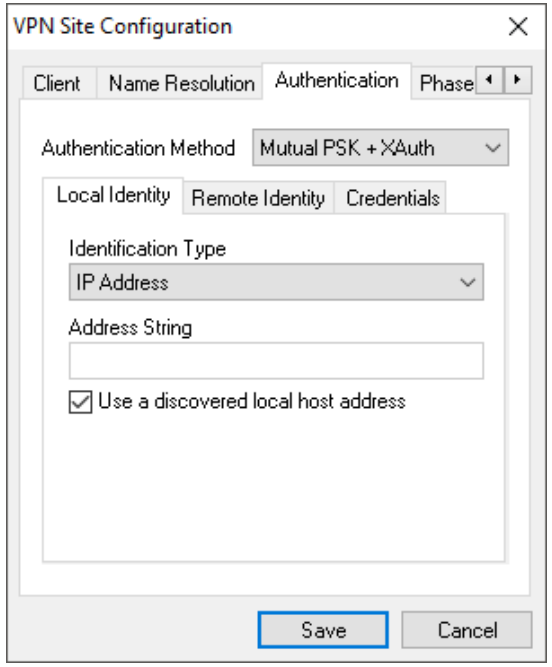
ShrewClient VPN
https://www.shrew.net/download

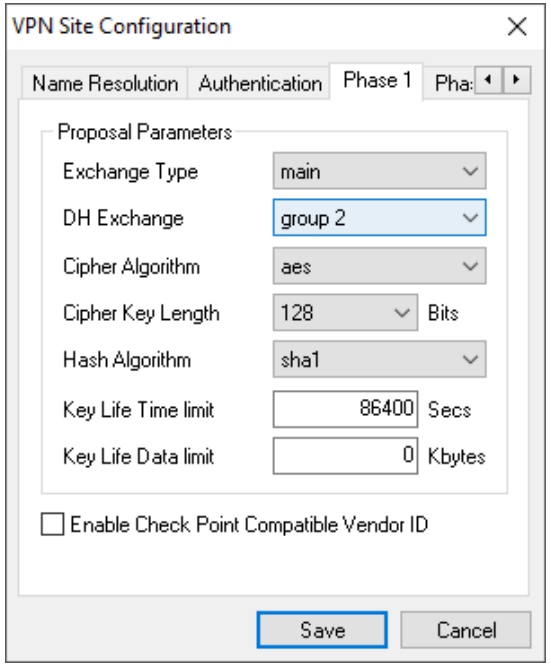


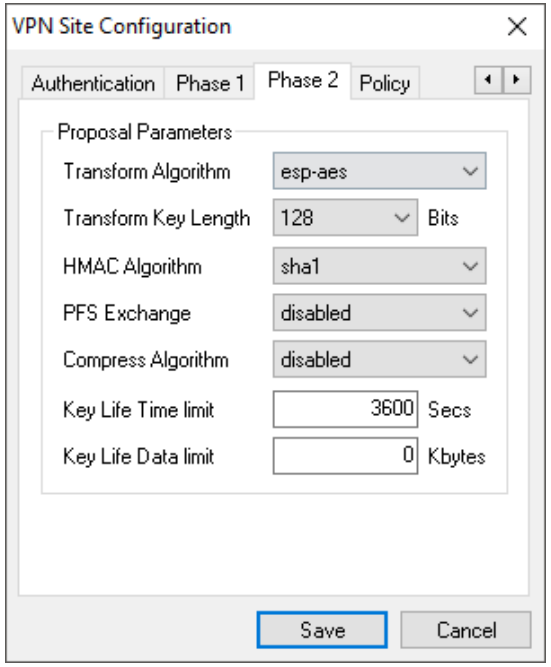


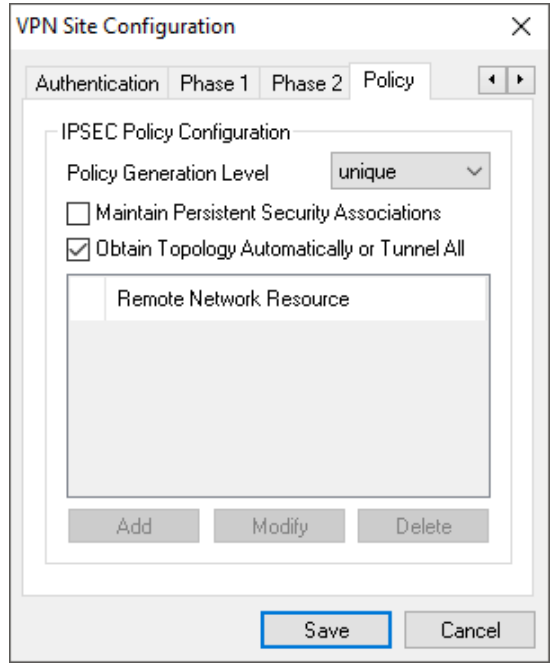


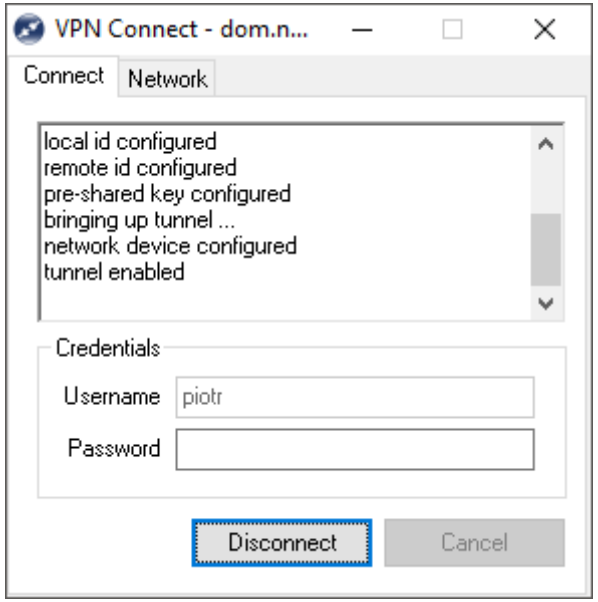
IPSEC Xauth mode-config – App Client dla MS Windows

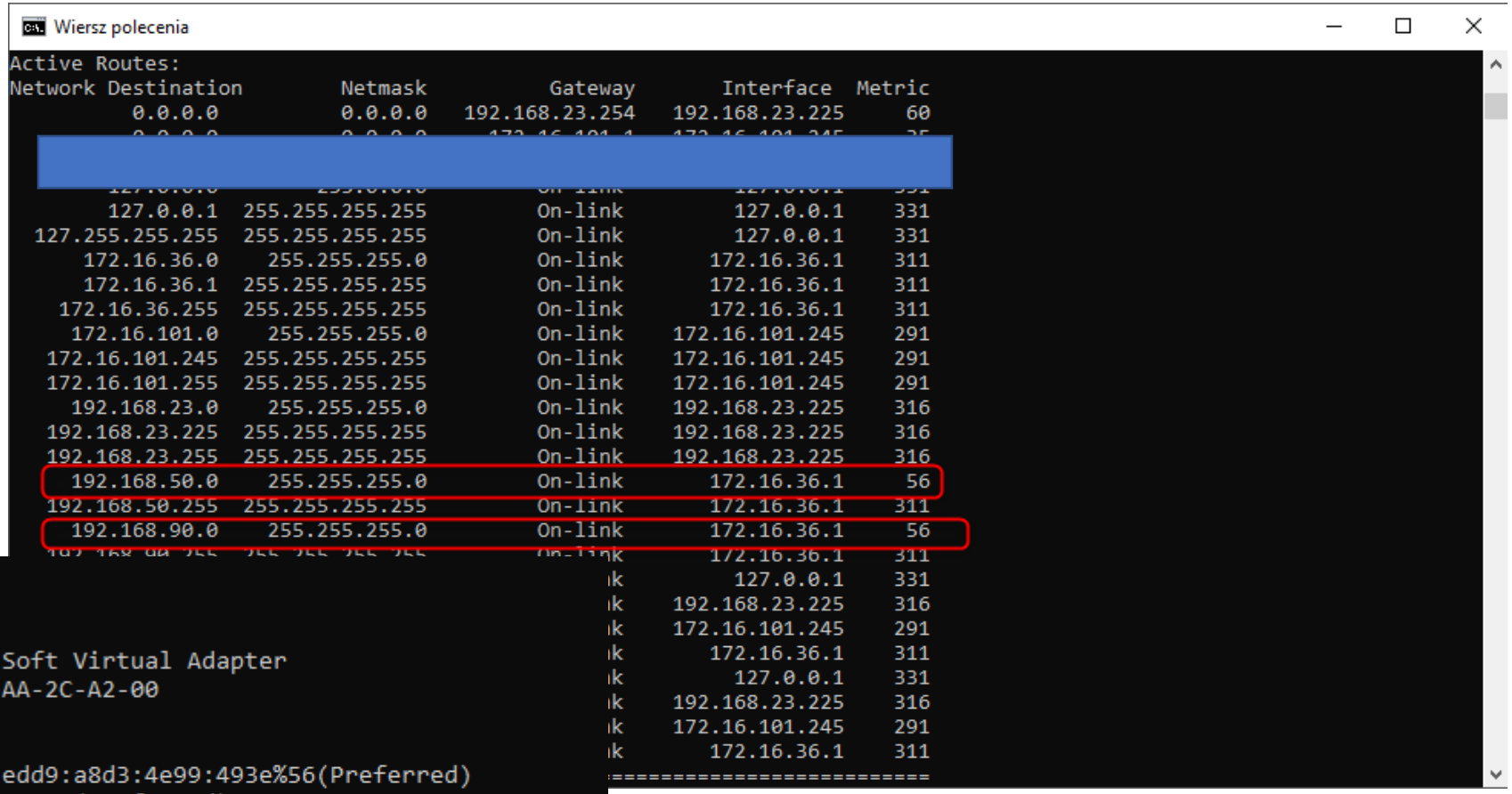








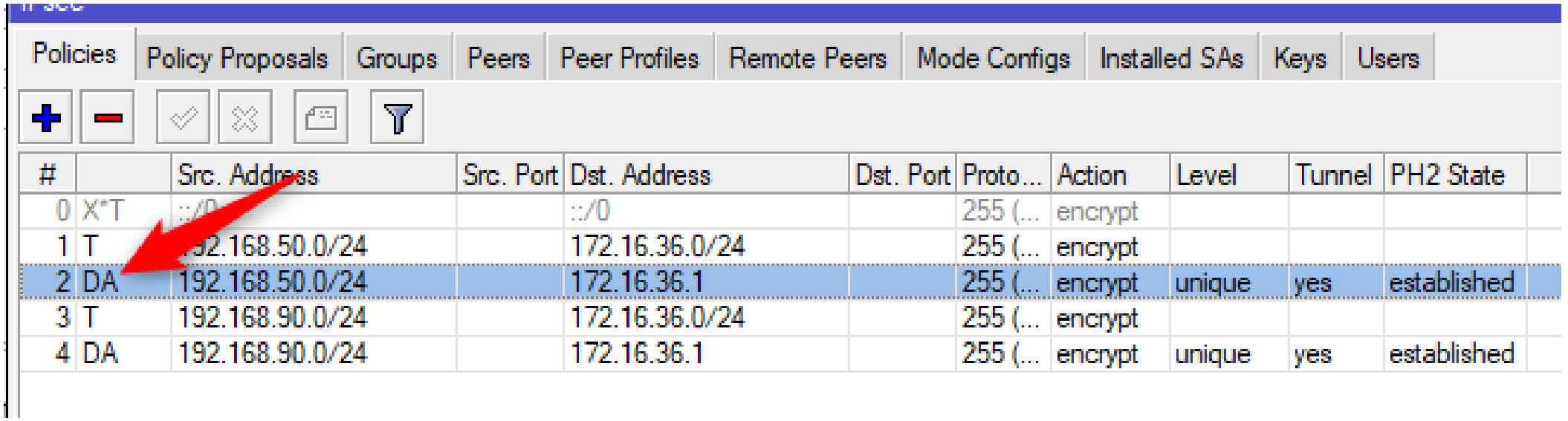





```
Ethernet adapter Połączenie lokalne* 12:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Shrew Soft Virtual Adapter
   Physical Address. . . . . . . . . : AA-AA-AA-2C-A2-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::edd9:a8d3:4e99:493e%56(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.36.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 950708906
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-AF-50-33-34-E6-D7-6B-D4-7A
   DNS Servers . . . . . . . . . . . : 192.168.50.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

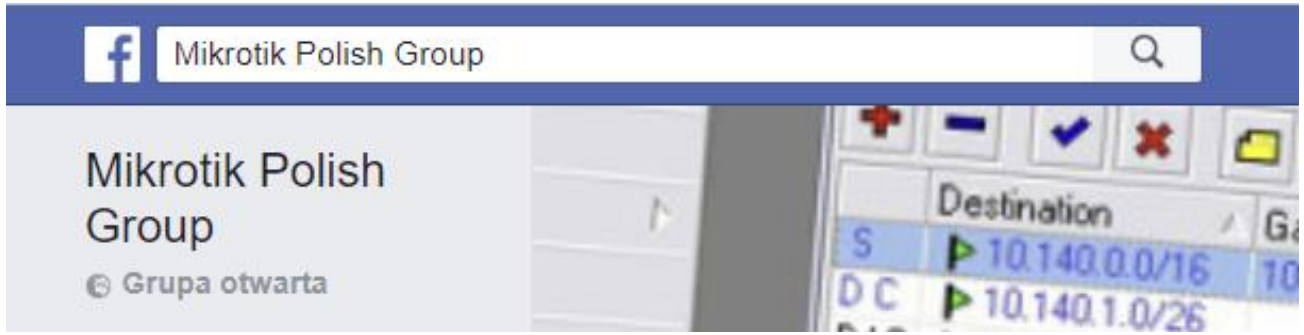
Dynamicznie utworzone Policy



#		Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	Action	Level	Tunnel	PH2 State
0	X*T	::/0		::/0		255 (...	encrypt			
1	T	192.168.50.0/24		172.16.36.0/24		255 (...	encrypt			
2	DA	192.168.50.0/24		172.16.36.1		255 (...	encrypt	unique	yes	established
3	T	192.168.90.0/24		172.16.36.0/24		255 (...	encrypt			
4	DA	192.168.90.0/24		172.16.36.1		255 (...	encrypt	unique	yes	established

Widza w Internecie

http://mikrotikacademy.pl



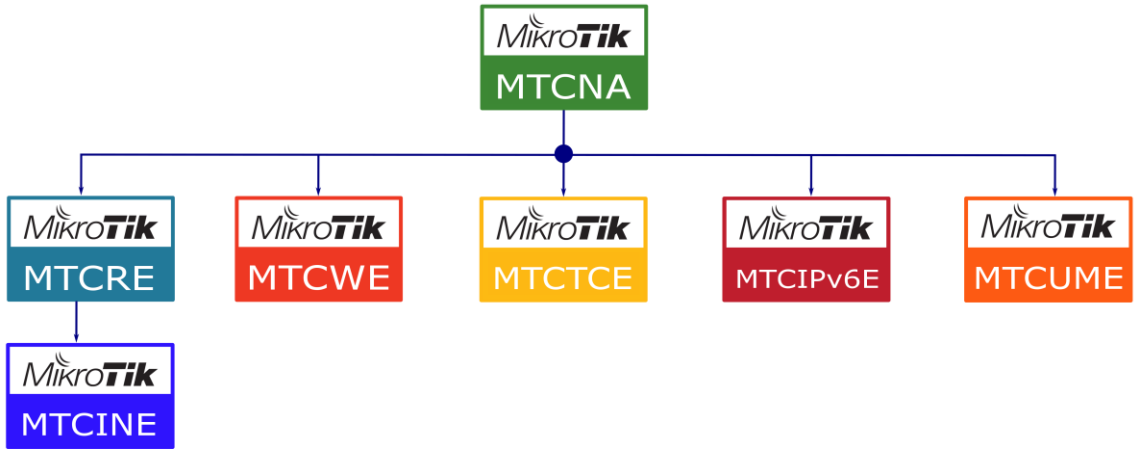
https://www.facebook.com/groups/151322025329859/

Ponad 2500 osób ☺ !!!

https://wiki.mikrotik.com

Zapraszamy na :

Szkolenia certyfikowane Mikrotik



Autorskie warsztaty

https://mwtc.pl