



IPSEC z Mikrotik – zero to hero

Piotr Wasyk
piotr@mwtc.pl

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

O mnie



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*



MikroTik Warsaw
Training Center

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

piotr@mwtc.pl

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 - MBUM#3 Kraków

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*

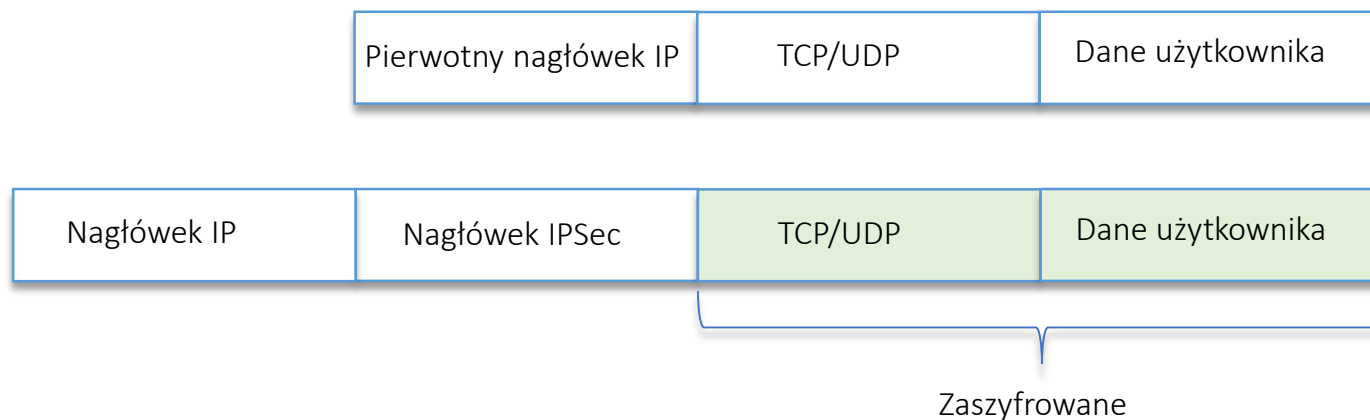
IPSec

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

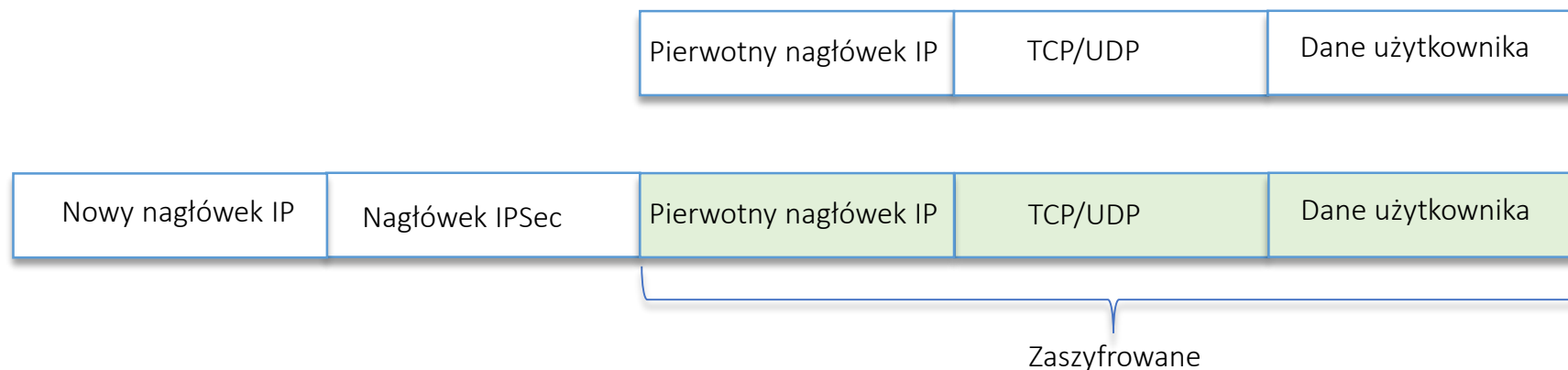
Obecnie najczęściej stosowanym podejściem jest **ESP**

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

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

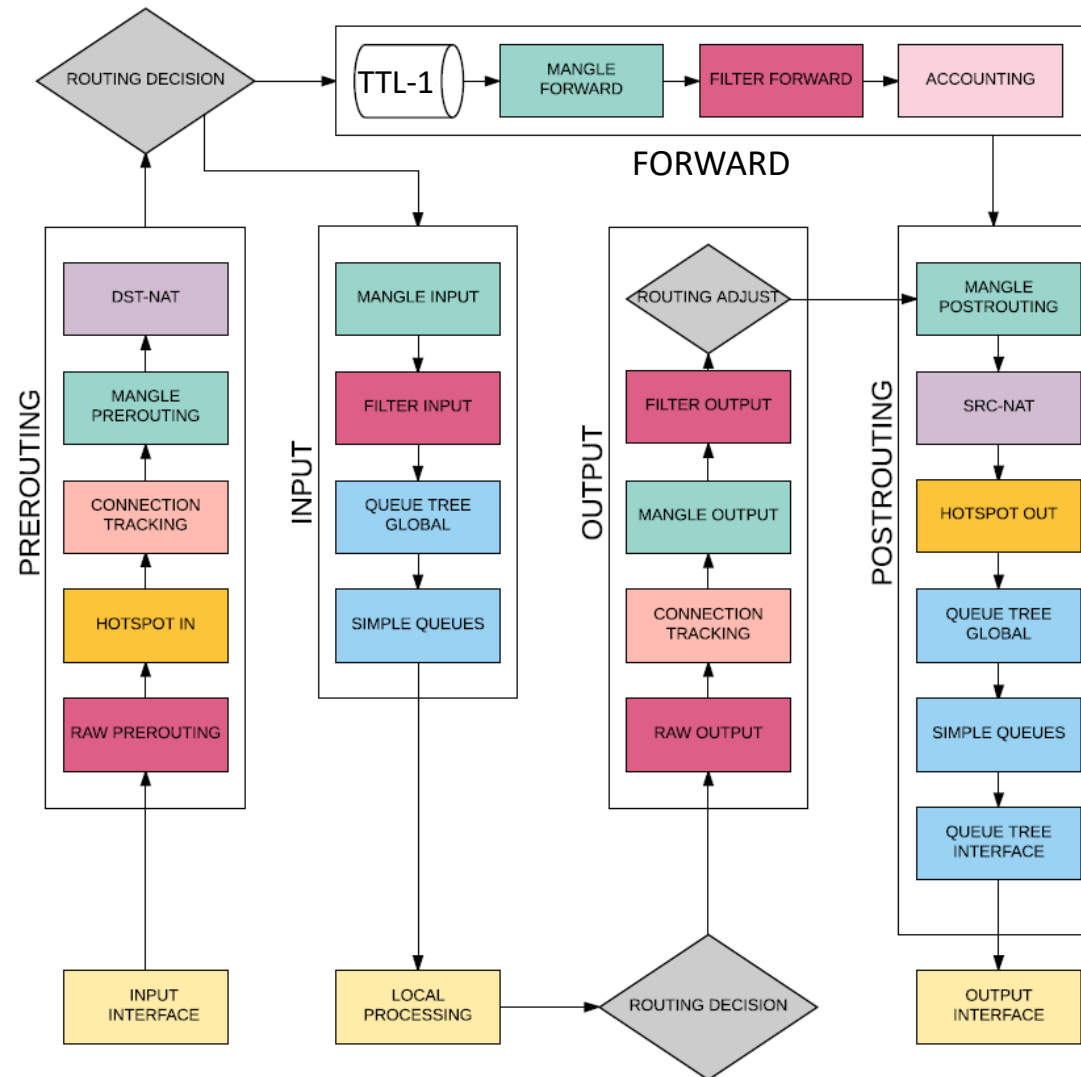


Tryb tunelowy – cały pierwotny pakiet IP jest enkapsulowany wewnątrz nagłówka IPsec. Jest stosowany do połączeń site-site.



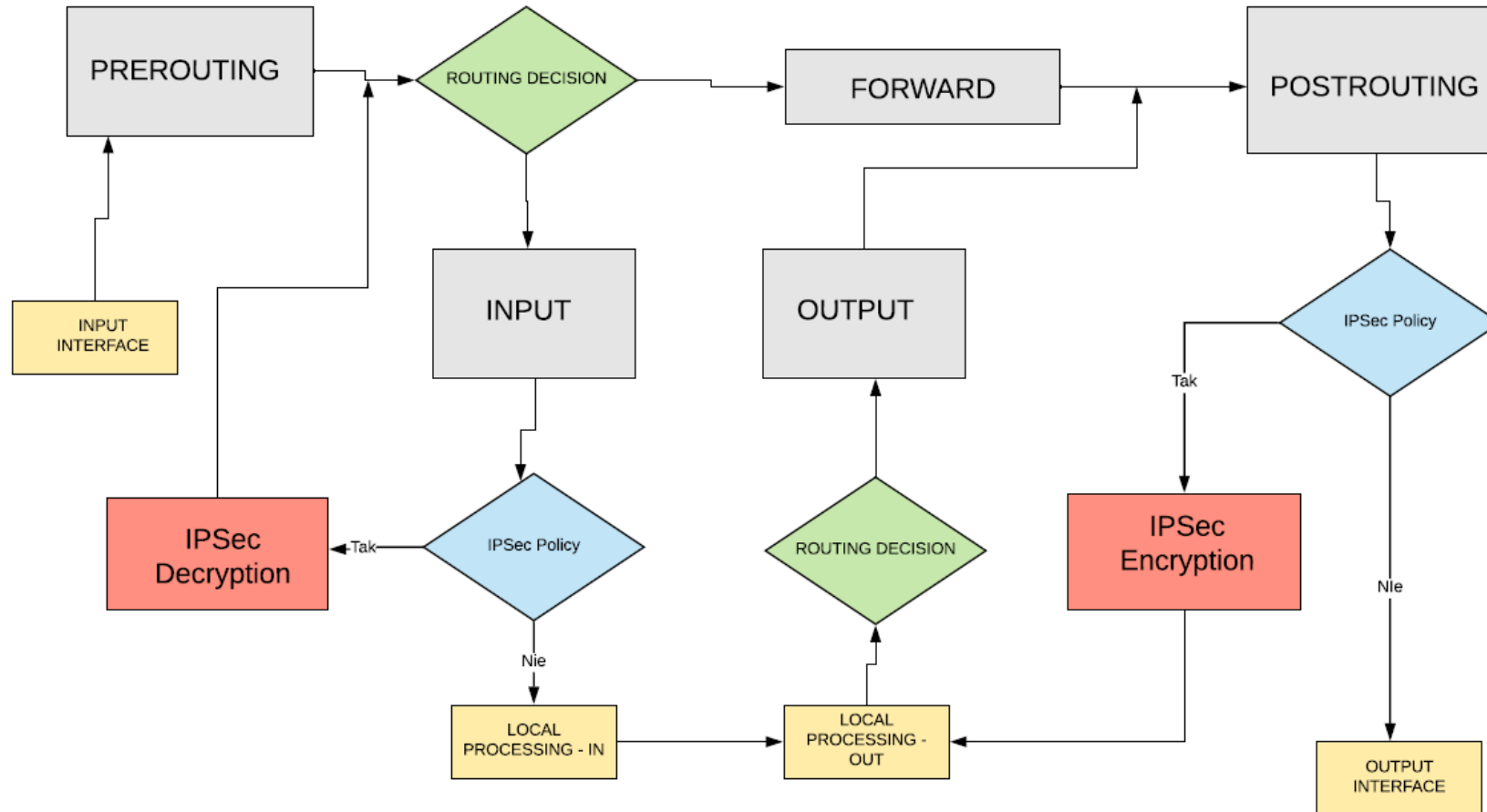
Firewall

Packet Flow



IPSec

Packet flow

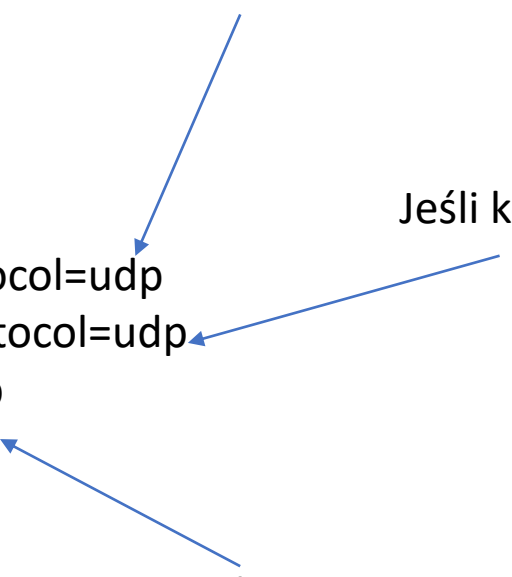


IP -> Firewall -> Filter

/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

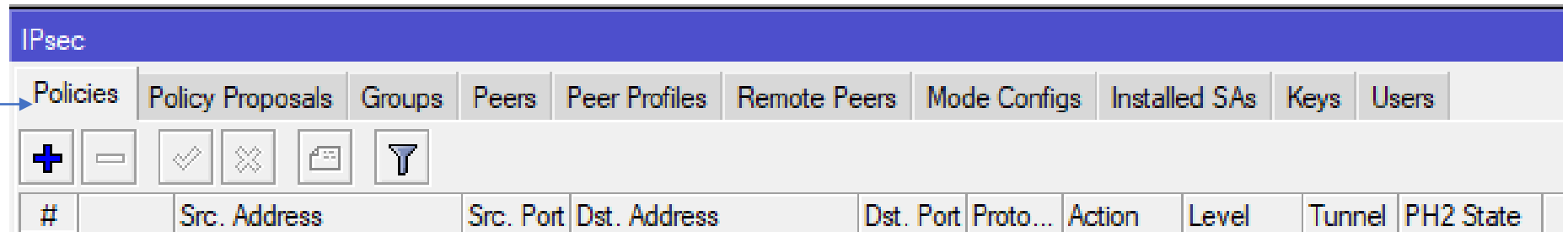
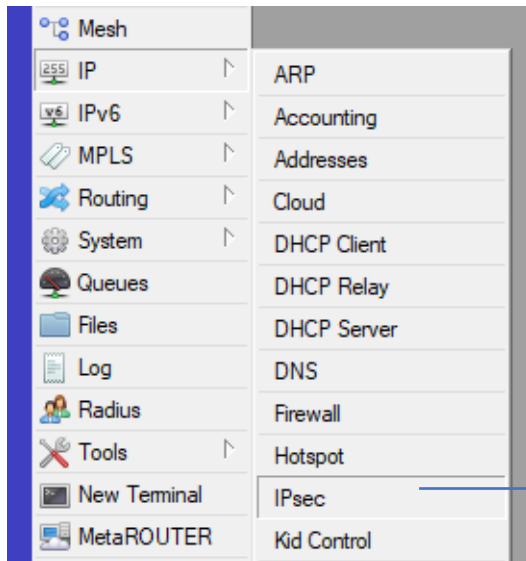
Odpowiedzialny za automatyczną negocjację parametrów połączenia:

- 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) –

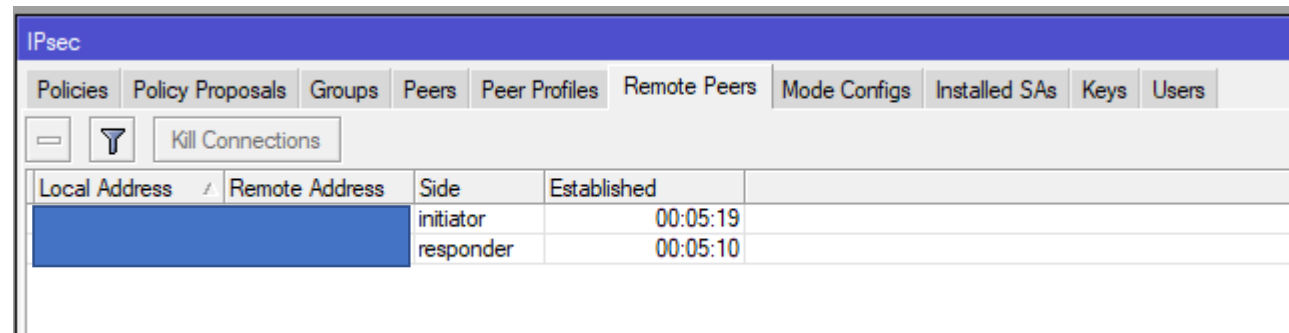
- odpowiada za uwierzytelnienie
- utworzenie kanału ISAKMP(jeden dwukierunkowy kanał)
- zarządzanie kanałem ISAKMP

Peer(y) wymieniają ze sobą informacje o:

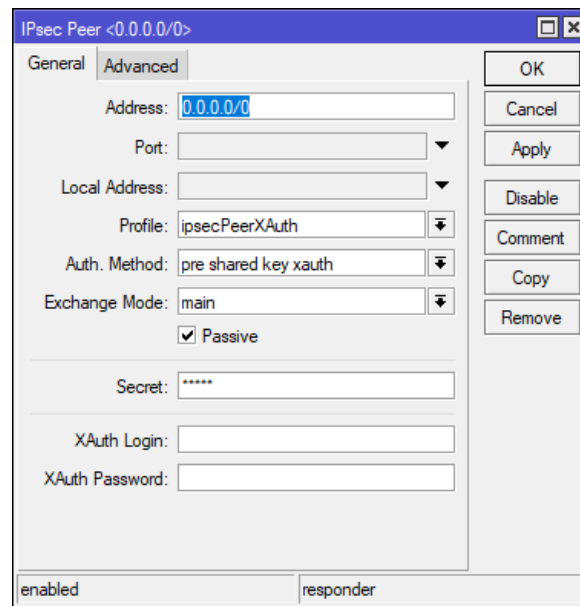
- Wspieranych algorytmach szyfrowania
- Wspieranych algorytmach dla uwierzytelnienia
- Wspieranych DH-group
- Współdzielony klucz

Uwierzytelnienie może być realizowane za pomocą:

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



IPsec				
Policies Policy Proposals Groups Peers Peer Profiles Remote Peers Mode Configs Installed SAs Keys Users				
Kill Connections				
Local Address	Remote Address	Side	Established	
		initiator	00:05:19	
		responder	00:05:10	



IPsec Peer <0.0.0.0/0>

General Advanced

Address: 0.0.0.0/0

Port: [dropdown]

Local Address: [dropdown]

Profile: ipsecPeerXAuth

Auth. Method: pre shared key xauth

Exchange Mode: main

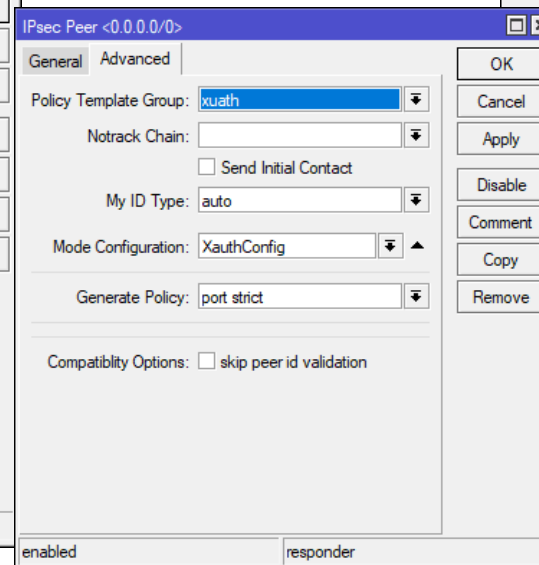
☒ Passive

Secret: *****

XAuth Login: [text]

XAuth Password: [text]

enabled responder



IPsec Peer <0.0.0.0/0>

General Advanced

Policy Template Group: xauth

Notrack Chain: [dropdown]

☐ Send Initial Contact

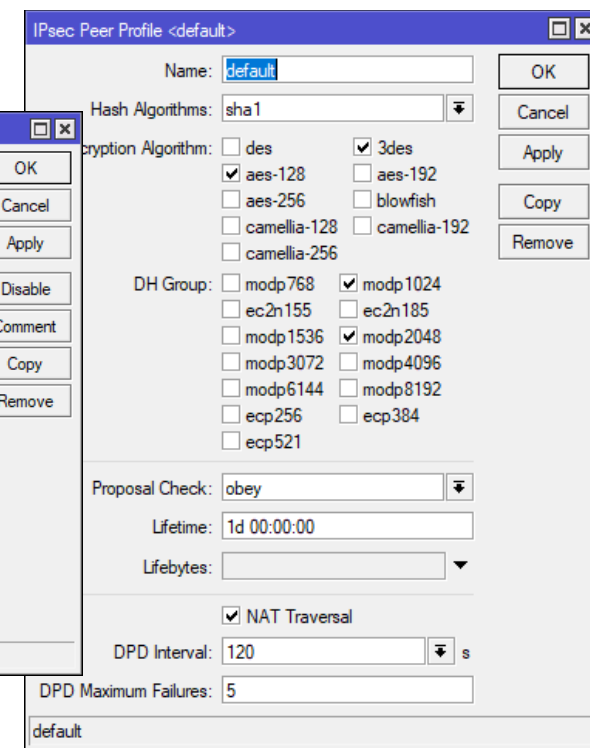
My ID Type: auto

Mode Configuration: XauthConfig

Generate Policy: port strict

Compatibility Options: ☐ skip peer id validation

enabled responder



IPsec Peer Profile <default>

Name: default

Hash Algorithms: sha1

Cryptation Algorithm:

☐ des ☒ 3des

☒ aes-128 ☐ aes-192

☐ aes-256 ☐ blowfish

☐ camellia-128 ☐ camellia-192

☐ camellia-256

DH Group:

☐ modp768 ☒ modp1024

☐ ec2n155 ☐ ec2n185

☐ modp1536 ☒ modp2048

☐ modp3072 ☐ modp4096

☐ modp6144 ☐ modp8192

☐ ecp256 ☐ ecp384

☐ ecp521

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifeytes: [dropdown]

☒ NAT Traversal

DPD Interval: 120 s

DPD Maximum Failures: 5

default

ISAKMP – Faza 1

Tryb normalny (main mode)

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

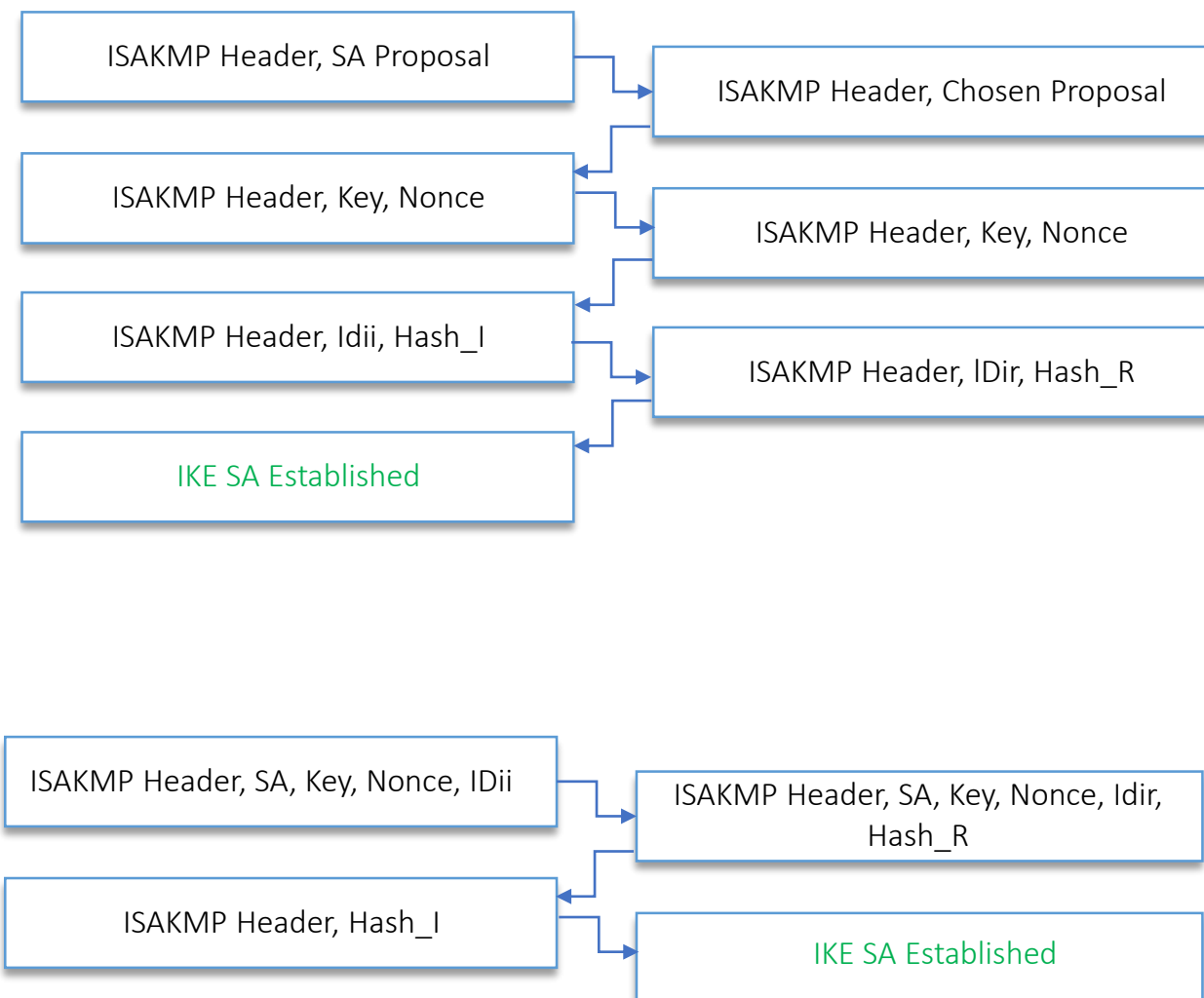
Tryb agresywny (aggressive mode)

- Wymieniane są 3 komunikaty
- Szybszy

Z racji, że część informacji jest wymieniana zanim ustanowiony zostanie bezpieczny kanał, możliwe jest podsłuchiwanie 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 zabezpieczona.

W związku z tym nie ma konieczności przeprowadzenia uwierzytelnienia, a dane przesyłane w jej trakcie są bezpieczne.

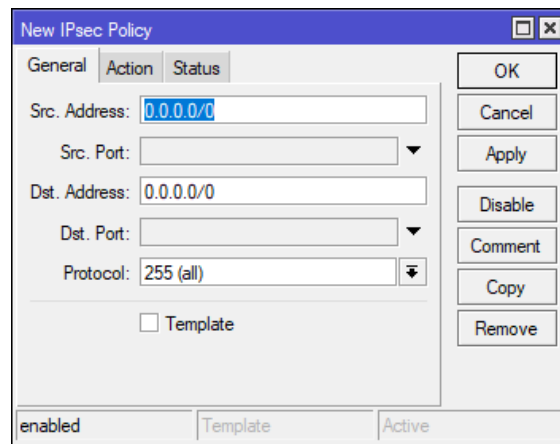
Jej zadaniem jest:

- Uzgadnianie kluczy wg algorytmu DH
- Uzgadnianie IPsec SA

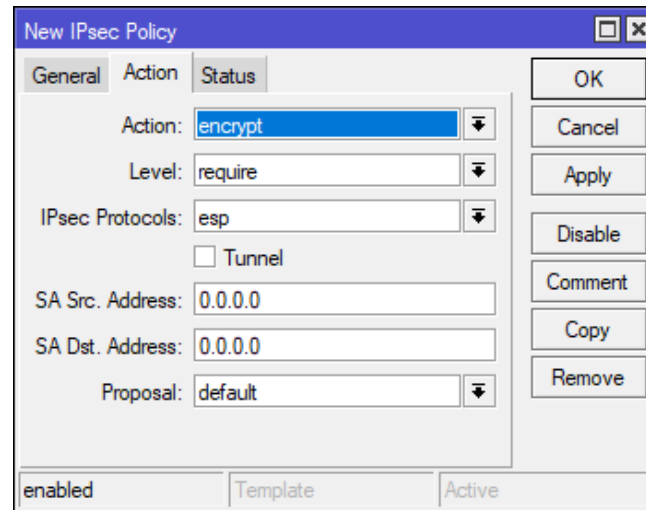
	Policies	Policy Proposals	Groups	Peers	Peer Profiles	Remote Peers	Mode Configs	Installed SAs	Keys	Users
	Flush									
	SPI	Src. Address	Dst. Address	Auth....	Encr....	Encr....	Current B...			
E	7ee8b83			sha1	aes c...	256	1773			
E	8902037			sha1	aes c...	256	1556			

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

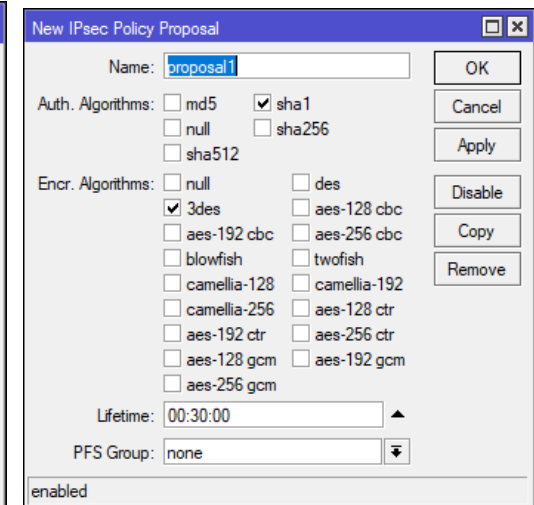
AH / ESP / AH+ESP



The 'New IPsec Policy' dialog box has three tabs: General, Action, and Status. The General tab is active, showing fields for Src. Address (0.0.0.0/0), Src. Port, Dst. Address (0.0.0.0/0), Dst. Port, and Protocol (255 (all)). There is a checkbox for 'Template' and buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom, there are three status indicators: 'enabled', 'Template', and 'Active'.



The 'New IPsec Policy' dialog box is shown with the Action tab selected. The 'Action' dropdown is set to 'encrypt'. The 'Level' is set to 'require'. The 'IPsec Protocols' dropdown is set to 'esp'. There is a checkbox for 'Tunnel'. The 'SA Src. Address' and 'SA Dst. Address' are both set to '0.0.0.0'. The 'Proposal' dropdown is set to 'default'. Buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove are present. At the bottom, there are three status indicators: 'enabled', 'Template', and 'Active'.

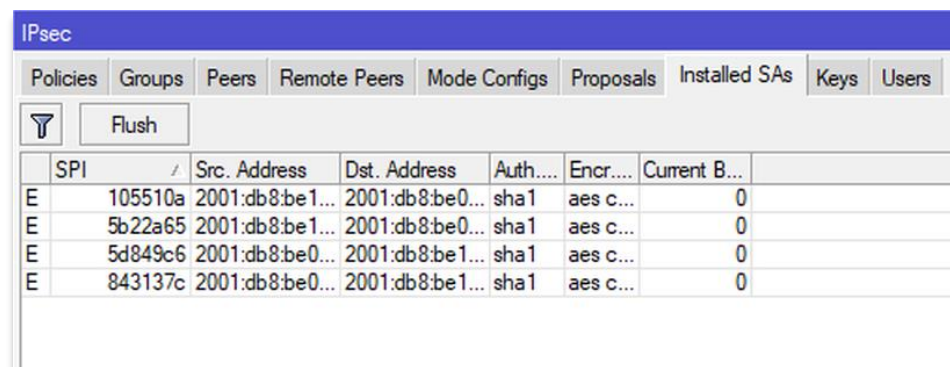


The 'New IPsec Policy Proposal' dialog box is shown. The 'Name' field is set to 'proposal1'. Under 'Auth. Algorithms', 'md5' and 'sha1' are checked. Under 'Encr. Algorithms', '3des' is checked. There are checkboxes for various other algorithms like aes-128 cbc, aes-256 cbc, etc. The 'Lifetime' is set to '00:30:00' and the 'PFS Group' is set to 'none'. Buttons for OK, Cancel, Apply, Disable, Copy, and Remove are present. At the bottom, there is a status indicator: 'enabled'.

Zawsze przebiega w trybie Aggressive

IPsec Security Association (SA)

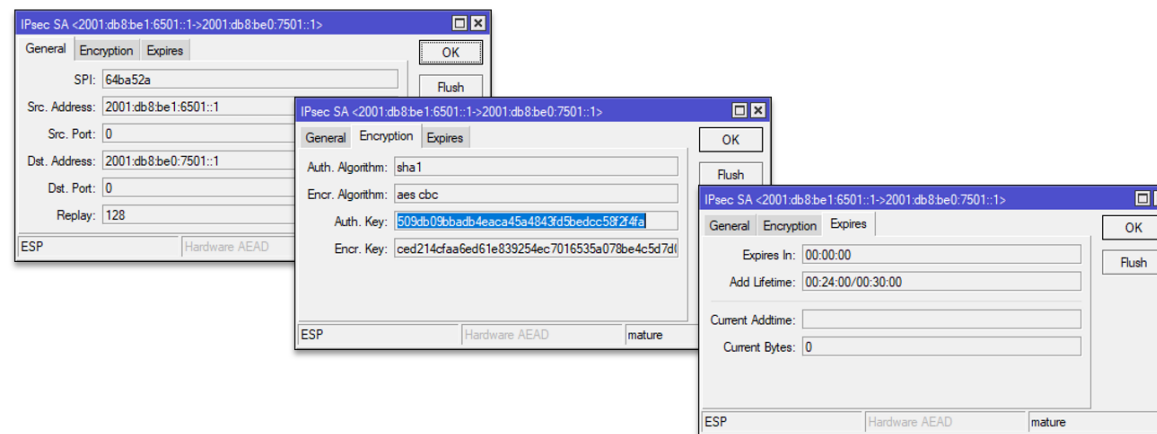
To **jednokierunkowy** kanał do przesyłania danych pomiędzy nadawcą i odbiorcą.



	SPI	/	Src. Address	Dst. Address	Auth....	Encr....	Current B...
E	105510a		2001:db8:be1...	2001:db8:be0...	sha1	aes c...	0
E	5b22a65		2001:db8:be1...	2001:db8:be0...	sha1	aes c...	0
E	5d849c6		2001:db8:be0...	2001:db8:be1...	sha1	aes c...	0
E	843137c		2001:db8:be0...	2001:db8:be1...	sha1	aes c...	0

Baza SAD – Security Association Database

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



The image shows three overlapping windows from the Mikrotik WinBox IPsec configuration interface. The top-left window is the 'General' tab for an SA between 2001:db8:be1:6501::1 and 2001:db8:be0:7501::1, showing SPI 64ba52a and a replay window of 128. The middle window is the 'Encryption' tab for the same SA, showing SHA1 authentication and AES-CBC encryption with specific keys. The bottom-right window is the 'Expires' tab, showing an expiration time of 00:00:00 and current bytes of 0.

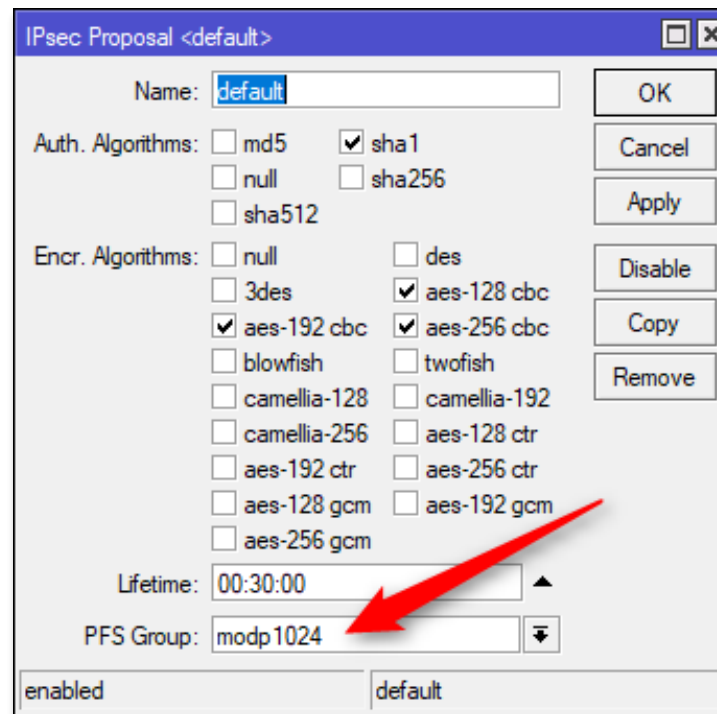
Baza SPD - Security Policy Database

- 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

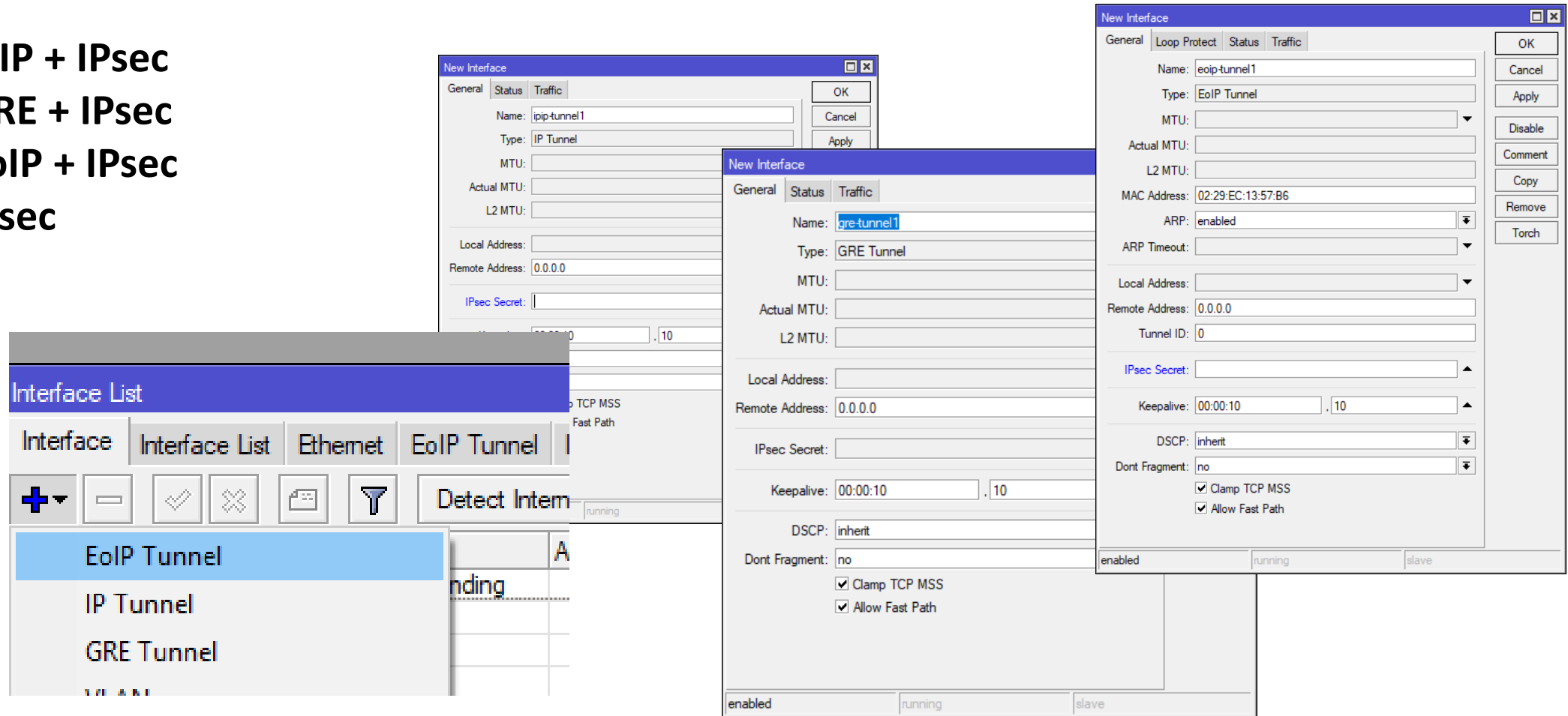
Wsparcie dla NAT jest możliwe. Dopuszczalna jest zmiana źródłowego adresu IP.

Występuje problem, gdy na tym samym NAT połączy się więcej niż jeden klient IPSEC.

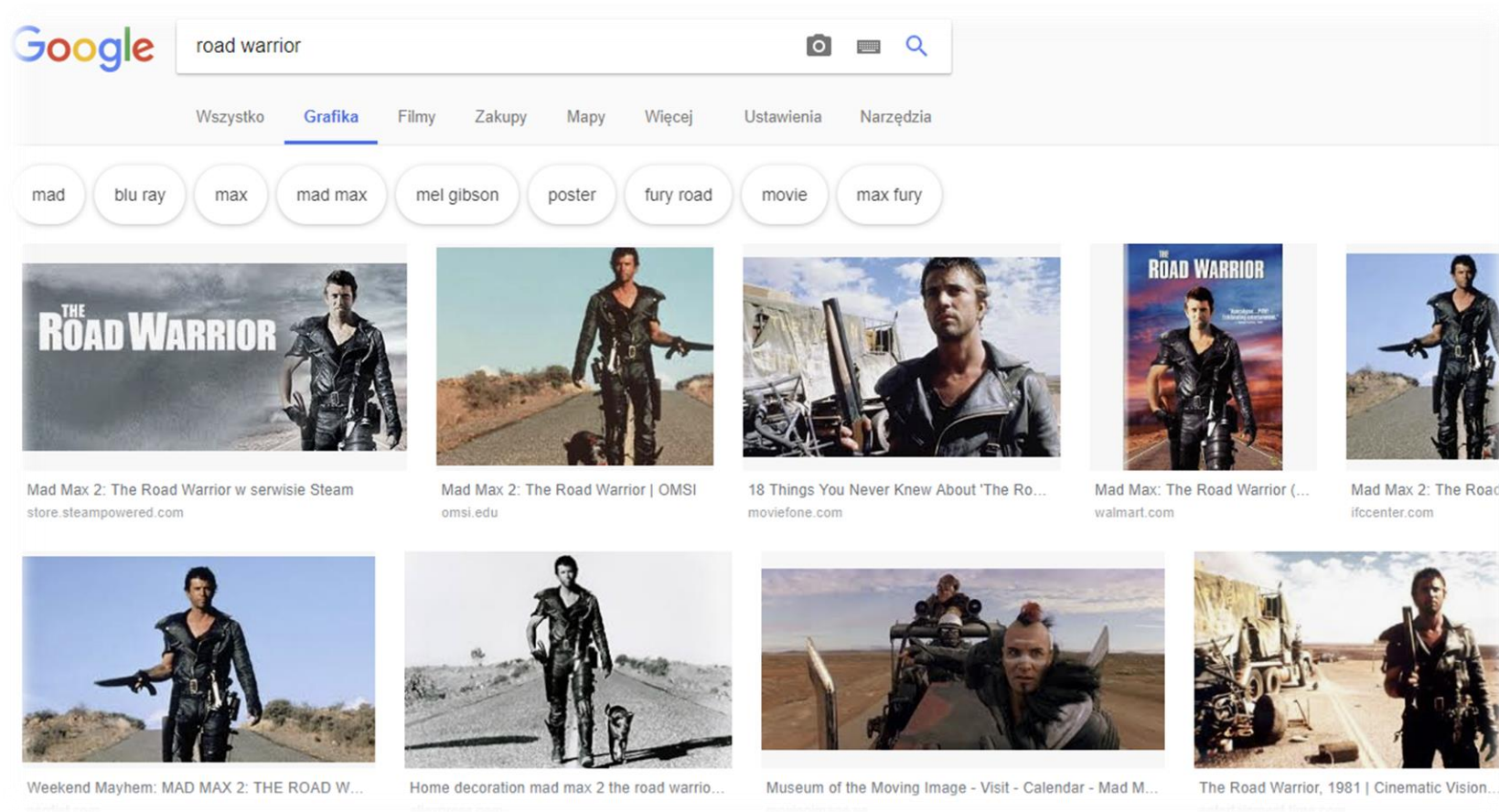
Rozwiązaniem jest wykorzystanie NAT-Traversal. Polega on na enkapsulacji ESP w UDP (domyślnie port 4500)

Połączenia site-site

IPIP + IPsec
GRE + IPsec
EoIP + IPsec
IPsec



Zdalni użytkownicy (road – warrior)



Jakie opcje (nie tylko IPSEC)

PPP (Point to Point Protocols)

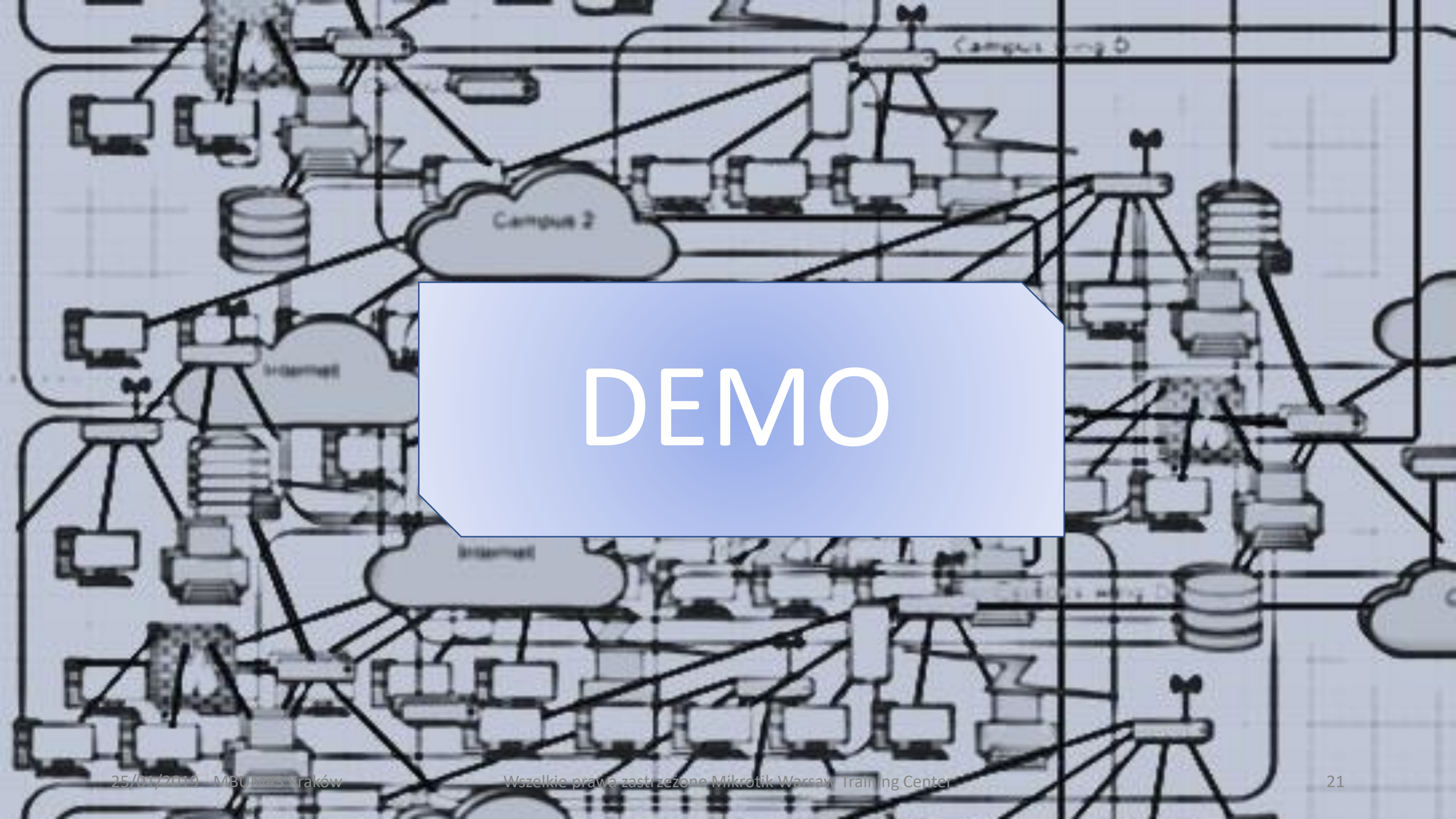
- PPTP (tcp, gre, niezalecane ze względów bezpieczeństwa)
- SSTP (tcp, słabe wsparcie natywne poza systemami Microsoft)
- L2TP (udp, szerokie wsparcie na praktycznie wszystkich OS)
- OVPN (udp/tcp, niepełna implementacja serwera na Mikrotik ☹️
- m.in. tylko tcp, brak push config, brak kompresji lzo)

IPSEC Xauth mode-config

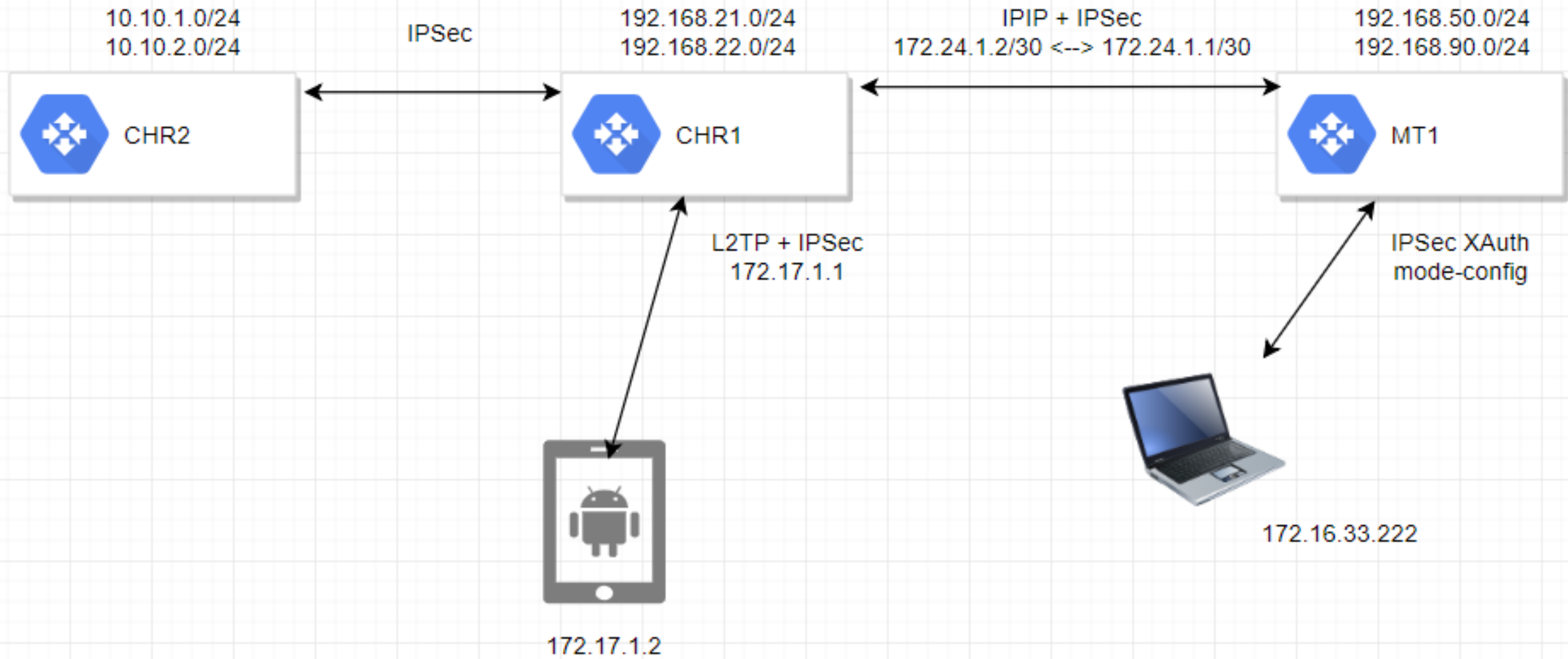
szerokie wsparcie na OS
nie jest oparty na tcp
częste wsparcie sprzętowe dla IPSEC
PSK, certyfikaty i dwuskładnikowe
push config (DNS, trasy routingu)

IKE2

to już nie dziś

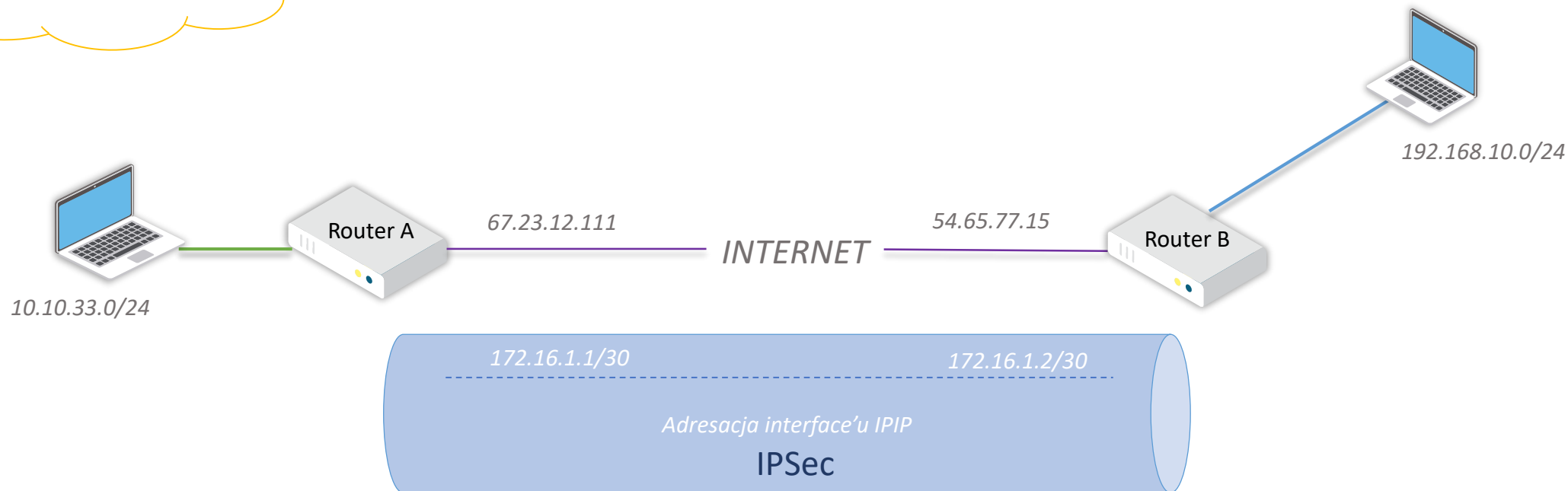
A complex network diagram in a light blue monochrome style serves as the background. It features numerous nodes representing various network components: desktop computers, server racks, storage units, and wireless access points. These nodes are interconnected by a dense web of lines representing network links. Several cloud shapes are integrated into the diagram, with labels such as 'Campus 2' and 'STAMPING' visible inside them. The overall layout suggests a multi-site or multi-segment network architecture.

DEMO



Site to site - IPIP+IPSec

Alternatywnie GRE



Pomogą nam „kreatory”

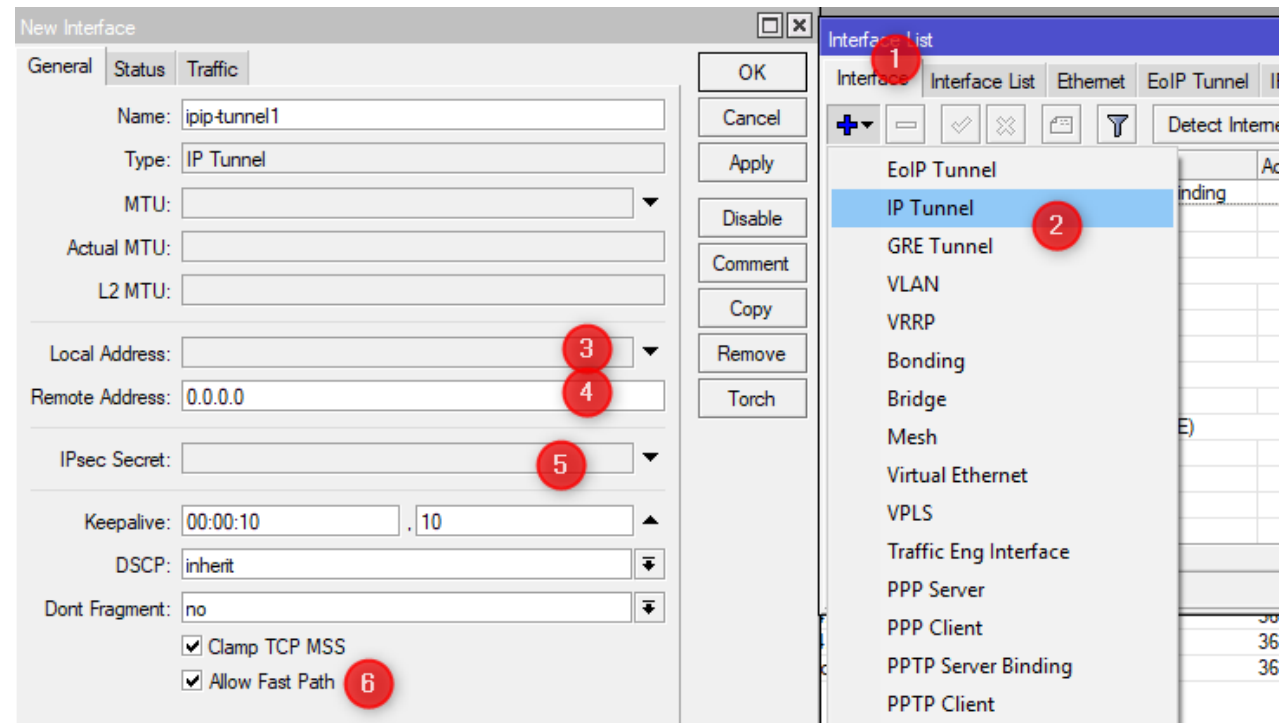
Utworzenie interfejsu dla zakończenia tunelu IPIP

Local Address : publiczny adres naszego koncentratora

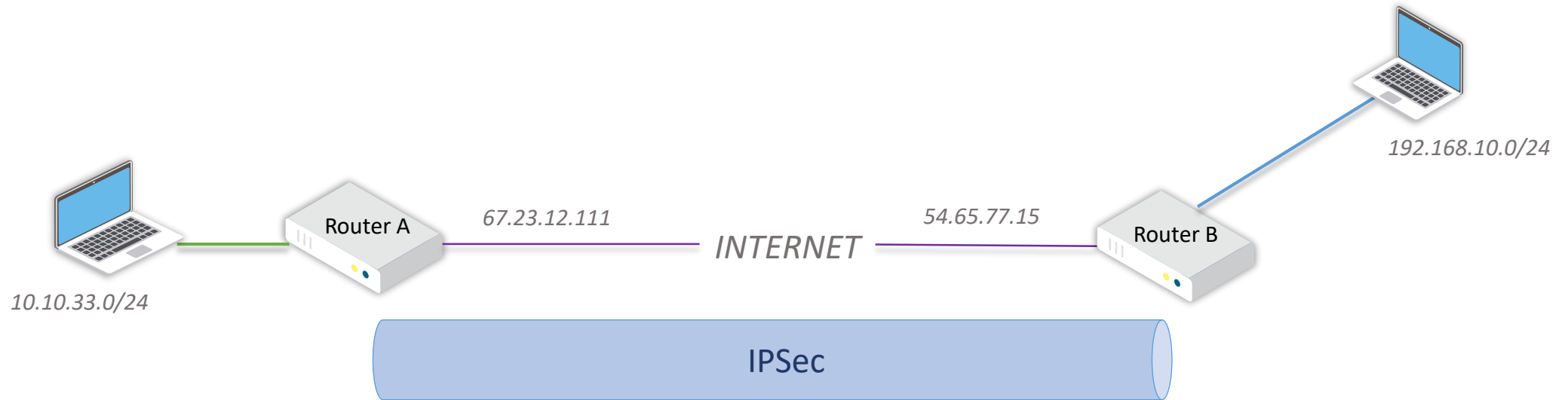
Remote Address : publiczny adres zakończenia tunelu

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

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

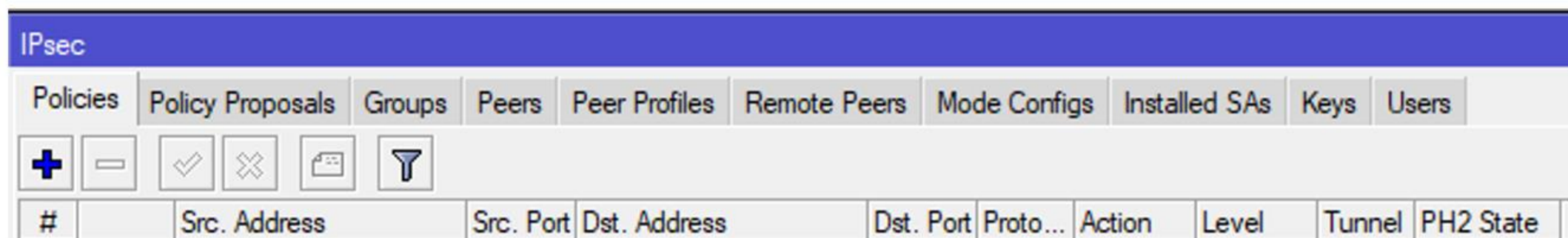
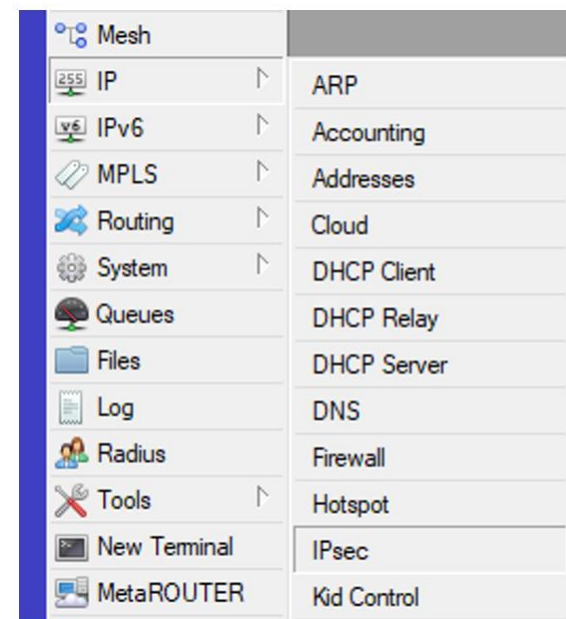


Site to site - IPSec

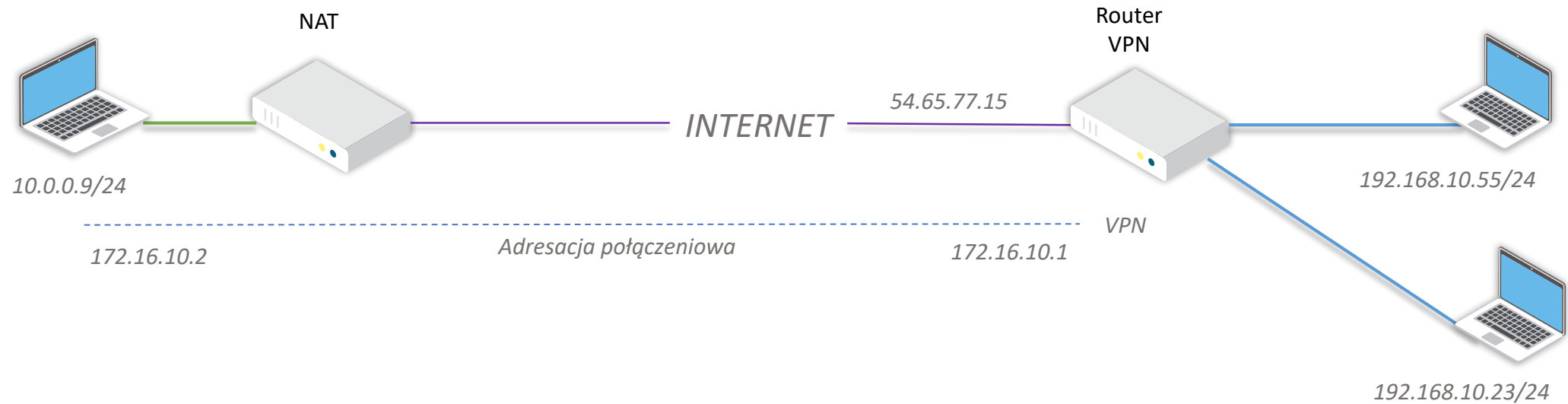


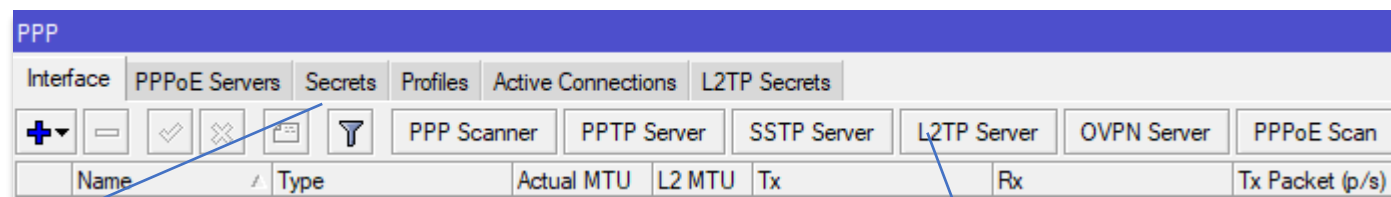
Określa jaki ruch ma
zostać obsłużony z IPsec,
określa jakie są parametry
szyfrowania (faza 2)

Określa zakończenia
tunelu oraz parametry dla
fazy 1



Użytkownicy mobilni – L2TP+IPSec





PPP Secret <piotr>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

L2TP Server

☒ Enabled

Max MTU:

Max MRU:

MRRU:

Keepalive Timeout:

Default Profile:

Max Sessions:

Authentication: ☒ mschap2 ☒ mschap1
☒ chap ☒ pap

Use IPsec:

IPsec Secret:

Caller ID Type:

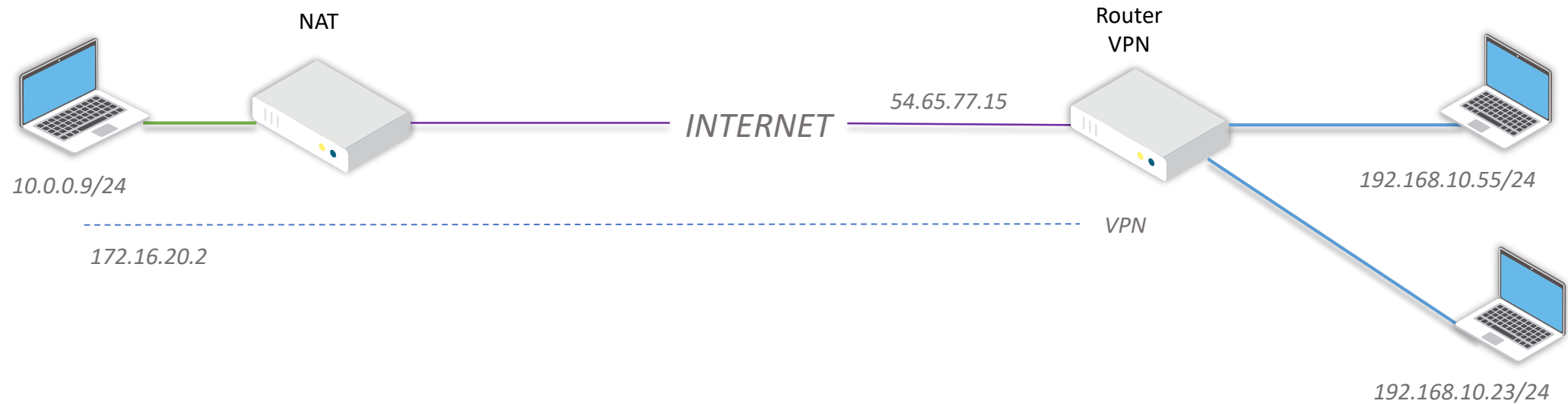
☐ One Session Per Host

☐ Allow Fast Path

Buttons: OK, Cancel, Apply

*Wymagana jest
zainstalowana i
włączona paczka PPP*

Użytkownicy mobilni – IPSec Xauth mode-config



IPSEC Xauth mode-config – peer profile

IPsec Peer Profile <ipsecPeerXAuth>

Name: ipsecPeerXAuth

Hash Algorithms: sha1

Encryption Algorithm:

☐ des	☐ 3des
☒ aes-128	☐ aes-192
☐ aes-256	☐ blowfish
☐ camellia-128	☐ camellia-192
☐ camellia-256	

DH Group:

☐ modp768	☒ modp1024
☐ ec2n155	☐ ec2n185
☐ modp1536	☐ modp2048
☐ modp3072	☐ modp4096
☐ modp6144	☐ modp8192
☐ ecp256	☐ ecp384
☐ ecp521	

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifebytes:

☒ NAT Traversal

DPD Interval: disable DPD s

DPD Maximum Failures: 5

OK Cancel Apply Copy Remove

IPsec

Policies Policy Proposals Groups Peers

+ -

Name

* default

xuath

New IPsec Group

Name: xauth

OK Cancel Apply

IPSEC Xauth mode-config – szablon Policy

IPsec Policy <192.168.50.0/24:0->172.16.36.0/24:0>

General Action Status

Src. Address: 192.168.50.0/24

Src. Port:

Dst. Address: 172.16.36.0/24

Dst. Port:

Protocol: 255 (all)

☒ Template

Group: xauth

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled Template Active

IPsec Policy <192.168.50.0/24:0->172.16.36.0/24:0>

General Action Status

Action: encrypt

IPsec Protocols: esp

SA Src. Address: 0.0.0.0

SA Dst. Address: 0.0.0.0

Proposal: default

OK

Cancel

Apply

Disable

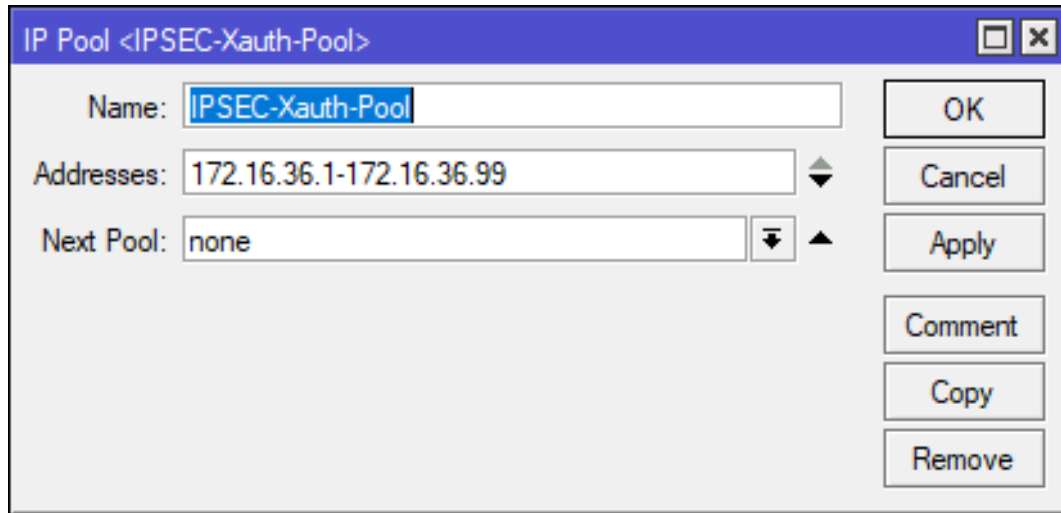
Comment

Copy

Remove

enabled Template Active

IPSEC Xauth mode-config – push config



IP Pool <IPSEC-Xauth-Pool>

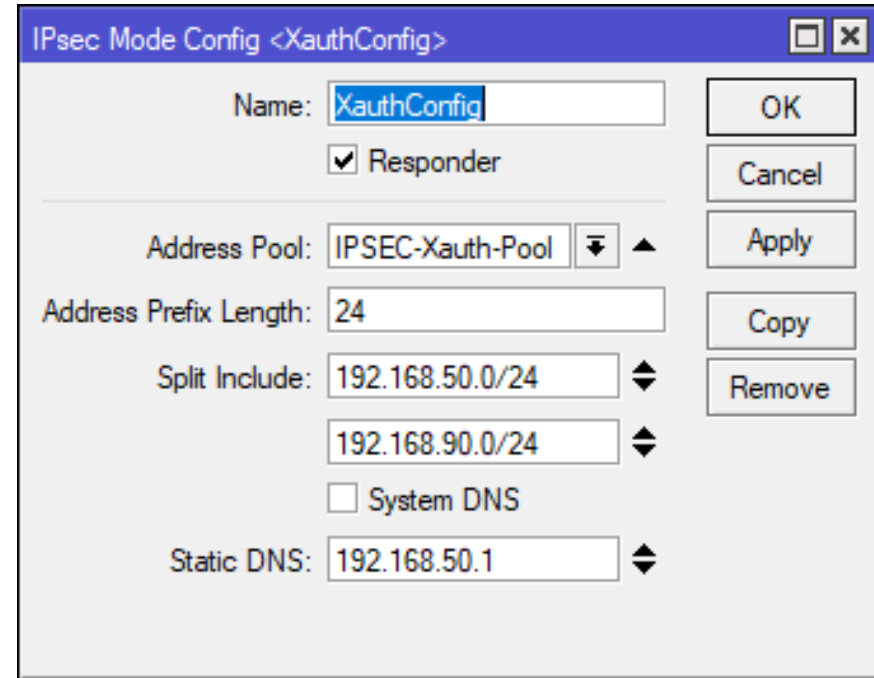
Name: IPSEC-Xauth-Pool

Addresses: 172.16.36.1-172.16.36.99

Next Pool: none

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

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



IPsec Mode Config <XauthConfig>

Name: XauthConfig

☒ Responder

Address Pool: IPSEC-Xauth-Pool

Address Prefix Length: 24

Split Include: 192.168.50.0/24, 192.168.90.0/24

☐ System DNS

Static DNS: 192.168.50.1

Buttons: OK, Cancel, Apply, Copy, Remove

Responder = YES (nasz Mikrotik będzie koncentratorom IPSEC)

Split Include – trasy przesyłane do Klienta

IPSEC Xauth mode-config – peer config

IPsec Peer <0.0.0.0/0>

General Advanced

Address: 0.0.0.0/0

Port:

Local Address:

Profile: ipsecPeerXAuth

Auth. Method: pre shared key xauth

Exchange Mode: main

☒ Passive

Secret: tajne

XAuth Login:

XAuth Password:

OK Cancel Apply Disable Comment Copy Remove

enabled responder

IPsec Peer <0.0.0.0/0>

General Advanced

Policy Template Group: xuath

Notrack Chain:

☐ Send Initial Contact

My ID Type: auto

Mode Configuration: XauthConfig

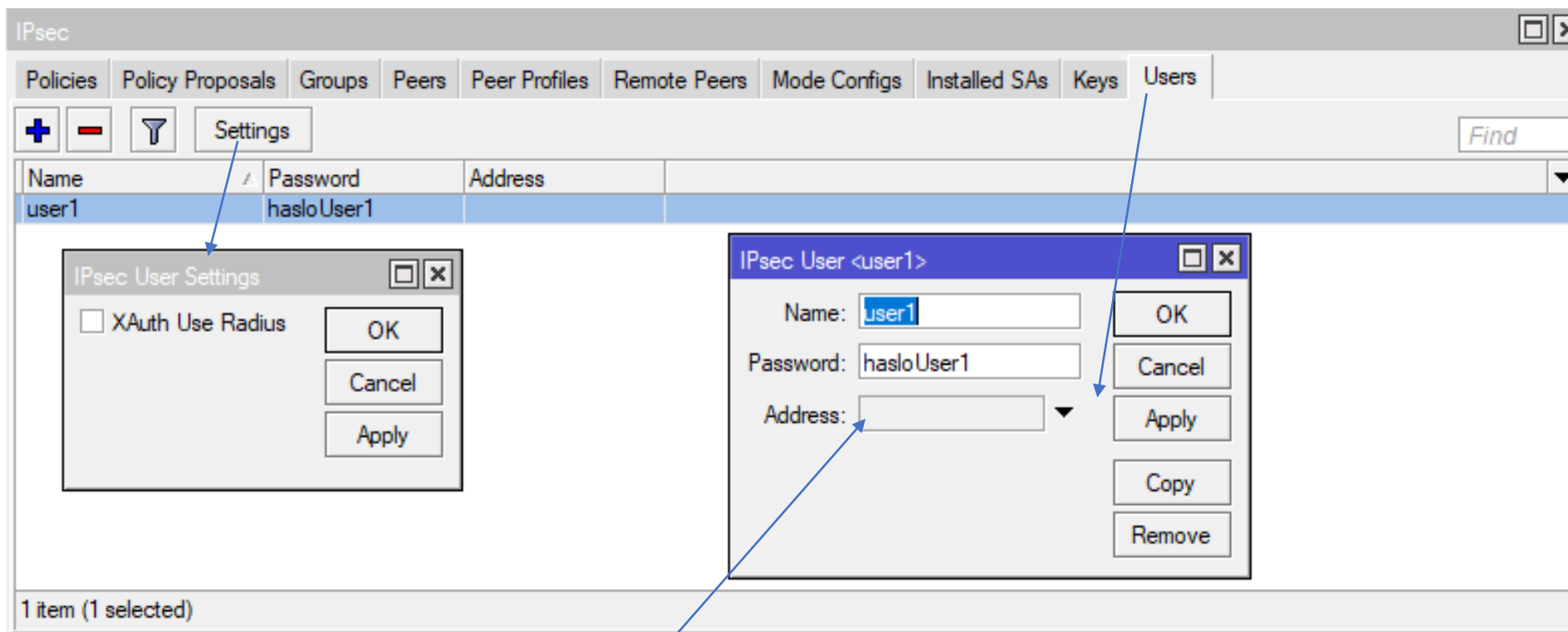
Generate Policy: port strict

Compatibility Options: ☐ skip peer id validation

OK Cancel Apply Disable Comment Copy Remove

enabled responder

IPSEC Xauth mode-config – użytkownicy



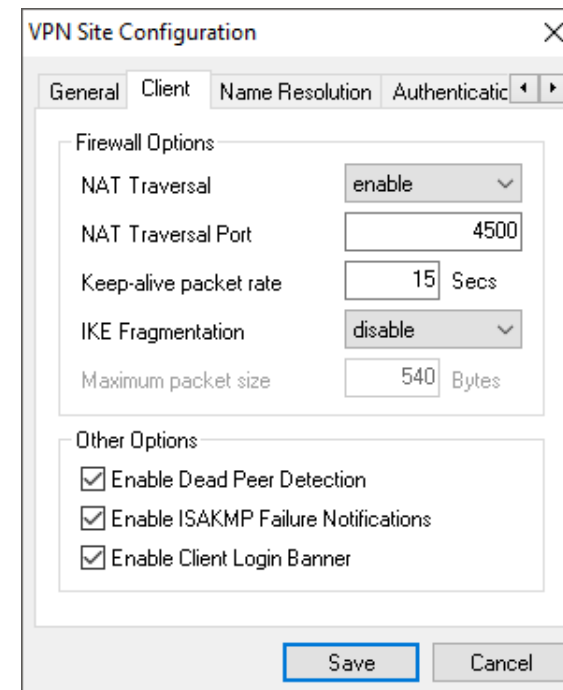
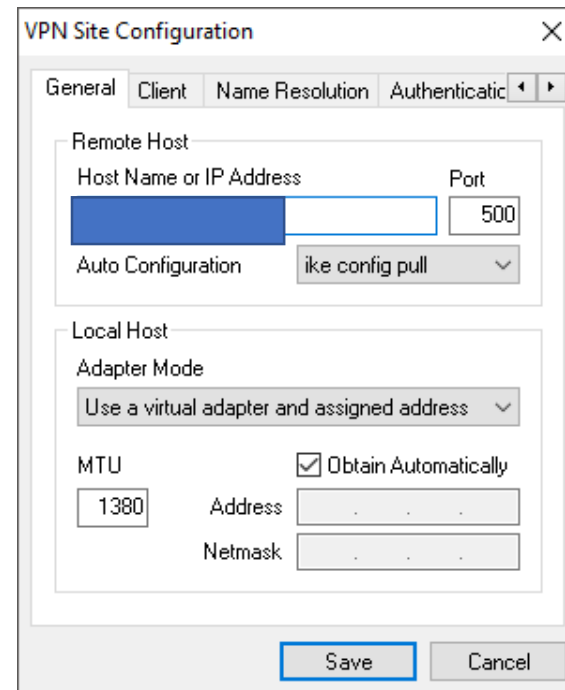
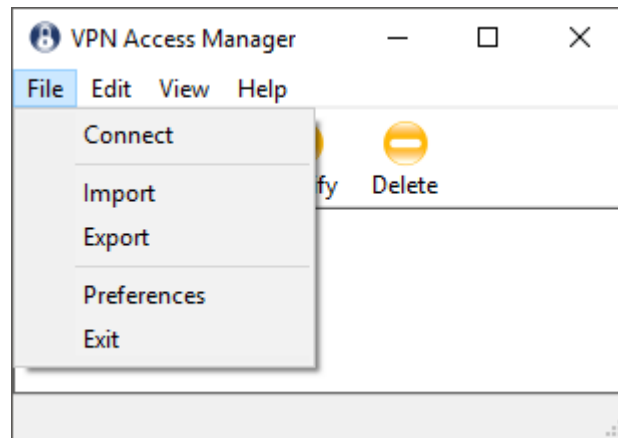
Przypisanie statycznie adresu IP dla Klienta, jeśli puste zostanie wybrany z puli

IPSEC Xauth mode-config – App Client dla MS Windows



ShrewClient VPN

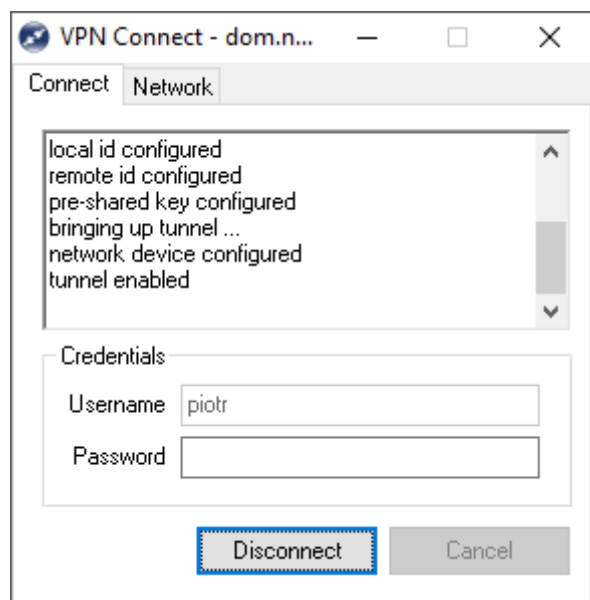
<https://www.shrew.net/download>



IPSEC Xauth mode-config – App Client dla MS Windows

The image displays four sequential screenshots of the Mikrotik WinBox 'VPN Site Configuration' dialog, illustrating the configuration steps for an IPSEC Xauth mode client.

- Client Tab:** Shows the 'Authentication Method' set to 'Mutual PSK + XAuth'. Under the 'Local Identity' sub-tab, the 'Identification Type' is set to 'IP Address'. The 'Address String' field is empty. The checkbox 'Use a discovered local host address' is checked.
- Authentication Tab:** Displays the 'Proposal Parameters' section with the following settings: Exchange Type (main), DH Exchange (group 2), Cipher Algorithm (aes), Cipher Key Length (128 Bits), Hash Algorithm (sha1), Key Life Time limit (86400 Secs), and Key Life Data limit (0 Kbytes). The 'Enable Check Point Compatible Vendor ID' checkbox is unchecked.
- Phase 1 Tab:** Shows the 'Proposal Parameters' section with the following settings: Transform Algorithm (esp-aes), Transform Key Length (128 Bits), HMAC Algorithm (sha1), PFS Exchange (disabled), Compress Algorithm (disabled), Key Life Time limit (3600 Secs), and Key Life Data limit (0 Kbytes).
- Policy Tab:** Displays the 'IPSEC Policy Configuration' section. The 'Policy Generation Level' is set to 'unique'. The checkbox 'Maintain Persistent Security Associations' is unchecked, and 'Obtain Topology Automatically or Tunnel All' is checked. Below this is a 'Remote Network Resource' section with 'Add', 'Modify', and 'Delete' buttons.



Wiersz polecenia

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.23.254	192.168.23.225	60
0.0.0.0	0.0.0.0	0.0.0.0	172.16.101.1	172.16.101.245	31
127.0.0.0	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
172.16.36.0	255.255.255.0	255.255.255.0	On-link	172.16.36.1	311
172.16.36.1	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311
172.16.36.255	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311
172.16.101.0	255.255.255.0	255.255.255.0	On-link	172.16.101.245	291
172.16.101.245	255.255.255.255	255.255.255.255	On-link	172.16.101.245	291
172.16.101.255	255.255.255.255	255.255.255.255	On-link	172.16.101.245	291
192.168.23.0	255.255.255.0	255.255.255.0	On-link	192.168.23.225	316
192.168.23.225	255.255.255.255	255.255.255.255	On-link	192.168.23.225	316
192.168.23.255	255.255.255.255	255.255.255.255	On-link	192.168.23.225	316
192.168.50.0	255.255.255.0	255.255.255.0	On-link	172.16.36.1	56
192.168.50.255	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311
192.168.90.0	255.255.255.0	255.255.255.0	On-link	172.16.36.1	56
192.168.90.255	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.23.225	255.255.255.255	255.255.255.255	On-link	192.168.23.225	316
172.16.101.245	255.255.255.255	255.255.255.255	On-link	172.16.101.245	291
172.16.36.1	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.23.225	255.255.255.255	255.255.255.255	On-link	192.168.23.225	316
172.16.101.245	255.255.255.255	255.255.255.255	On-link	172.16.101.245	291
172.16.36.1	255.255.255.255	255.255.255.255	On-link	172.16.36.1	311

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

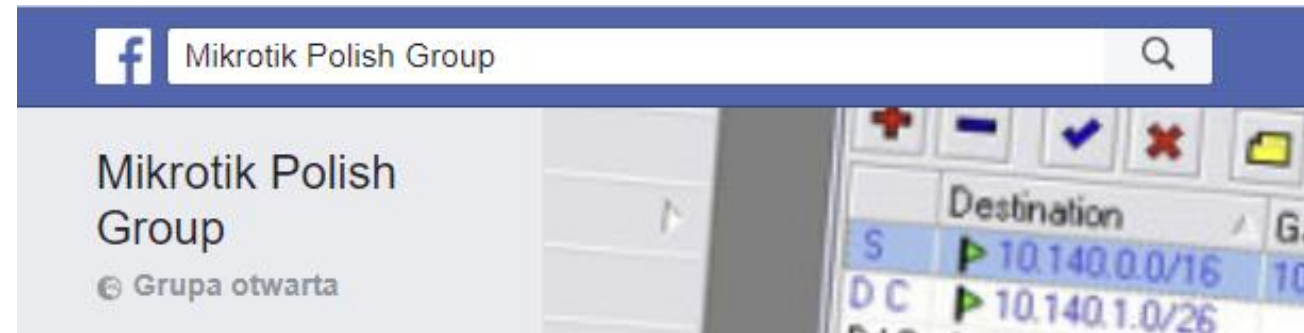
Policies											
Policy Proposals											
Groups											
Peers											
Peer Profiles											
Remote Peers											
Mode Configs											
Installed SAs											
Keys											
Users											
+ - ✓ ✗ [icon] [icon]											
#		Src. Address	Src. Port	Dst. Address	Dst. Port	Proto...	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/>

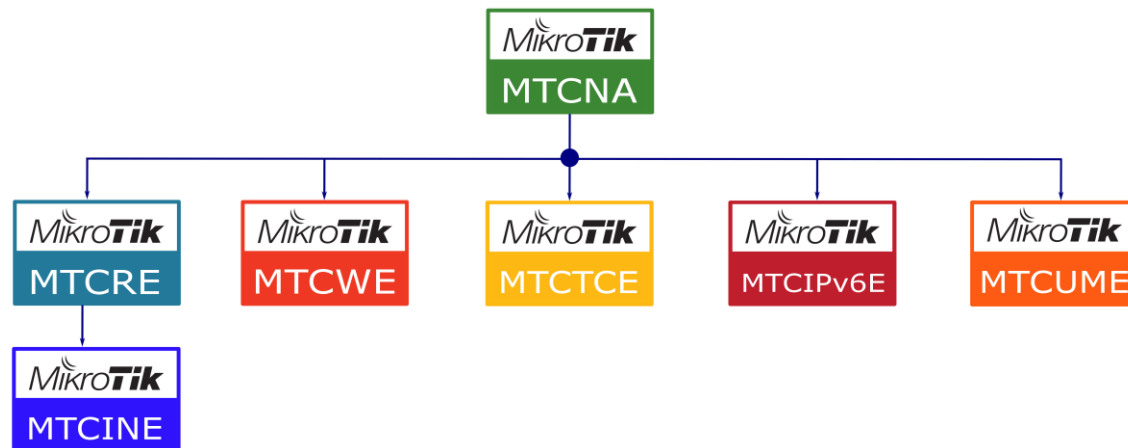
Ponad 2500 osób 😊 !!!



<https://wiki.mikrotik.com>

Zapraszamy na :

Szkolenia certyfikowane Mikrotik



Autorskie warsztaty



<https://mwtc.pl>