Profilowanie Sesji VPN

MBUM 2021
Grzegorz Rakuś

Parę słów o mnie

Specjalizuję się w rozwiązaniach VPN (Site-to-Site / Remote Access),
Firewallach L4 / L7 oraz systemach AAA (RADIUS / MFA / SAML)

- administracja i utrzymanie multi-platformowej infrastruktury sieciowej
- zarządzanie bezpieczeństwem sieci (L2 / L3 / 802.1x / NGFW)

- wsparcie dla środowisk MS (AD / Hyper-V / Microsoft 365 / Azure)

- wdrożenia / konsultacje / doradztwo IT

MTCNA / MTCRE / MTCTCE / MTCSE

CCNA CyberOps / Security / Routing and Switching

grzegorz.rakus@gmail.com

linkedin.com/in/grzegorz-rakus/

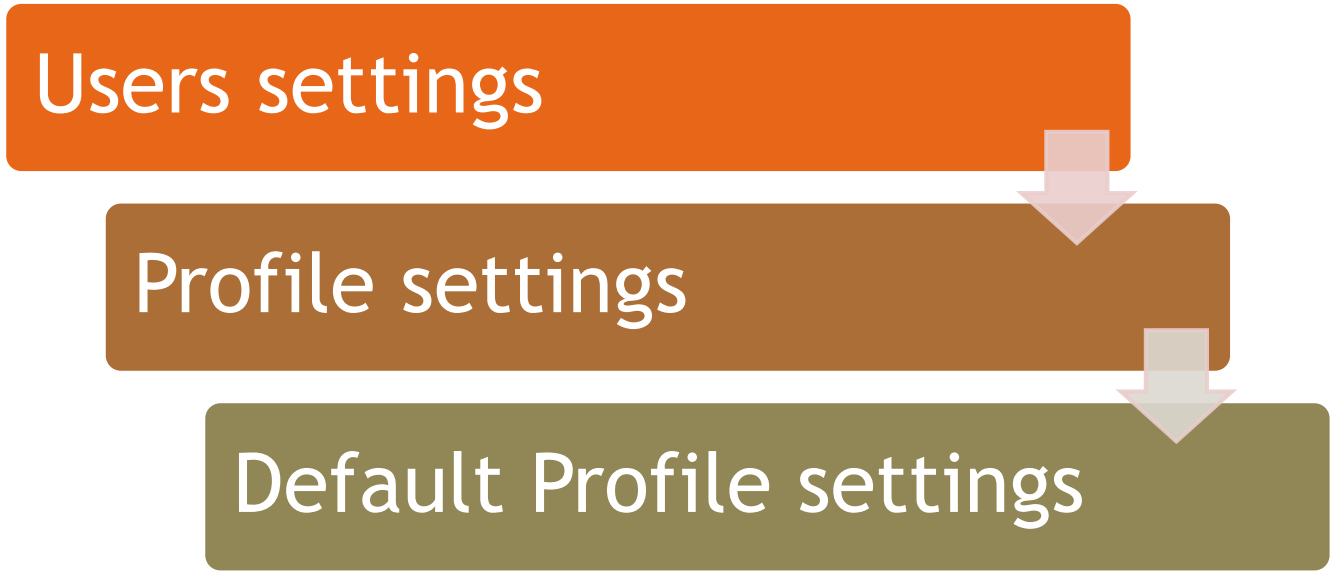
Prezentacja przedstawia możliwości separacji / rozdzielenia połączeń VPN w oparciu o grupy domenowe Active Directory.

Wymagania:

- RouterOS zintegrowany z Active Directory za pomocą protokołu RADIUS

  np. przy użyciu NPS (Network Policy Server) wbudowanego w Windows Server
  jak skonfigurować AD / NPS / CA przedstawia prezentacja - https://mbum.pl/archive/prelekcja-CAPsMAN-WPA2EAP-AD.pdf
- Certyfikat dla protokołów korzystających z SSL / TLS (np. dla SSTP)
- Skonfigurowane polityki / zasady na serwerze RADIUS
- Skonfigurowany RouterOS (Profile / Firewall / Interfejsy)

Kolejność przetwarzania reguł dla Serwerów PPP w RouterOS



Kolejność przetwarzania reguł dla Serwera PPP

(przykład dla protokołu PPTP)

Users settings

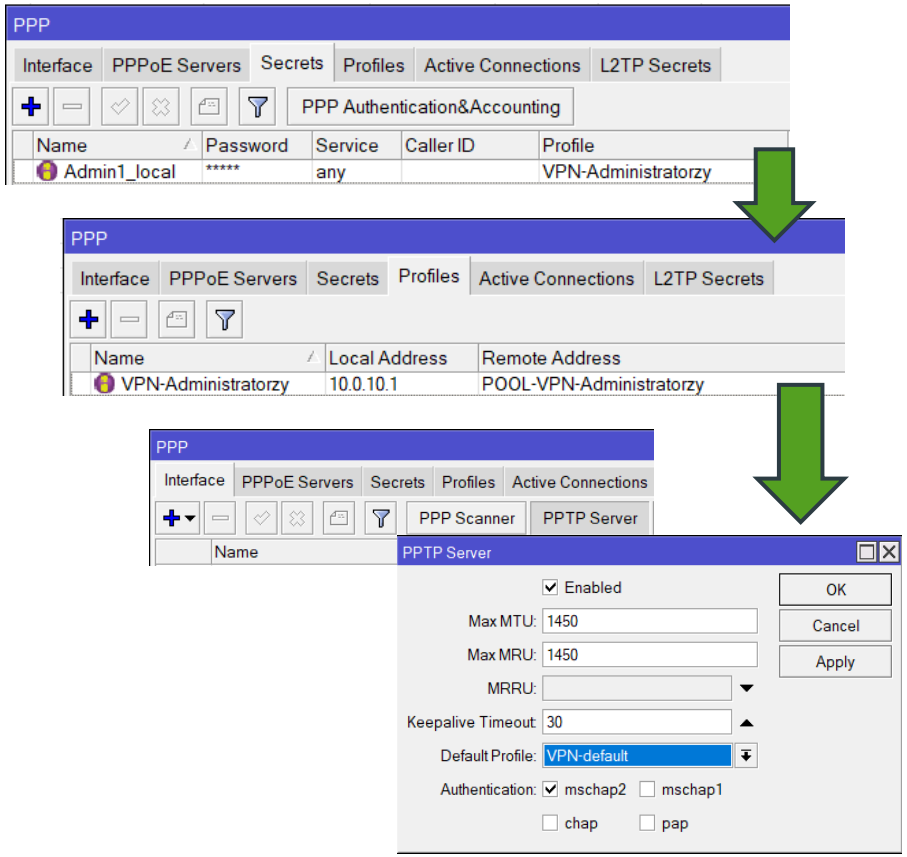
(zakładka Secret)

Profile settings

(zakładka Profiles)

Default Profile settings

(zakładka Default Profile w PPTP Server)



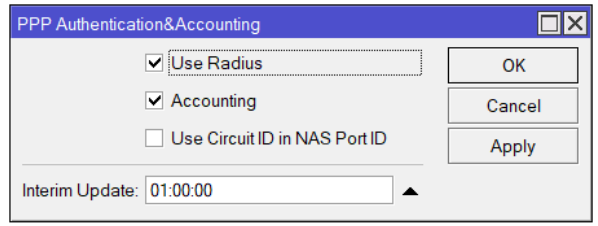
Kolejność przetwarzania reguł dla Serwera PPP z aktywnym protokołem RADIUS

Users settings

*Radius settings

Profile settings

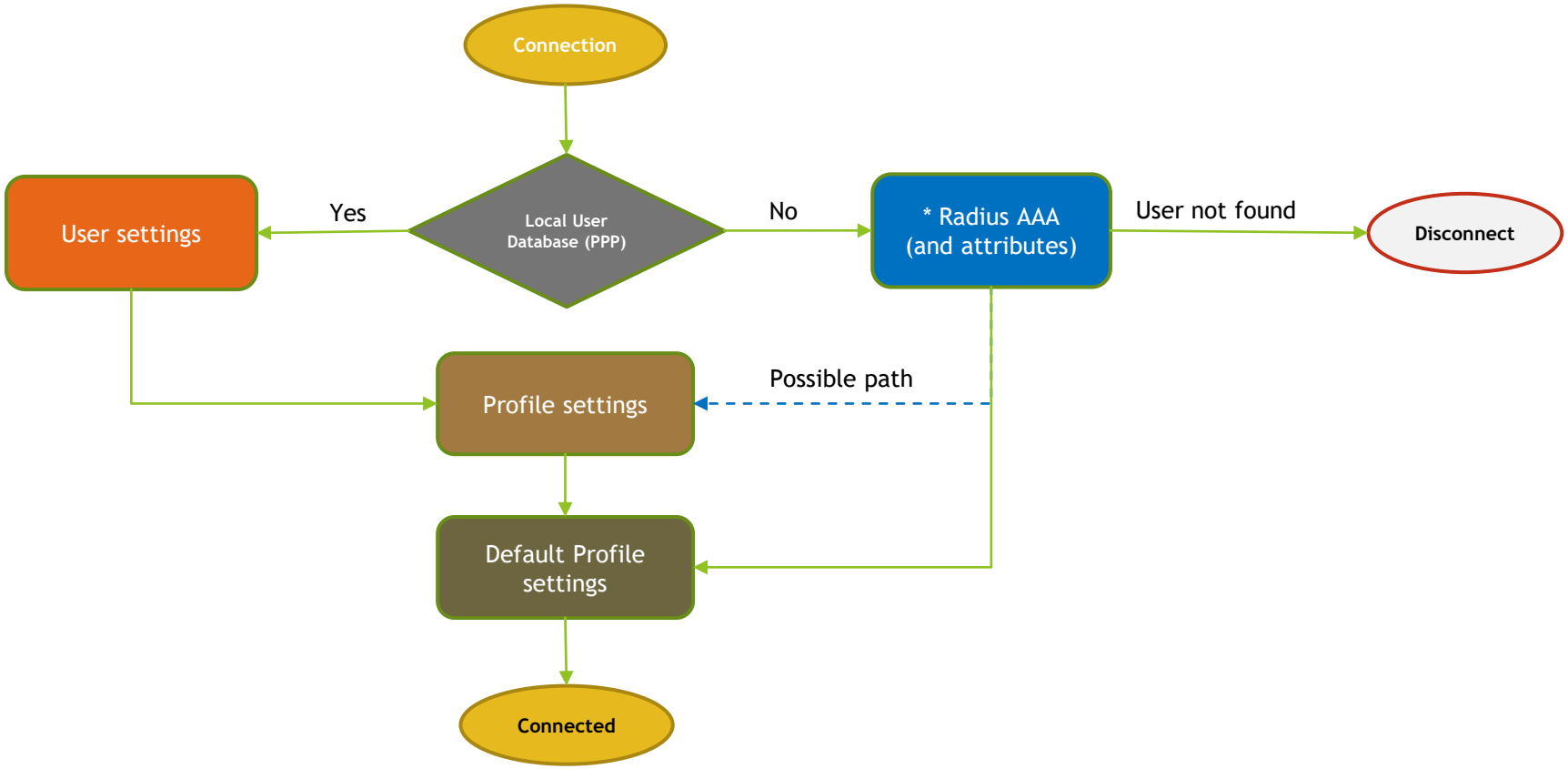
Default Profile settings



MikroTik WIKI

*** The RADIUS server database is consulted only if no matching user access record is found in the router's local database.**

Schemat blokowy dla sesji PPP z aktywnym protokołem RADIUS



MikroTik WIKI

*** The attributes received from the RADIUS server override the ones set in the default profile, but if some parameters are not received they are taken from the respective default profile.**

RADIUS Vendor-Specific Attributes (VSA) – RFC2865

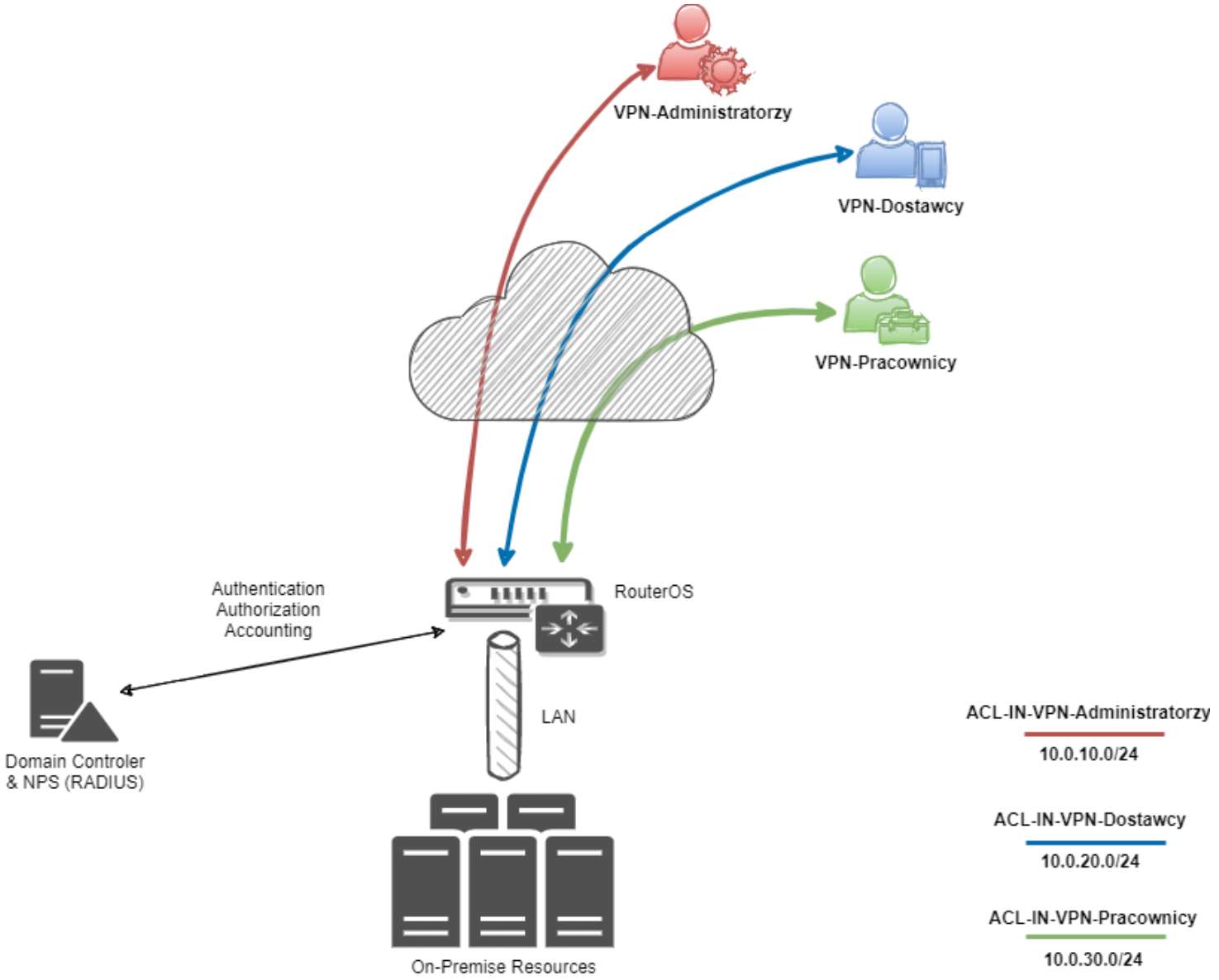
MikroTik WIKI

Attribute	Vendor ID	Type ID	Value type	Packet type	Description
Mikrotik-Group	14988 (Mikrotik)	3	string	Access-Accept	User's group for local users. HotSpot profile for HotSpot users. **PPP profile for PPP users.**

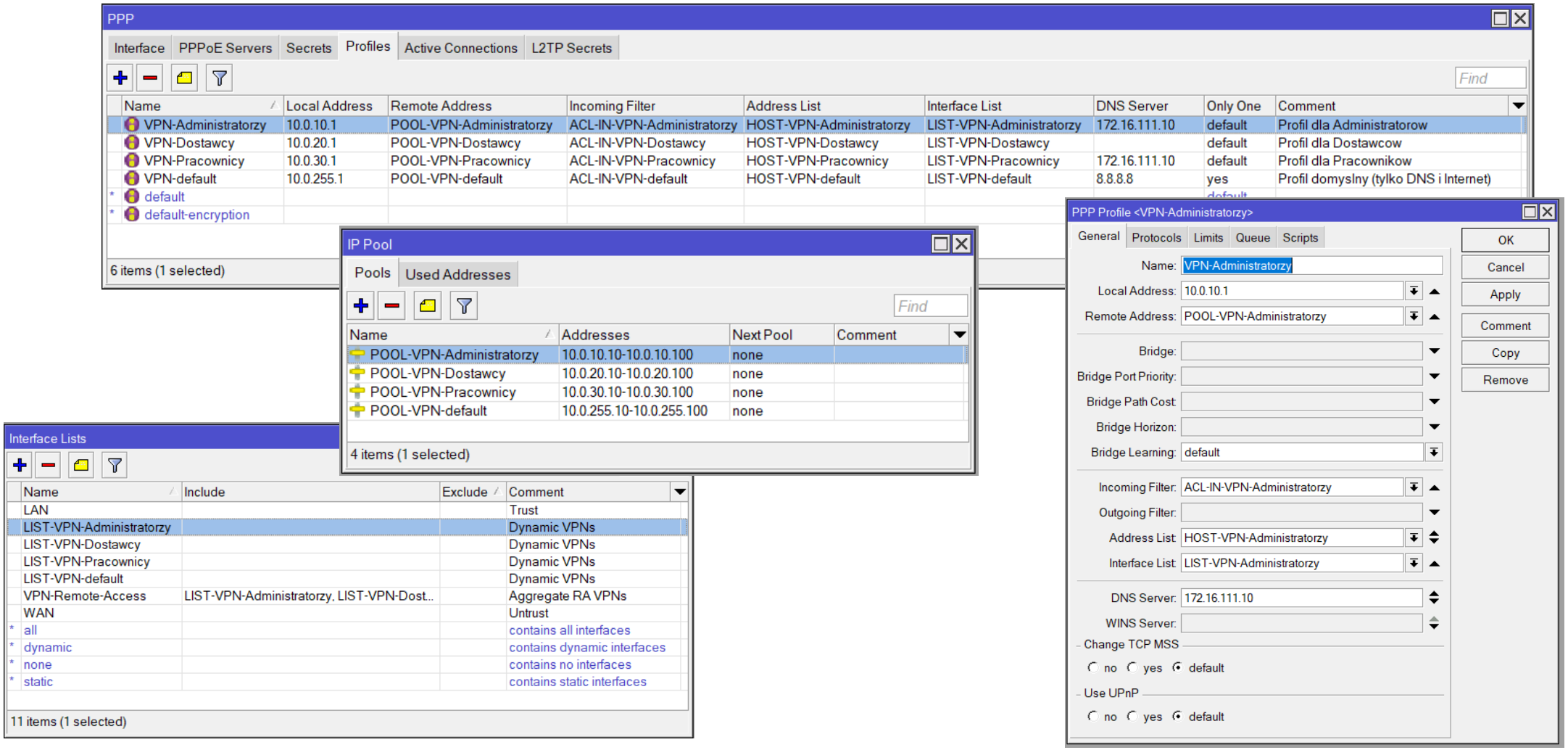
https://help.mikrotik.com/docs/display/ROS/User+Manager#UserManager-Attributes
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client/reference_dictionary

https://datatracker.ietf.org/doc/html/rfc2865#section-5.26

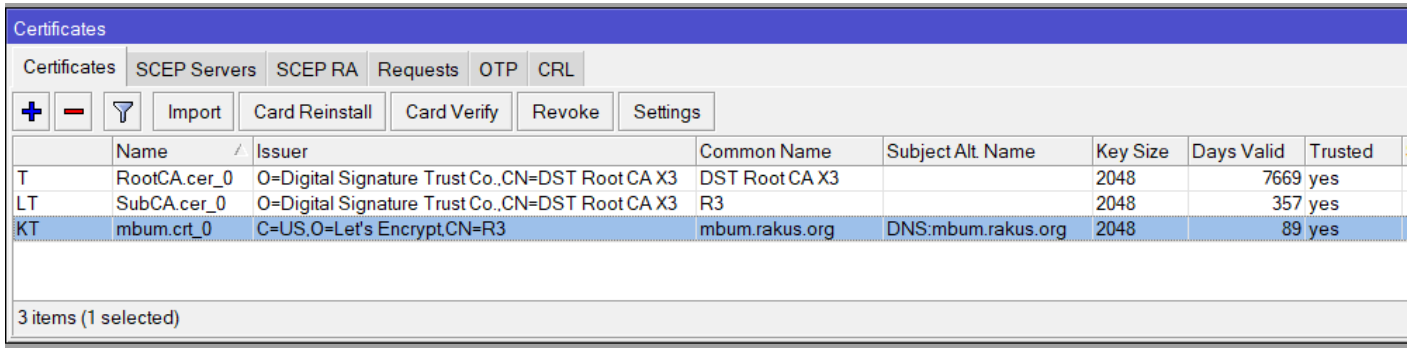
Schemat środowiska testowego

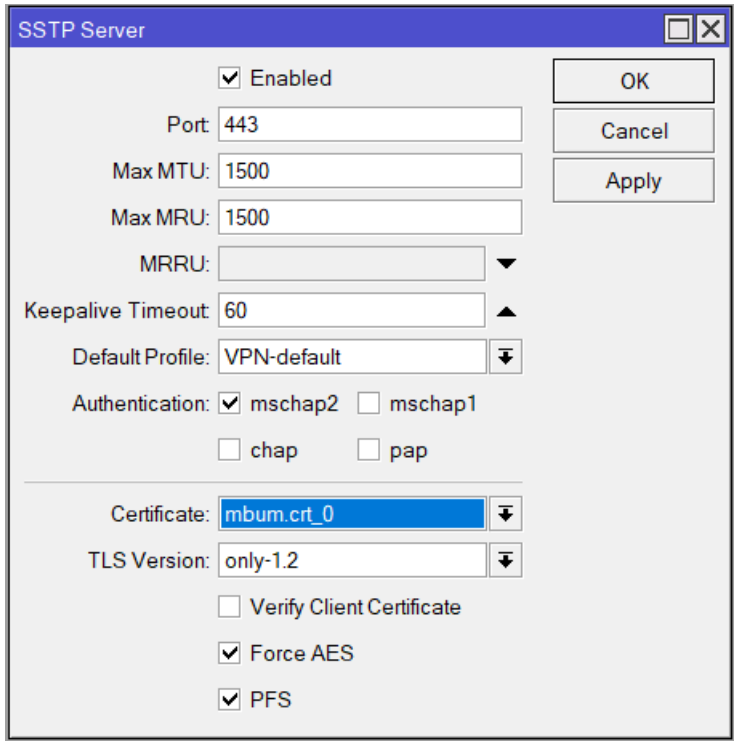


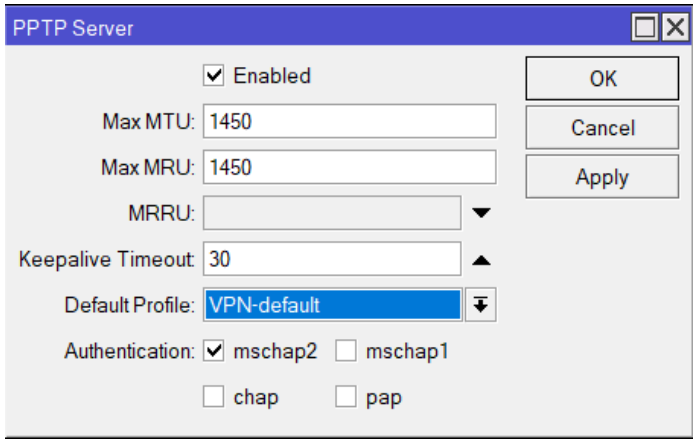
Ustawienia dla PPP Profiles / IP Pool / Interface Lists



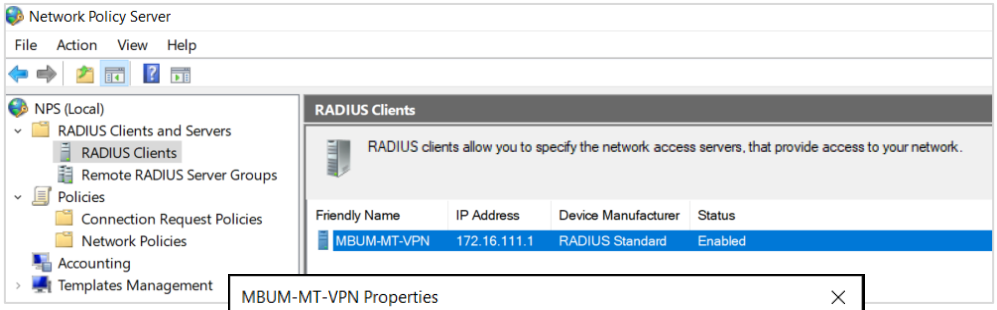
Ustawienia dla Certificates / PPP Servers

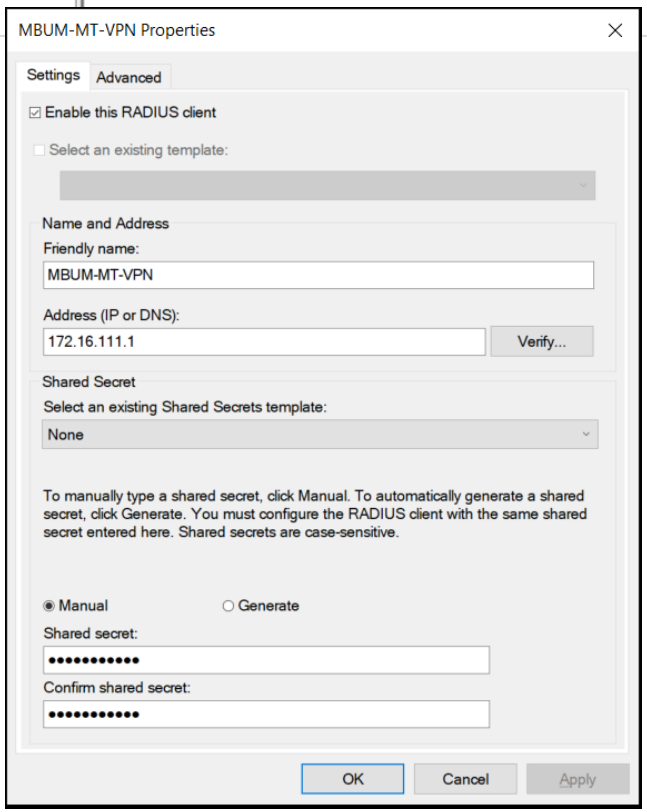


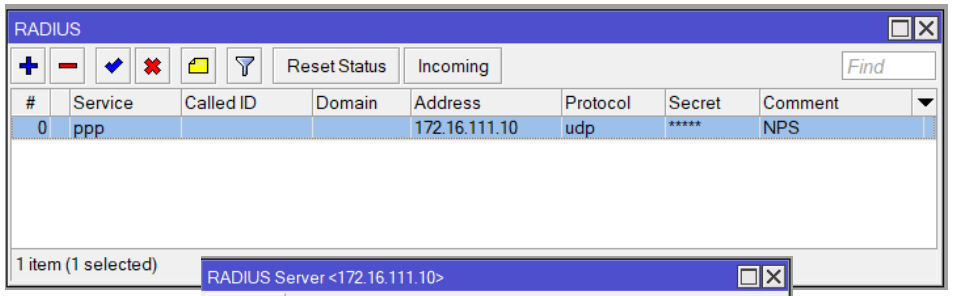


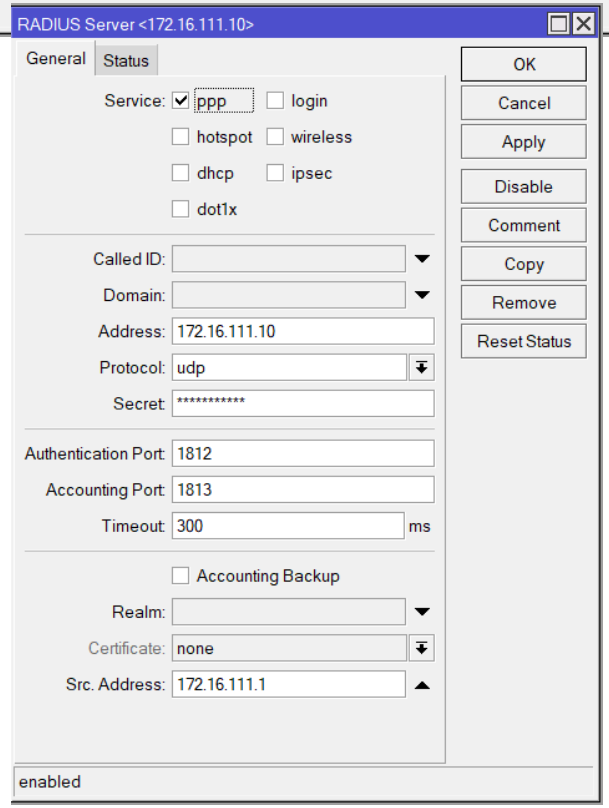


Konfiguracja Windows Server NPS <-> RouterOS (przypomnienie)





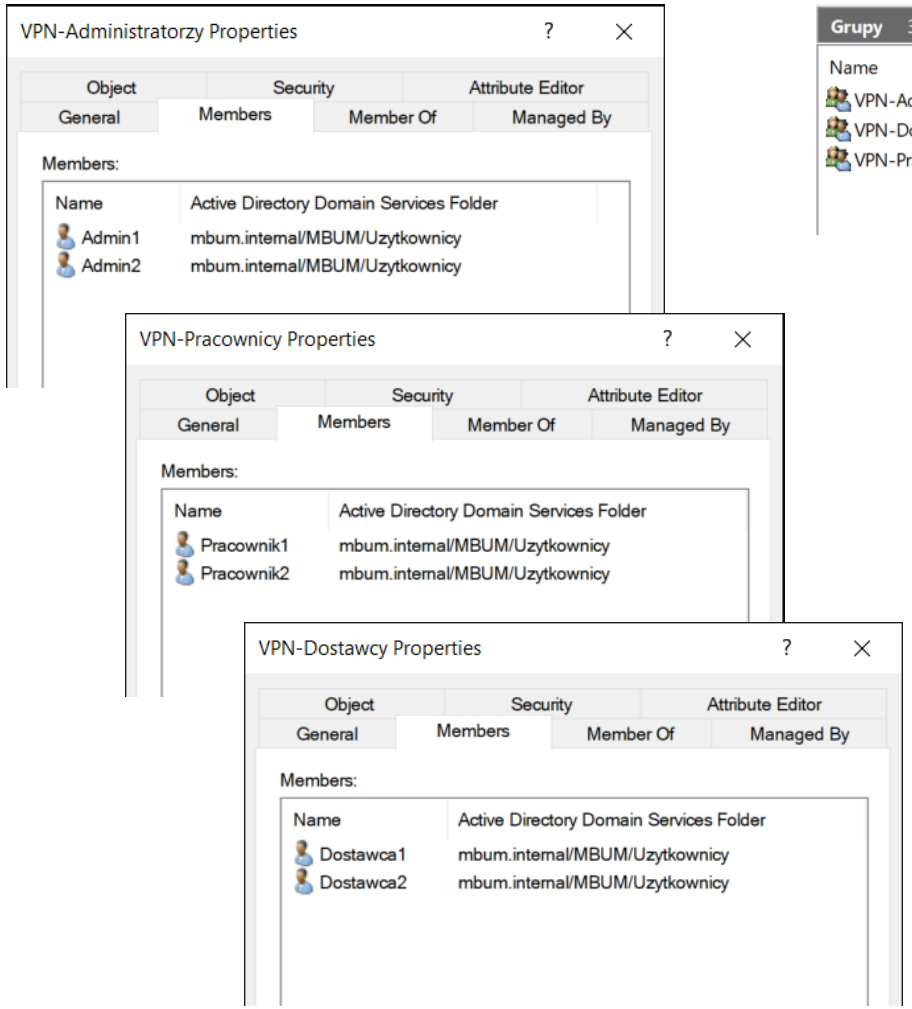


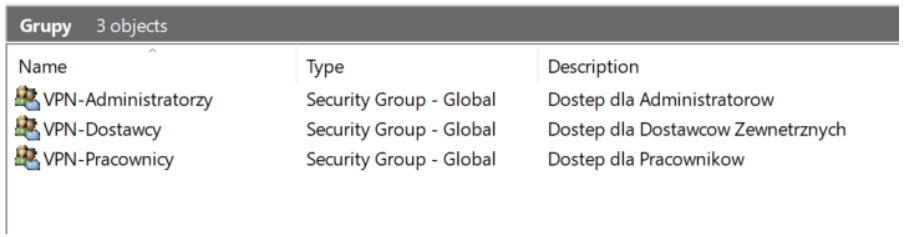


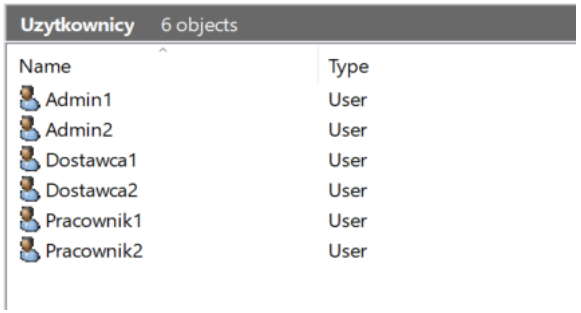
Fix for Windows Server 2019 bug Radius connections

- (open explicitly ports for 1812 / 1813 UDP on Windows Firewall) **OR** (run Powershell / cmd command : **sc sidtype IAS unrestricted**)

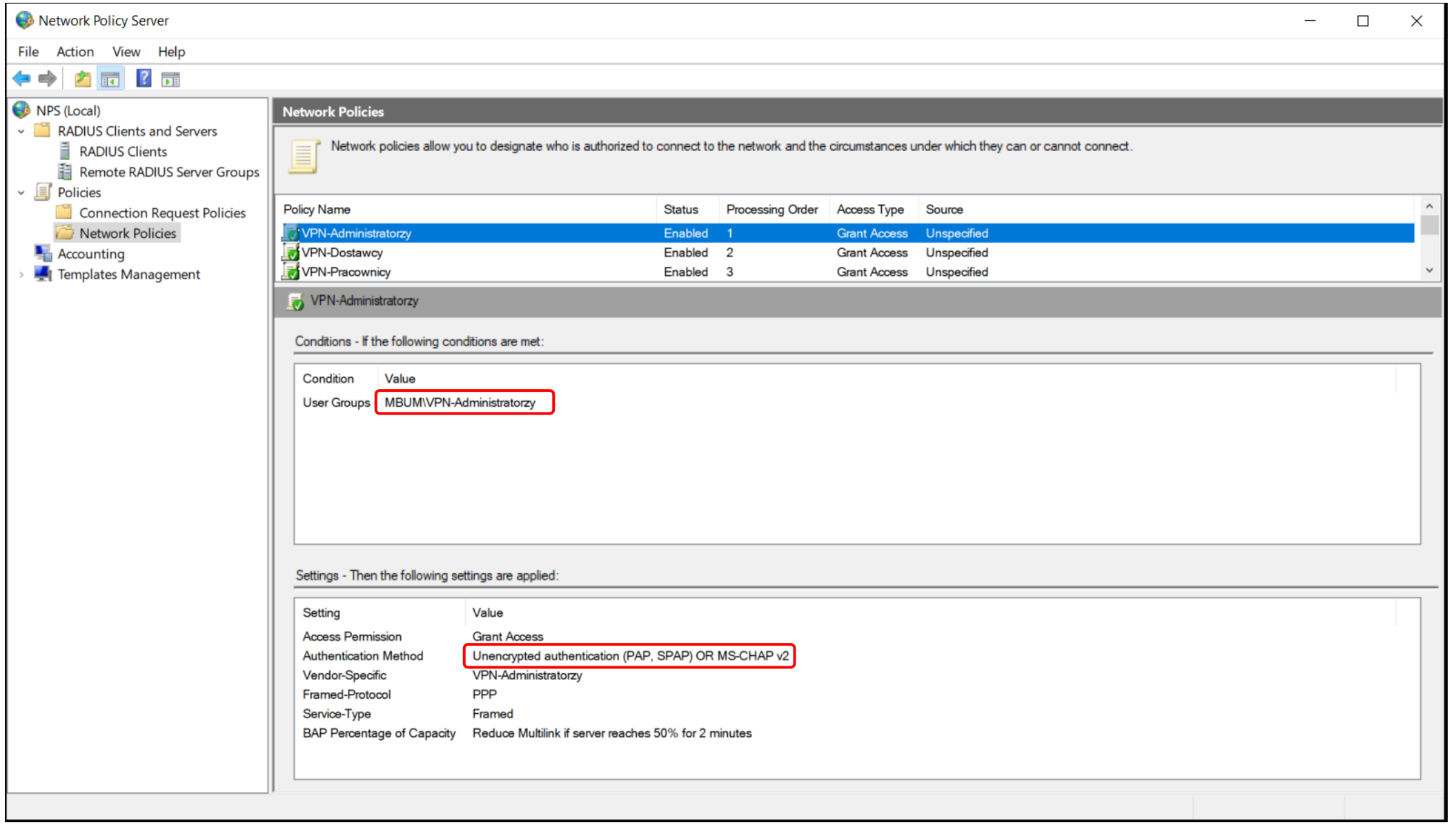
Konta i grupy w Active Directory





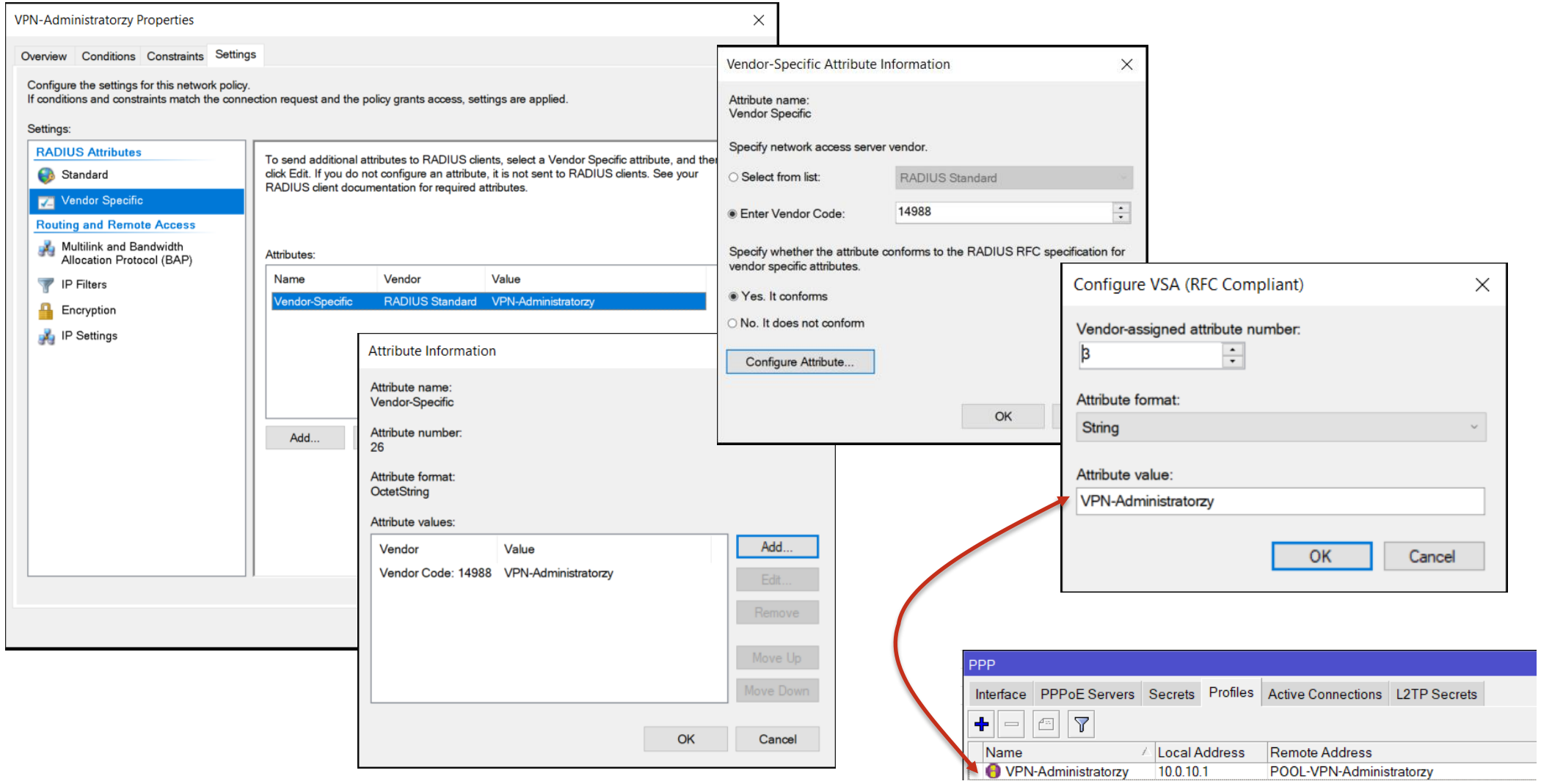


Konfiguracja Windows Server NPS – Network Policies



Konfiguracja NPS - Network Policies Properties (ustawienia dla VSA)

(*przykład dla grupy VPN-Administratorzy)



Konfiguracja Firewall - PPP Jump rule !

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters | Find: all

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface List	Dst. Address List	Log	Log Prefix	Jump Target	Bytes	Packets	Comment
18	accept	forward								no			168.9 MiB	321 934	defconf: accept established,related, untracked
19	jump	forward						VPN-Remote-Access		yes	== PPP JUMP ==	ppp	26.3 KiB	426	JUMP to PPP chains (VPN only)
20	drop	forward						VPN-Remote-Access		yes	== BLOCK VPN ==		6.8 KiB	117	BLOCK vpn traffic (last rule for all ACL)
21	drop	forward								no			0 B	0	defconf: drop invalid
22	drop	forward						WAN		no			0 B	0	defconf: drop all from WAN not DSTNATed

Interface Lists

Find

	Name	Include	Exclude	Comment
	LAN			Trust
	LIST-VPN-Administratorzy			Dynamic VPNs
	LIST-VPN-Dostawcy			Dynamic VPNs
	LIST-VPN-Pracownicy			Dynamic VPNs
	LIST-VPN-default			Dynamic VPNs
	VPN-Remote-Access	LIST-VPN-Administratorzy, LIST-VPN-Dost...		Aggregate RA VPNs
	WAN			Untrust
*	all			contains all interfaces
*	dynamic			contains dynamic interfaces
*	none			contains no interfaces
*	static			contains static interfaces

11 items (1 selected)

PPP Profile <VPN-Administratorzy>

General | Protocols | Limits | Queue | Scripts

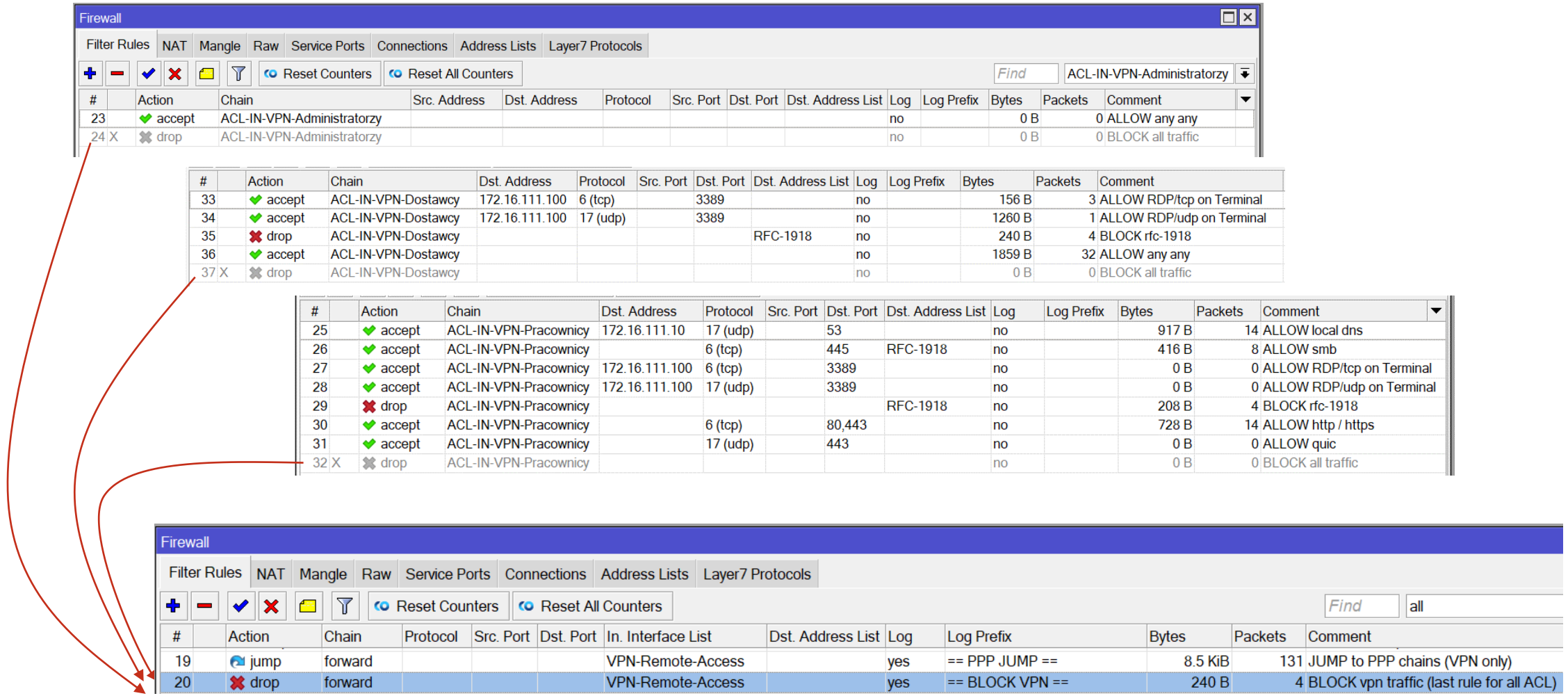
OK | Cancel | Apply | Comment | Copy | Remove

Name: VPN-Administratorzy
Local Address: 10.0.10.1
Remote Address: POOL-VPN-Administratorzy
Bridge:
Bridge Port Priority:
Bridge Path Cost:
Bridge Horizon:
Bridge Learning: default
Incoming Filter: ACL-IN-VPN-Administratorzy
Outgoing Filter:
Address List: HOST-VPN-Administratorzy
Interface List: LIST-VPN-Administratorzy

Incoming Filter - Firewall chain name for incoming packets. Specified chain gets control for each packet coming from the client.

[The ppp chain should be manually added and rules with action=jump jump-target=ppp should be added to other relevant chains in order for this feature to work.]

Konfiguracja Firewall – Incoming Filters (ACL)



Reguła 20 (opcjonalna) – sumarycznie blokuje ruch na końcu wszystkich VPN ACL zamiast dedykowanego DROP w każdym PPP chain

Końcowy efekt konfiguracji

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters | Find: ppp

#		Action	Chain	Protocol	Src. Port	Dst. Port	In. Interface	Dst. Address List	Log	Log Prefix	Jump Target	Bytes	Packets
44	D	jump	ppp				<sstp-Pracownik1>		no		ACL-IN-VPN-Pracownicy	0 B	0
39	D	jump	ppp				<l2tp-Pracownik2>		no		ACL-IN-VPN-Pracownicy	300 B	6
42	D	jump	ppp				<pptp-Dostawca2>		no		ACL-IN-VPN-Dostawcy	0 B	0
43	D	jump	ppp				<sstp-Dostawca1>		no		ACL-IN-VPN-Dostawcy	529 B	9
41	D	jump	ppp				<ovpn-Admin2>		no		ACL-IN-VPN-Administratorzy	0 B	0
40	D	jump	ppp				<sstp-Admin1>		no		ACL-IN-VPN-Administratorzy	600 B	12

PPP

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

	Name	Service	Caller ID	Encoding	Address	Uptime	Co
R	Admin1	sstp	192.168.10.11	AES256-CBC	10.0.10.100	00:24:52	
R	Admin2	ovpn	192.168.10.11	AES-128-CBC/SHA1	10.0.10.99	00:24:52	
R	Dostawca1	sstp	192.168.10.12	AES256-CBC	10.0.20.98	00:04:37	
R	Dostawca2	pptp	192.168.10.11	MPPE128 stateless	10.0.20.99	00:09:52	
R	Pracownik1	sstp	192.168.10.11	AES256-CBC	10.0.30.99	00:04:09	
R	Pracownik2	l2tp	192.168.10.11	MPPE128 stateless	10.0.30.100	00:24:53	

6 items

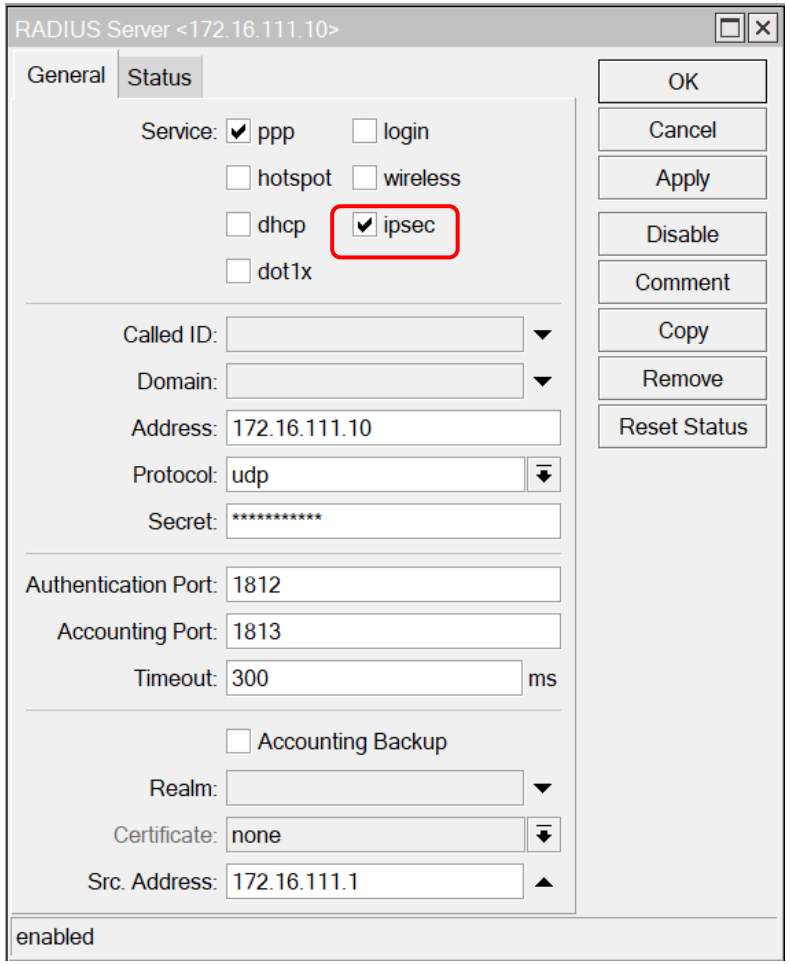
RADIUS	radius, debug, packet	User-Name = "Admin1"
RADIUS	radius, debug, packet	Calling-Station-Id = "192.168.10.11"
RADIUS	radius, debug, packet	Called-Station-Id = "0.0.0.0"
RADIUS	radius, debug, packet	Acct-Session-Id = "818008a1"
RADIUS	radius, debug, packet	MS-CHAP-Challenge = 0xb9cc07411a5017fbb444081d891b778d
RADIUS	radius, debug, packet	MS-CHAP2-Response = 0x01007d37b687043b6e6d7f9b01a282be
RADIUS	radius, debug, packet	f1f900000000000000000d03dbcffa04
RADIUS	radius, debug, packet	0ed79d3ea3ca605c63f431d434593c03
RADIUS	radius, debug, packet	35f6
RADIUS	radius, debug, packet	NAS-Identifier = "MBUM-MT-VPN"
RADIUS	radius, debug, packet	NAS-IP-Address = 172.16.111.1
RADIUS	radius, debug, packet	received Access-Accept with id 102 from 172.16.111.10:1812
RADIUS	radius, debug, packet	Signature = 0xa680144ad4b308ed6ff8b805d87061ee
RADIUS	radius, debug, packet	MT-Group = "VPN-Administratorzy"

Authentication Details:

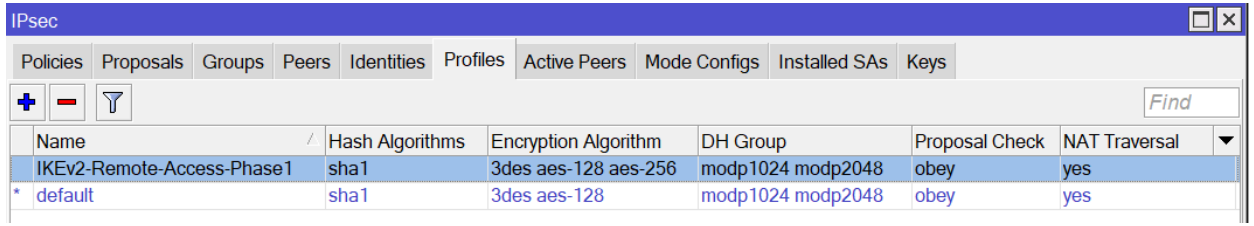
Connection Request Policy Name:	Use Windows authentication for all users
Network Policy Name:	VPN-Administratorzy
Authentication Provider:	Windows
Authentication Server:	MBUM-Win2K19.mbum.internal
Authentication Type:	MS-CHAPv2
EAP Type:	-
Account Session Identifier:	3831383030386131
Logging Results:	Accounting information was written to the local log file.

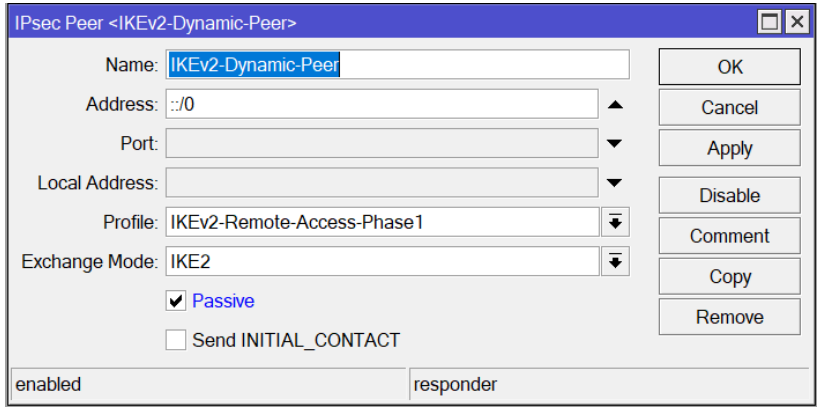
A może jakiś BONUS ???

IPsec (IKEv2) z EAP RADIUS plus separacja sesji



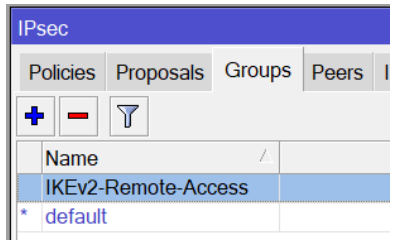
Ustawienia dla IKEv2 - Profiles(Phase1)/Peers

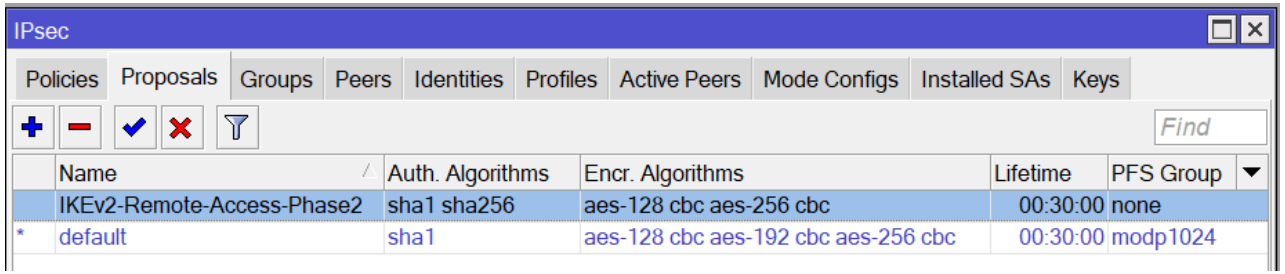


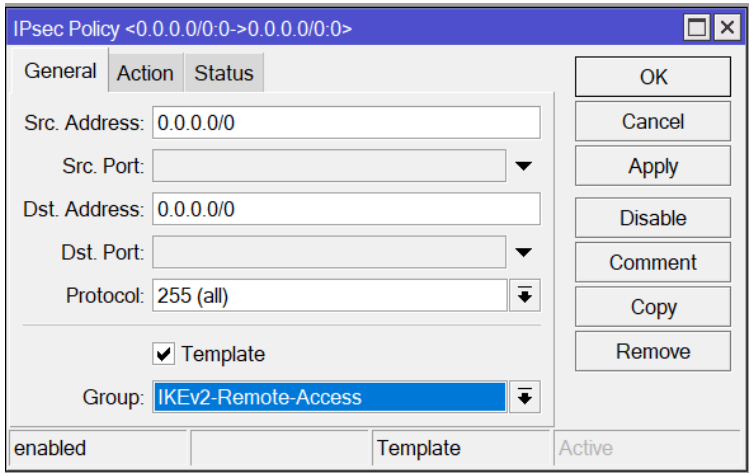


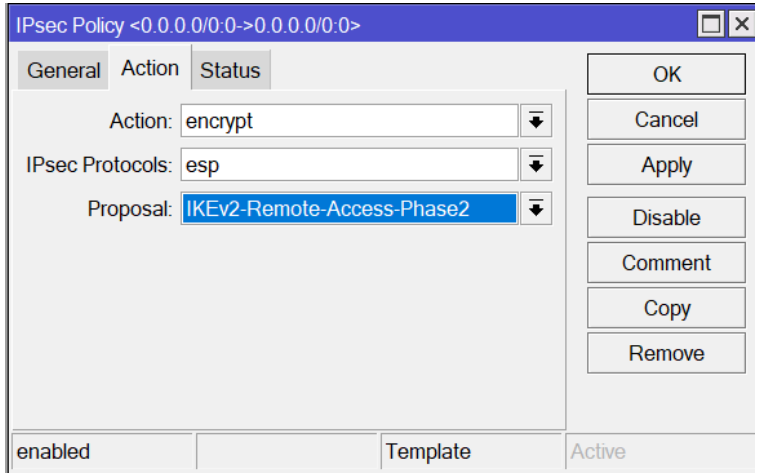
- **Ustawienia dla Phase1 i Phase2 są przykładowe – należy je dostosować do swoich klientów (najlepiej w opcji wspierającej sprzętowe szyfrowanie MikroTika aby uniknąć przeciążenia CPU)**
- **NAT Traversal (NAT-T) w konfiguracji IKEv2 dla Remote Access / Road Warriors jest wymagany**

Ustawienia dla IKEv2 – Groups / IPsec Policy / Proposals(Phase2)

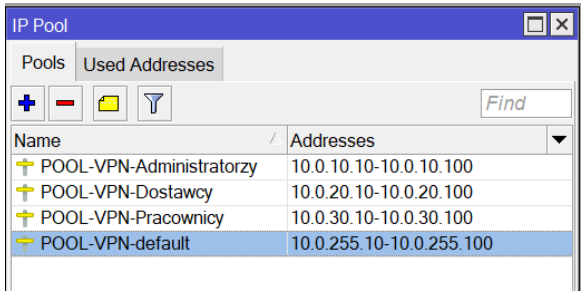


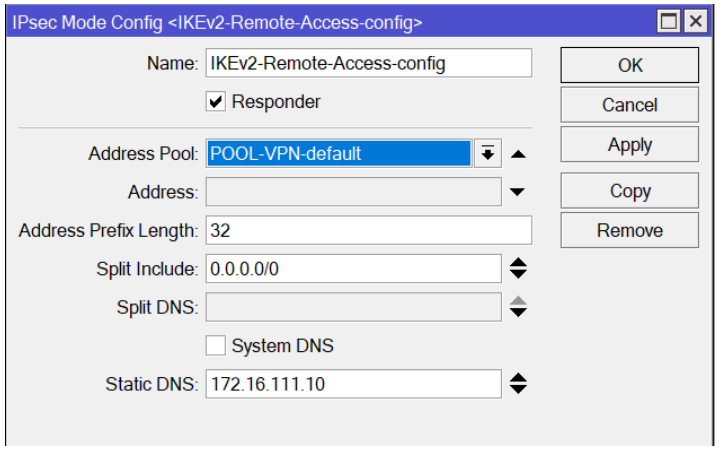


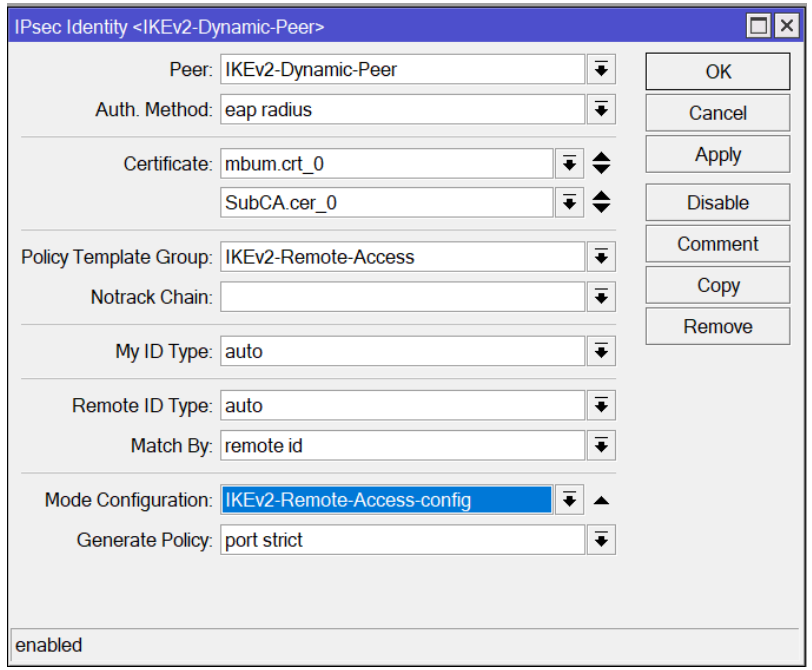




Ustawienia dla IKEv2 – IP Pool / Mode Configs / Identities







Radius Standard Attribute

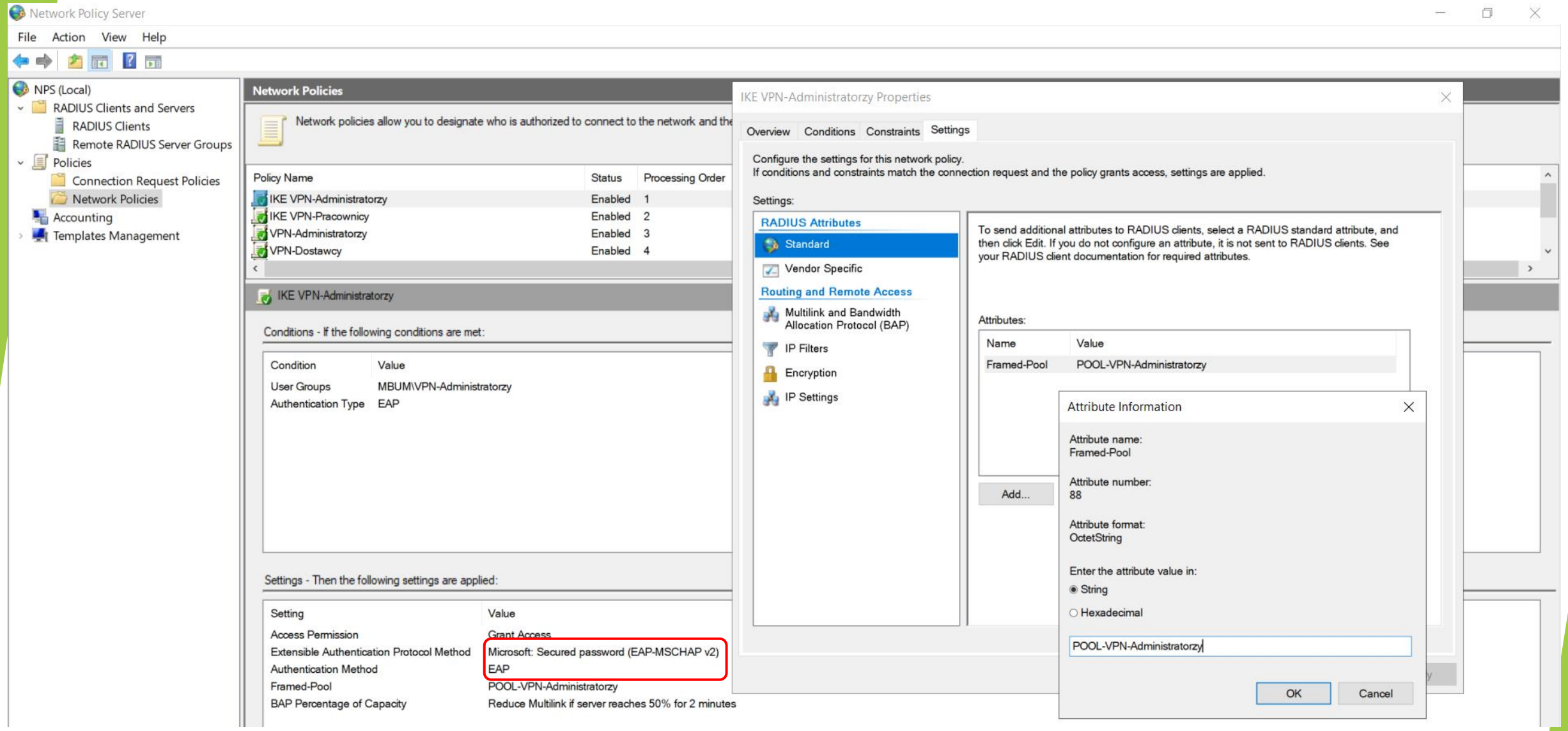
MikroTik WIKI

Attribute	Vendor ID	Type ID	Value type	Packet type	Description
Framed-Pool	0 (standard)	88	string	Access-Accept	IP pool name (on the router) from which to get IP address for the client. If Framed-IP-Address is specified, this attribute is ignored RFC2869 section 5.18

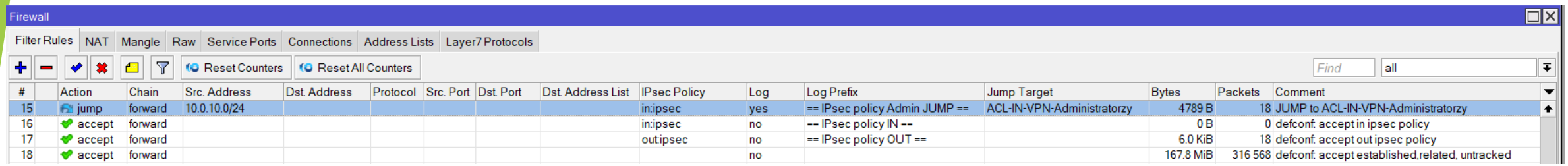
https://help.mikrotik.com/docs/display/ROS/User+Manager#UserManager-Attributes
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client
https://wiki.mikrotik.com/wiki/Manual:RADIUS_Client/reference_dictionary

https://datatracker.ietf.org/doc/html/rfc2869#section-5.18

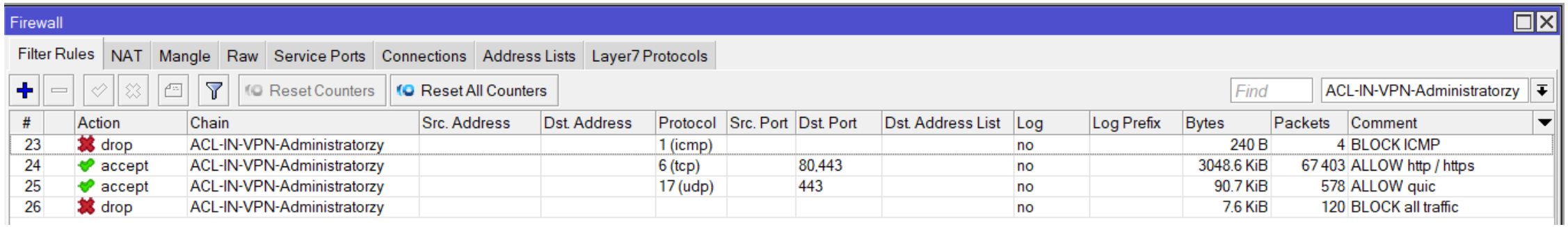
Ustawienia IKEv2 – Windows NPS Network Policies



Ustawienia Firewall – IPsec Jump do dedykowanego ACL Chain



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Dst. Address List	IPsec Policy	Log	Log Prefix	Jump Target	Bytes	Packets	Comment
15	jump	forward	10.0.10.0/24						in:ipsec	yes	== IPsec policy Admin JUMP ==	ACL-IN-VPN-Administratorzy	4789 B	18	JUMP to ACL-IN-VPN-Administratorzy
16	accept	forward							in:ipsec	no	== IPsec policy IN ==		0 B	0	defconf: accept in ipsec policy
17	accept	forward							out:ipsec	no	== IPsec policy OUT ==		6.0 KiB	18	defconf: accept out ipsec policy
18	accept	forward								no			167.8 MiB	316 568	defconf: accept established,related, untracked



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Dst. Address List	Log	Log Prefix	Bytes	Packets	Comment
23	drop	ACL-IN-VPN-Administratorzy			1 (icmp)				no		240 B	4	BLOCK ICMP
24	accept	ACL-IN-VPN-Administratorzy			6 (tcp)		80,443		no		3048.6 KiB	67 403	ALLOW http / https
25	accept	ACL-IN-VPN-Administratorzy			17 (udp)		443		no		90.7 KiB	578	ALLOW quic
26	drop	ACL-IN-VPN-Administratorzy							no		7.6 KiB	120	BLOCK all traffic

*** W przypadku IPsec na końcu każdej ACL powinien być jawny DROP aby zapobiec wyciekaniu nieporządanych połączeń poza Chain**

IKEv2 – wynik nawiązania sesji

RADIUS	radius, debug	new request 55:4a2e5 code=Access-Request service=ipsec called-id=192.168.10.10
RADIUS	radius, debug	sending 55:4a2e5 to 172.16.111.10:1812
RADIUS	radius, debug, packet	sending Access-Request with id 142 to 172.16.111.10:1812
RADIUS	radius, debug, packet	Signature = 0x70bd7b45bbfdbd8ae684a4fc8a469772
RADIUS	radius, debug, packet	User-Name = "Admin2"
RADIUS	radius, debug, packet	Called-Station-Id = "192.168.10.10"
RADIUS	radius, debug, packet	Calling-Station-Id = "192.168.10.12"
RADIUS	radius, debug, packet	NAS-Port-Id = 0x0000000a
RADIUS	radius, debug, packet	NAS-Port-Type = 5
RADIUS	radius, debug, packet	Service-Type = 2
RADIUS	radius, debug, packet	Event-Timestamp = 1633034078
RADIUS	radius, debug, packet	Framed-MTU = 1400
RADIUS	radius, debug, packet	State = 0x279d036a0000013700010200ac106f0a
RADIUS	radius, debug, packet	00000000000000000000000000000004
RADIUS	radius, debug, packet	a15a49b1
RADIUS	radius, debug, packet	EAP-Message = 0x020200061a03
RADIUS	radius, debug, packet	Message-Authenticator = 0xeb2c52892529e5799a049112037cc947
RADIUS	radius, debug, packet	NAS-Identifier = "MBUM-MT-VPN"
RADIUS	radius, debug, packet	NAS-IP-Address = 172.16.111.1
RADIUS	radius, debug, packet	received Access-Accept with id 142 from 172.16.111.10:1812
RADIUS	radius, debug, packet	Signature = 0x28afb3de13dc3b9a8641002a04b7b76e
RADIUS	radius, debug, packet	Framed-Pool = "POOL-VPN-Administratorzy"
RADIUS	radius, debug, packet	EAP-Message = 0x03020004

Buffer	Topics	Message
IPsec	ipsec, info	new ike2 SA (R): 192.168.10.10[500]-192.168.10.12[500] spi:907e6c6a125a8597:ca625c7dd6d09056
IPsec	ipsec, info, account	peer authorized: 192.168.10.10[4500]-192.168.10.12[4500] spi:907e6c6a125a8597:ca625c7dd6d09056
IPsec	ipsec, info	acquired 10.0.10.96 address for 192.168.10.12, Admin2

IP Pool

Pools | Used Addresses

Pool	Address	Owner	Info
POOL-VPN-Administratorzy	10.0.10.96	IPsec	192.168.10.12, Admin2

IPsec

Policies | Proposals | Groups | Peers | Identities | Profiles | Active Peers | Mode Configs | Installed SAs | Keys

Kill Connections | Find

ID	State	Local Address	Remote Address	Dynamic Address	Side	Uptime	PH2 Total	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Comment
Admin2	established	192.168.10.10	192.168.10.12	10.0.10.96	responder	00:07:21	1	104 458 012	1 678 848	74 995	38 595	IKEv2 Remote Access

IPsec

Policies | Proposals | Groups | Peers | Identities | Profiles | Active Peers | Mode Configs | Installed SAs | Keys

Statistics | Find

#		Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Protocol	Action	Level	PH2 State	Comment
0	*T			::/0		::/0		255 (all)	encrypt			
1	T			0.0.0.0/0		0.0.0.0/0		255 (all)	encrypt			IKEv2 Remote Access
2	DA	IKEv2-Dynamic-Peer	yes	0.0.0.0/0		10.0.10.96		255 (all)	encrypt	unique	established	

Czego brakuje w RouterOS ??

Dedykowany klient VPN od MikroTika – nierealne ;-)

Podział konfiguracji VPN na:
- Remote Access (niezależnie od protokołu) - bardzo mała szansa
- Site-to-Site

RADIUS VSA dla Mode Configs – prawdopodobne

zainteresowani powinni podbijać poniższe wątki na forum ;-)
https://forum.mikrotik.com/viewtopic.php?t=143139
https://forum.mikrotik.com/viewtopic.php?t=179254