

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

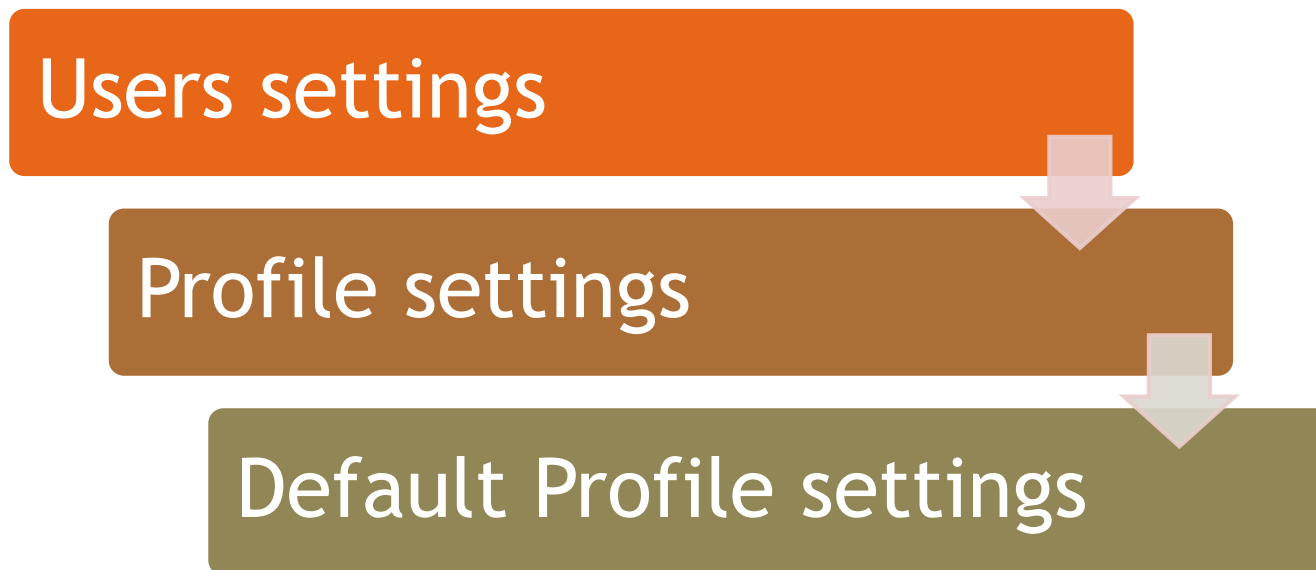
linkedin.com/in/grzegorz-rakus/

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

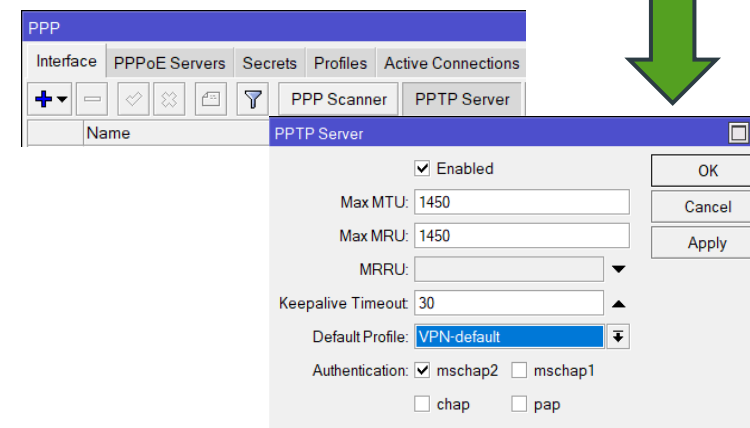
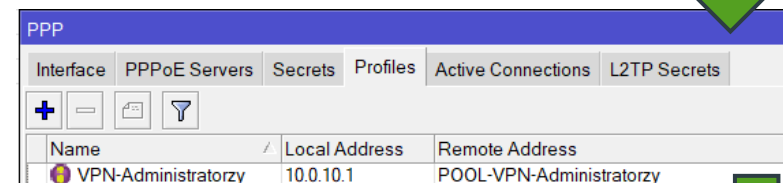
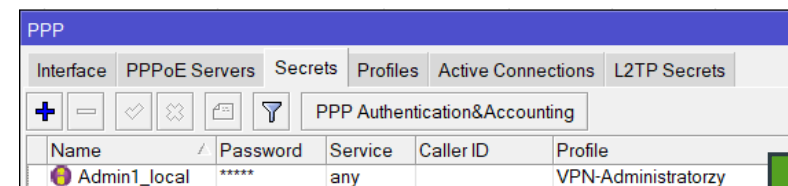
(zakładka Secret)

Profile settings

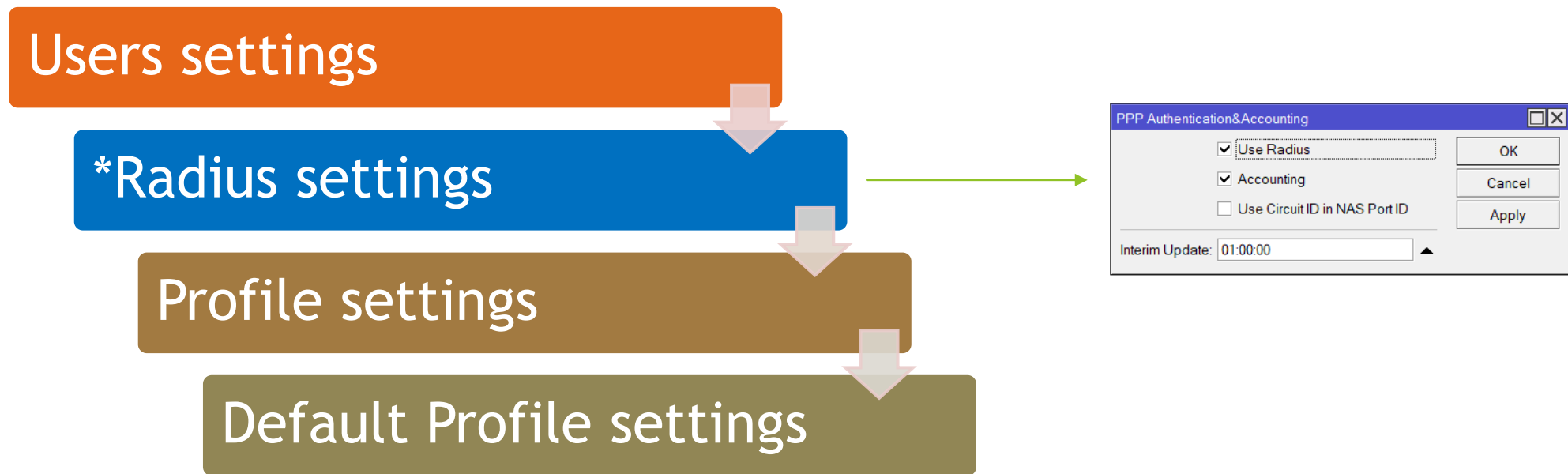
(zakładka Profiles)

Default Profile settings

(zakładka Default Profile w PPTP Server)



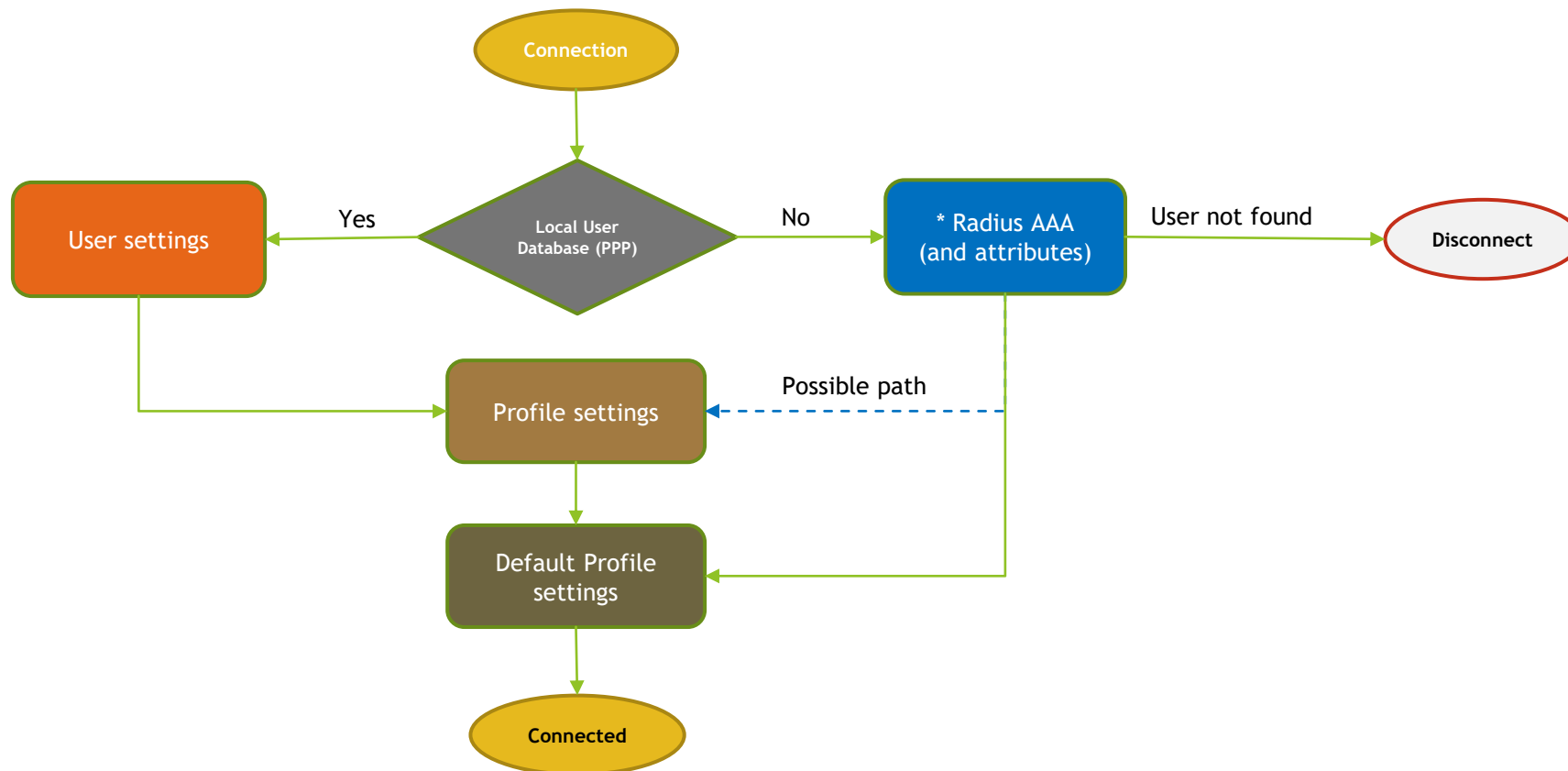
Kolejność przetwarzania reguł dla Serwera PPP z aktywnym protokołem RADIUS



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.

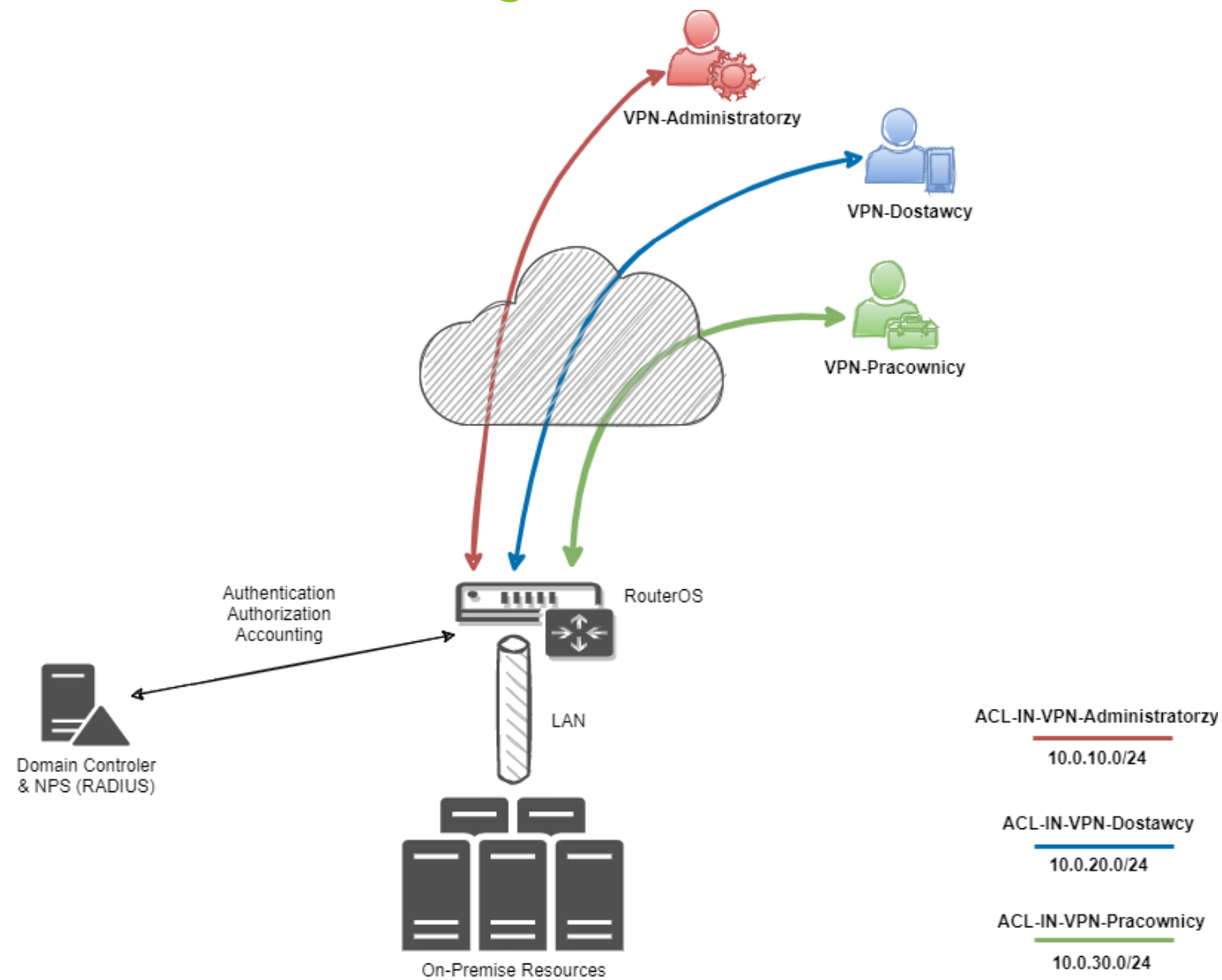
<https://help.mikrotik.com/docs/display/ROS/User+Manager#UserManager-Attributes>

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

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

Find

Name	Local Address	Remote Address	Incoming Filter	Address List	Interface List	DNS Server	Only One	Comment
VPN-Administratorzy	10.0.10.1	POOL-VPN-Administratorzy	ACL-IN-VPN-Administratorzy	HOST-VPN-Administratorzy	LIST-VPN-Administratorzy	172.16.111.10	default	Profil dla Administratorow
VPN-Dostawcy	10.0.20.1	POOL-VPN-Dostawcy	ACL-IN-VPN-Dostawcy	HOST-VPN-Dostawcy	LIST-VPN-Dostawcy		default	Profil dla Dostawcow
VPN-Pracownicy	10.0.30.1	POOL-VPN-Pracownicy	ACL-IN-VPN-Pracownicy	HOST-VPN-Pracownicy	LIST-VPN-Pracownicy	172.16.111.10	default	Profil dla Pracownikow
VPN-default	10.0.255.1	POOL-VPN-default	ACL-IN-VPN-default	HOST-VPN-default	LIST-VPN-default	8.8.8.8	yes	Profil domyslny (tylko DNS i Internet)
* default							default	
* default-encryption								

6 items (1 selected)

IP Pool

Pools Used Addresses

Find

Name	Addresses	Next Pool	Comment
POOL-VPN-Administratorzy	10.0.10.10-10.0.10.100	none	
POOL-VPN-Dostawcy	10.0.20.10-10.0.20.100	none	
POOL-VPN-Pracownicy	10.0.30.10-10.0.30.100	none	
POOL-VPN-default	10.0.255.10-10.0.255.100	none	

4 items (1 selected)

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

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

DNS Server: 172.16.111.10

WINS Server:

Change TCP MSS

☐ no ☐ yes ☒ default

Use UPnP

☐ no ☐ yes ☒ default

OK Cancel Apply Comment Copy Remove

Ustawienia dla Certificates / PPP Servers

Certificates							
Certificates SCEP Servers SCEP RA Requests OTP CRL							
+ - Filter Import Card Reinstall Card Verify Revoke Settings							
	Name	Issuer	Common Name	Subject Alt Name	Key Size	Days Valid	Trusted
T	RootCA.cer_0	O=Digital Signature Trust Co.,CN=DST Root CA X3	DST Root CA X3		2048	7669	yes
LT	SubCA.cer_0	O=Digital Signature Trust Co.,CN=DST Root CA X3	R3		2048	357	yes
KT	mbum.crt_0	C=US,O=Let's Encrypt,CN=R3	mbum.rakus.org	DNS:mbum.rakus.org	2048	89	yes

3 items (1 selected)

SSTP Server

☒ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 60

Default Profile: VPN-default

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

Certificate: mbum.crt_0

TLS Version: only-1.2

☐ Verify Client Certificate

☒ Force AES

☒ PFS

OK Cancel Apply

PPTP Server

☒ Enabled

Max MTU: 1450

Max MRU: 1450

MRRU:

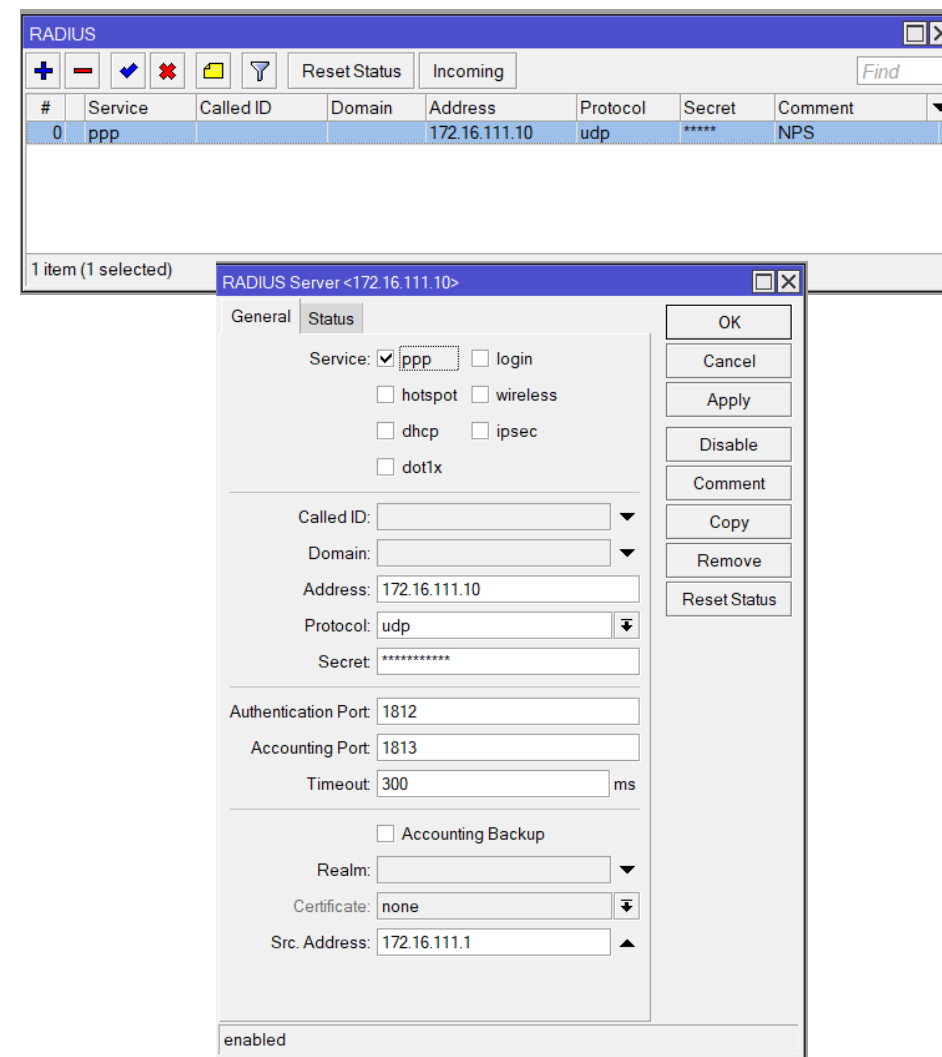
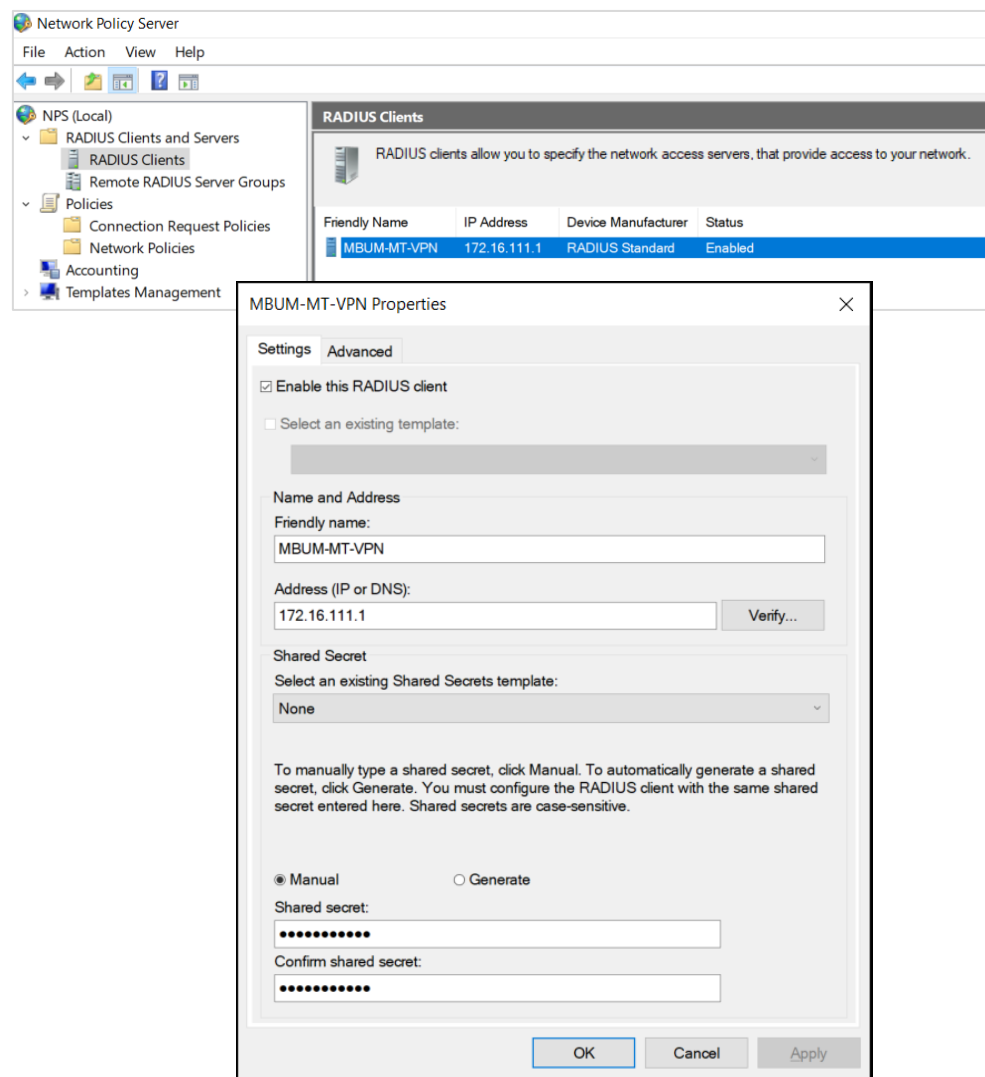
Keepalive Timeout: 30

Default Profile: VPN-default

Authentication: ☒ mschap2 ☐ mschap1
☐ chap ☐ pap

OK Cancel Apply

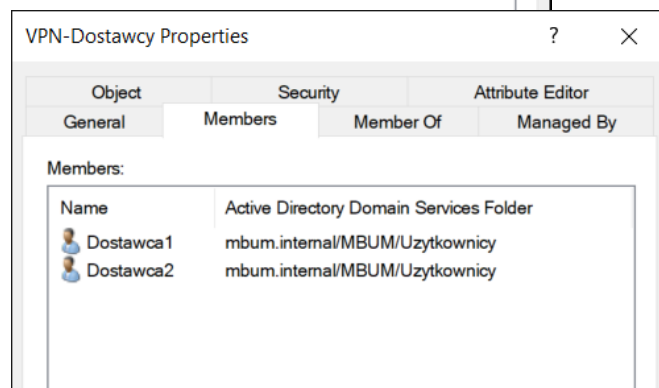
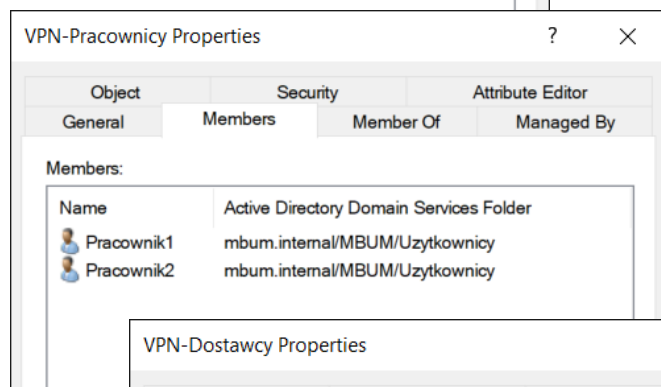
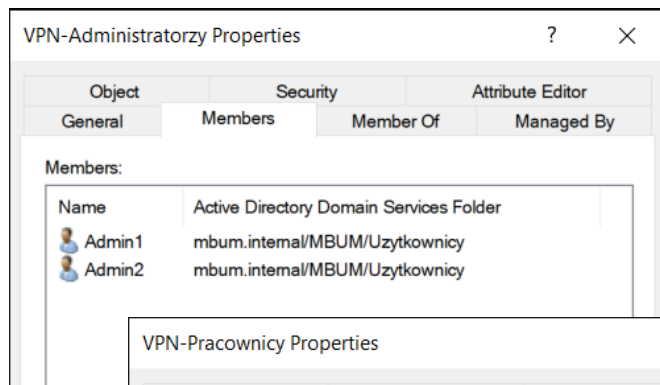
Konfiguracja Windows Server NPS <-> RouterOS (przypomnienie)



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



Grupy 3 objects		
Name	Type	Description
VPN-Administratorzy	Security Group - Global	Dostęp dla Administratorów
VPN-Dostawcy	Security Group - Global	Dostęp dla Dostawców Zewnętrznych
VPN-Pracownicy	Security Group - Global	Dostęp dla Pracowników

Uzytkownicy 6 objects	
Name	Type
Admin1	User
Admin2	User
Dostawca1	User
Dostawca2	User
Pracownik1	User
Pracownik2	User

Konfiguracja Windows Server NPS - Network Policies

The screenshot displays the Windows Network Policy Server (NPS) console. The left-hand navigation pane shows the tree structure: NPS (Local) > Policies > Network Policies. The main pane is titled 'Network Policies' and contains a list of three policies: 'VPN-Administratorzy', 'VPN-Dostawcy', and 'VPN-Pracownicy'. The 'VPN-Administratorzy' policy is selected and highlighted in blue. Below the list, the configuration details for this policy are shown. The 'Conditions' section, titled 'Conditions - If the following conditions are met:', contains a single condition: 'User Groups' with the value 'MBUM\VPN-Administratorzy'. The 'Settings' section, titled 'Settings - Then the following settings are applied:', contains a list of settings: 'Access Permission' (Grant Access), 'Authentication Method' (Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2), 'Vendor-Specific' (VPN-Administratorzy), 'Framed-Protocol' (PPP), 'Service-Type' (Framed), and 'BAP Percentage of Capacity' (Reduce Multilink if server reaches 50% for 2 minutes). The 'Authentication Method' value is highlighted with a red rectangle.

Network Policy Server

File Action View Help

NPS (Local)

- RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
- Policies
 - Connection Request Policies
 - Network Policies
- Accounting
- Templates Management

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
VPN-Administratorzy	Enabled	1	Grant Access	Unspecified
VPN-Dostawcy	Enabled	2	Grant Access	Unspecified
VPN-Pracownicy	Enabled	3	Grant Access	Unspecified

VPN-Administratorzy

Conditions - If the following conditions are met:

Condition	Value
User Groups	MBUM\VPN-Administratorzy

Settings - Then the following settings are applied:

Setting	Value
Access Permission	Grant Access
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2
Vendor-Specific	VPN-Administratorzy
Framed-Protocol	PPP
Service-Type	Framed
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

Konfiguracja NPS - Network Policies Properties (ustawienia dla VSA)

(*przykład dla grupy VPN-Administratorzy)

The image shows a sequence of steps for configuring Network Policy Server (NPS) for a specific group. The main window is 'VPN-Administratorzy Properties' with the 'Settings' tab selected. It shows a list of settings on the left, including 'RADIUS Attributes', 'Vendor Specific', 'Routing and Remote Access', 'Multilink and Bandwidth Allocation Protocol (BAP)', 'IP Filters', 'Encryption', and 'IP Settings'. The 'Vendor Specific' setting is highlighted, and its details are shown in the main pane. Below the details, there is a table of attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	VPN-Administratorzy

Below the table, there is an 'Add...' button. A red arrow points from the 'Add...' button to the 'Configure Attribute...' button in the 'Vendor-Specific Attribute Information' dialog box. This dialog box is open, showing the 'Attribute name' as 'Vendor Specific', the 'Specify network access server vendor' as 'RADIUS Standard', and the 'Enter Vendor Code' as '14988'. The 'Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes' is set to 'Yes. It conforms'. The 'Configure Attribute...' button is highlighted. A red arrow points from the 'Configure Attribute...' button to the 'Configure VSA (RFC Compliant)' dialog box. This dialog box is open, showing the 'Vendor-assigned attribute number' as '26', the 'Attribute format' as 'String', and the 'Attribute value' as 'VPN-Administratorzy'. The 'OK' button is highlighted. A red arrow points from the 'OK' button to the 'PPP' window. The 'PPP' window shows the 'Interface' tab selected, and a table of PPP connections:

Interface	PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets
+	-	+	+		
Name	Local Address	Remote Address			
VPN-Administratorzy	10.0.10.1	POOL-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

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

OK Cancel Apply Comment Copy Remove

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)

Firewall													
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols													
+ - ✓ ✗ [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon] [icon]													
Find ACL-IN-VPN-Administratory													
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Dst. Address List	Log	Log Prefix	Bytes	Packets	Comment
23	✓ accept	ACL-IN-VPN-Administratory							no		0 B	0	ALLOW any any
24 X	✗ drop	ACL-IN-VPN-Administratory							no		0 B	0	BLOCK all traffic

#	Action	Chain	Dst. Address	Protocol	Src. Port	Dst. Port	Dst. Address List	Log	Log Prefix	Bytes	Packets	Comment
33	✓ accept	ACL-IN-VPN-Dostawcy	172.16.111.100	6 (tcp)		3389		no		156 B	3	ALLOW RDP/tcp on Terminal
34	✓ accept	ACL-IN-VPN-Dostawcy	172.16.111.100	17 (udp)		3389		no		1260 B	1	ALLOW RDP/udp on Terminal
35	✗ drop	ACL-IN-VPN-Dostawcy					RFC-1918	no		240 B	4	BLOCK rfc-1918
36	✓ accept	ACL-IN-VPN-Dostawcy						no		1859 B	32	ALLOW any any
37 X	✗ drop	ACL-IN-VPN-Dostawcy						no		0 B	0	BLOCK all traffic

#	Action	Chain	Dst. Address	Protocol	Src. Port	Dst. Port	Dst. Address List	Log	Log Prefix	Bytes	Packets	Comment
25	✓ accept	ACL-IN-VPN-Pracownicy	172.16.111.10	17 (udp)		53		no		917 B	14	ALLOW local dns
26	✓ accept	ACL-IN-VPN-Pracownicy		6 (tcp)		445	RFC-1918	no		416 B	8	ALLOW smb
27	✓ accept	ACL-IN-VPN-Pracownicy	172.16.111.100	6 (tcp)		3389		no		0 B	0	ALLOW RDP/tcp on Terminal
28	✓ accept	ACL-IN-VPN-Pracownicy	172.16.111.100	17 (udp)		3389		no		0 B	0	ALLOW RDP/udp on Terminal
29	✗ drop	ACL-IN-VPN-Pracownicy					RFC-1918	no		208 B	4	BLOCK rfc-1918
30	✓ accept	ACL-IN-VPN-Pracownicy		6 (tcp)		80,443		no		728 B	14	ALLOW http / https
31	✓ accept	ACL-IN-VPN-Pracownicy		17 (udp)		443		no		0 B	0	ALLOW quic
32 X	✗ drop	ACL-IN-VPN-Pracownicy						no		0 B	0	BLOCK all traffic

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

+

-

✓

✗

📄

🔍

↺

Reset Counters

↺

Reset All Counters

Find

all

#	Action	Chain	Protocol	Src. Port	Dst. Port	In. Interface List	Dst. Address List	Log	Log Prefix	Bytes	Packets	Comment
19	<div>🔗 jump</div>	forward				VPN-Remote-Access		yes	== PPP JUMP ==	8.5 KiB	131	JUMP to PPP chains (VPN only)
20	<div>✗ drop</div>	forward				VPN-Remote-Access		yes	== BLOCK VPN ==	240 B	4	BLOCK vpn traffic (last rule for all 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	C
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	f1f900000000000000000000d03dbcffa04
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
Logqing Results:	Accounting information was written to the local log file.

A może jakiś BONUS ???

IPsec (IKEv2) z EAP RADIUS plus separacja sesji

RADIUS Server <172.16.111.10>

General Status

Service: ☒ ppp ☐ login
☐ hotspot ☐ wireless
☐ dhcp ☒ ipsec
☐ dot1x

Called ID:
Domain:
Address: 172.16.111.10
Protocol: udp
Secret:

Authentication Port: 1812
Accounting Port: 1813
Timeout: 300 ms

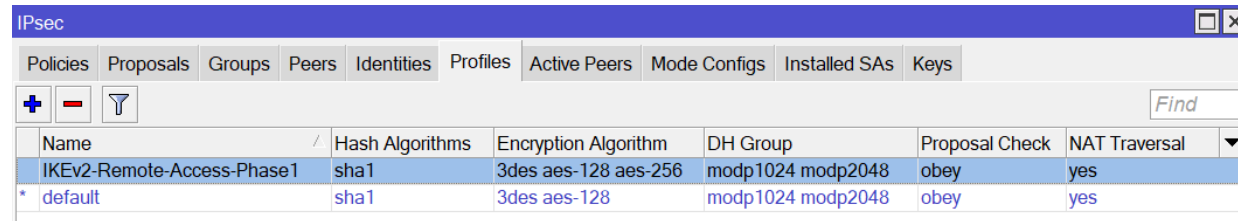
☐ Accounting Backup

Realm:
Certificate: none
Src. Address: 172.16.111.1

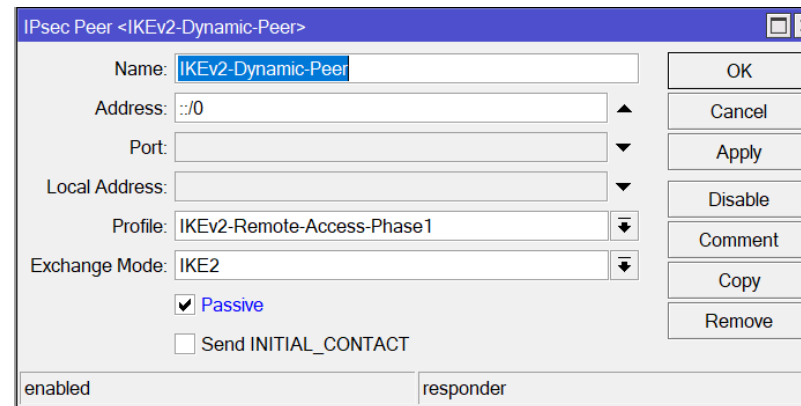
enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

Ustawienia dla IKEv2 - Profiles(Phase1)/Peers



Name	Hash Algorithms	Encryption Algorithm	DH Group	Proposal Check	NAT Traversal
IKEv2-Remote-Access-Phase1	sha1	3des aes-128 aes-256	modp1024 modp2048	obey	yes
* default	sha1	3des aes-128	modp1024 modp2048	obey	yes



IPsec Peer <IKEv2-Dynamic-Peer>

Name:

Address:

Port:

Local Address:

Profile:

Exchange Mode:

☒ Passive

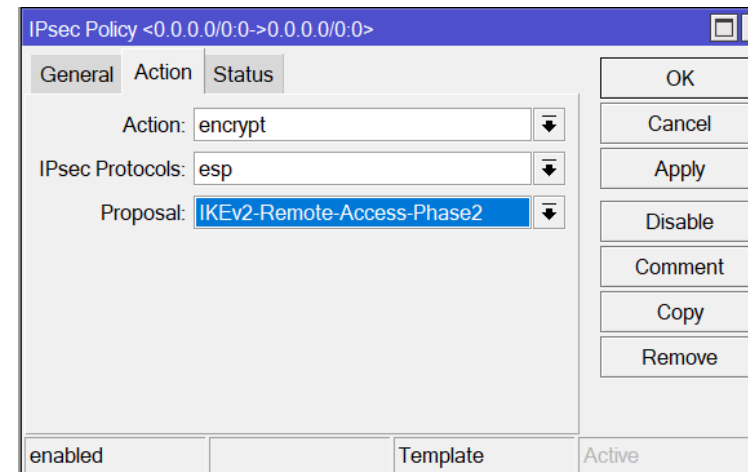
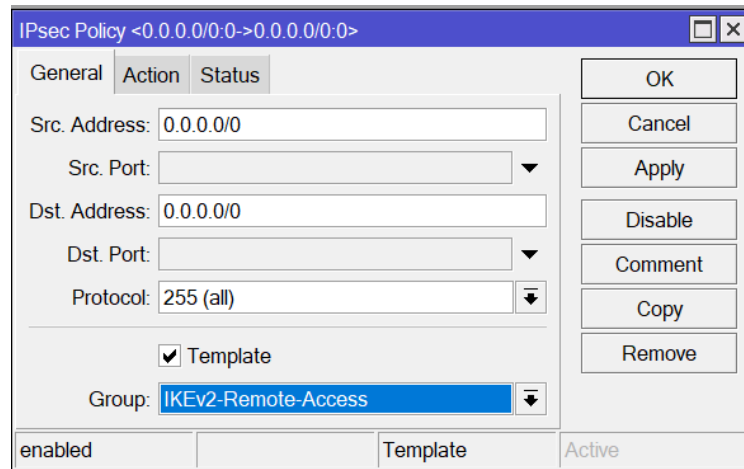
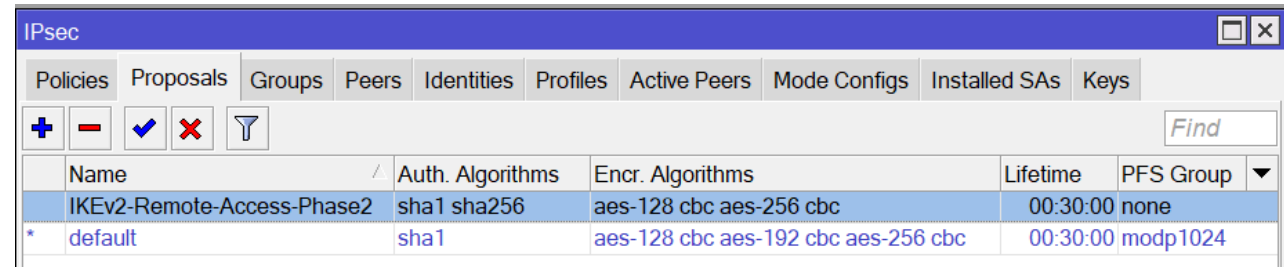
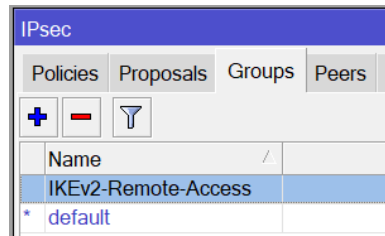
☐ Send INITIAL_CONTACT

enabled responder

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

- 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

IP Pool	
Pools Used Addresses	
+ - [icon] Find	
Name	Addresses
+ POOL-VPN-Administratorzy	10.0.10.10-10.0.10.100
+ POOL-VPN-Dostawcy	10.0.20.10-10.0.20.100
+ POOL-VPN-Pracownicy	10.0.30.10-10.0.30.100
+ POOL-VPN-default	10.0.255.10-10.0.255.100

IPsec Mode Config <IKEv2-Remote-Access-config>

Name: IKEv2-Remote-Access-config

☒ Responder

Address Pool: POOL-VPN-default

Address:

Address Prefix Length: 32

Split Include: 0.0.0.0/0

Split DNS:

☐ System DNS

Static DNS: 172.16.111.10

OK Cancel Apply Copy Remove

IPsec Identity <IKEv2-Dynamic-Peer>

Peer: IKEv2-Dynamic-Peer

Auth. Method: eap radius

Certificate: mbum.crt_0

SubCA.cer_0

Policy Template Group: IKEv2-Remote-Access

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

Mode Configuration: IKEv2-Remote-Access-config

Generate Policy: port strict

enabled

OK Cancel Apply Disable Comment Copy Remove

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

The screenshot displays the Windows Network Policy Server (NPS) console. The left pane shows the tree structure with 'Network Policies' selected. The main pane shows a list of policies, with 'IKE VPN-Administratorzy' selected. The 'Conditions' tab is active, showing a table of conditions. The 'Settings' tab is also visible, showing a table of settings. A red box highlights the 'Authentication Method' setting, which is 'Microsoft: Secured password (EAP-MSCHAP v2)'. An 'Attribute Information' dialog box is open, showing details for the 'Framed-Pool' attribute, including its name, number (88), format (OctetString), and value ('POOL-VPN-Administratorzy').

Network Policies

Network policies allow you to designate who is authorized to connect to the network and the conditions under which they are authorized.

Policy Name	Status	Processing Order
IKE VPN-Administratorzy	Enabled	1
IKE VPN-Pracownicy	Enabled	2
VPN-Administratorzy	Enabled	3
VPN-Dostawcy	Enabled	4

IKE VPN-Administratorzy

Conditions - If the following conditions are met:

Condition	Value
User Groups	MBUM\VPN-Administratorzy
Authentication Type	EAP

Settings - Then the following settings are applied:

Setting	Value
Access Permission	Grant Access
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)
Authentication Method	EAP
Framed-Pool	POOL-VPN-Administratorzy
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

IKE VPN-Administratorzy Properties

Overview Conditions Constraints Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Pool	POOL-VPN-Administratorzy

Add...

Attribute Information

Attribute name:
Framed-Pool

Attribute number:
88

Attribute format:
OctetString

Enter the attribute value in:
☒ String
☐ Hexadecimal

POOL-VPN-Administratorzy

OK Cancel

Ustawienia Firewall - IPsec Jump do dedykowanego ACL Chain

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	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			

Firewall

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

Reset Counters

Reset All Counters

Find

ACL-IN-VPN-Administratorzy

#	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 nieporządkanych 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)
- Site-to-Site

- bardzo mała szansa

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>