Mikrotik VPN

Wirtualna sieć prywatna (od ang. virtual private network – VPN) – to tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy nadawcą i odbiorcą za pośrednictwem publicznej sieci.

Routery firmy Mikrotik mają możliwość uruchomienia serwera VPN w oparciu o protokół L2TP z szyfrowaniem IPSEC z wykorzystaniem klucza. Poniżej instrukcja uruchomienia takiego serwera.

1. Tworzenie profilu na potrzeby VPN

Korzystając z WinBox wybieramy z lewej strony PPP

	Session Settings Dashb	oard
	Safe Mode	Session: 08:00:27:0D:92:CA
	🔰 🏏 Quick Set	
	CAPSMAN	
	📟 Interfaces	
	💭 Wireless	
	💢 Bridge	
	吉 PPP	
	ື ຼ ໍ Mesh	
0	🐺 IP 🛛 🗅	
	🕑 MPLS 🛛 🗅	
	🐺 IPv6 🛛 🗅	
	📑 Routing 🛛 🗅	
	🏹 System 🛛 🗅	
	🔍 🙅 Queues	

A następnie przechodzimy na zakładkę Profiles, gdzie dodajemy nowy profil

💭 CAPsMAN										
🛤 Interfaces										
💭 Wireless	PPP									
💥 Bridge	Interface	PPPoE Servers	Secrets	Profiles	Active	Connections	L2TP Secrets			
🛓 PPP				-						
📲 Mesh										
255 TD	Name		Δ	Local Addr	ess	Remote Addre	ess Bridge	Rate Limi	Only One	
* "	[* 🕝 defaul	t							default	
🕥 MPLS 🛛 🗅	🔹 🔒 defau	lt-encryption							default	

Uzupełniamy dane takie jak: nazwa w opcji Change TCP MSS zmieniamy na yes

	PPP Profile	<profile_l2t< th=""><th>:p></th><th></th><th></th><th></th></profile_l2t<>	:p>			
	General	Protocols	Limits	Queue	Scripts	ОК
		Na	me: pro	file_l2tp		Cancel
r		Local Addre	ss:		-	Apply
	R	emote Addre	ess:		 *	Comment
	Remote I	Pv6 Pretix Pi				Сору
-						Remove
	D.::J	Brid	ge:			
	Bridi	je Port Prior idae Path Cr	109:			
	0	Bridae Horiz	on:			
	E	Bridge Learni	ng: def	ault	₹	
		Incomina Fili	ter:			
		- Outgoing Fill	ter:		•	
		Address L	.ist:		\$	
		Interface L	.ist:		•	
		DNS Serv	/er:		\$	
İ		WINS Serv	/er:		\$	
	– Change	TCP MSS -				
		• yes O	detault			
		r Cyes ⊙	default			

Na zakładce Protocols możemy wyłączyć korzystanie z IPv6, możemy włączyć kompresję oraz domyślnie włączyć szyfrowanie.



Po dokonaniu konfiguracji akceptujemy wprowadzone zmiany.

2. Tworzenie użytkownika

Przechodzimy na zakładkę Secrets, gdzie dodajemy nowego użytkownika



Podajemy nazwę, hasło, adres ip lokalny oraz adres ip zdalny. Zmieniamy profil na wcześniej utworzony i akceptujemy zmiany.

PPP Secret <user_l2tp></user_l2tp>		
Name:	user_l2tp	ОК
Password:	*****	Cancel
Service:	I2tp 🗧	Apply
Caller ID:	▼	Disable
Profile:	profile_l2tp Ŧ	Comment
Local Address:	192.168.40.1	Commenc
Remote Address:	192.168.40.2	
Remote IPv6 Prefix:	•	Remove
Routes:	▼	
IPv6 Routes:	▼	
Limit Bytes In:	▼	
Limit Bytes Out:	▼	
Last Logged Out:		
Last Caller ID:		
Last Disconnect Reason:		
enabled		

3. Uruchomienie serwera

Uruchomienie samego serwera wykonamy na zakładce Interface wybierając L2TP Server. Zmieniamy domyślny profil na nasz wcześniej utworzony. W części autoryzacji zostawiamy zaznaczoną opcję mschap2. W celu dodatkowego zabezpieczenia używamy IPsec gdzie możemy podać dodatkowe hasło zabezpieczające. Możemy też określić pojedynczą sesję dla jednego hosta.

ve	r SSTP Server	L2TP Server	OVPN Serv	er	PPPoE Scan	
J	L2TP Server					
FUU		✓ Enabled			ОК	
	Max MTU:	1450			Cancel	
	Max MRU:	1450			Apply	
	MRRU:			•		
	Keepalive Timeout:	30		*		
	Default Profile:	profile_l2tp		Ŧ		
	Max Sessions:			•		
	Authentication:	💌 mschap2	mschap1			
		🗌 chap	🗌 рар			
	Use IPsec:	yes		Ŧ		
-	IPsec Secret:	****				-
	Caller ID Type:	ip address		Ŧ		
		One Sessio	on Per Host			
		Allow Fast	Path			

4. Konfiguracja Windows

Aby dodać nowe połączenie przechodzimy w Panelu sterowania do Centrum sieci i udostępniania, a następnie wybieramy Skonfiguruj nowe połączenie lub nową sieć

🚆 Centrum sieci i udostępniania		- 🗆 ×
← → × ↑ 🔽 « Sieć i Internet	 Centrum sieci i udostępniania 	✓ ່ັ Szukaj w Panelu sterowania ,
Strona główna Panelu sterowania	Wyświetl podstawowe informacje o sieci i Wyświetl aktywne sieci	skonfiguruj połączenia
Zmień ustawienia karty sieciowej Zmień zaawansowane ustawienia udostępniania	Sieć 8 Sieć prywatna	Typ dostępu: Internet Połączenia: 🛱 Ethernet
Opcje przesyłania strumieniowego multimediów	 Zmień ustawienia sieci Skonfiguruj nowe połączenie lub nową sieć Skonfiguruj połączenie szerokopasmowe, tele punkt dostępu. Rozwiąż problemy Zdiagnozuj i rozwiąż problemy z siecią lub uz problemów. 	efoniczne lub VPN albo skonfiguruj router lub zyskaj informacje na temat rozwiązywania
Zobacz też Opcje internetowe Zapora Windows Defender		

Zostaniemy zapytani o rodzaj połączenia - wybieramy Połącz z miejscem pracy

			—		\times
~	🚰 Skon	figuruj połączenie lub sieć			
	Wybie	rz opcję połączenia.			
		Połącz z Internetem Skonfiguruj połączenie szerokopasmowe lub telefoniczne z Internetem.			
	2	Skonfiguruj nową sieć Skonfiguruj nowy router lub punkt dostępu.			
		Połącz z miejscem pracy Skonfiguruj połączenie telefoniczne lub połączenie VPN z miejscem pracy.			
		D	alej	Anu	luj

A następnie Użyj mojego połączenia internetowego VPN

		×
~	Połącz z miejscem pracy	
	Jak chcesz się łączyć?	
	 Użyj mojego połączenia internetowego (VPN) Połącz przy użyciu połączenia wirtualnej sieci prywatnej (VPN) za pośrednictwem Internetu. 	
	ing	1
	→ Wybierz numer bezpośrednio Połącz bezpośrednio z numerem telefonu bez pośrednictwa Internetu.	
	An	uluj

Po wybraniu musimy podać adres internetowy w formie adresu IP lub adresu domenowego. Możemy też nazwać nasze połączenie z siecią VPN.

			_		\times
~	🌆 Połącz z miejscem pracy				
	Wpisz adres internetowy, z	którym chcesz się połączyć			
	Ten adres można uzyskać od admini	stratora sieci.			
1	Adres internetowy:	192.168.1.112			
	Nazwa miejsca docelowego:	Polacz_VPN_L2TP			
	🗌 Użyj karty inteligentnej				
	🗹 Zapamiętaj moje poświadcz	enia			
	Zezwalaj innym osobom na Ta opcja zezwala dowolnej o połączenia.	korzystanie z tego połączenia sobie z dostępem do tego komputera na używa	inie tego		
		U	twórz	Anul	uj

Po wybraniu Utwórz pojawi się nasze połączenie VPN w części sieciowej w trayu.



Aby skonfigurować nasze dodatkowe opcję należy w części Panel sterowania -> Sieć i Internet -> Połączenia sieciowe wybrać nasze połączenie, a następnie właściwości tego połączenia

😰 Połączenia sieciowe	– 🗆 ×
\leftarrow \rightarrow \checkmark \bigstar Panel sterowania \Rightarrow Sieć i Internet \Rightarrow Połączenia sieciowe \Rightarrow \checkmark \eth	Przeszukaj: Połączenia sieciowe 👂
Organizuj 🔻	
Ethernet Sieć 8 Intel(R) PRO/1000 MT Desktop Ad Polacz_VPN_L2TP VAN Miniport (IKEv2)	
Elementy: 2	

Możemy sprawdzić nasze ustawienia lub wprowadzić dodatkowe opcje konfiguracyjne

Wła	ściwości:	Polacz_VPN_L2T	P		\times
Ogólne	Opcje	Zabezpieczenia	Sieć	Udostępnianie	
Nazwa lub 15	hosta lui 7.54.0.1 a	b adres IP miejsca albo 3ffe:1234::111	docelow 1):	ego (np. microsof	t.com
192.1	68.1.112				
Łąca	enie najp	ierw			
Sys tak wirt	tem Wind ą jak Inte ualnego.	lows może najpierv met, przed próbą u	v połączy stanowie	yć z siecią public: nia połączenia	zną,
	Wybierz r	najpierw numer inne	ego połą	czenia:	
					\sim
Zasad	y zachow	ania poufności info	macji		

Na zakładce Zabezpieczenia zmieniamy typ wirtualnej sieci prywatnej na protokół L2TP

aólne Opcie	Zabezpieczenia	Sieć	Udostepnianie	
Tup with place	oiooi parustaoi A/PN	n.	Cocception	
Typ wittdariej	sieci prywatnej (vri	v).		
Automatyczn	y			~
Protokół PP1	/ P (Point to Point Tur	nnelina P	rotocol)	
Protokół L2T	P/IPSec (Layer 2 Tu	Inneling	Protocol with IPse	ec)
Protokół SST IKEv2	P (Secure Socket T	unneling	Protocol)	
Uwierzytelni	anie			
O Użyj prot	okołu uwierzytelniani	ia rozsze	rzonego (EAP)	
			2	~~
			Właściwości	
○ Zezwalai	na użycie tych proto	kołów		
Protokół IKEv2. V typów sie	EAP-MSCHAPv2 zo Vybierz dowolny z po ci VPN.	ostanie uż danych p	tyty dla sieci VPN protokołów dla inr	typu nych
Hasło	nieszyfrowane (PAP	P)		
Protol (CHA	cół uwierzytelniania t ?)	ypu Chal	lenge Handshake	
Micro	soft CHAP wersja 2 (MS-CHA	P v2)	
Au (o	utomatycznie użyj mo raz domeny, jeżeli ist	ijej nazwy nieje) sys	y logowania i hasł temu Windows	а

A następnie w ustawieniach zaawansowanych zaznaczamy Użyj klucza wstępnego do uwierzytelnienia i podajemy nasz wcześniej ustawiony klucz z części IPsec.

PF -	Właś	ciwości	Polacz_VPN_L21	ſP		\times		
	Ogólne	Opcje	Zabezpieczenia	Sieć	Udostępnianie	t i	L	
	Typ wirtualnej sieci prywatnej (VPN):							
	Protokół L2TP/IPSec (Layer 2 Tunneling Protocol with IPsec)							
	Szyfrowanie danych:							
	Opcjonalne szyfrowanie (połącz, nawet jeśli bez szyfrowania)							
w	łaściwo	ści zaaw	ansowane				×	
	iuseinio.	2007	ansowanc				ĺ	
L	2TP							
	Ożyj klucza wstępnego do uwierzytelnienia							
	Klucz: zaq1@WSX							
	O Użyj certyfikatu do uwierzytelnienia							
	V 5	prawdź a	atrybuty nazwy i u	życia cer	tyfikatu serwer	a		
		-		-	-			
					OK	Anuluj		
					ОК	Anuluj		

Akceptujemy wprowadzone zmiany a następnie możemy połączyć się z naszą siecią.



Po wybraniu Połącz zostaniemy zapytani o użytkownika oraz jego hasło

	Zabezpieczenia Windows	×					
	Zaloguj						
nia	user_l2tp						
Series Refer	•••••						
	OK Anului						
	OK Anuluj						
	nyo						

Jeżeli nasze dane się zgadzają naszym oczom ukaże się napis Połączono.



5. Sprawdzenie działania

Aby sprawdzić działanie naszej konfiguracji możemy wykorzystać wiersz polecenia oraz polecenie ipconfig.

```
Wiersz polecenia
Microsoft Windows [Version 10.0.18362.1256]
(c) 2019 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\ala>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::4557:11de:d2b2:3608%9
  Default Gateway . . . . . . . . : 10.10.50.1
PPP adapter Polacz_VPN_L2TP:
  Connection-specific DNS Suffix . :
  IPv4 Address. . . . . . . . . . . . . 192.168.40.2
  C:\Users\ala>_
```

W cepu sprawdzenia komunikacji z routerem skorzystamy z polecenia ping.



Możemy też zauważyć ze na routerze zostanie utworzone połączenie dla użytkownika user_l2tp.

IAPsMAN										
nterfaces										
Vireless		PPP								
)ridge		Interface PPPoE	Servers Secrets	Profiles	Active Connec	tions L2TP S	ecrets			
PP				DDD Scapper				TD Carvar	OVDN Server	Γ.
4esh										
n	Þ	Name		△ Type		Actual MTU	L2 MTU	Tx	RX	
r		DR 🐢 <l2to-us< td=""><td>er 2to></td><td>L2TP Serv</td><td>/er Bindina</td><td>1400</td><td></td><td></td><td>0 bos</td><td>_</td></l2to-us<>	er 2to>	L2TP Serv	/er Bindina	1400			0 bos	_
4PLS	Þ									
Pv6	\square									
louting	$ \rangle$									
System	\triangleright									
Queues										
ilor										