Konfiguracja połączenia VPN z wykorzystaniem protokołu L2TP IPSec na przykładzie routera Mikrotik

Wstępna konfiguracja RouterOS w Virtualbox:

Ogólne Sieć	
System Karta 1 Karta 2 Karta 3 Karta 4	
Ekran 🗹 Włącz kartę sieciową	
Podłączona do: Mostkowana karta sieciowa (bridged) 🔻	
Nazwa: [Intel(R) Dual Band Wireless-AC 3160	•
Sieć	
Porty szeregowe	
USB USB	
Udostępniane foldery	
Interfejs użytkownika	
	OK Anului
	OK Andaj
RouterOS - Ustawienia	? >
📃 Ogólne Sieć	
Ogólne Sieć System Karta 1 Karta 2 Karta 3 Karta 4	
Ogólne Sieć System Karta 1 Karta 2 Karta 3 Karta 4 Karta 1 Karta 2 Karta 4 Karta 1 Karta 2 Karta 4 Karta4 Karta 4	
Ogólne Sieć System Karta 1 Karta 2 Karta 3 Karta 4 Karta 1 Karta 2 Karta 3 Karta 4 Włącz kartę sieciową Podłączona do: Sieć wewnętrzna Podłączona do: Sieć wewnętrzna	
Ogólne Sieć System Karta 1 Karta 2 Karta 3 Karta 4 Karta 1 Karta 2 Karta 3 Karta 4 Karta 1 Karta 2 Karta 3 Karta 4 Polięczkartę sieciową Podączona do: Sieć wewnętrzna Nazwa: §1	v
Ogólne Sieć System Karta 1 Karta 2 Karta 3 Karta 4 Ekran Podłączona do: Sieć wewnętrzna Podłączona do: Sieć wewnętrzna Nazwa: s1 Zaawansowane	×
Ogólne Sieć System Karta 1 Karta 1 Karta 2 Karta 1 Karta 3 Karta 1 Karta 4 Karta 1 Karta 3 Karta 3 Karta 4 Values Sieć Sieć Zaawandowane	v
■ Ogólne Sieć ■ System Karta 1 Karta 2 Karta 4 ■ Ekran ✓ Włącz kartę sieciową ● Pamięć Podłączona do: Sieć wewnętrzna ● Dźwięk Image: Sieć ● Potły szeregowe Zaawansowane	
■ Ogólne Sieć ■ System Karta 1 Karta 2 Karta 4 ■ Ekran ✓ Włącz kartę sieciową ● Pamięć Podłączona do: Sieć wwwnętrzna ● Dźwięk Sieć ● Sieć Vazwa: s1 ● Zaawansowane	
■ Ogólne Sieć ■ System Karta 1 Karta 2 Karta 3 Karta 4 ■ Ekran ✓ Włącz kartę sieciową ▶ Dźwięk Podłączona do: Sieć wewnętrzna ▼ ● Dźwięk ■ Sieć ● Porty szeregowe ✓ Udostępniane foldery	v
■ Ogólne Sieć ■ System Karta 1 Karta 2 Karta 4 ■ Ekran ✓ Włącz kartę sieciową ☑ Pamięć ✓ Podłączona do: Sieć wewnętrzna ▼ ☑ Dźwięk ✓ Nazwa: s1 ☑ Sieć ✓ Zaawansowane ☑ Udostępniane foldery ✓ ☑ Interfejs użytkownika ✓	v
Image: Ogólne Sieć Image: Ogólne Karta 1 Karta 1 Karta 2 Karta 1 Karta 3 Karta 1 Karta 4 Image: Ogólne Varta 1 Karta 1 Karta 3 Karta 1 Karta 3 Karta 1 Karta 3 Karta 1 Karta 3 Karta 3 Karta 4 Image: Varta 3 Varta 4 Image: Varta 4 Varta 3 Karta 5 Varta 5 Image: Varta 7 Varta 7 Image: Varta 7 Varta 7 Varta 8 Varta 8 Varta 9 Varta 8 Image: Varta 7 Varta 9 Varta 8 Varta 9 Varta 7 Varta 9 Varta 8 Varta 9 Varta 8 Varta 9 Varta 8 Varta 9 Varta 9 Varta 9 <td>v</td>	v
Image: Siece System Siece Sie	
■ Ogólne Sieć ■ System Karta 1 Karta 3 Karta 4 ■ Ekran ✓ Włącz kartę siedową Podłączona do: Sieć wewnętrzna ▼ ② Pamięć ✓ Włącz kartę siedową Podłączona do: Sieć wewnętrzna ▼ ③ Dźwięk ✓ Zaawancowane ✓ Zaawancowane ③ Udostępniane foldery Interfejs użytkownika ✓	v

3	RouterOS - Ustawienia	? ×
Jególne Ogólne	Sieć	
System	Karta <u>1</u> Karta <u>2</u> Karta <u>3</u> Karta <u>4</u>	
Ekran	✓ Włącz kartę sieciową	
Pamięć	Podłączona do: Sieć wewnętrzna 🔻	
🕩 Dźwięk	Nazwa: s1	· · · · · · · · · · · · · · · · · · ·
Sieć		
Porty szeregowe	1	
SB USB		
Udostępniane foldery		
Interfejs użytkownika		
		OK Anului
		OK Anuluj
		OK Anuluj
	RouterOS - Ustawienia	OK Anuluj ?
Dgólne	RouterOS - Ustawienia	OK Anuluj ? ×
Ogólne System	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4	OK Anuluj ? ×
Ogólne System Ekran	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Wlącz kartę sieciową	OK Anuluj
Ogólne System Ekran Pamieć	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 W Wlącz kartę siedową Podłączona do: Sieć wewnętrzna	OK Anuluj ? ×
Ogólne System Ekran Parnięć Dźwiek	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 Wylącz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: s1	OK Anuluj ? ×
Ogólne System Ekran Pamięć Dźwięk Sięć	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 Wacz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: s1 Zawansowane	OK Anuluj ? ×
	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Wlącz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: s1 Zaawansowane	OK Anuluj ? ×
Cyólne C	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Włącz kartę sieciową Podłączona do: Sieć wewnętrzna Vjazwa: s1 Zaawansowane	OK Anuluj ? ×
Cyólne Cyólne System Ekran Ekran Dźwięk Sięć Vorty szeregowe USB USB	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Włącz kartę sieciową Podłączona do: Sieć wewnętrzna V Nazwa: s1 Zaawansowane	OK Anuluj ? ×
C Ogólne C Ogólne C System C Ekran C Parnięć C Dźwięk C Sieć C Sieć C VSB Udostępniane foldery	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Włącz kartę sieciową Podłączona do: Sieć wewnętrzna Nazwa: s1 2aawansowane	OK Anuluj ? ×
	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Wacz kartę sieciową Podłączona do: Sieć wewnętrzna • Nazwa: s1 Zaawansowane	OK Anuluj ? ×
C Ogólne C Ogólne C System C System C Ekran C Pamięć Dźwięk C Sieć C Sieć Vorty szeregowe V USB Udostępniane foldery Interfejs użytkownika	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Wacz kartę sieciową Podłączona do: Sieć wewnętrzna V Nazwa: s1 Zaawansowane	OK Anuluj ? ×
C Ogólne C Ogólne C System C Kran C Pamięć Dźwięk C Oźwięk C Sieć V Osty szeregowe V US8 Udostępniane foldery US8 Udostępniane foldery C Sieć C Use C	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 V Włącz kartę sieciową Podłączona do: Sieć wewnętrzna V Nazwa: 51 Zaawansowane	OK Anuluj ? ×
	RouterOS - Ustawienia Sieć Karta 1 Karta 2 Karta 3 Karta 4 ♥ Włącz kartę sieciową Podłączona do: Sieć wewnętrzna ▼ Nazwa: s1 ♥ Zaawansowane	OK Anuluj ? ×

Topologia sieci

W przedstawionej konfiguracji występują dwie sieci, sieć publiczna oraz sieć prywatna. Szczegóły topologii zostały przedstawione na poniższym rysunku.



Konfiguracja VPN

Ustawiamy interfejsy sieciowe wg. poniższej konfiguracji:

+ -	X X II Y	7					Find	
Addre	ess	A Network	Interfac	æ				
D 中 19	2.168.1.222/24	192.168.1.0	ether1					
+ 19	2.168.88.1/24	192.168.88.0	bridge 1					
2 items								
								_
Bridge								
Bridge	Ports Port Extensio	ns VLANs MSTI	s Port I	MST Over	rides Filters	NAT H	losts MDB	
+ -		7					Find	
#	Interface	Bridge	Horizon	Trusted	Priority (h	Path Cost	Role	•
0	🖀 ether2	bridge1		no	80	10	designated port	
1	🖀 ether3	bridge1		no	80	10	backup port	
2	🖀 ether4	bridge1		no	80	10	backup port	
•								+

Interfejs ether1 jest podłączony do sieci WAN, i jest automatycznie konfigurowany przez DHCP dostawcy internetu.

Interfejs bridge zapewnia połączenia wewnątrz firmy, jest to sieć prywatna. Komputery w tej sieci uzyskują automatycznie adres z zakresu 192.168.88.2 - 192.168.88.254.

Ustalamy zakres adresów IP, jakie będą mogły być przydzielane w ramach połączenia VPN. W tym celu ustalamy pulę 50 adresów z zakresu 10.11.12.100 - 10.11.12.150.

IP Pool <vpn></vpn>	
Name: vpn	OK
Addresses: 10.11.12.100-10.11.12.150	Cancel
Next Pool: none	Apply
	Comment
	Сору
	Remove

W następnym kroku włączamy usługę L2TP Server, wybierając z menu PPP zakładkę Interface i pozycję L2TP Server:

PPP						
Interface PPPoE Servers Secrets Profiles	Active Connections	L2TP Secrets				
🕂 📼 🧭 🐹 🖾 🍸 PPP Scann	er PPTP Server	SSTP Server	L2TP Server	OVPN Server	PPPoE Scan	Find
Name / Type	L2TP Server				Tx Packet (p	o/s) Rx Packet (p/s ▼
		✓ Enabled		ОК		
	Max MTU:	1450		Cancel		
	Max MRU:	1450		Apply		
	MRRU:		•			
	Keepalive Timeout:	30				
	Default Profile:	default-encryptic	on Ŧ			
•	Max Sessions:		•			+
0 items out of 5	Authentication:	✓ mschap2	✓ mschap1			
		✓ chap	✓ pap			
	Use IPsec:	required	Ŧ			
	IPsec Secret:					
	Caller ID Type:	ip address	₹			
		One Session	Per Host			
		Allow Fast Pa	ath			

Zalecane jest włączenie opcji "Use IPsec" na required i podanie hasła. Typ autentykacji należy dobrać do środowiska, w jaki będą pracowały komputery korzystające z VPN. Profil szyfrowania możemy ustawić w pozycji "Default Profile". Można pozostawić domyślny, który zostanie zmodyfikowany w kolejnym kroku.

	PPP Profile <default-encryption></default-encryption>	
	General Protocols Limits Queue Scripts	ОК
	Name: default-encryption	Cancel
	Local Address: 10.11.12.1	Apply
	Remote Address: vpn 🗧 🔺	Comment
	Remote IPv6 Prefix Pool:	Conv
	DHCPv6 PD Pool:	Demonstra
PPP	Bridge:	
Interface PPPoE Servers Secrets Profiles Active Connecti	Bridge Port Priority:	
+	Bridge Path Cost:	Find
Name / Local Address / Remote Address	Bridge Horizon:	
default	Bridge Learning: default	
derauit-encryption 10.11.12.1 vpn	Incoming Filter:	
	Outgoing Filter:	
	Address List:	
	Interface List:	
	DNS Server:	
	WINS Server:	
2 items (1 selected)	- Change TCP MSS	
	C no 📀 yes C default	
	- Use UPnP	
	C no C yes ፍ default	
	default	

W domyślnym profilu PPP ustawiamy adres IP, który będzie bramą dla klientów poprawnie zalogowanych serwera. Przydzielony adres będzie pochodził z puli o nazwie "vpn".

W ostatnim kroku dodajemy użytkownika, za pomocą którego będzie można utworzyć połączenie VPN z siecią prywatną (firmową).

	PPP Secret <fred></fred>			
	Name:	user	ОК	
	Password:	••••	Cancel	
	Service:	l2tp ∓	Apply	
DDD	Caller ID:			
Luci ann co. Cambo a ta la s	Profile:	default-encryption F	Disable	
Interface PPPoE Servers Secrets Profiles Active Con	Local Address:		Comment	
+ - V X C Y PPP Authentication&Acco	Remote Address:		Сору	Find
Name / Password Service Caller ID Pro	Remote IPv6 Prefix:		Remove	Last Caller ID
	Besteen			
	IPuC Portos:	·		
	IF VO HOULES.	· · · · · · · · · · · · · · · · · · ·		
	Limit Bytes In:			
	Limit Bytes Out:			
	Last Logged Out:	May/05/2021 23:40:49		
•	Last Caller ID:	192.168.1.14		•
1 item (1 selected)	Last Disconnect Reason:	hung up		
	enabled			

W tym kroku jest ważne, aby pozycja "Profile" wskazywała na wcześniej zmodyfikowany profil szyfrowania.

Ostatni etap konfiguracji dotyczy ustawień zabezpieczeń systemowych (firewall), które pozwolą na ustanawianie połączeń z zewnątrz, do sieci prywatnej z wykorzystaniem protokołów L2TP IPsec.

W tym celu należy odblokować możliwość wykonywania połączeń na portach: 500, 1701, 4500 dla protokołu UDP. Dodatkowo należy jeszcze zezwolić na połączenia typu ipsec-esp, które służą do wymiany kluczy autoryzacyjnych klientów z serwerem.

Konfiguracja firewalla powinna wyglądać następująco:

Firewall												
Filter Rules NAT	Mangle Raw Ser	vice Ports C	Connections A	Address Lists	Layer7 Protocols							
+- **	🖆 🍸 🕻 🖓 🖾	et Counters	C Reset All C	ounters					Find	1	all	₹
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter	Out. Int	In. Inter	. Out. I	Int. 🔻
::: L2TP Server												
0	💙 accept	input			17 (udp)		500					
;;; L2TP Server												
1	🔶 accept	input			17 (udp)		1701					
;;; L2TP Server												
2	📌 accept	input			17 (udp)		4500					
;;; wymiana klucz	у											
3	💙 accept	input			50 (ipsec-esp)							
•												•
4 items												

Jeśli serwer został poprawnie skonfigurowany, to możemy za pomocą połączenia WAN uzyskać dostęp do sieci firmowej, za pomocą połączenia VPN:

Change adapter settings Change adapter settings Competed sharing Elsewin Vite your active networks Connection details Property Correction specific DM. Property Correction specific DM. Property Property Correction specific DM. Property Correction specific DM. Property Correction specific DM. Property Correction specific DM. Property Property Property Property Correction specific DM. Property Correction specific DM. Property Property Correction specific DM. Property Property Property Property Correction specific DM. Property	Control Panel Home	Network and Internet	Network and Sharing Center	▼ € € Search Control Panel				
See also HomeGroup HomeGroup Internet Options Windows Firewall Connection Details Property Value Connection Details: e Decorption DN. Decorption DN. Description DN. Decorption DN. Description DN. Decorption DN. Description DN. Decorption The Rebox Baver Direct Address 08/027/39/815F DHCP Enabled No Internet meetion; or set up a router or Internet Options Windows Firewall NetWork Connection Details Internet access Windows Firewall Directory or set up a router or Prov Default Gateway Internet access Prov Default Gateway Internet Access Windows Firewall Internet Options Windows Firewall Internet Options	Change adapter settings Change advanced sharing settings	View your basic IE9WIN7 (This compute View your active netw	network information and set	up connections	P ct		_	
See also Property Value Internet Options Windows Firewall		Network Connection Deta Network Connection Details	ils 🛛 🖾	3 e: Internet ns: 🔋 VPN Connection	Network Connection Detail	ils		
See also IP-4 Default Gateway IP-4 Default Gateway Internet access Internet access IP-4 Diss Server 192,168.1.1 IP-4 Diss Server Internet access Internet Options IP-6 Default Gateway IP-6 Default Gateway IP-6 Default Gateway Windows Firewall IP-6 Default Gateway IP-6 Default Gateway IP-6 Default Gateway		Property Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask	Value VPN Connection No 10.11.12.150 255.255.255	e: Internet ns: 📮 Local Area Connection 2	Property Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask	Value netboot server hnet(R) PRO/1000 MT Desktop Adapte 08-00-27-99-81-5F Yes 192.168.1.14 255.255.255.0	Currently connected to: Network 11 Internet access VPN Connection	4,
Internet Options Windows Firevall Unrecode units of the sharing settings Unrecode units of the sharing setting setting settings Unrecode units of the sharing setting setting setting setting setting sett	See also HomeGroup	IPv4 Default Gateway IPv4 DNS Server IPv4 WINS Server NetBIOS over Topip En Link-local IPv6 Address IPv6 Default Gateway IPv6 DNS Server	192.168.1.1 Yes fe80::487b14fbb786.edee%23	onnection; or set up a router or PN network connection.	Lease Colaired Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DNS Server IPv4 WINS Server NetBIOS over Topip En	Vesi resolar, may coll 2021 3-48-24 AM 192,168.1.1 192,168.1.1 192,168.1.1 192,168.1.1 192,168.1.1	Dial-up and VPN	Connected
Close	Internet Options Windows Firewall			puters, or change sharing settings.	IPv6 Default Gateway IPv6 DNS Server	1600:2200:4013;4140;4331415	•	
			Close			Close	Occo Network and S	having Cartas

Aby autoryzacja się powiodła, przy nawiązywaniu połączenia VPN, należy wybrać typ sieci jako L2TP/IPsec z kluczem wstępnym, w przeciwnym wypadku połączenie nie zostanie nawiązane.