



GUIDA TECNICA

**Configurazione delle VPN
LAN-to-LAN su DRAYTEK
2865-2765-2927-2962**



Le guide hanno esclusivamente uno scopo esplicativo.
VoipVoice declina ogni responsabilità derivante dall'applicazione di quanto riportato nelle medesime.

1. Abilitazioni protocolli

Procedere in primis con l'abilitazione dei protocolli VPN che dovremmo utilizzare, isolando le altre.

Rechiamoci nella sezione VPN and Remote Access → Remote Access Control.

VPN and Remote Access >> Remote Access Control

Remote Access Control Setup	Bind to WAN
☐ Enable PPTP VPN Service	
☒ Enable IPsec VPN Service	
☐ Enable L2TP VPN Service	
☒ Enable SSL VPN Service	
☐ Enable OpenVPN Service	
☐ Enable WireGuard VPN Service	

Note:

1. To allow VPN pass-through to a separate VPN server on the LAN, disable the services listed above that use the same protocol and ensure that NAT **Open Ports** or **Port Redirection** is well-configured.
2. Disable unused VPN services, enable **Brute Force Protection**, and **block unknown IP access** to the used VPN services to reduce Cyberattacks.

OK Clear Cancel

2. IPsec IKEv2

Rechiamoci nella sezione VPN and Remote Access → LAN to LAN e selezioniamo un profilo, partiremo configurando il profilo per il Dial-In, quindi l'utente in ascolto, successivamente configureremo l'utente Dial-Out.

Configuriamo il profilo mettendo il flag su Enable, dandogli un nome e decidendo la direzione, in questo caso Dial-In, inseriamo inoltre da quale WAN desideriamo che esca la VPN;

In seguito, impostiamo il tipo di VPN da utilizzare, quindi teniamo il flag esclusivamente su IPsec e specifichiamo l'IP pubblico del Dial-Out con cui vogliamo fare il collegamento VPN;

Creiamo una Pre-Shared Key sicura da condividere con il Dial-Out;

Infine, compiliamo l'ultimi campi inserendo la nostra subnet locale e la subnet locale del Dial-Out con cui stiamo facendo il collegamento VPN.

Di seguito una schermata di esempio di corretta configurazione.

Profile Index : 4
Common Settings

☒ Enable this profile Profile Name: test-VPN	Always on: ☐ Enable Idle Timeout: 300 second(s) Quality Monitoring/Keep Alive: ☐ Enable
Call Direction: ☐ Both ☐ Dial-Out ☒ Dial-In Dial-Out Through: WAN1 Only	Netbios Naming Packet: ☒ Pass ☐ Block Multicast via VPN: ☐ Pass ☒ Block (for some IGMP, IP-Camera, DHCP Relay, etc.)

Dial-In Settings

Allowed VPN Type ☐ PPTP ☒ IPsec Tunnel(IKEv1/IKEv2) ☐ IPsec XAuth ☐ L2TP with IPsec Policy: Must ☐ SSL Tunnel ☒ OpenVPN Tunnel: UDP/TCP ☐ WireGuard	Username: Password: PPP Advanced Settings OpenVPN Advanced Settings Cipher Algorithm: AES256-CBC HMAC Algorithm: SHA256 Allowed IKE Authentication Method ☒ Pre-Shared Key: ***** ☐ X.509 Digital Signature: None Preferred Local ID: Alternative Subject Name Allowed IPsec Security Method ☒ AH ☒ ESP-DES ☒ ESP-3DES ☒ ESP-AES
☒ Specify Remote VPN Gateway Remote IP: 1.2.3.4 Peer ID: Local ID:	

Tunnel Settings

☐ Enable IPsec Dial-Out function GRE over IPsec Tunnel Local IP:	☐ Logical Traffic Tunnel Remote IP:
--	---

6in4 Settings

☐ Enable 6in4 over PPTP LAN Interface: LAN1 Remote LAN IP: 0.0.0.0 LAN IPv6 Prefix: :: / 64 Remote IPv6 Prefix: :: / 64 Tunnel TTL: 255	
--	--

TCP/IP Network Settings

Local Network IP: 192.168.10.0 / Mask: 255.255.255.0 / 24 Remote Network IP: 192.168.18.0 / Mask: 255.255.255.0 / 24 More Remote Subnet:	Mode: ☒ Routing ☐ NAT RIP via VPN: Disable Translate Local Network: ☐ Enable ☐ Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
--	--

OK Clear Cancel

Una volta stabilito il Dial-In, procediamo con il Dial-Out, la configurazione è simile, ma andremo a cambiare qualche parametro.

Configuriamo il profilo mettendo il flag su Enable, dandogli un nome e decidendo la direzione, in questo caso Dial-Out, inseriamo inoltre da quale WAN desideriamo che esca la VPN;

In seguito, impostiamo il tipo di VPN da utilizzare, quindi teniamo il flag esclusivamente su IPsec e IKEv2, specificando l'IP pubblico del Dial-In con cui vogliamo fare il collegamento VPN; Mettiamo il flag di Enable sul parametro Always on e riportiamo la Pre-Shared Key precedentemente creata;

Infine, compiliamo gli ultimi campi inserendo la nostra subnet locale e la subnet locale del Dial-In con cui stiamo facendo il collegamento VPN.

Di seguito una schermata di esempio di corretta configurazione.

Profile Index : 4
Common Settings

☒ Enable this profile Profile Name: test-VPN	Always on: ☒ Enable Idle Timeout: 1 second(s) Quality Monitoring/Keep Alive: ☐ Enable
Call Direction: ☐ Both ☒ Dial-Out ☐ Dial-In GRE Tunnel: ☐ GRE Tunnel Dial-Out Through: WAN1 Only	Netbios Naming Packet: ☒ Pass ☐ Block Multicast via VPN: ☐ Pass ☒ Block (for some IGMP, IP-Cameras, DHCP Relay, etc.)

Dial-Out Settings

VPN Server Type ☐ PPTP ☒ IPsec Tunnel IKEv2 ☐ L2TP with IPsec Policy Must ☐ SSL Tunnel ☐ OpenVPN Tunnel TCP ☐ WireGuard	IKE Phase 1 Settings Mode: ☒ Main mode ☐ Aggressive mode Authentication: Pre-Shared Key Pre-Shared Key: ***** Local ID(optional): Max 47 characters Proposal Encryption: Auto Proposal DH Group: Group 14 (2048 bit) Proposal Authentication: SHA256 Force UDP Encapsulation: ☐ Enable
Server IP/Host Name: 1.2.3.4 Dial-Out Schedule Profile: None	IKE Phase 2 Settings Security Protocol: ☒ ESP(High) ☐ AH(Medium) Proposal Encryption: AES256 Proposal Authentication: All
IKE Advanced Settings Ping to Keep Alive: ☐ Enable PING Target IP:	

Tunnel Settings

☐ Enable IPsec Dial-Out function GRE over IPsec Tunnel Local IP:	☐ Logical Traffic Tunnel Remote IP:
---	--

IPv4 Settings

☐ Enable IPv4 over PPTP LAN Interface: LAN1 Remote LAN IP: 0.0.0.0 LAN IPv6 Prefix: :: / 64 Remote IPv6 Prefix: :: / 64 Tunnel TTL: 255
--

TCP/IP Network Settings

Local Network IP: 192.168.10.0 / Mask: 255.255.255.0 / 24 Remote Network IP: 192.168.18.0 / Mask: 255.255.255.0 / 24 More Remote Subnet	Mode: ☒ Routing ☐ NAT RIP via VPN: Disable Translate Local Network: ☐ Enable ☐ Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
---	--

OK Clear Cancel

3. SSL Tunnel

Rechiamoci nella sezione VPN and Remote Access → LAN to LAN e selezioniamo un profilo, partiremo configurando il profilo per il Dial-In, quindi l'utente in ascolto, successivamente configureremo l'utente Dial-Out.

Configuriamo il profilo mettendo il flag su Enable, dandogli un nome e decidendo la direzione, in questo caso Dial-In, inseriamo inoltre da quale WAN desideriamo che esca la VPN; In seguito, impostiamo il tipo di VPN da utilizzare, quindi teniamo il flag su SSL Tunnel, specificando l'IP pubblico del Dial-Out con cui vogliamo fare il collegamento VPN; Infine, compiliamo gli ultimi campi inserendo username e password del profilo e la nostra subnet locale e la subnet locale del Dial-Out con cui stiamo facendo il collegamento VPN. Di seguito una schermata di esempio di corretta configurazione.

Profile Index : 1

Common Settings

☒ Enable this profile Profile Name: VPN-TEST	Always on: ☐ Enable Idle Timeout: 300 second(s) Quality Monitoring/Keep Alive: ☐ Enable
Call Direction: ☐ Both ☐ Dial-Out ☒ Dial-In ☐ GRE Tunnel	Netbios Naming Packet: ☒ Pass ☐ Block Multicast via VPN: ☐ Pass ☒ Block (for some IGMP, IP-Camera, DHCP Relay, etc.)
Dial-Out Through: WAN1 First	

Dial-In Settings

Allowed VPN Type ☐ PPTP ☐ IPsec Tunnel(IKEv1/IKEv2) ☐ IPsec XAuth ☐ L2TP with IPsec Policy: Must ☒ SSL Tunnel ☐ OpenVPN Tunnel ☐ WireGuard	Username: voipvoice-test Password: ***** PPP Advanced Settings OpenVPN Advanced Settings Cipher Algorithm: AES256-CBC HMAC Algorithm: SHA256 Allowed IKE Authentication Method ☒ Pre-Shared Key: Max: 128 characters ☐ X.509 Digital Signature: None Preferred Local ID: Alternative Subject Name Allowed IPsec Security Method ☒ AH ☒ ESP-DES ☒ ESP-3DES ☒ ESP-AES
☒ Specify Remote VPN Gateway Remote IP: 8.8.8.8 Peer ID: Max: 128 characters Local ID: Max: 47 characters	

Tunnel Settings

☐ Enable IPsec Dial-Out function GRE over IPsec Tunnel Local IP:	☐ Logical Traffic Tunnel Remote IP:
---	--

6in4 Settings

☐ Enable 6in4 over PPTP LAN Interface: LAN1 Remote LAN IP: 0.0.0.0 LAN IPv6 Prefix: :: / 64 Remote IPv6 Prefix: :: / 64 Tunnel TTL: 255
--

TCP/IP Network Settings

Local Network IP: 192.168.1.0 / Mask: 255.255.255.0 / 24 Remote Network IP: 192.168.5.0 / Mask: 255.255.255.0 / 24 More Remote Subnet: ☐	Mode: ☒ Routing ☐ NAT RIP via VPN: Disable Translate Local Network: ☐ Enable ☐ Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
---	--

Una volta stabilito il Dial-In, procediamo con il Dial-Out, la configurazione è simile, ma andremo a cambiare qualche parametro.

Configuriamo il profilo mettendo il flag su Enable, dandogli un nome e decidendo la direzione, in questo caso Dial-Out, inseriamo inoltre da quale WAN desideriamo che esca la VPN;

In seguito, impostiamo il tipo di VPN da utilizzare, quindi teniamo il flag esclusivamente su SSL Tunnel e specifichiamo l'IP pubblico del Dial-In con cui vogliamo fare il collegamento VPN;

Inseriamo la username e password per questo profilo precedentemente creata e teniamo il flag dell' Always on su Enable;

Infine, compiliamo l'ultimi campi inserendo la nostra subnet locale e la subnet locale del Dial-In con cui stiamo facendo il collegamento VPN.

Di seguito una schermata di esempio di corretta configurazione.

Profile Index : 3

Common Settings

☒ Enable this profile Profile Name: TEST-VPN	Always on: ☒ Enable Idle Timeout: -1 second(s) Quality Monitoring/Keep Alive: ☐ Enable
Call Direction: ☐ Both ☒ Dial-Out ☐ Dial-In GRE Tunnel: ☐ GRE Tunnel Dial-Out Through: WAN1 First	Netbios Naming Packet: ☒ Pass ☐ Block Multicast via VPN: ☐ Pass ☒ Block (for some IGMP, IP-Camera, DHCP Relay, etc.)

Dial-Out Settings

VPN Server Type ☐ PPTP ☐ IPsec Tunnel (IKEv2 EAP) ☐ L2TP with IPsec Policy (Must) ☒ SSL Tunnel (TCP) ☐ OpenVPN Tunnel ☐ WireGuard	Username: voipvoice-test Password: ***** PPP Advanced Settings
Server IP/Host Name: 8.8.8.8 : Port (SSL): 443	
Dial-Out: Schedule Profile None None None None	

Tunnel Settings

☐ Enable IPsec Dial-Out function GRE over IPsec Tunnel Local IP:	☐ Logical Traffic Tunnel Remote IP:
--	---

6in4 Settings

☐ Enable 6in4 over PPTP LAN Interface: LAN1 Remote LAN IP: 0.0.0.0 LAN IPv6 Prefix: :: / 64 Remote IPv6 Prefix: :: / 64 Tunnel TTL: 255
--

TCP/IP Network Settings

Local Network IP: 192.168.1.0 / Mask: 255.255.255.0 / 24 Remote Network IP: 192.168.4.0 / Mask: 255.255.255.0 / 24 More Remote Subnet:	Mode: ☐ Routing ☒ NAT RIP via VPN: Disable Translate Local Network: ☐ Enable ☐ Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
--	---

OK Clear Cancel

4. Overlapping

Nel caso si necessitasse di aggiungere più subnet su una VPN basterà recarsi sulla parte finale della configurazione ed espandere l'opzione More Remote Subnet.

TCP/IP Network Settings

Local Network IP: 192.168.10.0 / Mask: 255.255.255.0 / 24 Remote Network IP: 192.168.18.0 / Mask: 255.255.255.0 / 24 More Remote Subnet ☐ Create a unique SA for each subnet(IPsec) Network IP: 192.168.50.60 Subnet Mask: 255.255.240.0 / 20 Add Delete Edit	Mode: ☒ Routing ☐ NAT RIP via VPN: Disable Translate Local Network: ☐ Enable ☐ Change Default Route to this VPN tunnel (This only works if there is only one WAN online)
---	--

OK Clear Cancel