

## DRAYTEK ROUTERLARI ARASINDA IKEv2 VPN KURMA

IKEv1'den geliştirilen IKEv2, yeni bir VPN protokolüdür ve önceki sürümden çok daha fazla geliştirmeye sahiptir. IKEv1 ile karşılaştırıldığında, IKEv2 daha kararlıdır, bağlantıyı daha güvenli hale getiren en yeni şifreyi destekler ve kurulması daha kısa sürer ve point-to-point protokolü kaldırarak IKEv2'nin bağlantı kurması daha kısa sürer.

Bu makale iki Vigor Router arasında nasıl IKEv2 VPN kurulacağını göstermektedir.

### DrayOS

#### VPN Server (Dial-In) Ayarları

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin.
  - a. **Pre-Shared Key** girin.
  - b. **Pre-Share Key Confirm**'e tekrar girin.
  - c. **OK**'a tıklayın.

#### VPN and Remote Access >> IPsec General Setup

##### VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

<b>IKE Authentication Method</b>	
Certificate for Dial-in	None ▾
<b>Pre-Shared Key</b>	
Pre-Shared Key	.....
Confirm Pre-Shared Key	.....
<b>IPsec Security Method</b>	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.

OK

Cancel

2. **VPN and Remote Access >> LAN to LAN** sayfasına gidin ve uygun bir indexe tıklayın.
  - a. **Enable this profile** etkinleştirin.
  - b. Call Direction için **Dial-in** seçeneğini seçin.

#### VPN and Remote Access >> LAN to LAN

Profile Index : 1

##### 1. Common Settings

Profile Name	Server	Call Direction	<input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile		Tunnel Mode	<input type="radio"/> GRE Tunnel
VPN Dial-Out Through	WAN1 First	<input type="checkbox"/> Always on	
Netbios Naming Packet	<input checked="" type="radio"/> Pass <input type="radio"/> Block	Idle Timeout	0 second(s)
Multicast via VPN	<input type="radio"/> Pass <input checked="" type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	
(for some IGMP,IP-Camera,DHCP Relay..etc.)			
		PING to the IP	

- c. Dial-in Settings'de **IPsec Tunnel**'e izin verin.

## 3. Dial-In Settings

<b>Allowed Dial-In Type</b> <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> <b>IPsec Tunnel</b> <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy <span>None</span> <input type="checkbox"/> SSL Tunnel  <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <span>Max: 47 characters</span>	Username <input type="text" value="???"/> Password(Max 11 char) <span>Max: 11 characters</span> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off  <b>IKE Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <span>Max: 64 characters</span> <input type="checkbox"/> Digital Signature(X.509) <span>None</span> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First  <b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
--	---

- d. **Remote Network IP** ve **Mask** için için VPN Server tarafından kullanılan IP Subnet'ini girin.  
e. **OK**'a tıklayın.

## 5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.60.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.62.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <span>Disable</span> From first subnet to remote network, you have to do <span>Route</span> <input type="checkbox"/> IPsec VPN with the Same Subnets  <input type="checkbox"/> Change default route to this VPN tunnel ( Only active if one single WAN is up )
---	---

## VPN Client (Dial-Out) Ayarları

3. Benzer şekilde, **VPN and Remote Access >> LAN to LAN**'da bir profil oluşturun.
- Profile name** verin.
  - Enable this profile** etkinleştirin.
  - Call Direction için **Dial-Out** seçeneğini seçin.
  - Type of Server için **IPsec Tunnel** ve **IKEv2** seçeneklerini seçin.
  - Server IP/Host Name for VPN**'de VPN sunucusunun WAN IP'sini ya da domain adını girin.
  - VPN sunucusunun **Pre-Shared Key**'ini girin.

1. Common Settings

Profile Name <input type="text" value="Client"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> <b>Dial-Out</b> <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	Tunnel Mode <input type="radio"/> GRE Tunnel
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	<input type="checkbox"/> Always on
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	Idle Timeout <input type="text" value="300"/> second(s)
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP <input type="text"/>

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> <b>IPsec Tunnel</b> <input type="text" value="IKEv2"/> <input type="radio"/> IKEv2 EAP <input type="radio"/> IPsec XAuth <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel	Username <input type="text" value="???"/> Password <input type="text" value="Max: 15 characters"/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. <small>(such as draytek.com or 123.45.67.89)</small> <input type="text" value="ikev2.server.net"/>	<b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="....."/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
Server Port (for SSL Tunnel): <input type="text" value="443"/>	<b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="DES with Authentication"/> <input type="button" value="Advanced"/>

- g. **Remote Network IP** ve **Mask** için VPN Server tarafından kullanılan IP Subnet'ini girin.
- h. **OK**'a tıklayın.

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="Disable"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do <input type="text" value="Route"/>
Remote Network IP <input type="text" value="192.168.62.1"/>	<input type="checkbox"/> IPsec VPN with the Same Subnets
Remote Network Mask <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel ( Only active if one single WAN is up )
Local Network IP <input type="text" value="192.168.60.1"/>	
Local Network Mask <input type="text" value="255.255.255.0"/>	
<input type="button" value="More"/>	

- 4. VPN'i başlatmak için **VPN and Remote Access >> Connection Management** sayfasına gidin. VPN profilini seçin ve **Dial**'e tıklayın.

**VPN and Remote Access >> Connection Management**

**Dial-out Tool**

General Mode: <b>( Client ) ikev2.server.net</b>	<input type="button" value="Dial"/>
Backup Mode: <input type="text"/>	<input type="button" value="Dial"/>
Load Balance Mode: <input type="text"/>	<input type="button" value="Dial"/>

5. VPN başarıyla kurulduğunda, bağlantı durumu gösterilecektir.

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode:	( Client ) ikev2.server.net	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

VPN Connection Status

LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 ( Client )	IKEv2 IPsec Tunnel AES-SHA1 Auth	192.168.29.29 via WAN2	192.168.62.1/24	8	35.26	9	35.26	0:0:59

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.

Linux

1. VPN and Remote Access >> IPsec General Setup sayfasına gidin. Preshared Key'i girin ardından Apply'a tıklayın.

VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key : ..... (Max 46 characters)

WAN Profile : wan1

DHCP LAN Profile : lan1

IKE Port : 500

NAT-T Port : 4500

IPsec MSS : 1360

2. VPN and Remote Access >> VPN Profiles sayfasına gidin ve Add'e tıklayın.
- Local IP/Subnet Mask'da VPN istemcisinin kullandığı IP Subnet'i girin.
  - Remote IP/Subnet Mask'da VPN Server'ın kullandığı IP Subnet'ini girin.
  - IKE Protocol için IKEv2 seçeneğini seçin.
  - Apply'a tıklayın.

VPN and Remote Access >> VPN Profiles >> IPsec

IPsec PPTP Dial-out PPTP Dial-in SSL Dial-out SSL Dial-in GRE

**Add** Edit Delete Rename Refresh Profile Number

Profile : IKEv2\_Server

Enable

Basic Advanced GRE Proposal Multiple SAs

Auto Dial-Out :  Enable  Disable

For Remote Dial-In User :  Enable  Disable

Dial-Out Through : wan1  Default WAN IP  WAN Alias IP

Fallover to :

Local IP / Subnet Mask : 192.168.239.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : 0.0.0.0

Remote IP / Subnet Mask : 192.168.29.0 255.255.255.0/24

More Remote Subnet : 

IP	Subnet Mask
No items to show.	

IKE Protocol : IKEv2

Auth Type : PSK

Preshared Key :

Security Protocol : ESP

Add Save Profile Number Limit : 16

### VPN Client Ayarları

3. VPN and Remote Access >> VPN Profiles sayfasına gidin ve Add'e tıklayın.
  - a. Local IP/Subnet Mask'da VPN istemcisinin kullandığı IP Subnet'i girin.
  - b. Remote Host'da VPN Server'ın WAN IP'sini ya da domain adını girin.
  - c. Remote IP/Subnet Mask'da VPN Server'ın kullandığı IP Subnet'ini girin.
  - d. IKE Protocol için **IKEv2** seçeneğini seçin.
  - e. Adım 1'de ayarlanan Preshared Key'i yazın
  - f. Apply'a tıklayın.

IPsec

Profile : IKEv2\_Client

Enable

Basic Advanced GRE Proposal Multiple SAs

For Remote Dial-In User :  Enable  Disable

Dial-Out Through : wan1  Default WAN IP  WAN Alias IP

Fallover to :

Local IP / Subnet Mask : 192.168.29.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host : ikev2.server.net

Remote IP / Subnet Mask : 192.168.239.0 255.255.255.0/24

More Remote Subnet : 

IP	Subnet Mask
No items to show.	

IKE Protocol : IKEv2

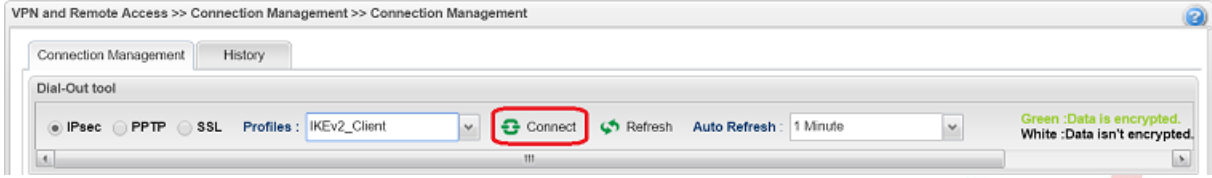
Auth Type : PSK

Preshared Key : .....

Security Protocol : ESP

Add Save Profile Number Limit : 16

4. VPN'i aramak için **VPN and Remote Access >> Connection Management** sayfasına gidin. VPN profilini seçin, Connect'a tıklayın.



5. VPN başarıyla kurulduğunda, VPN durumu gösterilecektir.

