

iOS'TAN VIGOR ROUTER'A IKEv2 VPN

Bu makale Vigor Router'ü IKEv2 VPN için bir VPN server olarak nasıl ayarlanacağını ve VPN'in bir iOS cihazından nasıl başlatılacağını göstermektedir.

Vigor Router Üzerinde Kurulum

DrayOS

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin. **Pre-Shared Key** girin. **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).

IKE Authentication Method	
Certificate for Dial-in	None ▼
Pre-Shared Key	
Pre-Shared Key
Confirm Pre-Shared Key
IPsec Security Method	
<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 >> Remote Dial-in User** sayfasına gidin. Profili ayarlamak için uygun bir index numarasına tıklayın.

- **Enable this account** işaretleyin.
- Allowed Dial-In Type sekmesinde **IPsec Tunnel** işaretleyin.
- Kaydetmek için **OK**'a tıklayın.

Index No. 4

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="0"/> second(s)	Username <input type="text" value="???"/> Password(Max 19 char) <input type="text"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> ▼ <input type="checkbox"/> SSL Tunnel	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> ▼
<input type="checkbox"/> Specify Remote Node Remote Client IP <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/>
Subnet <input type="text" value="LAN 1"/> ▼ <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>	

OK Clear Cancel

Tüm ayarlar tamamlandı. VPN kullanıcısı çevrim içi ise VPN and Remote Access >> Connection Management sayfasında VPN bağlantısının durumunu görebilirsiniz.

VPN and Remote Access >> Connection Management

Dial-out Tool

General Mode: 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 (Dynamic Client)	IKEv2 IPsec Tunnel AES-SHA256 Auth	192.168.29.18 via WAN2	192.168.86.11/32	4	4.35	4	1.41	0:0:4

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

Linux

1. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin. **Pre-Shared Key** girin. Kaydetmek için **Apply**'a tıklayın.

VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key : (Max 46 characters)

IPsec User Preshared Key : (Only for XAuth, Max 46 characters)

WAN Profile : wan1, wan2, wan3

DHCP LAN Profile : lan1

IKE Port : 500

NAT-T Port : 4500

IPsec MSS : 1360

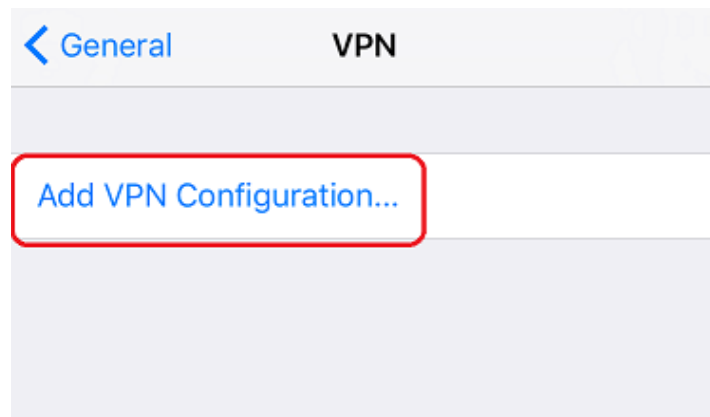
2. **VPN and Remote Access >> VPN Profiles** sayfasından bir IPsec VPN profil ekleyin.
 - **Profile name** girin.
 - **Enable**'i işaretleyin.
 - **For Remote Dial-in User** için "Enable" seçin.
 - **Local IP/Subnet Mask** 'ında VPN client için LAN ağını belirtin.
 - **IKE Protocol** için "IKEv2" seçin.
 - **Apply**'a tıklayın.

Tüm ayarlar tamamlandı. VPN kullanıcısı çevrim içi ise VPN and Remote Access >> Connection Management sayfasında VPN bağlantısının durumunu görebilirsiniz.

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation	
1	IKEv2:1	IKEv2:IPsec...	wan2	220.132...	192.168.29.16/32	00:00:40	8.51 (Kbps)	366.46 (Kbps)	443.59 (KB)	873.24 (KB)	

iOS'tan VPN Bağlantısı

1. **Settings >> General >> VPN**'e gidin ve **Add VPN Configuration** 'a tıklayın.



2. Konfigurasyonu aşağıdaki gibi ayarlayın.
 - **Type** için "IKEv2" seçin.
 - **Server and Remote ID**'de routerın WAN IP ya da hostname tipini yazın.

- **User Authentication için** “None” seçin.
- **Use Certificate**'i devre dışı bırakın.
- **Secret**'a routerin IPsec General Setup'taki Pre-Shared anahtarını yazın.
- **Done**'a tıklayın.

Cancel IKEv2 Done

Type IKEv2

Description IKEv2

Server ikev2.vpnserver.net

Remote ID ikev2.vpnserver.net

Local ID

AUTHENTICATION

User Authentication None >

Use Certificate

Secret ●●●●●●●●

PROXY

Off Manual Auto

3. IKEv2 VPN bağlantısını Vigor routera ile başlatmak için Status'u etkinleştirin.

< General VPN

VPN CONFIGURATIONS

Status Not Connected

✓ IKEv2 Unknown ⓘ

Add VPN Configuration...