

## WINDOWS 10'DAN VIGOR ROUTER'A IPsec ÜZERİNDEN L2TP

Bu makale, Vigor Router'ın IPsec üzerinden L2TP için VPN server olarak kurulmasının yanı sıra Vigor Router'a bir VPN kurmayı ve Vigor Router'ın LAN ağına erişmek için Windows 10'un gömülü VPN özelliğini nasıl kullanacağınızı anlatmaktadır.

### Vigor Router Üzerinde Kurulum

#### DrayOS

1. Routerın internete bağlı olduğundan emin olun. Routerın WAN IP adresini veya domain adını unutmayın.
2. "Enable IPsec VPN Service" ve "Enable L2TP VPN Service" seçeneklerinin işaretli olduğundan emin olmak için **VPN and Remote Access >> Remote Access Control Setup** sayfasına gidin.

#### VPN and Remote Access >> Remote Access Control Setup

##### Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPsec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

3. Uzaktan çevirmeli kullanıcı profili oluşturma: **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. Profili düzenlemek için uygun bir index numarasını tıklayın.

#### VPN and Remote Access >> Remote Dial-in User

##### Remote Access User Accounts:

[Set to Factory Default](#)

Index	User	Active	Status	Index	User	Active	Status
<b>1.</b>	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---

4. Profili aşağıdaki gibi düzenleyin.

- **Enable this account**'u etkinleştirin.
- **Allowed Dial-In Type** sekmesinde L2TP işaretleyin ve IPsec Policy için "Must" ayarlayın.
- **Username** ve **Password** girin.
- Kaydetmek için **OK**'a tıklayın.

#### VPN and Remote Access >> Remote Dial-in User

##### Index No. 1

##### User account and Authentication

Enable this account

Idle Timeout: 300 second(s)

##### Allowed Dial-In Type

PPTP

IPsec Tunnel

L2TP with IPsec Policy: **Must**

SSL Tunnel

Username: draytekfae

Password(Max 19 char): .....

Enable Mobile One-Time Passwords(mOTP)

PIN Code: [ ]

Secret: [ ]

##### IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: [ ]

5. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin. Bir **Pre-Shared Key** girin ve kaydetmek için **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**

Medium (AH)  
Data will be authentic, but will not be encrypted.

High (ESP)  DES  3DES  AES  
Data will be encrypted and authentic.

OK Cancel

6. Artık router uzaktan bağlantı kullanıcıları için kullanıma hazır. Ağ yöneticisi çevrimiçi olan kullanıcıları **VPN and Remote Access >> Connection Management** sayfasından kontrol edebilir.

VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh

General Mode: [Dropdown] Dial

Backup Mode: [Dropdown] Dial

Load Balance Mode: [Dropdown] Dial

VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime
1 ( draytekfae ) Local User Database	L2TP AES-SHA256 Auth	<del>192.168.186.18</del> via WAN2	192.168.46.14/32	0	0	1	24	0:0:5

vvvvvvvv · Data is encrypted

Linux

1. **User Management >> User Profile** 'a gidin. Yeni bir profil eklemek için **Add**'e tıklayın ve konfigürasyon için aşağıdaki adımları takip edin.
- **Enable**'yi işaretleyin.
  - **Username** ve **Password** girin.
  - L2TP Dial-In için "Enable" seçeneğini seçin.
  - Kullanıcı profilini kaydetmek için **Apply**'a tıklayın.

User Management User Profile

User Profile

**Add** ✕

Usema...

Username : user1

Enable

Password : ..... Strength : Good

System User : false

PPTP/L2TP/SSL/PPPoE/OpenVPN Server General Setup

Idle Timeout(sec) : 300

DHCP from : lan1

Static IP Address : (Optional)

^ User Management

^ PPTP/L2TP/SSL/OpenVPN Server

PPTP Dial-in :  Enable  Disable

**L2TP Dial-in :  Enable  Disable**

SSL Tunnel :  Enable  Disable

OpenVPN Dial-in :  Enable  Disable

XAuth / EAP :  Enable  Disable

Use mOTP :  Enable  Disable

Time Objects : [ ]

Apply Cancel

1. VPN >> Remote Access Control'e gidin ve Enable L2TP VPN Service 'i işaretleyin.

VPN and Remote Access >> Remote Access Control

Remote Access Control

Enable PPTP VPN Service

**Enable L2TP VPN Service**

Enable SSL Tunnel Service (While SSL VPN Port is equal to HTTPS Management Port, please ensure HT

Enable OpenVPN Service (OpenVPN will create interface tun0(udp) & tun1(tcp) automatically when servic

Enable IPsec Service

IPsec Remote Dial-In Service :  None  **L2TP over IPsec**  DHCP over IPsec

2. VPN >> IPsec General Setup 'a gidin ve Preshared Key girin.

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

User Authentication Type : Local (Local/Radius support IPsec XAuth/EAP user, LDAP c

DHCP LAN Profile : lan1

IKE Port : 500

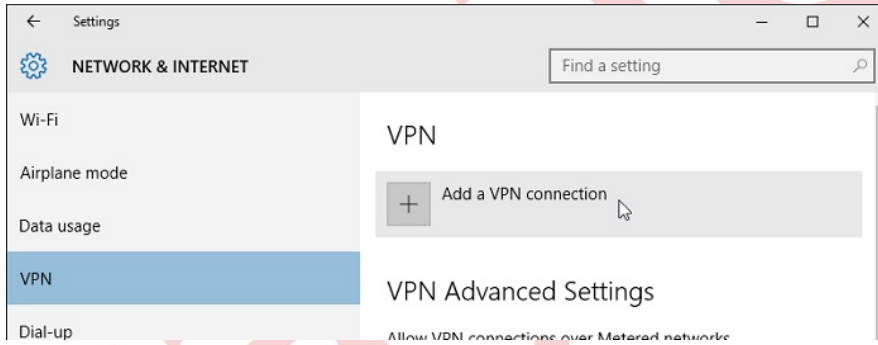
NAT-T Port : 4500

IPsec MSS : 1360

Security Method :  DES  3DES  AES

## Windows 10'dan VPN Kurma

1. Windows PC'de **Ayarlar >> Ağ & İnternet >> VPN'e** gidin. **VPN bağlantısı ekle'**ye tıklayın.



2. Server adı veya adresinde routerın WAN IP adresini ya da domain adını girin. "L2TP/IPsec with pre-shared key" olarak VPN türünü seçin. **IPsec General Setup** 'da ayarlanan Pre-shared anahtarını girin.

Add a VPN connection

VPN provider

Windows (built-in)

Connection name

Vigor Router

Server name or address

36.

VPN type

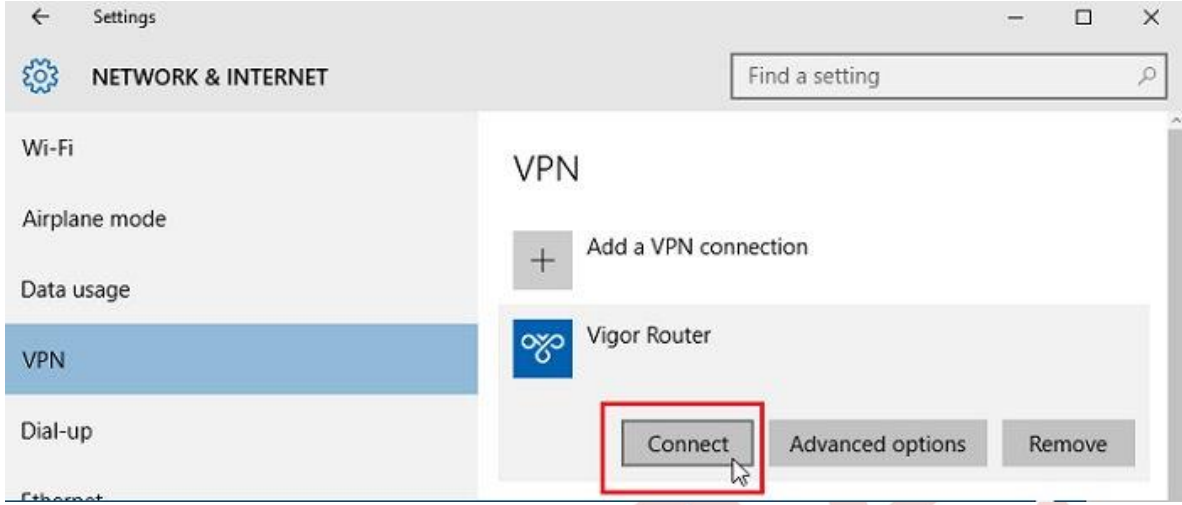
L2TP/IPsec with pre-shared key

Pre-shared key

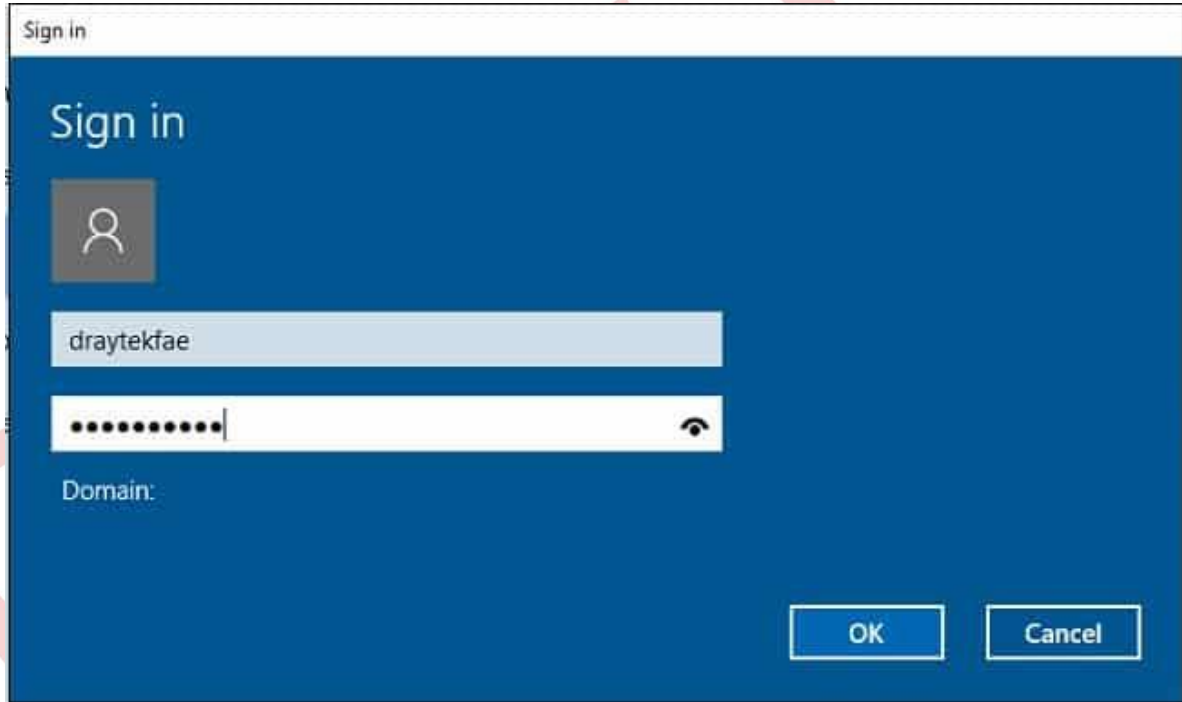
.....

Save Cancel

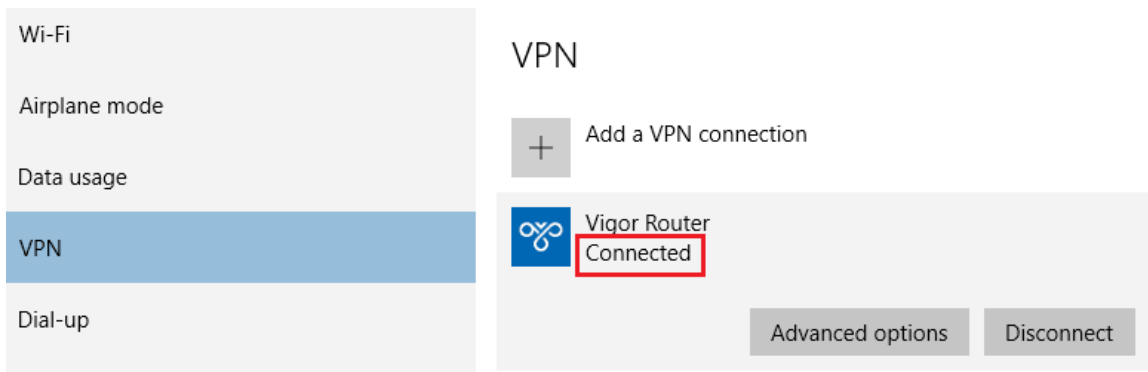
3. VPN'in kurulması için VPN bağlantısına ve ardından da **Bağlan**'at tıklayın.



4. Bir oturum açma penceresi açılacak routerın VPN kullanıcı profilinde ayarlanan **Username** ve **Password**'ü giriniz.



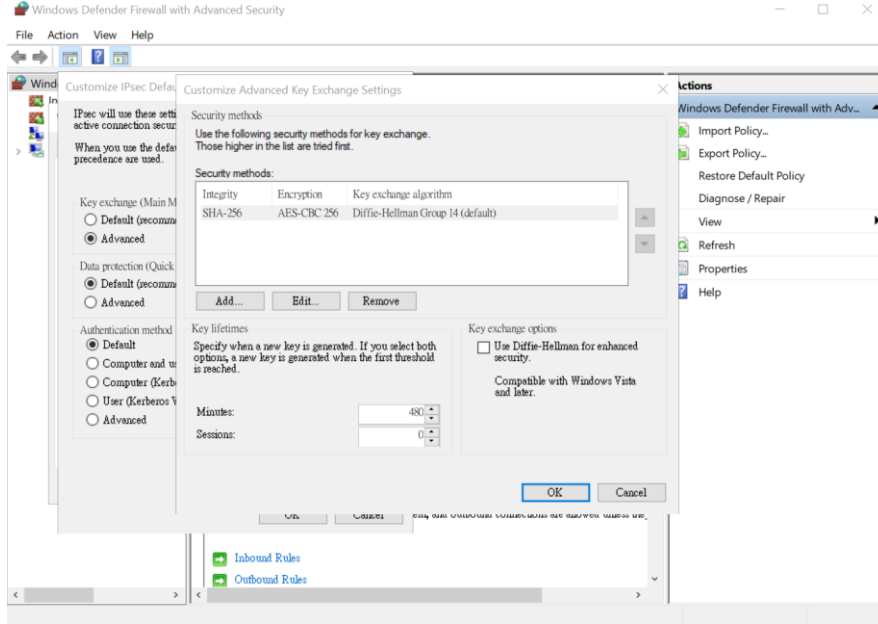
5. Kimlik bilgileri doğruysa VPN bağlanacaktır.





Not: Daha yüksek güvenlik için varsayılan IPsec Key Exchange algoritmalarının değiştirilmesi önerilir.

IPsec Key Exchange (IPsec Anahtar Değişimi), gelişmiş güvenlik özelliklerine sahip Windows güvenlik duvarında yapılandırılabilir -> (sağ panel) Özellikler -> IPsec Ayarları -> IPsec varsayılanlarını değiştirme -> Anahtar değişimi(gelişmiş)



## Sorun Giderme

VPN bağlantısı kurulamazsa kimlik doğrulamayla denemek için daha fazla protokol etkinleştirebilirsiniz. Denetim Masası > Ağ ve İnternet > Ağ Bağlantılarına gidin. VPN ile Vigor Router arasındaki bağlantıya sağ tıklayın ve ardından Özelliklere tıklayın. Güvenlik sekmesinde kimlik doğrulama için hem "PAP" hem de "CHAP" etkinleştirin ve uygulamak için Tamam'a tıklayın.

