

macOS'TAN VIGOR ROUTER'A IPsec ÜZERİNDEN L2TP

Bu makale Vigor Router'da IPsec VPN üzerinden L2TP'nin bir VPN server olarak nasıl ayarlanacağını ve macOS'dan VPN'nin nasıl başlatılacağını göstermektedir.

Vigor Router'da Kurulum

DrayOs

1. Routerın internete bağlandığından emin olun. Routerın WAN IP ya da domain adını unutmayın.
2. "Enable IPsec VPN Service" ve "Enable L2TP VPN Service"nin işaretli olup olmadığını kontrol etmek 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. **VPN and Remote Access >> IPsec General Setup** sayfasına gidin ve **Pre-Shared Key** girin. Ardından **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.	

4. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. Yeni bir hesap oluşturmak için uygun olan index numarasına tıklayın.
 - "Enable this account"u etkinleştirin.
 - **Allowed Dialin Type** sekmesinde "L2TP with IPsec"i etkinleştirin ve IPsec **Policy** için "Must" seçin.
 - **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

Specify Remote Node

Remote Client IP: _____

or Peer ID: _____

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Subnet

LAN 1

Assign Static IP Address

0.0.0.0

Username: demo

Password(Max 19 char):

Enable Mobile One-Time Passwords(mOTP)

PIN Code: _____

Secret: _____

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: _____

Digital Signature(X.509)

None

IPsec Security Method

Medium(AH)

High(ESP): DES 3DES AES

Local ID (optional): _____

OK Clear Cancel

5. VPN kullanıcısı çevrim içi ise **VPN and Remote Access >> Connection Management** sayfasında VPN bağlantı durumunu görebilirsiniz.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds: 10 Refresh

General Mode: _____ Dial

Backup Mode: _____ Dial

Load Balance Mode: _____ Dial

VPN Connection Status

Current Page: 1 Page No. _____ Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1 (demo) Local User Database	L2TP AES-SHA1 Auth	192.168.197.10 via WAN1	192.168.1.12/32	0	0	13	173	0:0:3 Drop

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

Linux

- User Management >> User Profile**'e gidin. Aşağıdaki gibi bir profil ekleyin.
 - Username girin.
 - Enable'yi etkinleştirin.
 - Password girin.
 - L2TP Dial-in için "Enable" seçeneğini seçin.
 - Apply'a tıklayın.

User Profile

Username : demo

Enable

Password : Strength : Normal

System User : false

PPTP/L2TP/SSL/PPPoE Server General Setup

Idle Timeout(sec) : 300

DHCP from : lan1

Static IP Address : (Optional)

^ User Management

v PPTP/L2TP/SSL Server

PPTP Dial-in : Enable Disable

L2TP Dial-in : Enable Disable

SSL Tunnel : Enable Disable

Use mOTP : Enable Disable

SSL Proxy : [] [X]

SSL Application(VNC) : [] [X]

SSL Application(RDP) : [] [X]

Remote IP/Host Name : (Optional)

Apply Cancel

2. VPN and Remote Access >> Remote Access Control sayfasına gidin.

- Enable L2TP VPN Service ‘in işaretli olduğundan emin olun.
- IPsec Remote Dial—In Service için “L2TP over IPsec” seçeneğini seçin.
- Apply’ya tıklayın.

VPN and Remote Access >> Remote Access Control

Remote Access Control

Enable PPTP VPN Service

Enable L2TP VPN Service

Enable SSL Tunnel Service (To use SSL Tunnel Service, please ensure HTTPS Allow is set as Enable via System Maintenance >>Access Control.)

Enable IPsec Service

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

3. VPN and Remote Access >> IPsec General Setup sayfasına gidin. Pre-Shared Key girin ardından Apply’ya tıklayın.

VPN and Remote Access >> IPsec General Setup

IPsec General Setup

Preshared Key :

WAN Profile : wan1 [X]

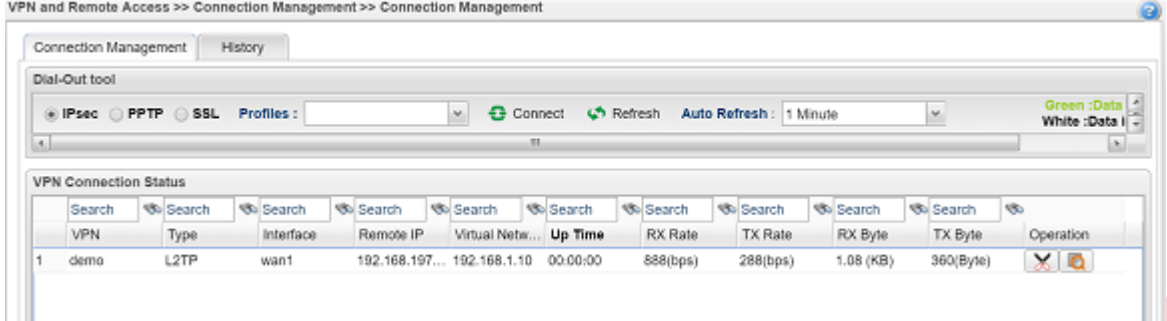
DHCP LAN Profile : lan1

IKE Port : 500

NAT-T Port : 4500

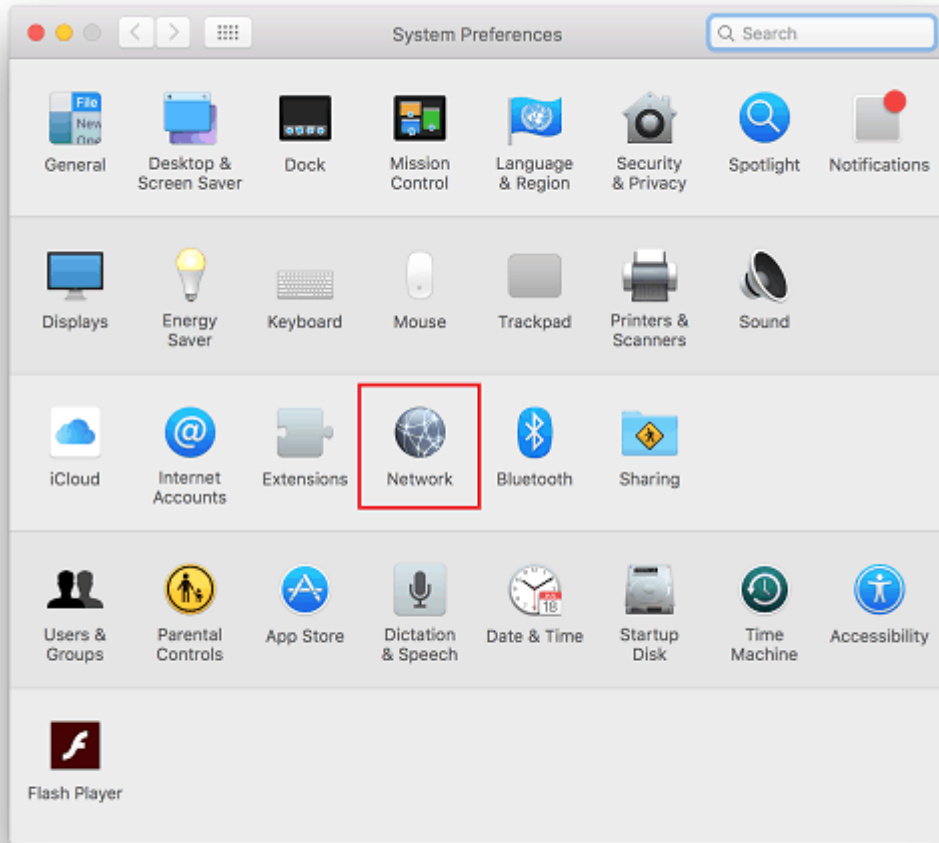
IPsec MSS : 1360

4. VPN kullanıcısı çevrim içi ise VPN bağlantı durumunu **VPN and Remote Access >> Connection Management** sayfasından görebilirsiniz.

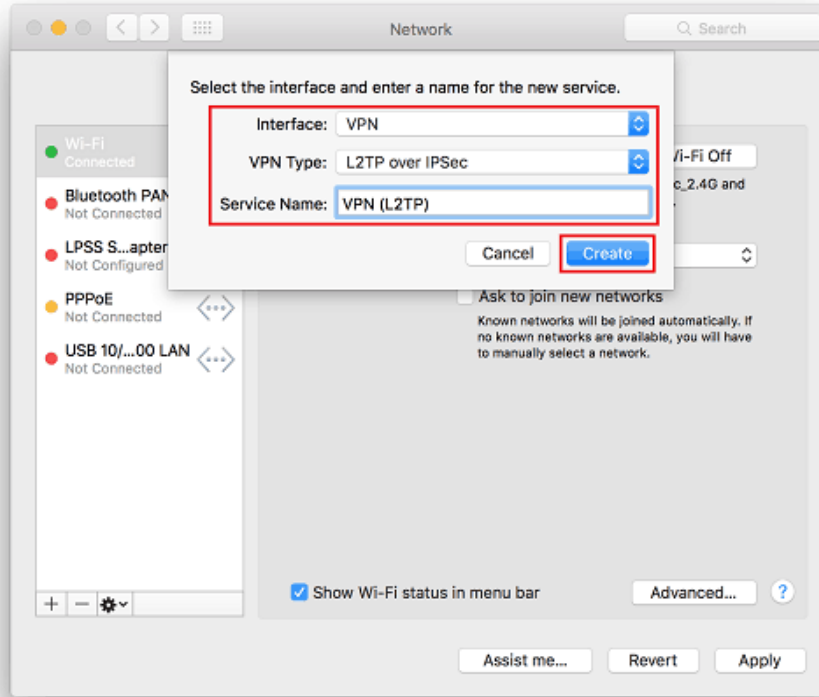


macOS'tan VPN Bağlantısı

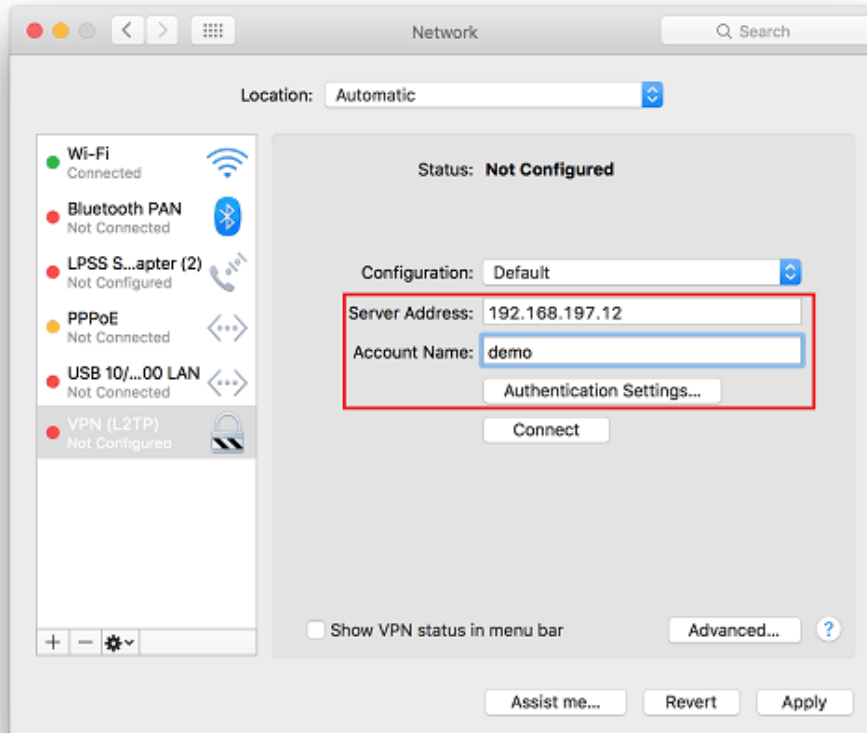
1. **System Preferences >> Network**'e gidin.



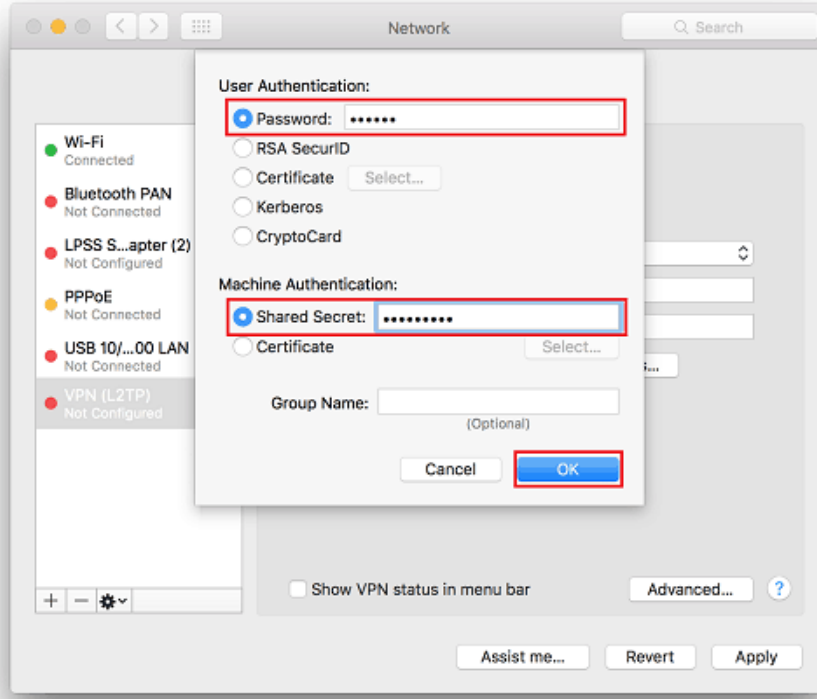
2. Yeni bir ağ eklemek için '+'ya tıklayın ve profili aşağıdaki gibi ayarlayın.
- **Interface** için VPN seçeneğini seçin
 - **VPN Type** için "L2TP over IPsec" seçeneğini seçin.
 - **Service Name** için bir servis adı girin.
 - **Create**'e tıklayın.



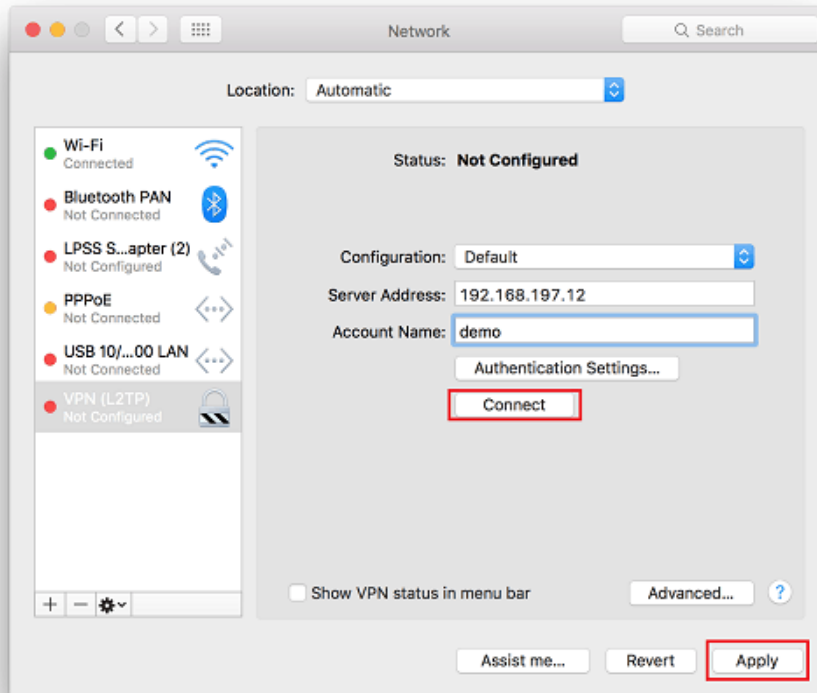
3. Routerin WAN IP'si olarak **Server Address** (Sunucunun IP adresi) ve kullanıcı profilinde kullanıcı adı olarak **Account Name** (hesap adı) girin. Ardından **Authentication Settings**'e tıklayın.



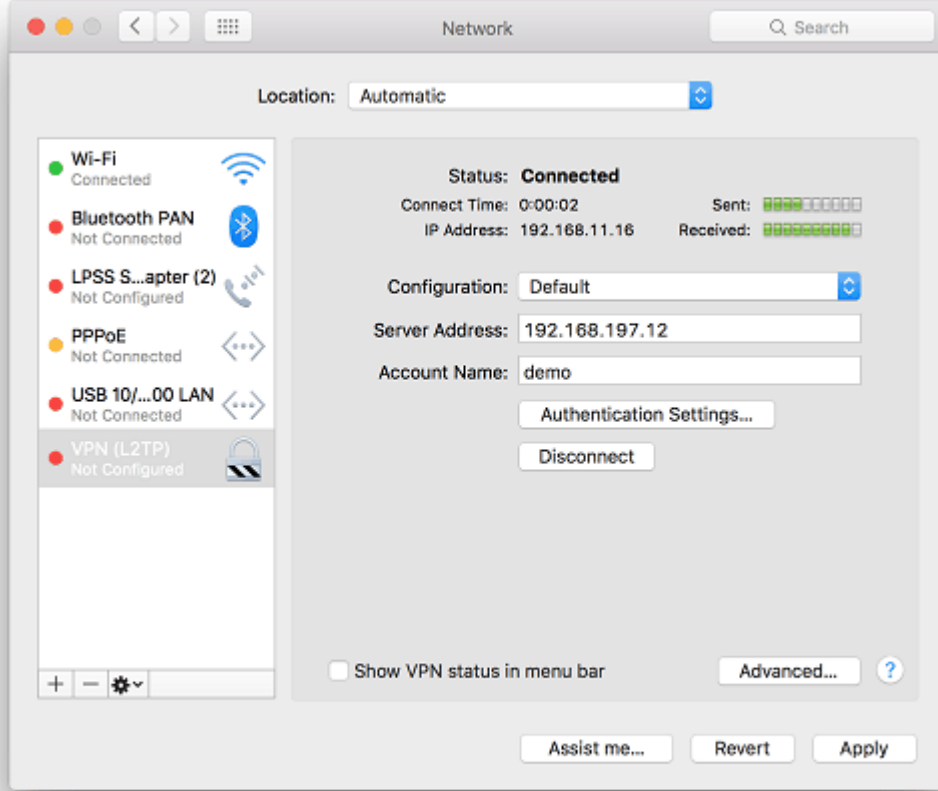
4. **User Authentication** için “Password” seçin ve kullanıcı profiline şifreyi girin. **Machine Authentication** için “Shared Secret” seçin ve routerın IPsec General Setup sayfasında ayarladığınız pre-shared key’i girin.



5. **Apply**'a, ardından da **Connect**'e tıklayın. Ve bağlantının kurulması için biraz bekleyin.



6. **Statusa** aşağıdaki görseldeki gibiyse VPN sunucusuna başarılı bir şekilde bağlanmışsınızdır.



Uzak ağdaki Local IP'ye ping yaparak bağlantıyı doğrulamak için Terminal'i kullanabiliriz.

```
mis — ping 192.168.11.1 — 80x24
Last login: Mon Jun 20 13:47:08 on ttys000
MISde-MacBook:~ mis$ ping 192.168.11.1
PING 192.168.11.1 (192.168.11.1): 56 data bytes
64 bytes from 192.168.11.1: icmp_seq=0 ttl=255 time=11.985 ms
64 bytes from 192.168.11.1: icmp_seq=1 ttl=255 time=5.593 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=255 time=1.950 ms
64 bytes from 192.168.11.1: icmp_seq=3 ttl=255 time=5.012 ms
64 bytes from 192.168.11.1: icmp_seq=4 ttl=255 time=6.168 ms
64 bytes from 192.168.11.1: icmp_seq=5 ttl=255 time=5.207 ms
64 bytes from 192.168.11.1: icmp_seq=6 ttl=255 time=1.656 ms
64 bytes from 192.168.11.1: icmp_seq=7 ttl=255 time=4.669 ms
64 bytes from 192.168.11.1: icmp_seq=8 ttl=255 time=4.594 ms
64 bytes from 192.168.11.1: icmp_seq=9 ttl=255 time=3.860 ms
```