

# VPN Uygulaması

## 1.IPSEC

### 1. IPSEC (Internet Protocol Security) Nedir?

Dođru bilginin dođru zamanda dođru kiřinin eline geçmesi bugün olduđu gibi yüz yıllar önce de oldukça önemli bir konuydu. Yüzyıllar önce Kriptex adı verilen ve rivayete göre Leonardo Da Vinci tarafından icat edilen bir Mekanizma kullanılıyordu. İletilmesi istenen gizli bilgi papirüs kađıdına yazılarak/çizilerek bu mekanik cihazın içindeki sirke dolu cama sarılıyordu, cam da bu mekanik aksamın içine yerleştiriliyordu, eđer şifreyi biliyor iseniz mekanizmayı açabiliyordunuz; yok eđer zor kullanarak mekanizmayı açmaya çalışır iseniz Kriptex içerisindeki Cam kırılıyor ve içindeki sirke Papirüs kađıdına dökülüyor böylece belgedeki gizli bilgi siz okuyamadan siliniyordu.

Günümüzde ise TCP/IP protokolündeki bilgilerini şifreleme güvenlik hizmeti kullanılarak daha güvenli ve özel haberleşme sağlanması için IPSEC kullanılır. IPsec veriyi, şifreleyen/kriptolayan (encryption), bütünlüğünü sağlayan (integrity) , kimlik dođrulaması (authentication) ve verinin network üzerinde güvenli iletimini (Secure transmission) sağlayan bir standarttır.

#### 1.1. Four Faith Routerlarda IPSEC Nasıl Uygulanır?

Router "WEB ARAYÜZÜ" 'ne girerek "VPN" menüsü altında "IPSEC" seçeneğine tıklıyoruz. Ardından "Bađlantı Durumu ve Kontrolü" kısmında "Ekle" tuşuna basarak IPSEC bađlantımızı kurmaya başlıyoruz.

**Menü**

- Genel Ayarlar
- Kablosuz
- Servis
- VPN**
  - PPTP
  - L2TP
  - OPENVPN
  - IPSEC**
  - SSE
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

**Genel Ayarlar**

Genel Ayarlar

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi: Hıçbiri

IPSEC OVER L2TP:  Etkinleştir  Devre Dışı bırak

[Kaydet](#)

**Bağlantı Durumu ve Kontrolü**

Bağlantı Durumu ve Kontrolü

Num	Adı	Tipi	Genel Adı	Durum	Eylem
<a href="#">Ekle</a>					

**Sertifika Yönetimi**

Sertifika Yönetimi

CA Adı	Referans Sayısı	Eylem
<a href="#">Ekle</a>		

**Yardım**

**NAT-Geçiş**  
NAT geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

**Log-Level**  
Hata ayıklamayı etkinleştirin yada devre dışı bırakın

**Bağlantı Durumu**  
15 bağlantı oluşturulabilir

## Şekil 1.IPSEC Aktifleştirme

Daha s  
doldur

**Menü**

- [Genel Ayarlar](#)
- [Kablosuz Servis](#)
- VPN**
  - [PPTP](#)
  - [L2TP](#)
  - [OPENVPN](#)
  - [IPSEC](#)
  - [GRE](#)
- [Güvenlik](#)
- [Erişim Kısıtlamaları](#)
- [NAT](#)
- [OoS Ayarları](#)
- [Uygulamalar](#)
- [Sistem Yönetimi](#)
- [Durum](#)

**Tipi**

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rol:  İstemci  Sunucu

**Bağlantı**

Bağlantı

Adı	<input type="text"/>	Etkin	<input checked="" type="checkbox"/>
Yerel WAN Arayüzü	WAN	Uzak WAN adresi	<input type="text"/>
Yerel Alt Ağ	<input type="text"/>	Uzak Alt Ağ	<input type="text"/>
Yerel ID	<input type="text"/>	Uzak ID	<input type="text"/>

**Alglama**

DPD Algılamayı Etkinleştir

Zaman Aralığı: 60 (Sn) Zaman aşımı: 60 (Sn) Eylem: restart

**Gelişmiş Ayarlar**

Gelişmiş ayarları etkinleştir

**Phase 1**

IKE Şifreleme: AES (256 bit) IKE Doğrulama: MD5 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 0 Saat

**Phase 2**

ESP Şifreleme: AES (256 bit) ESP Doğrulama: SHA2 (512) ESP Grup tipi: NULL

ESP Şifre Zamanı: 0 Saat

**Enable IKEv2**

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletilir)

Perfect Forward Secrecy (PFS)

**Doğrulama**

Doğrulama

Paylaşılan Şifreyi kullanın:

X.509 sertifikası oluşturun ve kullanın

**Yardım** [Gözetim](#)

**Not**

sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

**Tipi**

IPsec tipini seçin, tünel ya da transport

**Rol**

IPsec rolünü seçin, istemci ya da sunucu

**Bağlantının Adı**

IPsec bağlantı adı 20 karaktere kadar olmalıdır

**Yerel ve Uzak Ağ için ID**

Yerel ve uzak ağ ID tanımlamak için IP adresi veya bağında @ işaretini ekleyerek domain adı girilebilir

**PSK Değeri**

PSK değerinin uzunluğu 30'dan fazla olamaz

**IKEv2**

undefined

Şekil 2. IPSEC Bağlantı Ayarları

Bu özellikleri tam olarak anladıktan sonra aşağıdaki resimlerde IPSEC uygulamasını yap

Kay

Menu

- Genel Ayarlar
- Kablosuz Servis
- VPN
  - PP2P
  - L2IP
  - OPENVPN
  - IPSEC
  - GRE
- Güvenlik
- Fiziksel Kısıtlamalar
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Yeni

Tipi

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rol:  İstemci  Sunucu

Bağlantı

Adı: ZTtest Etkin:

Yerel WAN Arayüzü: WAN Uzak WAN adresi: 81.6.111.88

Yerel Alt Ağ: 192.168.1.0/24 Uzak Alt Ağ: 192.168.1.0/24

Yerel ID: @rt2 Uzak ID: @rt1

Algilama

DPD Algılamayı Etkinleştir:

Zaman Aralığı: 60 (Sn) Zaman aşımı: 180 (Sn) Eylem: restart

Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir:

Phase 1

IKE Şifreleme: 3DES IKE Doğrulama: SHA1 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 24 Saat

Phase 2

ESP Şifreleme: 3DES ESP Doğrulama: SHA1 ESP Grup tipi: NULL

ESP Şifre Zamanı: 24 Saat

Enable IKEv2:

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak letir!)

Perfect Forward Secrecy (PFS)

Doğrulama

Doğrulama

Paylaşılan Şifreyi kullanın: 123456

X.509 sertifikası oluşturun ve kullanın

Not: sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

Tipi: IPsec tipini seçin, tünel ya da transport

Rol: IPsec rolünü seçin, istemci ya da sunucu

Bağlantının Adı: IPsec bağlantı adı 20 karaktere kadar olmalıdır

Yerel ve Uzak Ağ için ID: Yerel ve uzak ağ ID tanımlamak için IP adresi veya bağında @ şareti ekleyerek domain adı girilebilir

PSK Değeri: PSK değerinin uzunluğu 30'dan fazla olamaz

IKEv2: undefined

### Şekil 3.IPSEC İstemci (Client)

Daha sonra sunucu (server) tarafı ayarlarını yaptıktan sonra aynı şekilde “Ayarları Kaydet” ’i tıklıyoruz.

## Genel Ayarlar

### Kablosuz

### Servis

### VPN

- o PPTP
- o L2TP
- o OPENVPN
- o IPSEC
- o GRE

### Güvenlik

### Erişim Kısıtlamaları

### NAI

### QoS Ayarları

### Uyulamalar

### Sistem Yönetimi

### Durum

#### Tipi

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rolü:  İstemci  Sunucu

#### Bağlantı

Bağlantı

Adı: Zttest Etkin:

Yerel WAN Arayüzü: WAN Uzak WAN adresi:

Yerel Alt Ağ: 192.168.1.0/24 Uzak Alt Ağ: 192.168.1.0/24

Yerel ID: @zt1 Uzak ID: @zt2

#### Alglama

DPD Algılamayı Etkinleştir

Zaman Aralığı: 60 (Sn) Zaman aşımı: 180 (Sn) Eylem: restart

#### Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir

**Phase 1**

IKE Şifreleme: 3DES IKE Doğrulama: SHA1 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 24 Saat

**Phase 2**

ESP Şifreleme: 3DES ESP Doğrulama: SHA1 ESP Grup tipi: NULL

ESP Şifre Zamanı: 24 Saat

Enable IKEv2:

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletir!)

Perfect Forward Secrecy (PFS)

#### Doğrulama

Doğrulama

Paylaşılan Şifreyi kullanın: 123456

X.509 sertifikası oluşturun ve kullanın

#### Not

sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

#### Tipi

IPsec tipini seçin, tünel ya da transport

#### Rol

IPsec rolünü seçin, istemci ya da sunucu

#### Bağlantının Adı

IPsec bağlantı adı 20 karaktere kadar olmalıdır

#### Yerel ve Uzak Ağ için ID

Yerel ve uzak ağ ID tanımlamak için IP adresi veya başında @ işareti ekleyerek domain adı girilebilir

#### PSK Değeri

PSK değerinin uzunluğu 30'dan fazla olmaz

#### IKEv2

undefined

## Şekil 4. IPSEC Sunucu (SERVER)

Daha sonra router'ları yeniden başlatıyoruz ve ayarların yapıldığı sekmeden bağlantı durumunu gözlemleyebiliyoruz.

**Menü**

[Genel Ayarlar](#)

[Kablosuz Servis](#)

**VPN**

- [PPoP](#)
- [L2TP](#)
- [OPENVPN](#)
- [IPSEC](#)
- [GRE](#)

[Güvenlik Erişim Kısıtlamaları](#)

[NAT](#)

[QoS Ayarları](#)

[Uygulamalar](#)

[Sistem Yönetimi](#)

[Durum](#)

**Genel Ayarlar**

Genel Ayarlar

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi: Hiçbiri

IPSEC OVER L2TP:  Etkinleştir  Devre Dışı bırak

[Kaydet](#)

---

**Bağlantı Durumu ve Kontrolü**

Bağlantı Durumu ve Kontrolü

Num	Adı	Tipi	Genel Adı	Durum	Eylem
1	Zttest	Tünel-server	192.168.1.0/24-[WAN1] server-[192.168.1.0/24]	Erişilmiyor	<a href="#">Sil</a> <a href="#">Yeni</a> <a href="#">Yenile</a> <a href="#">Ekle</a>

---

**Sertifika Yönetimi**

Sertifika Yönetimi

CA Adı	Referans Sayısı	Eylem
<a href="#">Ekle</a>		

**Yardım**

**NAT-Geçiş**

Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

---

**Log-Level**


Hata ayıklamayı etkinleştirin ya da devre dışı bırakın

---

**Bağlantı Durumu**

15 bağlantı oluşturulabilir

Şekil



Wireless Mobile Router

2. 5G/3G/3. 5G/4G

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std  
Zaman: 00:00:41 up 0 min, load average: 0.12, 0.03, 0.01  
WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0

**Menü**

[Genel Ayarlar](#)

[Kablosuz Servis](#)

**VPN**

- [PPoP](#)
- [L2TP](#)
- [OPENVPN](#)
- [IPSEC](#)
- [GRE](#)

[Güvenlik Erişim Kısıtlamaları](#)

[NAT](#)

[QoS Ayarları](#)

[Uygulamalar](#)

[Sistem Yönetimi](#)

[Durum](#)

**Genel Ayarlar**

Genel Ayarlar

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi: Hiçbiri

IPSEC OVER L2TP:  Etkinleştir  Devre Dışı bırak

[Kaydet](#)

---

**Bağlantı Durumu ve Kontrolü**

Bağlantı Durumu ve Kontrolü

Num	Adı	Tipi	Genel Adı	Durum	Eylem
1	Zttest	Tünel-client	192.168.1.0/24-[WAN1] 81.6.111.88-[192.168.1.0/24]	Erişilmiyor	<a href="#">Sil</a> <a href="#">Yeni</a> <a href="#">Yenile</a> <a href="#">Ekle</a>

---

**Sertifika Yönetimi**

Sertifika Yönetimi

CA Adı	Referans Sayısı	Eylem
<a href="#">Ekle</a>		

**Yardım**

**NAT-Geçiş**

Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

---

**Log-Level**

Hata ayıklamayı etkinleştirin ya da devre dışı bırakın

---

**Bağlantı Durumu**

15 bağlantı oluşturulabilir

Şekil 6. IPSEC İstemci(Client) Kurulmuş Bağlantı Örneği

**NOT 1:** Bağlantı durumunu gözlemlendiğimiz sayfada “çöp kutusu” ikonu ile bağlantıyı silebilir, “kalem” ikonu ile bağlantı ayarlarını değiştirebilir “yenile” ikonu ile bağlantı denemesini baştan başlatabilirsiniz. Bu kapsamda “kalem” ve “yenileme” ikonlarını sadece ihtiyaç duyduğumuzda kullanmamız gerekir. Aksi takdirde her seferinde işlem yeniden başlayacağı için IPSEC bağlantısının yapılması önlenir.

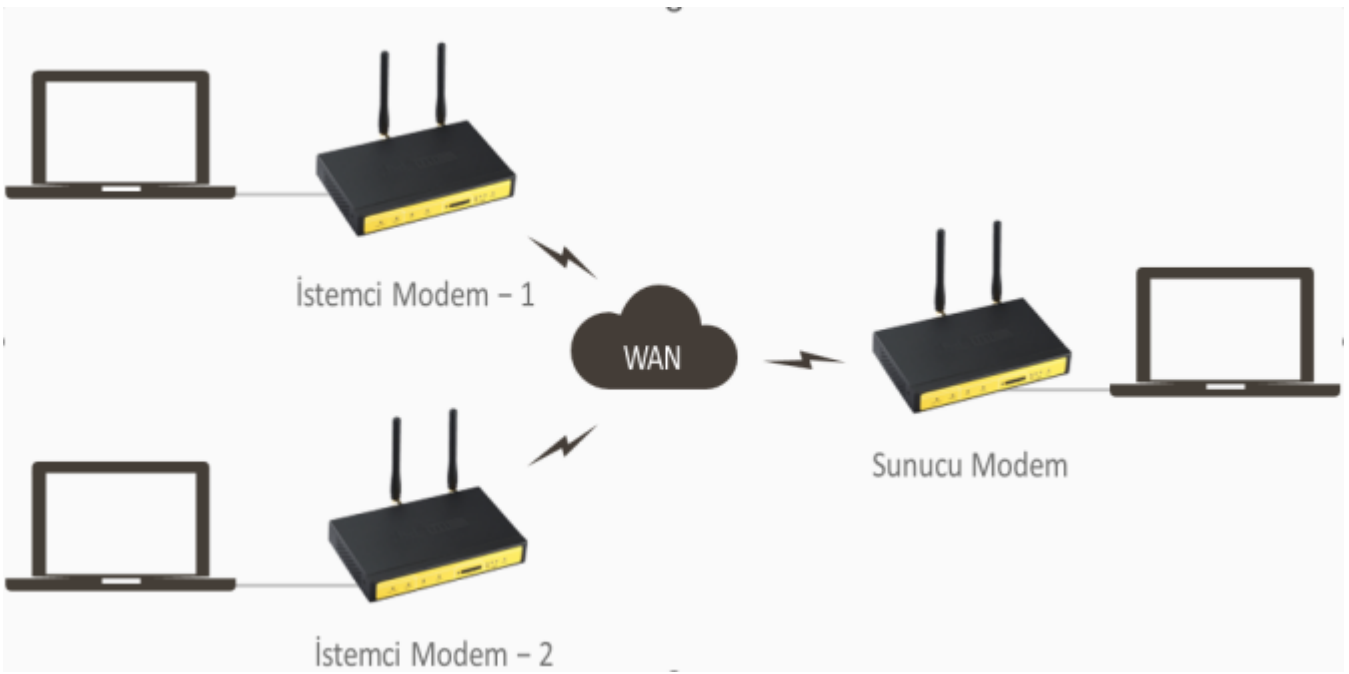
**NOT 2:** Çoğu uygulamada router modemlerin 4G’si BACKUP(yedekli) olarak kullanılmaktadır. Böyle uygulamalarda Router modemimizi internete çıkarmak için kullandığımız cihazlar(ADSL Modem, Uydunet Modem gibi) içerisinde herhangi bir değişiklik yapmadan IPSEC tüneli kullanabiliriz. Bu şekilde olan uygulamalarda sadece IPSEC tünel kurmak istediğimiz uzak Ağ’a hem 4G hem de yedek olarak kullandığımız internetin IP’sini kaydetmemiz gerekmektedir.

FF modemlerde IPsec VPN Uygulaması için örnek uygulama videosu:

## 2.OpenVPN

### 2. OpenVPN Uygulması

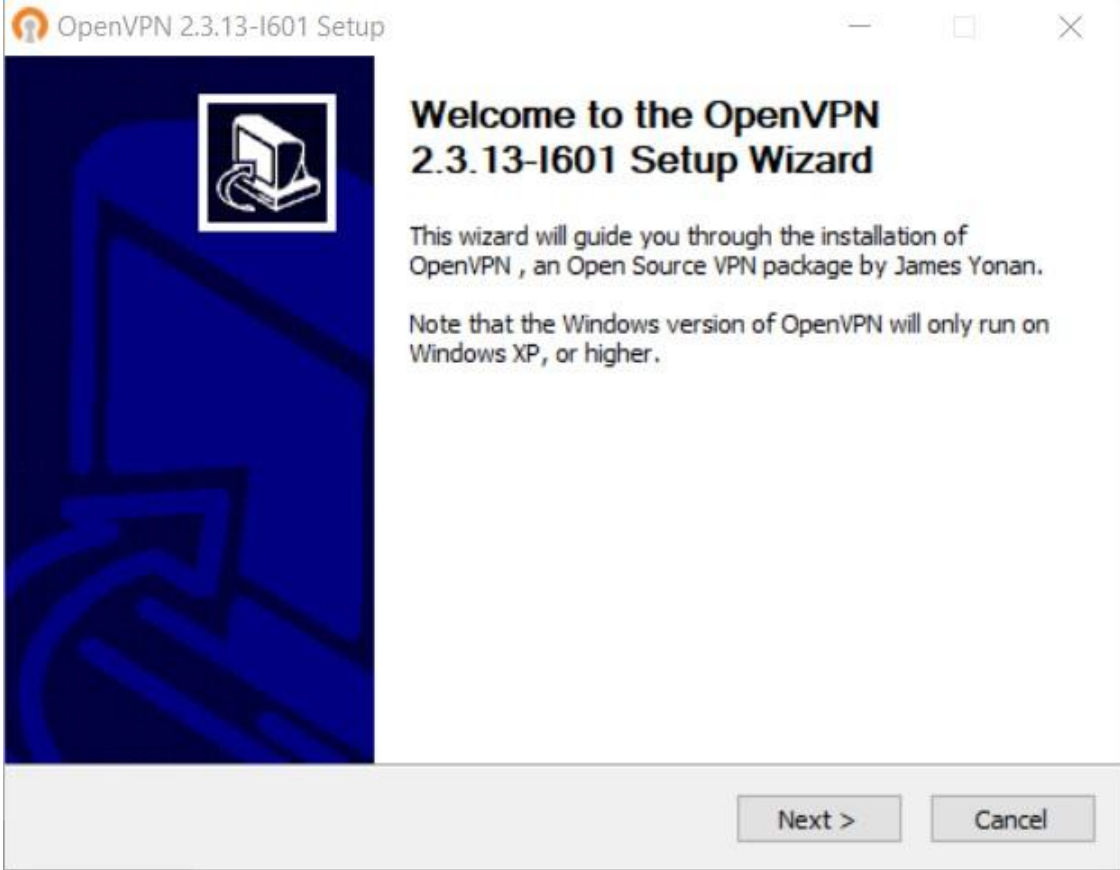
Four-Faith router modemler; PPTP, L2TP, IPSEC, GRE VPN türlerini desteklediği gibi OpenVPN’i de desteklemektedir. Kurulacak olan OpenVPN ağında bir sunucu ve birden çok istemci olmalıdır. Bu kılavuzda bir sunucu ve iki istemci olan örnek anlatılmıştır. Amaç, istemciler arasında VPN bağlantısının kurulması ve güvenli haberleşmenin sağlanmasıdır.



**Şekil 1. Open VPN Uygulama Şeması**

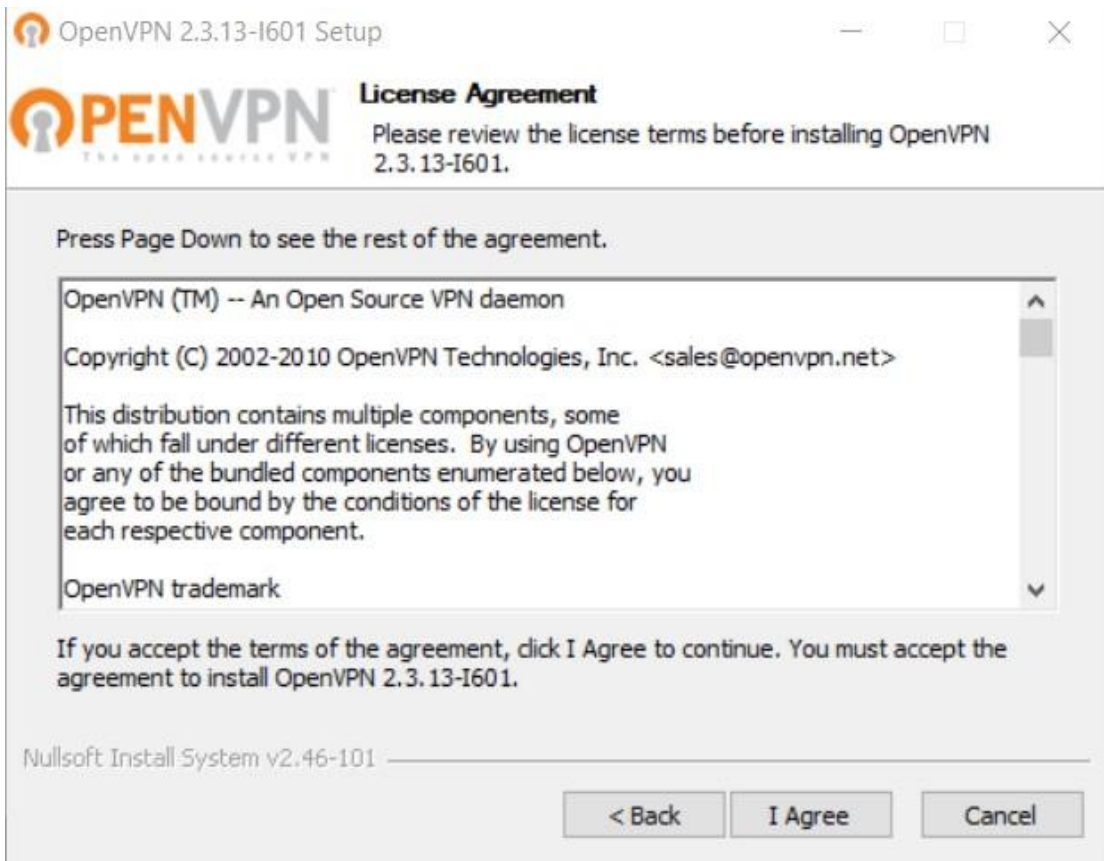
## 2.1 PC ile Modem Arasında OpenVPN Tünel Kurulumu

Öncelikli olarak OpenVPN programını PC'mize kuruyoruz. Aşağıdaki adımlar ile;

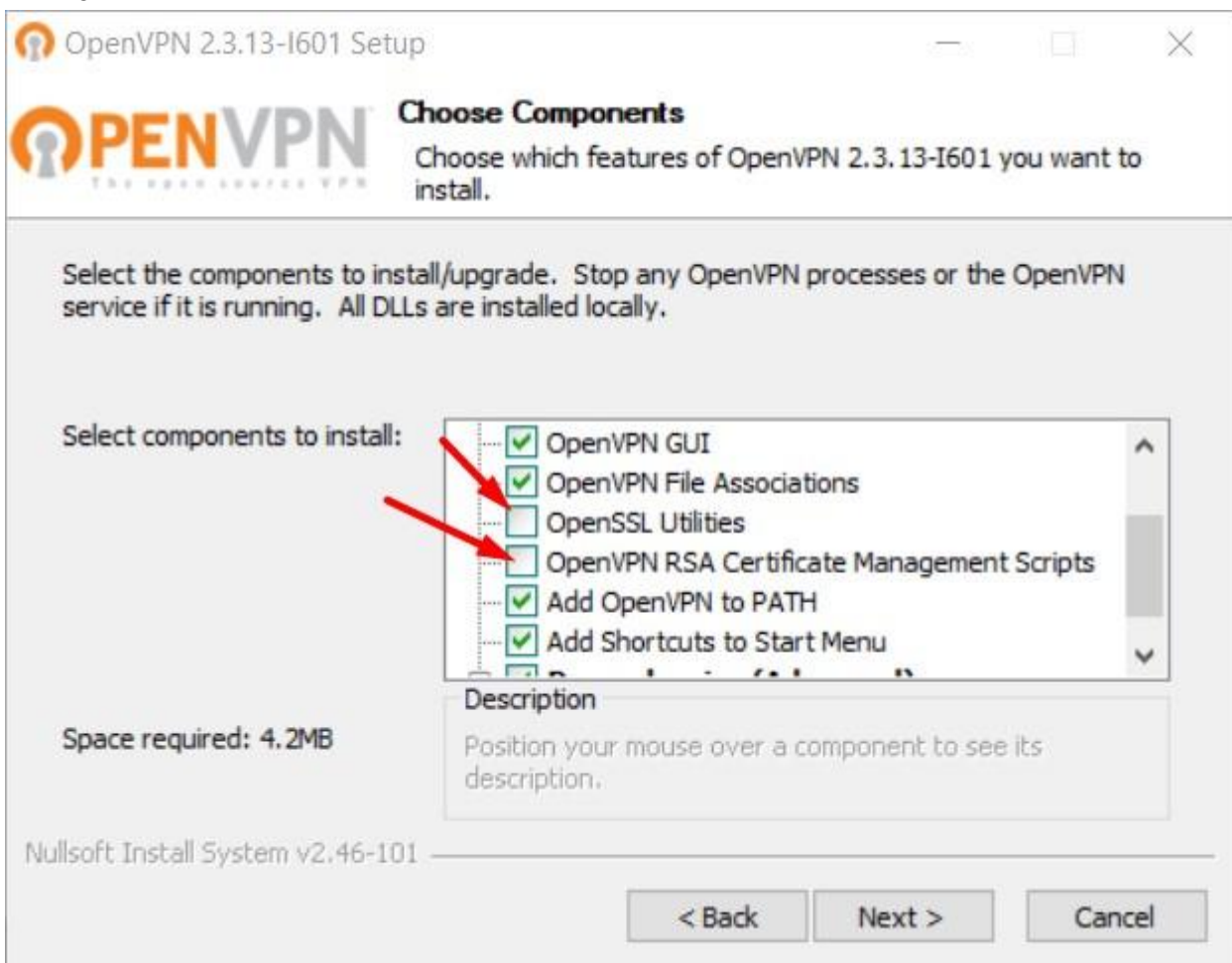


### 1. Adım



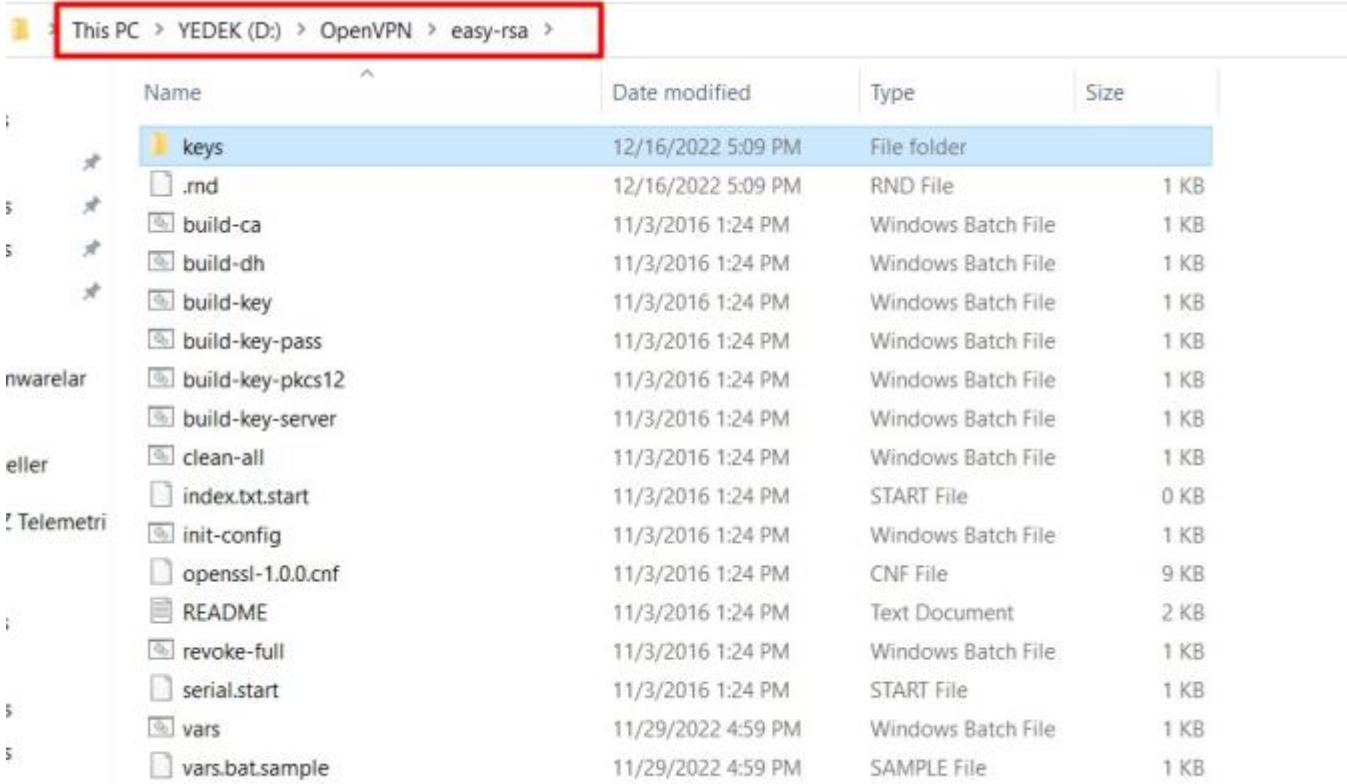


## 2. Adım



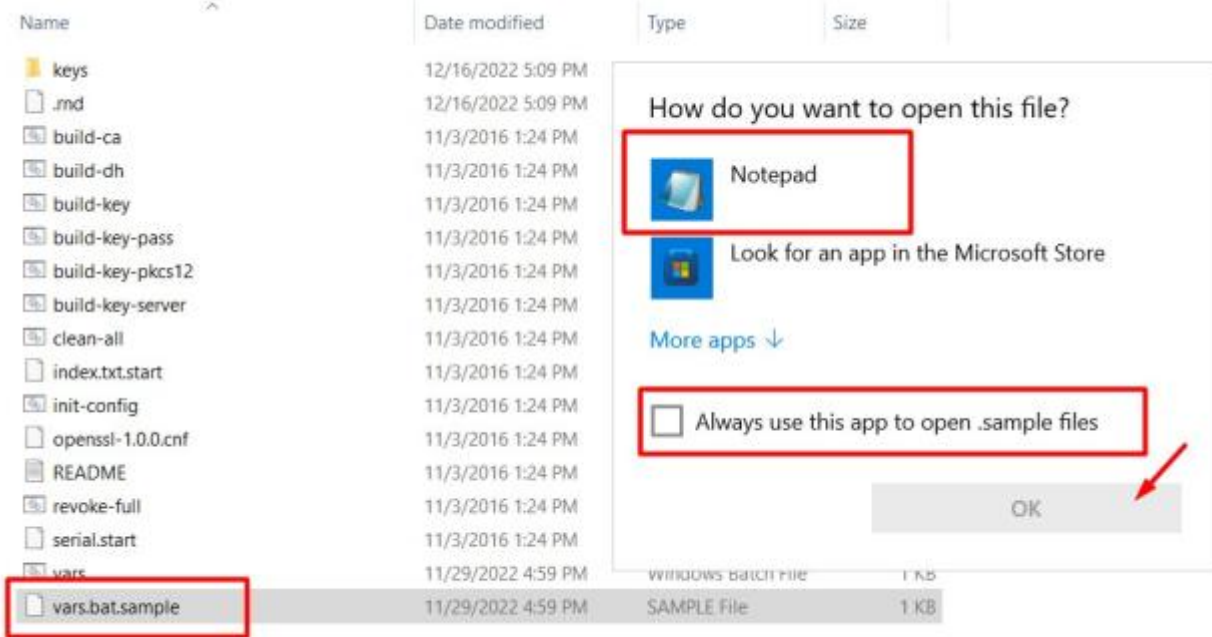
## 3. Adım

- Klasör içerisinde bulunan OpenVPN programını kurunuz. Kurulumu C:/ klasörüne yapacak kurulum dosyası içerisindeki easy-rsa klasörünü kopyalayıp D:/OpenVPN/easy-rsa uzantısı olacak şekilde kayıt edin. Aşağıda görselde olduğu gibi.



## Şekil 2. Easy-rsa Kayıt

Sırayla aşağıdaki adımları uygulayalım.



## 4. Adım Vars Bat Open

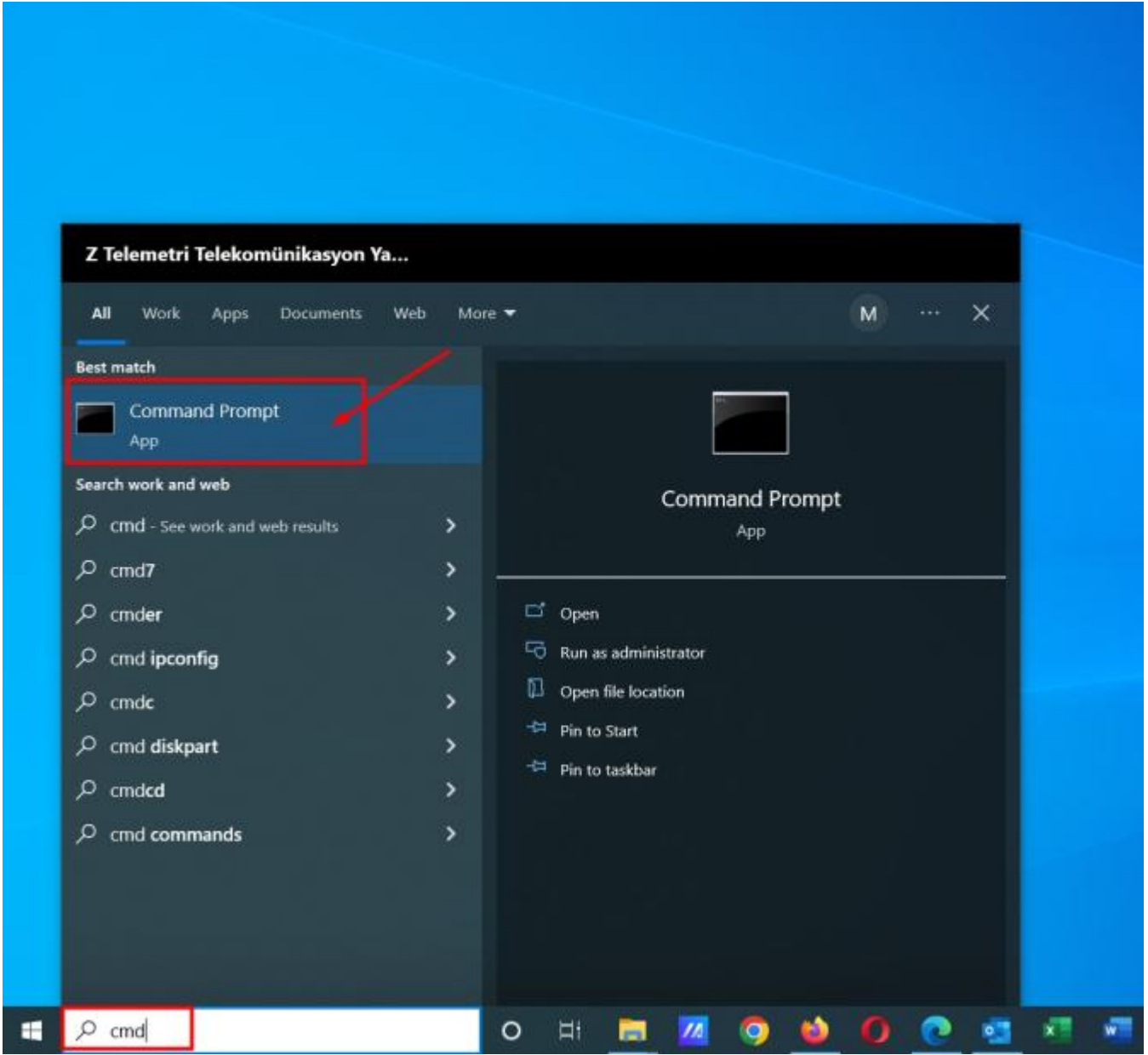
```
vars.bat.sample - Notepad
File Edit Format View Help
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.
set HOME=D:\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024
```

## 5. Adım Vars Bat Değişiklik

- PC mizde başlat menüsünden “cmd” yazarak Command Prompt açıyoruz. OpenVPN için Sertifikaları oluşturuyoruz kendimize ait aşağıdaki adımları izleyerek hepsini oluşturunuz.



## 6. Adım Cmd (Komut Sistemi) Açılması

- İlk aşamada gerekli dosyaya girerek Key klasörü oluşturuyoruz ve önceli sertifikaları temizliyoruz.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mustafa-Asus>d:

D:\>cd D:\OpenVPN\easy-rsa

D:\OpenVPN\easy-rsa>init-config

D:\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 file(s) copied.

D:\OpenVPN\easy-rsa>vars

D:\OpenVPN\easy-rsa>clean-all
1 file(s) copied.
1 file(s) copied.
```

## 7. Adım Commad 1

- **CA Cert Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.

```
Command Prompt
D:\OpenVPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:OPENVPN_CA
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com
```

## 8. Adım Command 2

- **Server Key Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.

```
Command Prompt
D:\OpenVPN\easy-rsa>build-key-server server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:SERVER
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:ZT
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'TR'
stateOrProvinceName  :PRINTABLE:'TURKEY'
localityName          :PRINTABLE:'ANKARA'
organizationName      :PRINTABLE:'ZT'
organizationalUnitName:PRINTABLE:'MUSTAFA'
commonName           :PRINTABLE:'SERVER'
name                  :PRINTABLE:'MUSTAFA'
emailAddress          :IASSTRING:'mustafa.unsal@ztelemetry.com'
Certificate is to be certified until Dec 13 14:05:10 2032 GMT (3650 days)
Sign the certificate? [y/n]:Y

1 out of 1 certificate requests certified, commit? [y/n]Y
Write out database with 1 new entries
Data Base Updated
```

## 9. Adım Command 3

- **DH Key Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.



```
Command Prompt
D:\OpenVPN\easy-rsa>build-key client
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:CLIENT
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:client_secret
An optional company name []:ZT
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'TR'
stateOrProvinceName :PRINTABLE:'TURKEY'
localityName      :PRINTABLE:'ANKARA'
organizationName  :PRINTABLE:'ZT'
organizationalUnitName:PRINTABLE:'MUSTAFA'
commonName        :PRINTABLE:'CLIENT'
name              :PRINTABLE:'MUSTAFA'
emailAddress      :IASSTRING:'mustafa.unsal@ztelemetry.com'
Certificate is to be certified until Dec 13 14:09:40 2032 GMT (3650 days)
Sign the certificate? [y/n]:Y

1 out of 1 certificate requests certified, commit? [y/n]Y
Write out database with 1 new entries
```

## 11. Adım Command 5

**NOT:** Bir modeme bağlanacak Client PC sayısı 1 den fazla ise bu işlem tekrarlanır ve client2,client3...

Oluşturduğumuz tüm sertifikalar ve keyler bu klasörde bulunur.



Name	Date modified	Type	Size
01.pem	12/16/2022 5:05 PM	PEM File	5 KB
02.pem	12/16/2022 5:09 PM	PEM File	4 KB
ca	12/16/2022 5:02 PM	Security Certificate	2 KB
ca.key	12/16/2022 5:02 PM	KEY File	1 KB
client	12/16/2022 5:09 PM	Security Certificate	4 KB
client.csr	12/16/2022 5:09 PM	CSR File	1 KB
client.key	12/16/2022 5:09 PM	KEY File	1 KB
dh1024.pem	12/16/2022 5:05 PM	PEM File	1 KB
index	12/16/2022 5:09 PM	Text Document	1 KB
index.txt.attr	12/16/2022 5:09 PM	ATTR File	1 KB
serial	12/16/2022 5:09 PM	File	1 KB
server	12/16/2022 5:05 PM	Security Certificate	5 KB
server.csr	12/16/2022 5:05 PM	CSR File	1 KB
server.key	12/16/2022 5:05 PM	KEY File	1 KB

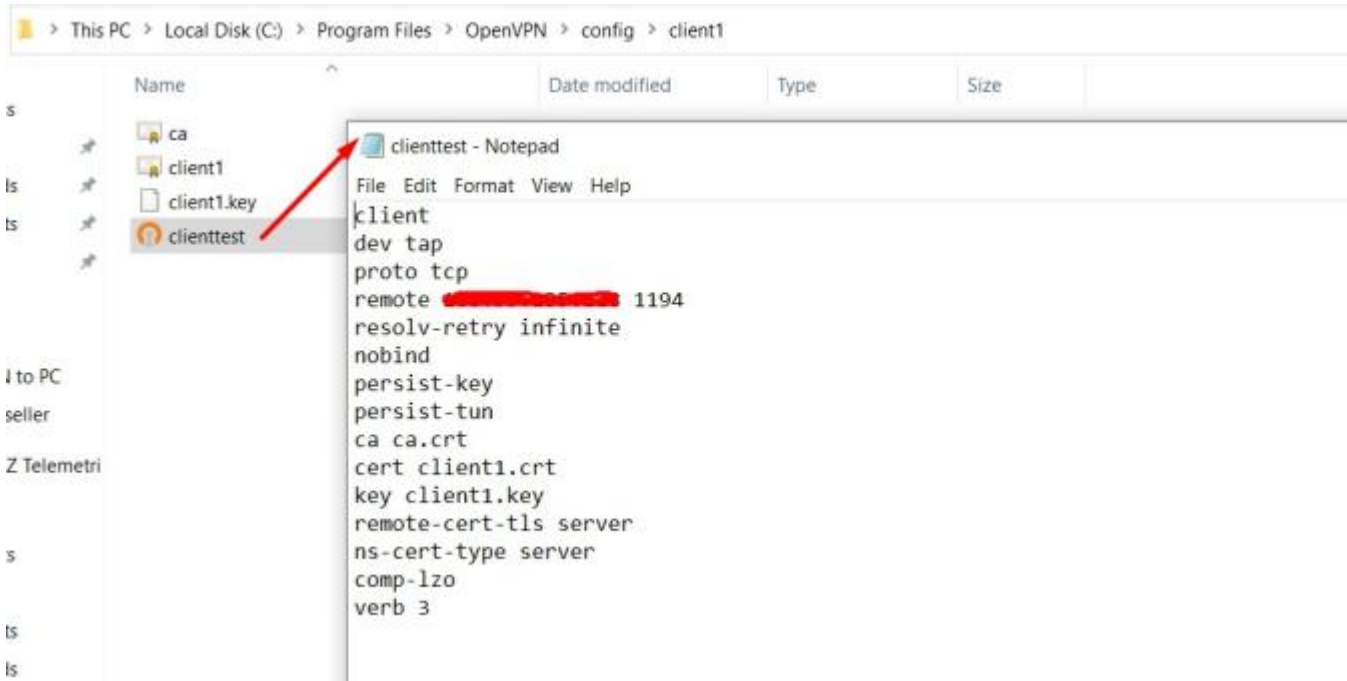
## 12. Adım Key Klasörü

- Config işlemlerini yapılandırmak için setifikalarımızı kopyalayıp aşağıdaki görselde bulunan dosya konumuna yapıştırıyoruz.

Name	Date modified	Type	Size
bin	11/29/2022 4:52 PM	File folder	
config	12/14/2022 3:58 PM	File folder	
doc	11/29/2022 4:52 PM	File folder	
easy-rsa	11/29/2022 4:52 PM	File folder	
include	11/29/2022 3:35 PM	File folder	
log	12/14/2022 4:00 PM	File folder	
res	11/29/2022 3:35 PM	File folder	
sample-config	11/29/2022 4:52 PM	File folder	
icon	9/27/2016 11:12 AM	Icon	22 KB
license	12/15/2021 8:04 AM	Text Document	28 KB
Uninstall	11/29/2022 4:52 PM	Application	117 KB

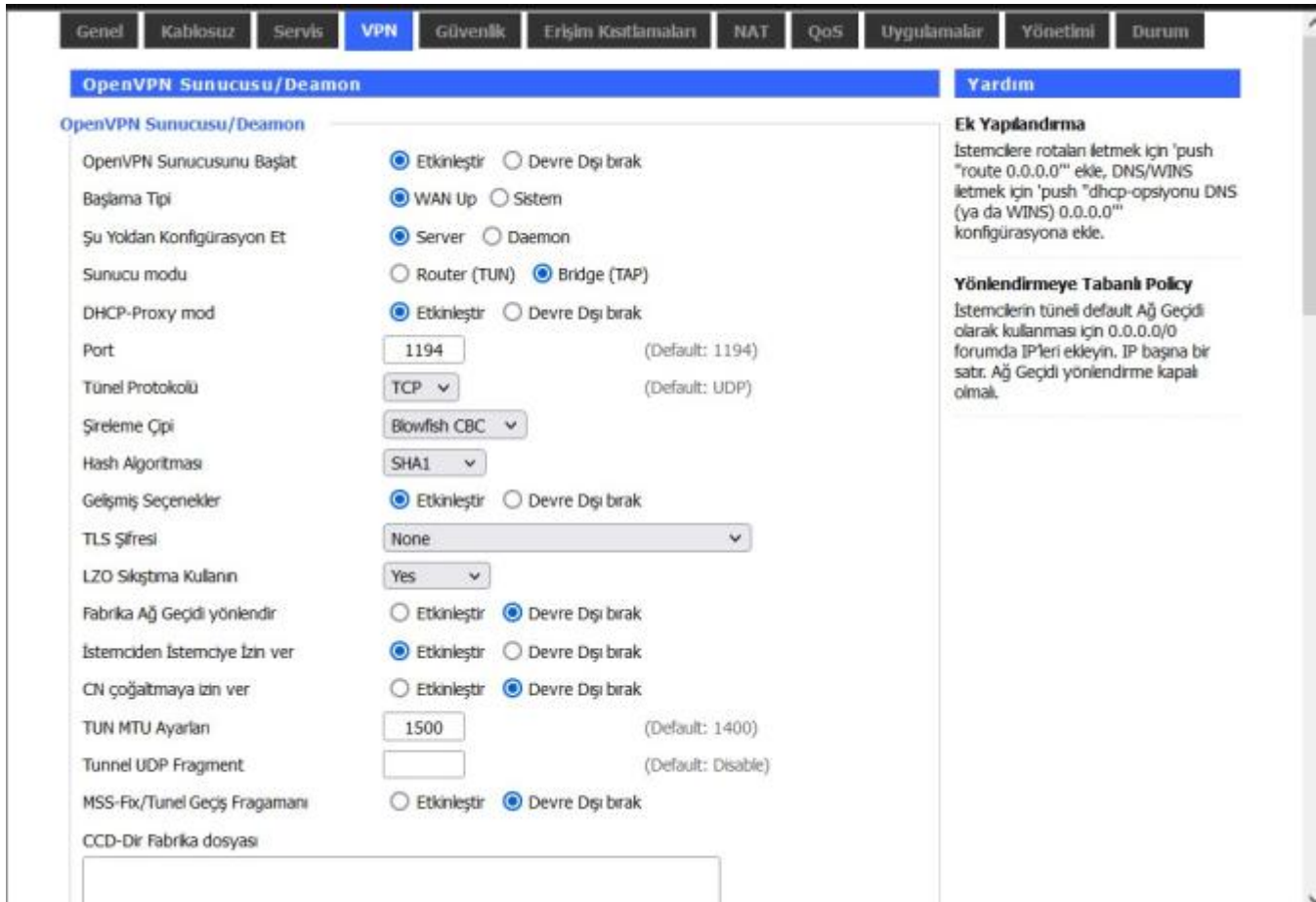
## 13. Adım Config Klasörü

- PC den modeme bağlantı için client dosyasını yapılandırıyoruz. Kırmızı çizgili kısma modeminize ait statik IP yazılmalıdır.



## 14. Adım Config Ayarı

- Modem ayarlarını yapılandırılalım. OpenVPN Server olarak yapılandırıyoruz.



## 15. Adım Modem Ayarları-1

- Sertifikaların gerekli yerlerine eklenmesi, sertifikaları eklemek için dosyaları not defteri ile birlikte açıyoruz ve kopyalayıp yapııştırıyoruz.

Empty text boxes for certificate and key uploads.

Kamu Sunucu Sertifikası

CA Sertifikası

Kişisel Sunucu Key

DH PEM

Ek Yapılandırma

TLS Doğrulama Şifresi

## 16. Adım Modem Ayarları-2

Name	Date modified	Type	Size
01.pem	12/16/2022 5:05 PM	PEM File	5 KB
02.pem	12/16/2022 5:09 PM	PEM File	4 KB
ca	12/16/2022 5:02 PM	Security Certificate	2 KB
ca.key	12/16/2022 5:02 PM	KEY File	1 KB
client	12/16/2022 5:09 PM	Security Certificate	4 KB
client.csr	12/16/2022 5:09 PM	CSR File	1 KB
client.key	12/16/2022 5:09 PM	KEY File	1 KB
dh1024.pem	12/16/2022 5:05 PM	PEM File	1 KB
index	12/16/2022 5:09 PM	Text Document	1 KB
index.txt.attr	12/16/2022 5:09 PM	ATTR File	1 KB
serial	12/16/2022 5:09 PM	File	1 KB
server	12/16/2022 5:05 PM	Security Certificate	5 KB
server.csr	12/16/2022 5:05 PM	CSR File	1 KB
server.key	12/16/2022 5:05 PM	KEY File	1 KB

3G/4G/4G+

Kamu Sunucu Sertifikası

CA Sertifikası

Kişisel Sunucu Key

DH PEM

Ek Yapılandırma

## 17. Adım Sertifika Yazma İşlemi-1

- Sertifikaların modem de yerlerine yazılmış hali.

Static Key

PKCS12 Key

Public Server Cert

```
-----BEGIN CERTIFICATE-----
MIIDxTCCAy6gAwIBAgIBATANBgkqhkiG9w0BAQFADB+MQswCQYDVQQG
```

CA Cert

```
-----BEGIN CERTIFICATE-----
MIIDYDCCAsmgAwIBAgIJAPv5J6Hlmag1MA0GC5qGS1b3DQEBBQUAMH4xC
```

Private Server Key

```
-----BEGIN PRIVATE KEY-----
MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBANLEdMb4E
```

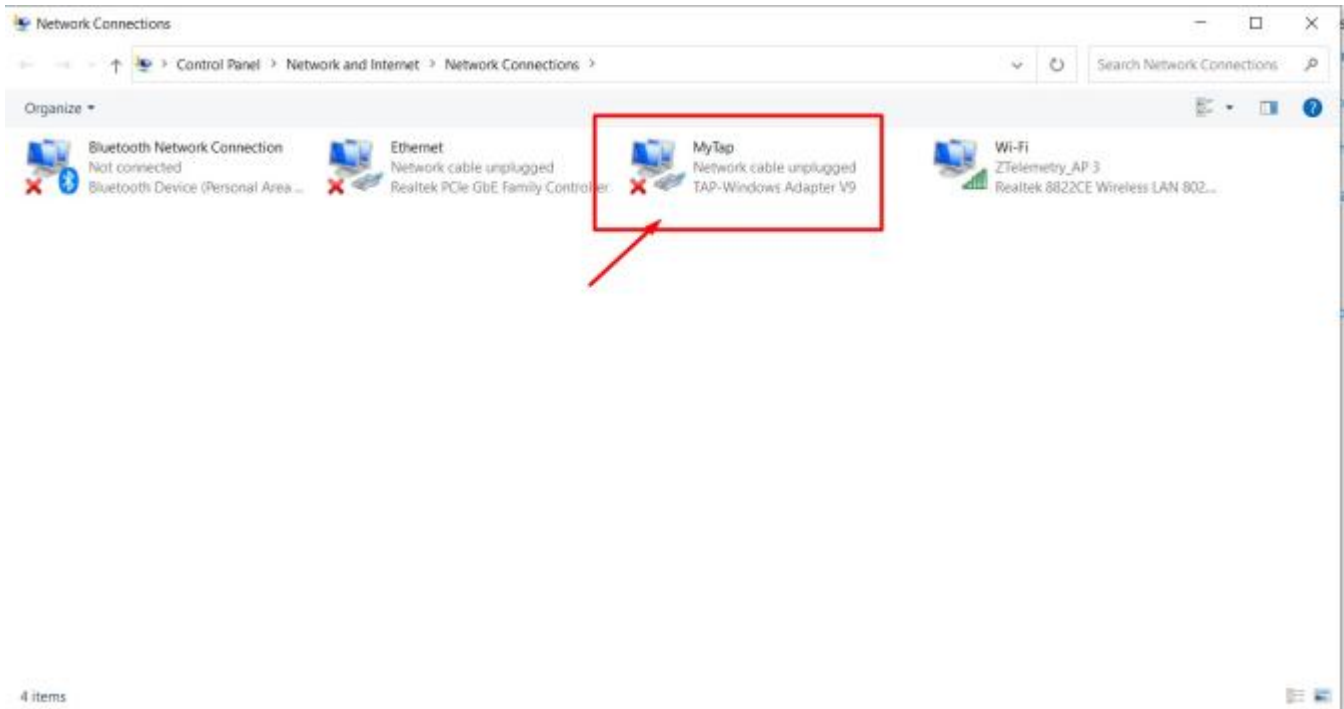
DH PEM

```
-----BEGIN DH PARAMETERS-----
MIGHAoGBAIFDVueSwx/Ruch+12Y1y0+O9H4unCYBVK+kE1B+sqP9VkwrtI0/
```

Additional Config

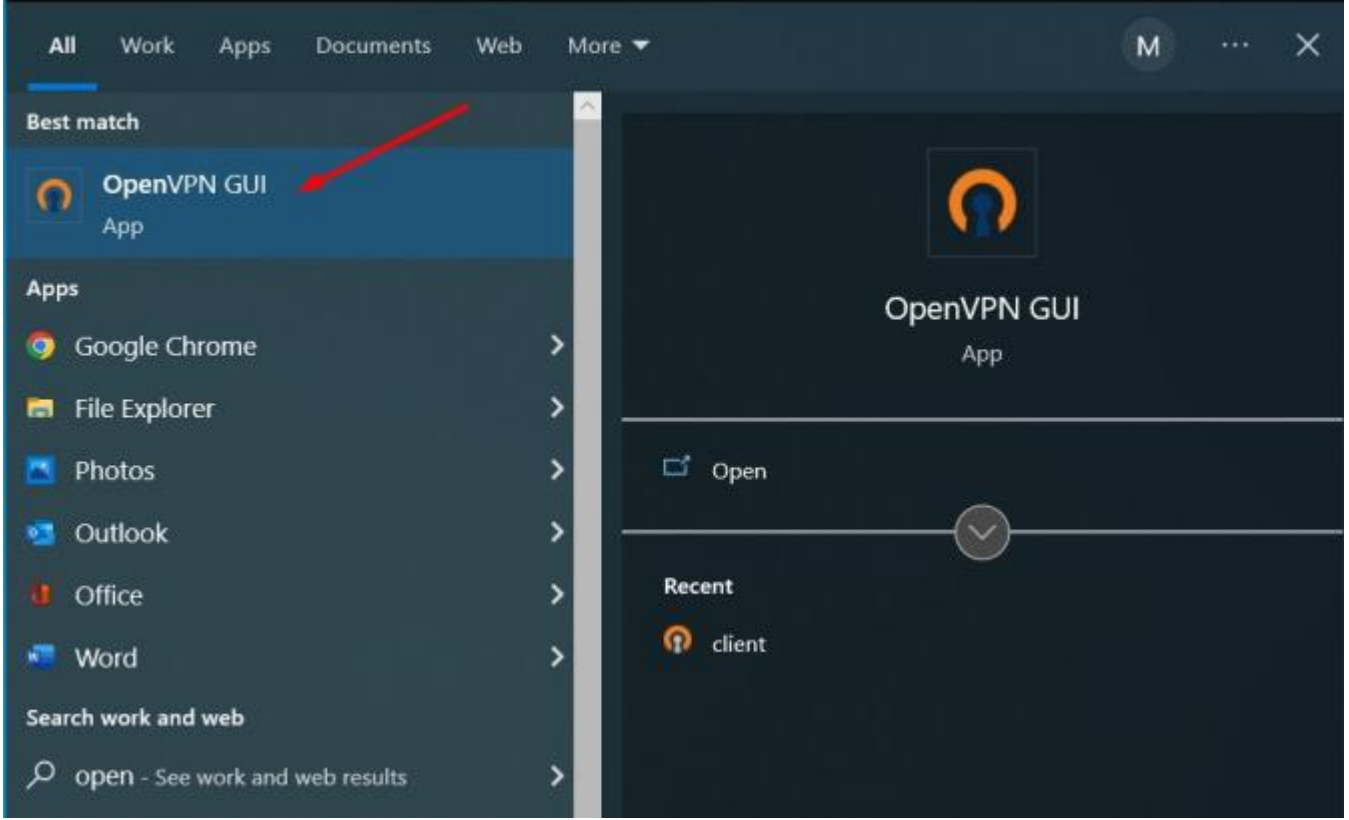
## 18. Adım Sertifika Yazma İşlemi-2

- PC tarafında OpenVPN bağlantısı için TAP kurulumu yapmalıyız sanal ağ bağdaştırıcısı **“tap-windows-9.21.2”**

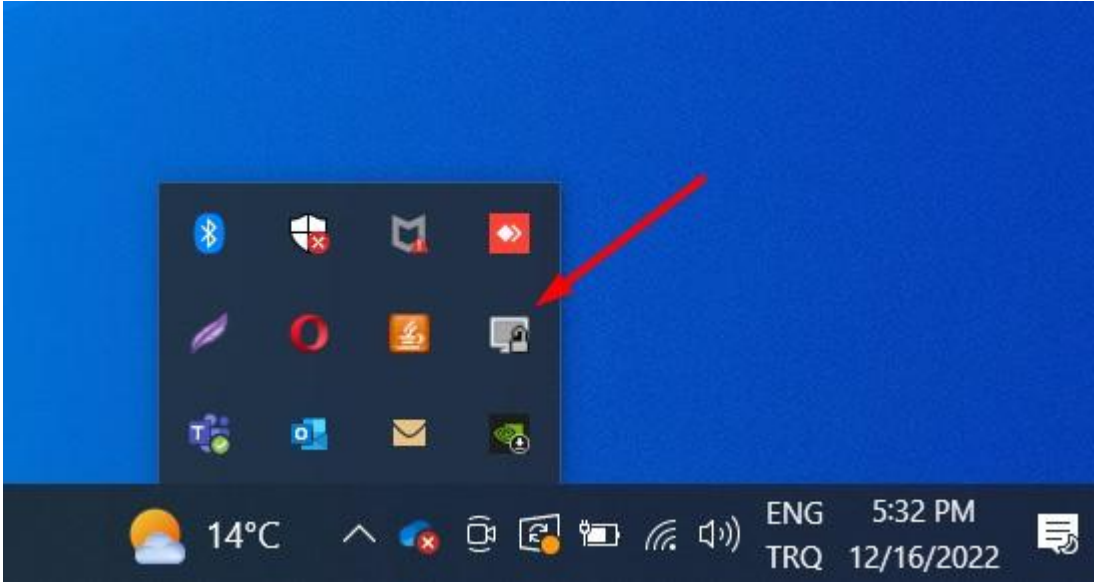


## 19. Adım Tap Kurulumu

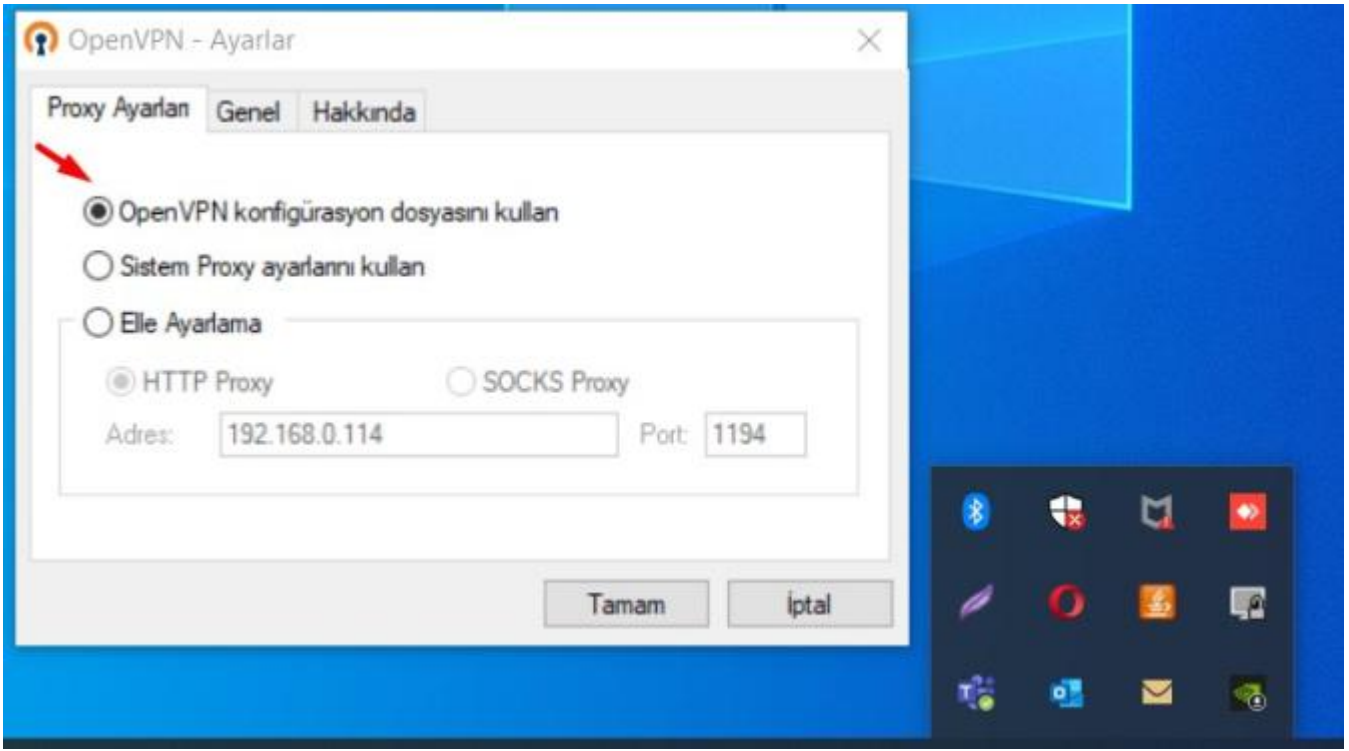
- Tüm ayarlarımızı bittikten sonra PC den OpenVPN programını açarak modemimize bağlantı sağlayacağız.



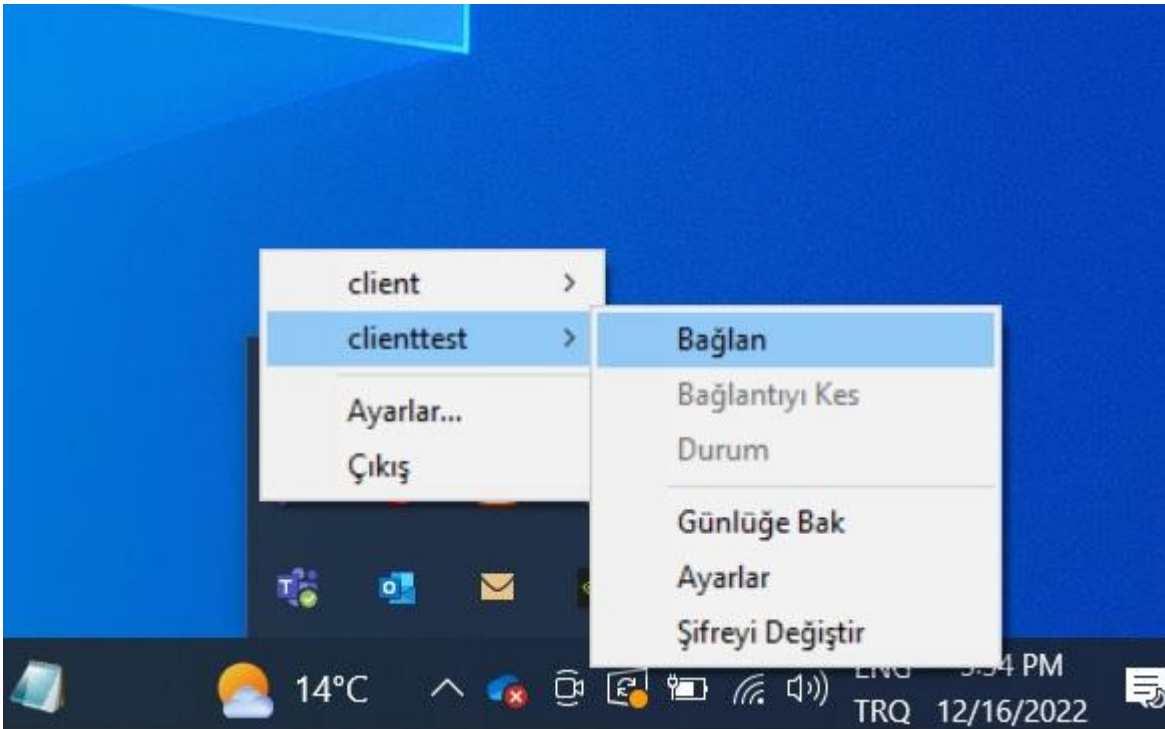
## 20. Adım OpenVPN Uygulaması Açılması-1



## 21. Adım OpenVPN Uygulaması Açılması-2



## 22. Adım OpenVPN Uygulaması Açılması-3



## 23. Adım OpenVPN Bağlatı Başlatılması

FF modemlerde sunucu tarafı için OPEN VPN örnek uygulama videosu:

FF modemlerde istemci tarafı için OPEN VPN örnek uygulama videosu:

## 3.PPTP

## 3. PPTP Uygulaması

Noktadan noktaya güvenli haberleşme için en yaygın VPN güvenli haberleşme metodlarından biri PPTP olup günümüzde birçok işletim sisteminde yaygın olarak kullanılmaktadır. Şirketimizin sunmuş olduğu Four Faith marka modemler de bu tip, güvenli haberleşme çözümlerini desteklemektedir.

## 3.1 Sunucu Modem Ayarları

Bu uygulamada, biri sunucu biri istemci olmak üzere iki adet F3x26Q Router Modem kullanılmıştır. İhtiyaca göre istemci modem sayısı arttırılabilir.

The screenshot displays the configuration page for a Wireless Mobile Router. The page title is "Wireless Mobile Router" and the status bar shows "2. 5G/3G/3. 5G/4G". The firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) stc" with a time of "Zaman: 00:02:56 up 2 min, load average: 0.09, 0.04, 0.01" and WAN IP addresses "WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0".

The main configuration area is titled "PPTP Sunucusu" (PPTP Server). It includes the following settings:

- PPTP Sunucusu:  Etkinleştir  Devre Dışı bırak
- Yayın Desteği:  Etkinleştir  Devre Dışı bırak
- MPPE Şifrelemeye Zorla:  Etkinleştir  Devre Dışı bırak
- DNS1:
- DNS2:
- WINS1:
- WINS2:
- Sunucu IP:
- İstemci IP:
- CHAP-Parola:

Below the PPTP Server settings, there is a section for "PPTP İstemcisi" (PPTP Client) with the following setting:

- PPTP İstemci Seçenekleri:  Etkinleştir  Devre Dışı bırak

At the bottom of the configuration area, there are three buttons: "Kaydet" (Save), "Ayarları Uygula" (Apply Settings), and "Değişiklikleri İptal Et" (Cancel Changes).

### Şekil 1. Sunucu Ayarları

#### Uygulanacak Adımlar

1. "PPTP Sunucu", "Yayın Desteğini" ve "MPPE Şifrelemeye Zorla" etkinleştirin.
2. Sunucu tünel IP'sini belirleyiniz.
3. İstemcilerin IP aralığını belirleyiniz.
4. CHAP Parola kutucuğuna, satır satıra sırasıyla istemcilerin ismi ve şifresini aralara "\*" işareti ve birer boşluk koyarak giriniz.

**Menü**

- Genel Ayarlar
  - Sistem Ayarları
  - DDNS
  - MAC Adres Kopyalama
  - Gelişmiş Yönlendirme
  - Ağ Oluşturma
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

**Gelişmiş Routing**

**Çalıştırma Modu**

Çalıştırma Modu: Ağ Geçidi

**Statik Routing**

Set değeri seçin: 1 (İstemci 1) 34

Router Adı: istemci 1

Metrik: 3

Hedef LAN NET: 192, 168, 2, 0

Alt Ağ Maskesi: 255, 255, 255, 0

Ağ Geçidi: 200, 200, 200, 2

Arayüz: ANY

Routing Tablosunu Göster

Kaydet Ayarları Uygula Değişiklikleri İptal Et

**Yardım** daha fazla...

**Çalıştırma Modu:**  
Eğer Router sizin internet bağlantınıza yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

**Set değeri seçin:**  
Eşleşmeyen Router sayıdır, en fazla 50 ayarlanabilir.

**Router Adı:**  
Router'a vermek istediğiniz adı giriniz.

**Hedef LAN NET:**  
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.

**Alt Ağ Maskesi:**  
Ağ ve Host bölümlerini belirler.

## Şekil 2. Sunucu Gelişmiş Yönlendirme Ayarları Uygulanacak Adımlar

1. Sunucu modem Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modem adını giriniz.
3. İstemci modem sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modem tünel IP adresini giriniz.

Sunucu modem ayarlarını tamamladıktan sonra istemci modem ayarlarına geçebilirsiniz.



## 3.2 İstemci Modem Ayarları

İstemci modem ayarlarını VPN menüsü altından PPTP seçeneğinden yapabilirsiniz. Kutucuklarda belirtilen ayarlar uygulamanıza özel olup diğer ayarları şekildeki gibi giriniz.

The screenshot shows the configuration page for PPTP Client on a wireless mobile router. The page is titled "Wireless Mobile Router" and "2. 5G/3G/3. 5G/4G". The firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) str". The time is "15:25:18 up 15 min, load average: 0.00, 0.01, 0.03". The WAN IP is "192.168.0.116, BKUP WAN IP: 0.0.0.0".

The page is divided into two main sections: "PPTP Sunucusu" (PPTP Server) and "PPTP İstemcisi" (PPTP Client). The "PPTP Sunucusu" section has a radio button for "Etkinleştir" (Enabled) and "Devre Dışı bırak" (Disable). The "PPTP İstemcisi" section has a radio button for "Etkinleştir" (Enabled) and "Devre Dışı bırak" (Disable). The "PPTP İstemcisi" section has the following fields:

- Sunucu IP'si ya da DNS Adı: 188.59.158.246
- Uzak Subnet: 192, 168, 1, 1
- Uzak Alt Ağ Maskesi: 255, 255, 255, 0
- MPPE Şifreleme: mppe stateless
- MTU: 1450 (Default: 1450)
- MRU: 1450 (Default: 1450)
- NAT: Etkinleştir (Enabled)
- Sabit IP: Devre Dışı bırak (Disable)
- Kullanıcı Adı: istemci1
- Şifre: \*\*\*\*\* (Göster button)

At the bottom of the page, there are three buttons: "Kaydet" (Save), "Ayarları Uygula" (Apply Settings), and "Değişiklikleri İptal Et" (Cancel Changes).

### Şekil 3. İstemci Ayarları

#### Uygulanacak Adımlar

1. PPTP istemci ayarlarını enable ediniz.
2. Sırasıyla sunucu modem WAN IP'si, sunucu modem LAN IP'si ve subnet mask'ını giriniz.
3. İstemci modem ismi ve şifresini giriniz.

192.168.2.1/Routing.asp

Four-Faith Wireless Mobile Router 2.5G/3G/3.5G/4G

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std  
Zaman: 15:25:01 up 15 min, load average: 0.00, 0.01, 0.03  
WAN IP: 192.168.0.116, BKUP WAN IP: 0.0.0.0

**Menü**

- Genel Ayarlar
  - Sistem Ayarları
  - DDNS
  - MAC Adres Kopyalama
  - Gelişmiş Yönlendirme
  - Ağ Oluşturma
- Kablosuz Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

**Gelişmiş Routing**

**Çalıştırma Modu**

Çalıştırma Modu: Ağ Geçidi

**Statik Routing**

Set değeri seçin: 1 (sunucu1) Sil

Router Adı: sunucu1

Metrik: 0

Hedef LAN NET: 192.168.1.0

Alt Ağ Maskesi: 255.255.255.0

Ağ Geçidi: 200.200.200.1

Arayüz: ANY

Routing Tablosunu Göster

Kaydet Ayarları Uygula Değişiklikleri İptal Et

**Yardım** daha fazla...

**Çalıştırma Modu:**  
Eğer Router sizin internet bağlantınızı yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

**Set değeri seçin:**  
Eşleşmeyen Router sayıdır, en fazla 50 ayarlanabilir.

**Router Adı:**  
Router'a vermek istediğiniz adı giriniz.

**Hedef LAN NET:**  
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.


**Alt Ağ Maskesi:**  
Ağ ve Host bölümlerini belirler.

## Şekil 4. İstemci Gelişmiş Yönlendirme Ayarları Uygulanacak Adımlar

1. Sunucu modemin Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modemin adını giriniz.
3. İstemci modemin sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modemin tünel IP adresini giriniz.

## 3.3 Bağlantı Testi

Sunucu ve istemci ayarlarını tamamladıktan sonra bağlantı testine geçebilirsiniz.

Four-Faith  Wireless Mobile Router

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) str  
Zaman: 14:42:50 up 3 min, load average: 0.01, 0.03, 0.01  
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

**Menü**

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum
  - Router
  - WAN
  - LAN
  - Kablosuz
  - Cihaz Yönetimi
  - Akıllı Kapı Durumu
  - Bant Genişliği
  - Sistem Bilgisi

**Yerel Ağ**

LAN Durumu

MAC Adres	54:D0:B4:37:CC:8E
Yerel IP	192.168.1.1
Alt Ağ Maskesi	255.255.255.0
Ağ Geçidi	0.0.0.0
Yerel DNS	0.0.0.0

Aktif İstemciler

Host Adı	Yerel IP	MAC Adres	Bağlı Sayın	Oran [16384]
- Hiçbiri -				

Dynamic Host Configuration Protocol (DHCP)


DHCP Durumu

DHCP Sunucusu	ETKİN
DHCP Daemon	DNSMasq
Bağlanç IP Adresi	192.168.1.100
Bitiş IP Adresi	192.168.1.149
İstemci Kira Süresi	1440 dakika

DHCP İstemcileri

Host Adı	Yerel IP	MAC Adres	İstemci Kira Süresi	Sil
- Hiçbiri -				

PPTP İstemcileri Bağlandı

Arayüz	Kullanıcı Adı	Uzak Tünel IP	Uzak IP	Sil
ppp0	istemci1	200.200.200.2	78.175.54.236	

[Bağlantı Testi](#)

**Yardım** [daha fazla...](#)

**MAC Adres:**  
Yerel, Ethernet ağında görüldüğü gibi bu Router'in MAC adresidir.

**Yerel IP:**  
Yerel, Ethernet ağında görüldüğü gibi bu Router'in IP adresini gösterir.

**Alt Ağ Maskesi:**  
Router bir Alt Ağ Maskesi kullandığında, o burda gösterilir.

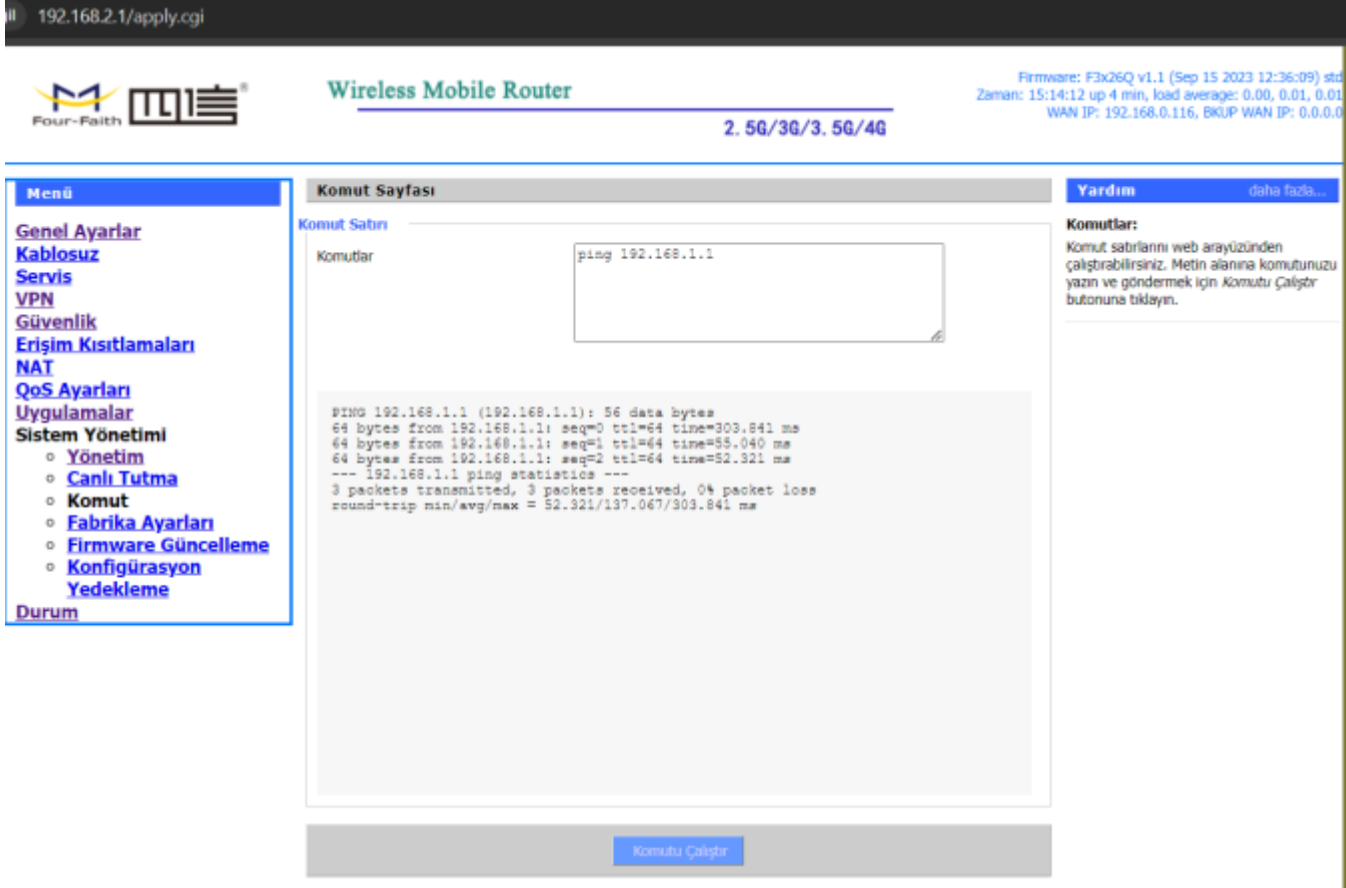
**DHCP Sunucusu:**  
Eğer Router'i DHCP sunucusu olarak kullanıyorsanız, burda görüntülenir.

**OUI Search:**  
Herhangi bir MAC adresine tıklayarak, ağ arayüzünün Organizationally Unique Identifier (OUI) sini göreceksiniz. (IEEE Standards OUI database search).

### Şekil 5. Bağlantı Testi

Sunucu modem istemci modemle ve sunucu modemle olan PPTP bağlantısını "PPTP İstemcileri Bağlandı" sekmesinden kontrol edebilirsiniz.

Son olarak sunucu ve istemci modemleri iki taraflı olarak LAN IP adreslerinden pingleyerek güvenli PPTP bağlantısının kurulduğunu doğrulayabilirsiniz



The screenshot shows the web interface of a Wireless Mobile Router. The page title is "Wireless Mobile Router" and the status bar indicates "2. 5G/3G/3. 5G/4G". The firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) std". The system time is "Zaman: 15:14:12 up 4 min, load average: 0.00, 0.01, 0.01" and the WAN IP is "WAN IP: 192.168.0.116, BKUP WAN IP: 0.0.0.0".

The interface is divided into three main sections: "Menü", "Komut Sayfası", and "Yardım". The "Menü" section on the left contains a list of navigation options: Genel Ayarlar, Kablosuz Servis, VPN, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar, Sistem Yönetimi, Yönetim, Canlı Tutma, Komut, Fabrika Ayarları, Firmware Güncelleme, Konfigürasyon, Yedekleme, and Durum.

The "Komut Sayfası" section is active and shows a "Komut Satırı" (Command Line) with the command "ping 192.168.1.1" entered. Below the command line, the output of the ping test is displayed:

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=303.841 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=55.040 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=52.321 ms
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 52.321/137.067/303.841 ms
```

The "Yardım" section on the right provides instructions on how to use the command line: "Komutları: Komut satırlarını web arayüzünden çalıştırabilirsiniz. Metin alanına komutunuzu yazın ve göndermek için Komutu Çalıştır butonuna tıklayın."

## Şekil 6. Ping Testi

FF modemlerde sunucu tarafı için PPTP VPN örnek uygulama videosu:

FF modemlerde istemci tarafı için PPTP VPN örnek uygulama videosu:

## 4.L2TP

### 4. L2TP Uygulaması

Diğer VPN protokollerinden farklı olarak, Layer 2 Tunnel Protocol, üzerinden geçen trafik ile ilgili herhangi bir gizlilik veya şifreleme sağlamaz. Bu sebeple, iletim öncesi verileri şifrelemek için IPsec olarak bilinen ve kullanıcıların gizliliğini ve güvenliğini sağlayan bir protokol paketiyle uygulanır. VPN uyumlu tüm modern cihazlar ve işletim sistemlerinde dahili olarak L2TP/IPsec bulunur. Four Faith marka modemler de bu tip, güvenli haberleşme çözümlerini desteklemektedir.

#### 4.1 Sunucu Modem Ayarları

Bu uygulamada, biri sunucu biri istemci olmak üzere iki adet F3x26Q Router Modem kullanılmıştır. İhtiyaca göre istemci modem sayısı arttırılabilir.



Menü

Genel Ayarlar  
Kablosuz  
Servis  
VPN  
o PPTP  
o L2TP  
o OPENVPN  
o IPSEC  
o GRE  
Güvenlik  
Erişim Kısıtlamaları  
NAT  
QoS Ayarları  
Uygulamalar  
Sistem Yönetimi  
Durum

L2TP Sunucusu

L2TP Sunucusu

L2TP Sunucu Seçenekleri  Etkinleştir  Devre Dışı bırak

MPPE Şifrelemeye Zorla  Etkinleştir  Devre Dışı bırak

Sunucu IP

İstemci IP

Tünel Kimlik Doğrulama Şifresi   Göster

CHAP-Parola

İstemci \* İstemci \*  
İstemci \* İstemci \*

L2TP İstemcisi

L2TP İstemci

L2TP İstemci Seçenekleri  Etkinleştir  Devre Dışı bırak

Kaydet Ayarları Uygula Değişiklikleri İptal Et

## Şekil 1. Sunucu Ayarları

### Uygulanacak Adımlar

1. "L2TP Sunucu", "Yayın Desteğini" ve "MPPE Şifrelemeye Zorla" etkinleştirin.
2. Sunucu tünel IP'sini belirleyiniz.
3. İstemcilerin IP aralığını belirleyiniz.
4. CHAP Parola kutucuğuna, satır satıra sırasıyla istemcilerin ismi ve şifresini aralara "\*" işareti ve birer boşluk koyarak giriniz.

**Menü**

**Genel Ayarlar**

- Sistem Ayarları
- DDNS
- MAC Adres Kopyalama
- Gelişmiş Yönlendirme
- Ağ Oluşturma

**Kablosuz**

**Servis**

**VPN**

**Güvenlik**

**Erişim Kısıtlamaları**

**NAT**

**QoS Ayarları**

**Uygulamalar**

**Sistem Yönetimi**

**Durum**

**Gelişmiş Routing**

**Çalıştırma Modu**

Çalıştırma Modu: Ağ Geçidi

**Statik Routing**

Set değeri seçin: 1 ( ) Sil

Router Adı: istemci 1

Metrik: 1

Hedef LAN NET: 192 168 4 0

Alt Ağ Maskesi: 255 255 255 0

Ağ Geçidi: 200 200 200 1

Arayüz: ANY

Routing Tablosunu Göster

Kaydet Ayarları Uygula Değişiklikleri İptal Et

**Yardım** daha fazla...

**Çalıştırma Modu:**  
Eğer Router sizin internet bağlantınızı yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

**Set değeri seçin:**  
Eşleşmeyen Router sayısıdır, en fazla 50 ayarlama yapabilirsiniz.

**Router Adı:**  
Router'a vermek istediğiniz adı giriniz.

**Hedef LAN NET:**  
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.

**Alt Ağ Maskesi:**  
Ağ ve Host bölümlerini belirler.


## Şekil 2. Sunucu Gelişmiş Yönlendirme Ayarları Uygulanacak Adımlar

1. Sunucu modem Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modem adını giriniz.
3. İstemci modem sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modem tünel IP adresini giriniz.

Sunucu modem ayarlarını tamamladıktan sonra istemci modem ayarlarına geçebilirsiniz.

## 4.2 İstemci Modem Ayarları

İstemci modem ayarlarını VPN menüsü altından L2TP seçeneğinden yapabilirsiniz. Kutucuklarda belirtilen ayarlar uygulamanıza özel olup diğer ayarları şekildeki gibi giriniz.

Four-Faith  Wireless Mobile Router

Firmware: F3x26Q v1.1 (Jul 4 2024 14:31:20) str  
Zaman: 16:55:25 up 25 min, load average: 0.01, 0.04, 0.0  
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

Menü **L2TP Sunucusu** Yardım daha fazla...

**Genel Ayarlar**  
**Kablosuz**  
**Servis**  
**VPN**  
o PPTP  
o L2TP  
o OPENVPN  
o IPSEC  
o GRE  
**Güvenlik**  
**Erişim Kısıtlamaları**  
**NAT**  
**QoS Ayarları**  
**Uygulamalar**  
**Sistem Yönetimi**  
**Durum**

**L2TP Sunucusu**

L2TP Sunucu Seçenekleri  Etkinleştir  Devre Dışı bırak

**L2TP İstemcisi**

L2TP İstemci Seçenekleri  Etkinleştir  Devre Dışı bırak

Tünel Adı

Kullanıcı Adı

Şifre   Göster

Tünel Kimlik Doğrulama Şifresi

Ağ Geçidi (L2TP Sunucusu)

Uzak Subnet

Uzak Alt Ağ Maskesi

MPPE Şifreleme

MTU  (Default: 1450)

MRU  (Default: 1450)

NAT  Etkinleştir  Devre Dışı bırak

Sabit IP  Etkinleştir  Devre Dışı bırak

CHAP Gerekli  Evet  Hayır

PAP'ı Reddet  Evet  Hayır

Kimlik Doğrulama Gerekli  Evet  Hayır

### Şekil 3. İstemci Ayarları Uygulanacak Adımlar

1. L2TP istemci ayarlarını enable ediniz.
2. Sırasıyla sunucu modem WAN IP'si, sunucu modem LAN IP'si ve subnet mask'ını giriniz.
3. İstemci modem ismi ve şifresini giriniz.

**Menü**

- Genel Ayarlar
  - Sistem Ayarları
  - DDNS
  - MAC Adres Kopyalama
  - Gelişmiş Yönlendirme
  - Ağ Oluşturma
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

**Gelişmiş Routing**

Çalıştırma Modu

Çalıştırma Modu: Ağ Geçidi

Statik Routing

Set değeri seçin: 1 ( ) Sil

Router Adı: istemci 1

Metrik: 1

Hedef LAN NET: 192 168 4 0

Alt Ağ Maskesi: 255 255 255 0

Ağ Geçidi: 200 200 200 2

Arayüz: ANY

Routing Tablosunu Göster

Kaydet | Ayarları Uygula | Değişiklikleri İptal Et

**Yardım** daha fazla...

**Çalıştırma Modu:**  
Eğer Router sizin internet bağlantınızı yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

**Set değeri seçin:**  
Eşleşmeyen Router sayıdır, en fazla 50 ayarlama yapabilirsiniz.

**Router Adı:**  
Router'a vermek istediğiniz adı giriniz.

**Hedef LAN NET:**  
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.

**Alt Ağ Maskesi:**  
Ağ ve Host bölümlerini belirler.

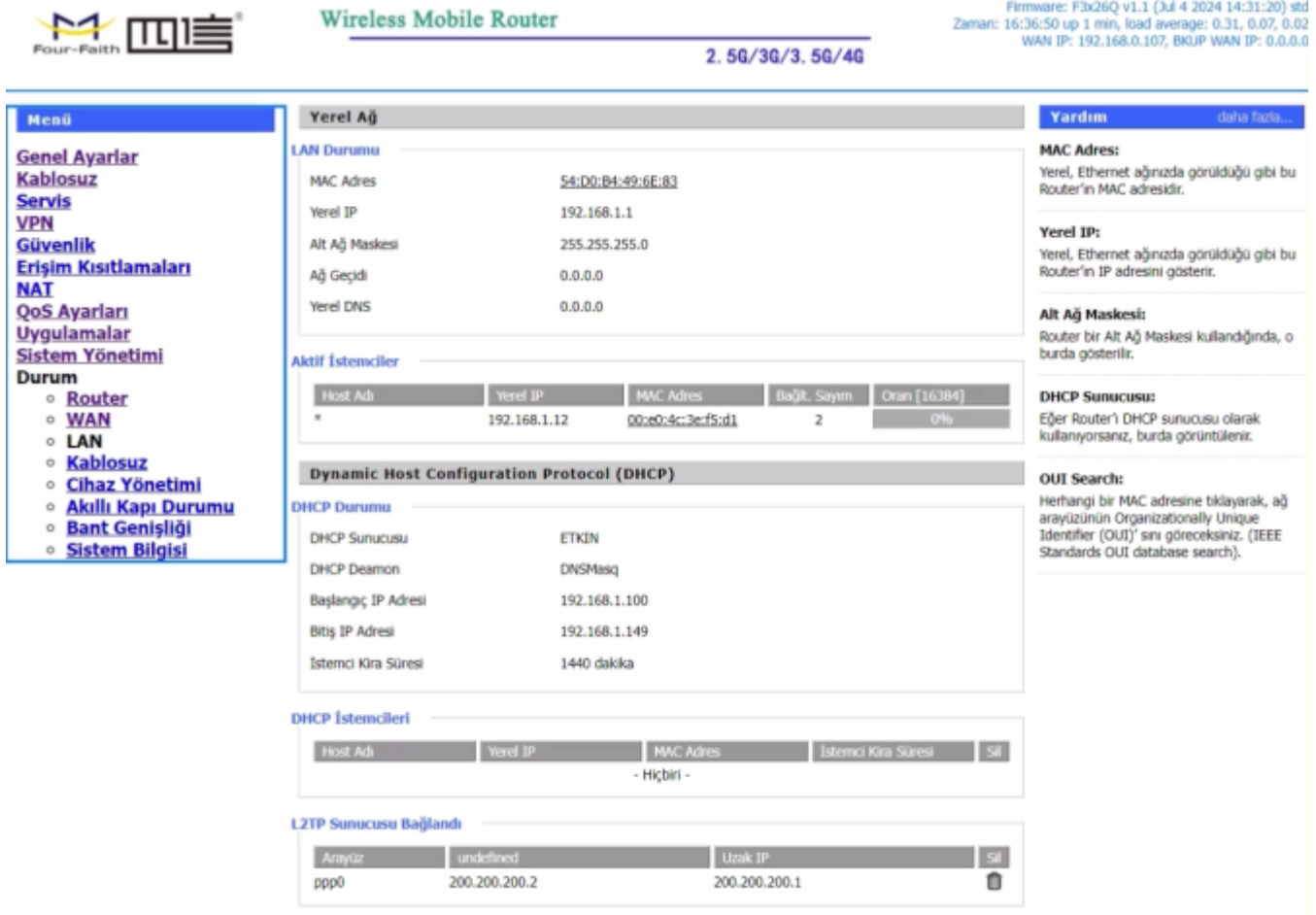
## Şekil 4. İstemci Gelişmiş Yönlendirme Ayarları Uygulanacak Adımlar

1. Sunucu modem Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modem adını giriniz.
3. İstemci modem sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modem tünel IP adresini giriniz.



## 4.3 Bağlantı Testi

Sunucu ve istemci ayarlarını tamamladıktan sonra bağlantı testine geçebilirsiniz.



**Wireless Mobile Router**  
Firmware: F3x26Q v1.1 (Jul 4 2024 14:31:20) std  
Zaman: 16:36:50 up 1 min, load average: 0.31, 0.07, 0.02  
WAN IP: 192.168.0.107, BKUP WAN IP: 0.0.0.0  
2. 5G/3G/3. 5G/4G

**Menü**  
Genel Ayarlar  
Kablosuz  
Servis  
VPN  
Güvenlik  
Erişim Kısıtlamaları  
NAT  
QoS Ayarları  
Uygulamalar  
Sistem Yönetimi  
Durum  
o Router  
o WAN  
o LAN  
o Kablosuz  
o Cihaz Yönetimi  
o Akıllı Kapı Durumu  
o Bant Genişliği  
o Sistem Bilgisi

**Yerel Ağ**

**LAN Durumu**

MAC Adres	54:D0:84:49:6E:83
Yerel IP	192.168.1.1
Alt Ağ Maskesi	255.255.255.0
Ağ Geçidi	0.0.0.0
Yerel DNS	0.0.0.0

**Aktif İstemciler**

Host Adı	Yerel IP	MAC Adres	Bağl. Sayım	Oran [16384]
*	192.168.1.12	00:e0:4c:3e:f5:d1	2	0%

**Dynamic Host Configuration Protocol (DHCP)**

**DHCP Durumu**

DHCP Sunucusu	ETKİN
DHCP Deamon	DNSMasq
Başlangıç IP Adresi	192.168.1.100
Bitiş IP Adresi	192.168.1.149
İstemci Kira Süresi	1440 dakika

**DHCP İstemcileri**

Host Adı	Yerel IP	MAC Adres	İstemci Kira Süresi	Sil
- Hiçbiri -				

**L2TP Sunucusu Bağlandı**

Arayüz	Uzak IP	Sil
ppp0	200.200.200.2	200.200.200.1

**Yardım** daha fazla...

**MAC Adres:**  
Yerel, Ethernet ağınızda görüldüğü gibi bu Router'in MAC adresidir.

**Yerel IP:**  
Yerel, Ethernet ağınızda görüldüğü gibi bu Router'in IP adresini gösterir.

**Alt Ağ Maskesi:**  
Router bir Alt Ağ Maskesi kullandığında, o burada gösterilir.

**DHCP Sunucusu:**  
Eğer Router'i DHCP sunucusu olarak kullanıyorsanız, burada görüntülenir.

**OUI Search:**  
Herhangi bir MAC adresine tıklayarak, ağ arayüzünüzün Organizationally Unique Identifier (OUI)'sını göreceksiniz. (IEEE Standards OUI database search).

### Şekil 5. Bağlantı Testi

Sunucu modemini istemci modemle ve sunucu modemle olan L2TP bağlantısını "L2TP İstemcileri Bağlandı" sekmesinden kontrol edebilirsiniz.

Son olarak sunucu ve istemci modemleri iki taraflı olarak LAN IP adreslerinden pingleyerek güvenli L2TP bağlantısının kurulduğunu doğrulayabilirsiniz

Four-Faith **Wireless Mobile Router** Firmware: F3x26Q v1.1 (Jul 4 2024 14:31:20) str  
Zaman: 16:37:19 up 1 min, load average: 0.39, 0.11, 0.04  
WAN IP: 192.168.0.107, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

**Menü** **Komut Sayfası** **Yardım** daha fazla...

**Genel Ayarlar**  
**Kablosuz**  
**Servis**  
**VPN**  
**Güvenlik**  
**Erişim Kısıtlamaları**  
**NAT**  
**QoS Ayarları**  
**Uygulamalar**  
**Sistem Yönetimi**  
o **Yönetim**  
o **Canlı Tutma**  
o **Komut**  
o **Fabrika Ayarları**  
o **Firmware Güncelleme**  
o **Konfigürasyon**  
**Yedekleme**  
**Durum**

**Komut Satırı**

Komutlar

```
ping 192.168.4.1
```

```
PING 192.168.4.1 (192.168.4.1): 56 data bytes  
64 bytes from 192.168.4.1: seq=0 ttl=64 time=0.927 ms  
64 bytes from 192.168.4.1: seq=1 ttl=64 time=0.713 ms  
64 bytes from 192.168.4.1: seq=2 ttl=64 time=0.839 ms  
--- 192.168.4.1 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 0.713/0.826/0.927 ms
```

**Komutlar:**  
Komut satırlarını web arayüzünden çalıştırabilirsiniz. Metin alanına komutunuzu yazın ve göndermek için **Komutu Çalıştır** butonuna tıklayın.

**Komutu Çalıştır**

## Şekil 6. Ping Testi

FF modemlerde sunucu tarafı için L2TP VPN örnek uygulama videosu:

FF modemlerde istemci tarafı için L2TP VPN örnek uygulama videosu:

## 5.MEDAS VPN

## 5. MEDAŞ VPN Ayarları

**Menü** **Genel Ayarlar** **Yardım**

**Genel Ayarlar**  
**Kablosuz**  
**Servis**  
**VPN**  
o **PPTP**  
o **L2TP**  
o **OPENVPN**  
o **IPSEC**  
o **GRE**  
**Güvenlik**  
**Erişim Kısıtlamaları**  
**NAT**  
**QoS Ayarları**  
**Uygulamalar**  
**Sistem Yönetimi**  
**Durum**

**Genel Ayarlar**

**Genel Ayarlar**

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi **Hiçbir**

IPSEC OVER L2TP  Etkinleştir  Devre Dışı

**Bağlantı Durumu ve Kontrolü**

Num Adı	Tipi	Genel Adı	Durum	Eylem
1	medas	tünel-client 10.123.11.0/27-[WAN1] vpn1.meramedas.com.tr- [10.34.255.0/24,10.107.0.0/17]	Bağlantı Kuruldu	

**Sertifika Yönetimi**

**Sertifika Yönetimi**

CA Adı	Referans Sayısı	Eylem

**Yardım**

**NAT-Geçiş**  
Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

**Log-Level**  
Hata ayıklamayı etkinleştirin veya devre dışı bırakın

**Bağlantı Durumu**  
15 bağlantı oluşturulabilir

**Çift Altağı destekliyor. 2 ayrı tünel birleştirilebiliyor**

## Şekil 7. MEDAŞ VPN 1

- [L2TP](#)
- [OPENVPN](#)
- [IPSEC](#)
- [GRE](#)
- [Güvenlik](#)
- [Erişim Kısıtlamaları](#)
- [NAT](#)
- [QoS Ayarları](#)
- [Uygulamalar](#)
- [Sistem Yönetimi](#)
- [Durum](#)

### Bağlantı

Bağlantı -iki ayrı alt ağı aralarında virgül koyarak "," boşluk bırakmadan yazabilir

Adı	medaş	Etkin	<input checked="" type="checkbox"/>
Yerel WAN Arayüzü	WAN	Uzak WAN adresi	vpn1.meramedas.cor
Yerel Alt Ağ	10.123.21.0/27	Uzak Alt Ağ	10.107.0.0/17,10.34.
Yerel ID	10.123.21.1	Uzak ID	88.255.44.70

Modem-Local IP Medaş statik IP

### Algılama

DPD Algılamayı Etkinleştir

Zaman Aralığı 60 (Sn) Zaman aşımı 180 (Sn) Eylem restart

### Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir

**Phase 1**

IKE Şifreleme 3DES IKE Doğrulama SHA1 IKE Grup tipi Grup2(1024)

IKE Ömrü 24 Saat

**Phase 2**

ESP Şifreleme 3DES ESP Doğrulama SHA1 ESP Grup tipi NULL

ESP Şifre Zamanı 24 Saat

Enable IKEv2

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşan şifre açık metin olarak iletilir!)

Perfect Forward Secrecy (PFS)

### Doğrulama

Doğrulama

Bağlantının Adı: IPsec bağlantısı olmalıdır

Yerel ve Uzak: Yerel ve uzak ağı adresi veya başlangıç domain adı girilebilir

PSK Değeri: PSK değerinin uzunluğu 16 karakterden fazla olamaz

IKEv2: undefined

## Şekil 8. MEDAŞ VPN 2

Bağlantı Sorgulama

Algılama Periyodu: 300 Sn

Terah Edilen Sunucu IP: 8 8 8 8

Diğer Sunucu IP: 8 8 4 4

Bağlantı Hataları Restart:  Etkinleştir  Devre Dışı bırak (Default: 10 dakika)

Fixed WAN Netmask Address:  Etkinleştir  Devre Dışı bırak

STP:  Etkinleştir  Devre Dışı bırak

**Maksimum DHCP Kullanıcı:**  
Router'ınız dağıtmış olduğu adres sayısını sınırlayabilirsiniz. 0 (sıfır) sadece önceden tanımlanan statik adreslerin dağıtılacağı anlamına gelir.

**Zaman Ayarı:**  
Bulunmuş olduğunuz zaman dilimini ve Yaz Saati Uygulama (YSU) dönemini seçiniz. Router yerel zamanı veya UTC zamanını kullanabilir.

**IPSEC Çevirini Devam et**

Bağlantı Sorgulama: Ping

Algılama Periyodu: 3600 Sn

Terah Edilen Sunucu IP: 10 34 255 18

**Özel Ayarlar**

Router Adı: GENCBEYGES

Host Adı:

Domain Adı:

MTU: Auto 1500

Force Net Card Mode: Auto

**Ağ Ayarları**

**Router IP**

Yerel IP Adresi: 10 123 11 1

Şekil 9. MEDAŞ VPN 3

Four-Faith TL1 Wireless Mobile Router 3G/4G/4G+

Firmware: R100 v1.0 (Sep 21 2023 14:18:51) std  
Zaman: 19:43:52 up 15 min, load average: 0.02, 0.03, 0.03  
WAN IP: 192.168.0.108, BKUP WAN IP: 0.0.0.0  
Dil: Türkçe

**Cron**

Cron:  Etkinleştir  Devre Dışı bırak

Ek Cron Görevleri:

**Dil Seçimi**

Dil: Türkçe

**Uzaktan Yönetim**

Uzaktan Yönetim:  Etkinleştir  Devre Dışı bırak

Protokol:  V1.0  V2.0

Sunucu IP'si: 47.88.21.65

Sunucu Portu: 9901 (Default: 44008, Aralık: 1 - 65535)

Canlılık Periyodu: 60 (Default: 60Sn Aralık: 1 - 999)

3G Veri Akışı Yükleme Periyodu: 300 (Default: 300Sn Aralık: 1 - 86400)

Aygıt Kodu: SN

Cihaz Tipi Tanımlama: F3x26Q


Özelleştirilmiş Yerel Domain: wifi.cn

**Firmware Güncelleme**

Firmware Güncelleme:  Etkinleştir  Devre Dışı bırak

Kaydet Ayarları Uygula Değişiklikleri İptal Et Router'ı Yeniden Başlat

Şekil 10. MEDAŞ Uzaktan Yönetim Ayarları

Four-Faith  Wireless Mobile Router 3G/4G/4G+

Firmware: R100 v1.0 (Sep 21 2023 14:18:51) std  
Zaman: 17:15:11 up 9 min, load average: 0.53, 0.56, 0.29  
WAN IP: 5.229.193.126, SCLP WAN IP: 0.0.0.0  
Dil: (Türkiye) v

Genel Kablosuz Servis VPN Güvenlik Erişim Kestirimler NAT QoS Uygulamalar **Yönetim** Durum

**Komut Sayfası** Yardım daha fazla...

**Komut Satırı**

Komutlar

```
PING 10.34.255.18 (10.34.255.18): 56 data bytes
64 bytes from 10.34.255.18: seq=0 ttl=255 time=51.080 ms
64 bytes from 10.34.255.18: seq=1 ttl=255 time=54.320 ms
64 bytes from 10.34.255.18: seq=2 ttl=255 time=53.300 ms
--- 10.34.255.18 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 51.080/52.900/54.320 ms
```

**Komutlar:**  
Komut satırlarını web arayüzünden çalıştırabilirsiniz. Metin alanına komutunuzu yazın ve göndermek için *Komutu Çalıştır* butonuna tıklayın.

## Şekil 11. MEDAŞ VPN Testi

### 6.BEDAS VPN

## 6. BEDAŞ VPN Ayarları

**Menü**

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
  - o PPTP
  - o L2TP
  - o OPENVPN
  - o IPSEC
  - o GRE
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

**Tipi**

Tipi:

IPSEC rol:  İstemci  Sunucu

---

**Bağlantı**

Bağlantı

Adı: <input type="text" value="VPN"/>	Etkin: <input checked="" type="checkbox"/>
Yerel WAN Arayüzü: <input type="text" value="WAN"/>	Uzak WAN adresi: <input type="text" value="85.111.45.4"/>
Yerel Alt Ağ: <input type="text" value="0.0.0.0/0"/>	Uzak Alt Ağ: <input type="text" value="0.0.0.0/0"/>
Yerel ID: <input type="text" value="0.0.0.0/0"/>	Uzak ID: <input type="text" value="0.0.0.0/0"/>

---

**Algılama**

DPD Algılamayı Etkinleştir:

Zaman Aralığı:  (Sn) Zaman aşımı:  (Sn) Eylem:

---

**Gelişmiş Ayarlar**

Gelişmiş ayarları etkinleştir:

**Phase 1**

IKE Şifreleme:  IKE Doğrulama:  IKE Grup tipi:

IKE Ömrü:  Saat

**Phase 2**

ESP Şifreleme:  ESP Doğrulama:  ESP Grup tipi:

ESP Şifre Zamanı:  Saat

Enable IKEv2:

IKE agresif moda izin ver: Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletir!)

Perfect Forward Secrecy (PFS)

---

**Doğrulama**

Doğrulama

Paylaşılan Şifreyi kullanın:

X.509 sertifikası oluşturun ve kullanın

**Yardım** [daha fazla...](#)

**Tipi**

IPsec tipini seçin, tünel ya da transport

**Rol**

IPsec rolünü seçin, istemci ya da sunucu

**Bağlantının Adı**

IPsec bağlantı adı 20 karaktere kadar olmalıdır

**Yerel ve Uzak Ağ için ID**

Yerel ve uzak ağa ID tanımlamak için IP adresi veya bağında @ işareti ekleyerek domain adı girilebilir

**PSK Değeri**

PSK değerinin uzunluğu 30'dan fazla olamaz

**IKEv2**

undefined

**Şekil 12. BEDAŞ VPN Ayarları**

**NOT:** BEDAS VPN IPSEC Kurulumu gerçekleştirildikten sonra modeme uzaktan erişim kapanır. Wan IP ile uzaktan 8088 portu ile erişemezsiniz. Ayrıca tüm yönlendirmeler VPN üzerine olduğu için açılan portlara da erişim olmayacaktır. Cihaz sadece local erişime açıktır.

