

Kendi kendine oluşturulan sertifikayı kullanarak OpenVPN'den Vigor Router'a

Vigor Router, üretici yazılımı sürümü 3.9.4'ten beri OpenVPN için sertifika oluşturmayı destekler. Bu makale, kendi kendine oluşturulan sertifikalarla farklı istemcilerden Vigor Router'a OpenVPN'in nasıl oluşturulacağını gösterir.

1. Bir uzaktan çevirmeli kullanıcı profili oluşturun: VPN and Remote Access>> Remote Dial-in User'a gidin, profili düzenlemek için mevcut bir dizine 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
1.	???	<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"/>	---

2. Profili aşağıdaki gibi düzenleyin:

- Etkinleştir'i işaretleyin
- Allowed Dial-in Type için OpenVPN Tunnel'i seçin.
- Bir kullanıcı adı ve şifre belirleyin.
- Kaydetmek için Tamam'ı tıklayın

VPN and Remote Access >> Remote Dial-in User

Index No. 2

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="0"/> second(s)</p>	<p>Username <input type="text" value="openvpn"/></p> <p>Password <input type="password" value="...."/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input type="text"/></p> <p>Secret <input type="text"/></p>
<p>Allowed Dial-In Type</p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> IKEv1/IKEv2 <input checked="" type="checkbox"/> IKEv2 EAP <input checked="" type="checkbox"/> IPsec XAuth</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input checked="" type="checkbox"/> OpenVPN Tunnel</p>	<p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input type="text" value=""/> Max: 64 characters</p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p>

3. VPN and Remote Dial-in User>>Remote Access Control Setup'a gidin ve OpenVPN Hizmetinin etkinleştirildiğinden emin olun.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input 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
<input checked="" type="checkbox"/>	Enable OpenVPN Service

4. System Maintenance >> Time and Date sayfasından yönlendiricideki saatin doğru olduğunu onaylayın .

System Maintenance >> Time and Date

Time Information

Current System Time	2020 Jun 2 Tue 10 : 43 : 5	Inquire Time
---------------------	----------------------------	--------------

Time Setup

<input type="radio"/>	Use Browser Time
<input checked="" type="radio"/>	Use Internet Time
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT+08:00) Taipei
Enable Daylight Saving	<input type="checkbox"/> Advanced
Automatically Update Interval	30 mins
Send NTP Request Through	Auto

OK Cancel

5. VPN and Remote Access >> OpenVPN >> OpenVPN Server Setup'a gidin ,

- OpenVPN bağlantıları için hangi aktarım protokolünü kullanmak istediğinize bağlı olarak TCP Modunu veya UDP Modunu etkinleştirin
- İsterseniz TCP Bağlantı Noktasını ve UDP Bağlantı Noktasını özelleştirin

OpenVPN Server Setup	Client Config
General Setup	
UDP	<input checked="" type="checkbox"/> Enable
UDP Port	1194
TCP	<input checked="" type="checkbox"/> Enable
TCP Port	1194
Cipher Algorithm	AES128
HMAC Algorithm	SHA1
Certificate Authentication	<input type="checkbox"/>

6. Sertifikalar oluşturun

- Yönlendirici tarafından oluşturulan sertifikaları seçin
- OLUŞTUR'a tıklayın
- Tamam'ı tıklayın

Certificates Setup

Certificate Source Router generated certificates Uploading certificates to Router

GENERATE

Generated certificates

Root Certificate: **Openvpn Root CA**

Server Certificate: **openvpn server**

Client Certificate: **openvpn client**

Trust Certificate: **Trusted CA-1**

Delete all certificates

Note: OpenVPN on vigor only support TUN device interface currently. So please setup corresponding configurations on the client side.

OK

7. OpenVPN Client Config sayfasına gidin:

- Arayüz için OpenVPN bağlantısına izin veren WAN'ı seçin
- Kullanmak istediğiniz Protokolü seçin
- Bir Yapılandırma dosya adı verin
- VPN yapılandırma dosyasını kaydetmek ve OpenVPN istemci cihazlarına göndermek için Dışa Aktar'a tıklayın .

VPN and Remote Access >> OpenVPN

OpenVPN Server Setup **Client Config**

Remote Server IP WAN2 111.251.212.22 Domain

Transport Protocol TCP

Auto Dial-Out Enable Disable

Set VPN as Default Gateway Enable Disable

UDP Ping 10 Second

UDP Ping exit 60 Second

File Name openvpn.ovpn

Export

UDP Ping'in değeri, en az n saniye boyunca hiçbir paket gönderilmemişse, yönlendiricinin TCP/UDP kanalı üzerinden uzaktan ping atacağı anlamına gelir. İki kullanım amacı vardır:

- Durum bilgisi olan güvenlik duvarlarıyla uyumluluk. Periyodik ping, OpenVPN UDP paketlerinin geçmesine izin veren durum bilgisi olan bir güvenlik duvarı kuralının zaman aşımına uğramamasını sağlayacaktır.
- Uzaktan kumandanın eşinin varlığını test etmesi için bir temel sağlamak.

UDP Ping çıkışının değeri, uzaktan bir ping veya başka bir paket alınmadan n saniye geçtikten sonra OpenVPN'in çıkacağı anlamına gelir.

Örneğin, UDP Ping çıkışı 60 olarak ayarlandığında, eşinin bağlantısı kesilirse OpenVPN 60 saniye içinde çıkacaktır.

8. VPN and Remote Access >> SSL General Setup'a gidin ve sunucu sertifikası olarak openvpn sunucu sertifikasını seçin .

VPN and Remote Access >> SSL General Setup

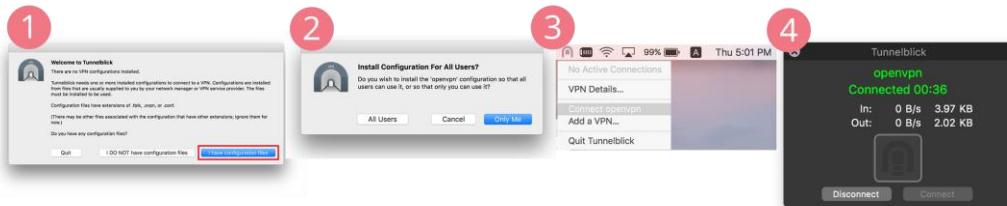
SSL General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> WAN4	<input checked="" type="checkbox"/> LTE	<input checked="" type="checkbox"/> WAN6
Port	443 (Default: 443)					
Server Certificate	openvpn server					

Bağlantı için herhangi bir OpenVPN İstemci Uygulamasını kullanabilirsiniz. Tek yapmanız gereken, yönlendiriciden dışa aktarılan yapılandırma dosyasını içe aktarmak ve kimlik bilgileri istendiğinde kullanıcı adını ve parolayı girmektir.

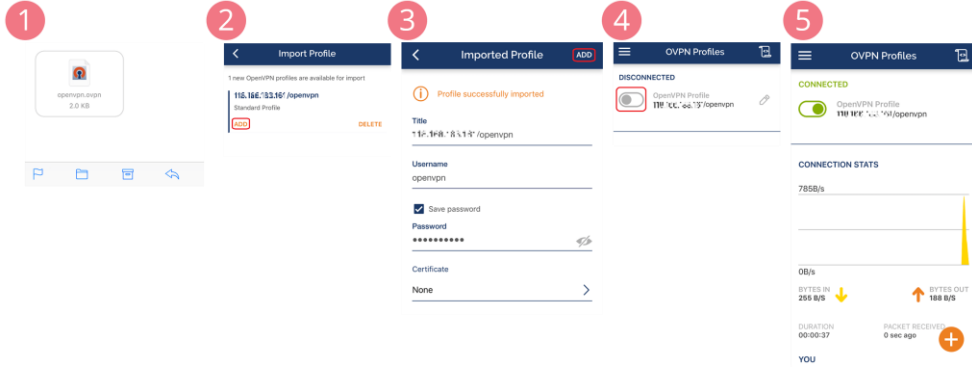
Tunnelblick ile macOS'tan bağlanma

1. OpenVPN istemci yazılımını indirin ve kurun. Yazılımı başlatın ve yapılandırma dosyalarını var'a tıklayarak istemci yapılandırma dosyasını içe aktarın.
2. İstemci yapılandırma dosyasına çift tıklayın, ardından bu VPN profilinin diğer kullanıcılarla paylaşılıp paylaşılmayacağına bağlı olarak "Tüm Kullanıcılar" veya "Yalnızca Ben"i seçin. (Not: İstemci yapılandırmasını çift tıklayarak içe aktaramazsanız, lütfen openvpn dosyasını menü çubuğundaki veya dock'taki Tunnelblick simgesine sürükleyip bırakmayı deneyin.
3. VPN tünelini başlatmak için, menü çubuğundaki Tunnelblick simgesine sağ tıklayın, ardından Openvpn'yi Bağla'ya tıklayın ("openvpn", istemci yapılandırma dosyasının adıdır)
4. Bağlantı kurulduktan sonra VPN durumunu kontrol edebiliriz.



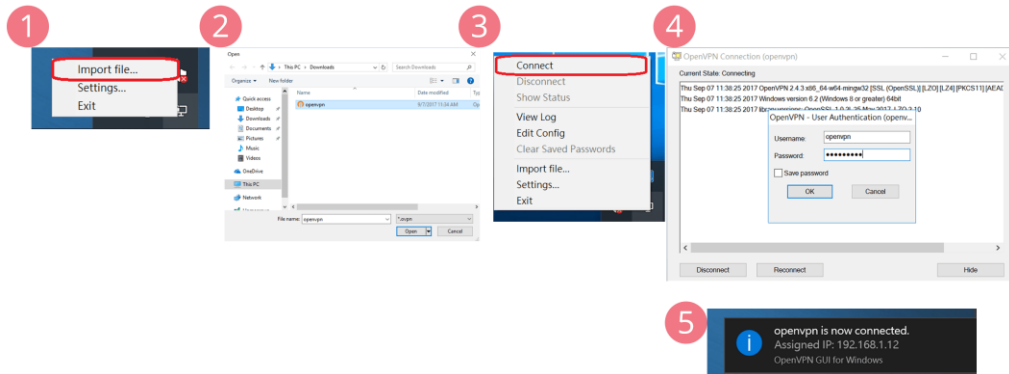
OpenVPN Connect ile iOS'tan bağlanma

1. App Store'dan OpenVPN Connect'i indirin. Ardından config dosyasını iOS cihazına gönderin, burada mail olarak gönderiyoruz. iOS cihazında dosyaya dokununuz ve OpenVPN uygulamasıyla açın.
2. İstemci yapılandırmasını içe aktarmak için 'EKLE'ye dokununuz.
3. Kullanıcı Adı ve Parolayı girin, ardından EKLE'ye dokununuz.
4. VPN'yi açın.
5. Bağlantı kurulduktan sonra VPN durumunu kontrol edebiliriz.



OpenVPN ile Windows'tan Bağlanma

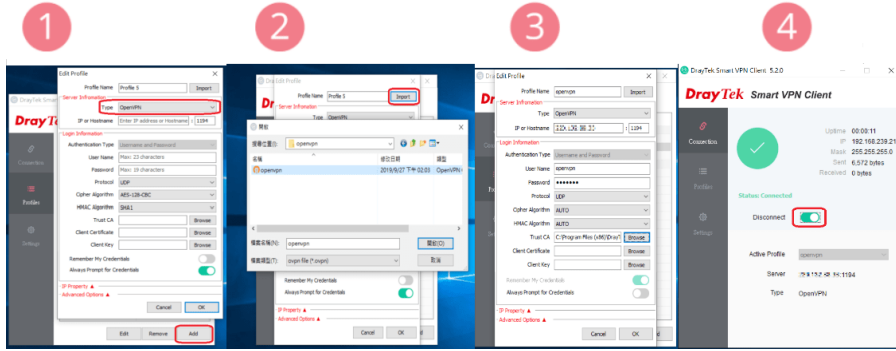
1. Windows için OpenVPN'i indirip yükleyin. Görev çubuğundaki OpenVPN simgesine sağ tıklayarak istemci yapılandırma dosyasını içe aktarın, ardından Dosyayı içe aktar... ögesini tıklayın.
2. Yapılandırma dosyasını seçin ve Aç'a tıklayın.
3. Görev çubuğundaki OpenVPN simgesine sağ tıklayıp ardından Bağlan'ı tıklayarak VPN bağlantısı kurun.
4. Kullanıcı Adı ve Parolayı girin, ardından bağlanmak için Tamam'ı tıklayın.
5. Bağlantı kurulduktan sonra VPN durumunu kontrol edebiliriz.



Smart VPN istemcisi ile Windows'tan OpenVPN ile bağlanma

OpenVPN, v5.2.0'dan beri Smart VPN istemcisi tarafından desteklenmektedir, lütfen önce Windows için OpenVPN'i kurun .

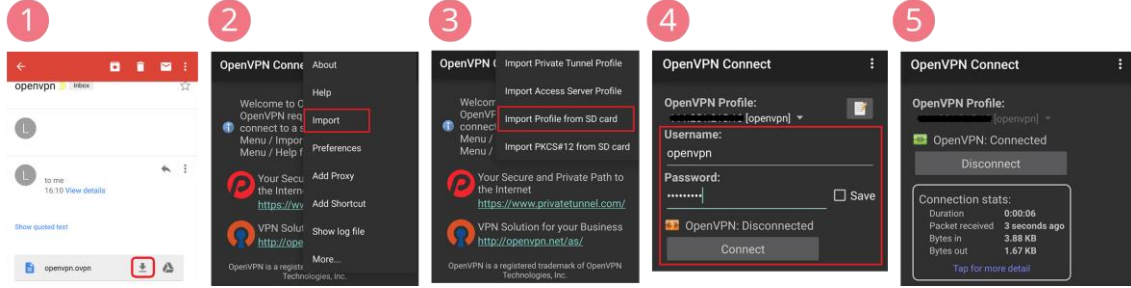
1. Yeni profil ekleyin ve VPN türü OpenVPN'i seçin.
2. openvpn.ovpn'yi Smart VPN istemcisine aktarın.
3. Kullanıcı Adı ve Parolayı girin, ardından kaydetmek için Tamam'a tıklayın.
4. Bağlan düğmesini değiştirin ve ardından bağlantı kurulduktan sonra VPN durumunu kontrol edebiliriz.



OpenVPN Connect ile Android'den bağlanma

1. OpenVPN Connect'i Play mağazasından indirin. Yapılandırma dosyasını Android cihaza gönderin, burada mail ile gönderiyoruz, ardından cihaza indiriyoruz.
2. İstemci yapılandırma dosyasını içe aktarın: OpenVPN Connect'i açın, ardından uygulamanın sağ üst tarafındaki menü simgesine dokununuz.
3. Profili SD karttan içe aktar'ı seçin ve istemci yapılandırma dosyasını seçin.
4. VPN bağlantısı kurun, Kullanıcı Adı ve Parolayı girin, ardından Bağlan'a dokununuz.

5. Bağlantı kurulduktan sonra VPN durumunu kontrol edebiliriz.



Linux'tan Bağlanma (Ubuntu)

1. Yapılandırma dosyasını yönlendiriciden indirin ve CLI'yi çalıştırın.
2. Yapılandırma dosyasının bulunduğu dizine gidin
3. OpenVPN paketini komutla kurunsudo apt-get install openvpn
4. OpenVPN'i komutla bağlayınsudo openvpn --config [openvpn config filename]
5. Kullanıcı adını ve şifreyi girin

```

louis@louis-VirtualBox: ~/Downloads
louis@louis-VirtualBox:~$ cd Downloads
louis@louis-VirtualBox:~/Downloads$ sudo apt-get install openvpn
[sudo] password for louis:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  easy-rsa
The following NEW packages will be installed:
  openvpn
0 upgraded, 1 newly installed, 0 to remove and 103 not upgraded.
Need to get 0 B/391 kB of archives.
After this operation, 1,008 kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously unselected package openvpn.
(Reading database ... 201046 files and directories currently installed.)
Preparing to unpack ../openvpn_2.3.2-7ubuntu3.2_amd64.deb ...
Unpacking openvpn (2.3.2-7ubuntu3.2) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up openvpn (2.3.2-7ubuntu3.2) ...
* Restarting virtual private network daemon(s)...
* No VPN is running.
Processing triggers for libc-bin (2.19-0ubuntu6.14) ...
louis@louis-VirtualBox:~/Downloads$
louis@louis-VirtualBox:~/Downloads$ sudo openvpn --config test.ovpn
Thu Jun 21 17:16:04 2018 OpenVPN 2.3.2 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[EPOLL] [PKCS11] [eurephia] [MH] [IPv6] built on Jun 22 2017
Enter Auth Username:dray
Enter Auth Password:
Thu Jun 21 17:16:34 2018 Initialization Sequence Completed
  
```