

Android Smart VPN İstemcisinden Vigor Router'a OpenVPN

Android Smart VPN Client artık OpenVPN protokolünü destekliyor. Bu belge, OpenVPN'in Android Smart VPN Client'tan Vigor Router'a nasıl kurulacağını gösterecektir.

Vigor Router

1. VPN and Remote Access >> Remote Access Control'e gidin ve OpenVPN Hizmetinin etkinleştirildiğinden emin olun.

VPN and Remote Access >> Remote Access Control

Remote Access Control Setup	Bind to WAN
<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	
<input checked="" type="checkbox"/> Enable OpenVPN Service	

Note:
To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT [Open Ports](#) or [Port Redirection](#) is also configured.

OK Clear Cancel

2. Bir Remote Dial-In User profili oluşturun: VPN and Remote Access >> Remote Dial-In User seçeneğine gidin , profili düzenlemek için mevcut bir dizine tıklayın.

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: [Set to Factory Default](#)

View: All Online Offline

Index	Enable	User	Status	Index	Enable	User	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"/>	???	---
5.	<input type="checkbox"/>	???	---	21.	<input type="checkbox"/>	???	---

3. Profili aşağıdaki gibi düzenleyin:
 - a. Etkinleştir'i işaretleyin
 - b. İzin verilen çevirmeli bağlantı türü için OpenVPN tünelini etkinleştirin
 - c. Bir Kullanıcı Adı ve Şifre Verin
 - d. Kaydetmek için Tamam'ı tıklayın

VPN and Remote Access >> Remote Dial-in User

Index No. 1

<input checked="" type="checkbox"/> Enable this Account <input checked="" type="checkbox"/> Multiple Concurrent Connections Allowed Idle Timeout: 300 second(s)	User Account and Authentication Username: openvpn Password: ***** <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) <input type="checkbox"/> Enable Time-based One-time Password(TOTP) <input type="button" value="Regenerate"/>
Allowed Dial-In Type <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> IKEv1/IKEv2 <input type="checkbox"/> IKEv2 EAP <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy: Must <input type="checkbox"/> SSL Tunnel <input checked="" type="checkbox"/> OpenVPN Tunnel	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key: _____ Max: 128 characters <input type="checkbox"/> Digital Signature(X.509) None
<input type="checkbox"/> Specify Remote Node Remote Client IP: _____ or Peer ID: _____ 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 type="checkbox"/> DES <input type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional): _____
Subnet: LAN 1 <input type="checkbox"/> Assign Static IP Address 0.0.0.0	Schedule Profile (None) (None) (None) (None)
Two-Factor Authentication <input type="checkbox"/> Send Authentication Code via Email <input type="checkbox"/> Send Authentication Code via SMS <input type="checkbox"/> Time-based One-time Password (TOTP) <input type="button" value="Regenerate"/> <input type="button" value="Reset"/> Secret: <input type="text"/> <input type="button" value="Leave blank to let user define"/> <input type="button" value="Copy"/>	Notification <input type="checkbox"/> Send Email when VPN is up Email Object: 1-??? Mail to: _____ <input type="checkbox"/> Send SMS when VPN is up SMS Object: 1-??? SMS to: _____

Note:
 1. Username can not contain characters '.' and '\\.
 2. When you are trying to use OpenVPN tunnel and the router is behind NAT, you may have to enable the **VPN-Matcher** feature to bypass the NAT.
 3. VPN-Matcher can only be used behind Cone NAT.

4. Sistem Bakımı >> Saat ve Tarih sayfasına giderek yönlendiricideki saatin doğru olduğunu onaylayın .

System Maintenance >> Time and Date

Time Information

Current System Time	2022 Sep 5 Mon 6 : 23 : 22	<input type="button" value="Inquire Time"/>
---------------------	----------------------------	---

Time Setup

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time	
Primary Server	pool.ntp.org
Secondary Server	
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	<input type="checkbox"/> <input type="button" value="Advanced"/>
Automatically Update Interval	30 mins
Send NTP Request Through	Auto

5. VPN and Remote Access >> Open VPN >> OpenVPN Sunucu Kurulumu sayfasına gidin .

- OpenVPN bağlantıları için kullanmak istediğiniz protokole bağlı olarak TCP Modunu veya UDP Modunu etkinleştirin.
- İsterseniz TCP Bağlantı Noktasını ve UDP Bağlantı Noktasını özelleştirin.

VPN and Remote Access >> OpenVPN



OpenVPN Server Setup | Client Config | Import Certificate

General Setup

UDP	<input checked="" type="checkbox"/> Enable
UDP Port	<input type="text" value="1194"/>
TCP	<input checked="" type="checkbox"/> Enable
TCP Port	<input type="text" value="1194"/>
Cipher Algorithm	<input type="text" value="AES256"/>
HMAC Algorithm	<input type="text" value="SHA256"/>
Certificate Authentication	<input checked="" type="checkbox"/>

6. Sertifikalar oluřturun.

- Yönlendirici tarafından oluřturulan sertifikaları seçin .
- Oluřtur'u tıklayın .
- Tamam'ı tıklayın .

Certificates Setup

Certificate Source

Router generated certificates
 Uploading certificates to Router

Generated certificates

Root Certificate: [Openvpn Root CA](#)
Server Certificate: [openvpn server](#)
Client Certificate: [openvpn client](#)
Trust Certificate: [Trusted CA-3](#)

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

7. VPN and Remote Access >> Open VPN >> Client Config sayfasına gidin .

- OpenVPN bağlantısına izin veren WAN arayüzünü seçin
- Kullanmak istediğiniz Protokolü seçin
- Bir Yapılandırma Dosyası Adı Verin
- VPN Yapılandırma Dosyasını kaydetmek ve OpenVPN istemci cihazına göndermek için Dışa Aktar'ı tıklayın.

VPN and Remote Access >> OpenVPN



OpenVPN Server Setup	Client Config	Import Certificate
Remote Server	<input type="radio"/> IP WAN1 <input type="radio"/> Domain <input type="radio"/> VPN Matcher	<input type="text" value="192.168.1.1"/> <input type="text" value="192.168.1.1"/>
Transport Protocol	UDP	
Auto Dial-Out	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Set VPN as Default Gateway	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Cache password for auto reconnect	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
UDP Ping	<input type="text" value="10"/> Seconds(s)	
UDP Ping exit	<input type="text" value="60"/> Seconds(s)	
File Name	<input type="text" value="openvpn"/> .ovpn	
Mail Profile	<input type="text" value="1 - ???"/>	<input type="text" value=""/> <input type="button" value="Send Email"/>

Note:

1. Please make sure the Client cert and the Client key are located in the same folder with .ovpn file.
2. Please make sure that WAN can be used as OpenVPN server.
3. Cache password for auto reconnect.
Enabled: Cache password in virtual memory for re-authentication to keep VPN always connected.
Disabled: Type password manually when re-authentication needed. VPN may disconnect during re-authentication.

8. Certificate Management >> Local Services List sayfasına gidin ve openvpn sunucu sertifikasının OpenVPN Hizmetine uygulanıp uygulanmadığını kontrol edin.

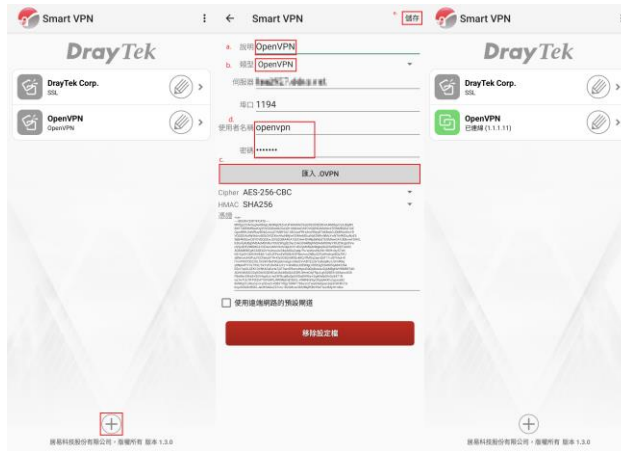
Certificate Management >> Local Services List

Default Certificate

Certificate Name	Local Services
Default Certificate	Router Management -- Web Access from LAN or WAN
	Router Management -- SSH
	VPN and Remote Access >> LAN to LAN -- SSL VPN
	VPN and Remote Access >> Remote Dial-in User -- SSL VPN
	Hotspot Web Portal
	Applications >> Internal RADIUS
	Applications >> Local 802.1X General Setup
	Applications >> High Availability
	CSM >> DNS Filter -- block page
	USB Application >> USB User Management
DrayDDNS (Global)	
openvpn client	
openvpn server	VPN and Remote Access >> OpenVPN -- OpenVPN
None	VPN and Remote Access >> IPsec General Setup

OpenVPN'i Android Smart VPN İstemcisinden Bağlama

1. Yeni bir VPN profili oluşturun.
2. Profili aşağıdaki gibi düzenleyin:
 - a. Açıklamayı girin
 - b. VPN Türü olarak OpenVPN'i seçin
 - c. Vigor Router'dan dışa aktarılan OpenVPN Yapılandırma Dosyasını içe aktarın
 - d. Kullanıcı Adı ve Parolayı Girin
 - e. Kaydet'e tıklayın
3. Bağlantıyı çevirin.



Not:

- Bu uygulamayı henüz yüklemiyorsanız, Smart VPN istemcisi sizi Android için OpenVPN indirmeye yönlendirecektir.
- Android için OpenVPN sürümünüz 0.7.30 veya üzeri ise, Vigor Router ile uyumluluk sorununu karşılayacaktır. Lütfen Android Uygulaması için OpenVPN >> AYARLAR'a gidin, uyumluluk sorununu iyileştirmek için OpenVPN 3 Core seçeneğini etkinleştirin.

