

## ANDROID TELEFONLARDAN VIGOR ROUTER'A SSL VPN

Bu makale Vigor Router'ın Internet istemcileri, özellikle Android akıll telefonların local ağa bir SSL VPN tüneli üzerinden erişebilmesi için SSL VPN ağ geçidi olarak nasıl ayarlanacağını göstermektedir. Makalede routera için gereken yalındırmanın yanı sıra, DrayTek tarafından sağlanan ücretsiz VPN istemci uygulaması olan SmartVPN'i kullanarak Android'den SSI VPN bağlantısının nasıl başlatılacağını gösteriyoruz.

## Vigor Router Üzerinde Kurulum

## DrayOS

1. Router'ın internete bağlı olduğundan ve internetteki VPN istemcilerinin erişebilmesi için ortak bir WAN IP adresine sahip olduğundan emin olun.
2. **VPN and Remote Access >> Remote Access Control** sayfasına gidin ve "SSL VPN Service"nin etkin olduğundan emin olun.

## VPN and Remote Access &gt;&gt; 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

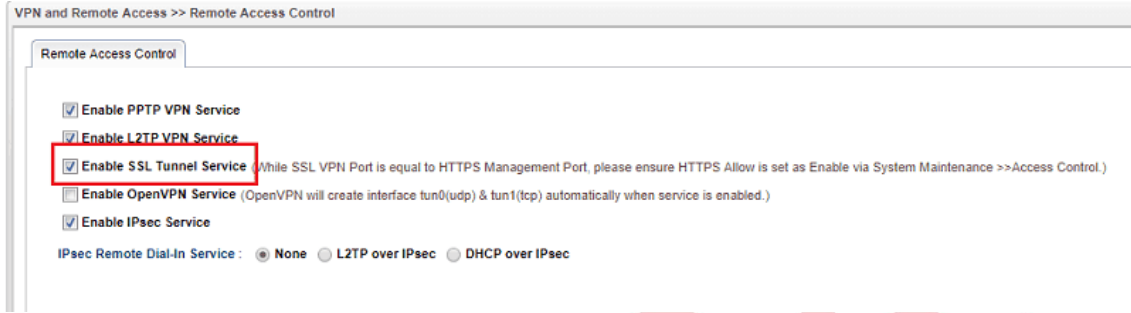
3. SSL VPN istemcileri için kullanıcı profilleri oluşturun. **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin ve profili aşağıdaki adımlardaki gibi ekleyin.
  - **Allowed Dial-In Type** sekmesinde "SSL Tunnel"i etkinleştirin.
  - **Username** ve **Password** girin.
  - Profili kaydetmek için **OK**'a tıklayın.

## VPN and Remote Access &gt;&gt; Remote Dial-in User

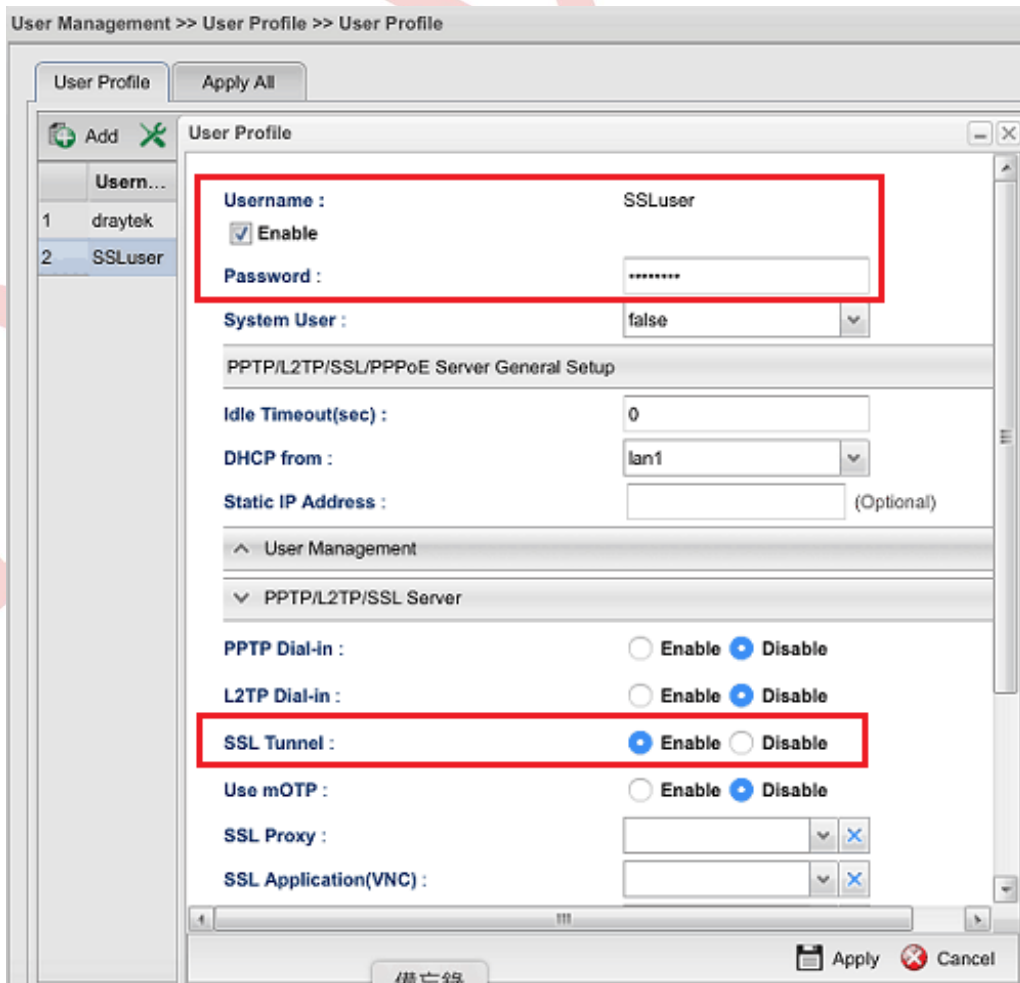
<b>Index No. 5</b>	
<b>User account and Authentication</b>	
<input checked="" type="checkbox"/> Enable this account	<b>Username</b> SSLuser
Idle Timeout 0 second(s)	<b>Password(Max 19 char)</b> .....
<b>Allowed Dial-In Type</b>	
<input type="checkbox"/> PPTP	<input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)
<input type="checkbox"/> IPsec Tunnel	<b>PIN Code</b> .....
<input type="checkbox"/> L2TP with IPsec Policy None	<b>Secret</b> .....
<input checked="" type="checkbox"/> SSL Tunnel	<b>IKE Authentication Method</b>
<input type="checkbox"/> Specify Remote Node	<input checked="" type="checkbox"/> Pre-Shared Key
<b>Remote Client IP</b>	<b>IKE Pre-Shared Key</b> .....
or Peer ID .....	<input type="checkbox"/> Digital Signature(X.509)
<b>Netbios Naming Packet</b> <input checked="" type="radio"/> Pass <input type="radio"/> Block	<b>IPsec Security Method</b>
<b>Multicast via VPN</b> <input type="radio"/> Pass <input checked="" type="radio"/> Block	<input checked="" type="checkbox"/> Medium(AH)
(for some IGMP,IP-Camera,DHCP Relay..etc.)	<b>High(ESP)</b> <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
<b>Subnet</b>	<b>Local ID (optional)</b> .....
<b>LAN 1</b>	
<input type="checkbox"/> Assign Static IP Address	
0.0.0.0	

## Linux

1. Router'ın internete bağlı olduğundan ve internetteki VPN istemcilerinin erişebilmesi için ortak bir WAN IP adresine sahip olduğundan emin olun.
2. **VPN and Remote Access >> Remote Access Control** sayfasına gidin ve “SSL VPN Service”in etkin olduğundan emin olun.



3. SSL VPN istemcileri için kullanıcı profilleri oluşturun. **User Management >> User Profile**'a gidin ve **Add**'e tıklayın.
  - **Enable**'yi etkinleştirin.
  - **Username** ve **Password** girin.
  - PPTP/L2TP SSL Server'da, **SSL Tunnel** için “Enable” seçeneğini seçin.
  - Profili kaydetmek için **Apply**'a tıklayın.



### Android Telefonlarda SSL VPN Kurulumu

1. Smart VPN uygulamasını Google Play'den indirin ve kurun.
2. Uygulamayı başlatın ve yeni bir profil eklemek için "+"ya dokununuz.



3. Profili aşağıdaki gibi ayarlayın.
  - Bu bağlantı için bir **Description** (açıklama) girin.
  - **Server**'da routerin WAN IP'sini girin.
  - Routerin SSL VPN için varsayılan olarak kullandığı 443 portunu **Port**'a girin.
  - Profili kaydetmek için **SAVE**'e tıklayın.

SmartVPN

SAVE

Description SSL VPN

Server 192.168.195.100

Port 443

Automatically get IP and DNS server address

Manually set IP and DNS server address

Manually set DNS server address

IP Address e.g. 192.168.1.150

DNS Server e.g. 8.8.8.8

Enable SSL 3.0

Enable server certificate authentication

Use default gateway on remote network

More Route e.g. 172.16.1.0/24

Note: We recommend keeping SSL 3.0 disabled to protect against SSLv3 vulnerabilities including POODLE attacks, but the remote SSL server must support TLS 1.0.

Not:

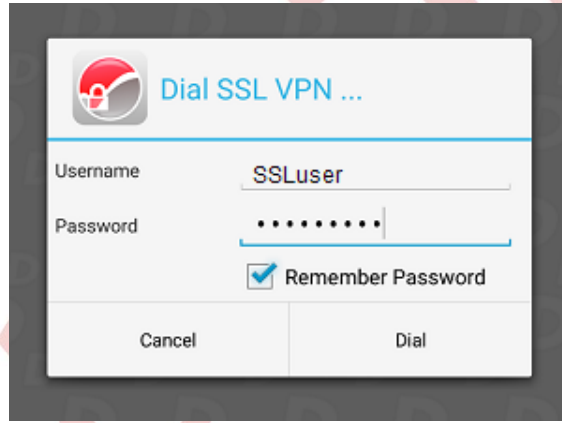
Sunucu sertifikası doğrulamasını etkinleştirmek için önce ilgili Root CA'yı yüklemeniz gerekir.

Uzak ağda varsayılan ağ geçidi kullan seçeneğini işaretlerseniz VPN bağlantıya tüm internet trafiği VPN yönlendiricisine gönderilir.

1. SSL VPN bağlantısını başlatmak için profile dokunun.



2. Routerın kullanıcı profilinde ayarlanan **Username** ve **Password**'ü girin. Arından **Dial**'e dokunun.



3. VPN bağlandığında profilin rengi yeşile dönecektir. Profile tekrar dokununca bağlantı kesilecektir.



4. Profili düzenlemek veya kaldırmak için kalem simgesine dokunun.

