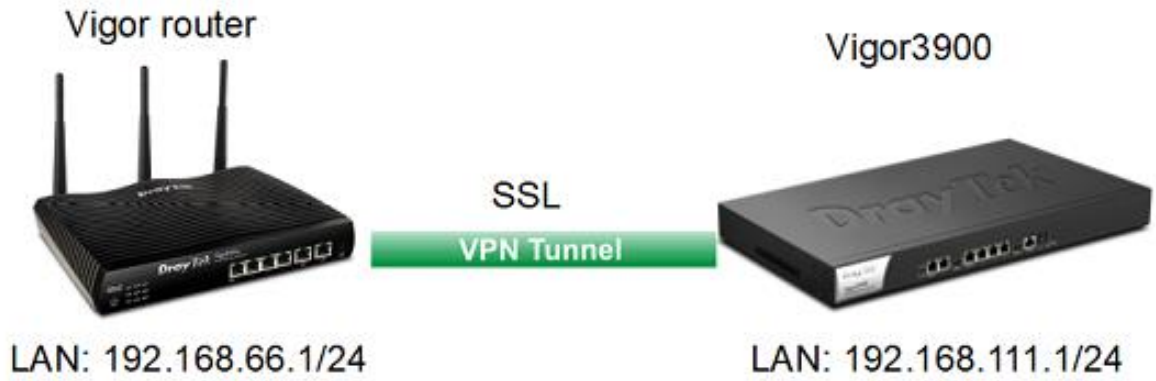


## DRAYOS ROUTER VE VIGOR3900 ARASINDA SSL VPN

Bu makalede, aşağıdaki topoloji tarafından DrayOS Router (Vigor router) ve Vigor3900 / 2960 arasında LAN to LAN SSL VPN gösterilmektedir. DrayOS Router ve Vigor3900 / 2960, VPN sunucusu ve istemcisi olabilir. Bu nedenle, sırasıyla VPN sunucusu olarak kullanıldığında Vigor Router ve Vigor3900 / 2960 arasında SSL VPN bağlantısının nasıl kurulacağını göstermek için bu makaleyi iki bölüme ayırdık.

(TwoVigor Routerlar veya iki Vigor3900 arasında SSL VPN tüneli için İki Vigor Router Arasında SSL VPN makalesine başvurun.)

<https://youtu.be/yEPs6bn3qAs> adresinden makalenin videosuna ulaşabilirsiniz.



VPN yapılandırmasını yapmadan önce, lütfen routerdaki VPN and Remote Access >> Remote Access Control sayfasındaki SSL VPN hizmetinin etkin olduğundan emin olun, böylece SSLVPN, VPN sunucusu rolünü üstlenir.

### 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

#### 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

Not: Vigor3900 / 2960'ı SSL VPN sunucusu olarak kullanıyorsanız, SSL VPN ve HTTPS'nin varsayılan port olarak 443 numaralı bağlantı noktasını kullanması nedeniyle, System Maintenance >> Access Control sayfasında HTTPS erişimine izin vermek gerekir.

System Maintenance >> Access Control >> Access Control

Access Control | Fail to Ban | Access Barrier

Default: Disable Auto-Logout :  Enable  Disable

Use Validation Code :  Enable  Disable

Customized Login Image :  Enable  Disable

Enforce HTTPS Management :  Enable  Disable

Internet Access Control

Apply to WAN Interface : wan1, wan2, wan3,...

Web Allow :  Enable  Disable

Telnet Allow :  Enable  Disable

SSH Allow :  Enable  Disable

**HTTPS Allow :  Enable  Disable**

SSL Proxy Allow :  Enable  Disable

FTP Allow :  Enable  Disable

SAMBA Allow :  Enable  Disable

TR069 Allow :  Enable  Disable

Server Certificate : Default

Access List :  Enable  Disable

Alternatif olarak, HTTPS veya SSL VPN bağlantı noktasını değiştirebilir, ardından SSL VPN bağlantısını etkilemeden HTTPS erişimini devre dışı bırakabilirsiniz.

Management Port Setup

Web Port :	80	Default:80
Telnet Port :	23	Default:23
SSH Port :	22	Default:22
<b>HTTPS Port :</b>	<b>443</b>	<b>Default:443</b>
SSL Proxy Port :	44300	Default:44300
<b>SSL VPN Port :</b>	<b>443</b>	<b>Default:443</b>
FTP Port :	21	Default:21

SSL VPN portu, Vigor Routerların SSL VPN >> General Setup sayfasında yapılandırılabilir.

## SSL VPN &gt;&gt; General Setup

## SSL VPN 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
Port	8443 (Default: 443)			
Server Certificate	self-signed			

## Note:

- The settings will act on all SSL applications.
- Please go to [System Maintenance >> Self-Signed Certificate](#) to generate a new "self-signed" certificate.

OK

Cancel

## Bölüm A: Vigor Router'ı VPN sunucusu olarak alın

## Vigor Router Ayarı (Dial-in):

- VPN and Remote Access Control >> LAN to LAN seçeneğine gidin ve uygun bir index numarasına tıklayın.
- Dial-In Ayarlar
  - Profil adını girin.
  - Enable this profile'i etkinleştirin.
  - Call Direction olarak Dial-in seçeneğini seçin.

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

## Profile Index : 4

## 1. Common Settings

Profile Name	SSLin	Call Direction	<input type="radio"/> Both	<input type="radio"/> Dial-Out	<input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile		Tunnel Mode	<input type="radio"/> GRE Tunnel		
VPN Dial-Out Through	WAN1 First	<input type="checkbox"/> Always on	Idle Timeout		
	1-11 111 1111*	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	0 second(s)		
Netbios Naming Packet	<input checked="" type="radio"/> Pass	<input type="radio"/> Block	PING to the IP		
Multicast via VPN	<input type="radio"/> Pass	<input checked="" type="radio"/> Block			
(for some IGMP,IP-Camera,DHCP Relay..etc.)					

- Allowed Dial-In Type sekmesinde SSL Tunnel'i işaretleyin.
- Username ve Password girin.

## 3. Dial-In Settings

Allowed Dial-In Type	Username	SSLuser
<input type="checkbox"/> PPTP	Password(Max 11 char)	*****
<input type="checkbox"/> IPsec Tunnel	VJ Compression	<input checked="" type="radio"/> On
<input type="checkbox"/> L2TP with IPsec Policy	None	
<input checked="" type="checkbox"/> SSL Tunnel	IKE Authentication Method	
<input type="checkbox"/> Specify Remote VPN Gateway	<input checked="" type="checkbox"/> Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
or Peer ID	<input type="checkbox"/> Digital Signature(X.509)	
	None	
	Local ID	
	<input checked="" type="radio"/> Alternative Subject Name First	
	<input type="radio"/> Subject Name First	
	IPsec Security Method	
	<input checked="" type="checkbox"/> Medium(AH)	
	High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	

- f. Remote Network IP/Mask'da Vigor3900'ün LAN'ını girin.
- g. OK'a tıklayın.

#### 5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	Route
Remote Network IP	192.168.111.1	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> Change default route to this VPN tunnel ( Only active if one single WAN is up )	
Local Network IP	192.168.66.1		
Local Network Mask	255.255.255.0		
	More		

OK Clear Cancel

#### Vigor3900 Ayarı (Dial-out):

1. VPN and Remote Access >> VPN Profiles sayfasına gidin ve SSL Dial-out sekmesinde Add'e tıklayın.
  - a. Profil adını girin.
  - b. Profili etkinleştirmek için "Enable" yi işaretleyin.
  - c. Dial-Out için WAN ara yüzünü seçin.
  - d. Sunucu IP / Host adına Vigor Router'ın WAN IP adresini veya domain adını ve SSL VPN portunu girin.
  - e. SSL Username ve Password girin.
  - f. Local IP / Subnet Mask'inde Vigor3900'ün LAN'ını girin.
  - g. Remote IP / Subnet Mask'inde Vigor Router'ın LAN'ını girin.
  - h. Apply'a tıklayın.

VPN and Remote Access >> VPN Profiles >> SSL Dial-out

IPsec PPTP Dial-out PPTP Dial-in SSL Dial-out SSL Dial-in GRE

Add Edit Delete Rename Refresh

SSL Dial-out

Profile : SSLout

Enable

Always On :  Enable  Disable

Dial-Out Through : wan3  Default WAN IP  WAN Alias IP

Fallover to :

Idle Timeout (sec) : 0 (Optional)

Server IP/Host Name : vpn.server.net:8443

SSL User Name : SSLUser

SSL Password : .....

Local IP / Subnet Mask : 192.168.111.1 255.255.255.0/24

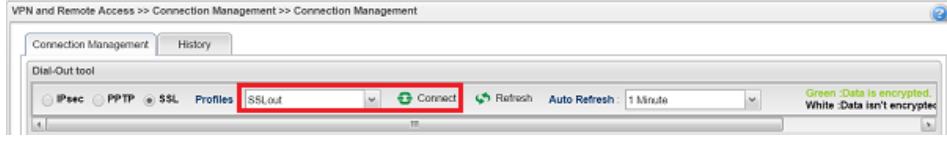
Add Save Profile Number Limit :

Remote IP / Subnet Mask	IP	Subnet Mask
192.168.66.1	192.168.66.1	255.255.255.0

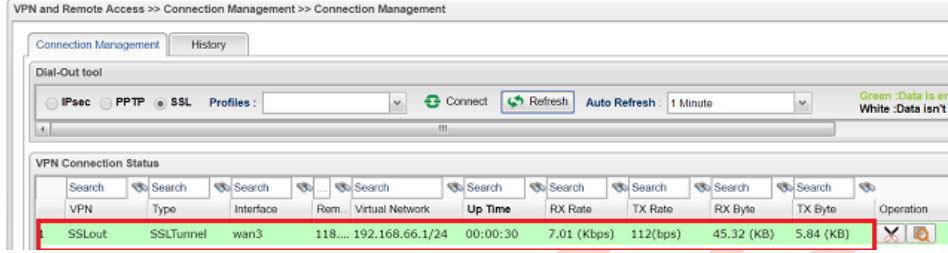
Route / NAT Mode : Route

Netlink Namings Packet  Enable  Disable

Artık VPN bağlantısı için VPN and Remote Access >> Connection Management sayfasına gidebiliriz.



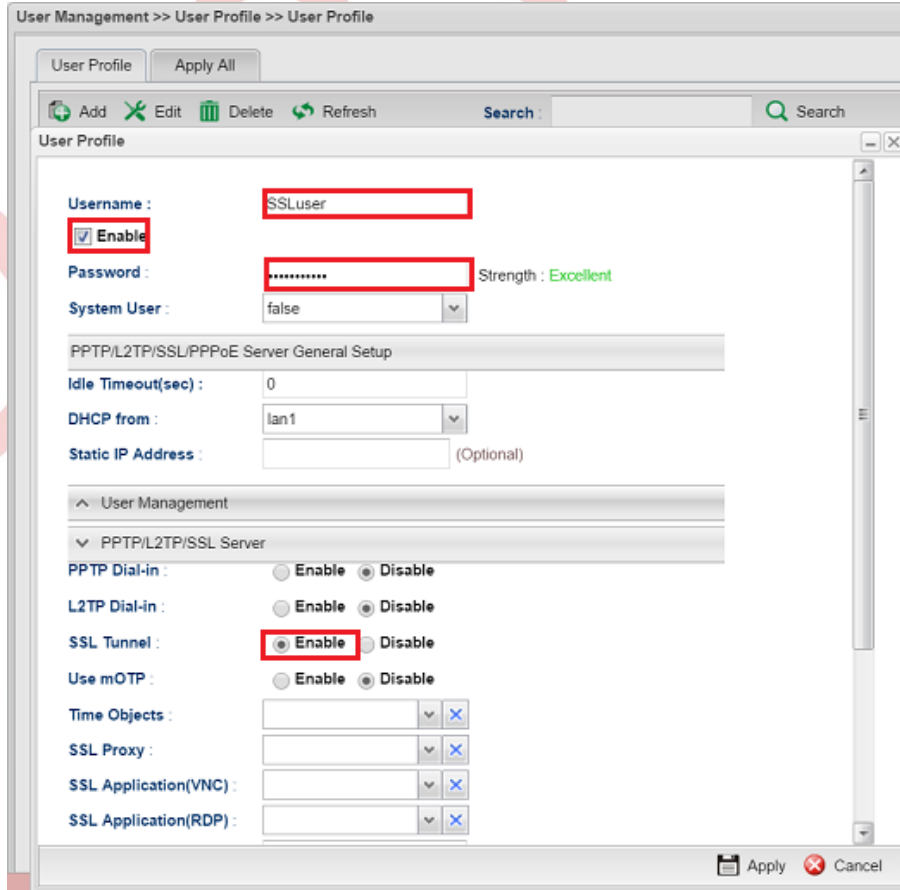
VPN başarıyla bağlandıktan sonra VPN durumunu aşağıdaki gibi görebiliriz.



## Bölüm B: Vigor3900'ü VPN sunucusu olarak alın.

### Vigor3900 Ayarı (Dial-in):

1. User Management >> User Profiles'a gidin ve Add'e tıklayın.
2. Dial-In Ayarları
  - a. Username ve Password girin.
  - b. Profili etkinleştirmek için "Enable" yi işaretleyin.
  - c. PPTP / L2TP / SSL Server bölümünde SSL Dial-in'i etkinleştirin.
  - d. Apply'a tıklayın.





3. VPN and Remote Access >> VPN Profiles'a gidin ve SSL Dial-in sekmesinde Add'e tıklayın.
  - a. Bir profil adı girin ve Enable'yi işaretleyin.
  - b. SSL VPN bağlantısı için SSL Username seçeneklerinde kullanıcı profilini seçin.
  - c. Local IP/Subnet Mask'ında Vigor3900'ün LAN'ını girin.
  - d. Remote IP/Subnet Mask'ında Vigor Router'ın LAN'ını girin.
  - e. Apply'a tıklayın.

### Vigor Router Ayarı (Dial-Out):

1. VPN and Remote Access Control >> LAN to LAN seçeneğine gidin ve uygun bir index numarasına tıklayın.
2. Dial-In Ayarlar
  - a. Profil adını girin.
  - b. Enable this profile'i etkinleştirin.
  - c. Call Direction olarak Dial-in seçeneğini seçin.
  - d. Allowed Dial-In Type sekmesinde SSL Tunnel'i işaretleyin.
  - e. Server IP / Host Adına Vigor3900'ün WAN IP'sini veya domain adını girin.
  - f. Username ve Password girin.
  - g. Remote Network IP / Mask'a Vigor3900'ün LAN'ını girin.
  - h. OK'a tıklayın.

3. Dial-In Settings

<p><b>Allowed Dial-In Type</b></p> <p><input type="checkbox"/> PPTP</p> <p><input type="checkbox"/> IPsec Tunnel</p> <p><input type="checkbox"/> L2TP with IPsec Policy <span>None</span></p> <p><input checked="" type="checkbox"/> <b>SSL Tunnel</b></p> <p><input type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP</p> <p>or Peer ID</p>	<p>Username <span>SSLUser</span></p> <p>Password(Max 11 char) <span>*****</span></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p><b>IKE Authentication Method</b></p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key</p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <p><b>IPsec Security Method</b></p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>
---	--

Artık VPN bağlantısı için VPN and Remote Access >> Connection Management sayfasına gidebiliriz.

#### VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 ▾ Refresh

General Mode:	( SSLout ) 192.168.1.100	▾ Dial
Backup Mode:		▾ Dial
Load Balance Mode:		▾ Dial

VPN başarıyla bağlandıktan sonra VPN durumunu aşağıdaki gibi görebiliriz.

#### 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 ( Server )	SSL Tunnel	192.168.1.100		103	151	148	1052	0:1:33	Drop

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.