

İKİ VIGOR ROUTER ARASINDA SSL VPN

Bu makale, iki Vigor Router arasında nasıl SSL VPN tüneli kurulacağını tanıtmaktadır. (Vigor Yönlendirici ve Vigor3900 arasında SSL VPN tüneli için DrayOS Router ve Vigor3900 arasında SSL VPN makalesine başvurun.)

İki Vigor Router arasında

LAN to LAN SSL VPN özelliği, Vigor2860 serisi 3.8.1 firmware ve Vigor2925 serisi 3.8.2 firmware versiyonundan başlar. Diğer modellerde olduğu gibi, özelliklerine bakın.



VPN Server (Dial-in Site) Kurulumu

1. LAN to LAN VPN Profili oluşturun: VPN and Remote Access >> LAN to LAN sayfasına gidin. Bir profil eklemek / düzenlemek için uygun bir indexe tıklayın.

VPN and Remote Access >> LAN to LAN



LAN-to-LAN Profiles:

| [Set to Factory Default](#) |View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---

2. Profili aşağıdaki gibi ayarlayın:
 - a. Profil adı girin.
 - b. "Enable this profile" ı etkinleştirin.
 - c. Call Direction için Dial-in seçeneğini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Server"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	PING to the IP <input type="text"/>

- d. Allwed Dial-In Type için "SSL Tunnel" i işaretlediğinizden emin olun.
- e. Username ve Password girin.
- f. Remote Network IP/Mask için VPN istemcisinin LAN IP'sini ve Subnet Mask'ını girin.
- g. Kaydetmek için 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	
Remote Network IP	192.168.2.1	Route	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Local Network IP	192.168.1.1	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network Mask	255.255.255.0		
More			

3. Enable SSL VPN Service'in işaretli olduğundan emin olmak için VPN and Remote Access >> Remote Access Control sayfasına gidin.

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

VPN Client (Dial-out Site) Kurulumu

4. LAN to LAN profili oluşturun: VPN and Remote Access >> LAN to LAN sayfasına gidin ve uygun bir index numarasına tıklayın.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

[Set to Factory Default](#)View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---

5. VPN profilini aşağıdaki gibi ayarlayın:
- Profil adı girin.
 - Enable this profile'ı etkinleştirin.
 - Call Direction için "Dial-out" seçeneğini seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	Client	Call Direction	<input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile		<input type="checkbox"/> Always on	
VPN Dial-Out Through	WAN1 First	Idle Timeout	300 second(s)
Netbios Naming Packet	<input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	
Multicast via VPN	<input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP	
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

- Type of Server I am Calling sekmesinde “SSL Tunnel” seçeneğini seçin.
- Adım 2’deki VPN istemcisi için girilen Username ve Password’u girin.
- Server IP/Host Name için VPN Server’ın WAN IP’sini girin.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None <input checked="" type="radio"/> SSL Tunnel	Username <input type="text" value="draytek"/> Password(Max 15 char) <input type="password" value="....."/> PPP Authentication <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/>
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="100.100.100.100"/> Server Port (for SSL Tunnel): <input type="text" value="443"/>	

- Remote Network IP/Mask için VPN Server’ın LAN’ını girin. (Bunun 2. Adımda Local Network IP/Mask ayarıyla aynı olması gerektiğini unutmayın.)
- Kaydetmek için OK’a tıklayın.

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.1.1"/> Remote Network Mask <input type="text" value="255.255.255.0"/> Local Network IP <input type="text" value="192.168.2.1"/> Local Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="Disable"/> From first subnet to remote network, you have to do <input type="text" value="Route"/> <input type="checkbox"/> IPsec VPN with the Same Subnets <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	--

VPN Tünelini kurma:

- VPN Dial için VPN istemcisinde VPN and Remote Access >> Connection Management sayfasına gidin. Daha önce oluşturulmuş profili seçin ve “Dial” e tıklayın.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : <input type="text" value="10"/> <input type="button" value="Refresh"/> General Mode: <input type="text" value="(Client) 100.100.100.100"/> <input type="button" value="Dial"/> Backup Mode: <input type="text" value=""/> <input type="button" value="Dial"/> Load Balance Mode: <input type="text" value=""/> <input type="button" value="Dial"/>
--

- Tüm kimlik bilgileri Network yöneticisi ise kurulan VPN’i ve çalışma süresini VPN and Remote Access >> Connection Management sayfasından kontrol edebilir.

VPN Connection Status

Current Page: 1

Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1 (Server)	SSL Tunnel	100.100.100.100	192.168.2.1/24	103	151	148	1052	0:1:33 <input type="button" value="Drop"/>

xxxxxxx : Data is encrypted.

xxxxxxx : Data isn't encrypted.

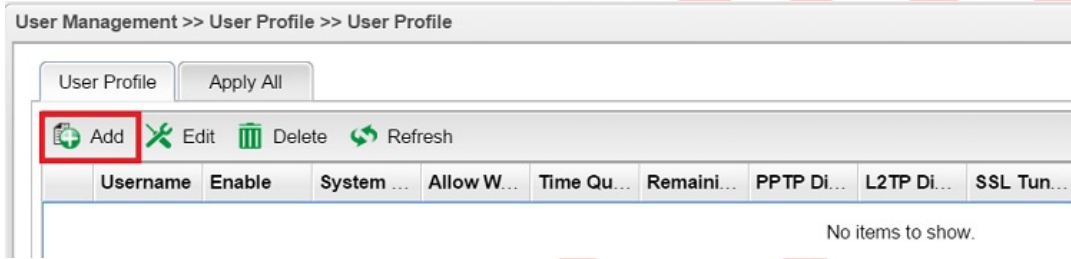
İki Vigor3900'ler arasında

Firmware 1.1.0 veya üst versiyonundan beri Vigor2960 ve Vigor3900 LAN-to-LAN SSL VPN'i desteklemektedir. Bu dokümanda, iki Vigor2960 veya Vigor3900 arasında LAN-to-LAN SSL VPN'in nasıl kurulacağı gösterilmektedir.

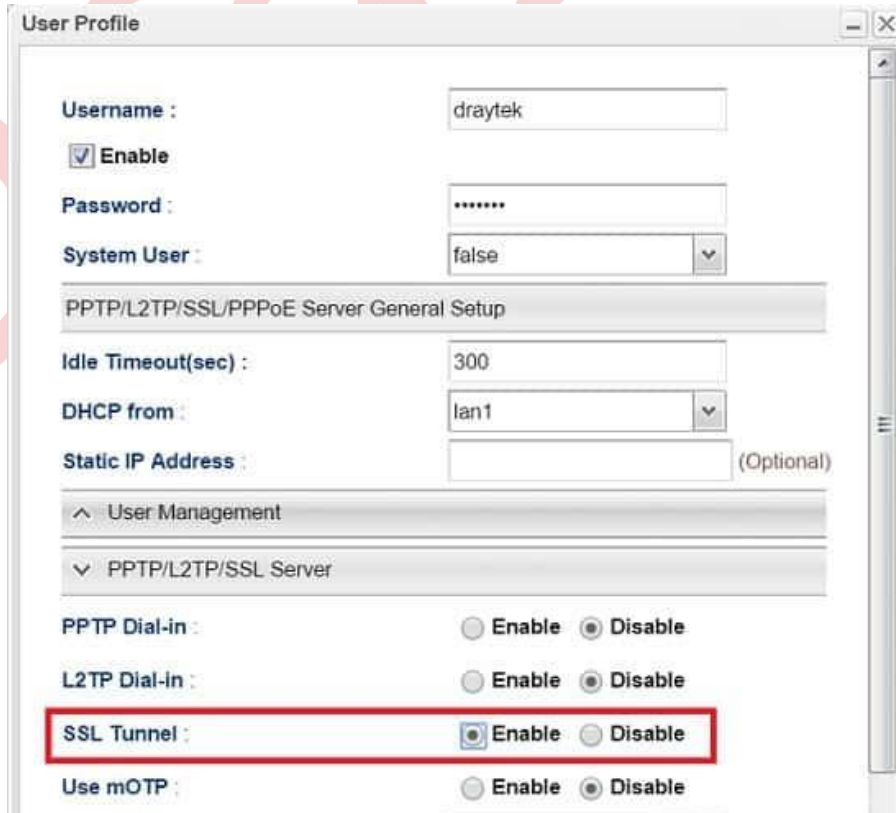


VPN Server (Dial-in Site) Kurulumu

1. SSL VPN girişi için kullanıcı profili oluşturun. User Management >> User Profile sayfasına gidin. Yeni bir profil oluşturmak için Add'e tıklayın.



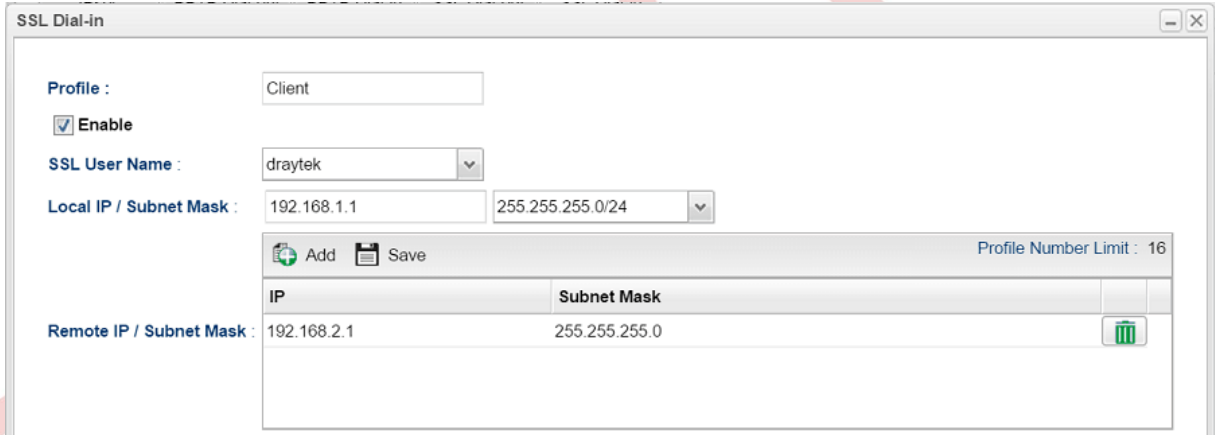
2. Profili aşağıdaki gibi ayarlayın.
 - a. Profil adı girin.
 - b. "Enable this profile" ı etkinleştirin.
 - c. Password girin.
 - d. PPTP/L2TP/SSL Server sekmesinde SSL Tunnel için "Enable" seçeneğini seçin.
 - e. Kaydetmek için "Save" e tıklayın.



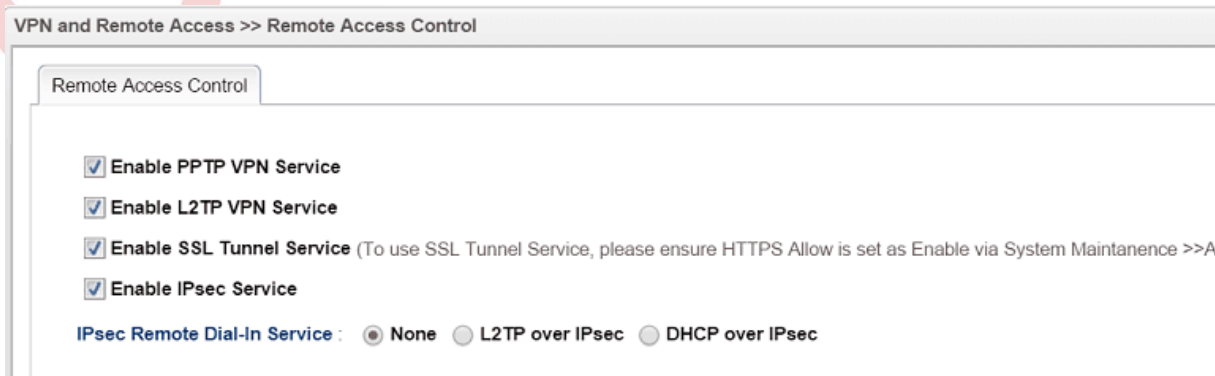
3. VPN profili oluşturun: VPN and Remote Access >> VPN Profiles >> SSL Dial-in sayfasına gidin ve yeni profil oluşturmak için Add'e tıklayın.



4. Profili aşağıdaki gibi ayarlayın:
- Profil adını girin.
 - "Enable this profile" ı etkinleştirin.
 - SSL User Name için listeden 3. Adımda oluşturulan profili seçin.
 - VPN Server'da Local IP/Subnet Mask'ı LAN ayarları olarak girin
 - Remote IP/Subnet Mask için Add'e tıklayın ve VPN istemcisinin LAN ayarlarını girin.
 - Kaydetmek için Apply'a tıklayın.



5. SSL Tünel Hizmeti'nin etkin olduğundan emin olmak için VPN and Remote Access >> Remote Access Control sayfasına gidin.



6. HTTPS Allow 'un etkin olduğundan emin olmak için System Maintenance >> Access Control >> Internet Access Control sayfasına gidin.

System Maintenance >> Access Control >> Access Control

Access Control Fail to Ban Access Barrier

Use Validation Code : Enable Disable

Internet Access Control

Web Allow : Enable Disable

Telnet Allow : Enable Disable

SSH Allow : Enable Disable

HTTPS Allow : Enable Disable

FTP Allow : Enable Disable

VPN Client (Dial-Out) Kurulumu

7. VPN profili oluşturun: VPN and Remote Access >> VPN Profiles >> SSL Dial-out sayfasına gidin. Profil oluşturmak için Add'e tıklayın.

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

IPsec PPTP Dial-out PPTP Dial-in **SSL Dial-out** SSL Dial-in

Add Edit Delete Refresh

Profile	Enable	Dial-Out Through	Server IP/Host Name
No items to show.			

8. Profili aşağıdaki gibi ayarlayın:
- Profil adı girin.
 - "Enable this profile" i etkinleştirin.
 - Server IP/ Host Name için VPN Server'ın AN IP adresi veya Hostname'ini girin.
 - SSL User Name ve SSL Password için 2. Adımda girilen username ve password'u girin.
 - Remote siteye bağlamak istediğiniz local LAN Subnet olarak Local IP/Subnet Mask'ını girin.
 - Remote IP/Subnet Mask için Add'e tıklayın ve VPN Server'ın LAN ayarlarını girin.
 - Kaydetmek için Apply'a tıklayın.

SSL Dial-out

Profile : Client

Enable

Always On : Enable Disable

Dial-Out Through : wan1 Default WAN IP WAN Alias IP

Failover to :

Idle Timeout (sec) : 300 (Optional)

Server IP/Host Name : 100.100.100.100

SSL User Name : draytek

SSL Password :

Local IP / Subnet Mask : 192.168.2.1 255.255.255.0/24

Add Save

IP	Subnet Mask
192.168.1.1	255.255.255.0

Remote IP / Subnet Mask :

Route / NAT Mode : Route

Netbios Naming Packet : Enable Disable

VPN'in Kurulumu

- VPN'i bağlamak için VPN istemcisinde VPN and Remote Access >> Connection Management sayfasına gidin. SSL'yi seçin açılan listeden 3. Adımda oluşturulan VPN profilini seçin. VPN tüneline kurmak için Connect'e tıklayın.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : Client Refresh Auto Refresh : 1 Minute

- Tüm kimlik bilgileri Network yöneticisi ise kurulan VPN'i ve çalışma süresini VPN and Remote Access >> Connection Management sayfasından kontrol edebilir.

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

Connection Management History

Dial-Out tool

IPsec PPTP SSL Profiles : Refresh Auto Refresh : 1 Minute

Green :Data is encrypt
White :Data isn't encrypt

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Netw...	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation	
1	Client	SSLTunnel	wan1	100.100.100...	192.168.1.1/...	00:03:31	0(bps)	0(bps)	481.32 (KB)	233.91 (KB)	<input type="button" value="Refresh"/> <input type="button" value="Stop"/>