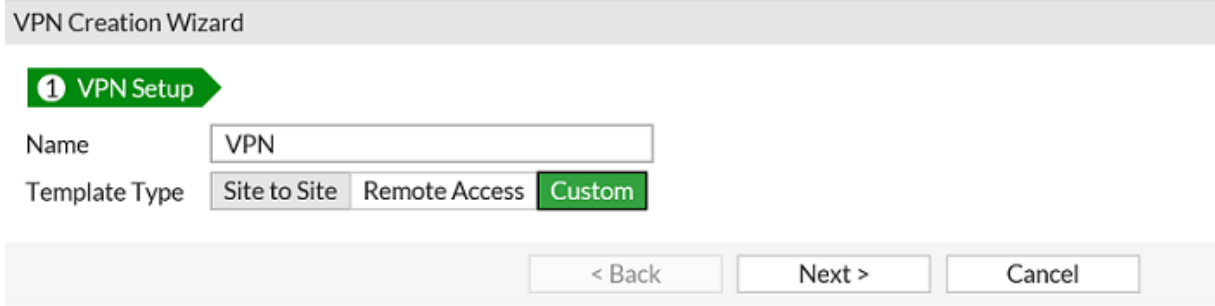


## FORTIGATE VE DRAYTEK ARASINDA IPSEC VPN

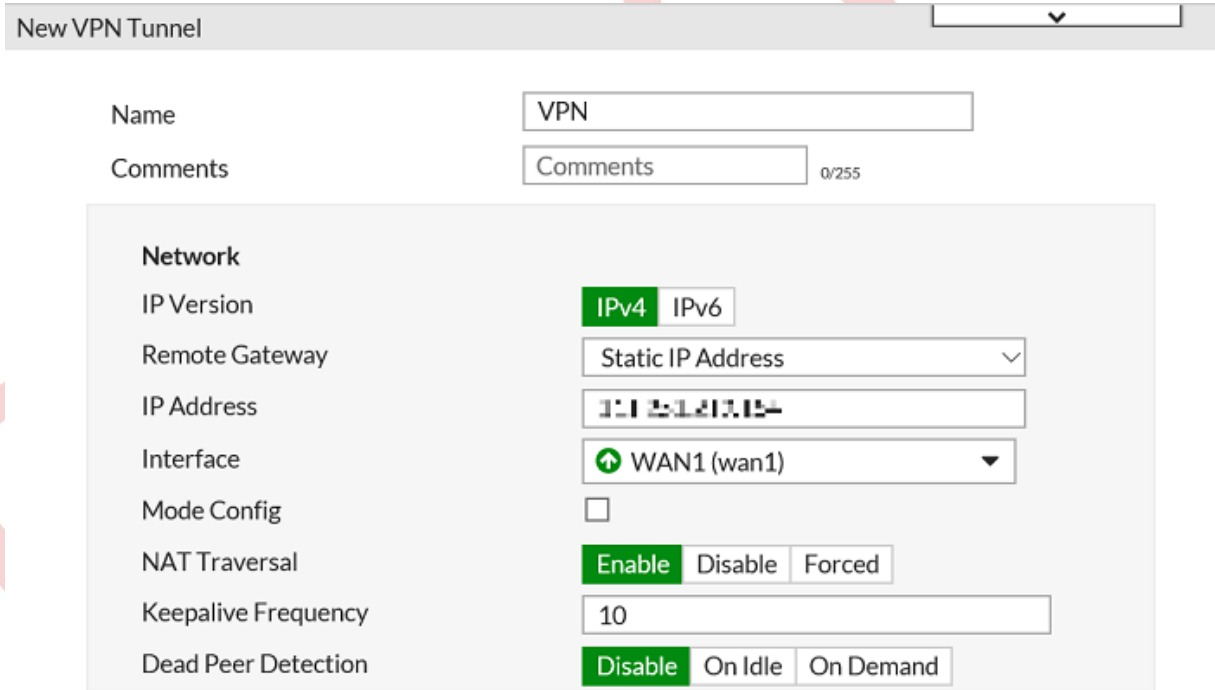
Bu makale FortiGate Router ve Vigor Router arasında nasıl iPsec VPN tüneli kurulacağını gösteriyor. Örnek olarak, FortiOS 5.4.0'da bir FortiGate router kullanıyor.

### FortiGate'in Yapılandırması

1. **VPN >> IPsec Wizard** sayfasına gidin, isim verin, Template Type için Custom seçin ardından **Next >** 'e tıklayın.



2. Network ayarlarında, **IP address**'e Vigor Router'ın WAN IP'sini ve **Interface** için Vigor Router'ın WAN Interface'sini girin.



3. Authentication ayarlarında, **Pre-shared Key** girin ve **Key Lifetime** ayarlayın. ( Vigor Router default olarak "28800" saniye kullanır.)

**Authentication**

Method: Pre-shared Key

Pre-shared Key: .....

**IKE**

Version: 1 2

Mode: Aggressive Main (ID protection)

**Phase 1 Proposal** + Add

Encryption	AES128	Authentication	SHA256	
Encryption	AES256	Authentication	SHA256	
Encryption	3DES	Authentication	SHA256	
Encryption	AES128	Authentication	SHA1	
Encryption	AES256	Authentication	SHA1	
Encryption	3DES	Authentication	SHA1	

Diffie-Hellman Groups:  21  20  19  18  17  16  
 15  14  5  2  1

Key Lifetime (seconds): 86400

- Phase 2 ayarlarında, FortiGate üzerine **Local Address** için Vigor Router ile bağlanmak istediğiniz IP subnetini ve **Remote Address** için Vigor Router'ın LAN IP subnetini yazın.

**Phase 2 Selectors**

Name	Local Address	Remote Address	
VPN	192.168.0.0/24	192.168.1.0/24	

**New Phase 2** ✓ ↺

Name: VPN

Comments: Comments

Local Address: Subnet 192.168.0.0/24

Remote Address: Subnet 192.168.1.0/24

- Phase 2 Proposal ayarlarında **Replay Detection** ve **Perfect Forward Secrecy (PFS)** seçeneklerini işaretlemeyin ve **Key Lifetime** ayarlayın. (Vigor Router default olarak "3600" saniye kullanır.)

**Advanced...**

Phase 2 Proposal **+ Add**

Encryption	AES128	Authentication	SHA1	
Encryption	AES256	Authentication	SHA1	
Encryption	3DES	Authentication	SHA1	
Encryption	AES128	Authentication	SHA256	
Encryption	AES256	Authentication	SHA256	
Encryption	3DES	Authentication	SHA256	

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Local Port All

Remote Port All

Protocol All

Auto-negotiate

Autokey Keep Alive

Key Lifetime

Seconds

**OK** **Ca**

1. Policy ayarı için bir adres profili oluşturun: **Policy & Objects >> Addresses >> Create New >> Address** sayfasına gidin, profile isim girin ve **Subnet /IP Range** için Vigor Router'ın LAN IP subnetini girin. **Interface** için az önce oluşturulan IPsec Tunnel'ini seçin ve uygulamak için **OK**'a tıklayın.

New Address

Name	<input type="text" value="Vigor"/>
Type	<input type="text" value="IP/Netmask"/>
Subnet / IP Range	<input type="text" value="192.168.1.0/255.255.255.0"/>
Interface	<input type="text" value="VPN"/>
Show in Address List	<input checked="" type="checkbox"/>
Static Route Configuration	<input type="checkbox"/>
Comments	<input type="text" value=""/>

0/255

**OK** **Cancel**

4. VPN trafiği için Güvenlik Firewall kuralları oluşturun: **Policy & Objects >> IPv4 Policy >> Create New** sayfasına gidin. İki tür trafik kabul etmemiz gerekir: Internal Network'ten Vigor ağına ve Vigor ağdan Internal Network'e. ( Not: Kural sırasını aklınızda bulundurun, çünkü onların önceliğini manuel olarak ayarlamamız gerekebilir. Genellikle, IPsec trafiği, yönetim kuralı dışındaki kuralların çoğundan daha yüksek önceliğe sahip olacaktır.)

New Policy	
Name	FortiGate to Vigor
Incoming Interface	↑ internal ×
Outgoing Interface	👤 VPN ×
Source	📄 LAN ×
Destination Address	📄 Vigor ×
Schedule	always ▼
Service	👤 ALL ×
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

New Policy	
Name	Vigor to FortiGate
Incoming Interface	👤 VPN ×
Outgoing Interface	↑ internal ×
Source	📄 Vigor ×
Destination Address	📄 LAN ×
Schedule	always ▼
Service	👤 ALL ×
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

5. VPN için Static Route oluşturun: **Network >> Static Routes >> Create New** sayfasına gidin. **Destination** için Vigor Router'ın LAN IP'sini girin ve **Device** için IPsec Tunnel'i seçin.

New Static Route

Destination ⓘ **Subnet** Named Address Internet Service

192.168.1.0/24

Device VPN ▼

Administrative Distance ⓘ 10

Comments 0/255

+ Advanced Options

OK Cancel

## Vigor Router Yapılandırması

### DrayOS

1. **VPN and Remote Access >> LAN to LAN** sayfasına gidin ve uygun bir indexe tıklayın. Common Settings'te profil adı girin, **Enable this profile** etkinleştirin ve **Call Direction** için "Dial-Out" seçin.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

#### 1. Common Settings

Profile Name	toHQ	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 checked="" type="checkbox"/> Always on	
VPN Dial-Out Through	WAN1 First	Idle Timeout	-1 second(s)
1-1 1.1.1.1/24		<input type="checkbox"/> Enable PING to keep IPsec tunnel alive	
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.)			

2. Dial-out settings'de,
  - **Type of Server I am Calling** için "IPsec Tunnel" seçin.
  - **Server IP**'de FortiGate routerın WAN IP'sini girin.
  - FortiGate routerda girdiğiniz **Pre-shared Key** değerini buraya da giriniz.
  - IPsec Security Method'da, **High(ESP) AES with Authentication** seçeneğini seçin ve **Advanced**'a tıklayın.

## 2. Dial-Out Settings

<b>Type of Server I am calling</b> <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <span>None</span>	Username <span>???</span> Password(Max 15 char) PPP Authentication <span>PAP/CHAP/MS-CHAP/MS-CHAPv2</span> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <span>220.132.88.33</span>	<b>IKE Authentication Method</b> <input checked="" type="radio"/> Pre-Shared Key <input checked="" type="radio"/> IKE Pre-Shared Key <span>.....</span> <input type="radio"/> Digital Signature(X.509) Peer ID <span>None</span> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <span>None</span>
	<b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <span>DES without Authentication</span> <input checked="" type="button"/> Advanced

1. Açılır pencerede, FortiGate Router'da girilen ayarların aynısını burada **Key Lifetime** ve **Proposals** için yapılandırın.

IKE advanced settings - Google Chrome

192.168.1.1/doc/l2IkeDt.htm

## IKE advanced settings

IKE phase 1 mode	<input checked="" type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	<span>AES128_SHA1_G5</span>	
IKE phase 2 proposal	<span>AES128_SHA1/AES128_MD5</span>	
IKE phase 1 key lifetime	<span>86400</span>	(900 ~ 86400)
IKE phase 2 key lifetime	<span>3600</span>	(600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Local ID	<input type="text"/>	

Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote include: DES\_(MD5/SHA)\_G1, 3DES\_MD5\_G1, 3DES\_MD5\_G2, 3DES\_(MD5/SHA)\_G5, AES128\_MD5\_(G2/G5), AES256\_S1, AES256\_SHA\_G14

OK

Close

2. TCP/IP Network Settings'de **Remote Network IP**'de FortiGate Router'ın LAN IP'sini girin ve 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	192.168.0.1		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 active if one single WAN is up )	
Local Network Mask	255.255.255.0		
	<a href="#">More</a>		

OK Clear Cancel

3. Profil etkin olduğu sürece Vigor Router VPN'i başlatmaya çalışacaktır. Bununla birlikte,VPN'yi manuel olarak aramak için **VPN and Remote Access >> Connection Management** sayfasına gidebilirsiniz. Ardından profili seçin ve **Dial**'e tıklayın.

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

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode:	( VPN ) 192.168.214.232	Dial
Backup Mode:		Dial

4. VPN başarıyla kurulduktan sonra, aşağıdaki durumu 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 ( VPN )	IPsec Tunnel AES-SHA1 Auth	192.168.214.232 via WAN2	192.168.0.1/24	3	16	3	19	0:0:30 Drop

xxxxxxx : Data is encrypted.  
xxxxxxx : Data isn't encrypted.

### Linux

1. **VPN and Remote Access >> VPN Profiles >> IPsec**'e gidin ve VPN profili oluşturmak için **Add**'e tıklayın. Profil adı girin ve Enable'yi işaretleyin.
2. Basic sekmesinde,
  - FortiGate yönlendiricisine bağlamak istediğiniz local subnet IP aralığını **Local IP/Subnet Mask**'a yazın.
  - **Remote IP/Subnet Mask**'da FortiGate Routerın LAN IP'sini yazın.
  - **Remote Host**'da FortiGate'in WAN IP'sini yazın.
  - **Auth Type** için "PSK" seçin ve FortiGate Router'daki ayarındaki **Pre-shared Key**'i girin.

IPsec

Profile : VPN

Enable

Basic Advanced GRE Proposal

Auto Dial-Out :  Enable  Disable

For Remote Dial-In User :  Enable  Disable

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

Failover to :

Local IP / Subnet Mask : 192.168.39.1 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 : default gateway)

Remote Host :

Remote IP / Subnet Mask : 192.168.0.1 255.255.255.0/24

Add Save Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

IKE Phase 1 :  Main Mode  Aggressive Mode

Auth Type : PSK

Preshared Key :  (If Aggressive mode is disabled and Remote Host IP is 0.0.0.0 then the Preshared Key is instead set vi

Security Protocol : ESP

1. Advanced sekmesine gidin, Phasel' i ve 2' i ayarlayın ve **Key Life Time**' a, FortiGate Router' da girilen değeri girin.

IPsec

Profile : VPN

Enable

Basic Advanced GRE Proposal

Phase1 Key Life Time : 86400

Phase2 Key Life Time : 86400

Perfect Forward Secrecy Status :  Enable  Disable

Dead Peer Detection Status :  Enable  Disable

Ping to Keep Alive :  Enable  Disable

Route / NAT Mode : Route

Source IP : auto\_detect\_srcip

Apply NAT Policy :  Enable  Disable

Netbios Naming Packet :  Enable  Disable

Multicast via VPN :  Enable  Disable

RIP via VPN :  Enable  Disable



3. Proposal sekmesine gidin. FortiGate Router ayarlarıyla eşleşen **IKE Proposals**'ı seçin. Ardından, kaydetmek için **Apply**'ı tıklayın .

The screenshot shows the IPsec configuration page for a profile named 'VPN'. The 'Enable' checkbox is checked. The 'Proposal' tab is selected. The configuration is as follows:

IKE Phase1 Proposal [Dial-Out] :	AES128 G5
IKE Phase1 Authentication [Dial-Out] :	SHA2_256
IKE Phase2 Proposal [Dial-Out] :	AES128 with auth
IKE Phase2 Authentication [Dial-Out] :	SHA1
Accepted Proposal [Dial-In] :	acceptall

4. VPN'i başlatmak için **VPN and Remote Access >> Connection Management** sayfasına gidin, VPN profilini seçin ve Connect'e tıklayın.

The screenshot shows the 'VPN and Remote Access >> Connection Management' page. The 'Dial-Out tool' section is active. The 'IPsec' radio button is selected, and the 'Profiles' dropdown is set to 'VPN'. The 'Connect' button is highlighted. The 'Auto Refresh' is set to '1 Minute'. A status indicator shows 'Green :Data is encrypted' and 'White :Data isn't encrypte'.

5. VPN başarıyla bağlandıktan sonra, aşağıdaki VPN Bağlantı Durumunu görebiliriz.

The screenshot shows the 'VPN Connection Status' table. The table has the following columns: VPN, Type, Interface, Remote IP, Virtual Netw..., Up Time, RX Rate, TX Rate, RX Byte, TX Byte, and Operation. The table contains one entry:

VPN	Type	Interface	Remote IP	Virtual Netw...	Up Time	RX Rate	TX Rate	RX Byte	TX Byte	Operation
1	VPN	IPsec/AES_...	wan1	192.168.0.0/...	00:41:20	0(bps)	0(bps)	588(Byte)	2.52 (KB)	