

## NORDVPN VE VIGOR ROUTER ARASINDA IKEv2 EAP

Firmware 3.9.0 versiyonundan beri Vigor Router, IKEv2 EAP VPN tüneline NordVPN sunucusuna aramayı desteklemektedir. Bu makalede, Vigor Router'dan NordVPN sunucusuna IKEv2 EAP VPN tüneline nasıl oluşturulacağı anlatılmaktadır.

Not: Vigor2860 / 2925 v3.8.9.4'ten bu yana bu özelliği destekliyor.

1. Bir NordVPN hesabına ihtiyacınız olacak. <https://free.nordvpn.com/> adresinden 3 günlük ücretsiz deneme NordVPN hesabı için başvurabilirsiniz.

For 3 days surf the web in full security and privacy. No credit card required, no questions asked. Simply enter your email address and get started with your free NordVPN trial.

protected by reCAPTCHA  
Privacy Terms

2. <https://downloads.nordvpn.com/certificates/root.der> adresinden NordVPN Root CA sertifikasını indirin.
3. NordVPN sunucu domainini <https://nordvpn.com/servers/> adresinden edinin. Bulduğunuz ülkeyi seçerek önerilen bir sunucu alabilirsiniz. Aşağıdaki resimde, **de241.nordvpn.com** VPN sunucusunun Hostname'idir.

**Server recommended by NordVPN**

Let our smart algorithm select the best server for you.

Server recommended for you

Adjust server preferences

Germany

Show advanced options

Reset

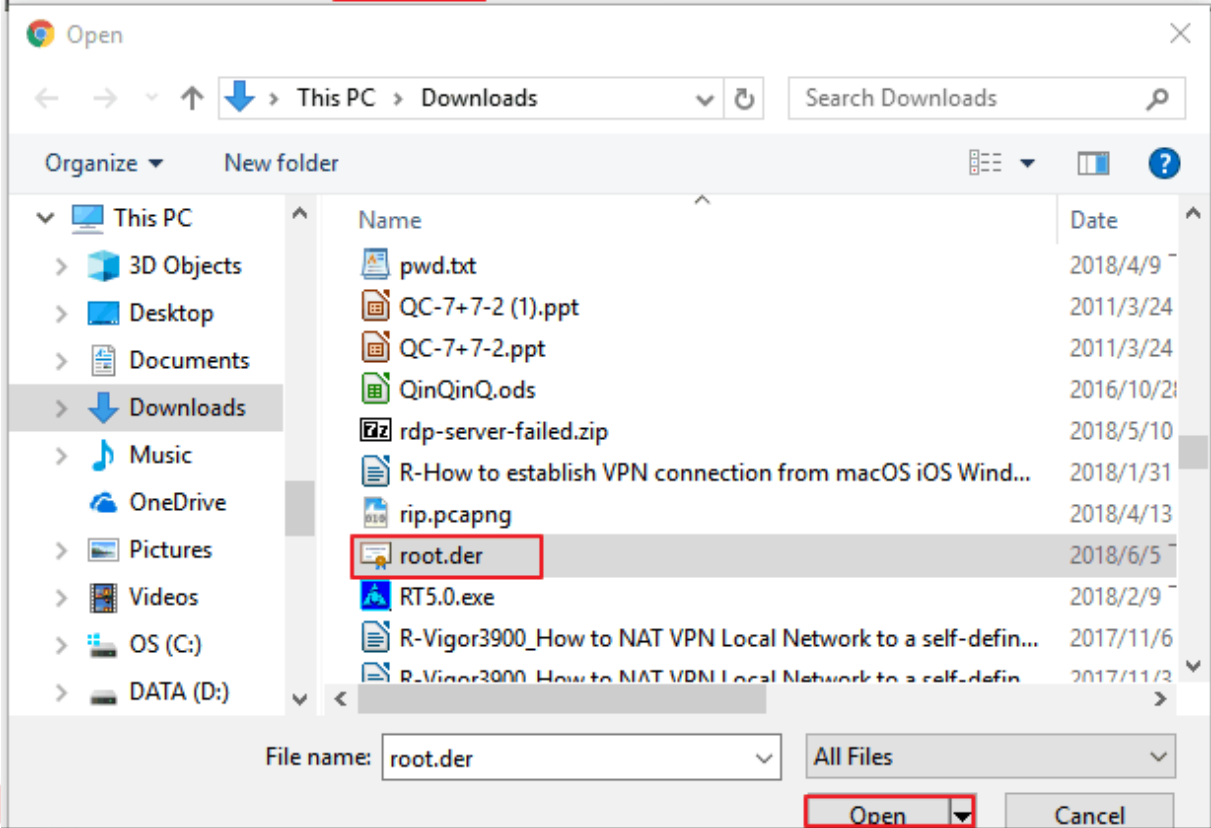
**de241.nordvpn.com**  
Germany #241

4. Yönlendiricinin yönetim sayfasına giriş yapın. **Certificate Management** >> **Trusted CA Certificate** sayfasına gidin ve **IMPORT**'a tıklayın. Ardından 2.adımda indirilen root.der dosyayı seçmek için **Choose File**'a tıklayın ve sonra **Import**'a tıklayın.

## Certificate Management &gt;&gt; Trusted CA Certificate

## Import X509 Trusted CA Certificate

Select a trusted CA certificate file.  
 No file chosen  
 Click [Import](#) to upload the certification.



Open

This PC > Downloads

Organize New folder

Name	Date
pwd.txt	2018/4/9
QC-7+7-2 (1).ppt	2011/3/24
QC-7+7-2.ppt	2011/3/24
QinQinQ.ods	2016/10/21
rdp-server-failed.zip	2018/5/10
R-How to establish VPN connection from macOS iOS Wind...	2018/1/31
rip.pcapng	2018/4/13
<b>root.der</b>	2018/6/5
RT5.0.exe	2018/2/9
R-Vigor3900_How to NAT VPN Local Network to a self-defin...	2017/11/6
R-Vigor3900_How to NAT VPN Local Network to a self-defin...	2017/11/3

File name: root.der All Files

- Router "Import Success" yanıtını verene ve Sertifika Durumu OK görünene kadar birkaç saniye bekleyin.

## Certificate Management &gt;&gt; Trusted CA Certificate

## X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	<input type="button" value="Create"/>
Trusted CA-1	/C=PA/O=NordVPN/CN=NordVPN R...	<b>OK</b>	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>

**Note:**

- Please setup the "System Maintenance >> [Time and Date](#)" correctly before you try to generate a RootCA!!
- The Time Zone MUST be setup correctly!!

5. **VPN and Access >> IPsec Peer Identity** sayfasına gidin ve NordVPN sunucusu için profili ayarlayın.
- **Enable this account**'ı işaretleyin.
  - **Accept Any Peer ID** seçeneğini seçin.

VPN and Remote Access >> IPsec Peer Identity

Profile Index : 1

<input checked="" type="checkbox"/> Enable this account	
Profile Name	<input type="text" value="NordVPN"/>
<input checked="" type="radio"/> <b>Accept Any Peer ID</b>	
<input type="radio"/> Accept Subject Alternative Name	
Type	<input type="text" value="IP Address"/>
IP	<input type="text"/>
<input type="radio"/> Accept Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>

6. **VPN and Access >> LAN to LAN** sayfasına gidin. Uygun bir index numarasına tıklayın ve profili aşağıdaki gibi ayarlayın. Common Settings'de,
- **Profile name** girin.
  - **Enable this profile**'ı etkinleştirin.
  - **Call Direction** için "Dial-Out" u ayarlayın.
  - **Dial-Out Through** sekmesinde VPN bağlantısı için WAN Interface'sini seçin

Profile Index : 3

1. Common Settings

Profile Name	<input type="text" value="toNordVPN"/>	Call Direction	<input type="radio"/> Both <input checked="" type="radio"/> <b>Dial-Out</b> <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile		Tunnel Mode	<input type="radio"/> GRE Tunnel
VPN Dial-Out Through	<input type="text" value="WAN2 Only"/>	<input checked="" type="checkbox"/> Always on	
	<input type="text" value="1-118.166.187.44"/>	Idle Timeout	<input type="text" value="-1"/> 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	<input type="text"/>
<small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>			

7. Dial-Out Settings'de,
- VPN Server type için **IKEv2 EAP** seçeneğini seçin.
  - **Server IP address / Hostname**'e VPN sunucusunun 3.adımda girilen domainini girin.
  - **Username** girin. ( NordVPN hesabını uygulamak için kullandığınız posta adresidir.)

- **Password** girin. ( NordVPN deneme servisini aktif hale getirirken yapılandırduğunuz şifredir.)
- **IKE Authentication Method** için “Dışgıtal Signature” u seçin ve **Peer ID** için 6.adımda oluşturulan IPsec Peer Identity profilini seçin.
- **IPsec Security Method** için “AES with Authentication” seçeneğini seçin.
- **Advanced**'a tıklayın.

## 2. Dial-Out Settings

<b>Type of Server I am calling</b> <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel IKEv2 <input checked="" type="radio"/> IKEv2 EAP <input type="radio"/> IPsec XAuth <input type="radio"/> L2TP with IPsec Policy None <input type="radio"/> SSL Tunnel	Username vkao.draytek@gmail.com Password ..... PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPV2 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) de241.nordvpn.com Server Port (for SSL Tunnel): 443	<b>IKE Authentication Method</b> <input type="radio"/> Pre-Shared Key IKE Pre-Shared Key ..... <input checked="" type="radio"/> Digital Signature(X.509) Peer ID NordVPN Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate None
	<b>IPsec Security Method</b> <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) AES with Authentication <input checked="" type="radio"/> Advanced

8. Advanced butonuna tıklayın. IKE advanced settings’de aşağıdaki yapılandırmaları yapın:

- **IKE phase 1 Proposal**’ı “AES256\_SHA1\_G14” olarak ayarlayın.
- **IKE phase 2 Proposal**’ı “AES256\_SHA1” olarak ayarlayın.
- **IKE phase 1 key lifetime**’ı “3600” olarak ayarlayın.
- **IKE phase 2 key lifetime**’ı “1200” olarak ayarlayın.

IKE advanced settings - Google Chrome

192.168.6.1/doc/I2IlikeDt.htm

## IKE advanced settings

IKE phase 1 mode(IKEv1)	<input type="radio"/> Main mode	<input type="radio"/> Aggressive mode
IKE phase 1 proposal	AES256_SHA1_G14	
IKE phase 2 proposal	AES256_SHA1	
IKE phase 1 key lifetime	3600	(900 ~ 86400)
IKE phase 2 key lifetime	1200	(600 ~ 86400)
Perfect Forward Secret	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Local ID		

9. Pencereyi kapatmak için **OK**'a tıklayın. TCP / IP Network Settings’de:

- **Remote Network IP**'yi “0.0.0.0” olarak girin.
- **Remote Network Mask**'ı “0.0.0.0/00” olarak seçin.
- VPN bağlantısı için Routing’i NAT olarak değiştirin.
- (isteğe bağlı) Tüm NordVPN trafiğini istiyorsanız, “Change default route to this tunnel” seçeneğini etkinleştirin.

## 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	NAT
Remote Network IP	0.0.0.0		
Remote Network Mask	0.0.0.0 / 00	<input type="checkbox"/> Change default route to this VPN tunnel ( Only active if one single WAN is up )	
Local Network IP	192.168.6.1		
Local Network Mask	255.255.255.0 / 24		
	<a href="#">More</a>		

1. Yukarıdaki ayarları tamamladıktan sonra, **VPN and Remote Access >> Connection Management** sayfasından kontrol edebiliriz.

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

## Dial-out Tool

[Refresh](#)

General Mode:	( toNordVPN ) de241.nordvpn.cc	Dial
Backup Mode:		Dial
Load Balance Mode:		Dial

## VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status		Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
1 ( toNordVPN )	IKEv2 IPsec Tunnel AES-SHA1 Auth	185.230.127.13 via WAN2	0.0.0.0/0	53155	24	53036	24	20:1:27	<a href="#">Drop</a>

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

2. (isteğe bağlı) NordVPN tüneline özel trafik göndermek için, **Routing >> Load-Balance/Route Policy** ile Policy Route oluşturabiliriz . Politikayı doğrulamak için, tanımlanmış trafiğin VPN tüneline doğru bir şekilde geçip geçmediğini kontrol etmek için “tracert” komutunu kullanabiliriz.

## C:\ Command Prompt

```
Microsoft Windows [Version 10.0.17134.48]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ul>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  192.168.6.1
  2  14 ms  16 ms  15 ms  168.95.98.254
  3  14 ms  14 ms  14 ms  168.95.90.62
  4  14 ms  19 ms  14 ms  220.128.8.242
  5  22 ms  22 ms  22 ms  220.128.8.26
^C
C:\Users\ul>tracert -d 203.149.64.198

Tracing route to 203.149.64.198 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  192.168.6.1
  2  301 ms  301 ms  301 ms  185.230.127.13
  3  302 ms  301 ms  301 ms  185.230.127.1
  4  301 ms  301 ms  301 ms  176.10.83.29
  5  323 ms  301 ms  302 ms  80.81.192.172
  6  310 ms  362 ms  327 ms  72.52.92.13
^C
```

← an IP of Australia

← vpn