



# EAP KİMLİK DOĞRULAMA İLE iOS'TAN VIGOR ROUTER'A IKEv2 VPN

DrayOS firmware 3.9.0 versiyonundan beri EAP kimlik doğrulaması ile IKEv2'yi desteklemektedir. Vigor3900 ile Vigor2960 da firmware 1.4.0 versiyonundan beri EAP kimlik doğrulaması ile IKEv2'yi destekliyor. Ek olarak kullanıcı adı/şifre ve sertifika doğrulama ile IKEv2 VPN'i daha güvenli hale getirebilirsiniz. Bu makale server kimlik doğrulaması için self-signed bir sertifika oluşturmayı, Vigor Router'ı bir IKEv2 VPN server kurmayı ve iOS ile bağlantı kurmayı gösterir.

## Vigor Router Kurulumu

# DrayOS

1. Certificate Management >> Trust CA Certificate sayfasına gidin. Ve Create'e tıklayın.

Certificate Management >> Trusted CA Certificate

#### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA			Create
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

Note:

 Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before you try to generate a RootCA!!

2. The Time Zone MUST be setup correctly !!

IMPORT R	EFRESH
----------	--------

2. Sertifika bilgilerini girin. Key Size için "2048 Bit" girin. Sonra Generate'e tıklayın.

#### Certificate Management >> Root CA Certificate

Generate Root CA		
Certificate Name	Root CA	
Subject Alternative Name		
Туре	None ~	
Subject Name		
Country (C)	TW	
State (ST)	Hsinchu	
Location (L)	Hukou	
Organization (O)	Draytek	
Organization Unit (OU)	Vigor	
Common Name (CN)	Root	
Email (E)	example@ikev2vpn.net	
Кеу Туре	RSA ~	
Key Size	2048 Bit ~	
Algorithm	SHA-256 ~	

Generate

3. RootCA'yı indirmek için **Export'**a tıklayın.





#### Certificate Management >> Trusted CA Certificate

### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	/C=TW/ST=Hsinchu/L=Hukou/O=D	OK	Export View Delete
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

#### Note:

 Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before you try to generate a RootCA!!

2. The Time Zone MUST be setup correctly !!

IMPORT REFRESH	1
----------------	---

- 4. Certificate Management >> Local Certificate sayfasına gidin ve Generate'e tıklayın.
  - Subject Alternative Name Type için "Domain Name" girin.
  - Domain Name ve Common Name(CN) için routerın domainini girin.
  - Sertifika için diğer tüm bilgileri doldurun.
  - Key Size için "2048 Bit" girin.
  - Generate'e tıklayın.

Generate Certificate Signing Requ	est	
Certificate Name	certificate	
Subject Alternative Name		
Туре	Domain Name 🗸	
Domain Name	ikev2server.ddns.net	
Subject Name		
Country (C)	TW	
State (ST)	Hsinchu	
Location (L)	Hukou	
Organization (O)	Draytek	
Organization Unit (OU)	Vigor	
Common Name (CN)	ikev2server.ddns.net	
Email (E)	example@ikev2vpn.net	
Кеу Туре	RSA ~	
Key Size	2048 Bit ~	
Algorithm	SHA-256 ~	

Generate

5. Sertifikayı oluşturmak için Sign'a tıklayın.

Certificate Management >> Local Certificate Signing

Local Certificate Signing	
Certificate Name	certificate
Validity	YYYY-MM-DD
Not Before	2017-09-13
Not After	2025 ~ - 9 ~ - 13 ~
Algorithm	SHA-256 ~

Sign Back





6. Geçerli olan tarihi belirtin sonra Sign'a tıklayın.

## Certificate Management >> Local Certificate

### X509 Local Certificate Configuration

Name	Subject	Status	Modify
certificate	/C=TW/ST=Hsinchu/L=Hukou/O=D	Requesting	Sign View Delete
			View Delete
			View Delete

### Note:

. . . . . .

. -

. .

- Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before signing the local certificate.
- 2. The Time Zone MUST be setup correctly !!

GENERATE	IMPORT
----------	--------

7. VPN and Remote Access >> IPsec General Setup sayfasına gidin, Certificate for Dial-in için önceki adımlarda oluşturulan yerel sertifikayı seçin.

REFRESH

VPN IKE/IPsec General Setup	
Dial-in Set up for Remote Dial-in users a	and Dynamic IP Client (LAN to LAN).
IKE Authentication Method	
Certificate for Dial-in	certificate ~
Local ID	
Alternative Subject Nar	me First
O Subject Name First	
General Pre-Shared Key	
Pre-Shared Key	•••••
Confirm Pre-Shared Key	•••••
Pre-Shared Key for XAuth User	
Pre-Shared Key	•••••
Confirm Pre-Shared Key	•••••
IPsec Security Method	
Medium (AH)	
Data will be authentic, but wi	ll not be encrypted.
High (ESP) 🗹 DES 🗹 3DE	ES 🗹 AES
Data will be encrypted and a	thentic

OK

 VPN and Remote Access >> Remote Dial-in User sayfasına gidin. Uygun bir index numarasını seçin ve profili aşağıdaki gibi düzenleyin.

Cancel

- Allowed Dial-In Type'de IKEv2 EAP seçin.
- Username ve Password girin.
- Kaydetmek için **OK'**a tıklayın.





VPN and	Remote	Access >>	Remote	Dial-in	User
vi it anu	itemote i	Autess	remote	Dial-III	0361

User account and Authentication	Username	EAP
Enable this account	Password(Max 19 char)	•••••
Idle Timeout 0 second(s)	Enable Mobile One-Ti	me Passwords(mOTP)
Allowed Dial-In Type	PIN Code	
	Secret	
☑ IPsec Tunnel	IKE Authentication Method	4
☑ IPsec XAuth	Pre-Shared Key	J
✓ L2TP with IPsec Policy None ~	IKE Pre-Shared Key	
SSL Tunnel	Digital Signature(X.5	09)
☑ IKEv2 EAP	None ~	
Specify Remote Node	IDa a Caravita Mathad	
Remote Client IP	IPsec Security Method	
	Medium(AH)	
or Peer ID	High(ESP) 🗹 DES 🗹	3DES 🗹 AES
Netbios Naming Packet 💿 Pass 🔿 Block	Local ID (optional)	
Multicast via VPN 🛛 🔿 Pass 💿 Block		
(for some IGMP, IP-Camera, DHCP Relayetc.)		

# Linux

- 1. Certificate Management >> Trusted CA 'ya gidin Build RootCA'yı tıklayın.
  - Tüm bilgileri girin.
  - **Key Size** için "2048" girin.
  - Yerel sertifikayı imzalamak için **Passphrase'yi** (Parolayı) girin.
  - Kaydetmek için **Apply**'a tıklayın.

	📑 💓 Up	oload 前 Delete 🗔	Download 🏼 🄊 Bu	ild RootCA 🛛 👩 View
	Name	lss	suer	Subject
		Trusted CA		
		Certificate Nan	ne : RootCA	
		Organization Unit	t: Vigor	
		Organization :	Draytek	
		Locality(City) :	Hukou	
, i i i i i i i i i i i i i i i i i i i		State/Province :	Hsinchu	
		Common Name :	Root	
		Email Address :	example@test.net	
		Key Size :	2048	~
		Country :	TW	
		Passphrase :	•••••	





2. VPN istemcisine kurulması gereken Root CA'yı dışa aktarmak için Download'a tıklayın.

💓 Upl	oad <u> î</u> Delete	🗔 Download 🔉	Build RootCA 🛛 👸 View		
Name		Issuer	Subject	s	
RootCA		Root	Root	R	
	Local C     PKCS1:     Certific	Certificate 2 Certificate ate and Private Key			

- 3. Certificate Management >> Local Certificate 'e gidin. Generate 'e tıklayın.
  - **ID Type** için "Domain Name" seçin ve **ID Value** için routerın domainini girin.
  - Tüm bilgileri girin.
  - Common Name için routerın domainini girin.
  - Key Size için "2048" seçeneğini seçin.
  - Self Sign için "Enable" seçeneğini seçin.
  - CA Key Passphrase'de Root CA'nın parolasını girin.
  - Apply'a tıklayın.

Certificate	Management >> Local	Certificate	
Local Ce	rtificate		
🔯 U	pload 📺 Delete 国	Download 🧔 Generate	👸 Viev
Name Lo	ocal Certificate		-×
	Certificate Name :	EAP	
	Subject Alternative Name		
	ID Type :	Domain Name	
	ID Value :	ikev2server	
	Subject Name		
	Country (C)	W	
	State (S):	Hsinchu	
	Locality (L)	Hukou	
	Organization (O)	Draytek	
	Organization Unit (OU) :	Vigor	
	Common Name (CN) :	ikev2server.ddns.net	
	Email (E) :	example@test.net	
	Кеу		
	Key Size :	2048	
	Self Sign :	Enable Disable	
	CA Key Passphrase :	•••••	





- 4. Kullanıcı profili eklemek için User Management >> User Profile'a gidin.
  - Enable'yi aktifleştirin.
  - Username ve Password girin.
  - PPTP/L2TP/SSL/OpenVPN Server'da Xauth/EAP için "Enable" seçin.

Add 🔀 Edit 🔟 Del	lete 🏟 Refresh Search :	Q Search
er Profile		
		<u> </u>
Username :	EAP	
Enable		
Password :	Strength : Good	
System User :	false 👻	
PPTP/L2TP/SSL/PPPoE	OpenVPN Server General Setup	
Idle Timeout(sec) :	300	
DHCP from :	lan1 👻	
Static IP Address :	(Optional)	
∧ User Management		
V PPTP/L2TP/SSL/0	penVPN Server	
PPTP Dial-in :	Enable  Disable	
L 2TP Dialain	Enable Disable	
CCI Tunnal		
SSL lunnel :		
OpenVPN Dial-in :	Enable	
XAuth / EAP	Enable Disable	

- 5. Profil eklemek için VPN and Remote Access >> VPN Profiles >> IPsec'e gidin.
  - **Profil adı** girin ve **Enable'**yi aktifleştirin.
  - **Remote Dial-In User** için "Enable" seçeneğini seçin.
  - Local IP / Subnet Mask için routerın LAN ağını girin.
  - **IKE Protocol** için "IKEv2" seçeneğini seçin.
  - Auth Type için "RSA" seçin ve Local Certificate için önceki adımlarda oluşturulan sertifikayı seçin.

	TTTT Darsa		- Due bails		
DbA 🖨	🗶 Edit 🛛 📋	🛛 Delete 🔾 🔓	Rename 🤤	5 Refresh	
rofile :	IKEv2E/	ψ			
Cnable 2					
Basic	Advanced	GRE	Proposal	Multiple SAs	
For Remote	Dial-In User :	Enable	Disable		
Dial-Out The	sugh :	wan1	~	Default WAN IP      WAN Alias IF	
Failover to :			×		
ocal IR / Se	hnat Mark -	102 100 1 0	26.5.265.265.024		
	Man .	0.0.0.0			
Local Next	Hop :	0.0.0.0		u.u.u.u : derauk gakeway)	
Nemote nos		0.0.0.0			
Kemote IP 7	SUDNET Mask	. 0.0.0.0		200.200.200.200/32	
		🕼 Add  🗎	Save		Profile Number Limit : 16
		IP		Subnet Mask	
More Remot	a Subnet :			No items to show.	
IKE Protocol		IKEv2	×		
Auth Type :		RSA	*		
Local Certifi	sate :	EAP	*		
Local ID -		Subject Name	v		





# iOS'tan Bağlantı

1. Router'dan indirilen RootCA dosyasını iOS cihazına gönderin.



2. Dosyayı açarak CA'yı iOS cihazına iOS cihazına CA'yı yükleyin ve **Install**'a tıklayın. RootCA'nın doğrulandığından emin olduktan sonra **Done**'a tıklayın.

Cancel Install Profile	Install	Profile Installed	Done
Root		Root	
Signed by Root Not Verified Contains Certificate		Signed by Root Verified ✓ Contains Certificate	
More Details	>	More Details	>

- 3. General >> VPN 'e gidin ve konfigürasyonu ekleyin.
  - **Type** için "**I**KEv2" seçin.
  - Server ve Remote ID için routerın domainini girin.
  - Username ve Password girin.

Cancel	Add Configuration	on Done
Туре		IKEv2 >
Description	EAP	
Server	ikev2server.ddns	.net
Remote ID	ikev2server.ddns	.net
Local ID		
AUTHENTICAT	ION	
User Auther	ntication	Username >
Username	EAP	
Password	•••••	



4. VPN bağlantısını açarak VPN'i başlatın.



netfast

5. Başarılı bir şekilde bağlanırsa VPN durumu aşağıdaki gibi görünür.

< VPN	EAP Edit
Туре	IKEv2
Server	vigorikavZeap.coms.net
Account	EAP
Server IP Address	111.251.218.74
Assigned IP Address	192.168.1.33
Connect Time	0:12
Dele	ete VPN