

EAP KİMLİK DOĞRULAMA İLE macOS'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 macOS 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:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT

REFRESH

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	
Type	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
Key Type	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:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before you try to generate a RootCA!!
2. The Time Zone MUST be setup correctly!!

IMPORT

REFRESH

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 Request

Certificate Name	certificate
Subject Alternative Name	
Type	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
Key Type	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	
Not Before	YYYY-MM-DD
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:

1. Please setup the "System Maintenance >> **Time and Date**" correctly before signing the local certificate.
2. The Time Zone MUST be setup correctly!!

GENERATE

IMPORT

REFRESH

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

VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Certificate for Dial-in certificate ▾

Local ID

Alternative Subject Name First
 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 will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

OK

Cancel

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

Index No. 3

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="0"/> second(s)		Username <input type="text" value="EAP"/> Password(Max 19 char) <input type="password" value="....."/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>
Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> IPsec XAuth <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> SSL Tunnel <input checked="" type="checkbox"/> IKEv2 EAP <input type="checkbox"/> Specify Remote Node Remote Client IP <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
		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 Local ID (optional) <input type="text"/>

Linux

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

Certificate Management >> Trusted CA

Trusted CA

Upload Delete Download **Build RootCA** View

Name	Issuer	Subject
Trusted CA		

Certificate Name : RootCA

Organization Unit : Vigor

Organization : Draytek

Locality(City) : Hukou

State/Province : Hsinchu

Common Name : Root

Email Address : example@test.net

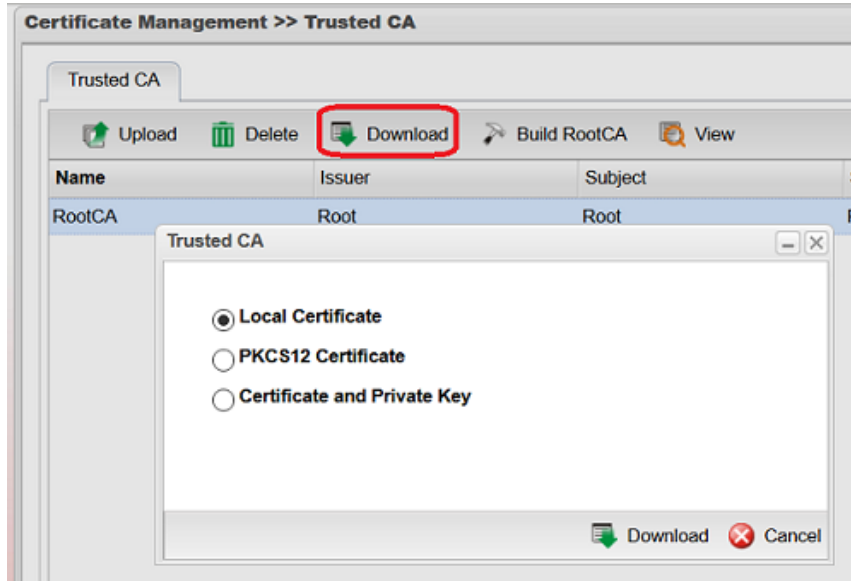
Key Size : 2048

Country : TW

Passphrase :

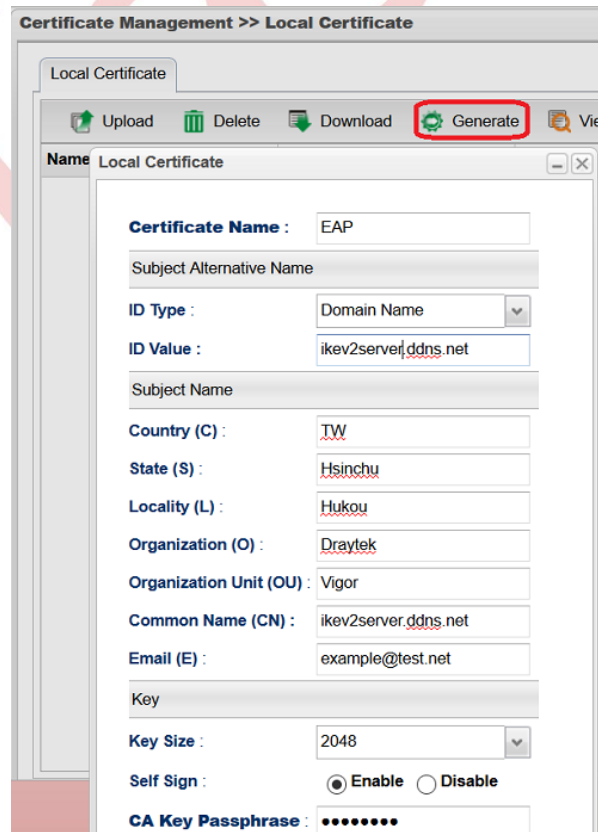
Apply Cancel

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



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.



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.

User Management >> User Profile >> User Profile

User Profile Apply All

Add Edit Delete Refresh Search

User Profile

Username : EAP

Enable

Password : [masked] 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

PPTP/L2TP/SSL/OpenVPN Server

PPTP Dial-in : Enable Disable

L2TP Dial-in : Enable Disable

SSL Tunnel : Enable Disable

OpenVPN Dial-in : Enable Disable

XAuth / EAP : Enable Disable

Use mOTP : Enable Disable

Time Objects : [dropdown]

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.

VPN and Remote Access >> VPN Profiles >> IPsec

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

Add Edit Delete Rename Refresh

Profile : IKEv2EAP

Enable

Basic Advanced GRE Proposal Multiple SAs

For Remote Dial-In User : Enable Disable

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

Fallover to : [dropdown]

Local IP / Subnet Mask : 192.168.1.0 255.255.255.0/24

Local Next Hop : 0.0.0.0 (0.0.0.0 - default gateway)

Remote Host : 0.0.0.0

Remote IP / Subnet Mask : 0.0.0.0 255.255.255.0/32

Profile Number Limit : 15

More Remote Subnet : No items to show

IKE Protocol : IKEv2

Auth Type : RSA

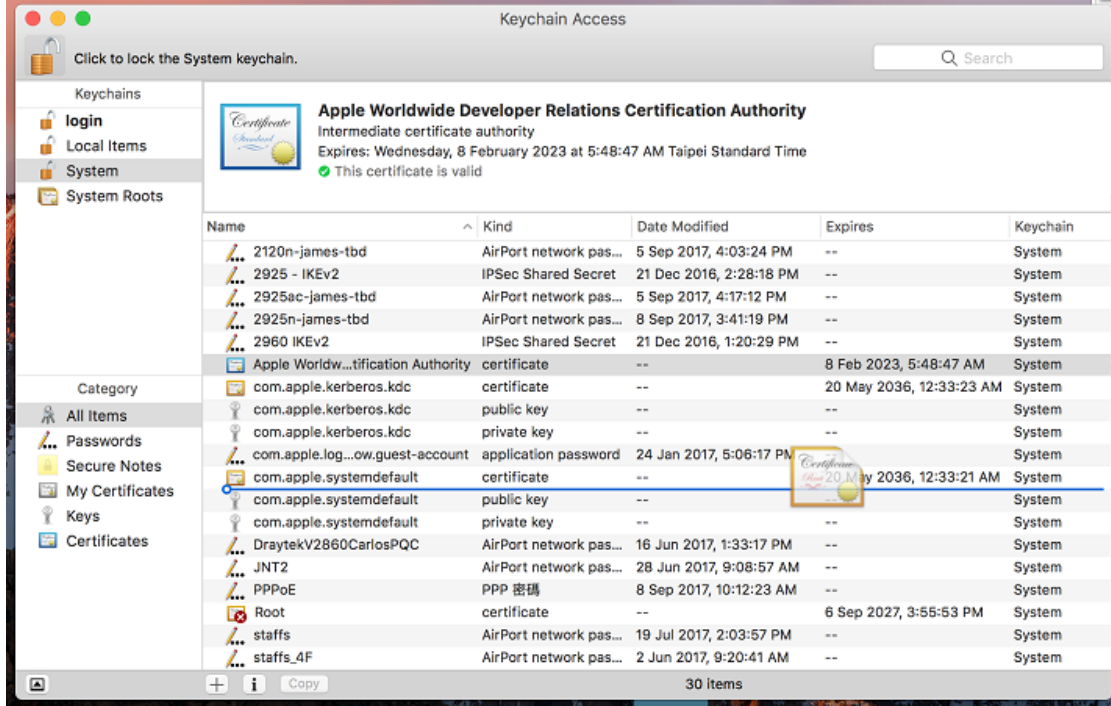
Local Certificate : EAP

Local ID : Subject Name

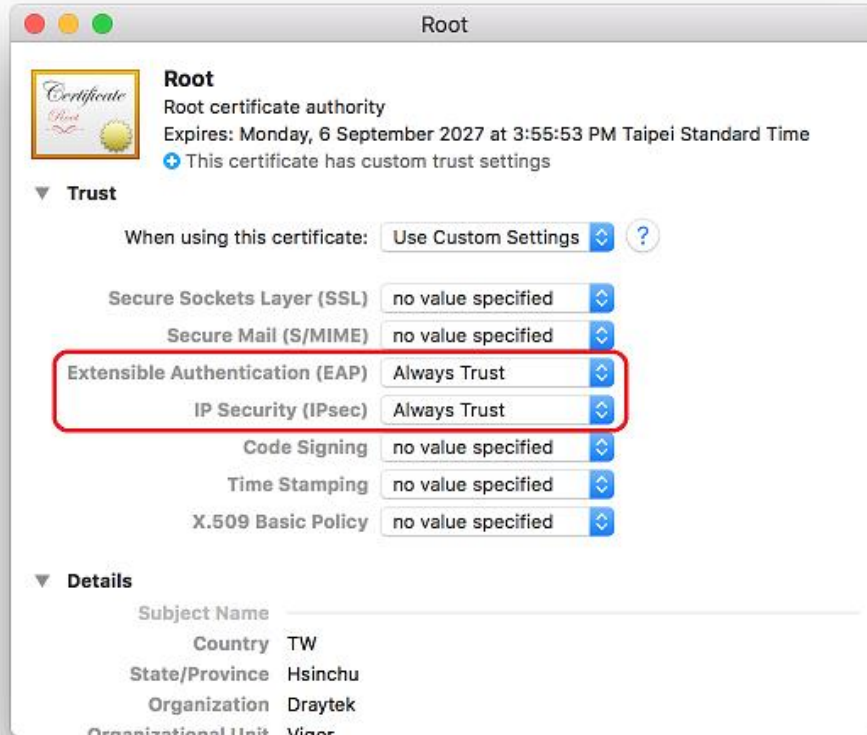
Remote ID : Accept Any

macOS'tan Bağlantı

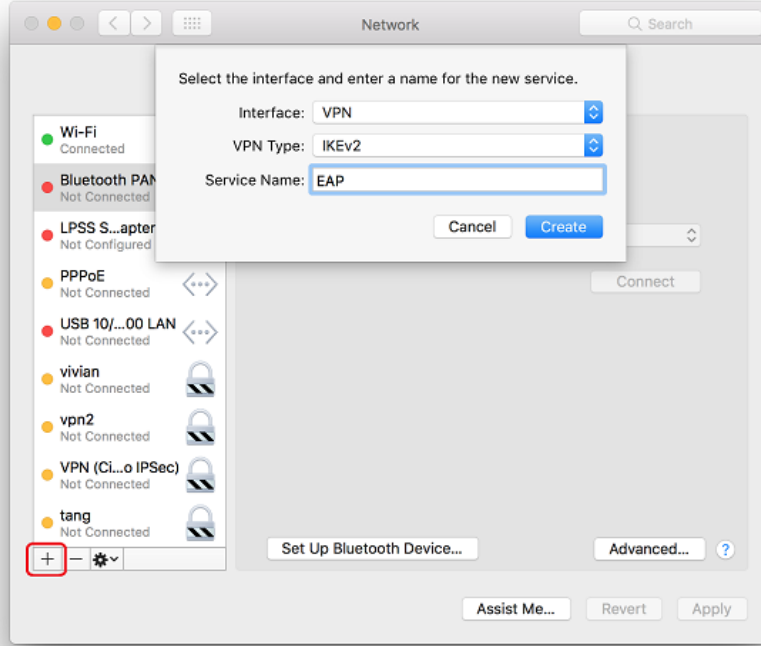
1. Keychain Access'i açın. Router'dan indirilen RootCA'yı pencereye sürükleyerek kurun.



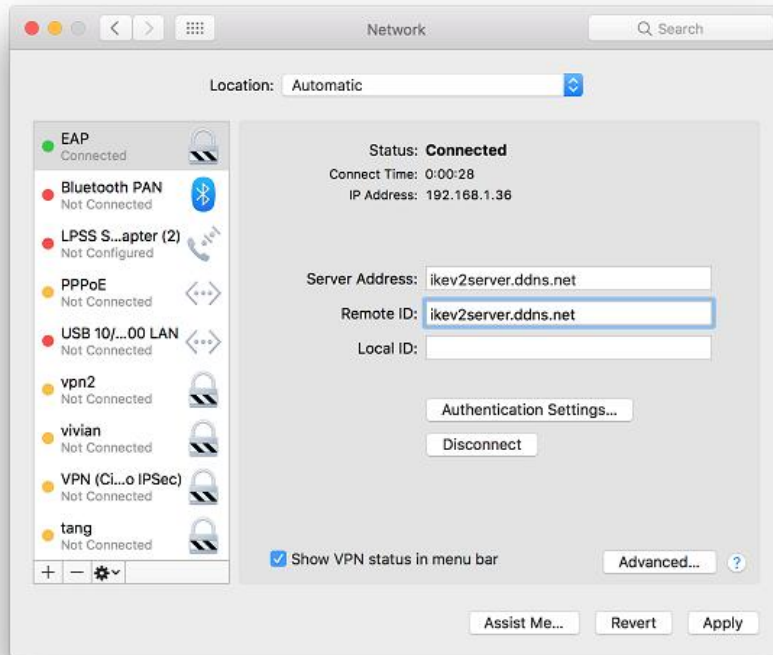
2. Extensible Authentication (EAP) ve IP Security (IPsec) için "Always Trust" seçeneğini seçin.



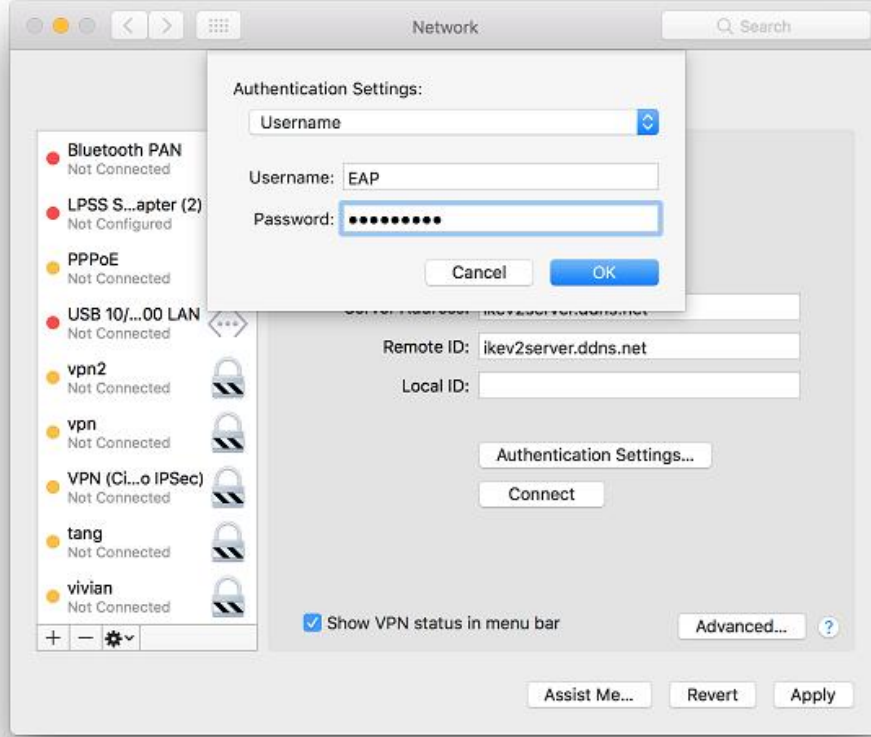
- Network ayarlarına gidin ve yeni bir ağ oluşturmak için '+'a tıklayın.
 - Interface** için "VPN" seçeneğini seçin.
 - VPN Type** için "IKEv2" seçeneğini seçin.
 - Create**'e tıklayın.



- Server Address** ve **Remote ID** için routerin domainini girin. Sonra **Authentication Settings...**'e tıklayın



5. Username seçeneğini seçin ve **Username** ve **Password** girin. Sonra **OK**'a tıklayın.



6. Routera VPN bağlantısı başlatmak için **Connect**'e tıklayın.

