

VIGOR ROUTER'DA XCA İLE OpenVPN KURUUMU

OpenVPN, ağ santralleri için SSL/TLS kullanan özel bir güvenlik protokolü kullandığından network address translators (NAT) ve Firewall'a geçiş yapabilen açık kaynaklı bir VPN teknikleridir. Sertifika OpenVPN'in desteklediği client kimlik doğrulama yöntemlerinden biridir. Sertifikayı imzalamak için bir Certificate Authority (CA) yazılımı olan XCA'yı kullanacağız. Bu makale şunları içermektedir.

- Bölüm 1. Router üzerinde Server Sertifikası Yapma
- Bölüm 2. XCA'a yeni bir CA Oluşturma
- Bölüm 3. Signed Server Sertifikası ile CA Sertifikasını Router'a Alma
- Bölüm 4. VPN client için Private Sertifika ve Private Key Oluşturma
- Bölüm 5. OpenVPN Serveri olarak Router Kurulumu
- Bölüm 6. OpenVPN GUI'de Client Kurulumu

Bölüm 1. Router Üzerinde Server Sertifikası Yapma

1-1. Sertifikanın geçerli bir süresi olduğundan routerın saat ayarlarının **System Maintenance >> Time and Date** sayfasından doğru olup olmadığını kontrol edin.

System Maintenance >> Time and Date

Time Information

Current System Time: 2018 Jul 31 Tue 16 : 29 : 19

Time Setup

Use Browser Time

Use Internet Time

Time Server:

Priority:

Time Zone:

Enable Daylight Saving:

Automatically Update Interval:

Send NTP Request Through:

1-2. Yeni bir sertifika oluşturmak için **Certificate Management >> Local Certificate** sayfasına gidin. Bilgileri doldurun ve sonra **Generate**'e tıklayın.

Certificate Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name:

Subject Alternative Name

Type:

IP:

Subject Name

Country (C):

State (ST):

Location (L):

Organization (O):

Organization Unit (OU):

Common Name (CN):

Email (E):

Key Type:

Key Size:

Algorithm:

1-3. Generate'e tıkladıktan sonra CA tarafından imzalanması gereken Sertifika Sign Request 'i göreceksiniz. Sertifikayı PEM Format Content'den kopyalayın.

Certificate Signing Request Information

Certificate Name :	openvpn
Issuer :	
Subject :	C=TW, ST=OPEN, L=VPN, O=Draytek, OU=Vigor, CN=118.166.188.111, emailAddress=root@ca.com
Subject Alternative Name :	IP:118.166.188.111
Valid From :	
Valid To :	
PEM Format Content :	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIC6jCCAdICAQAwYIx CzA JBgNVBAYTA1RXMQ0wCwYDVQQIDARPUVOMQwwCgYD VQ QHDANWUE4xEDA0BgNVBAoMB0RyYX10ZWxsXDJAMBgNVBA sMBVZpZ29yMRgwFgYD VQ QDDA8xMTguMTY2LjE4OC4xMTE xGjAYBgkqhkiG9w0BCQEWc3Jvb3RAY2EuY29t MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASBfoSXCc4zPe8A/ktTuK IbkNh12pr7Lkni3SAfTKW7yg5fNQ921L5MJ3kYVZVGA7v9K6yKLTvPzm4j5dI 4huRmxyQntABvakvd3HEqKEmYtfrYya64Vk/MOW38ZxagfTzu7D05h09S7IcHInk gFn+Aiee/nJfxLKe4pJfJfRIaIRezdN/s00wIMguhFN5Qe9d1J78rQczqVEvKYE 5xRN48wc8muBEwL10QpOc/6c/RfEzIABTFoi19VDHTSMNB1aVLgd1wQ5qCjk3JX BIZ4CjOn6AnskPK7CcWeQhZM0juweoqQKJcT2vG//7Zw7D0d/t+GEsd8PHXgP9L6 nwIDAQABoCIwIAYJKoZIhvcNAQKOMRmWETAPBgNVHREEDAGhwR2prxvMA0GCSqG SIb3DQEBCwUAA4IBAQDi6yheahTw2r7bE70Xp7ImKK2RTo1A21INS5j96aQaQtcd </pre>

Close

Bölüm 2. XCA'da Yeni Bir CA Oluşturma

2-1. XCA'yı başlatın Certificates sekmesine gidin **New Certificate**'e tıklayın. **Create a self-signed Certificate with the serial**'i seçin. CA şablonunu uygulamak için **Apply all**'a tıklayın.

X Certificate and Key management

File Import Token Extra Help

Private Keys Certificate signing requests Certificates Templates Revocation lists

Internal name commonName CA Serial Expiry date CRL Expiration

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Signing request

Sign this Certificate signing request

Copy extensions from the request

Modify subject of the request

Signing

Create a self signed certificate with the serial 1

Use this Certificate for signing

Signature algorithm SHA 256

Template for the new certificate [default] CA

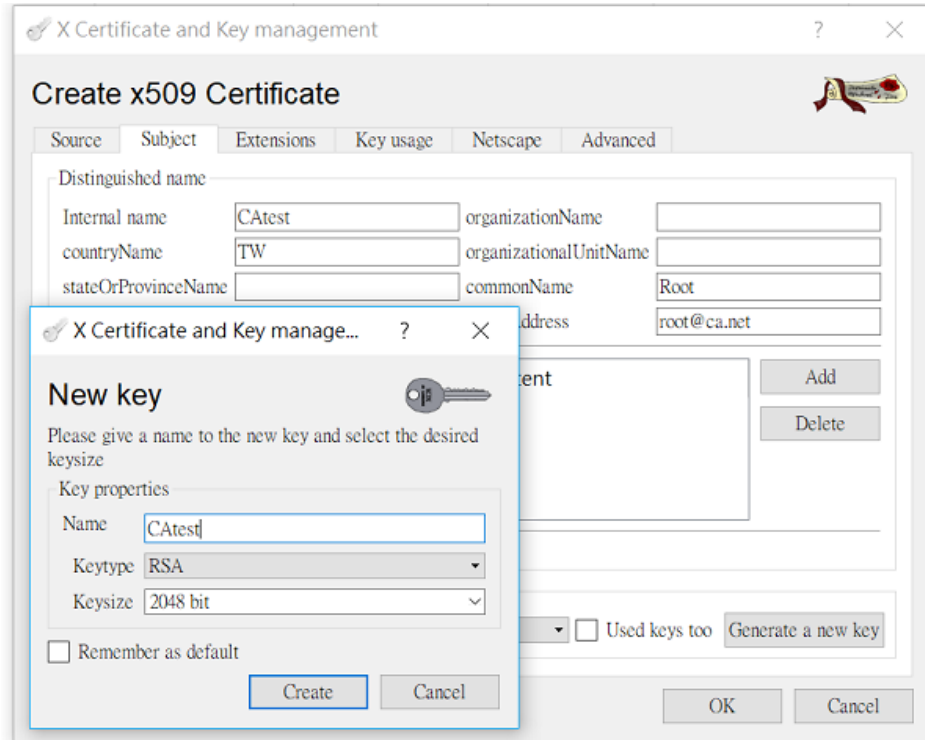
Apply extensions Apply subject **Apply all**

OK Cancel

Database: D:/User/Documents/EAPxdb

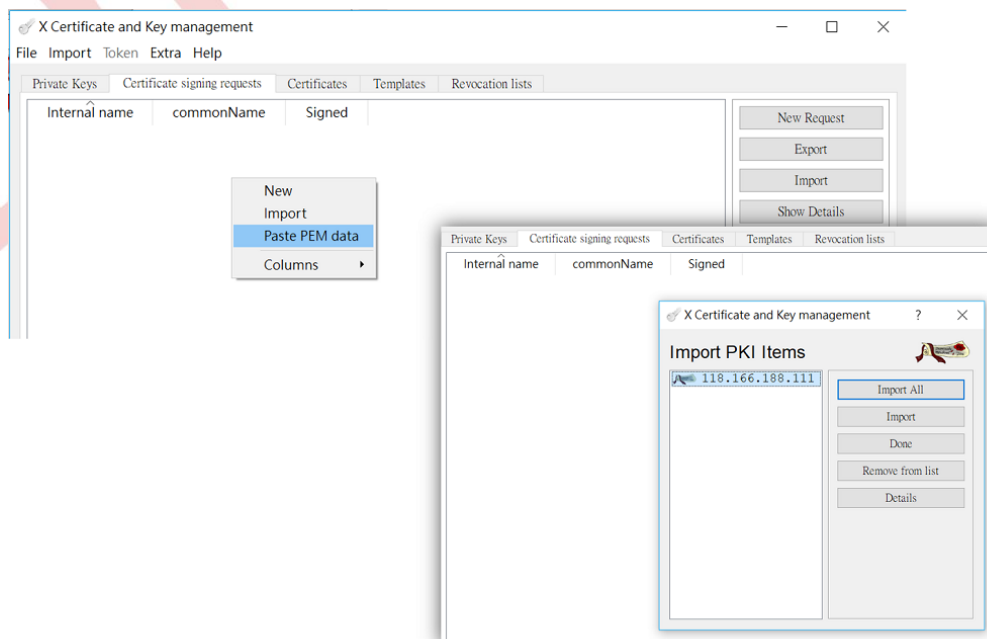
2-2. Subject sekmesine gidin.

- Sertifika için ayırt edici özellikler girin sonra **Generate a new key**'e tıklayın.
- **Keytype** için "RSA" ve **Keysize** için "2048 bit" seçin sonra **Create**'e tıklayın.
- CA sertifikasını oluşturmak için OK'a tıklayın. Artık server sertifikası ve client sertifikası imzalamak için Trusted (Güvenilir) CA Sertifikamız var.

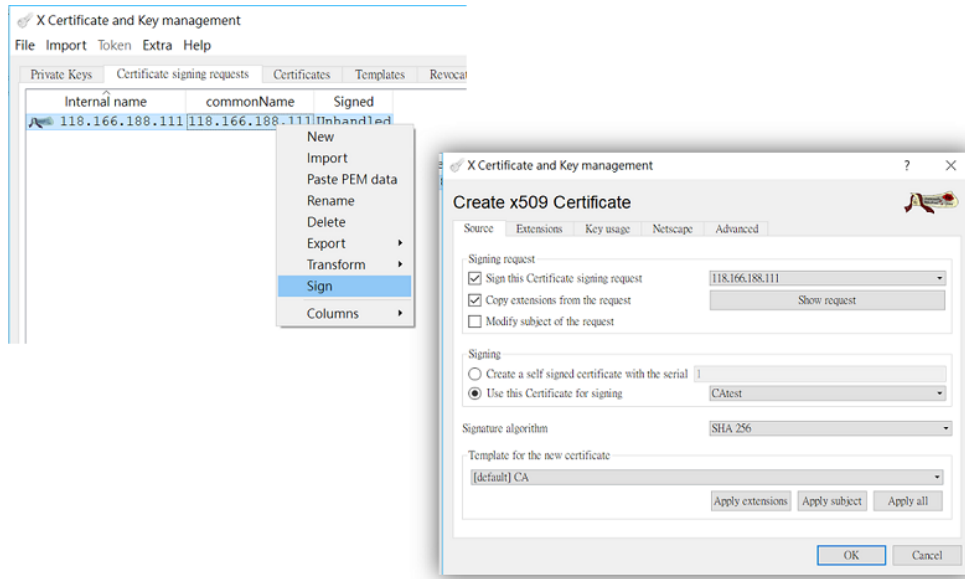


Bölüm 3. Signed Server Certificate ve CA Certificate Router'a Alma

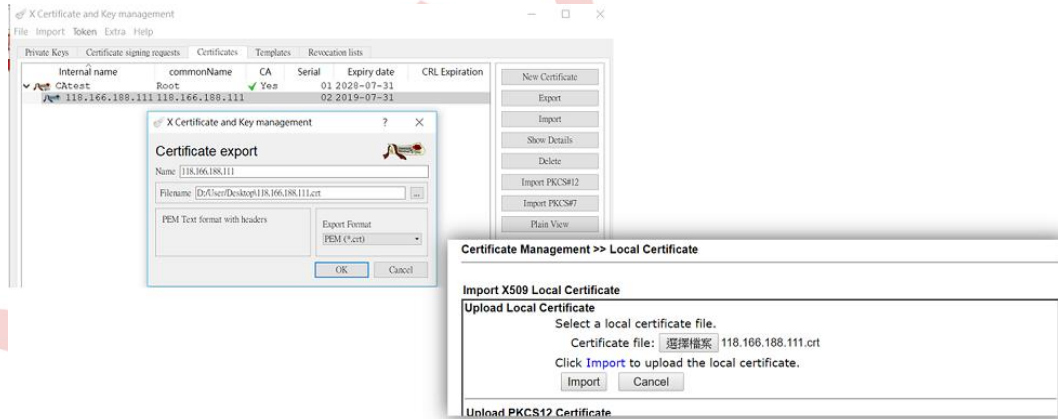
3-1. Certificate signing requests sekmesine gidin. Paste PEM data'yı seçin ve 1-3'te routerdan kopyalanan PEM Format Content'ini yapıştırın.



3-2. Alınan sertifikayı sağ tıklayın ve **Sign** seçeneğini seçin. İmzalamak 2. adımda oluşturulan sertifikayı kullanın.



3-3. Signed Local Certificate'ı .crt formatında export edin. Router'ın GUI'sine geri dönün ve export edilen belgeyi **Certificate Management >> Local Certificate >> Upload Local Certificate** sayfasından routera alın.



3-4. Yüklenen sertifikanın durumunun OK olduğundan emin olun.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

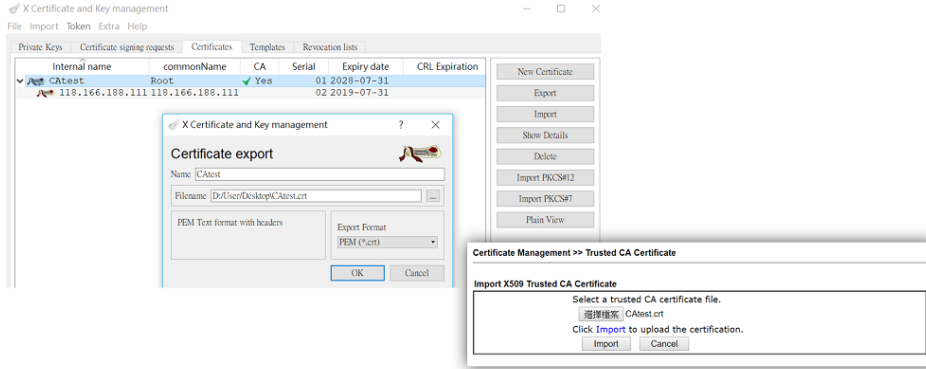
Name	Subject	Status	Modify	
openvpn	/C=TW/ST=OPEN/L=VPN/O=Drayte...	OK	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

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

3-5. XCA'da Certificate sekmesine gidin CA sertifikasını seçin ve .crt formatında dışarı aktarın. **Certificate Management >> Trusted CA Certificate** sayfasından routera alın.



3-6. Alınan Trusted CA'nın durumunun **OK** olduğundan emin olun.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA	---	---	Create
Trusted CA-1	/C=TW/CN=Root/emailAddress=r...	OK	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

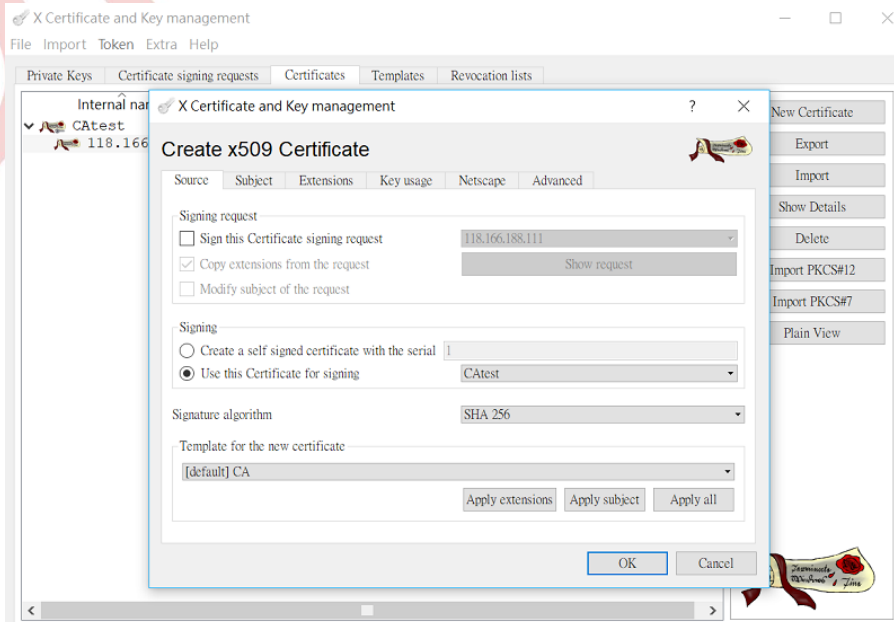
Note:

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

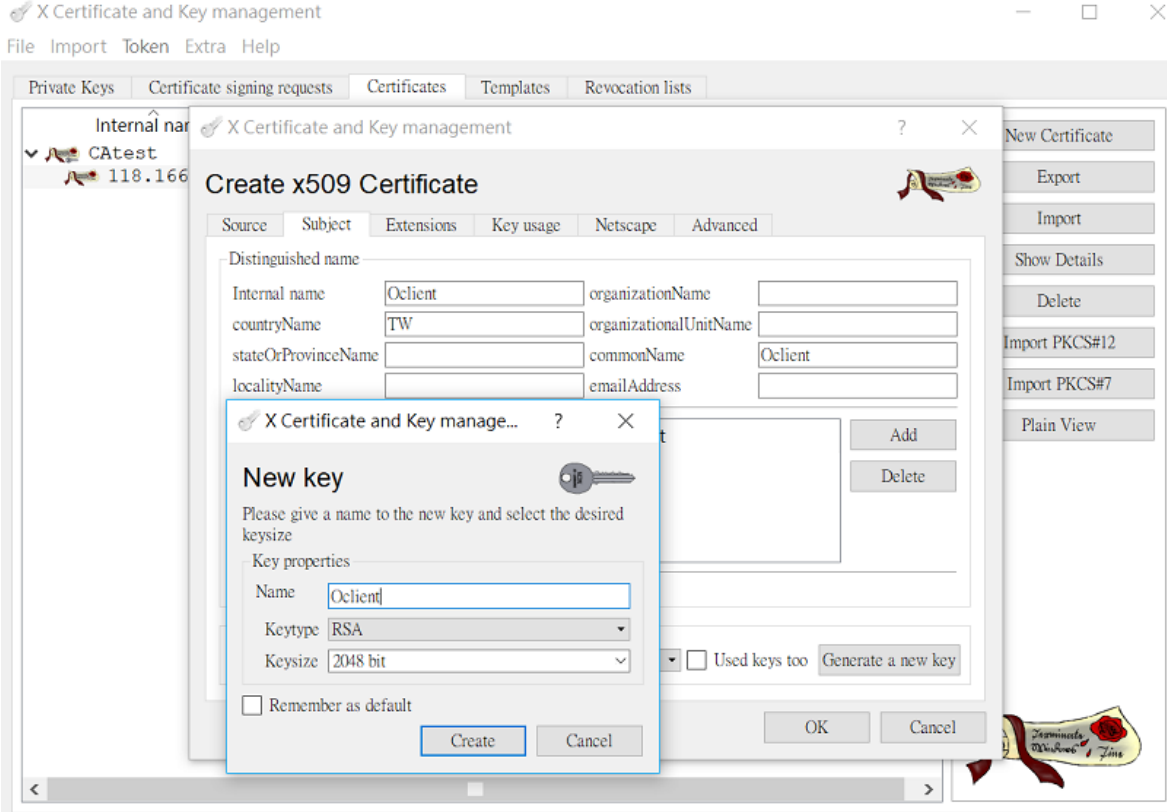
Bölüm 4. VPN Client için Private Sertifika ve Private Key Oluşturma

4-1. XCA'da Certificates'e gidin, **New Certificate**'e tıklayın. Signing başlığı altında imzalanan sertifikayı kullanmak için Use this Certificate for signing 2i seçin.

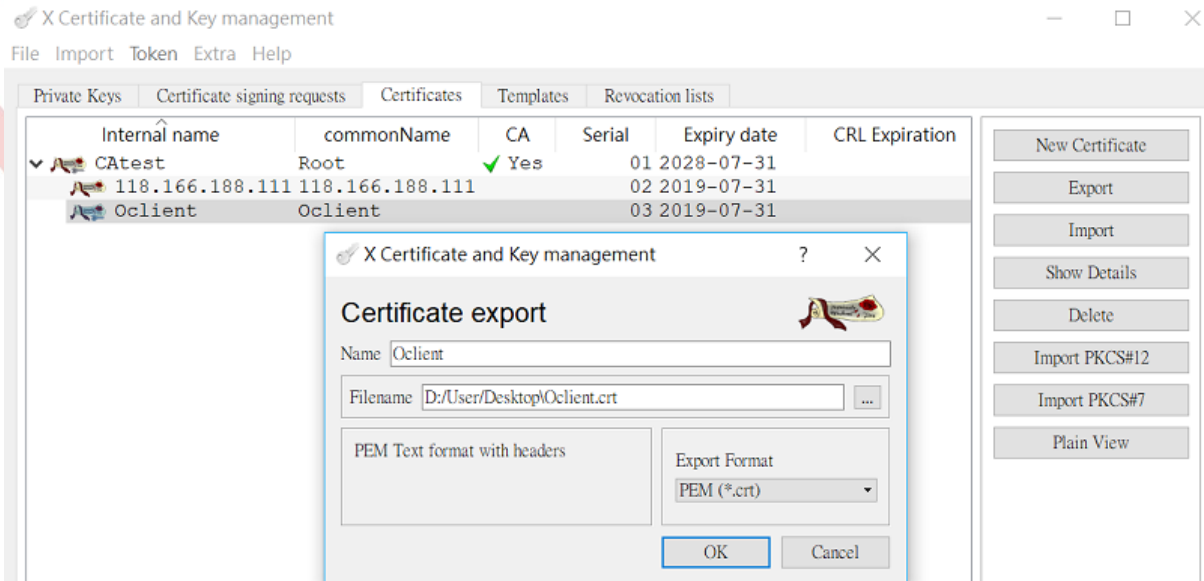


4-2. Subject sayfasına gidin.

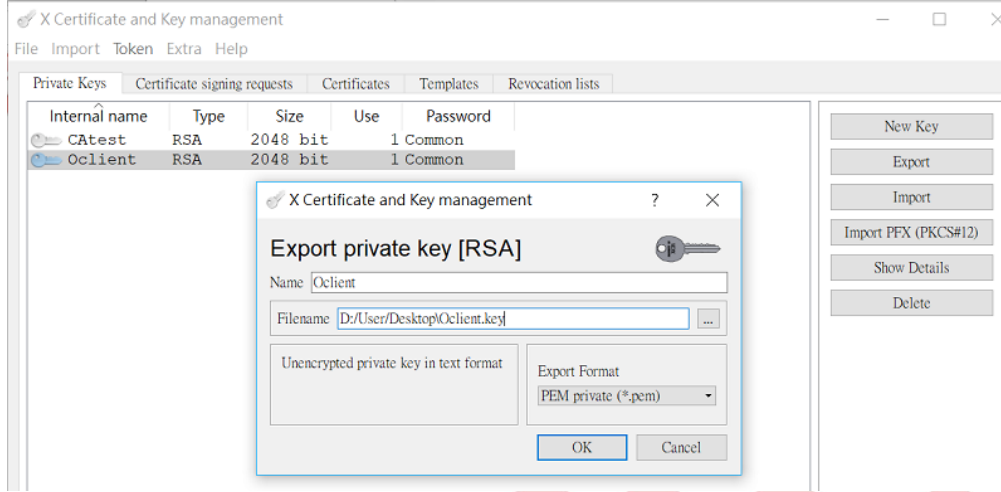
- Sertifika için ayırt edici özellikler girin sonra **Generate a new key**'e tıklayın.
- **Keytype** için "RSA" ve **Keysize** için "2048 bit" seçin sonra **Create**'e tıklayın.
- CA sertifikasını oluşturmak için OK'a tıklayın. Artık VPN Client'ı içinde özel bir sertifikamız var.



4-3. Certificates'e gidin, yeni oluşturduğunuz sertifikayı seçin. Sertifikayı .crt formatında dışa aktarın ve VPN Client'ına ekleyin.

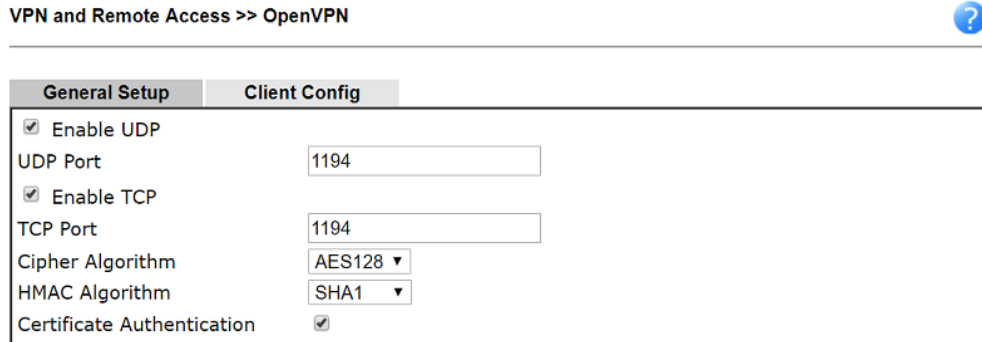


4-4. Private Keys'e gidin, Private Key (Oclien.key) dışa aktarın, uzantı adını elle .key olarak değiştirin. Ardından VPN Client'a ekleyin.

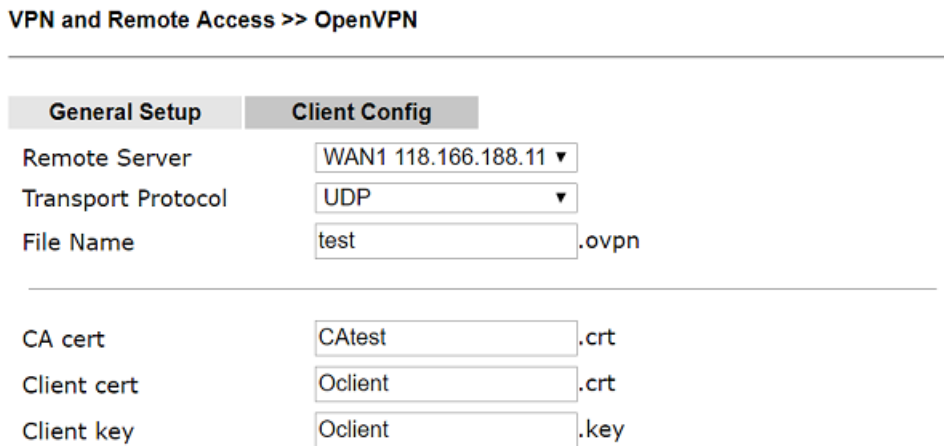


Bölüm 5. OpenVPN Serveri olarak Router Kurulumu

5-1. VPN and Remote Access >> OpenVPN General Setup sayfasına gidin ve görseldeki konfigürasyonları yapın.



5-2. Client Config sekmesine gidin. CA Certificate, Client Certificate ve Client Key dosya adlarını belirtin. Sonra **Export**'a tıklayın.



Note:

Please make sure the CA files are located in the same folder with .ovpn file.

Export

5-3. OpenVPN Dial-in kullanıcılarına yeni kullanıcı profili oluşturmak için **VPN and Remote Access >> Remote Dial-in User** sayfasına gidin. **Enable this account**'u etkinleştirin. **Username/Password** girin ve Allowed Dial-in Type'de **OpenVPN Tunnel**'i etkinleştirin.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account

Idle Timeout second(s)

Allowed Dial-In Type

PPTP

IPsec Tunnel

IPsec XAuth

L2TP with IPsec Policy

OpenVPN Tunnel

IKEv2 EAP

Specify Remote Node

Remote Client IP

or Peer ID

Netbios Naming Packet Pass Block

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Username

Password

Enable Mobile One-Time Passwords(mOTP)

PIN Code

Secret

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key

Digital Signature(X.509)

IPsec Security Method

Medium(AH)

High(ESP) DES 3DES AES

Local ID (optional)

5-4. Server sertifikasını bölüm 2'de oluşturulan Local sertifikaya değiştirmek için **SSL VPN >> General Setup** sayfasına gidin.

SSL VPN >> General Setup

SSL VPN General Setup

Bind to WAN WAN1 WAN2 WAN3 WAN4

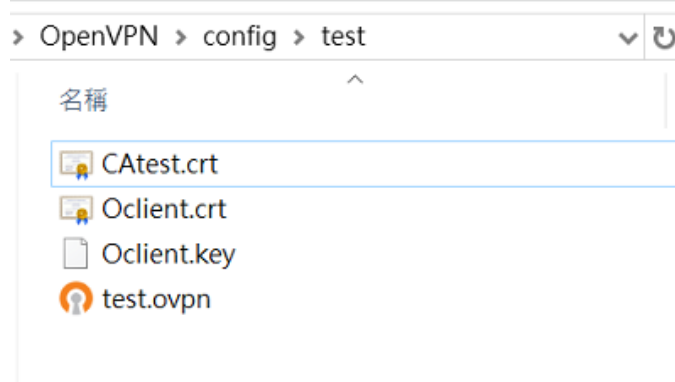
Port (Default: 443)

Server Certificate

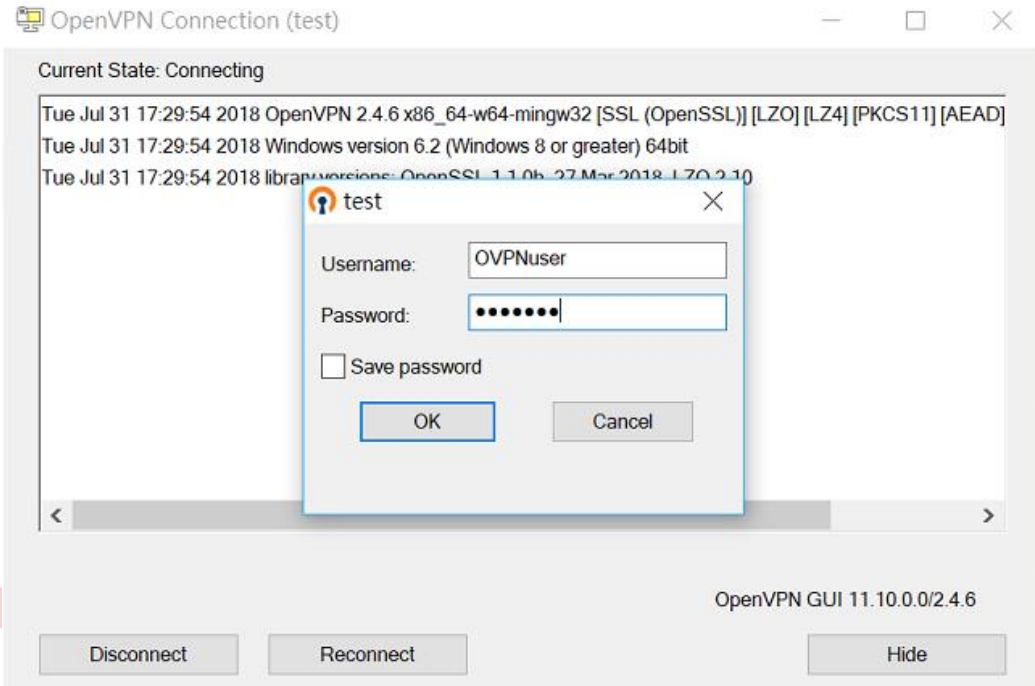
Bölüm 6. OpenVPN GUI'de Client Kurulumu

6-1. OpenVPN konfigürasyonunu (test.vpn) OpenVPN GUI'ye aktarın. OpenVPN config klasörüne koymak için üç dosya vardır.

- Trusted CA Certificate (CAtest.crt)
- Private Certificate (Oclient.crt)
- Private Key (Oclient.key)



6-2. **Connect**'e tıklayın ve 5-3 adımdaki yapılandırılan username/password girin.



OpenVPN Tunnel'i kurulduktan sonra VPN durumunu **VPN and Remote Access >> Connection Management** sayfasından görebilirsiniz.

VPN and Remote Access >> Connection Management

Dial-out Tool | Refresh |

General Mode:		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(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime
1 (OVPNuser) Local User Database	OpenVPN AES-SHA1 Auth	118.166.186.70 via WAN1	192.168.89.11/32	1048	438.40	947	56.10	0:3:56

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

Sorun Giderme**VERIFY ERROR: error=self signed certificate**

Router ie aktardığımız sertifika yerine VPN iin kendinden imzalı sertifika kullanıyor. SSLVPN >> General Setup sayfasında Server Sertifikası ayarlarını kontrol edin (adım 5-4).

DrayTek