



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 Sertikasını Router'a Alma
- Bölüm 4. VPN client için Private Sertifika ve Private Key Oluşturma
- Bölüm 5. OpenVPN Serverî 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.

nformation			
Current System Time	2018 Jul	31 Tue 16 : 29 : 19	Inquire Time
etup			
Use Browser Time			
Use Internet Time			
Time Server		pool.ntp.org	
Priority		Auto 🔻	
Time Zone		(GMT+08:00) Taipei	•
Enable Daylight Savir	ig	Advanced	
Automatically Update	Interval	30 mins 🔻	
Send NTP Request Th	rough	Auto 🔻	

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

Generate Certificate Signing Reque	st	
Certificate Name	openvpn	
Subject Alternative Name		
Туре	IP Address	
IP	118.166.188.111	
Subject Name		
Country (C)	TW	
State (ST)	OPEN	
Location (L)	VPN	
Organization (O)	Draytek	
Organization Unit (OU)	Vigor	
Common Name (CN)	118.166.188.111	
Email (E)	root@ca.com	
Кеу Туре	RSA *	
Key Size	2048 Bit 🔻	
Algorithm	SHA-256 •	





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 :	BEGIN CERTIFICATE REQUEST MIIC6jCCAdICAQAwgYIxCzAJBgNVBAYTA1RXMQ0wCwYDVQQIDARPUEVOMQwwCgYD VQQDDANWUE4xEDAODgNVBAOMB0RYYX10ZWsxDjAMBgNVBASMBVZpZ29YMRgWFgYD VQQDDA8xMTguMTY2LjE40C4xMTExGjAYBgkqhkiG9w0BCQEWC3Jvb3RAY2EuY29t MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEASBfoSXCC42Pe8A/ktTuK IbkNh12pr7Lkni3SAfTKW7yg5fNQ921L5MJ3kYVZVGaBU7v9K6ykLHtvPzm4j5dI 4huRmxyQntABvakvd3HEqKEmYtfrYya64Vk/MOW38ZxagfTZu7D05h09S7IcHInk gFnN+Aiee/nJfxLke4pJfJfRIaIRezdN/SOOWIMguhFNSQe9d1J78rQczqVEvKYE 5xRN48wc8muBEdWL10Qp0c/6c/RFEzIABTFoi19VDHTSMNBlaVLgd1wQ5qCjk3JX BIZ4Cj0n6AnskPK7CcWeQhZM0juweoqQKJcT2vG//7Zw7D0d/t+GEsd8PHXgP9L6 nwIDAQABoCIWIAYJKoZIhvcNAQkOMRMwETAPBgNVHREECDAGhwR2prxvMA06CSqG SIb3DQEBCwUAA4IBAQDi6yheahTw2r7bE70Xp7ImKK2RT0lA21INS5j96aQaAQtd

Close

Bölüm 2. XCA'da Yeni Bir CA Oluşturma

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

Internal nar	me commonName	CA	Serial	Expiry date	CRI Exr	iration		
	X Cartificate and Key ma	nagement	Jeria	copity dute	CITE EN	2	\mathbf{v}	New Certifi
	A certificate and key ma	nagement				1	^	Export
0	Create x509 Certifi	cate				, Au	1	Import
	Source Subject Extens	ions Key u	sage Net	scape Advar	iced			Show Deta
	-Signing request							Delete
	Sign this Certificate signing	1g request					*	Import PKC
	Copy extensions from the	request			Show request			Import PK(
	Modify subject of the requ	iest						Disia Via
	Signing						_	Fiam vie
	• Create a self signed certif	icate with the s	erial 1					
	 Use this Certificate for signal 	gning					w.	
	Signature algorithm		SE	IA 256			-	
	-Template for the new certifica	te						
	[default] CA						•	
			Aj	ply extensions	Apply subject	Apply all	- 11	
							-	
					OF	Can	aal	Jegmineste Minfing
					OK	Can	cei	





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.

0.11					
ource Subject	Extensions Key u	isage Netscape	Advanced		
Distinguished name -					
Internal name	CAtest	organizationNa	ame		
countryName	TW	organizationalU	UnitName		
stateOrProvinceNam		commonNama	Deet		
state off formeet all.	<i>L</i>	commonwante	KOOL		
X Certificate and	™d Key manage	? × ddress	root@ca.n	et Add	
X Certificate an Jew key lease give a name to sysize	d Key manage the new key and select	? × ddress ent the desired	root@ca.n	et Add Delete	
X Certificate and V Certificate and Vew key lease give a name to sysize Key properties	d Key manage d Key manage the new key and select	? × ddress the desired	root@ca.n	et Add Delete	
X Certificate and V Certificate and lease give a name to sysize Key properties Name CAtest	d Key manage d Key manage the new key and select	? × ddress ent the desired	root@ca.n	et Add Delete	
X Certificate an V Certificate an V Certificate an Vexture a name to sysize Key properties Name CAtest Keytype RSA	d Key manage the new key and select	? × ddress ent the desired	root@ca.n	et Add Delete	
X Certificate an V Certificate an Vertificate an Vertificat	d Key manage the new key and select	? × ddress ent the desired	root@ca.n	Add Delete	

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 yapştırın.

X Certificate and Key management File Import Token Extra Help Private Keys Certificate signing requests Certificates Templates	Revocation lists	- 0 X
Internal name commonName Signed New Import Paste PEM data Columns	Private Keys Certificate signing requests Certificate Internal name commonName Signed Image: CommonName Signed X Certificate Image: CommonName Signed Image: CommonName Image: CommonName Signed Image: CommonName Image: CommonName CommonName Signed Image: CommonName Signed Image: CommonName Image: CommonName Signed Image: CommonName Signed Image: CommonName Signe <td< td=""><td>New Request Export Import Show Details s Templates Revocation lists ficate and Key management ? × PKI Items \$.166.188.1111 Import All Import All Done Remove from list Details</td></td<>	New Request Export Import Show Details s Templates Revocation lists ficate and Key management ? × PKI Items \$.166.188.1111 Import All Import All Done Remove from list Details





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

🛷 X Certificate and Key management					
File Import Token Extra Help					
Private Keys Certificate signing requests	Certificates Templates	Revocal			
Internal name commonN.	ame Signed 8.111 Inhand Led New Import Paste PEM data Rename Delete Export • Transform • Sign Columns •	X Certificate and Key management Create x509 Certificate Surce Extension Key usage Netscape Signing request Copy extensions from the request Copy extensions from the request Copy extensions from the request Copy extensions from the request Signing Create a self signed certificate with the serial Copy Extensions Signature algorithm Template for the new certificate Gefault] CA	Advanced 118.166,188.111 Show request CAtest SHA 256 Apply extensions Apply subject OK	? ×	

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

A A	ing requests Certificates Templates	Revocation lists		
Internal name	commonName CA S Root Ves	Serial Expiry date CRL 01 2028-07-31	L Expiration New Certificate	
A 118.166.188.1	11 118.166.188.111	02 2019-07-31	Export	
	S Certificate and Key manageme	ent ? ×	Import	
	Certificate export	0	Show Details	
	Name 118.166.188.111		Delete	
	Elemente Dr./ Local Desironi 118 166 188	lllot 100	Import PKCS#12	
	The many Development of the footboard		Import PKCS#7	
	PEM Text format with headers	Export Format	Plain View	
		(PEM (*.crt) •	Certificate Management >> Local Certificate	
		OK Cancel		
			Import X509 Local Certificate	
			Upload Local Certificate	
			Select a local certificate file.	
			Click Insert to unload the local settificate	
			Click Import to upload the local certificate.	

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	ОК	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 REFRESH





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

		- 🗆 X
Private Keys Certificate signing requests Certificates Templates Revocation lists		
Internal name commonName CA Serial Expiry date	CRL Expiration	New Certificate
Ar 118.166.188.111 118.166.188.111 02 2019-07-31		Expert
SX Certificate and Key management ?	×	Import Show Details
Certificate export		Delete
Name CAtest		Import PKCS#12
Filename D:/User/Desktop/CAtest.crt		Import PKCS#7
PEM Text format with headers Expert Format TTTT (A		Ptain View
(PEM (*20)	Certificate	te Management >> Trusted CA Certificate
OK C	Cancel Import X5	K509 Trusted CA Certificate
		Select a trusted CA certificate file. 通過階級人 Coast or Click Import to upload the certification. Import Cancel

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	ОК	View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

Note:

1. 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
--------	---------

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.

Internal nar	X Certificate and Key management	2 ×	
✓ A CAtest			New Certificate
A 118.166	Create x509 Certificate		Export
	Source Subject Extensions Key usage	Netscape Advanced	Import
	(Contine another t		Show Details
	Signing request	119 166 199 111	Dalata
	General and an and a second se	Phone accurat	Delete
	Copy extensions from the request	Show request	Import PKCS#12
	Modify subject of the request		Import PKCS#7
	Signing		Plain View
	O Create a self signed certificate with the serial	1	Than The tr
	 Use this Certificate for signing 	CAtest	
	Signature algorithm	SHA 256 *	
	Template for the new certificate		
	[default] CA	•	
		Apply extensions Apply subject Apply all	

 \wedge





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.

	are signing requests contractes reinplaces revocation rises		
Internal nar	♂ X Certificate and Key management	? ×	New Certificate
▲ 118.166	Create x509 Certificate	A a constant	Export
	Source Subject Extensions Key usage Netscape Advanced		Import
	Distinguished name		Show Details
	Internal name Oclient organizationName		Delete
	countryName TW organizationalUnitName stateOrProvinceName Oclient		Import PKCS#12
	localityName emailAddress		Import PKCS#7
	√ X Certificate and Key manage ? × t	Add	Plain View
	New key	Delete	
	Please give a name to the new key and select the desired keysize Key properties		
	Name Oclient		
	Keytype RSA ·		
	Keysize 2048 bit Used keys too C	Benerate a new key	
	Remember as default	Cancel	
	Create Cancel	cancer	H Distante

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

Internal name commonName CA Serial Expiry date CRL Expiration CAL Expiration CAL Expiration CAL Expiration New C C		ig requests Certificates Template	es Revocation lists		
Oclient 03 2019-07-31 X Certificate and Key management ? × Certificate export Import Name Oclient Import Filename D:/User/DesktopVOclient.crt Import PEM Text format with headers Export Format	Internal name A CAtest A 118.166.188.1	commonName CA Root ✓ Yes 11 118.166.188.111	Serial Expiry date 01 2028-07-31 02 2019-07-31	CRL Expiration	New Certificate
Certificate export D Name Oclient Import Filename D:/User/Desktop\Oclient.crt Import PEM Text format with headers Export Format	At Oclient	Oclient	03 2019-07-31 anagement	? ×	Import Show Details
Filename D:/User/Desktop\Oclient.crt Import PEM Text format with headers Export Format Plain		Certificate export			Delete Import PKCS#12
PEM Text format with headers Export Format Plai		Filename D:/User/Desktop\O	client.crt		Import PKCS#7
PEM (*.crt)		PEM Text format with header	S Export Format PEM (*.crt)	•	Plain View





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

X Certificate and Key man le Import Token Extra F	lagement Help	- 🗆 X
Private Keys Certificate sign	ning requests Certificates Templates Revocation lists	
Internal name Type Chrest RSA Chrest RSA	e Size Use Password 2048 bit 1 Common 2048 bit 1 Common 2048 bit 1 Common X Certificate and Key management ? × Export private key [RSA] Name Oclient Filename D:/User/Desktop/Oclient.key Unencrypted private key in text format PEM private (*.pem) OK Cancel	New Key Export Import Import PFX (PKCS#12) Show Details Delete

Bölüm 5. OpenVPN Serveri olarak Router Kurulumu

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

VPN and Remote Access	>> OpenVPN	?
General Setup	Client Config	
Enable UDP		
UDP Port	1194	
Enable TCP		
TCP Port	1194	
Cipher Algorithm	AES128 V	
HMAC Algorithm	SHA1 🔻	
Certificate Authentication	n 🕑	

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

	Chem Conng	
lemote Server	WAN1 118.166.18	3.11 🔻
ransport Protocol	UDP	V
-ile Name	test	.ovpn
CA cert Client cert	CAtest Oclient	.crt .crt
Client kev	Oclient	.key





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

Jser account and Authentication	Username	OVPNuser
Enable this account	Password	•••••
dle Timeout 0 second(s)	Enable Mobile One-Tir	ne Passwords(mOTP)
Allering d Diel I.e. Truce	PIN Code	
	Secret	
PPTP		
IPsec Tunnel	IKE Authentication Method	
IPsec XAuth	🖉 Pre-Shared Key	
L2TP with IPsec Policy None 🔻	IKE Pre-Shared Key	Max: 64 characters
SSL Tunnel	Digital Signature(X.50)9)
OpenVPN Tunnel	None V	
IKEv2 EAP		
Specify Remote Node	IPsec Security Method	
Remote Client IP	Medium(AH)	
	High(ESP) 🗹 DES 🗹	3DES 🗹 AES
or Peer ID	Local ID (optional)	
Netbios Naming Packet 💿 Pass 🔘 Block		
Multicast via VPN 🛛 🔍 Pass 💿 Block		
(for some IGMP IP-Camera DHCP Relay, etc.)		

VPN and Remote Access >> Remote Dial-in User

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

SSL VPN >> General Setu	1p
	·
SSL VPN General Setup	
Bind to WAN	🖉 WAN1 🖉 WAN2 🖉 WAN3 🖉 WAN4
Port	443 (Default: 443)
Server Certificate	openvpn 🔻

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)







<		2
	OpenVPN	N GUI 11.10.0.0/2.4.6

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

Dial-out Tool Refresh General Mode: Dial Backup Mode: Dial Load Balance Mode: Dial

VPN Connection Status

VPN and Remote Access >> Connection Management

All VPN Status	LAN-to-LAN VPN Status		Remote Dia	Remote Dial-in User Status					
VPN	Туре	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	Drop
					XXXXXXXX	: Dat	a is encrypt	ed.	

xxxxxxxx : Data isn't encrypted.





Sorun Giderme

VERIFY ERROR: error=self signed certificate

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