How to Establish OpenVPN Tunnels (Authenticate with CA) via SmartVPN Client?

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure pointto-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchanges. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority.



Note:

The OpenVPN choice supported by Vigor3200 Series can work with Windows, Linux and Mac OS. For the Windows-based PC, users can use SmartVPN client to simplify settings in the client devices.

Following is the step-by-step setting.

**Before setting, please make sure SmartVPN Client 4.1.0.1 is installed on the PC, and the firmware of the router is the latest version. Also please install XCA on the PC to utilize the CA Server feature.

**We define the network diagram as below :

PC----- Internet------ Vigor 3200------ LAN

Settings of PC :

IP address = 188.188.188.188

Settings of Vigor 3200 :

- WAN IP address = 200.200.200.200
- LAN: IP address = 192.168.1.1/24

XCA is a freeware for the CA Server. This article describes making the CA (Certificate Authentication) for Vigor users.

Part A : Time Setup

Please make sure the router is using Internet Time Client.

System Maintenance >> Time and Date

urrent System Time	2012 Mar 9 Fri 17 : 20 : 11	Inquire Time
tup		
) Use Browser Time		
◉ Use Internet Time Client		
Server IP Address	pool.ntp.org	
Time Zone	(GMT+08:00) Taipei	*
Enable Daylight Saving		
Automatically Undate Int.	erval 30 min 💙	

OK Cancel

Server IP Address	pool.ntp.org	
Time Zone	(GMT+08:00) Taipei	*
Enable Daylight Saving		
utomatically Update Interval	30 min 💌	

Part B : Making a Local Certificate and Trusted CA Certificate

Please go to **Certificate Management >> Local Certificate** to generate a Certificate Signing Request, and type related information in the **Subject Alternative Name** and **Subject Name** sections.

ick Start Wizard	Generate Certificate Signing Requ	st	
line Status	Subject Alternative Name		
N	Туре	Domain Name 💌	
	Domain Name	draytek.com	
ewall r Management	Subject Name		
ects Setting	Country (C)	TW	
m ndwidth Management	State (ST)		
N and Remote Access	Location (L)		
ocal Certificate	Organization (O)		
usted CA Certificate			
P	Organization Unit (UU)	draytek	
eless LAN	Common Name (CN)	vigor	
B Application tem Maintenance	Email (E)		
gnostics			
ernal Devices	Кеу Туре	RSA -	
	Koy Siza	1024 Bit M	

After clicking Generate, you will see the following screenshot.

Name	Subject	Status	Modify
Local	/C=TW/OU=draytek/CN=vigor	Requesting	View Delet
ENERATE	IMPORT REFRESH		
X509 L o	cal Certificate Request		
MIIBmD BgNVBA rgkSvG TjSuzi deR7S6 GDAWBg djFheg KMdr5A	CCAQECAQAWLZELMAKGA1UEBhMCVFcxEDAG MTBXZpZ29yMI6fMADGCSqGSIb3DQEBAQU W19JuvbmAR+Q6XBnTa96MwQ1EKQOodT37G JUjr745ECfwp9sFKrgskvwWMRMROwpXXXI OEuuVkcrLXMaBp8/+H++sDrv7dzQIDAQA NVHREEDZANggtkcmF5dGVrLmNvbTANBgkc Rjydo4hvtT+tJYN1upHDUHNI19tAQR8CyI SV9263tH7ujvF0/f4+Dy921akoR0Et1Rs] +KNG2FWGatVbn1520w4Br0fC2875360=	OBGNVBASTB2RyVX1 AAGNADCB1QKBgQD dfQCPexzja1OSd1k Decm8NAa1V1JVqF BCCkwJwVA0Z1hvc1 qhk1G9w0BAQUFAAO NTGV1uQNkcQIP+72 UUJQzv+qXhucNH4M =	DZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb MACKOMRow BgQBnuCnA gUYaMoOcG tYInctYtg

Launch XCA as CA Server

- 1. Click New Certificate.
- 2. Choose Create a self signed Certificate with the serial in the signing section.
- 3. Click **Apply All** to apply the CA Template.

2 of 12	│ 🛠 佇列 × 🗙 2012 × 🔘 drayi × 👔 Goo; × 🔘	🖋 X Certificate and Key management	
2 01 12	← → C ③ 192.168.1.1	<u>File Import Ioken H</u> elp	
	ಶ 免費的 Hotmail 🚺 建議的網站 🔇 網頁快訊圖庫 🌘	Private Keys Certificate signing requests Certificates Templates Revocation lists	
	Viziona	Internal name CA Serial Expiry date	
	X Certificate and Key management	Export	

3. Click **Apply All** to apply the CA Template.

倍列 × 🔆 2012 × 🔘 drayi × 👔 Goo₂ × 🦉 🖌 z	ertificate and Key management	
→ C (© 192.168.1.1	Import Ioken Help	
第件的 Hotmail 全部的 Hotmail 全部的 Hotmail 全部的 Hotmail 全部的 Hotmail 中 に 中 に 中 に に に に い の の い の い の い の い の い の い の い	te Keye Certificate iguing request Certificate Template Revocation lists temal name CA Senial Expiry date Revocation lists temal name Advanced	New Certificate Export Import Show Details Delete Import EKCS#12 Import PKCS#7
Gopy extensions from the request Copy extensions from the request Modify subject of the request Signing Orests a gelf signed certificate with the serial 1 Dis this Certificate for simple	Show request	Plain View
car Ist iff Signature algorithm A err	SHA 1	
[[default] C-Program FileStocalCA	Apply extensions] (Apply subject) Apply all	
3.9	OK Cancel	▼ ■ 顯示所有下載
開始 🔄 SW 🥱 Dra 💲 Sk 🗁 F4	🔁 A.U 🚺 D.L 🗪 C.A 🔁 X.C 📄 3rd 🖋 X	🚺 兼 CE 🕏 🗊 🐺 T 🕂 (

- 4. In Subject page, type a distinguishable or preferred name.
- 5. Click Generate a new key to create a RSA 1024 bit for this Certificate.
- 6. Click **OK**, and we have generated a Trusted CA Certificate well.

/ 🛠 佇列 × 🔆 🛠 2012 × 🔘 drayi × 🚺 Goo; × 🔘 🖌 X Certificat	te and Key management	_ 🗆 🔀
← → C ③ 192.168.1.1	Ioken Help	
ಶ 免費的 Hotmail 🚺 建簇的網站 🔇 網頁快訊圖庫 🚺 Private Keys	Certificate signing requests Certificates Templates Revocation lists	
	me CA Serial Expiry date	ew Certificate
AC		Export
Create x509 Certificate		Import
Off Source Subject Extensions Key usage Netscape #	Advanced	Show Details
Duick 1 Distinguished name		Delete
Service Online Dray CA test	organizationName	port PKCS#12
countryName TW	organizationalUnitName	port PKCS#7
LAN stateOrProvinceName	commonName jos	Plain View
NAT localityName	emailAddress jos@dreytek.com	
Object 1ype Object 1ype CSM Bandw Applicit VEN at Certifice New Key Trust New key Trust Place give a name to the new key and select the desired keysize Wirele Name USB At Dray CA ted System Keytype		To minacte
Extern:	te Cancel OK Cancel AU CA. CALCE CALCEL	↓ 顕 <u>元所有下載</u> × CE 《 <u>◎</u> 下午 05:31

From Certificate Management >> Local Certificate, we copy the X509 Local Certificate Request and paste to the XCA.

3 of 12 Certificate Management >> Local Certificate

9 Local Certifi	cate Configuration		
Name	Subject	Status	Modify

From Certificate Management >> Local Certificate, we copy the X509 Local Certificate Request and paste to the XCA.

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local	/C=TW/OU=draytek/CN=vigor	Requesting	View Delete
	IMPORT DEEDESH		
	INFORT RETREST		
X509 Loca	Certificate Request		
BEC	IN CERTIFICATE REQUEST		
BEC MIIBmDCC	IN CERTIFICATE REQUEST AQECAQAWLZELMAKGA1UEBhMCVFCXEDA	OBgNVBAsTB2RyYX1	OZWaxDjAM
BEC MIIBmDCC BgNVBAMT	IN CERTIFICATE REQUEST AQECAQAwLzELMAKGA1UEBhMCVFcxEDA BXZpZZ9yMIGfMAGCSqGSIb3DQEBAQU	OBGNVBASTB2RyYX1 AA4GNADCBiQKBgQD	OZWsxDjAM Q/ADOP/tt
HIIBmDCC BgNVBAM7 rgkSvGW1	IN CERTIFICATE REQUEST AQECAQAwLZELMARGA1UEBhMCVFCXEDA BXZpZ29yMIGfMAOGCSqGSIb3DQEBAQU 9JuvbmAR+Q6XBnTa96MwQ1EKQ0od137 (OBgNVBAsTB2RyYX1 AA4GNADCB1QKBgQU dfQCPexzja10Sd1k	OZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKoburb
BEC MIIBmDCC BgNVBAM7 rgkSvGW1 TjSuzijU deP7560B	IN CERTIFICATE REQUEST AQECAQAwLZELMARGA1UEBhMCVFCXEDA BXZpZ29yMIGfMAOGCSqGSIb3DQEBAQU 9JuvbmAR+Q6XBnTa96MwQ1EKQOodT37 (jr745ETy985F/tq3kvwUMRMROPXXx uVUVcr1V9858/t41+2Dvr7doDA0A	OBgNVBAsTB2RyVX1 AA4GNADCBiQKBgQD dfQCPexzja1OSd1k Decm8NAaiV1JVqeF BaCkriuvIVa7Tuvc	OZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb NAOKOMPan
BEC MIIBmDCC BgNVBAM rgkSvGWJ TjSuzijU deR7S60B GDAWBGN	IN CERTIFICATE REQUEST AQECAQAHLZELMAKGA1UEBBMCVFCXEDA BXZpZ29yMIGfMA0GCSqGSID5DQEBAQU 9JuvbmAR+Q6XBnTa96MwQ1EKQ0odT37 (jr745ECfwp9sFKrqskvwUNRMROwpXXX uuVKcrLXMa8Bs/+H++sDzv7dzQIDAQA HDFFD2AMortkrmF5GVL1wMbTANBck	OBgNVBAsTB2RyYX1 AA4GNADCBiQKBgQD dfQCPexzja10Sd1k Decm8NAaiV1JVqeF BoCkwJwYJKoZ1hvci abkiG9wDBA0UFAA0	02WsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb NAQKOMRow BaCBRuCnà
BEC MIIBmDCC BgNVBAMJ rgkSvGWJ TjSuzijU deR7S60B GDAWBgNV diFhecR ²	IN CERTIFICATE REQUEST AQECAQAWLZELMAKGAIUEBBMCVFCXEDA BX2pZ29yMIGFMAOGCSqGSIb3DEBAQU 9JuvbmAH-Q6XBnTq96Mw01EFQQDaT37 (jr745ECfwp9sFKrqskvwUMRMROwpXXX uuVKcrLXMa8p8/+H++sDrv7dz0IDA0A HREEDZANggbKcmF5dGVrLmNvbTANBgk vdc4hvrTqrLsJMiubHDUHNI19140R8C0	OBgNVBAsTB2RyVX1 AA4GNADCB1QKBqQD dfQCPexzja10Sd1k Decm8NAa1V1JVqeF BoCkwJWYJK0Z1Nvc; qhk1G9w0BAQUFAA0 NTaV1u0Nkc0IP+72	OZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb NAQKoMRow BqQBnuCnA WUYaMoOcG
BEC MIIBmDCC BgNVBAM rgkSvGWJ TjSuzijU deR7S60B GDAWBgNV djFhegR KMdr5ASV	IN CERTIFICATE REQUEST AQECAQAwLZELMAKGA1UEBhMCVFCXEDA BXZDZ299MIGEMAOCCSqGSIb3DQEBAQU 9JuvbmAR+Q6XBnTa96MwQ1EKQOodT37 jr745ECfwp9sFKrqskvwUMRMROwpXXx uuVkcrLXMa8p8/+H++sDrv7dzQIDAQA HREEDzANggtkcmF5dGVtLmNvbTANBgk ydo4hvtT+tJYMiupHDUHNI19tAQR8Cy 9265tH7uVr0/f4H0921akcR0EtLR8	OBgNVBAsTB2RyV1 AAGNADCB1QKBgQD dfQCPexzja10Sd1k Decm8NAaV1VJVge BoCkwJwYJKoZIhvc qhk1G9w0BAQUFAA0 NTgV1uQNkcQIP+72 UUJQ2v4aXhucNH4M	OZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb NAQKOMRow BgQBnuCnA yUYaMoOCG tyInctYtq
BEC MIIBmDCC BgNVBAM rgkSvGWJ TjSuzij deR7S60 GDAWBgNV djFhegR KMdr5ASV jriogn+B	IN CERTIFICATE REQUEST AQECAQAwLZELMAKGA1UEBhNCVFCXEDA BXZDZ29yMIGFMAOGCSqGSIb3DQEBAQU 9JuvbmAR+Q6XBnTa96MwQ1EKQOodT37 (jr745ECEwp9FKrqskvwUMRMROwDXXX uvVkcrLXMa8p8/+H++sDrv7dzQIDAQA HREEDzANggtkcmF5dGVrLmNvbTANBgk ydo4hvT+tJVMiupHDUBNI19tAQR6Cy 9263tH7ujvFd74H09921akoROEtIR3 UG2rMq3tVho15204BrOfC2875SGQ=	OBgNVBAsTB2RyYX1 AA4GNADCB1QKBgQD dfQCPexzja10Sd1k Decm8NAa1VJJVqeF BCCkwJwYJKoZ1hvcj qhkiG9w0BAQUFAA0 NTgViuQNkcQIP+72 UUJQzv+qXhucNH4M =	OZWsxDjAM Q/ADOP/tt OLrqwE3Js 4DTKebutb NAQKOMRow BgQBnuCnA yUVaMoOcG tYInctYtg



? 🛛
Import
Done
<u>R</u> emove from list
Details



7. Sign Certificate with right click and choose the Sign option.





Dray CA test
SHA 1
Apply extensions Apply subject Apply all

8. Export the Local Certificate to Vigor.

internal name 🔶 commor New Dray CA test jos	Name CA Serial Expiry date Revocation Yes 01 2022-03-09 GMT CRL expires: 2012-03-09 GMT	New Certificate
Net vigor vigor	02 2013-03-09 GMT	Export
la la companya da companya		Import
		Show Details
	✓ X Certificate and Key management	Delete
		Import PKCS#12
	Certifikate export	Import PKCS#7
	Please enter the filename for the certificate.	Plain View
	Filename D/李元祺集重次件/2330_scalvigor.ort DER is a binary format of the Certificate PEM is a based encoded Certificate PEM is a based encoded Certificate PEM is a based encoded Certificate PECS#12 is an official Certificate schemage format PECS#12 is an encrypted official Key-Certificate exchange format Export Format PEM with Certificate chain	
		Jerminache Mindemo , Zine



Certificate Backup VolP Wireless LAN USB Application System Maintenance Diagnostics External Devices	桌面 谈问 我的文件	
Support Area Product Registration	我的電腦 一個 網路上的芳鄉 檔案類型(1):	vigor.crt マ 開啓()) 所有檔案 マ 取消 〕以唯讀方式開啓(R)
Off Cer	rtificate Management >> Local Certific	ite
LAN X5	09 Local Certificate Configuration	
Firewall	Name Subje	ct Status Modify
User Management	Local /C=TW/OU=drav	tek/CN=vigor OK View Delete
Objects Setting		
Bandwidth Management	GENERATE MPORT REFRE	SH
Applications	👦 Certificate Information - Google Chr	ome 🔲 🗰 🗶
VPN and Remote Access Certificate Management	() 192.168.1 1/doc/XLoCfVi.htm	
> Local Certificate	Name :	Local
Trusted CA Certificate	- 28 CM - 2	
VoIP Wireless LAN	Issuer :	<script>reorder_subject("/C=TU/CN=</th></tr><tr><th>System Maintenance Diagnostics External Devices</th><th>Subject :</th><th><pre><script>reorder_subject("/C=TW/OU=dra ytek/CN=vigor");</script>
Support Area Product Registration	Subject Alternative Name :	DNS:draytek.com
	Valid From :	Mar 9 09:48:00 2012 GMT
Logout	Valid To :	Mar 9 09:48:00 2013 GMT
All Rights Reserved.		

9. Export the Trusted CA Certificate (Dray_CA_test.crt) to Vigor.





VPN and Remote Access Certificate Management > Local Certificate > Trusted CA Certificate > Certificate Backup VolP Wireless LAN USB Application System Maintenance Diagnostics External Devices	 ・ 教員近的文件 ・ ・ ・	B 300-party CA_est ort	-X HOW 10 CONNECTIFISE WITH A JUST HOM SIMAT WITH CLEARING VI
Support Area	我的電腦		
Product Registration			
Off Cert WAN LAN X500 NAT	ificate Manager 9 Trusted CA Ce Name	ment >> Trusted CA Ce entificate Configuration Subie	rtificate ct Status Modify
Firewall User Management		(C-TIAL (Chi-iss (amo	
Objects Setting	usied CA-1	/c=1w/cN=jos/ema	IIIAuuress=ju UK View Delete
CSM Bandwidth Management	🐬 Certificate In	formation - Google Chro	
Applications	C 192 168 1 1/4-	c/XCaCfVil.htm	
VPN and Remote Access	G INTIONITIA	The second is a second se	
Local Certificate		Cert	ificate Detail Information
Certificate Backup	Certific	ate Name:	Trusted CA-1
VolP			
Whereast LAN USB Application System Maintenance	Issuer:		/C=TW/CN=jos/email&ddress=jos@draytek .com
External Devices	Subjec	t:	/C=TW/CN=jos/email&ddress=jos@draytek .com
Support Area Product Registration	Subjec	t Alternative Name:	
Logout	Valid F	rom:	Mar 9 09:28:00 2012 GMT
An Rights Reserved.	Valid T	o:	Mar 9 09:28:00 2022 GMT

Part C : Making a Private Certificate and Private key for the PC

- 1. Click New Certificate button on XCA.
- 2. Sign with the Trusted Certificate, and go to the $\ensuremath{\textbf{Subject}}$ tab.

X Certificate and Key management	?
Create x509 Certificate	
Source Subject Extensions Key usage Netscape	Advanced
	N
-Signing request	42
Sign this Certificate signing request	vigor
Copy extensions from the request	Show request
Modify subject of the request	
 Use this Certificate for signing 	Dray CA test
Signature algorithm	SHA 1
- Template for the new certificate	
[default] C:\Program Files\xxa\CA	×
	Apply extensions Apply subject Apply all

Apply extensions Apply subject Apply all

- 3. In Subject page, type a distinguishable or preferred name.
- 4. Click Generate a new key and create a RSA 1024 bit key for this Certificate.
- 5. Click **OK**, and we have generated the Trusted CA Certificate well.

Create x509 C	ertificate		A	New Certificate
Source Subject Distinguished name	Extensions Key usage	Netscape Advanced		Export
Internal name	jos TW	prganizationName		<u>S</u> how Details
stateOrProvinceName		commonName jo	\$	Delete
localityName Tv	pe	emailAddress	Add	Import PKCS#7
of X Certificate and	Key management	? 🛛	Delete	Flam View
S X Certificate and New key Please give a name to t Key properties	Key management ne new key and select the dec	eed keyrize	Delete	Pian Yew
S X Certificate and New Key Please give a name to t Key properties Name jos Keytope ISSA Keytine IO24 bit	Key management he new key and select the dec	ied keysize	Delete	Pan Yew

6. Export the Private Certificate (jos.crt) to PC.

Internal name commonName CA Serial Expiry date Revocation Image: Drayth CA set jos 01 2023-12-24 GMT CRI expire: 2012-12-24 GMT ip is jos 03 2013-12-24 GMT Export Export Vigor vigor 02 2013-12-24 GMT Export Export Import Import Import Show Details Delete Certificate and Key management Import ECS#12 Import ECS#12 Import ECS#12 Please onler the filename for the certificate. Import ECS#12 Import ECS#12 Import ECS#12 DER is a binacy format of the Certificate Export Import ECS#12 Import ECS#12 Export Format Export format Export Plain Yaw OK Cancel OK Cancel	ate Keys Certificate	signing requests	Certificates	Templates	Revocation lists		
Daydek CA bert jos Yes 01 2022-12.24 GMT Cettificate jos jos 03 2013-12.24 GMT Export Vigor vigor 02 2013-12.24 GMT Import X Certificate and Key management Import Stow Details Certifikate export Import ECS#12 Import ECS#12 Please enter the filename for the certificate. Import ECS#12 Import ECS#12 Please enter the filename for the certificate Import ECS#7 Plain View DER is a binacy format of the Certificate explange format PKCS#12 is an encrypted official Key-Certificate explange format Plain View OK Cancel OK Cancel	Internal name	commonl	Name CA	Serial	Expiry date	Revocation	
jos 03 2013-12:24 GMT Wigor vigor OZ 2013-12:24 GMT Import Certificate and Key management Certificate export Please enter the filename for the certificate Please enter the filename for the certificate Please enter the filename for the certificate DER is a base64 encoded Certificate PKCS\$77 is an official Certificate exchange format PKCS\$72 is an encrypted official Key-Certificate exchange format PKCS\$72 is an encrypted official Key-Certificate exchange format PKCS\$72 is an encrypted official Key-Certificate exchange format PKCS\$71 is an official Certificate exchange format PKCS\$72 is an encrypted official Key-Certificate exchange format OK Cancel	Neg Draytek CA te	est jos	×	les	01 2022-12-24 GMT	CRL expires: 2012-12-24 GMT	<u>N</u> ew Certificate
Vigor Vigor U2 2013-12-24 GM1 Import Import Import Stow Details Certificate and Key management Import Certificate and Key management Import Please enter the filename for the certificate Import PKCS#12 Please enter the filename for the certificate Import PKCS#12 DER is a based encoded Certificate Import PKCS#12 DER is a based encoded Certificate Please PKCS#12 is an encorpted official Key-Certificate exchange format PKCS#12 is an encorpted official Key-Certificate exchange format Import PKCS#12 Export Format EM with Certificate chain OK Cancel	A jos	jos			03 2013-12-24 GMT		Export
X Certificate and Key management	Vigor	Vigor			02 2013-12-24 GMT		Import
Certifikate export		J X Cartificate	and Var mor				Show Details
Certifikate export import PKCS#12 Please enter the filename for the certificate. Import PKCS#12 Filename D./李元祝承面/os crt DER is a binary format of the Certificate Plain View Plain View Plain View Plain View OK Cancel OK		A Common	s and Roy ha	идошонт			Delete
Please enter the filename for the certificate. Import P <u>K</u> CS#7 Filename D./李元桃/孫面fos.crt DER is a bancy format of the Certificate Plain View PEM is a banced encoded Certificate Plain View PEM is a banced encoded Certificate exchange format PKCS#7 is an official Certificate exchange format PKCS#1 is an official Certificate exchange format Import Piccs#7 Export Format PEM with Certificate chain OK Cancel		Certifikate	e export				Import PKCS#12
Filename D/学元税/共而/jos.cst … DER is a binary format of the Certificate Plain View PEM is a base64 encoded Certificate Plain View RCS#7 is an official Certificate exchange format PKCS#12 is on encorpted official Key-Certificate exchange format Export Format PEM with Certificate cheain OK Cancel		Please enter the	filename for the	certificate.			Import PKCS#7
DER is a binary format of the Certificate PEM is a base64 encoded Certificate PKCS#12 is an encrypted official Key-Certificate exchange format PKCS#12 is an encrypted official Key-Certificate exchange format Export Format PEM with Certificate chain OK Cancel		Filename D:/	年元棋/桌面/jos.	ert			Plain View
OK Cancel		PEM is a base6 PKCS#7 is an o PKCS#12 is an Export Format	4 encoded Certif fficial Certificat encrypted offici PEM with Cert	icate e exchange fo: al Key-Certifu ficate chain	rmat cate exchange format		
						OK Cancel	



7. Export the Private Key (jos.key) to PC.



Part D : Setup for OpenVPN Dial-In User on the Router

1. Please go to VPN and Remote Access >> OpenVPN General Setup, and follow the OpenVPN setting as the screenshot below.

Vigor3200 Se Multi-WAN Security	eries Router	Dray Tek
Off IR6	VPN and Remote Access >> Op OpenVPN General Setup Port	1194
WAN LAN NAT Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access VPN and Remote Access VPN Client Wizard PP General Setup PP General Setup P PSec Peer Identity P OpenVPN General Setup P Remote Dial-in User > LAN to LAN VPN HRUNK Management Certificate Management	Cipher Algorithm HMAC Algorithm Certificate Authentication Note: OpenVPN on vigor only corresponding configure	AES128 V SHAT V support UDP protocol and TUN device interface currently. So please setup stions on the client side.

2. Go to VPN and Remote Access >> Remote Dial-in User to set up the profiles for Dial-in users. About the user name and password, we define jos/jos for OpenVPN.

Off 💌 IRO	VPN and Remote Access >> Remote Dial-in User				
uick Start Wizard	Index No. 1				
ervice Activation Wizard	User account and Authentication	Username	jos		
AN AN	Idle Timeout 300 second(s)	Password(Max 19 char)			
AT		🔲 Enable Mobile One-T	ime Passwords(mOTP)		
irewall	Allowed Dial-In Type	PIN Code			
ser Management bjects Setting		Secret			
SM	IDcoc Tuppel	Martine and A			

Status	User account and Authentication	Username	jos
	Idle Timeout 300 second(s)	Password(Max 19 char)	me Passwords(mOTP)
ll anagement	Allowed Dial-In Type	PIN Code	
s Setting		Secret	
idth Management ations	L2TP with IPsec Policy None	IKE Authentication Method	1
Client Wizard		IKE Pre-Shared Key	
note Access Control 9 General Setup	Specify Remote Node	Digital Signature(X.5	J9)
ec General Setup ec Peer Identity	Remote Client IP	None 🗸	
to LAN	or Peer ID	IPsec Security Method Medium(AH)	
TRUNK Management	Netbios Naming Packet 💿 Pass 🔘 Block	High(ESP) 🗹 DES 🗹	3DES 🗹 AES
ate Management	Multicast via VPN O Pass O Block (for some IGMP,IP-Camera,DHCP Relayetc.)	Local ID (optional)	
plication Maintenance	Subnat	-	

3. Go to SSL VPN >> General Setup to set up the Server Certificate Handshake Key for Dial-in users, and here for the Server Certificate we choose "Local", which represents the Local Certificate for OpenVPN user we have generated in Part B.

Vigor3200 s Multi-WAN Security	eries Router	Dray Tek
Off ⊻ I₽6	SSL VPN >> General Setup	
Quick Start Wizard Service Activation Wizard	SSL VPN General Setup	
	Port 443 (Default: 443)	
WAN LAN NAT	Server Certificate	
Firewall	Enclyption Key Algorithm	
User Management	High - AES(128 bits) and 3DES	
CSM	Default - RC4(128 bits)	
Bandwidth Management	O Low - DES	
Applications Certificate Management SSL VPN > General Setup > SSL Web Proxy > SSL Meb Proxy > SSL Application > User Account > User Coup	Note: The settings will act on all SSL applications.	91

Part E : Setup for SmartVPN Client

11 of

Now there are three files to import into the SmartVPN client—Trusted CA Certificate (Draytek_CA_test.crt), Private Certificate (jos.crt), and Private Key (jos.key).

Vigor 3200 Series	Profile Name :	Profile 6		Dra	y Tek
Dray Tek Smart VPN Client	Auto re-dial after die Redial attempts : Redial interval :	sconnect.	€ Diseconds		
	Auto run when syste	em start up.	OpenVPN Setting		×
Step 0 Enable/Allow IDSer NAT-Travercal and L2TD	VPN Server IP/HOST Na	ame(such as 123.45.67.8	Port:	1194	
This step will add the Prohibit IpSec registry value and the	200.200.200.2	:00	Cipher methods:	AES-128-CBC	~
AssumeUDPEncapsulationContextOnSendRule registry value to computer. For more infomation, please read the article Q240262 and Q210013 in the Misseart Kendledment Res.	User Name : jo:	s	Authentication:	SHA1	~
and Qoroovs in the Microsoft Knowledgement base.	Password : **	car.	Certificate Authentical	tion	
Configure	Enable mobile One	Time Password (mOTP)	CA cert:	Draytek_CA_test.crt	Browse
Step 1. Dial to ISP	·	nfigure Secret for mOTP	Client cert:	jos.crt	Browse
If you have already gotten a public IP, you can skip this step.	Type of VPN		Client key:	jos.key	Browse
Dial	OPPTP	OL2TP	Fallback to SSL Tunnel		
Step 2. Connect to VPN Server	SSL VPN Tunnel	C21P over OpenVPN	Port:	443	
Profile 6 Connect	PPTP Encryption No encryption		0	Cancel	
Insert Remove Setup	Maximum streng	ith encryption			
Auto-Run when start up:	Authentication met	hod PAP	~		
tatus: No connection OpenVPN ISP @ VPN (Use default gates	way on remote network	More		
Lertificate Management SL VPN	ОК	Cance			

17/11/13 23:33

After establishing the OpenVPN tunnels, the PC will be able to access the Vigor 3200's LAN successfully.

Auto-Run when start up:			Authentication method	PAP	~	
Status: No connection	OpenVPN	ISP @ VPN @	Use default gateway on remote network More			
Certificate Manageme SSL VPN USB Application	nt		ОК	Cance		

After establishing the OpenVPN tunnels, the PC will be able to access the Vigor 3200's LAN successfully.

Off 💌 📧	VPN and Remote Access >> Connection Management
Quick Start Wizard Service Activation Wizard Online Status	Dial-out Tool Refresh Seconds : 10 V Refresh
WAN LAN NAT Firewall User Management	General Mode: Dial Backup Mode: Dial Load Balance Mode: Dial
Objects Setting CSM Eandwidth Management Applications VPN and Remote Access	VPN Connection Status Current Page: 1 Page No. Go >> VPN Type Remote IP Virtual Network Tx Tx Rx Rx VPN Type Remote IP Virtual Network Pkts Rate(Bps) UpTime
VPN Client Wizard VPN Server Wizard Remote Access Control PPP General Setup IPsec General Setup	1 (jos) OpenVPN Local User Database AES-SHA1 Auth 188.188.188 192.168.1.11/32 14 52 20 52 0:0:31 Drop
P Desc Peer Identity PoperVPM Ceneral Setup Permote Dial-in User Permote Dial-in User Pomote Name VPN TRUNK Management Connection Management SSL VPN USB Application System Maintenance	Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time<1ns TTL=255 Reply from 192.168.1.1: bytes=32 time<1ns TTL=255
Admin mode	Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Read 25 times

Last modified on Wednesday, 02 January 2013 12:21