

DrayTek

SSL VPN

***Connectie problemen bij iOS13 &
MacOS 10.15***



SSL VPN connectie problemen bij gebruik van iOS13 & MacOS 10.15

Apple heeft in iOS13 en MacOS 10.15 het beveiligingsniveau verhoogd. Deze aanpassing heeft invloed op de SmartVPN app. Hierdoor is het voor DrayTek gebruikers niet meer mogelijk een SSL VPN tunnel op te zetten via hun Apple device.

Om te voldoen aan het nieuwe security beleid van Apple heeft DrayTek twee oplossingen beschikbaar:

1. Maak gebruik van Let's Encrypt i.c.m. DrayDDNS.
2. Gebruik een bepaalde firmware en genereer een nieuw self-signed certificaat in de DrayTek modem/router.

Beide oplossingen zullen in dit document worden besproken.

Maak gebruik van Let's Encrypt icm DrayDDNS

Om gebruik te kunnen maken van Let's Encrypt dient u de DrayTek router te registreren bij de DrayDDNS dienst van DrayTek. Met deze DrayDDNS dienst kunt u een eigen domein naam registreren, deze dienst is gratis te gebruiken. Voor het aanmaken van een DrayDDNS account kunt u de handleiding op onze www.draytek.nl website volgen.

Let's Encrypt certificaat aanvragen

Belangrijk: De DrayTek router moet op basis van HTTP poort 80 bereikbaar zijn vanaf het internet. U dient Remote Management in te schakelen bij System Maintenance >> Management. Het aanvragen van het Let's Encrypt certificaat verloopt namelijk via HTTP poort 80.

System Maintenance >> Management

IPv4 Management Setup IPv6 Management Setup LAN Access Setup

Router Name: DrayTek

Default: Disable Auto-Logout
 Enable Validation Code in Internet/LAN Access

Internet Access Control
 Allow management from the Internet
Domain name allowed:

FTP Server
 HTTP Server Enforce HTTPS Access
 HTTPS Server
 Telnet Server
 TR069 Server
 SSH Server
 SNMP Server
 Disable PING from the Internet

Management Port Setup
 User Define Ports Default Ports

Telnet Port: 23 (Default: 23)
HTTP Port: 80 (Default: 80)
HTTPS Port: 443 (Default: 443)
FTP Port: 21 (Default: 21)
TR069 Port: 8069 (Default: 8069)
SSH Port: 22 (Default: 22)

Note:
Ports 8001 and 8043 are used for Hotspot Web Portal.

Brute Force Protection
 Enable brute force login protection
 FTP Server

Ga in de DrayTek router naar Applications >> Dynamic DNS Setup, open hier het DrayDDNS profiel welke u hebt aangemaakt. Klik bij Let's Encrypt certificate op 'Create'.

Index : 1

Enable Dynamic DNS Account

Service Provider: DrayDDNS (Global)

Status: **Activated** [Start Date:2018-06-25 Expire Date:2019-06-25]

Domain Name: louis2862.drayddns.com Edit domain

Determine WAN IP: WAN IP IPv4 IPv6

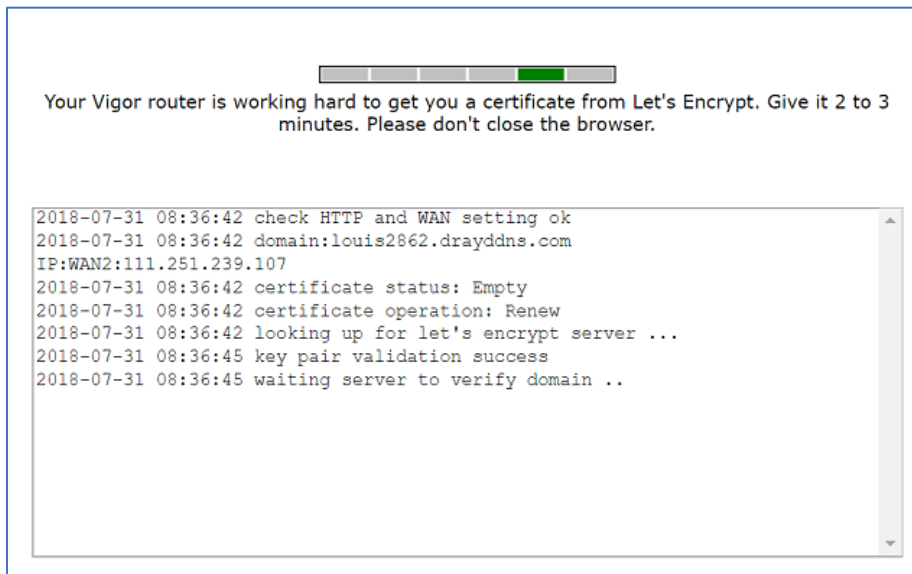
WAN Interfaces: WAN 1 WAN 2 WAN 3 WAN 4

Let's Encrypt certificate
Status: Empty **Create**

Auto Update:

OK Clear Cancel

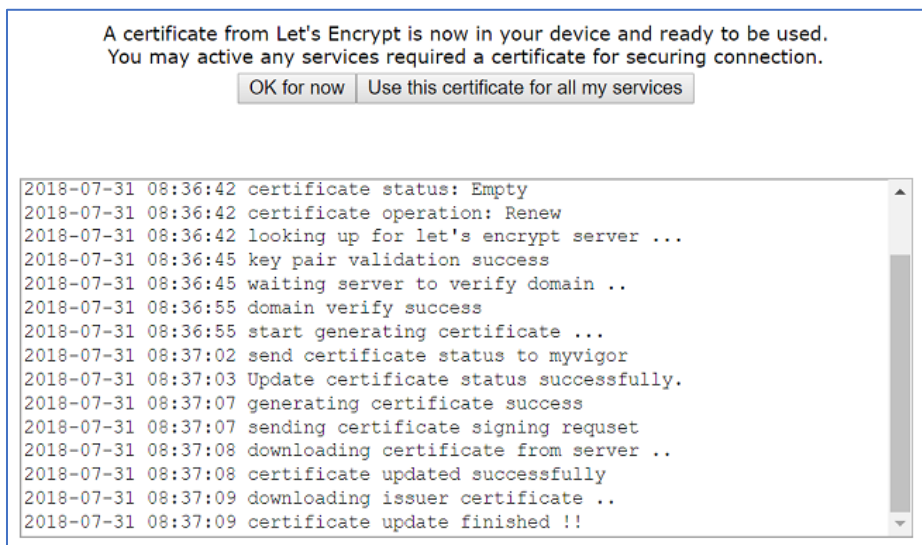
De DrayTek router zal een certificaat aanvragen bij de Let's Encrypt servers, deze procedure kan enkele minuten duren.



Your Vigor router is working hard to get you a certificate from Let's Encrypt. Give it 2 to 3 minutes. Please don't close the browser.

```
2018-07-31 08:36:42 check HTTP and WAN setting ok
2018-07-31 08:36:42 domain:louis2862.drayddns.com
IP:WAN2:111.251.239.107
2018-07-31 08:36:42 certificate status: Empty
2018-07-31 08:36:42 certificate operation: Renew
2018-07-31 08:36:42 looking up for let's encrypt server ...
2018-07-31 08:36:45 key pair validation success
2018-07-31 08:36:45 waiting server to verify domain ..
```

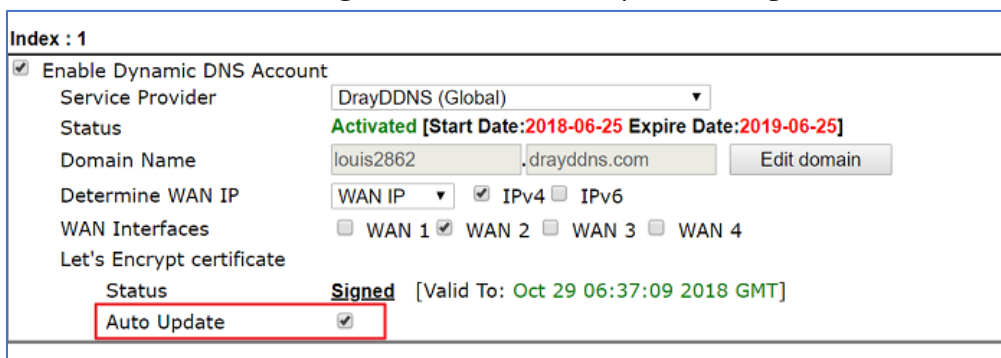
Wanneer dit proces is voltooid krijgt u de vraag of u dit certificaat direct wil gebruiken. Klik op 'Use this certificate for all my services'.



A certificate from Let's Encrypt is now in your device and ready to be used. You may active any services required a certificate for securing connection.

```
2018-07-31 08:36:42 certificate status: Empty
2018-07-31 08:36:42 certificate operation: Renew
2018-07-31 08:36:42 looking up for let's encrypt server ...
2018-07-31 08:36:45 key pair validation success
2018-07-31 08:36:45 waiting server to verify domain ..
2018-07-31 08:36:55 domain verify success
2018-07-31 08:36:55 start generating certificate ...
2018-07-31 08:37:02 send certificate status to myvigor
2018-07-31 08:37:03 Update certificate status successfully.
2018-07-31 08:37:07 generating certificate success
2018-07-31 08:37:07 sending certificate signing request
2018-07-31 08:37:08 downloading certificate from server ..
2018-07-31 08:37:08 certificate updated successfully
2018-07-31 08:37:09 downloading issuer certificate ..
2018-07-31 08:37:09 certificate update finished !!
```

Uw Let's Encrypt certificaat is 3 maanden geldig, na deze 3 maanden zal de DrayTek router deze automatisch verlengen wanneer 'Auto Update' is ingeschakeld.



Index : 1

Enable Dynamic DNS Account

Service Provider

Status **Activated** [Start Date:2018-06-25 Expire Date:2019-06-25]

Domain Name

Determine WAN IP IPv4 IPv6

WAN Interfaces WAN 1 WAN 2 WAN 3 WAN 4

Let's Encrypt certificate

Status **Signed** [Valid To: Oct 29 06:37:09 2018 GMT]

Auto Update

Selecteer bij SSL VPN >> General Setup het DrayDDNS/Let's Encrypt certificaat. Vervolgens kunt u weer gebruik maken van SSL VPN op uw iOS13 device.

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN3
Port	<input type="text" value="443"/>	(Default: 443)
Server Certificate	<input type="text" value="DrayDDNS"/> ▼	

Note:

1. The settings will act on all SSL applications.
2. Please go to [System Maintenance >> Management](#) to enable SSLv3.0 .
3. Please go to [System Maintenance >> Self-Signed Certificate](#) to generate a new "self-signed" certificate.

Genereer een nieuw self-signed certificaat

Wanneer u minimaal onderstaande firmware gebruikt kunt u een nieuw self-signed certificaat genereren om zodoende weer succesvol een SSL VPN op te zetten.

Vigor2133	: 3.9.2
Vigor2620	: 3.8.14
Vigor2765	: 4.0.5
VigorLTE200	: 3.8.14
Vigor2860	: 3.8.9.6
Vigor2862	: 3.9.1.3
Vigor2925	: 3.8.9.6
Vigor2926	: 3.9.1.3
Vigor2952	: 3.9.1.2
Vigor2960	: 1.5.0
Vigor3900	: 1.5.0

Voor de Vigor2860 & Vigor2925 serie: Ga naar System Maintenance >> Self-Signed Certificate. Overige modellen: Ga naar Certificate Management >> Self-Signed Certificate.

System Maintenance >> Self-Signed Certificate

Self-Signed Certificate Information

Certificate Name :	self-signed
Issuer :	C=TW, ST=Taiwan, L=Hsinchu city, O=Draytek, OU=F AE, CN=F AE, emailAddress=victor_wang@draytek.com
Subject :	C=TW, ST=Taiwan, L=Hsinchu city, O=Draytek, OU=F AE, CN=F AE, emailAddress=victor_wang@draytek.com
Subject Alternative Name :	
Valid From :	Sep 24 06:36:49 2019 GMT
Valid To :	Sep 23 06:36:49 2049 GMT
PEM Format Content :	<pre>-----BEGIN CERTIFICATE----- MIIDSjCCApqAwIBAgIJAPdfQco41nW3MA0GCSqGSIb3DQEBCwUAMIGLMQswCQ YD VQQGEwJUVzEPMA0GA1UECAwGVGFpd2FuMRUwEwYDVQQHDAxIc2luY2h1IGNpdH kx EDA0BgNVBAoMB0RyYXl0ZWsxDDAKBgNVBAsMA0ZBRETEHMAoGA1UEAwDRKFFMS Yw JAYJKoZIhvcNAQkBFhd2aWNoMjNDND1aMIGLMQswCQYDVQQGEwJUVzEPMA0GA1UECA wG VGFpd2FuMRUwEwYDVQQHDAxIc2luY2h1IGNpdHkxEDA0BgNVBAoMB0RyYXl0ZW sX DDAKBgNVBAsMA0ZBRETEHMAoGA1UEAwDRKFFMSYwJAYJKoZIhvcNAQkBFhd2aW No b3Jfd2FuZ0BkcmlF5dGVRmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQ oC ggEBAMsXe7zEEu7zxJJMzWzrEQ2RXZGIKq249k0FZUmI0X4JasIg9uWCSXV7 g2 MplJejSs1hrWNNPR0rKdp7A3pL70DexA602VBQKzfwT7Xln31f0Ya+2+gv3NeL sU HyEG0t51E64AluamIfUuk6QYkeDkorfEk329A0Tx1cbrSuRQAtXS8QSz9PHbGn -----</pre>

Note:

1. Please setup the **System Maintenance >> Time and Date** correctly before you try to regenerate a self-signed certificate!!
2. The Time Zone MUST be setup correctly!!

Klik op Regenerate.

Vul op basis van Domain Name of IP de gegevens in en klik op Generate. U kunt zelf bepalen welke gegevens u invult.

System Maintenance >> Regenerate Self-Signed Certificate

Regenerate Self-Signed Certificate

Certificate Name	self-signed
Subject Alternative Name	
Type	Domain Name ▾
Domain Name	victor1234.drayddns.com
Subject Name	
Country (C)	TW
State (ST)	Taiwan
Location (L)	Hsinchu city
Organization (O)	DrayTek Corp.
Organization Unit (OU)	DrayTek Support
Common Name (CN)	Victor
Email (E)	victor_wang@draytek.com
Key Type	RSA ▾
Key Size	2048 Bit ▾

Selecteer vervolgens bij SSL VPN >> General Setup het nieuwe self-signed certificate en klik op OK. U kunt nu weer gebruik maken van de SmartVPN App op uw iOS device.

Voorbehoud

We behouden ons het recht voor om deze en andere documentatie te wijzigen zonder de verplichting gebruikers hiervan op de hoogte te stellen. Afbeeldingen en screenshots kunnen afwijken.

Copyright verklaring

© 2020 DrayTek

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder voorafgaande schriftelijke toestemming van de uitgever.

Ondanks alle aan de samenstelling van deze handleiding bestede zorg kan noch de fabrikant, noch de auteur, noch de distributeur aansprakelijkheid aanvaarden voor schade die het gevolg is van enige fout uit deze uitgave.

Trademarks

Alle merken en geregistreerde merken zijn eigendom van hun respectievelijke eigenaren.