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.

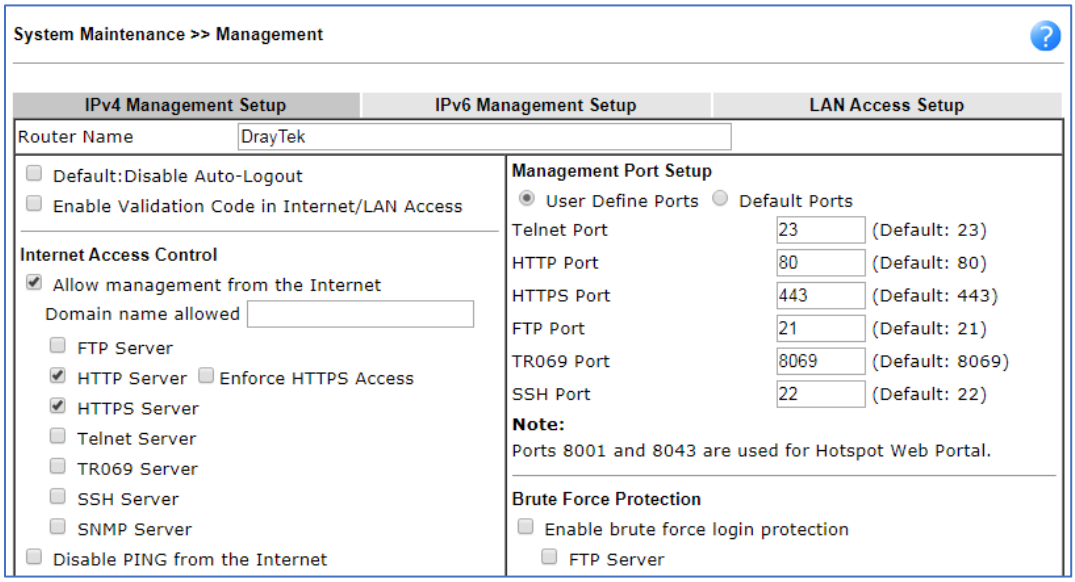
Beide oplossingen zullen in dit document worden besproken.

Maak gebruik van Let's Encrypt icm DrayDDNS

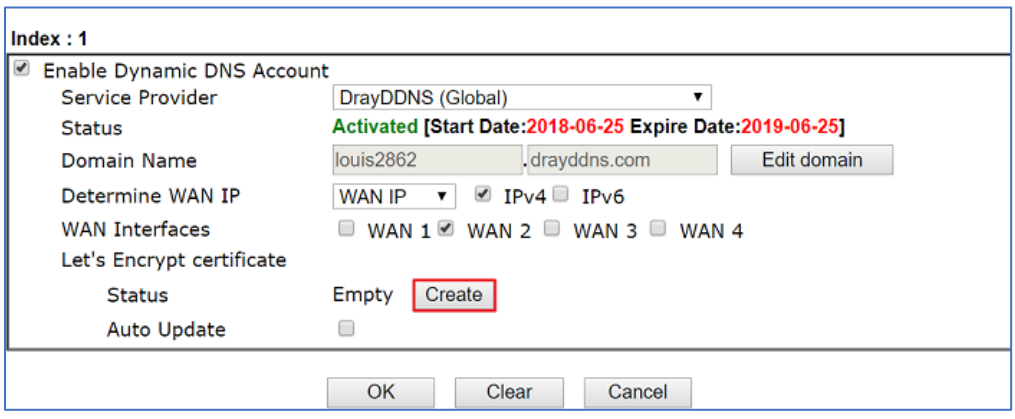
Om gebruik te kunnen maken van Let's Encrypt dient u de DrayTek router te registreren bij de DrayDDNS dienst van DrayTek. Met deze DrayDDNS dienst kunt u een eigen domein naam registreren, deze dienst is gratis te gebruiken. Voor het aanmaken van een DrayDDNS account kunt u de handleiding op onze www.draytek.nl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

Let's Encrypt certificaat aanvragen

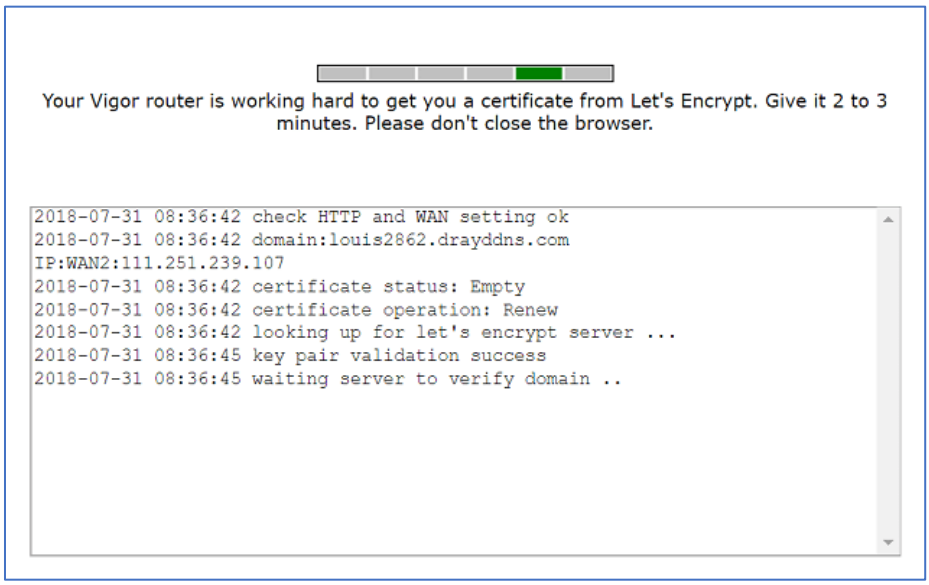
Belangrijk: De DrayTek router moet op basis van HTTP poort 80 bereikbaar zijn vanaf het internet. U dient Remote Management in te schakelen bij System Maintenance >> Management. Het aanvragen van het Let's Encrypt certificaat verloopt namelijk via HTTP poort 80.



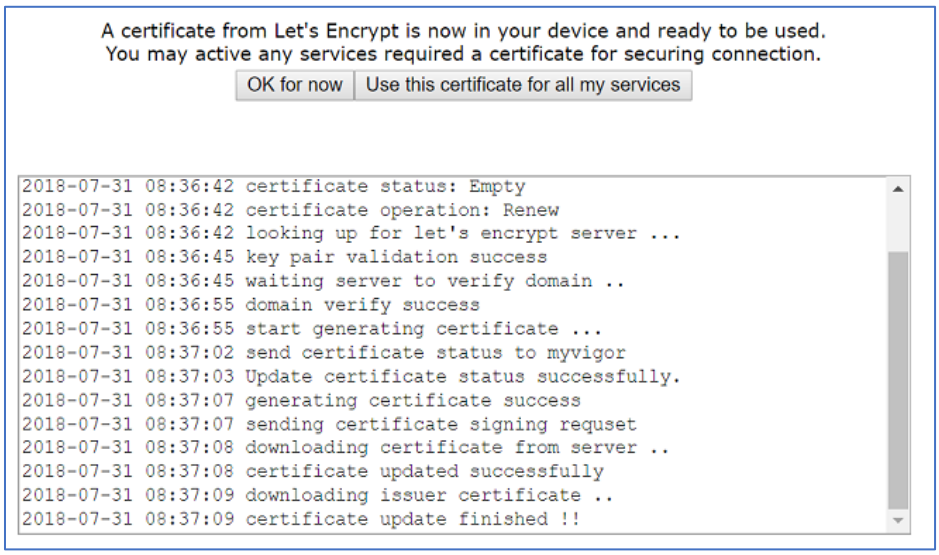
Ga in de DrayTek router naar Applications >> Dynamic DNS Setup, open hier het DrayDDNS profiel welke u hebt aangemaakt. Klik bij Let's Encrypt certificate op 'Create'.



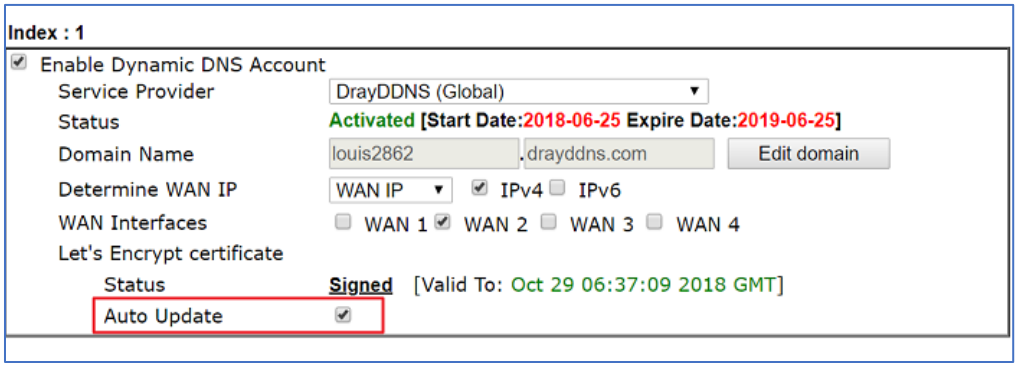
De DrayTek router zal een certificaat aanvragen bij de Let's Encrypt servers, deze procedure kan enkele minuten duren.



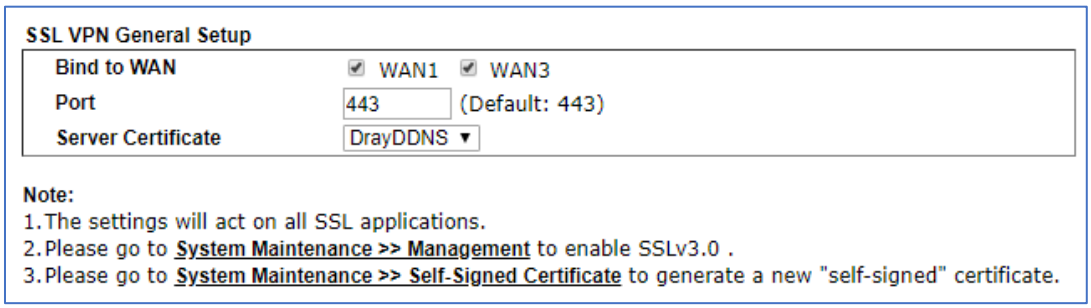
Wanneer dit proces is voltooid krijgt u de vraag of u dit certificaat direct wil gebruiken. Klik op 'Use this certificate for all my services'.



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.



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.

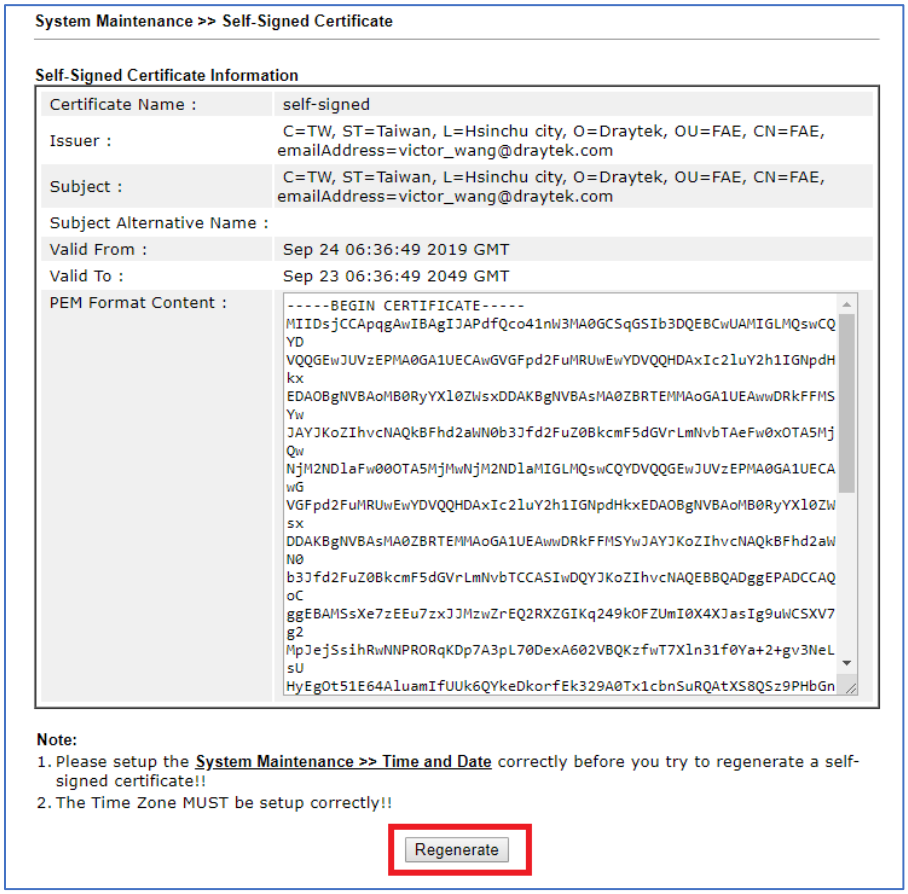


Genereer een nieuw self-signed certificaat

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

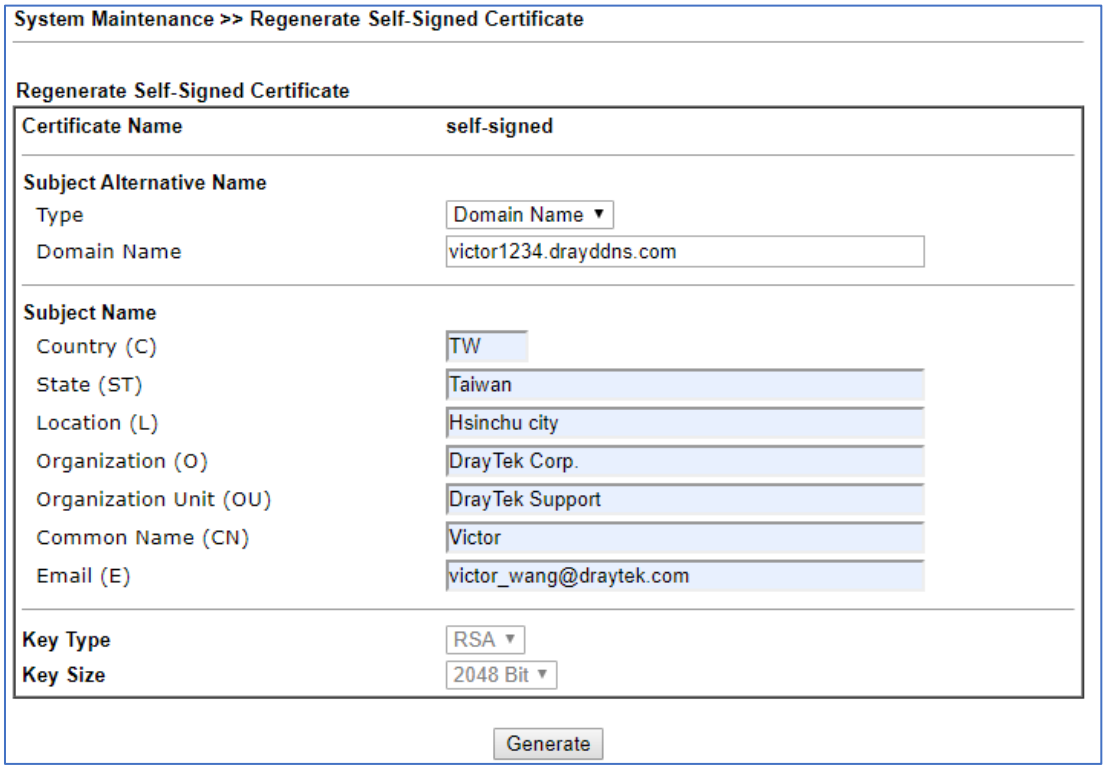
Vigor2133 : 3.9.2
Vigor2620 : 3.8.14
Vigor2765 : 4.0.5
VigorLTE200 : 3.8.14
Vigor2860 : 3.8.9.6
Vigor2862 : 3.9.1.3
Vigor2925 : 3.8.9.6
Vigor2926 : 3.9.1.3
Vigor2952 : 3.9.1.2
Vigor2960 : 1.5.0
Vigor3900 : 1.5.0

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



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.



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.