YourSafetynet: Custom SSL Certificate

Setup steps for custom SSL certificate for YSN Management Server and YSN Filter Gateway

Wil je een eigen (geldig) SSL/TLS certificaat gebruiken in plaats van het self-signed certificaat, dan moet je handmatig de .crt en .key files aanpassen die door de webserver van de management server (nginx) worden gebruikt.

Neem daarvoor de volgende stappen in de command console.
TIP: Je kunt de console ook via PuTTY over SSH bereiken op poort 2224. Dat is wellicht makkelijker met kopiëren/plakken van je certificaat.

Wijzig de CRT file

- Console commando: `sudo nano -w /etc/ysn/ssl/ysn-default.crt`
- Plak hier de public CRT van jullie certificaat in (overschrijven wat er staat). Let op: het format moet hetzelfde zijn, dus beginnend met -----BEGIN CERTIFICATE-----.
- Als het certificaat een Intermediate CA vereist, dan moet je die in dezelfde file erachter aan plakken. Dus na de '-----END CERTIFICATE-----' krijg je dan op de volgende regel weer een '-----BEGIN CERTIFICATE-----' van de Intermediate CA crt.
- Type dan CTRL-X en kies 'y' + ENTER om op te slaan.

Wijzig de KEY file

- Console commando: `sudo nano -w /etc/ysn/ssl/ysn-default.key`
- Plak hier de private KEY van jullie certificaat in (overschrijven wat er staat). Let op: het format moet hetzelfde zijn, dus beginnend met -----BEGIN PRIVATE KEY-----.
- Type dan CTRL-X en kies 'y' + ENTER om op te slaan.

Herstart nu de webserver

- Console commando: `sudo service nginx restart`
- Als alternatief kun je uiteraard ook de gehele appliance herstarten via commando: `sudo reboot`

Daarna zou de webserver jullie certificaat moeten gebruiken in plaats van het self-signed certificaat.

Let op, zoals gebruikelijk bij webservercertificaten: het certificaat kan geen wachtwoordbeveiliging hebben. De webserver kan dan namelijk niet automatisch starten (kent het wachtwoord niet uiteraard).