

Hoe IPSec configureren voor een iPhone in combinatie met xauth?

Benodigdheden:

Een vast IP met een fully qualified domainname (FQDN).

Bijvoorbeeld: applenetasq.dyndns.org.

1.) Maak een gebruiker:

ID: gebruiker

Name: gebruiker

mail:gebruiker@netasq.com

2) Maak een nieuwe root CA (via Configuration -> Objects -> Certificates and PKI).

Root ca naam: iphone

3) Maak een user certificate voor gebruiker: gebruiker via Configuration -> Objects -> Certificates and PKI ->add->add a user certificate).

Zorg ervoor dat het email adres overeen komt met de email van deze gebruiker in de ldap database (in het geval van een AD koppeling het opgegeven email adres in de AD). Publiceer het het certificaat in ldap (selecteer het certificaat en klik op LDAP publication).

4) Maak een server certificaat (via Configuration -> Objects -> Certificates and PKI ->add->add a server certificate).

FQDN: applenetasq.dyndns.org

ID:fwnetasq

5) Maak de IPSec tunnel

Configuration -> VPN ->IPSec VPN ->Anonymous mobile users ->add -> New policy

selecteer de locale resources en maak een nieuwe peer.

selecteer een naam voor deze peer en certificate en xauth als authentication method.

Het certificaat correspondeert met het server certificate van stap 4, fwnetasq.

Wijzig het encryptie profiel van deze peer in IphoneEncryption.
Select een range voor het "local network" en activeer config mode.

Er moet een bestand aangepast worden via de console

open met vi of joe ~/ConfigFiles/VPN/peer

zonder wijzigingen:

[nomade_iphone] (naam van het ipsec profiel).

```
Method=psk
dst=Any
src=Any
conf=GoodEncryption
Mode=AUTO
with modifications
```

met wijzigingen:

```
[nomade_iphone]
Method=xauth_pki
```

```
dst=Any
src=Any
```

```
conf=GoodEncryption
```

```
cert=iphone:fwnetasq
```

```
mode=MAIN
```

Sla het document op en type: `envpn vpn_slot_number`

Exporteer het gebruikers certificaat als P12 bestand en de CA root als PEM bestand en importeer deze op de iPhone

(verstuur ze bijvoorbeeld als email naar de iPhone gebruiker).

Export gaat via Configuration -> Objects -> Certificates and PKI -> Download

Daarna kan de vpn op de iPhone ingesteld worden via:

settings-->networks->VPN



servernaam is gelijk aan de fqdn van het certificaat en moet dus ook echt bestaan en naar het juiste ip adres verwijzen.



login & password zijn die van de betreffende ldap gebruiker het certificaat = het betreffende gebruikers certificaat.

Ga naar Settings ->General -> Network -> VPN -> Add VPN Configuration

Description: maakt niet uit

Server: de gebruikte fqdn (in mijn geval netasq.uk.to).

Account: de gebruiker zijn naam in de ldap.

Password: als deze op Ask every time staat moet de gebruiker zijn wachtwoord elke keer invoeren wanneer hij verbinding maakt.

Certificate: het gebruikers certificaat.