Syn-3 Internet Server RoadWarrior configuratie met GreenBow Windows 2000/XP VPN client

Dit document beschrijft hoe, Syn-3 geconfigureerd kan worden om RoadWarrior tunnels te ondersteunen.
RoadWarriors zijn anders dan tuiswerkers, roadwarriors werken niet thuis(geen vaste plek dus), roadwarriors kunnen over de hele wereld zijn. Dus veiligheid is hier zeer van belang.
Er zijn verschillende veilige methodes mogelijk, van certificaat tot en met een simpele sleutels of simpele unieke ID's tot en met pincode beveiligde sleutel keepers(usb sticks alleen gemaakt om sleutels te bewaren)
waarbij de sleutel benodigd om in te loggen naar het VPN netwerk op de stick is versleuteld.

Hier volgen de config/sleutel bestanden die afhankelijk zijn van een Roadwarrior tunnel in het '/etc/ipsec.d/roadwarriors/' pad op de Syn-3 Internet Server.

Roadwarrior.conf:

```
conn roadwarrior
        left=%defaultroute
        #define here the local network of the office.
        leftsubnet=192.168.13.0/24
        right=%any
        #In this context, the rightsubnet can only be the private addresses defined in RFC1918 (172.16..,192.168.. etc..)
        rightsubnet=vhost:%no,%priv
        #gateway for the  <rightsubnet>
        rightsourceip=0.0.0.0
        #(Optional) give here an uniqueue ID for the roadwarrior(s) (Email,IP,SleutelID)
        #rightid=rick@datux.nl
        keyingtries=3
        authby=secret
        auto=add
        pfs=yes
~
```

rightid is standaard %any(meerdere connecties)
Voor stefieke connectie aan een user kopieer de roadwarrior.conf naar een andere file bijvoorbeeld roadwarrior_piet.conf en stel de eerste regel van deze file in, bijvoorbeeld 'conn roadwarrior_piet' . Stel een rightid in. Pas de file verder na wens aan.

Roadwarrior.key

In dit geval word er gebruikt gemaakt van een PSK(Pre-shared Key).

```
212.120.115.191: PSK "aabbccddeeaabbccddeeaabbccddeeaabbccddee"
```

Koppel hier het ip adres van de syn-3 server aan de sleutel.
Een licentie systeem is natuurlijk beter.

Xauth authenticatie(Optioneel)

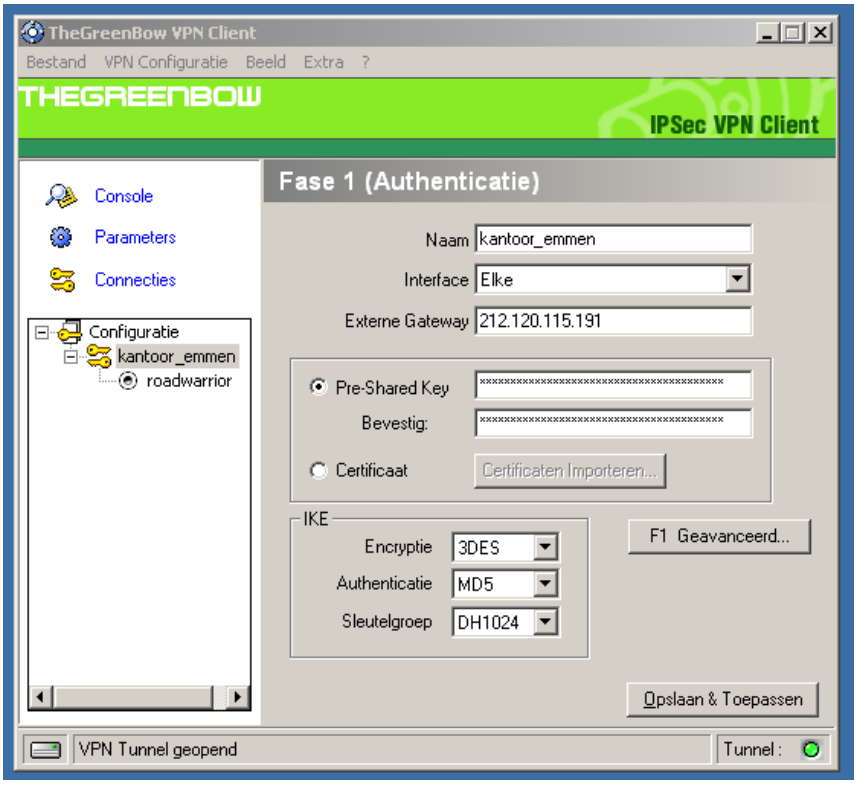
Voeg deze 2 regels toe aan roadwarrior.conf :
leftxauthserver=yes
rightauthclient=yes

Stel de users in op 'htpasswd' stijl in /etc/ipsec.d/passwd
piet:d35fg56s654s0:roadwarrior
piet:d35fg56s654s0:roadwarrior_piet

Commando:
htpasswd /etc/ipsec/passwd piet

Om de SCC users rechstreeks te koppelen aan het Xauth systeem kan PAM gebruikt worden.

Green bow configuratie:
Fase1



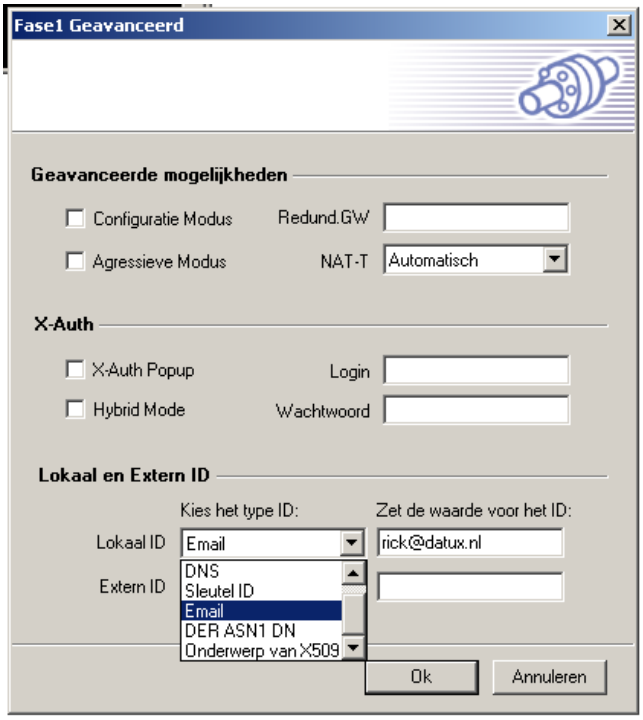
-Geef bij Externe gateway(hier 212.120.115.191) het adres naar de Syn-3 Internet Server op het internet.
-Kies bij interface de netwerk adapter die gekoppeld is aan het internet.
-Afhankelijk van de authenticatie methode, stel de PSK of Certificaat in(In dit geval PSK).
-Stel de IKE(Internet Key Exchange) in (3DES,MD5, DH1024).

-Wanneer in 'Roadwarrior.conf' 'rightid' is geconfigureerd. Stel deze in onder F1(Fase1)

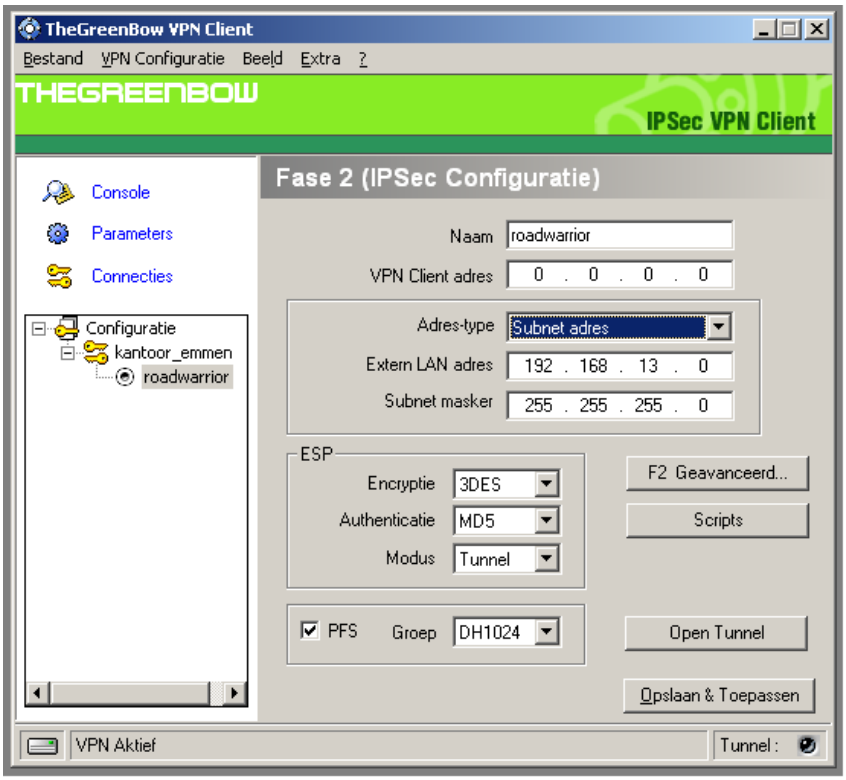
Geavanceerd. (Opmerking: Deze moet in beide zijn vermeld OF in geen van beide).

-Stel onder deze venster NAT-T op automatisch in, bij moeite om verbinding te krijgen stel hem dan geforceerd in.

-Voor Xauth authenticatie stel de Login en Wachtwoord velden voor de desbetreffende gebruiker in. (piet:geheim)



Fase2



-Geef onder Naam(Hier roadwarrior), de naam van de op te bouwen connectie(Zie eerste regel, roadwarrior.conf).

-VPN Client adres kan bij een roadwarrior alles zijn, dus vul hier 0.0.0.0 in.
-Stel nu de netwerk van kantoor in bij (Adres-type,Extern LAN adres en veld Subnet masker), hier is enige netwerk kennis voor vereist, zie ook roadwarrior.conf.

-Geef bij ESP (Encapsulated Security Payload), de Encryptie, Authenticatie en modus, bovenstaande word standaard support door Syn-3.

-Vink veldje PFS af en stel Groep als bovenstaande afbeelding als aangeven is in.

De tunnel is nu geconfigureerd.
-Sla de configuratie op door 'Opslaan & toepassen' knop in te drukken.
-Open nu de tunnel door 'Open Tunnel' aan te klikken. Wanneer het lampje rechsonderin groen gaat branden, is de tunnel geopend.

Problemen oplossen.

Server zijde.
Om de status van geconfigureerde tunnels of bestaande tunnels te weergeven.
Syn-3 shell> ipsec auto –status

Log van IPSEC
Syn-3 shelll> tail -f /var/log/secure

Greenbow zijde:
Onder 'Extra' kan een console geopend worden, die de error meldingen aan de client zijde vertoond.

Auteur: rick@datux.nl
Datum: 10-07-2007
Website: http://www.datux.nl