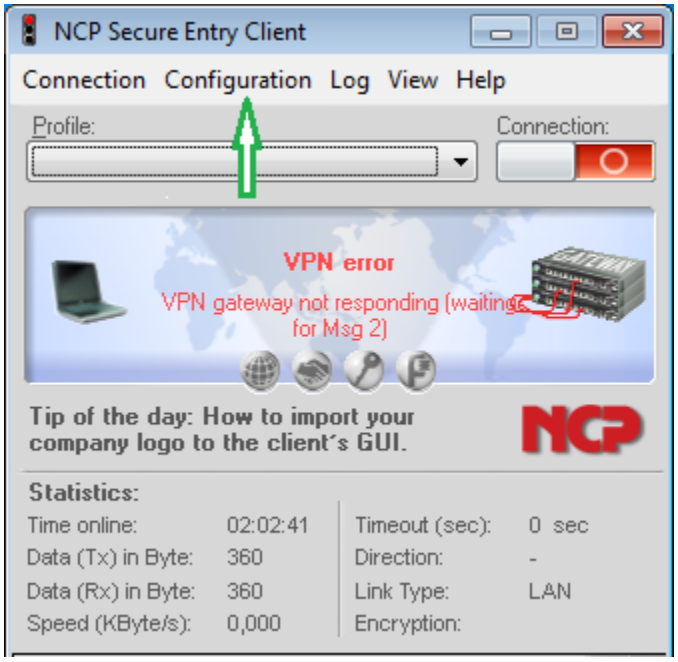
NCP Secure Entry Client Configuration

This a simple configuration of the NCP Client connecting to a Juniper firewall (ISG, SSG, NS device).

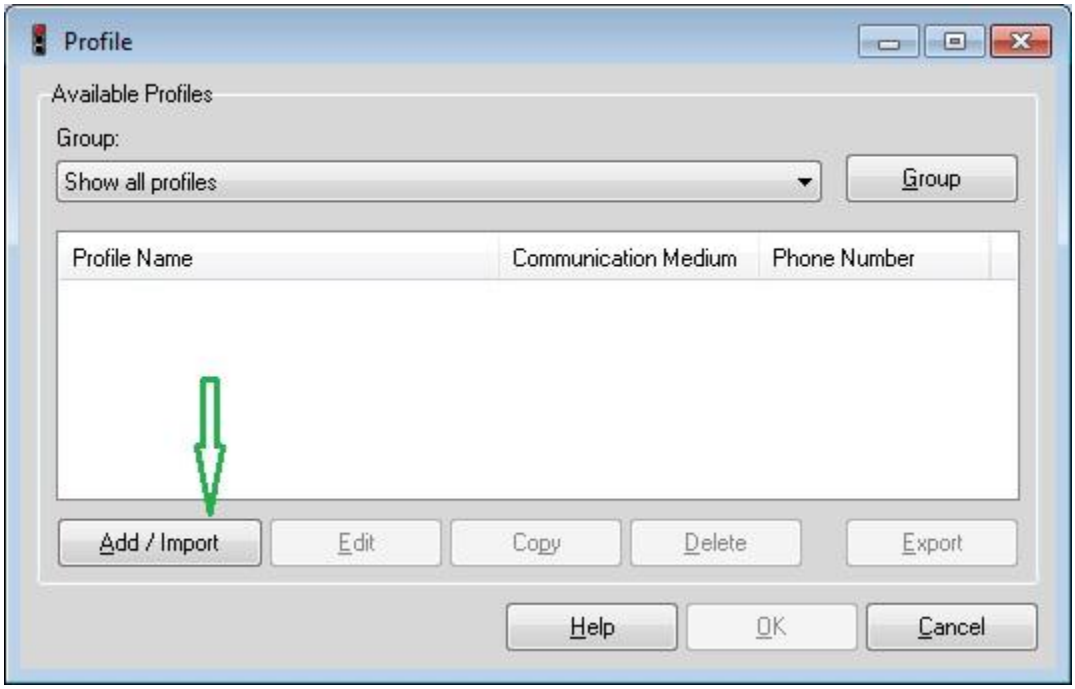
Note that there are other possible configurations.

This is useful for those familiar with configuring NS Remote and are new to the NCP client.

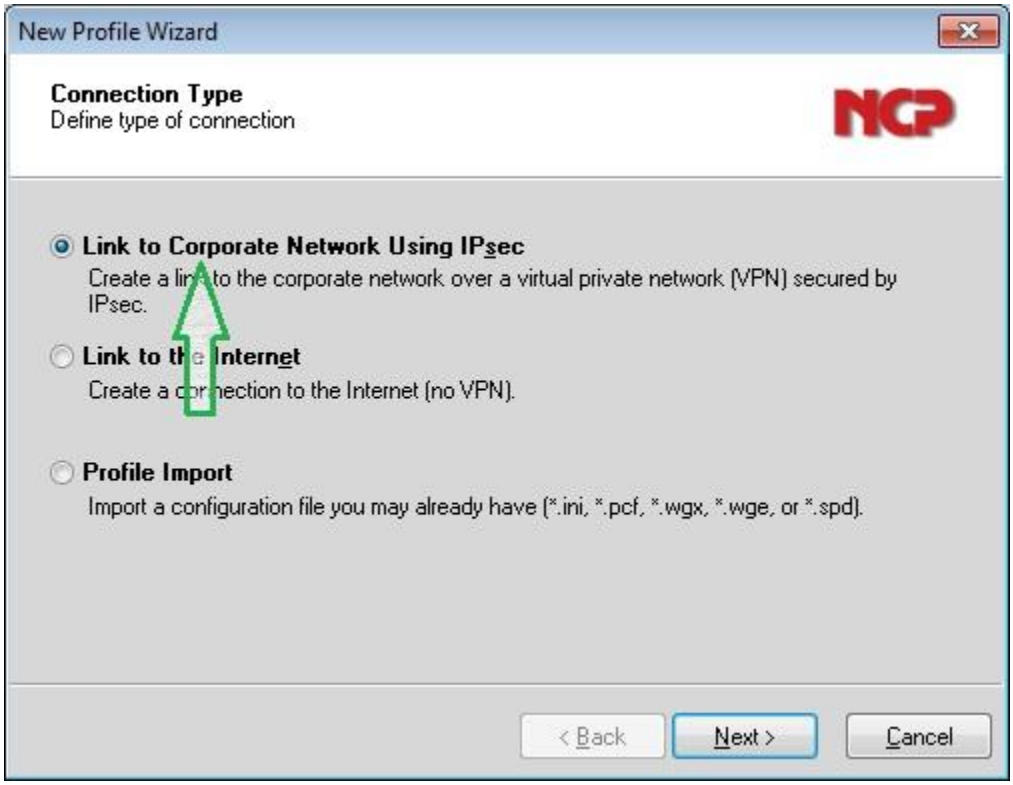
- For a New connection, please click on “Configuration” on the Mail Page of the NCP Client.



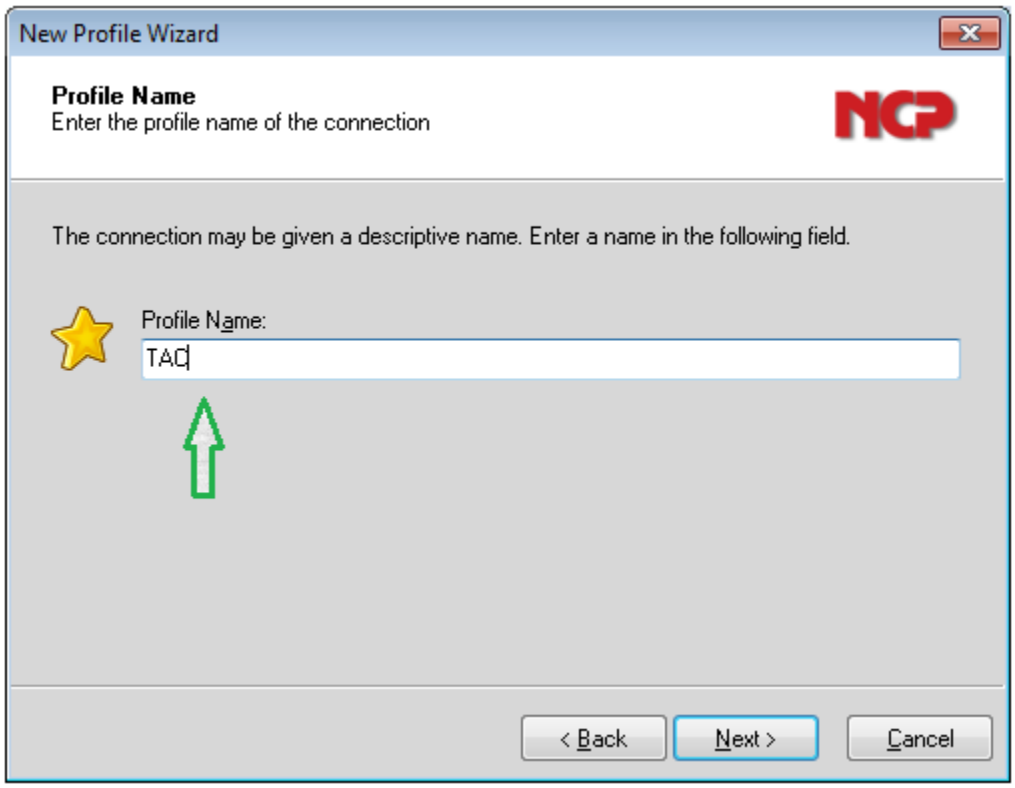
- Click on “Add Profile”



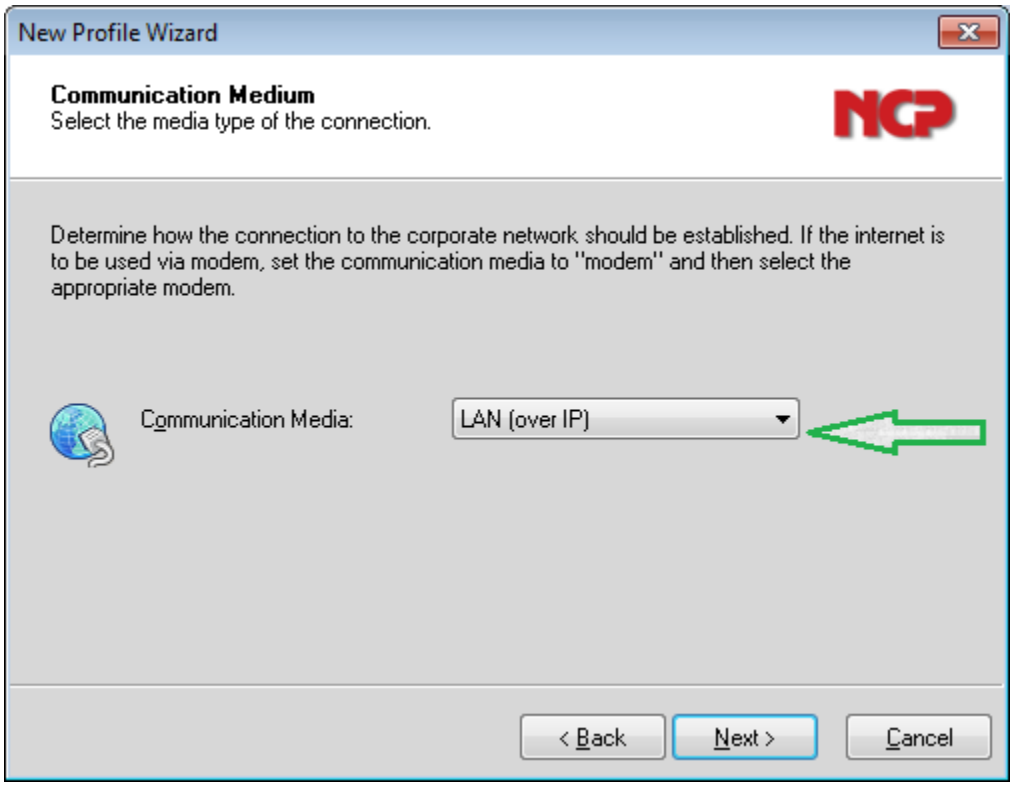
- Click on “Link to Corporate Network Using IPSec”



- Enter Profile Name



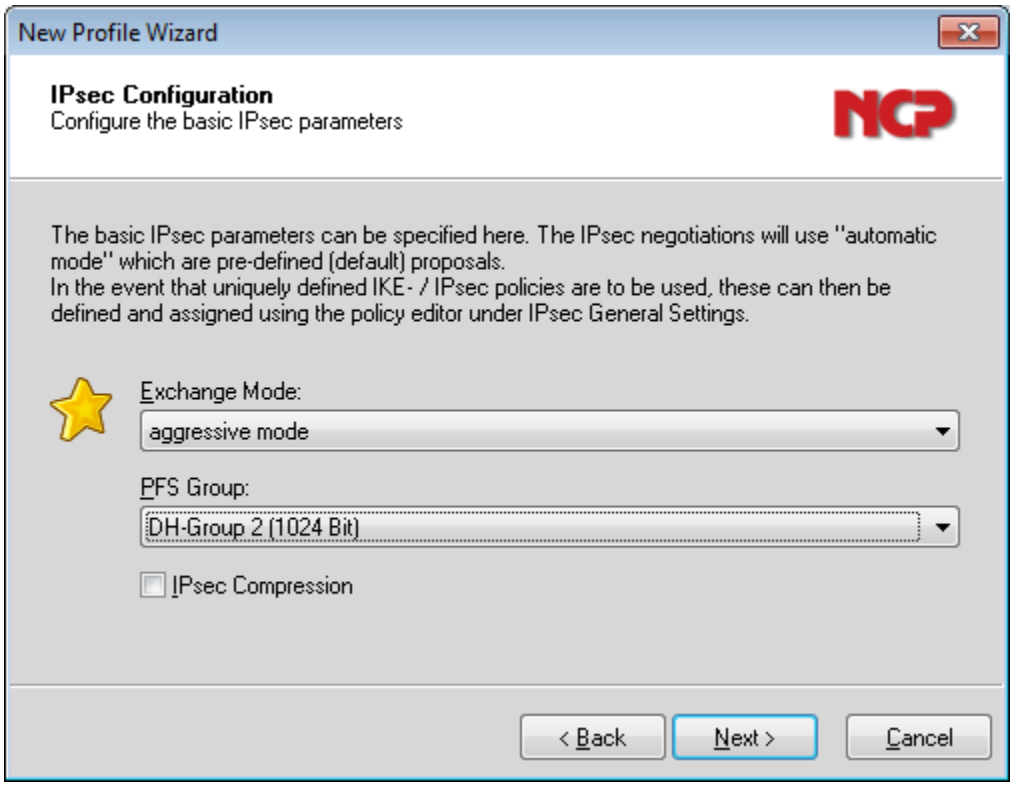
- Choose “LAN (Over IP)” – For most scenarios this is the setting as we have our PCs in the LAN.



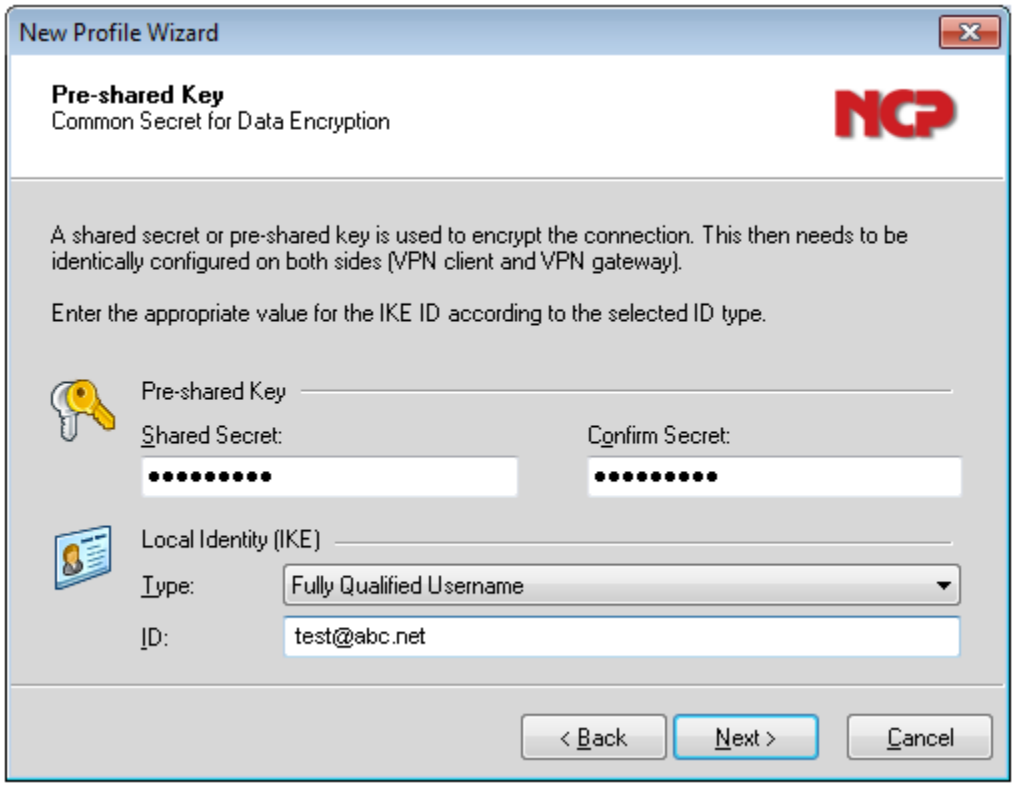
- Give the “Gateway” IP and “XAuth” Username and Password:

Please note that XAuth can be unchecked as well and this would depend on the XAuth Settings on the Firewall.

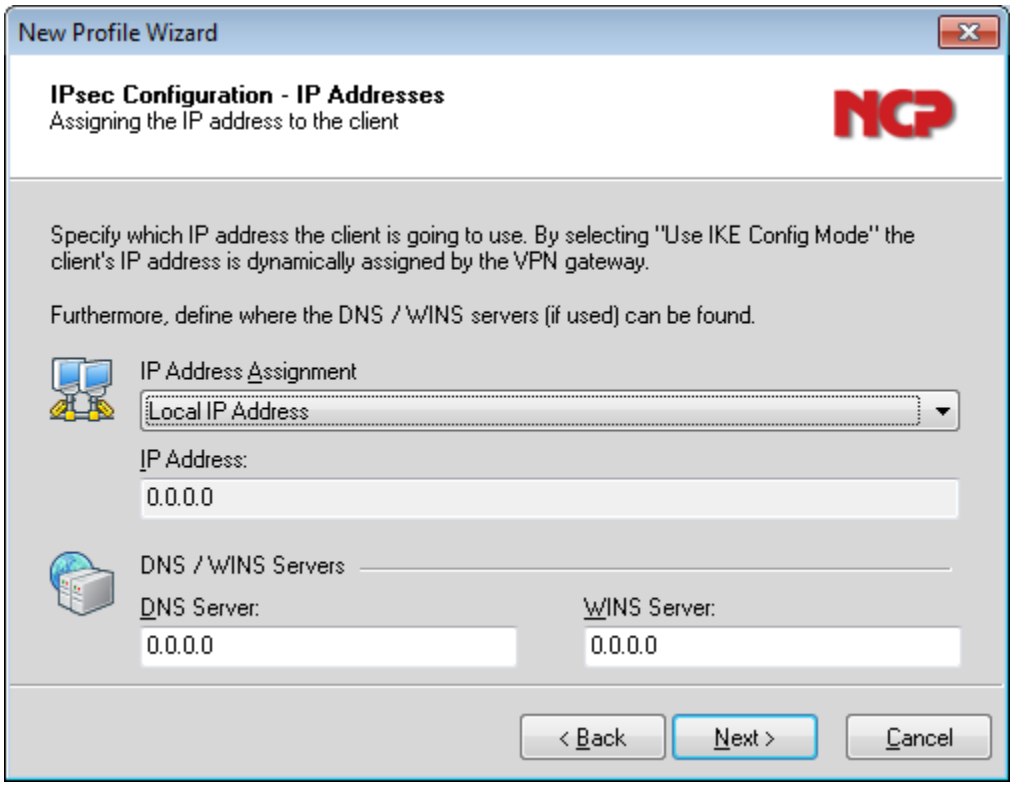
- Select the Mode as “Aggressive” and select the PFS Group:



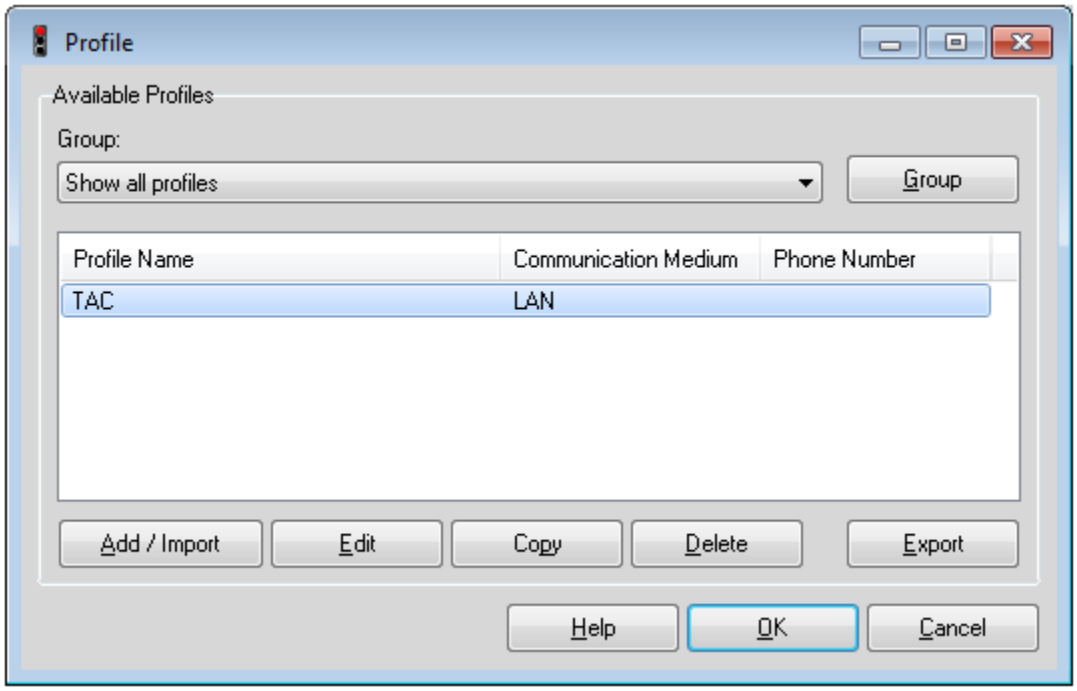
- Enter “Pre-Shared Key” and the IKE identity. If you are using Email as the identity then select “Fully Qualified Username”



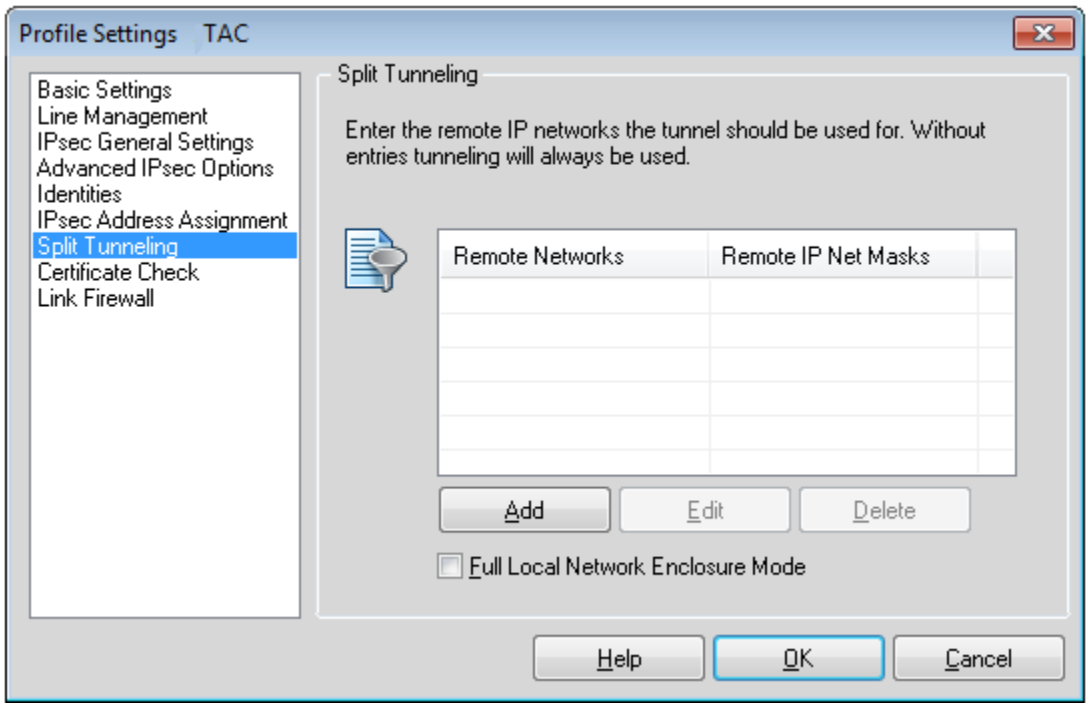
- As shown in the below screenshot, you can also specify the IP that will be used as the Source IP by the Client. (If an IPPool is chosen in the XAuth on the firewall, an IP from the IPPool is taken). Otherwise, you can define it Manually on the client using the dropdown. If you choose “Local IP Address”, and no IP Pool is defined on the Firewall XAuth settings, then the PC’s IP is taken as the Source IP.



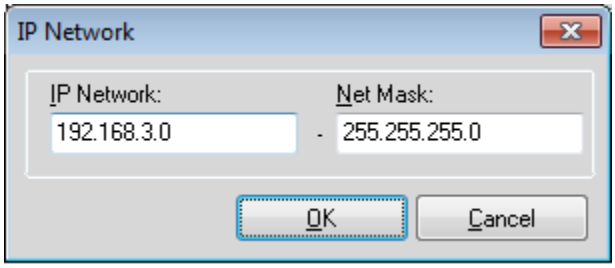
- The profile is now created and will be seen as below:



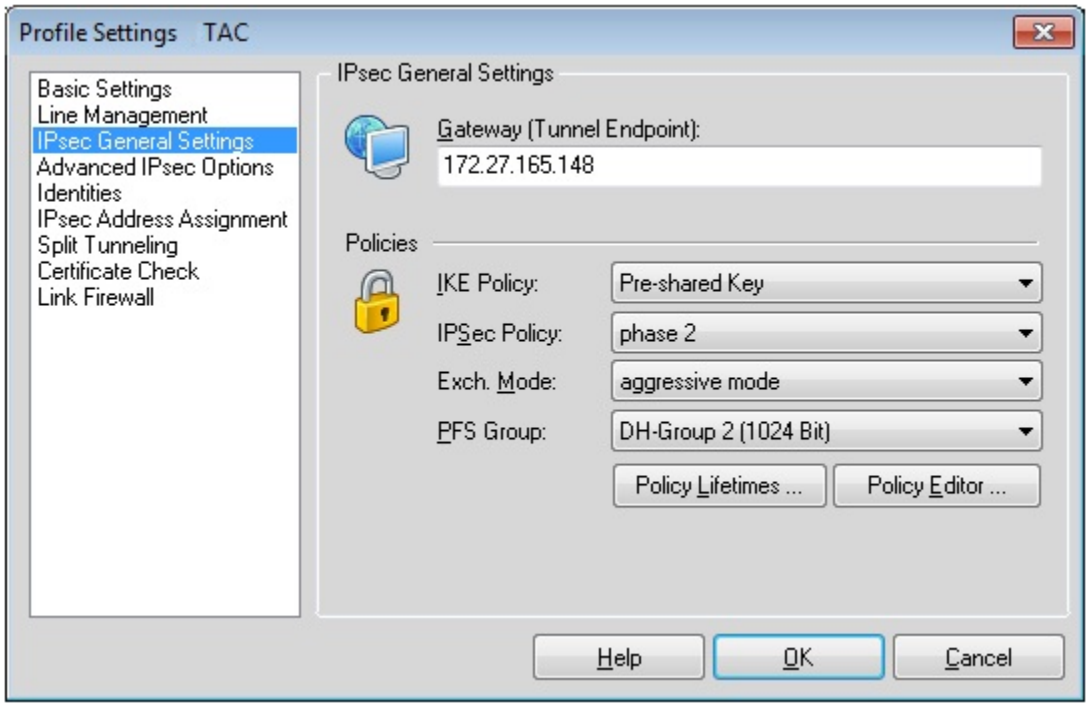
- Note that we have still not defined the Remote side private IPs that we want to reach through the VPN. By default the NCP client takes the subnet as 0.0.0.0/0 which means all traffic from the client will go to the firewall. This also affects the Untrust to Trust policy that we will have to configure at the firewall. If we have to define specific subnets to which we have to reach, we have to define split tunneling. Click on Edit on the profile and go to “Split Tunneling”:



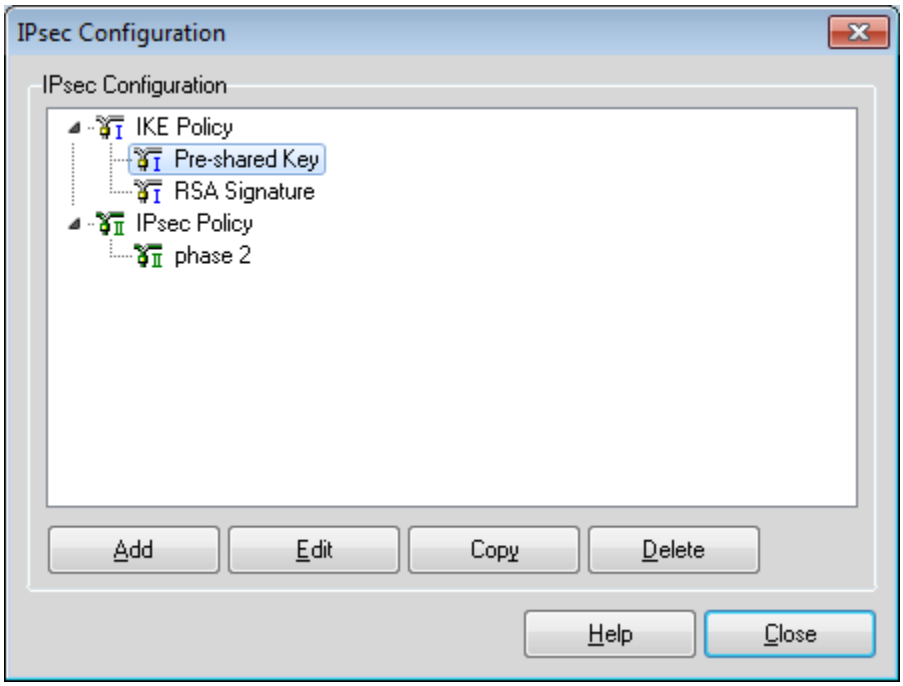
- Add a Network

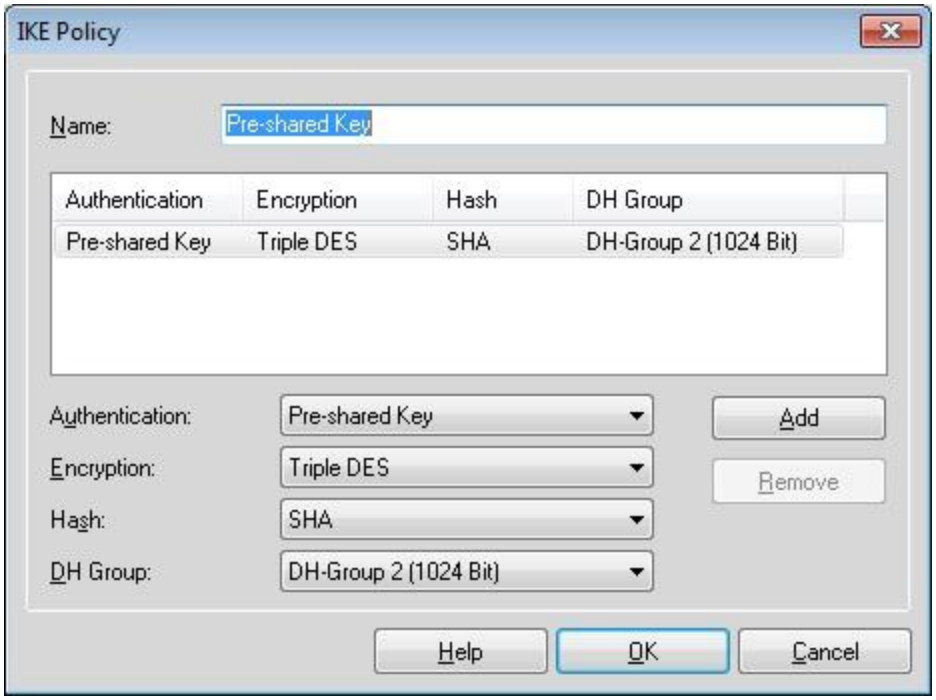


- The Proposals can be chosen/modified in the “IPSec General Settings” when we edit the profile:

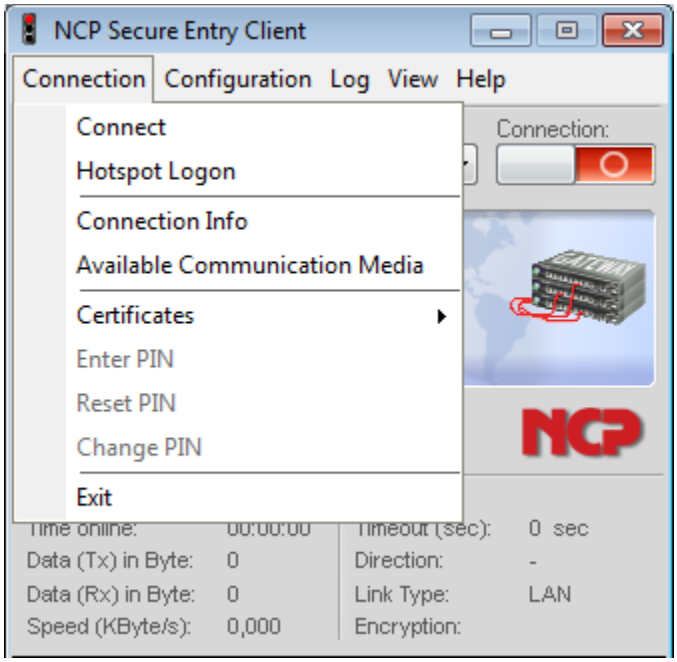


- Click on “Policy Editor” Edit the IKE (Phase 1) and IPSec (Phase 2) proposals. One can also make new proposals.

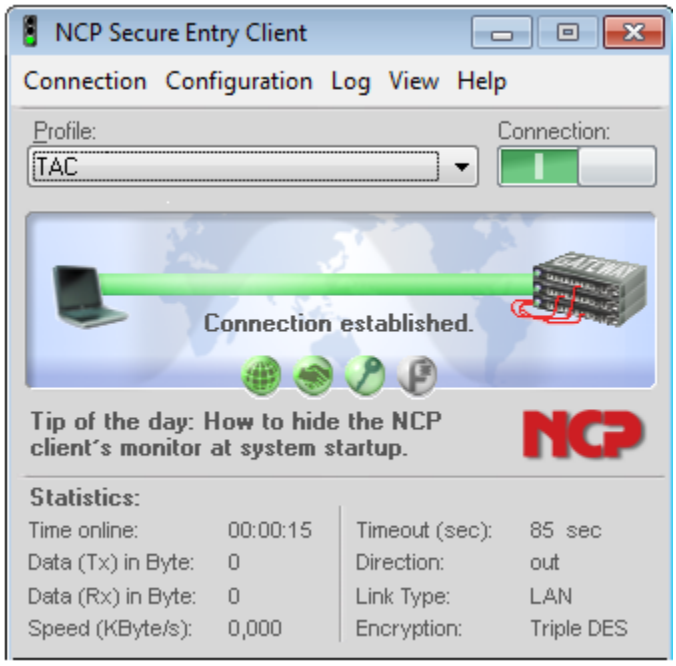




- To connect click on the connection tab



- The connection shows as established.



Note that you can use VPN Monitor with the NCP Client. Otherwise, note that the timeout on NCP is only 100 Seconds by default. We can increase it by editing the profile and going to the "Line Management" option.