

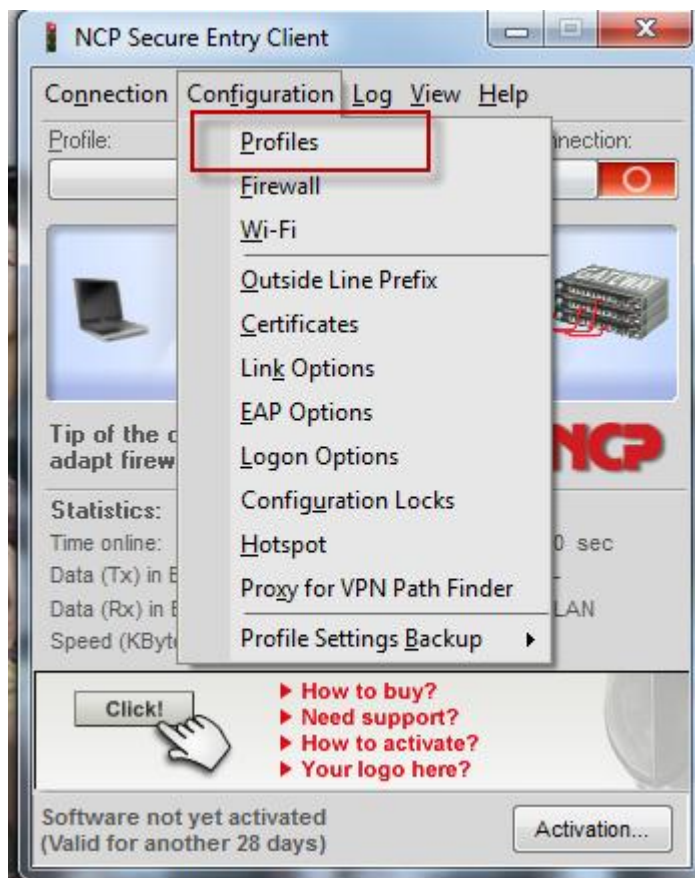
How to setup NCP software with DSR

Topology:

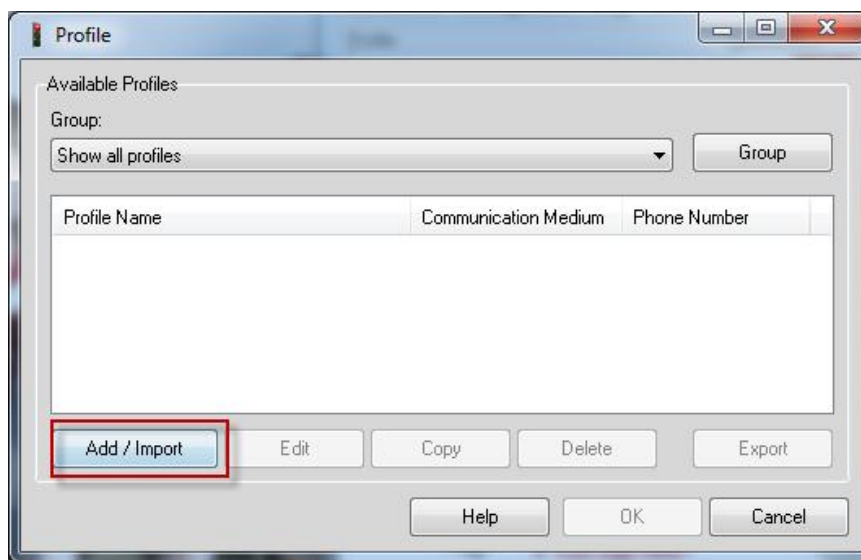


Please follow these procedures to setup. This file just for normal RA IPsec not include "X-Auth" and "mode configuration".

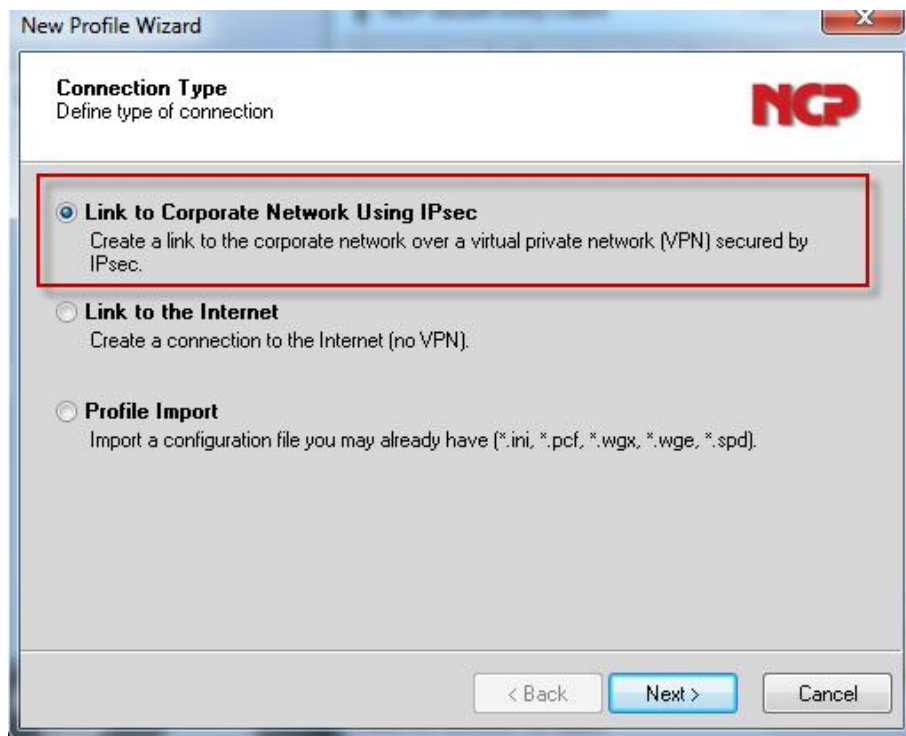
(1)



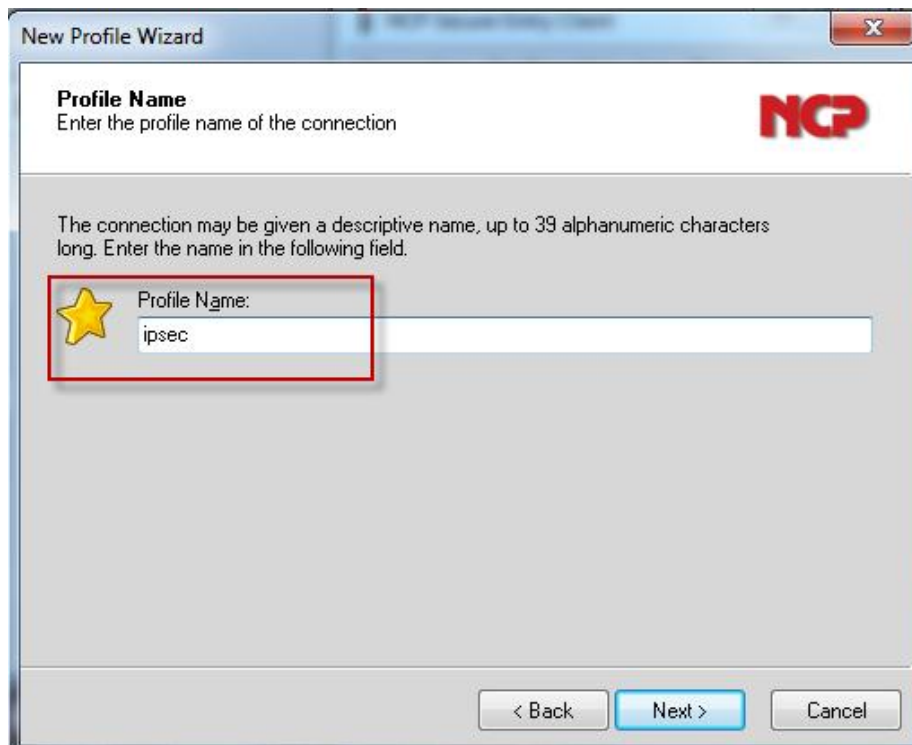
(2)



(3)



(4)



(5)

New Profile Wizard [X]

VPN Gateway Parameters

To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to. Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint):
218.210.16.29

Extended Authentication (XAUTH)

User ID:
[Empty field]

Password: [Empty field] Password (confirm): [Empty field]

[< Back] [Next >] [Cancel]

(6)

New Profile Wizard [X]

VPN Gateway Parameters

To which VPN gateway should the connection be established?

Enter the DNS name (i.e. vpnserver.domain.com) or the official IP address (i.e. 212.10.17.29) of the VPN gateway you want to connect to. Using Extended Authentication (XAUTH) you can enter the user ID and password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

Gateway (Tunnel Endpoint):
218.210.16.29

Extended Authentication (XAUTH)

User ID:
[Empty field]

Password: [Empty field] Password (confirm): [Empty field]


[< Back] [Next >] [Cancel]

(7)

New Profile Wizard

IPsec Configuration
Configure the basic IPsec parameters

The basic IPsec parameters can be specified here. The IPsec negotiations will use "automatic mode" which are pre-defined (default) proposals. In the event that uniquely defined IKE- / IPsec policies are to be used, these can then be defined and assigned using the policy editor under IPsec General Settings.

 Exchange Mode:
main mode (IKEv1)

PFS Group:
DH-Group 2 (1024 Bit)

IPsec Compression

< Back Next > Cancel

(8)

New Profile Wizard

Pre-shared Key
Common Secret for Authentication

A shared secret or pre-shared key is used to encrypt the connection. This then needs to be identically configured on both sides (VPN client and VPN gateway).

Enter the appropriate value for the IKE ID according to the selected ID type.

 Pre-shared Key _____

Shared Secret: _____ Confirm Secret: _____

Local Identity (IKE) _____

Type: IP Address

ID: _____

< Back Next > Cancel

(9)

New Profile Wizard

IPsec Configuration - IP Addresses
Assigning the IP address to the client

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

Furthermore, define where the DNS / WINS servers (if used) can be found.

IP Address Assignment
Local IP Address
IP Address:
0.0.0.0

DNS / WINS Servers
DNS Server: 0.0.0.0
WINS Server: 0.0.0.0

< Back Next > Cancel

(10)

New Profile Wizard

IPsec Configuration - IP Addresses
Assigning the IP address to the client

Specify which IP address the client is going to use. By selecting "Use IKE Config Mode" the client's IP address is dynamically assigned by the VPN gateway.

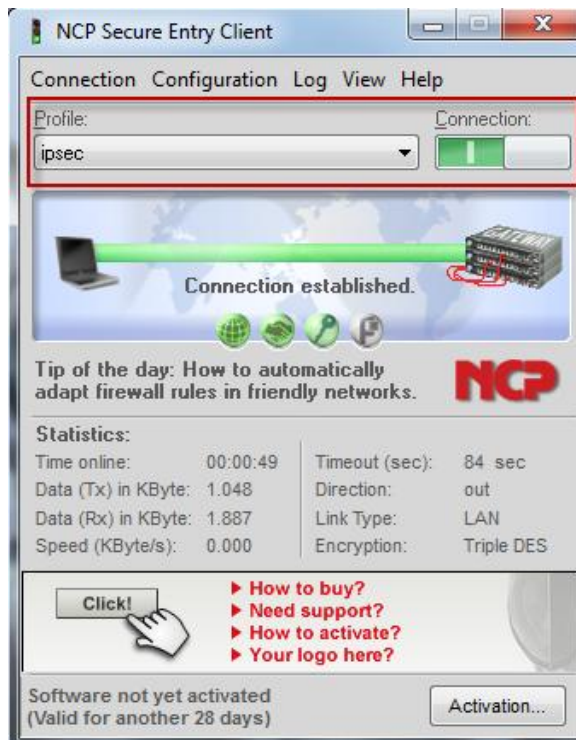
Furthermore, define where the DNS / WINS servers (if used) can be found.

IP Address Assignment
Manual IP Address
IP Address:
124.8.64.198

DNS / WINS Servers
DNS Server: 0.0.0.0
WINS Server: 0.0.0.0

< Back Next Cancel

(11)



(12)

