



SECURE COMMUNICATIONS ■

NCP Secure Entry Client

A quick configuration guide to setting up the NCP Secure Entry Client in typical VPN scenarios

These scenarios were developed by the VPN Consortium

Scenario 1. **Client-to-Gateway using pre-shared secrets**

Typical client-to-gateway VPN using a preshared secret for authentication.
Description how to configure the NCP Secure Entry Client for Windows.

Scenario 2. **Client-to-Gateway with certificates**

Typical client-to-gateway VPN that utilizing certificates for authentication
Description how to configure the same scenario but then instead of using pre-shared keys, PKIX (x509v3) certificates are used for authentication.

Document version 3.02

Using **NCP Secure Entry Client v9.23** build 18

Prepared by:

NCP Engineering GmbH
Dombuehler Strasse 2,
90449 Nürnberg, Germany
Phone: +49-911-99.68.0
Fax: +49-911-99.68.299

Disclaimer

Considerable care has been taken in the preparation of this quick guide, errors in content, typographical or otherwise may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP as desired.

NCP makes no representations or warranties with respect to the contents or use of this quick guide, and explicitly disclaims all expressed or implied warranties of merchantability or use for any particular purpose. Furthermore, NCP reserves the right to revise this publication and to make amendments to the content, at any time, without obligation to notify any person or entity of such revisions and changes.

Copyright

This quick guide is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH, Dombühler Str.2, D-90449 Nürnberg, Germany.

Trademarks

All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© 2010 NCP Engineering GmbH. All rights reserved.

NCP Quick Configuration Guide: Secure Entry Client

Section 1: Client-to-Gateway using pre-shared secrets

- 1.1: *Scenario Setup*
- 1.2: *Using the Profile Wizard*
- 1.3: *Checking/Modifying the Configuration*
- 1.4: *Establishing the Connection*

Section 2: Client-to-Gateway with certificates

- 2.1: *Scenario Setup*
- 2.2: *Installing the trusted CA certificate for Trusted Root CA*
- 2.3: *Installing new user certificate*
- 2.4: *Using the Profile Wizard*
- 2.5: *Checking/Modifying the Configuration*
- 2.6: *Establishing the connection*
- 2.7: *Verifying the Defined Certificate*

1. Scenario 1: Client-to-gateway with pre-shared secrets

1.1 Scenario Setup

The following is a typical client-to-gateway VPN that uses a preshared secret for authentication.

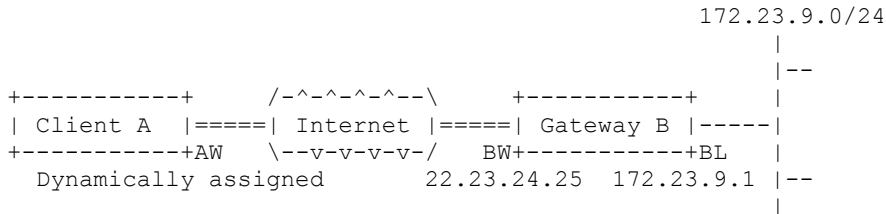


figure 1.1.1: Scenario

Client A's WAN interface (AW) has the address dynamically assigned to it by the ISP. Client A will access Gateway B's internal LAN, by means of a secure tunnel.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Client A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying

Selectors for all IP protocols, all ports, between the client and 172.23.9.0/24, using IPv4 subnets

1.2 Using the Profile Wizard

The very first time you start up the NCP Entry Client you will be prompted to create a profile which will allow you to connect to the NCP Demo VPN gateway. A connection using only pre-shared keys or one using certificate based authentication can be selected and working example profiles are then generated.

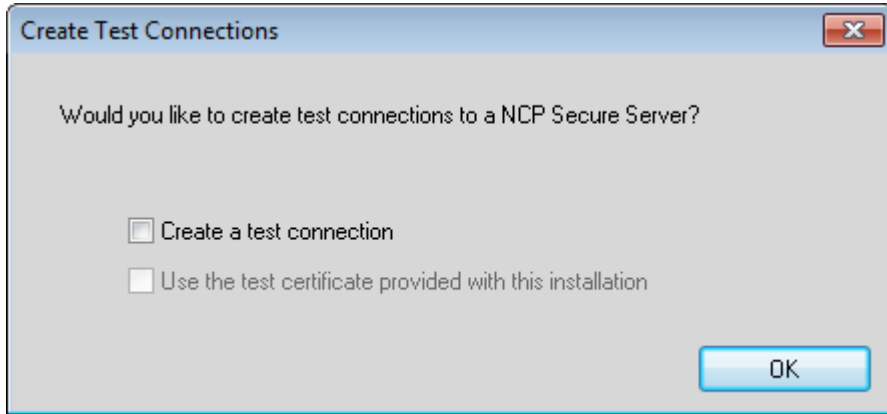


figure 1.2.1: Create Test Connections

For the scope of this document, we are not required to select anything here: one can however, use these profiles to ensure that the client has been installed and functioning correctly.

Either way, we'll create a (or another) profile from scratch that fits the scenario as outlined in section 1.1.

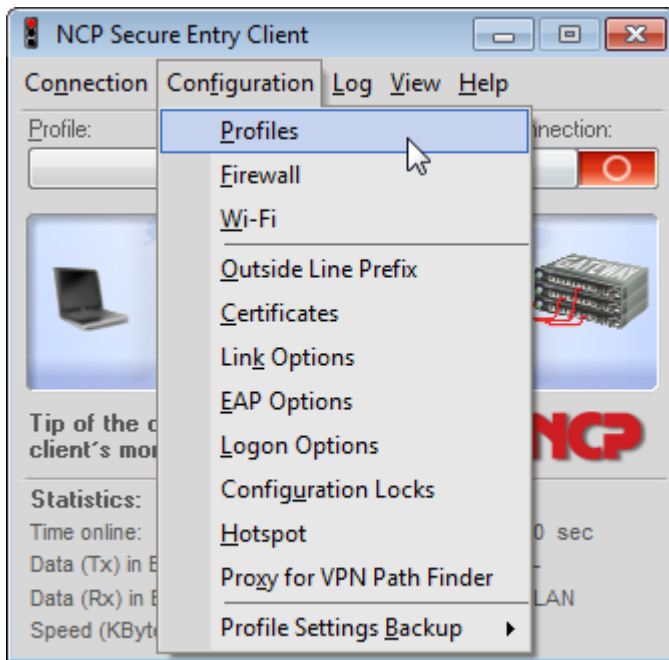


figure 1.2.2: Configuration

Open up the profiles by selecting **Profiles** from the drop down list under **Configuration**.

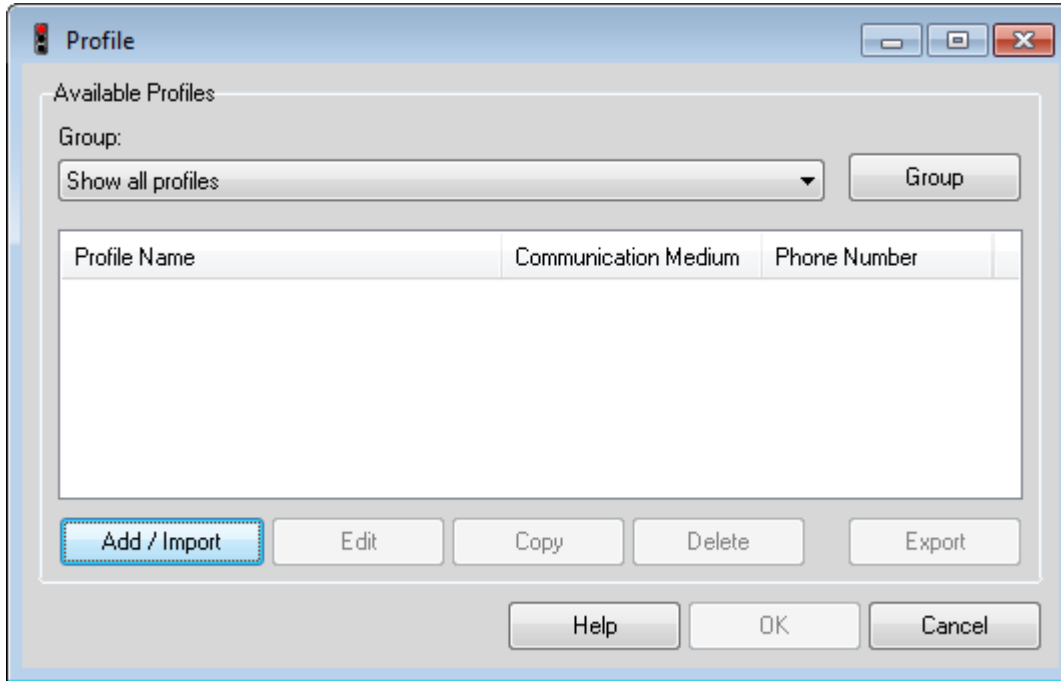


figure 1.2.3: Profile

You can either use the wizard as outlined in this section, or modify an existing profile as in section 1.3. Click **Add / Import** to create a configuration / connection profile from scratch using a wizard.

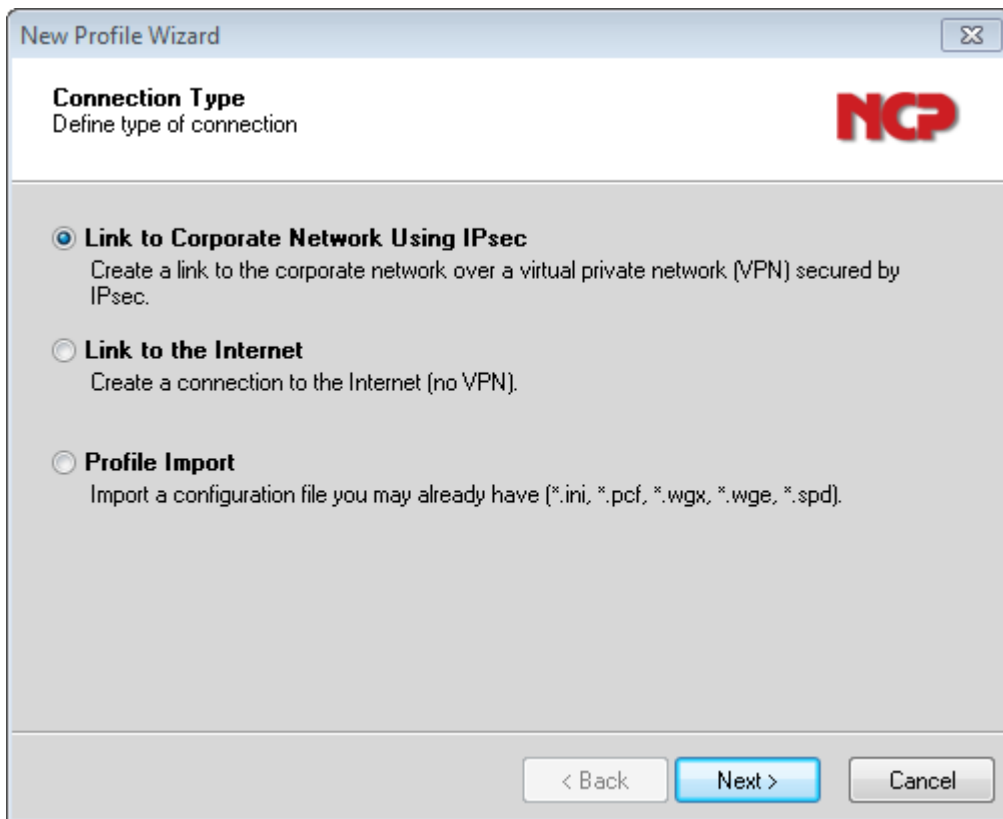


figure 1.2.4: New Profile Wizard: Connection Type

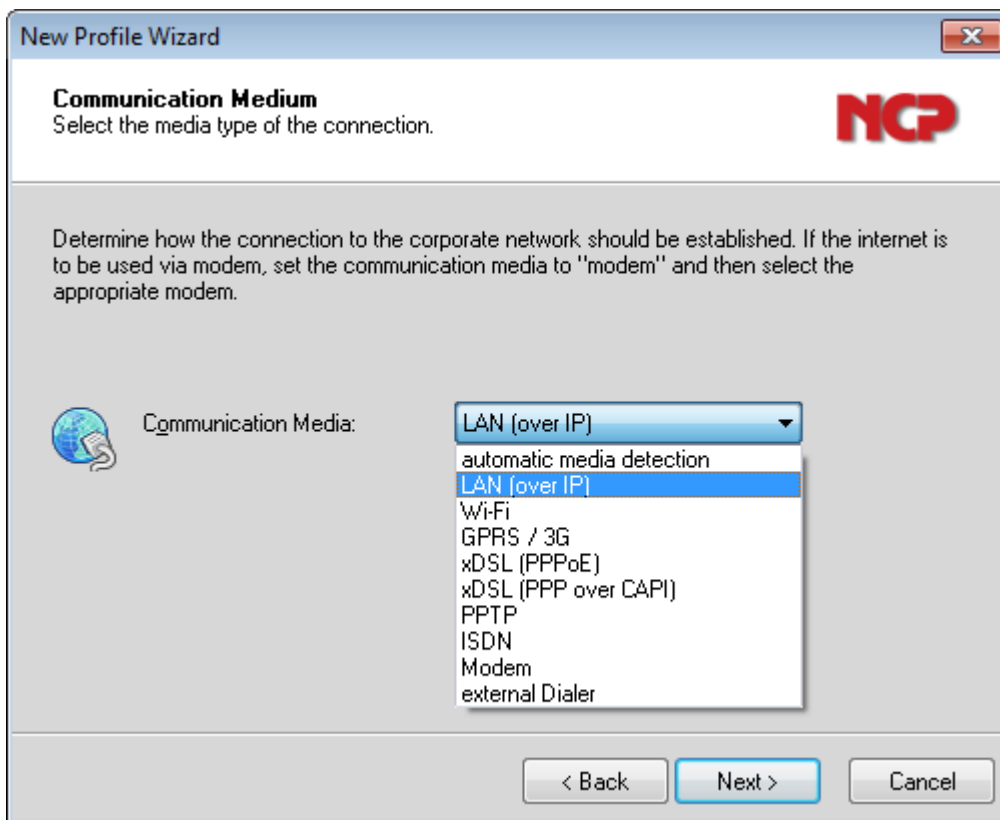
Select **Link to Corporate Network using IPsec** to create a connection profile with the parameters needed to establish a connection to the VPN Gateway **Gateway B** as illustrated in Figure 1.1.1. Click **Next >**.



The screenshot shows a window titled "New Profile Wizard" with a close button in the top right corner. The main heading is "Profile Name" with the instruction "Enter the profile name of the connection". A yellow star icon is positioned to the left of the "Profile Name:" label. Below the label is a text input field containing "Gateway B". A descriptive paragraph states: "The connection may be given a descriptive name, up to 39 alphanumeric characters long. Enter the name in the following field." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted in blue.

figure 1.2.5: New Profile Wizard: Profile Name

Several profiles can be created and each given different name. In this example, this profile is created and given the name **Gateway B**. Click **Next >**.



The screenshot shows a window titled "New Profile Wizard" with a close button in the top right corner. The main heading is "Communication Medium" with the instruction "Select the media type of the connection". A globe icon is positioned to the left of the "Communication Media:" label. Below the label is a dropdown menu with "LAN (over IP)" selected. The dropdown list includes: "automatic media detection", "LAN (over IP)", "Wi-Fi", "GPRS / 3G", "xDSL (PPPoE)", "xDSL (PPP over CAPI)", "PPTP", "ISDN", "Modem", and "external Dialer". A descriptive paragraph states: "Determine how the connection to the corporate network should be established. If the internet is to be used via modem, set the communication media to 'modem' and then select the appropriate modem." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted in blue.

figure 1.2.6: New Profile Wizard: Communication Media

The NCP Secure Entry Client supports different communication media types; the integrated dialer for example, can be used to establish a connection to the ISP with a modem (if available to the system) prior to building the VPN Tunnel. (see manual for further details)

In this example however, select **LAN (over IP)**. Click **Next >**.

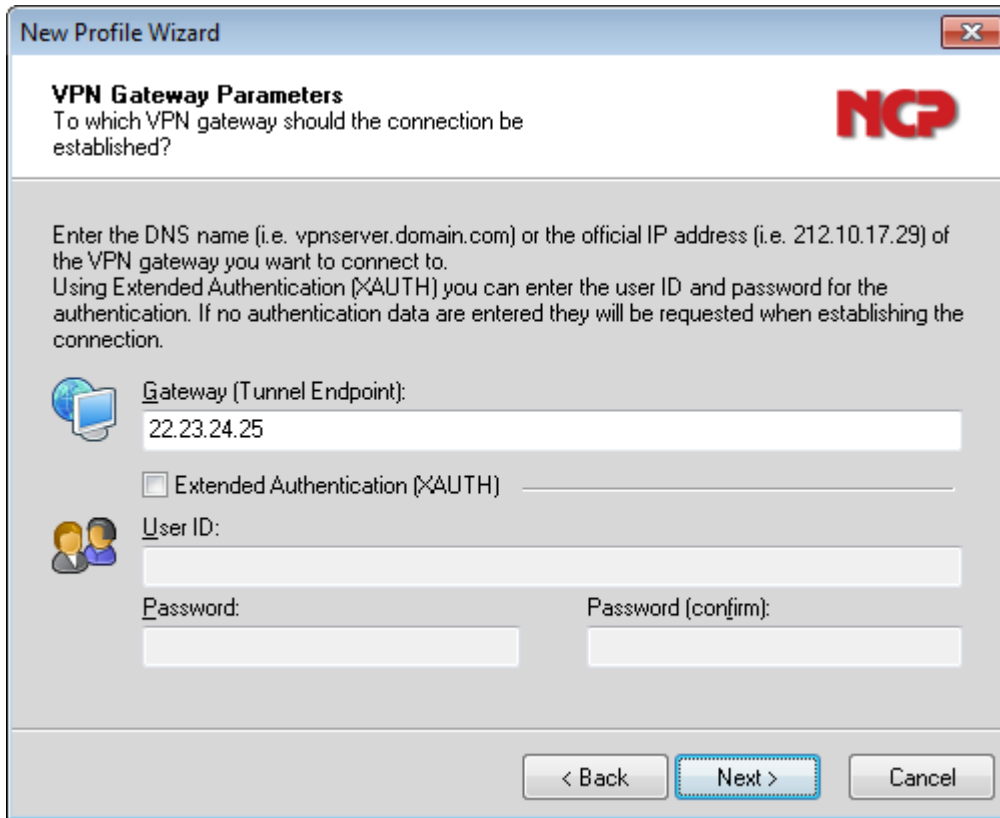


figure 1.2.7: New Profile Wizard: VPN Gateway Parameters

Enter in the gateway's IP address or DNS name. (If the VPN Gateway supports extended authentication (XAUTH) as defined in draft-beaulieu-ike-xauth-02 then enter in the appropriate **Username** and **Password**.) Click **Next >**.

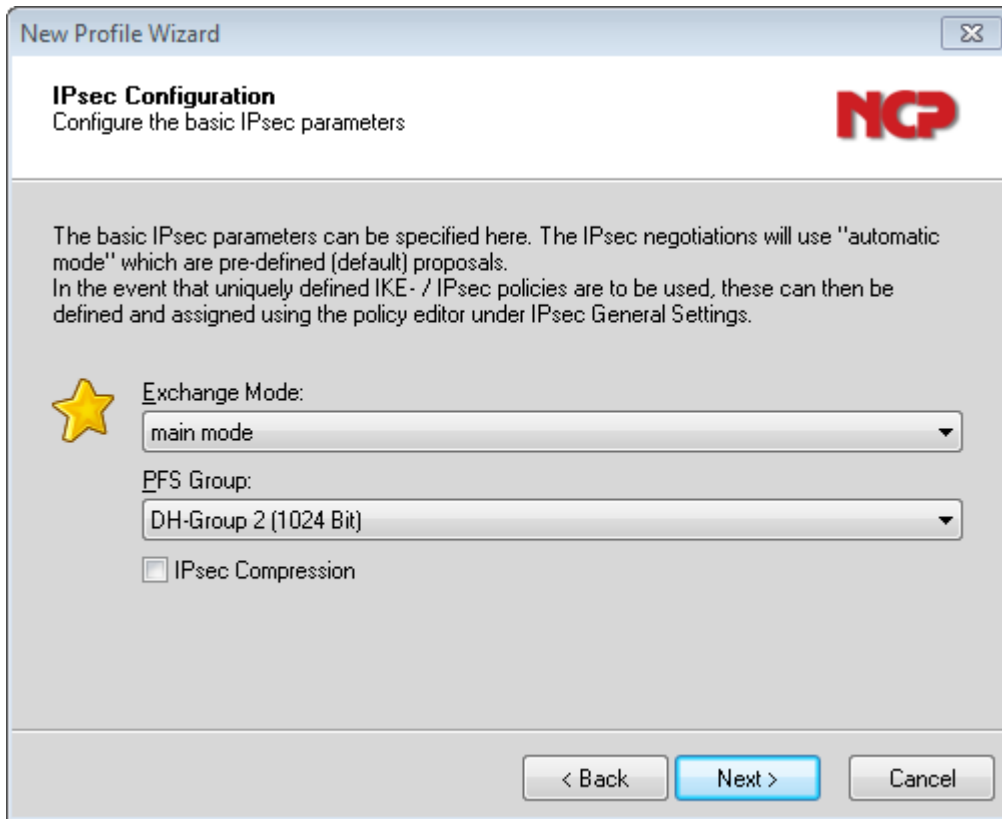


figure 1.2.8: New Profile Wizard: IPsec Configuration

This example will use **Main Mode** and **Perfect Forward Secrecy** seamless re-keying, employing **DH-Group2 (1024 Bit)** as indicated in section 1.1. Click **Next >**.

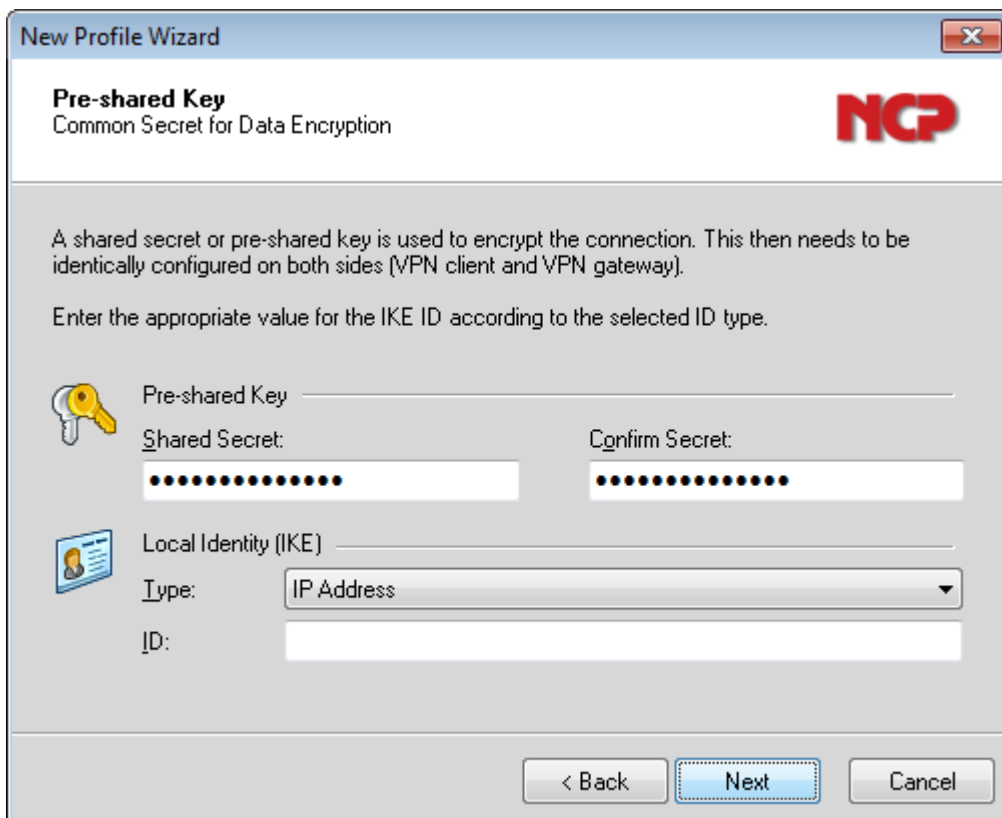


figure 1.2.9: New Profile Wizard: Pre-shared Keys

In this example, a pre-shared key or shared secret is used, identical passwords on the two IPsec communicating peers. Enter in the given **hr5xb84l6aa9r6** (see section 1.1) and confirm this to ensure that it is entered in correctly.

The **Next >** button will not be available until the values have been correctly entered in and match.

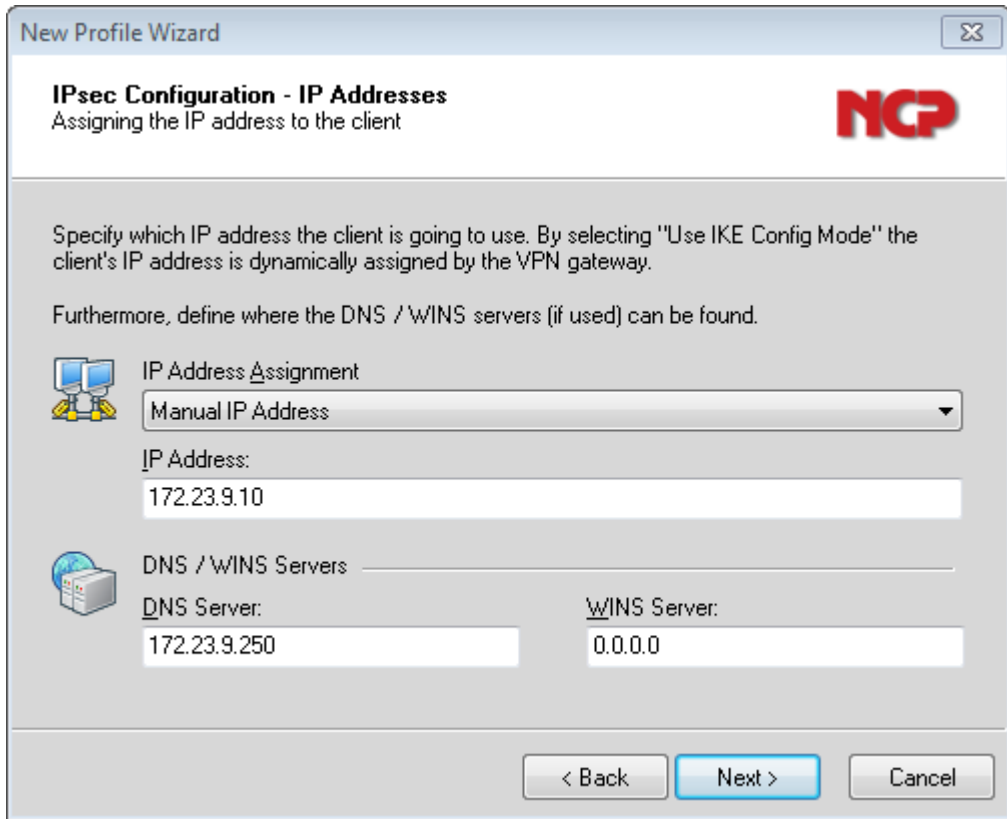


figure 1.2.10: New Profile Wizard: IPsec Configuration – IP addresses

Often the VPN Gateway will designate a virtual IP address to the incoming VPN connection. The NCP Secure Entry client supports three options, manual IP address assignment, IKE-Config Mode, or using the IP address assigned to the physical network interface ("AW": see figure 1.1.1). In this example, one assumes that the IP address and the appropriate subnet mask is manually assigned to the client.

Click **Next >** to continue.

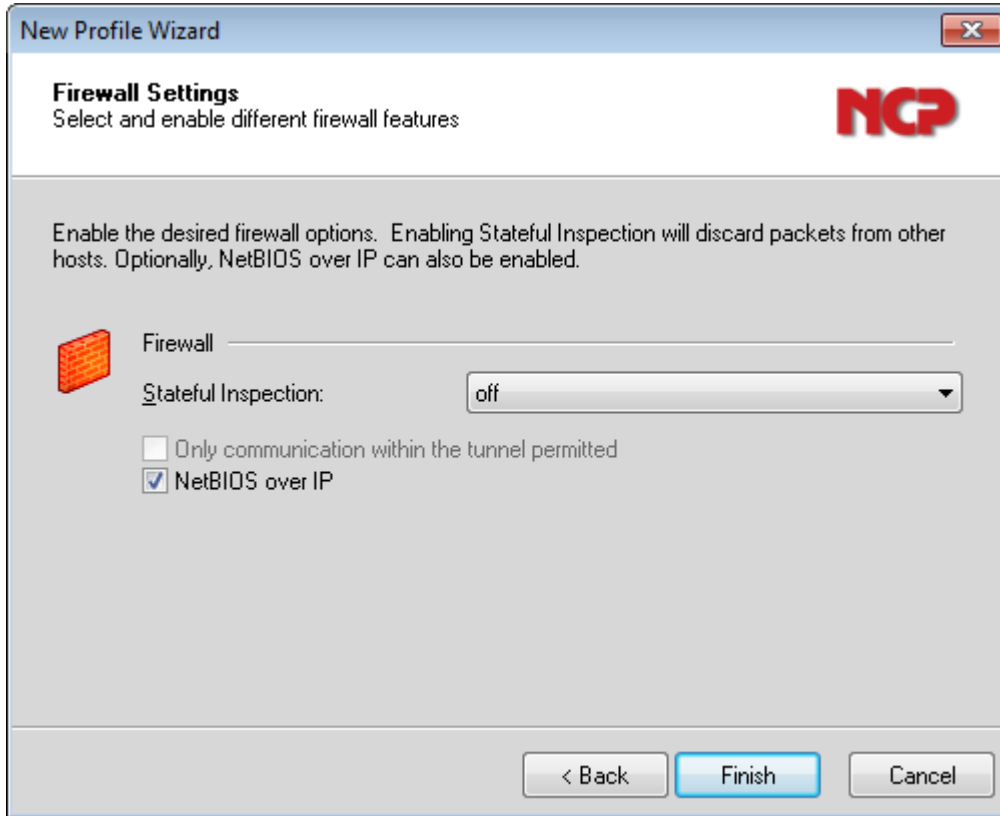


figure 1.2.11: New Profile Wizard: Firewall settings

The NCP Secure Entry Client also comes with a personal firewall that can be configured in detail or one could enable the **Link Firewall** (meaning that stateful inspection can be enabled ONLY when this profile has been selected). Not enabled for this scenario. Click **Finish** to save the setting to this profile.

1.3 Checking/Modifying the Configuration

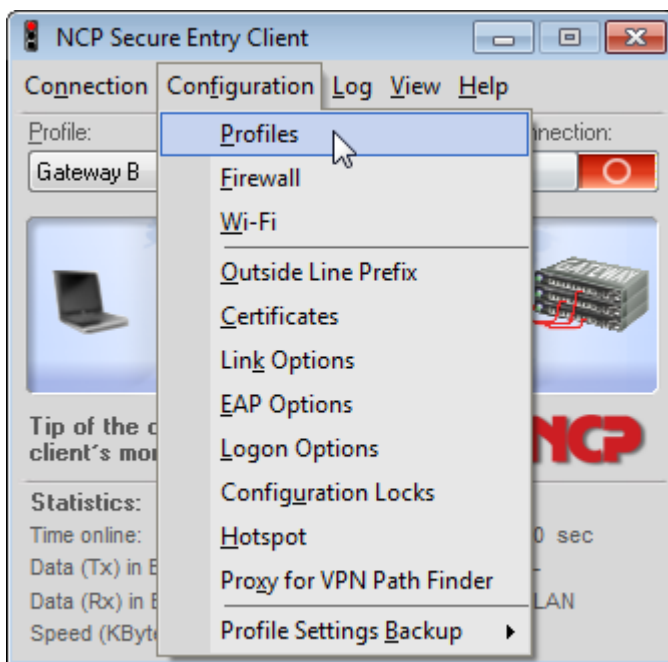


figure 1.3.1: Configuration -> Profiles

Open the **Profiles** to modify the parameters to define the specific IKE and IPsec proposals as specified in section 1.1.

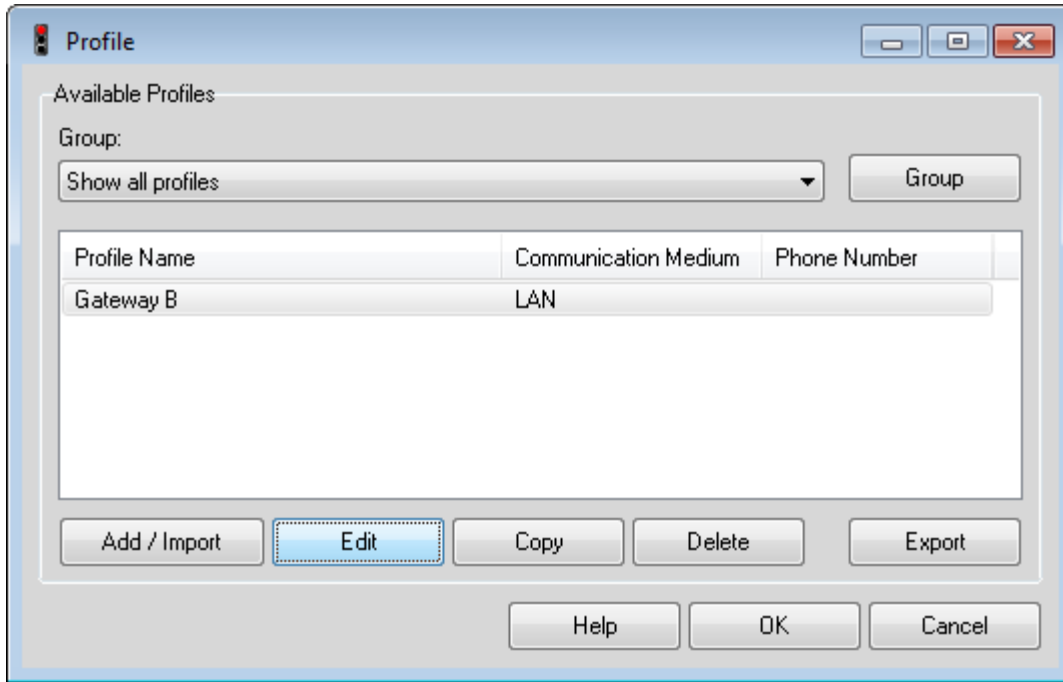


figure 1.3.2: Profile

Either double-click on the profile that is going to be modified, or select the profile and then click on **Edit**.

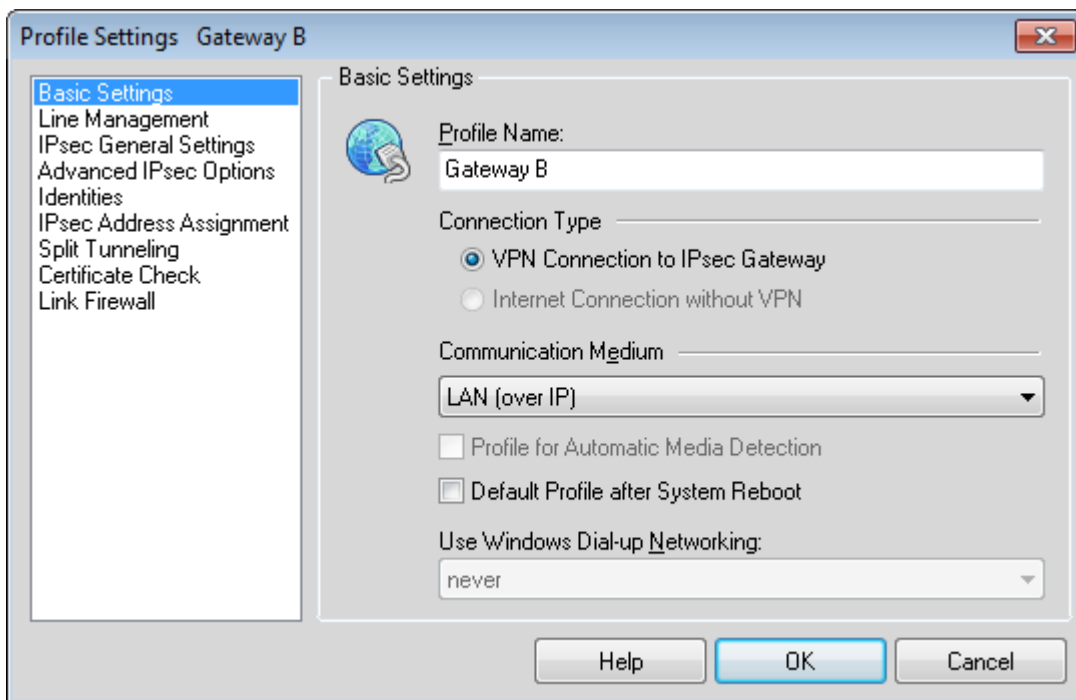


figure 1.3.3: Profile Settings: Basic Settings

Review the parameters and ensure they are correct. Select **Line Management** to continue...

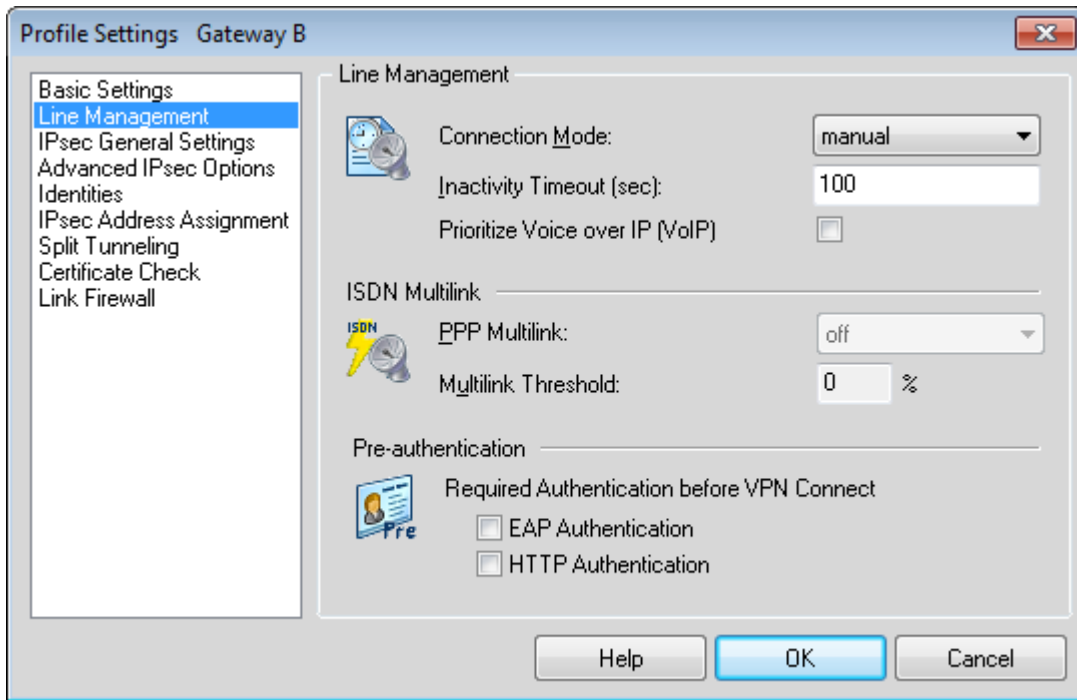


figure 1.3.4: Profile Settings: Line Management

The **Connection Mode** can be set to connect automatically, meaning that any time a packet is destined for Gateway B's LAN, the VPN Tunnel can automatically be established. In this example however, one manually establishes the connection. The **Inactivity Timeout** is set to 100 seconds.

Select **IPsec General Settings** to continue...

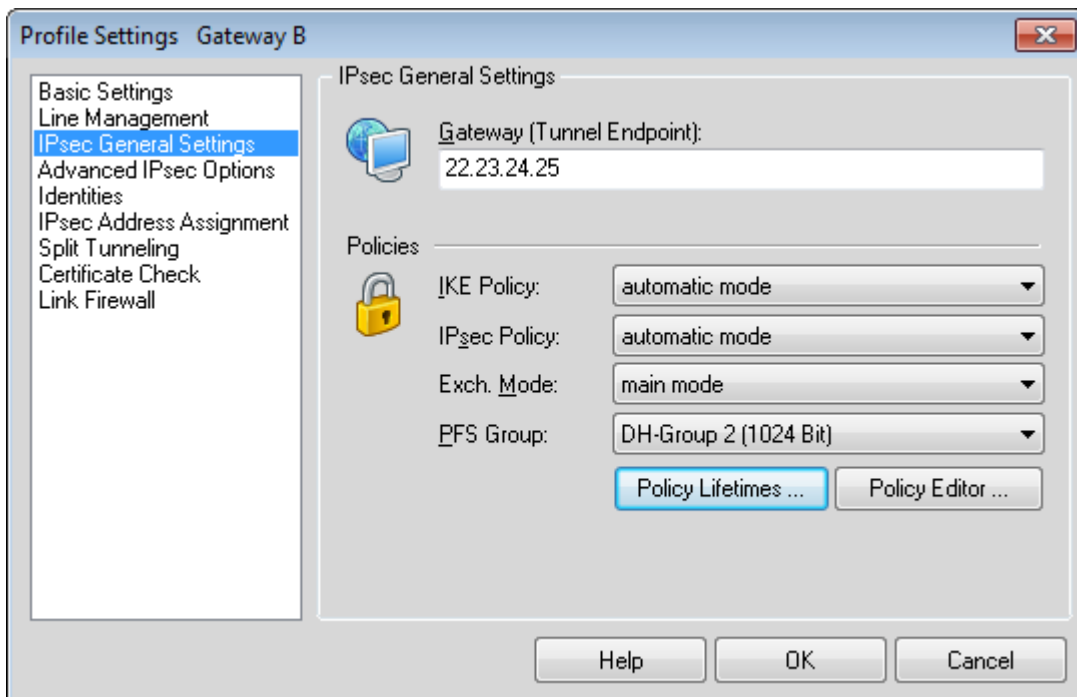


figure 1.3.5: Profile Settings: IPsec General Settings: Policy Lifetimes

When **automatic mode** is selected for both the **IKE** (Phase 1) and **IPsec** (Phase 2) **Policies**, the client will transmit a range of different commonly used proposals and the VPN Gateway can then select one to use for the connection. However, in this example, both the IKE and IPsec policies have been specifically defined in section 1.1; so select **Policy lifetimes...**

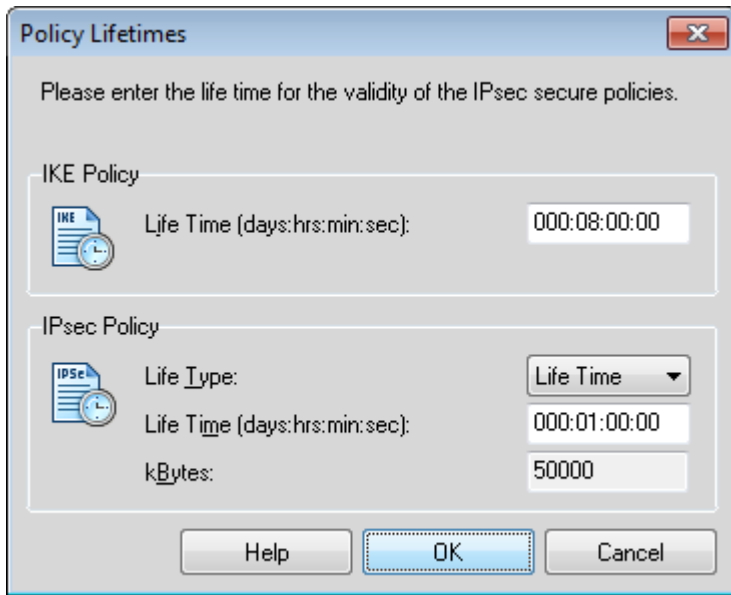


figure 1.3.6: Policy Lifetimes

The duration for the IKE Policy (SA lifetime) has been set to 8 hours (28800 seconds), and the IPsec Policy (SA) lifetime is limited to 1 hour (3600 seconds). Simplified, this means the connection will be re-authenticated as it were every 8 hours, and the session key (used to encrypt the payload) is refreshed every hour.

Click **OK** to return to define the Proposals...

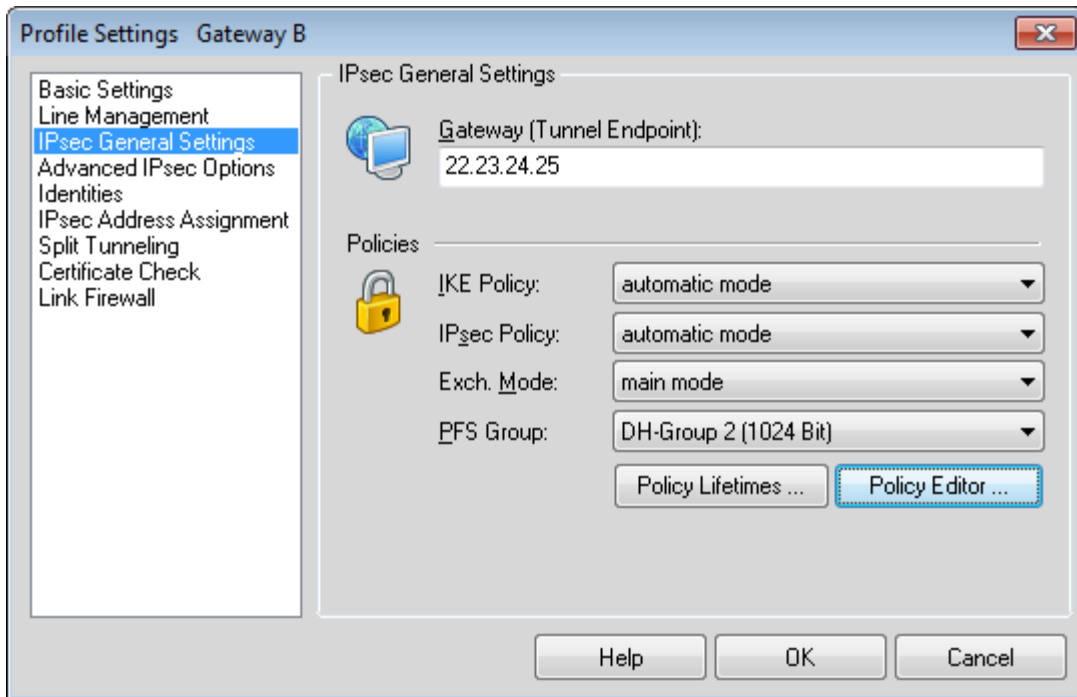


figure 1.3.7: Profile Settings: IPsec General Settings: Policy Editor

Select the **Policy Editor ...** to define specific proposals to be used in this connection as lined out in section 1.1.

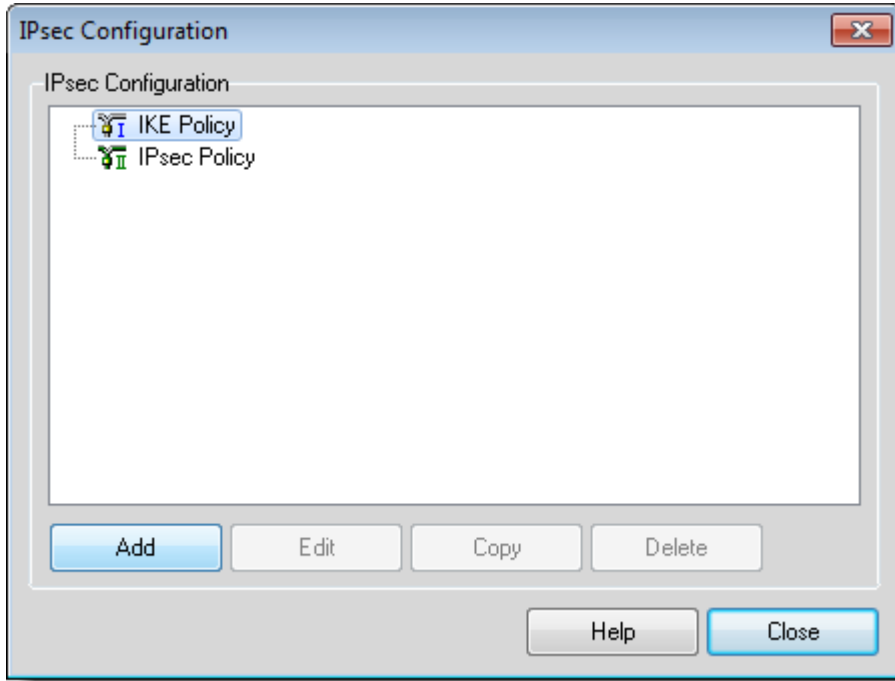


figure 1.3.8: Proposal Definitions: IKE Policy Configuration

First select **IKE Policy** and click on **Add** to define a new IKE Policy (Phase 1 parameters) to be used.

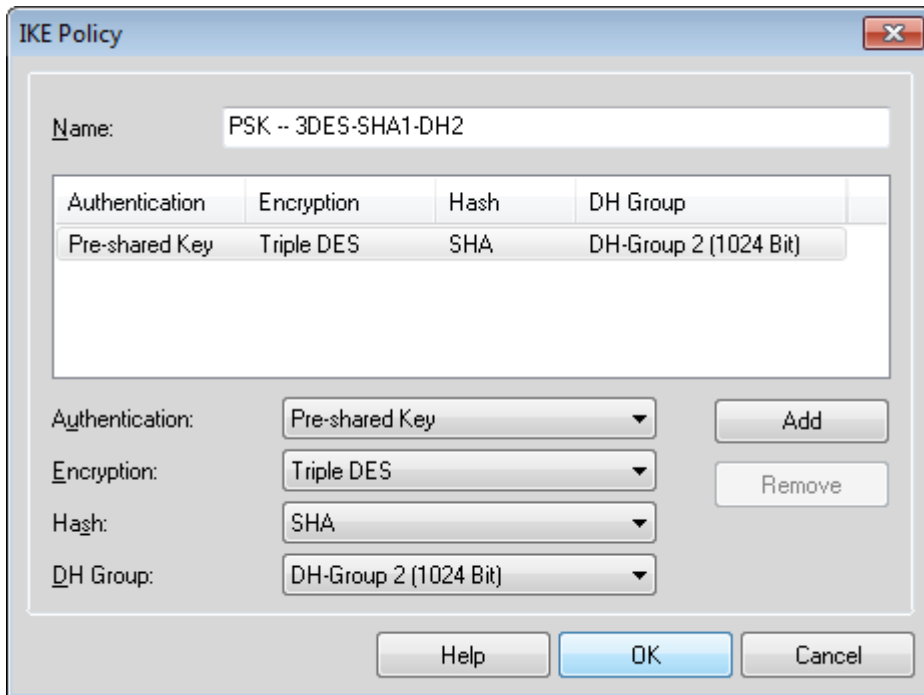


figure 1.3.9: Defining an IKE Policy

Simply select the parameters for this proposal. Several proposals may be grouped together under the name, but for the purpose of this example, only one proposal is defined. Select **Pre-shared Key** for the IKE mode, **Triple DES** (168bit 3DES) for the encryption algorithm to be used, **SHA1** (160bit SHA-1) for the authentication algorithm, and finally **DH-Group 2 (1024 Bit)** for the key exchange protocol.

Click **OK** to return to the previous dialog box.

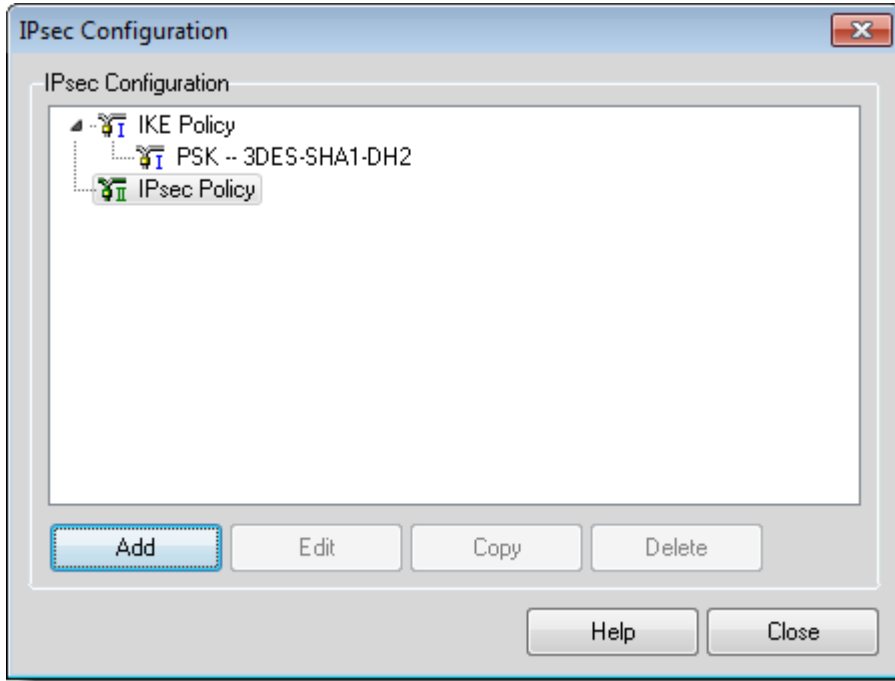


figure 1.3.10: Proposal Definitions: IPsec Policy Configuration

In the same way, select **IPsec Policy** and click **Add** to define the IPsec proposal (Phase 2 parameters).

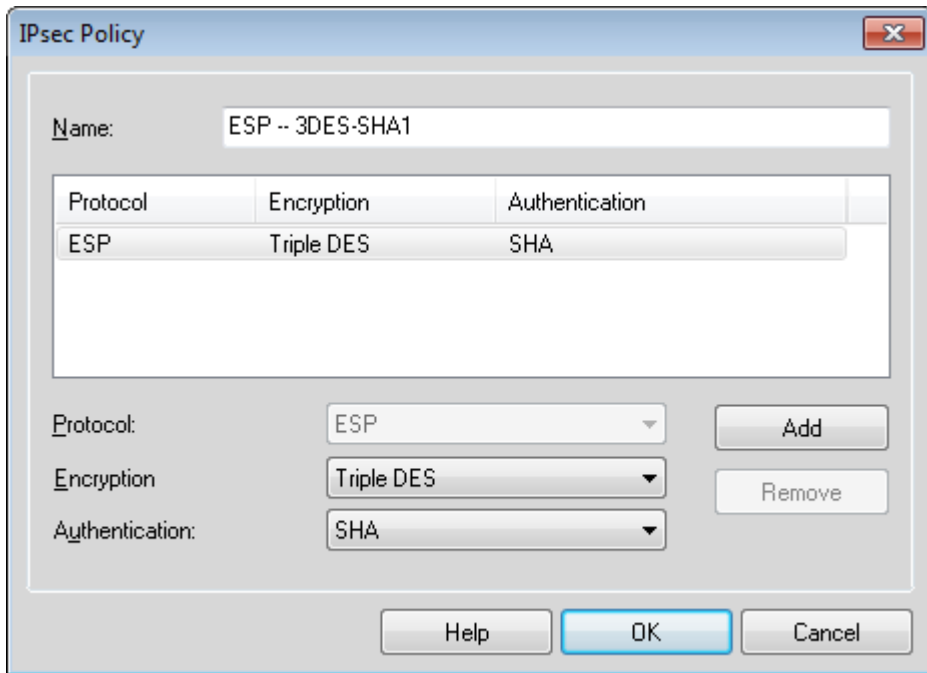


figure 1.3.11: Defining an IPsec Policy

Simply select the parameters for this policy: **ESP** tunnel mode, **Triple DES** (168bit 3DES-CBC) for encryption algorithm and **SHA1** (SHA-1 160 Bit) for the authentication code/hash algorithm.

Click **OK** to continue...

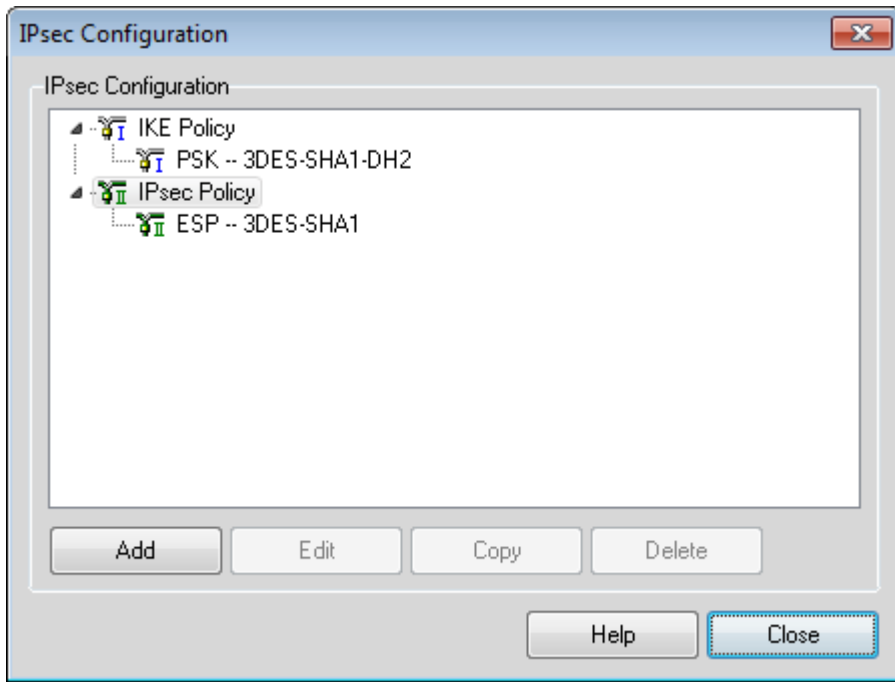


figure 1.3.12: IPsec/IKE (ISAKMP) parameters defined

Click on **Close** to save the proposals created, and return to the **Profile Settings | IPsec General Settings** dialog box.

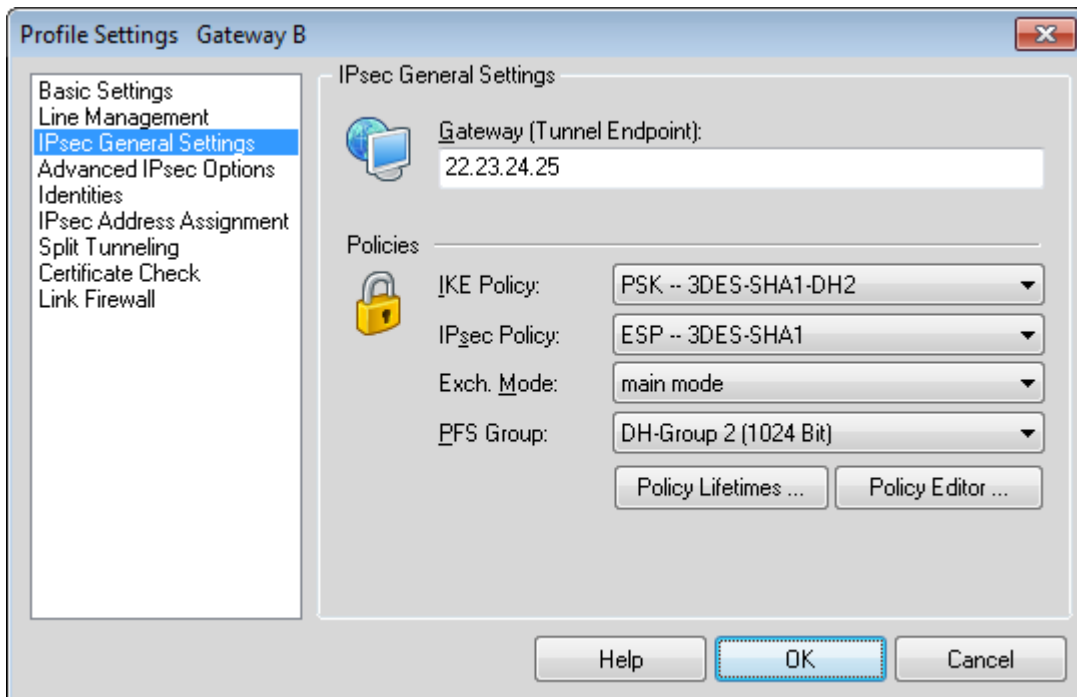


figure 1.3.13: Profile Settings: IPsec General Settings, Policy Definitions

Select the newly defined **IKE-** (ISAKMP) "PSK – 3DES-SHA1-DH2" and **IPsec** "ESP – 3DES-SHA1" **Policies** from the dropdown list to apply the **IKE-** and **IPsec Policy** as shown above, and click on **Advanced IPsec Options** to move to the next dialog box.

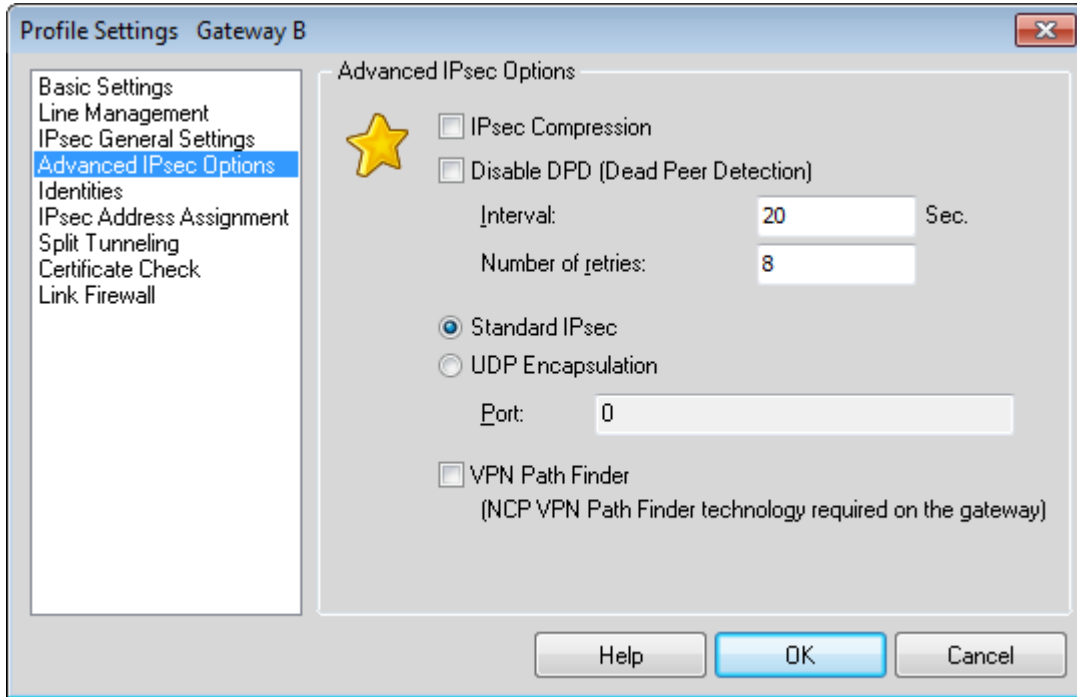


figure 1.3.14: Profile Settings: Advanced IPsec Options

Ensure that **Standard IPsec** is selected here (other options available here are beyond the scope of this quick configuration guide). Click on **Identities** to move to the next dialog box.

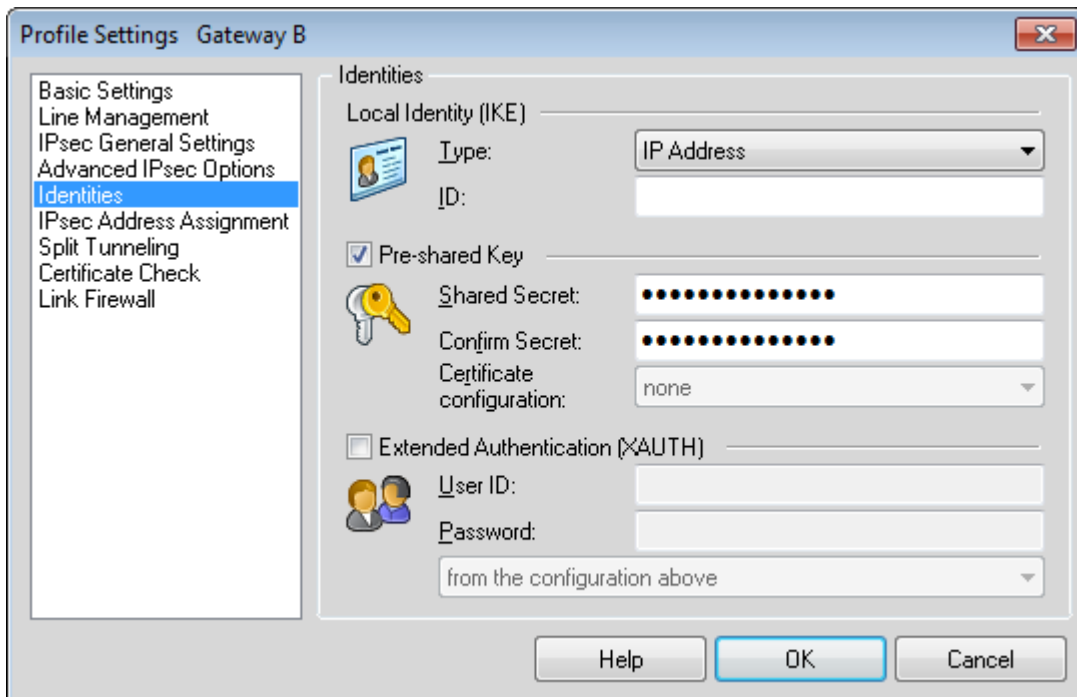


figure 1.3.15: Profile Settings: Identities

In this scenario, the gateway will not know what the IP Address is going to be, so the value is left blank. Other IKE-ID types can be used, but are again beyond the scope of this document; please refer to the manual for more details.

Click on **IPsec Address Assignment** to continue...

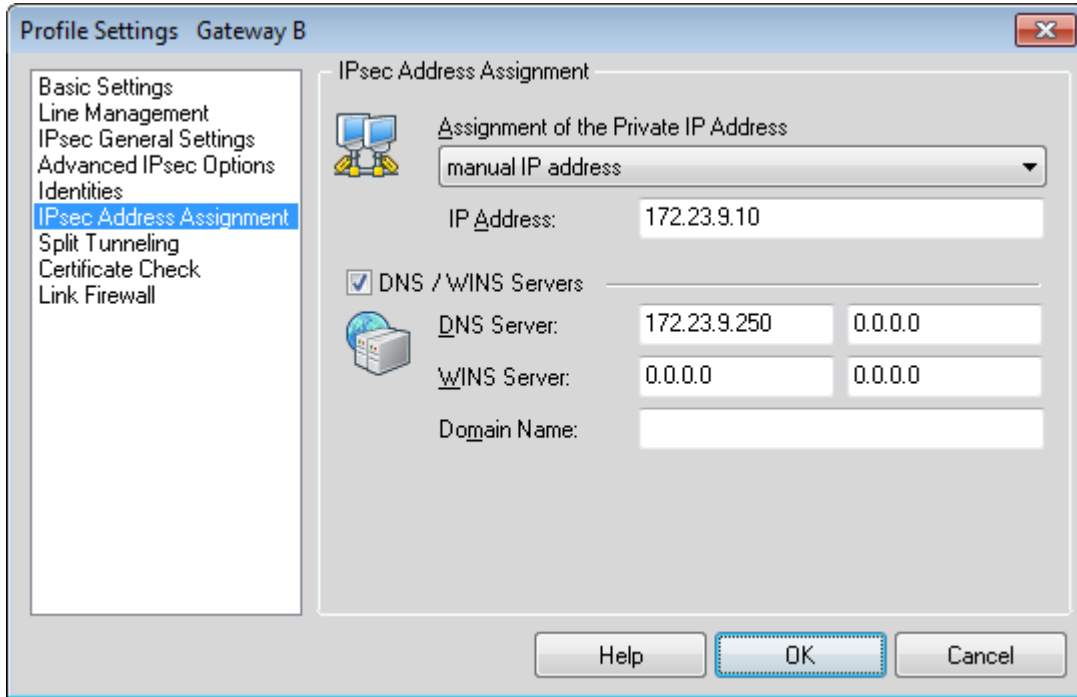


figure 1.3.16: Profile Settings: IPsec Address Assignment

Confirm the settings as entered in figure 1.2.10. Then click on **Split Tunneling** to move to the next dialog box.

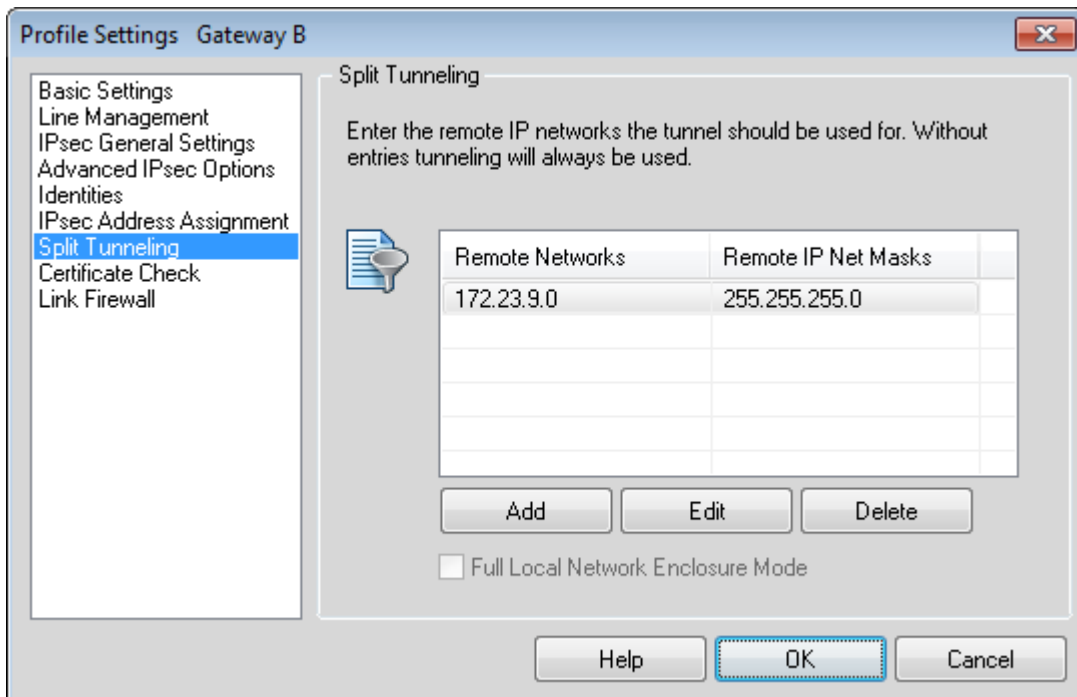


figure 1.3.17: Profile Settings: Split Tunneling

Add the remote address (depending on the subnet masks defined, these can be individual host[s] or network segment[s] that are to be reached. This is used in the Phase 2 negotiation(s) and often the cause for configuration mistakes depending on the gateway used. In this scenario, Gateway B's LAN segment, **172.23.9.0/24** (or netmask **255.255.255.0**) is to be reached, so that can be added here as shown above.

Skip **Certificate Check**, because this scenario does not call for the use of certificates (this will be covered in section 2.0), select the **Link Firewall** instead...

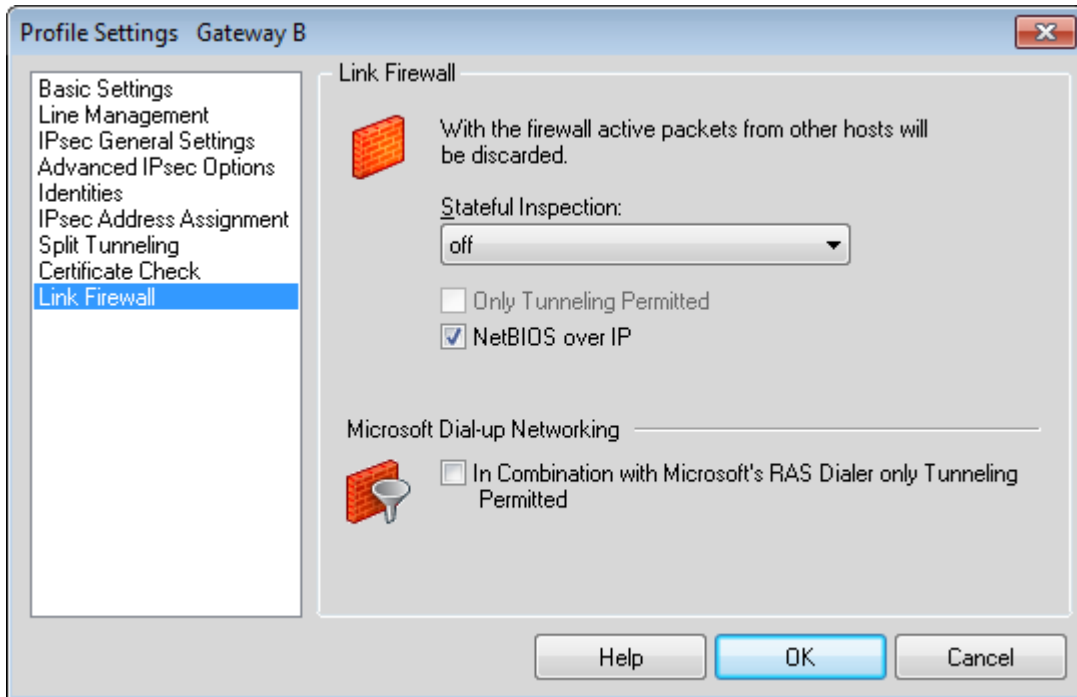


figure 1.3.18: Profile Settings: Link Firewall

Confirm the settings here as entered in figure 1.2.9. Click on **OK** to return to the main **Profile Settings** dialog box.

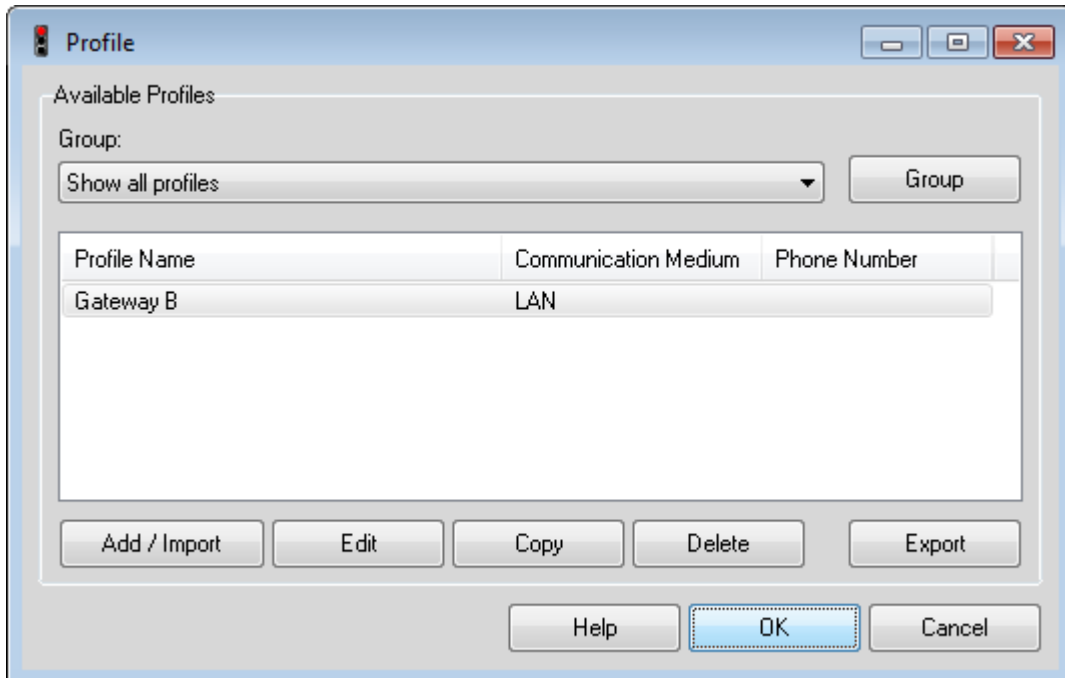


figure 1.3.19: Profile Settings

Select **OK** to return to the monitor (the graphical user interface of the VPN Client)

1.4 Establishing the connection

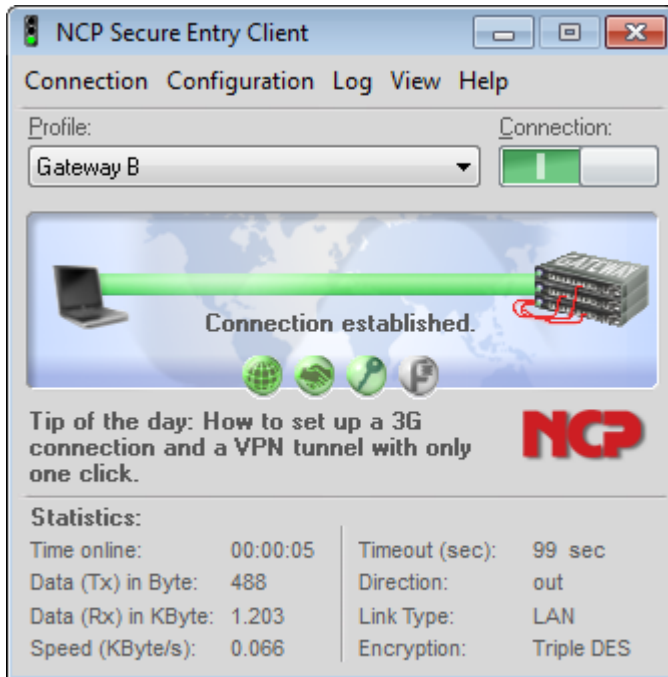


figure 1.4.1: NCP Secure Entry Client Monitor

Seeing as the connection is set to be established manually, click on the **Connection** slider to initiate the tunnel. A successful connection is shown in the screen shot above. Then open a 'dos' box, and ping the internal network interface of the VPN Gateway to confirm the connection has been successfully established. Depending on the VPN Gateway's configuration other hosts on the Gateway B's internal LAN can be reached.

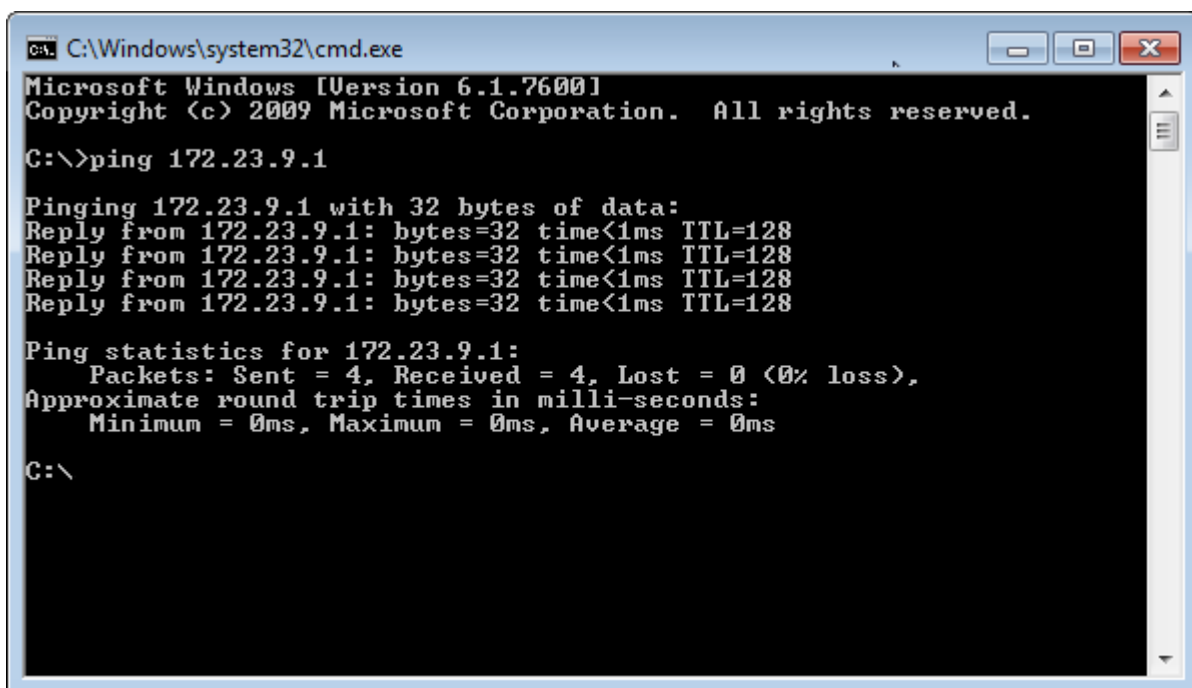


figure 1.4.2: Command Prompt: Ping response

2. Scenario 2: Client-to-gateway with certificates

2.1. Scenario Setup

The following is a typical client-to-gateway VPN that uses PKIX certificates for authentication.

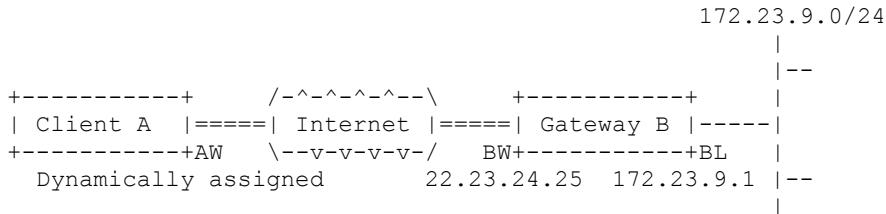


Figure 2.1.1: Scenario

Client A's WAN interface (AW) has the address dynamically assigned to it by the ISP. Client A will access Gateway B's internal LAN, by means of a secure tunnel.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Client A.

The **IKE Phase 1 parameters** used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- Authentication with signatures authenticated by PKIX certificates; both Client A and Gateway B have end-entity certificates that chain to a root authority called "Trusted Root CA"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying

Selectors for all IP protocols, all ports, between the client and 172.23.9.0/24, using IPv4 subnets

2.2 Installing the trusted CA certificate for Trusted Root CA

In this scenario, the client requires two certificates: one of the Certification Authority (CA) that issued the certificates, known in this example as the "Trusted Root CA" filename: **CERT_Trusted_Root_CA.pem**, and a client certificate referred to as **ClientA** (see section 2.3). Copy the **CERT_Trusted_Root_CA.pem** file into the **CaCerts** subdirectory within the **ncple** directory. Any CA certificates placed here can be then set to be trusted; please refer to the manual for more details.

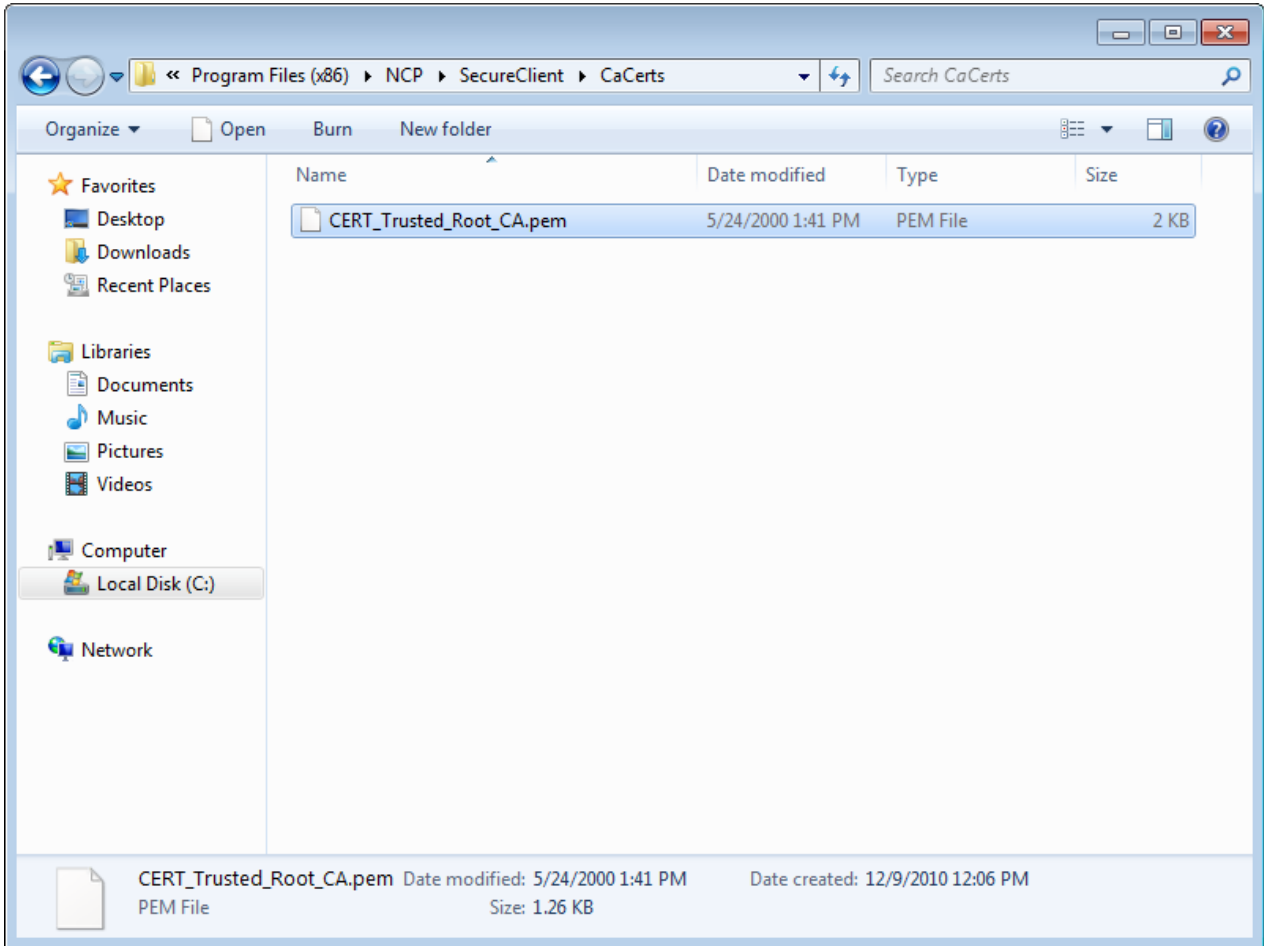


figure 2.2.1: Placing the Certificate .PEM in %PROGRAMFILES(x86)%\NCP\SecureClient\CaCerts folder

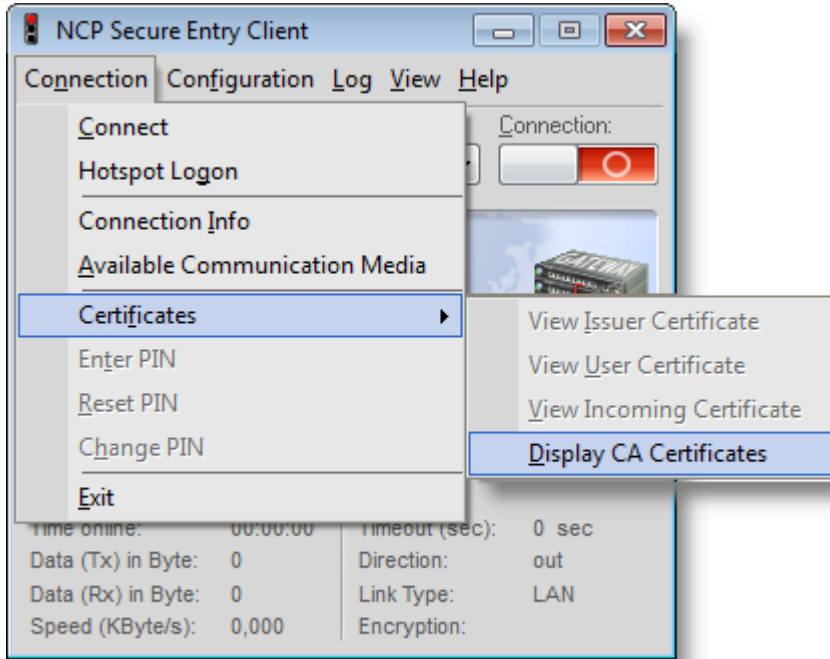


figure 2.2.2: Connection -> Certificates -> Display CA Certificates

You can view and verify the certificate by going to **Connection->Certificates->Display CA Certificates**.

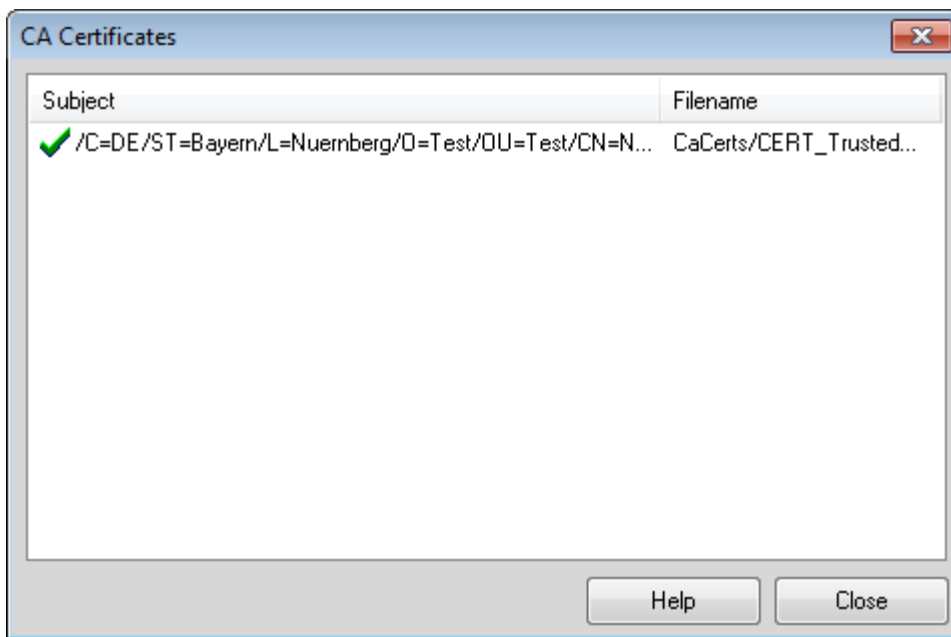


figure 2.2.3: Verify CA Certificates

The green tick denotes that this Certification Authority is to be trusted.

2.3 Installing new user certificate

In the same way, place the certificate to be used to authenticate the client in a FOLDER where it can easily be found. For the sake of this quick configuration guide, so-called soft-certificates are used. These are encrypted files containing the user's private- and public-keys. These keys could optionally, to obtain a higher security level be generated and stored exclusively on external devices such as smart cards or USB cryptographic devices. These then can be accessed using the PKCS#11 interface that comes with the Secure Client.

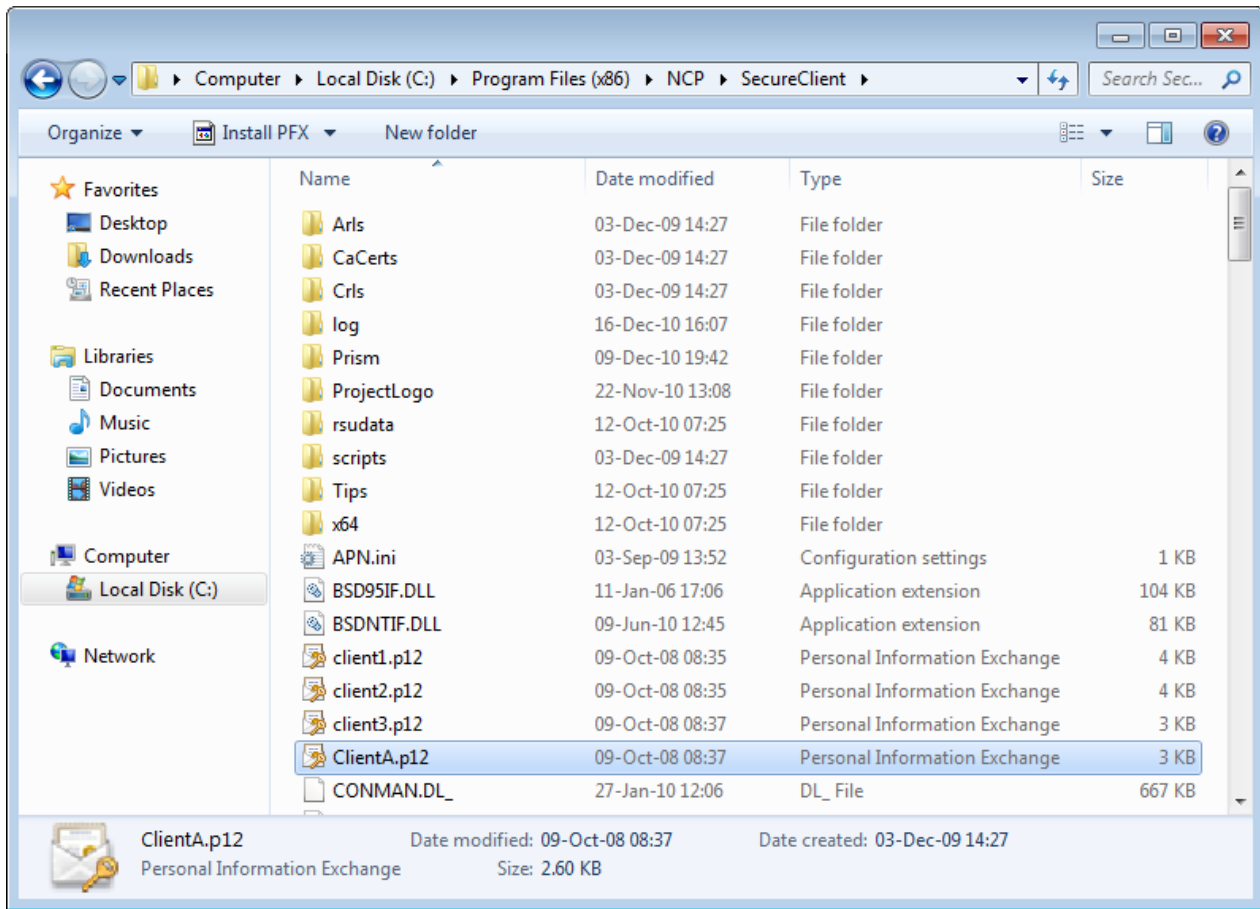


figure 2.3.1: Placing Client certificate

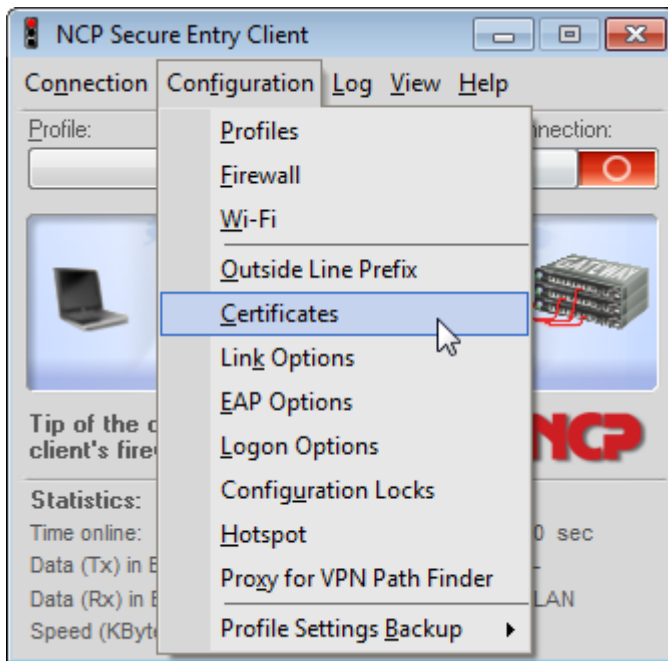


figure 2.3.2: Defining the certificate to use: Configuration -> Certificates...

Next step is to define which and where the certificate is to be located. We first have to create a so-called *Certificate Profile*, which contains the 'pointer' to the certificate. *Connection Profiles* can have individual *Certificate Profiles* assigned to them.

Configuration -> **Certificates** brings up the following dialog box:

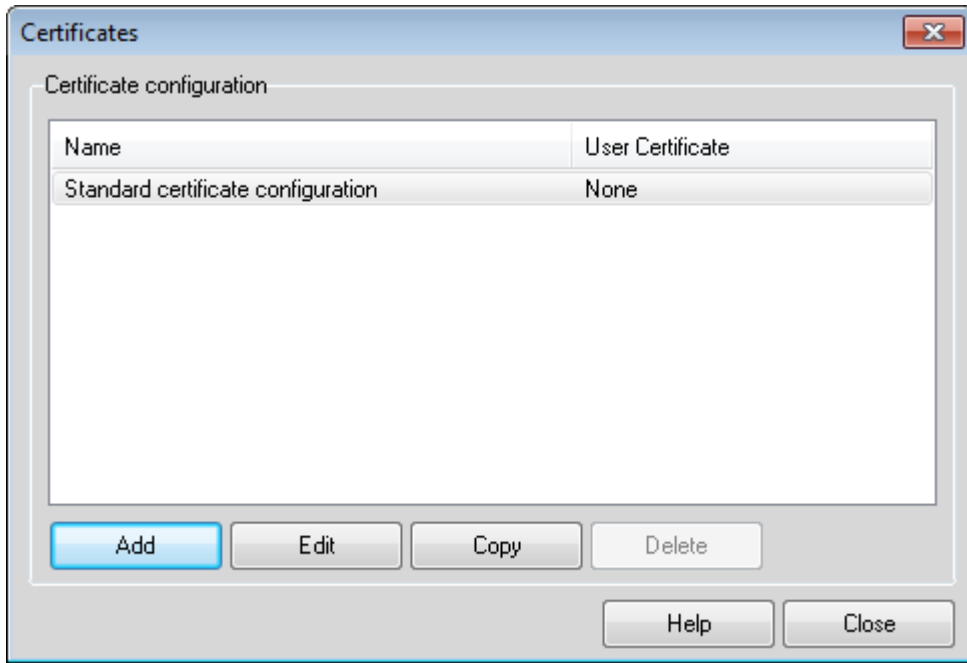


figure 2.3.3: Defining the user's certificate

Click **Add** to create a certificate profile as shown below.

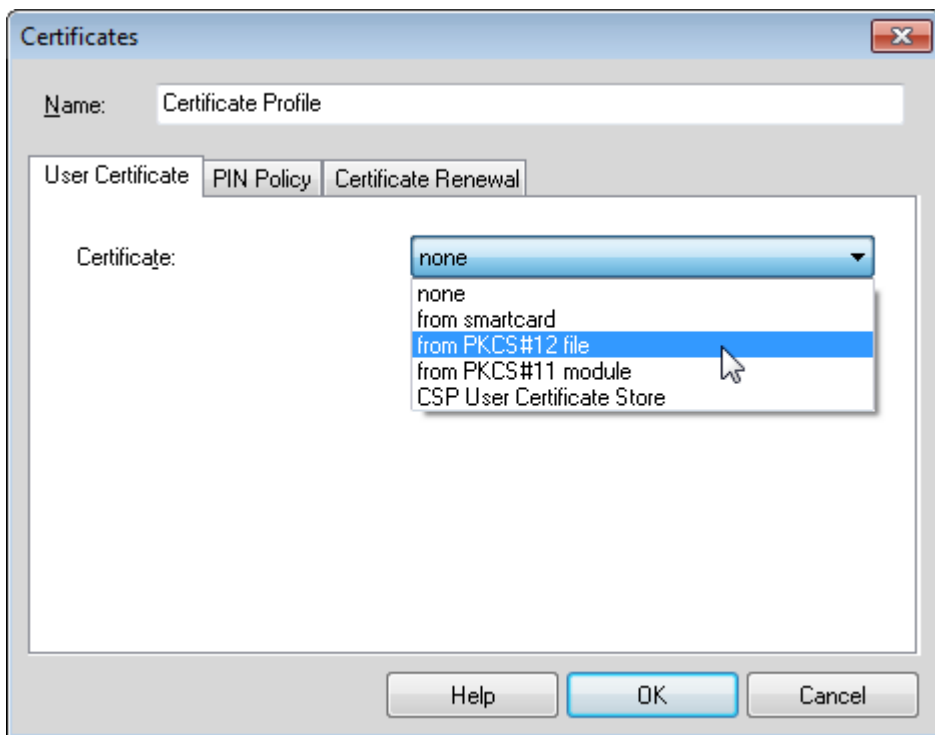


figure 2.3.4: Defining the (soft) user certificate to use

Select **from PKCS#12 File**, to set the use of 'soft certificates'. Then the appropriate path and file name are to be filled in where the certificate is located.

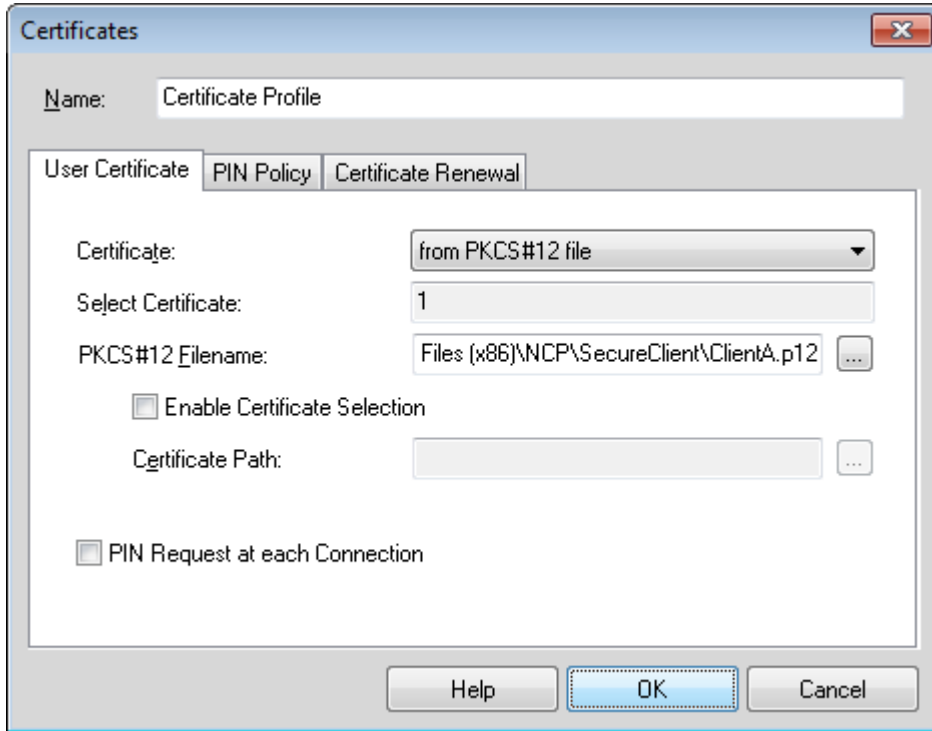


figure 2.3.5: Defining the user's certificate

We've now configured a certificate profile. Next step is to define a connection profile which will refer to this certificate profile.

2.4 Using the Profile Wizard

You can either use the wizard as outlined in this section (and similar to section 1.2), or modify an existing profile as in section 2.5.

Click **Add / Import** to create a configuration / connection profile from scratch using a wizard.

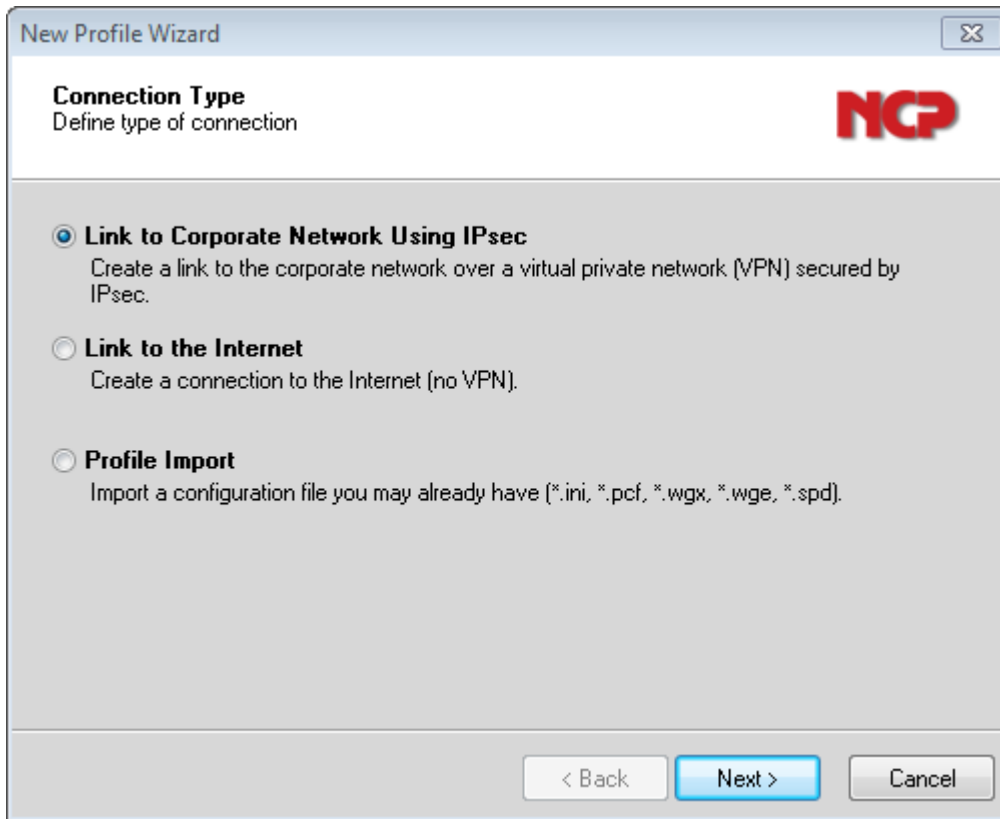


figure 2.4.1: New Profile Wizard: Connection Type

Select **Link to Corporate Network using IPsec** to create a profile with the parameters needed to establish a connection to the VPN Gateway **Gateway B** as illustrated in Figure 1.1.1. Click **Next >**.

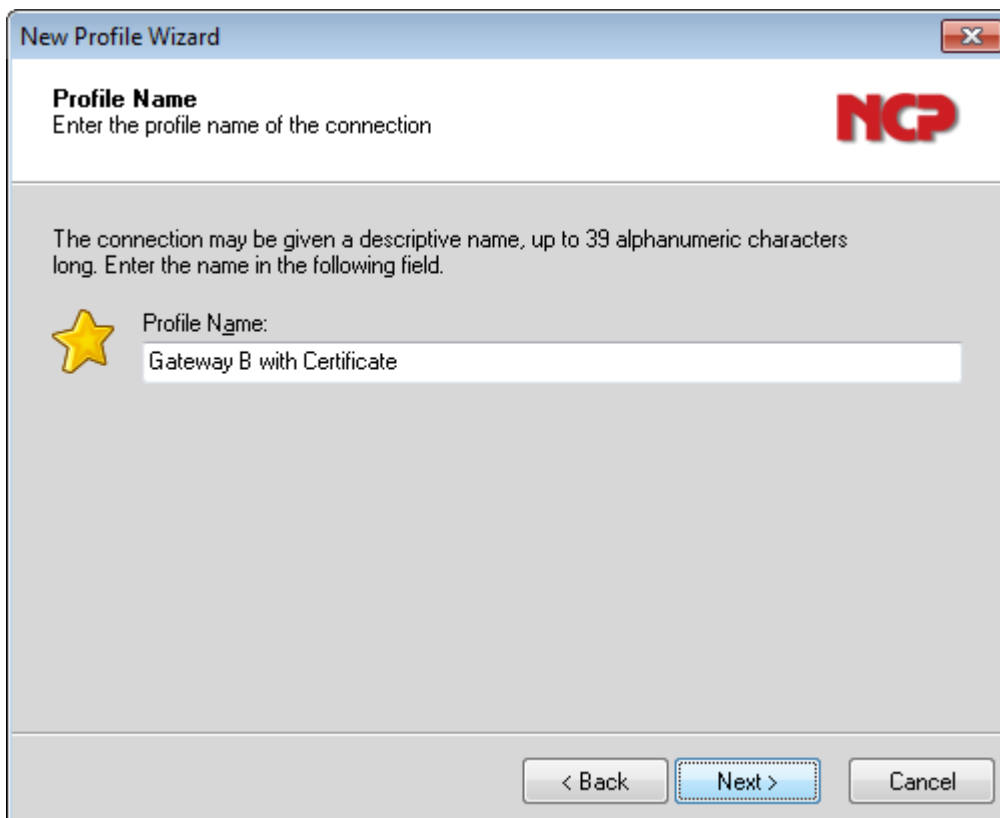


figure 2.4.2: New Profile Wizard: Profile Name

Several profiles can be created and each given different name. In this example, this profile is created and given the name **Gateway B with Certificate**.

Click **Next >**.

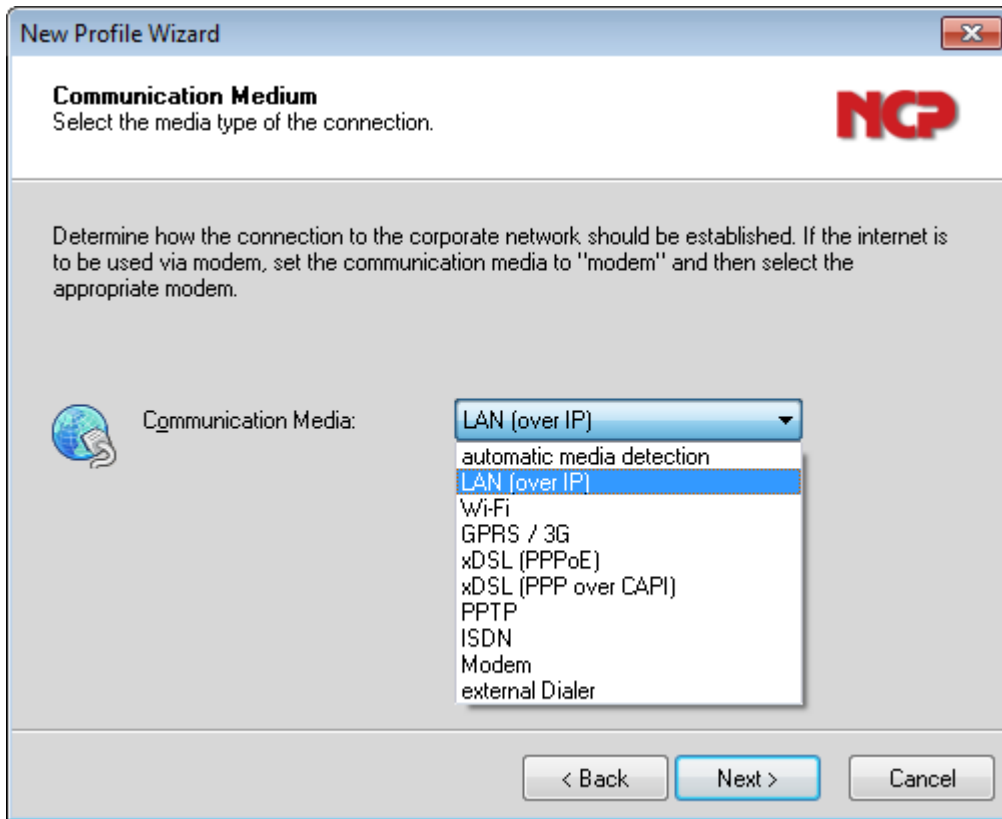


figure 2.4.3: New Profile Wizard: Communication Media

The NCP Secure Entry Client supports different media types; the integrated dialer for example, can be used to establish a connection to the ISP with a modem (if available to the system) prior to building the VPN Tunnel. In this example, select **LAN (over IP)**.

Click **Next >**.



New Profile Wizard


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.

 **G**ateway (Tunnel Endpoint):
22.23.24.25

Extended Authentication (XAUTH)

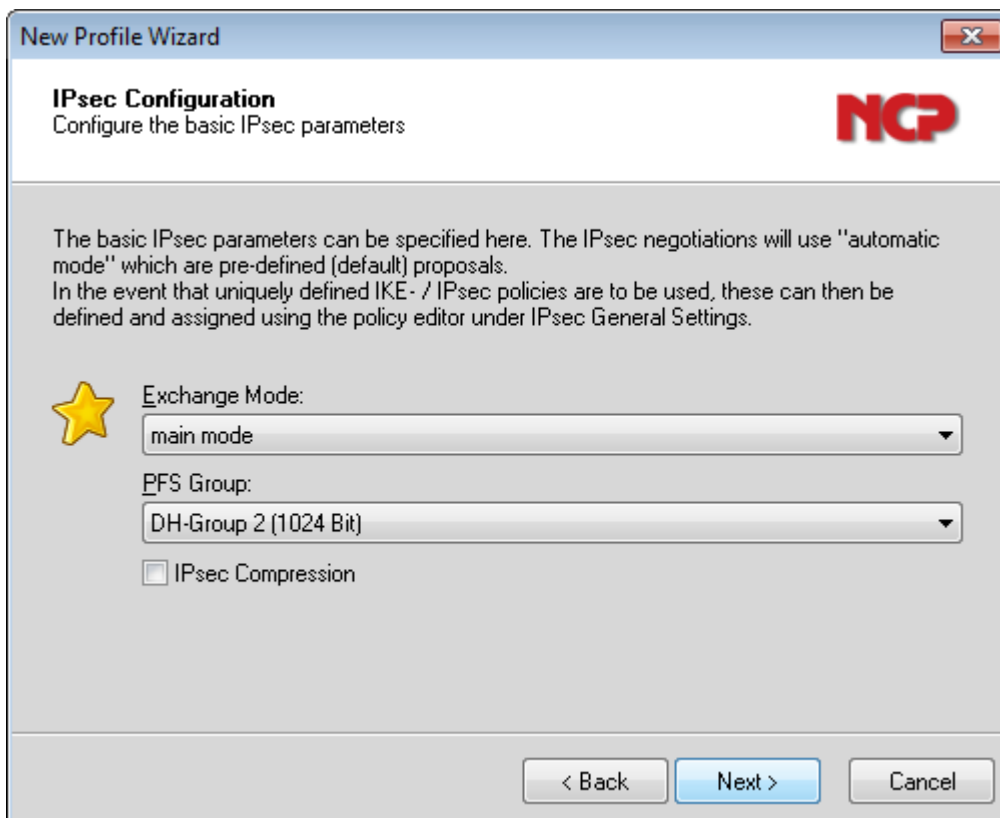
 **U**ser ID:

Password: _____ **P**assword (confirm): _____

< Back Next > Cancel

figure 2.4.4: New Profile Wizard: VPN Gateway Parameters

Enter in the gateway's IP address or DNS name. (If the VPN Gateway supports extended authentication (XAUTH) then enter in the appropriate **Username** and **Password**.) Click **Next >**.




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.

 **E**xchange Mode:
main mode

PFS Group:
DH-Group 2 (1024 Bit)

IPsec Compression

< Back Next > Cancel

figure 2.4.5: New Profile Wizard: IPsec Configuration

This example will use **main mode** and **Perfect Forward Secrecy** seamless re-keying, employing **DH-Group2 (1024 Bit)** as indicated in section 1.0. Click **Next >**.

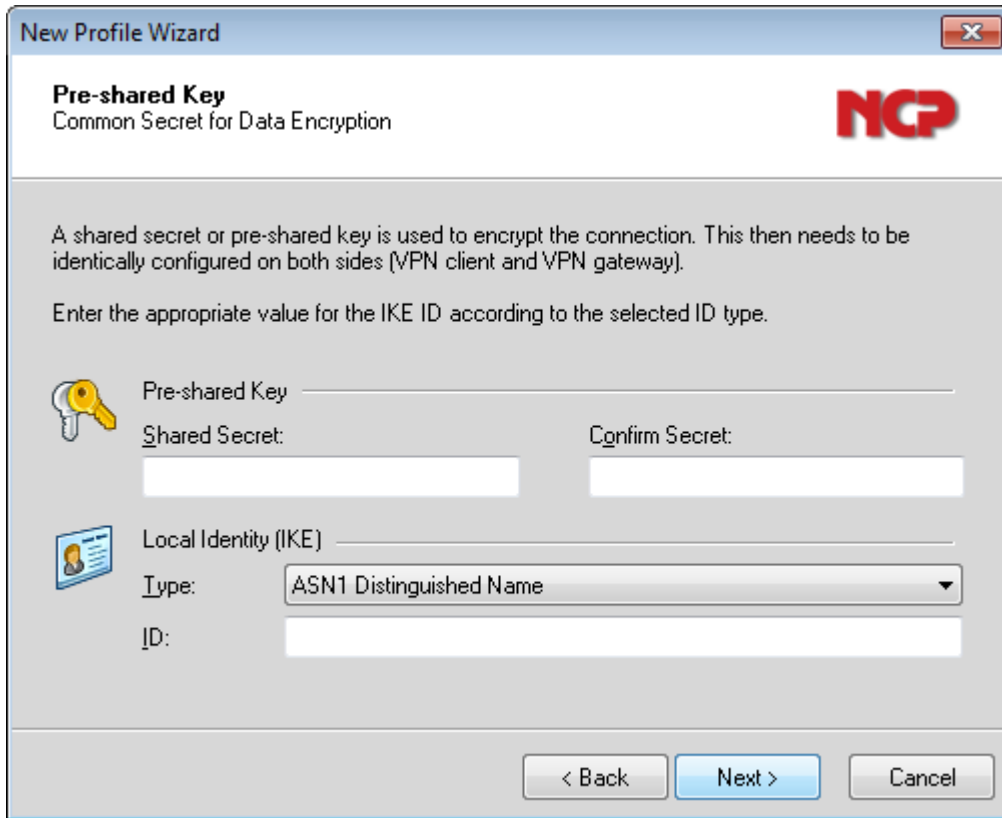


figure 2.4.6: New Profile Wizard: Pre-shared Keys / Local Identity

In this scenario, a certificate is used. The **ASN1 Distinguished Name** can be taken from the certificate (see section 2.1) as shown in the above example.

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:
172.23.9.10

DNS / WINS Servers

DNS Server: 172.23.9.250 WINS Server: 0.0.0.0

< Back Next > Cancel

figure 2.4.7: New Profile Wizard: IPsec Configuration – IP addresses

In this example the VPN Gateway will designate a virtual IP address to the incoming VPN connection. The NCP Secure Entry client supports three options, manual IP address assignment, IKE-Config Mode, or using the IP address assigned to the physical network interface ("AW": see figure 1.1.1). In this example, one assumes that the IP address and the appropriate subnet mask is manually assigned to the client.

Click **Next >** to continue.

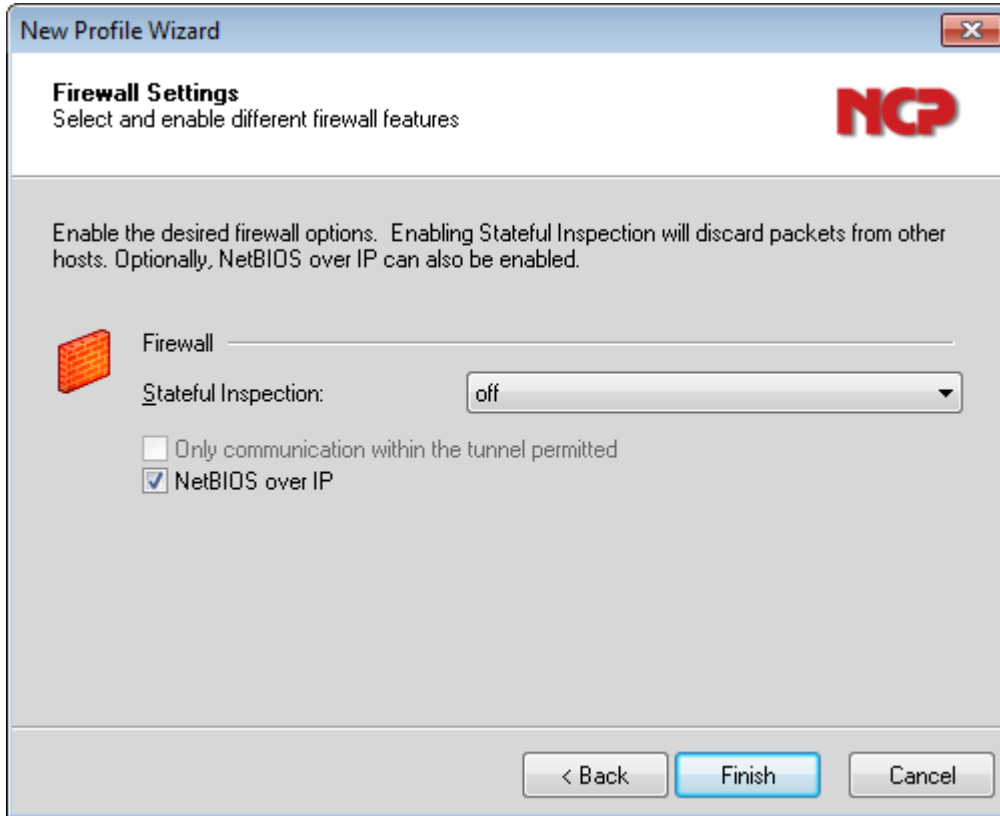


figure 2.4.8: New Profile Wizard: Firewall settings

Stateful inspection can be enabled when this specific link has been selected to provide protection against attacks from i.e. the local LAN (this overrides settings from the personal firewall: see **Configuration | Firewall** settings for more details/configuration options). Click **Finish** to save the setting to this profile.

2.5 Checking/Modifying the Configuration

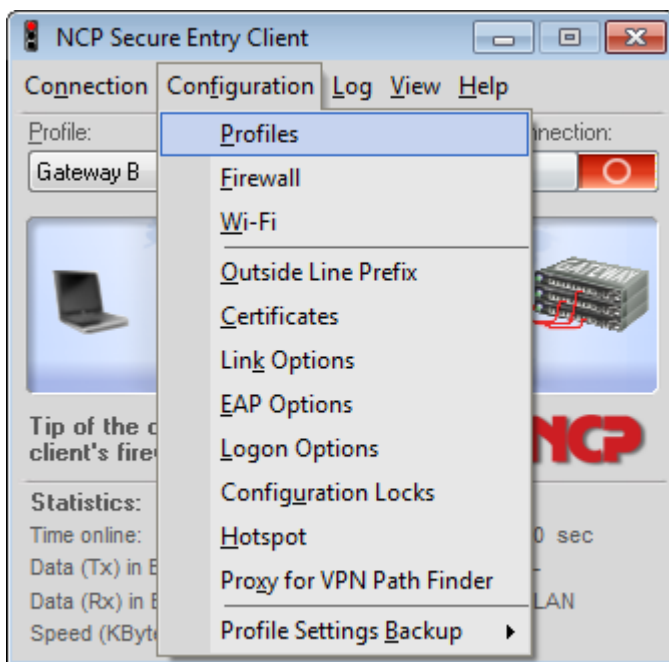


figure 2.5.1: Configuration -> Profiles

Open the **Profile** to modify the parameters to define the specific IKE and IPsec proposals as specified in section 2.1.

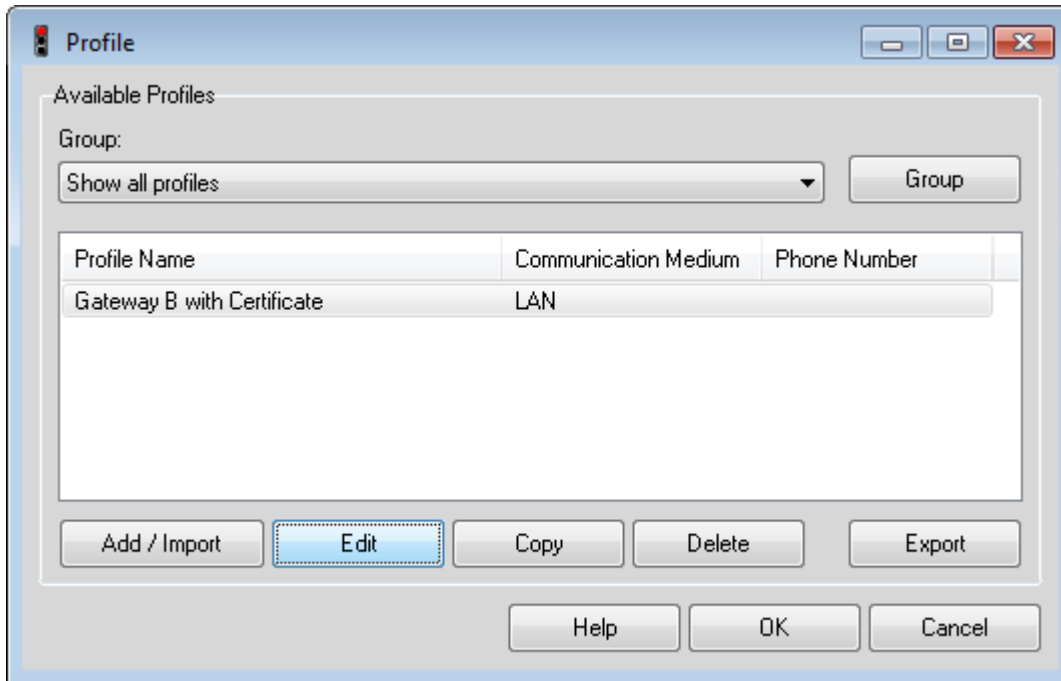


figure 2.5.2: Profile Settings

Either double click on the profile **Gateway B with Certificate** that is going to be modified, or select the profile and then click on **Edit**.

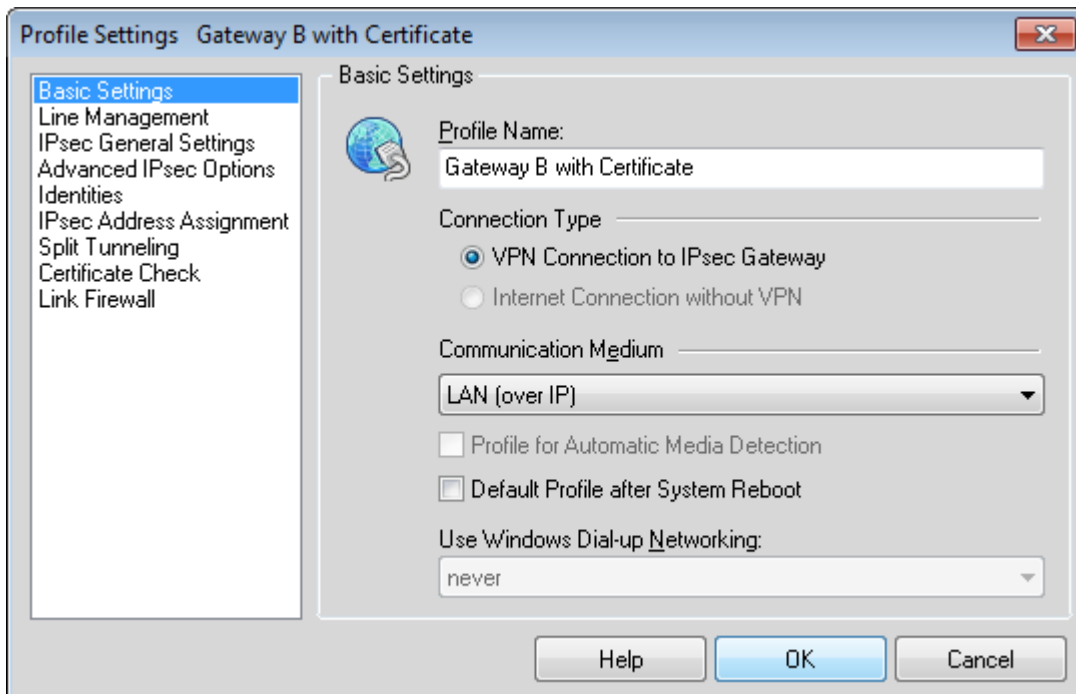


figure 2.5.3: Profile Settings: Basic Settings

Review the parameters and ensure they are correct. Select **Line Management** to continue...

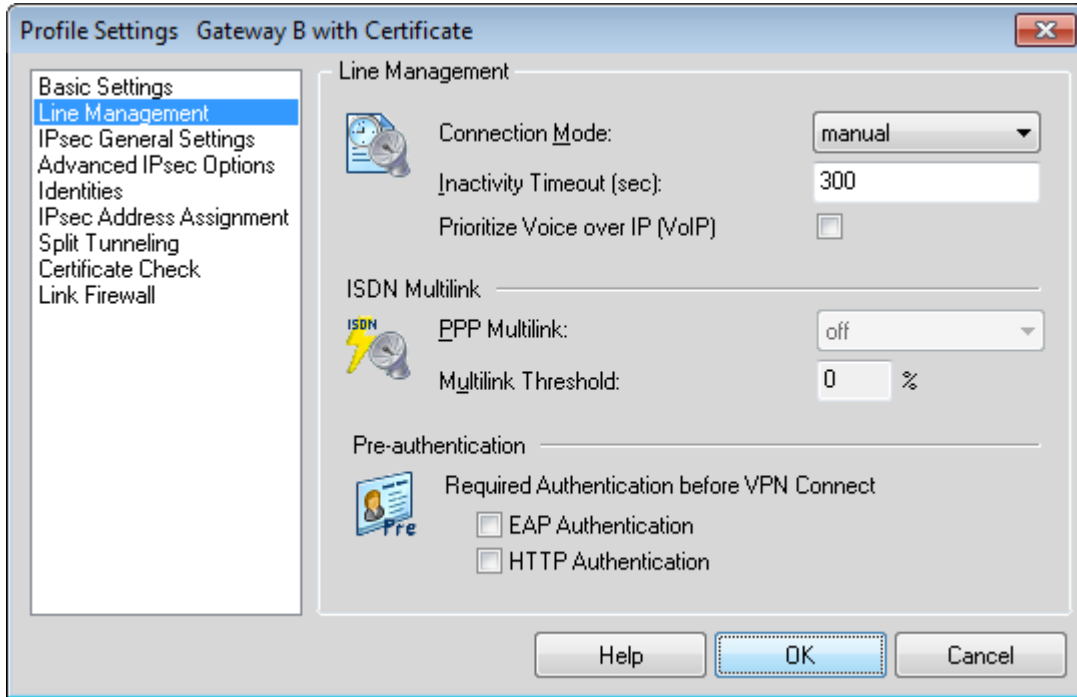


figure 2.5.4: Profile Settings: Line Management

The **Connection Mode** can be set to connect automatically, meaning that any time a packet is destined for Gateway B's LAN, the VPN Tunnel can automatically be established. In this example however, one manually establishes the connection. The **Inactivity Timeout** is set to 300 seconds. Select **IPsec General Settings** to continue...

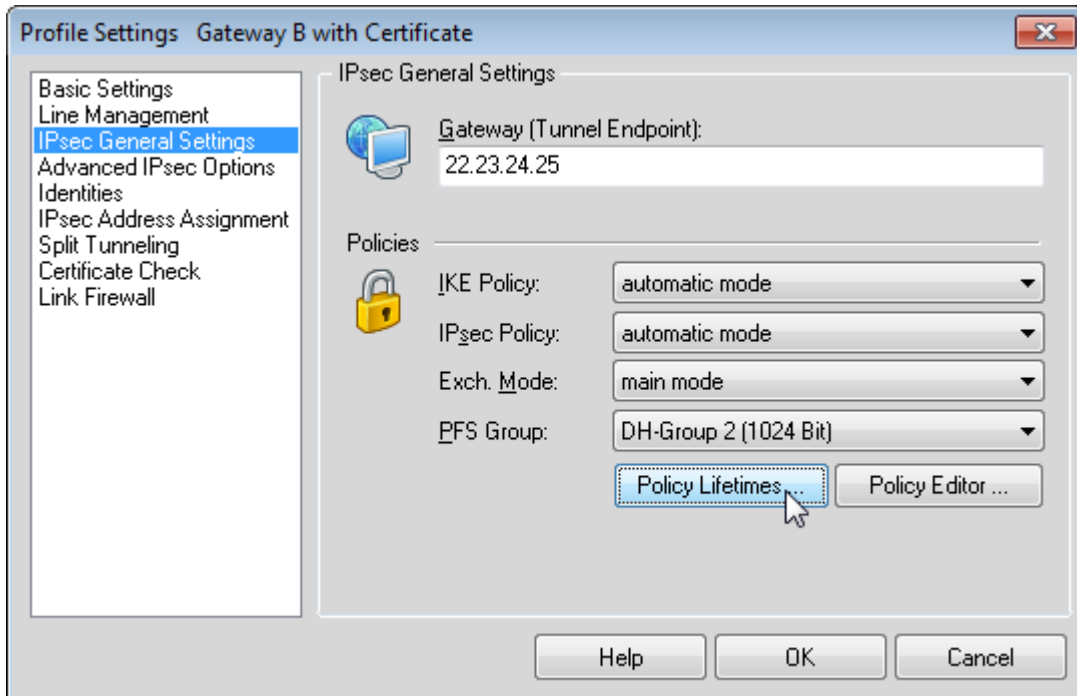


figure 2.5.5: Profile Settings: IPsec General Settings: Policy Lifetimes

When **automatic mode** is selected for both the **IKE** (Phase 1) and **IPsec** (Phase 2) **Policies**, the client will transmit a range of different commonly used proposals and the VPN Gateway can then select one to use for the connection. However, in this example, both the IKE and IPsec policies have been specifically defined in section 2.1; so select **Policy Lifetimes...**

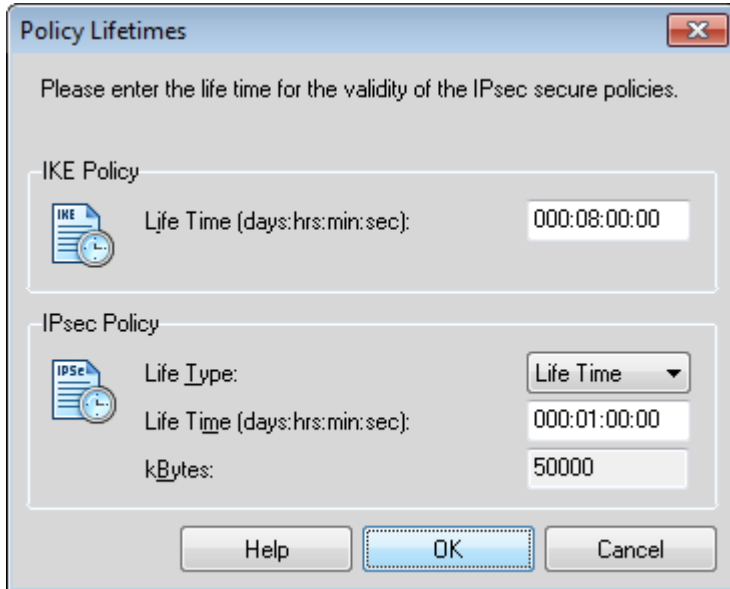


figure 2.5.6: Policy Lifetimes

The duration for the IKE Policy (SA lifetime) has been set to 8 hours (28800 seconds), and the IPsec Policy (SA) lifetime is limited to 1 hour (3600 seconds). Click **OK** to return to define the Proposals...

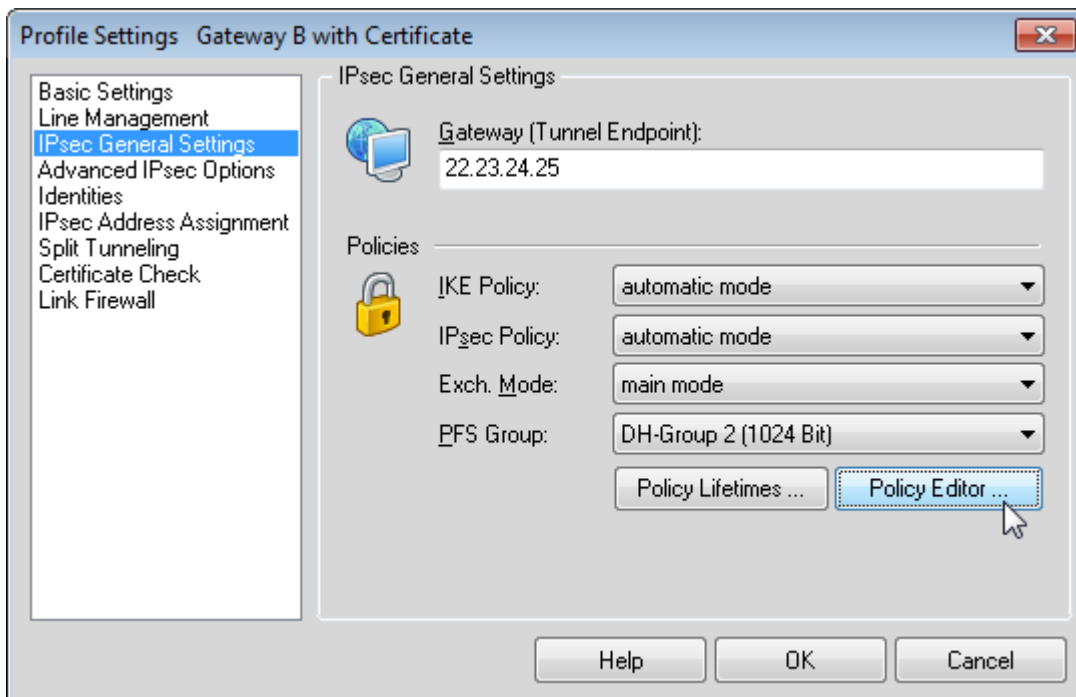


figure 2.5.7: Profile Settings: IPsec General Settings: Policy Editor

Select the **Policy Editor...** to define specific proposals to be used in this connection as lined out in section 2.1.

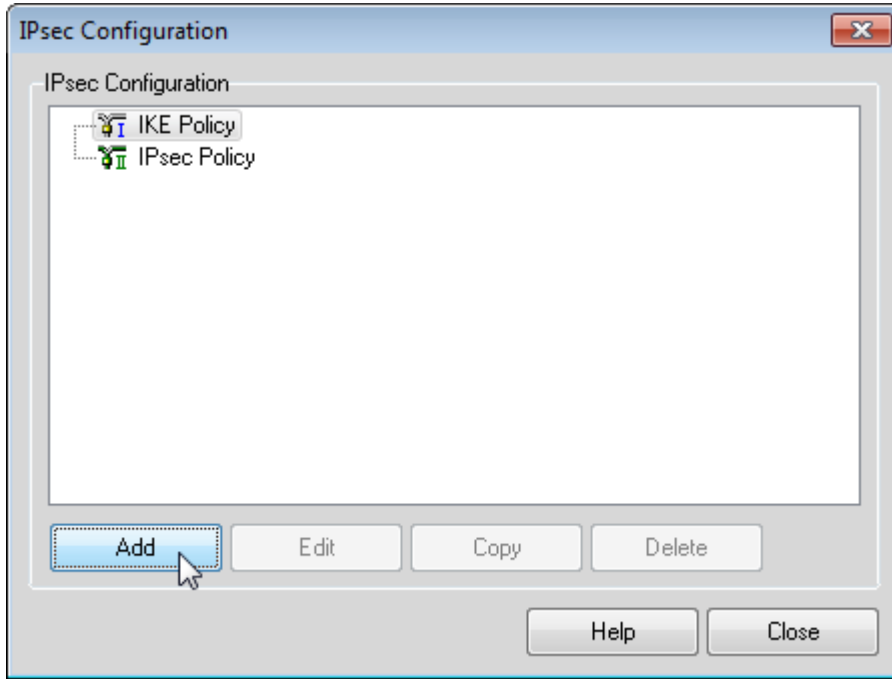


figure 2.5.8: Proposal Definitions: IKE Policy

First select **IKE Policy** and click on **Add** to define a new IKE Policy (Phase 1 parameters) to be used.

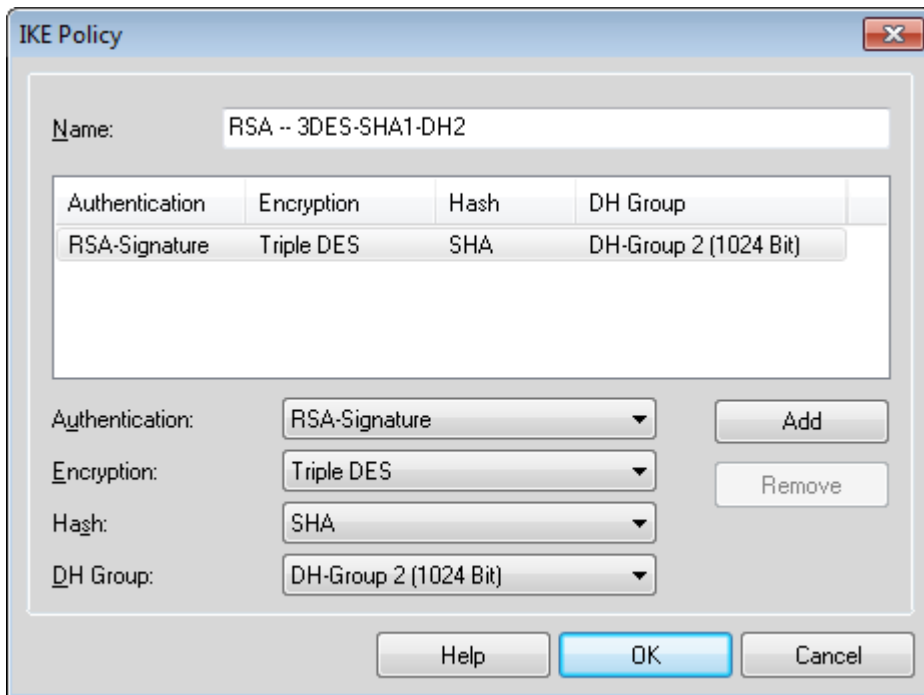


figure 2.5.9: Defining an IKE Policy

Simply select the parameters for this proposal. Several proposals may be grouped together under the name, but for the purpose of this example, only one proposal is defined. Select **RSA-Signature** for the IKE mode, **Triple DES** (168bit 3DES) for the encryption algorithm to be used, **SHA** (160bit SHA-1) for the authentication algorithm, and finally **DH-Group 2 (1024 Bit)** for the key exchange protocol.

Click **OK** to return to the previous dialog box.

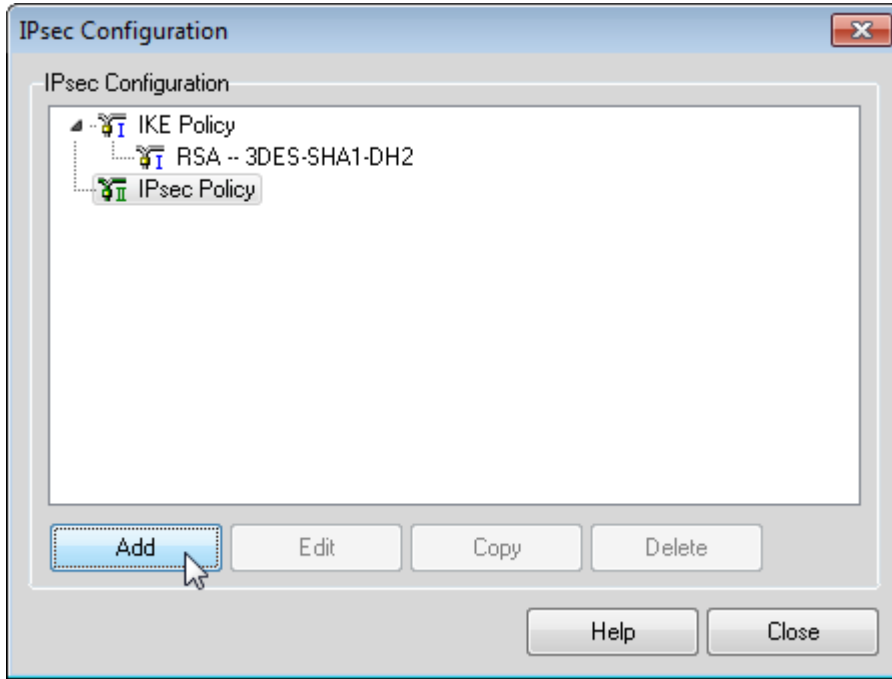


figure 2.5.10: Proposal Definitions: IPsec Policy

In the same way, select **IPsec Policy** and click on **Add** to define the IPsec proposal (Phase 2 parameters).

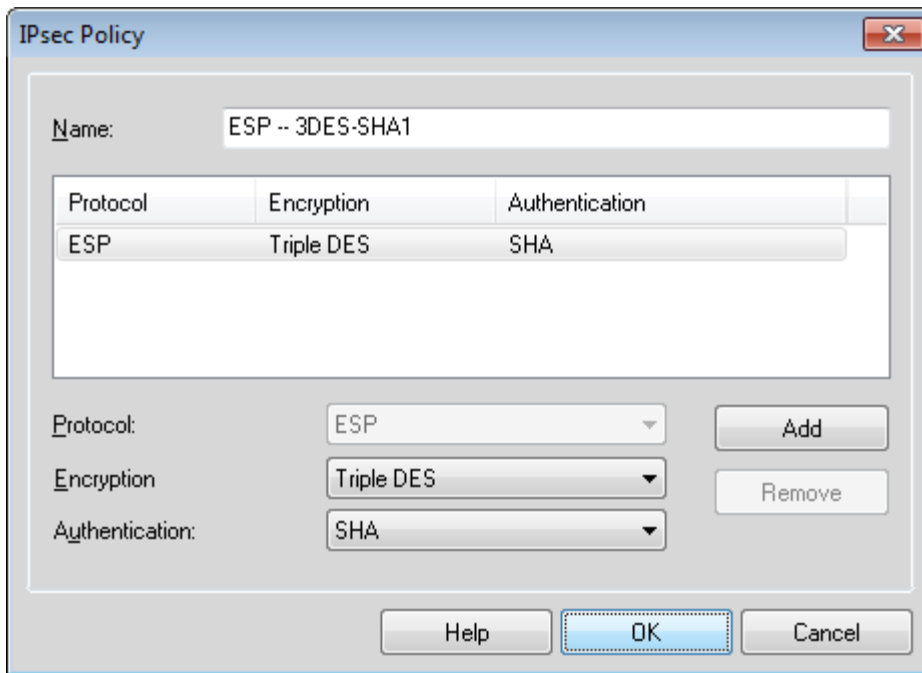


figure 2.5.11: Defining an IPsec Policy

Simply select the parameters for this policy: **ESP** tunnel mode, **Triple DES** (168bit 3DES-CBC) for encryption algorithm and **SHA** (SHA-1 160 Bit) for the authentication code/hash algorithm.

Click **OK** to continue...

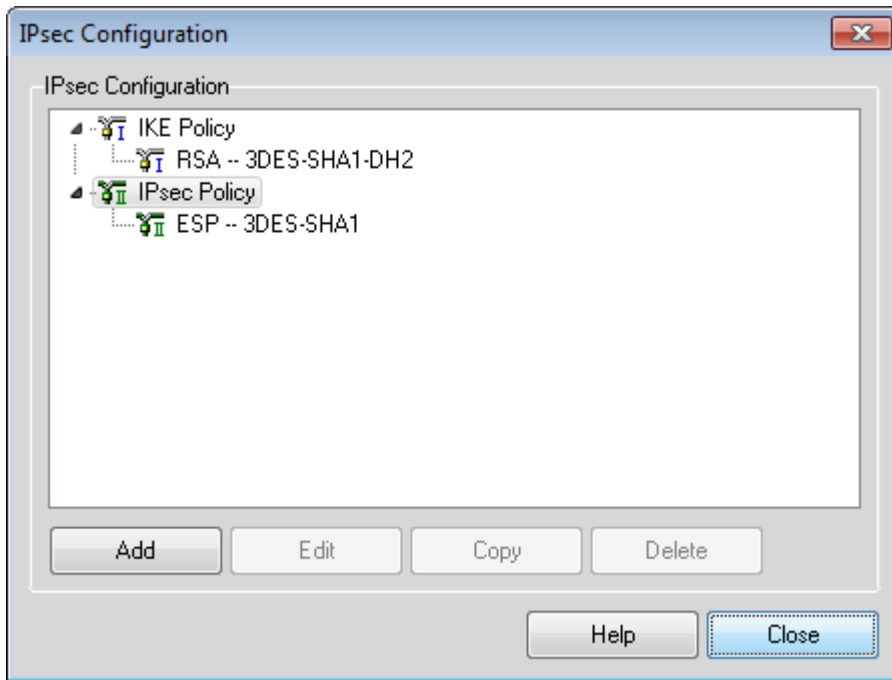


figure 2.5.12: IPsec/IKE (ISAKMP) parameters defined

Click on **Close** to save the proposals created, and return to the **Profile Settings | IPsec General Settings** dialog box.

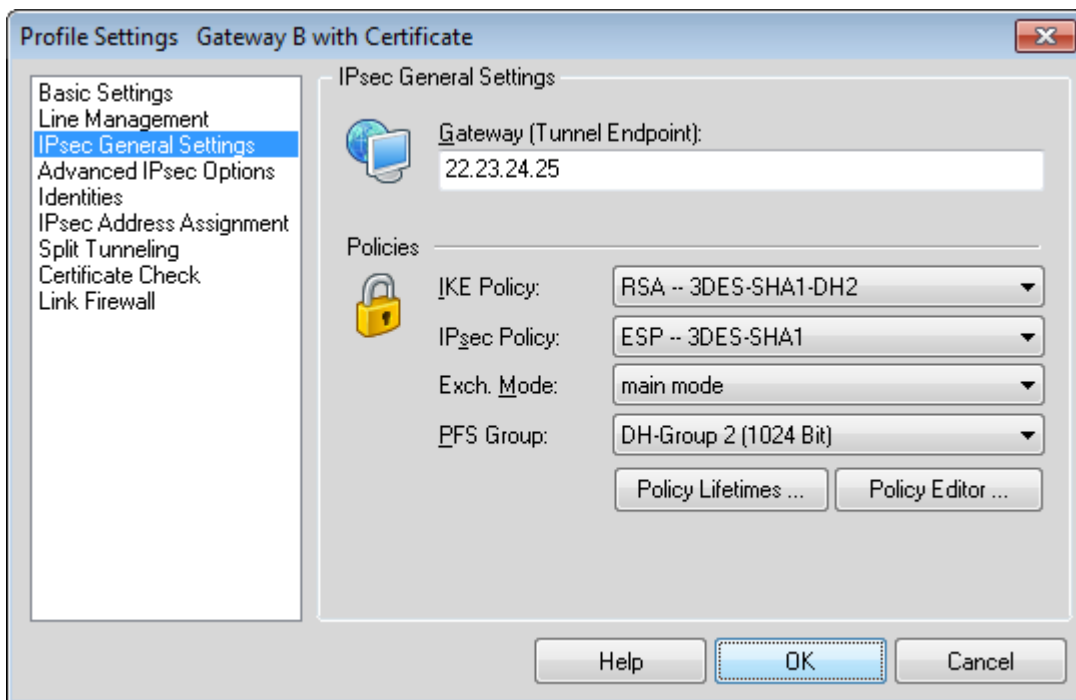


figure 2.5.13: Profile Settings: IPsec General Settings, Policy Definitions

Select the newly defined **IKE-** (ISAKMP) "**RSA – 3DES-SHA1-DH2**" and **IPsec-** "**ESP – 3DES-SHA1**" **Policies** from the dropdown list to apply the **IKE-** and **IPsec Policy** as shown above, and click on **Advanced IPsec Options** to move to the next dialog box.

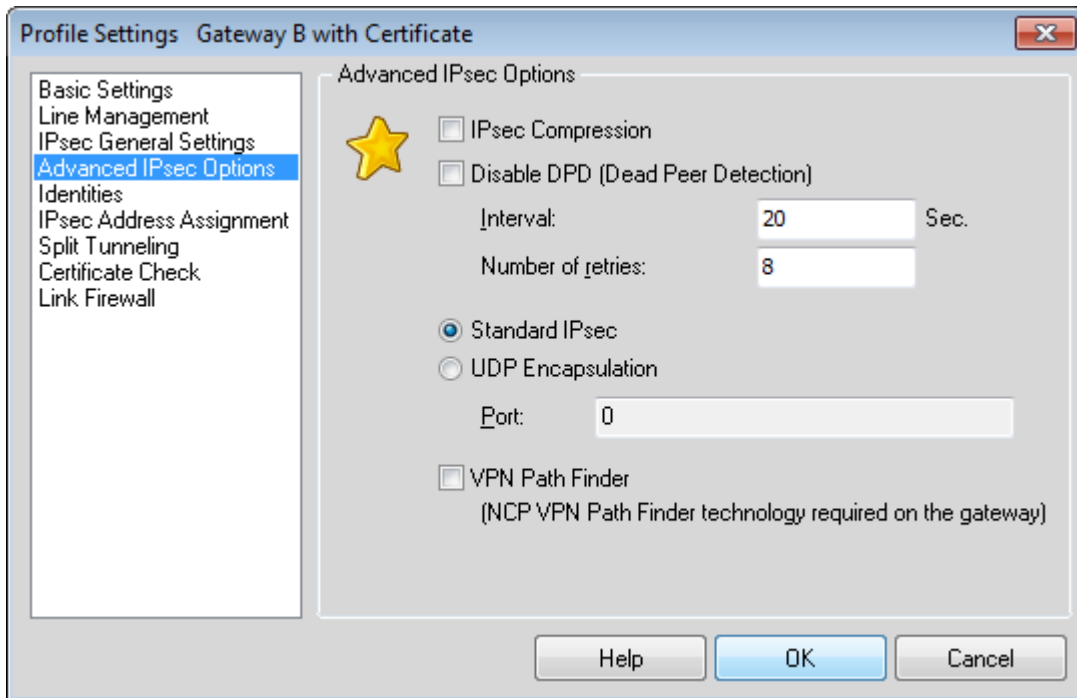


figure 2.5.14: Profile Settings: IPsec Advanced IPsec Options

Ensure that **Standard IPsec** is selected here (other options available here are beyond the scope of this quick configuration guide).

Then click on **Identities** to move to the next dialog box.

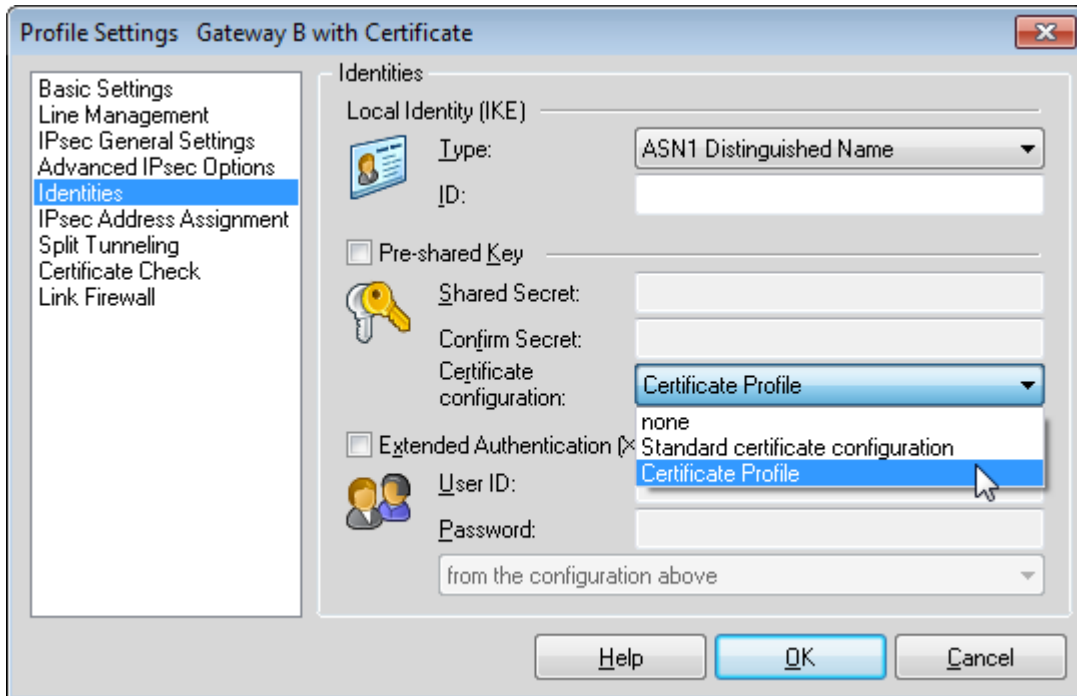


figure 2.5.15: Profile Settings: Identities

In this scenario, the IKE-ID type is taken from the certificate, in the form of the **ASN1 Distinguished Name**. Other IKE-ID types can be used, but are beyond the scope of this document; please refer to the manual for more details.

Remember to also select and apply the Certificate Profile created earlier which points to the certificate to be used for authentication purposes. Then click on **IP Address Assignment** to continue...

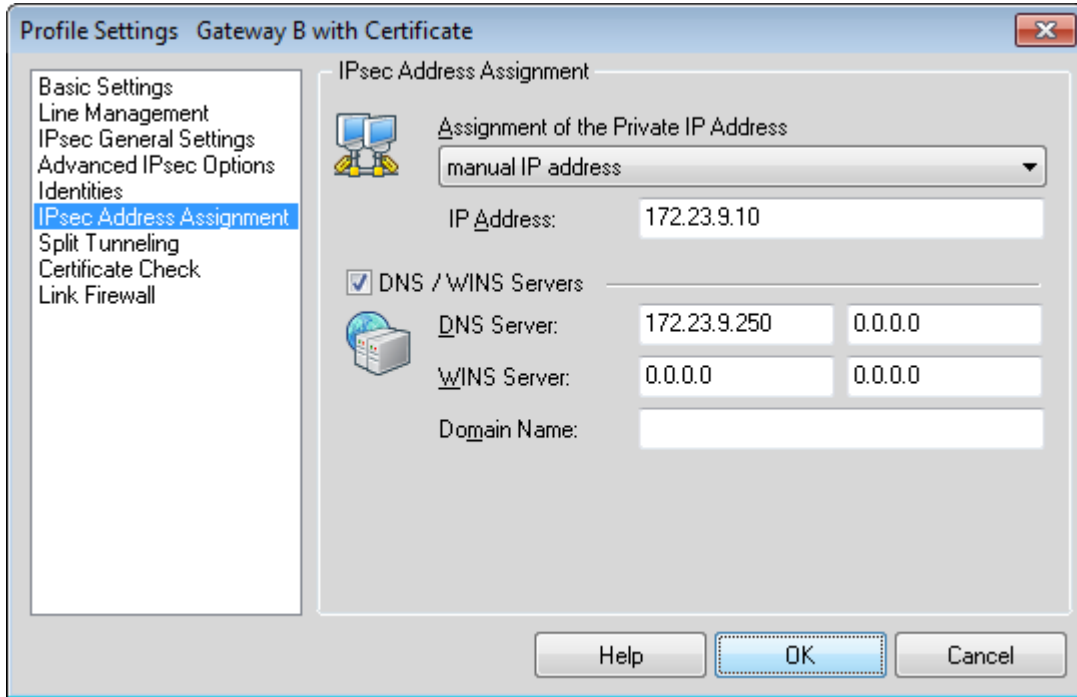


figure 2.5.16: Profile Settings: IPsec Address Assignment

Confirm the settings as entered in figure 1.2.8. Then click on **Split Tunneling** to move to the next dialog box.

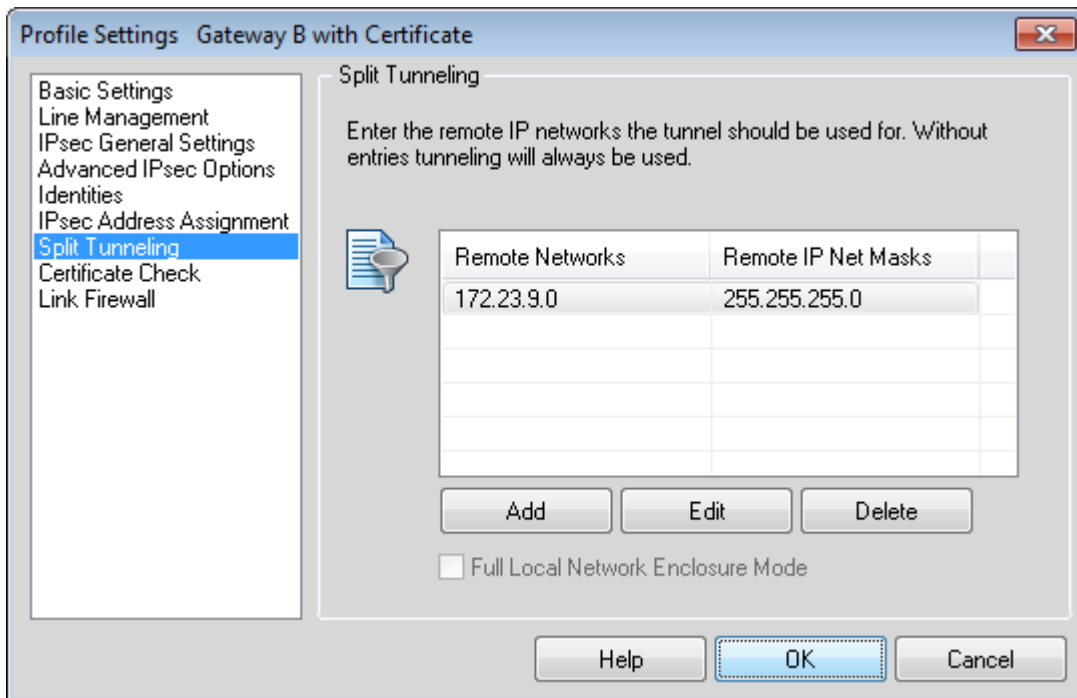


figure 2.5.17: Profile Settings: Split Tunneling

Add the remote address (depending on the subnet masks defined, these can be individual host[s] or network segment[s] that are to be reached. This is used in the Phase 2 negotiation(s) and often the cause for configuration mistakes depending on the gateway used. In this scenario, Gateway B's LAN segment, **172.23.9.0/24** (or netmask **255.255.255.0**) is to be reached, so that can be added here as shown above.

Click **Certificate Check** to continue...

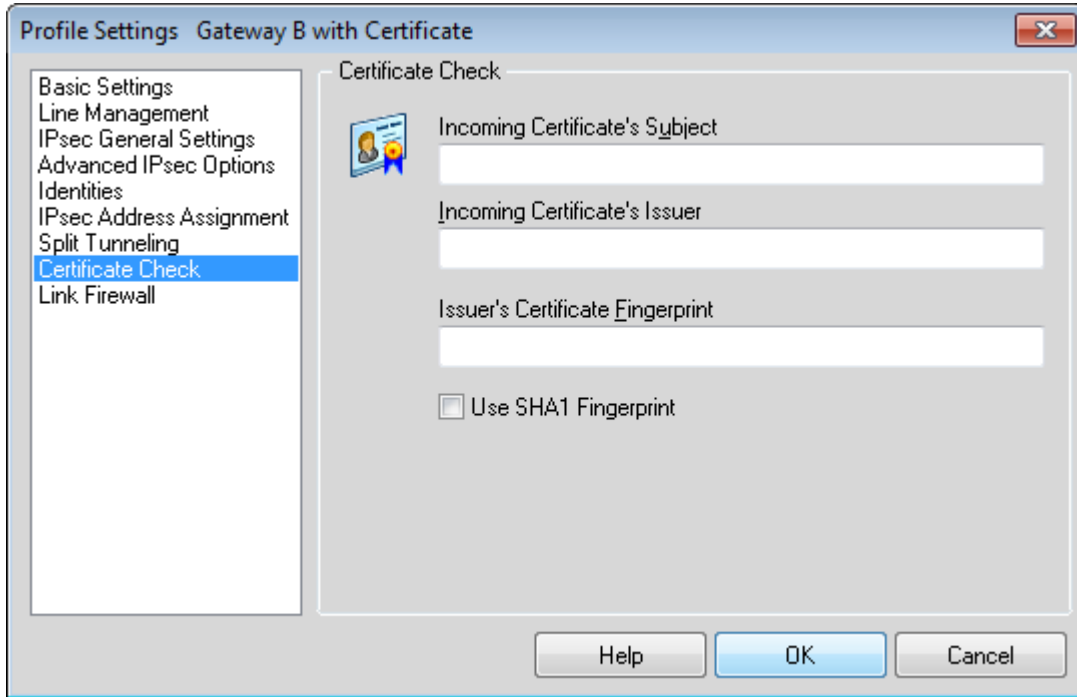


figure 2.5.18: Profile Settings: Certificate Check

Additional security can be applied by entering the appropriate values here that will then be compared to the values in the certificate presented by the VPN gateway. In other words, additional checks are done on the certificate that the Gateway B presents when establishing a connection. See the manual for more details.

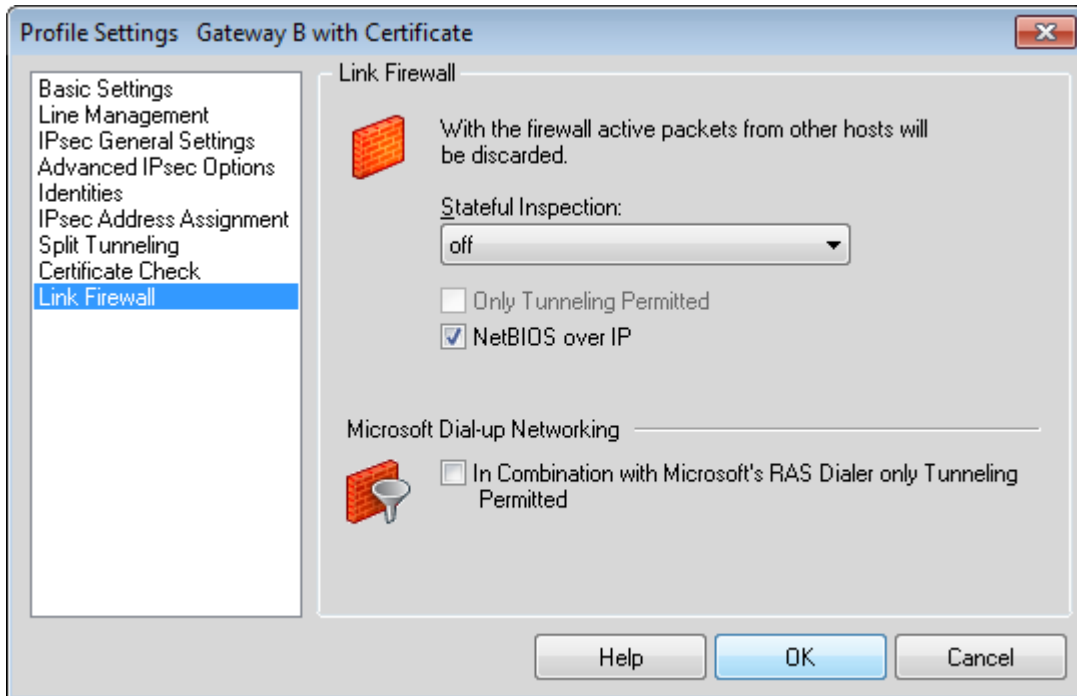


figure 2.5.19: Profile Settings: Link Firewall

Confirm the settings here as entered in figure 2.4.8. Click on **OK** to return to the main **Profile Settings** dialog box.

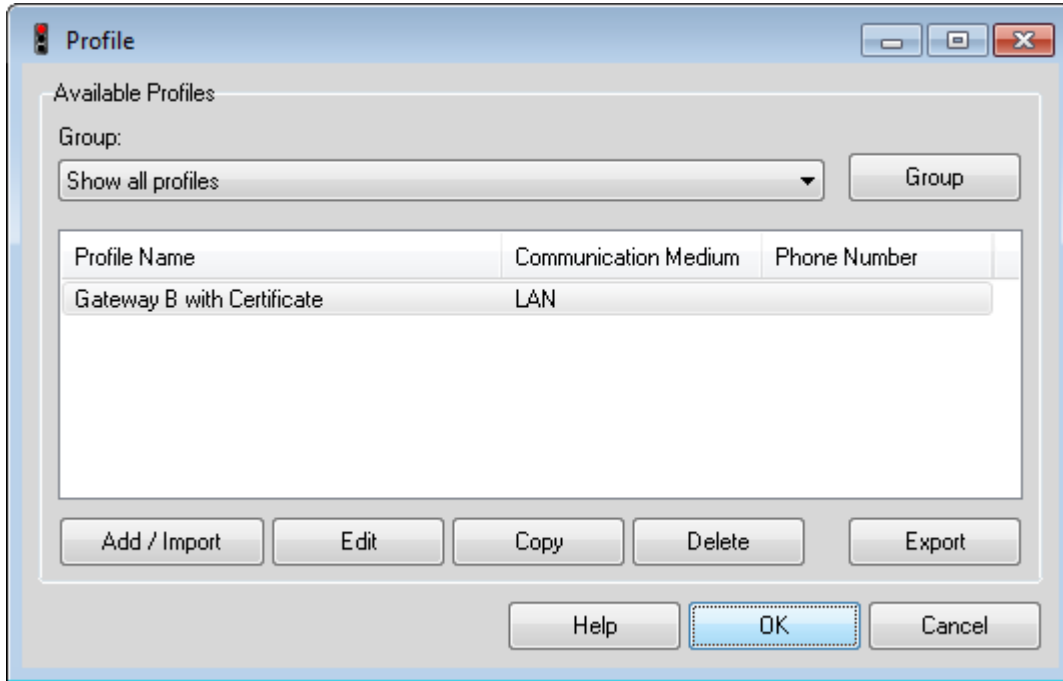


figure 2.5.20: Profile Settings

Select **OK** to return to the monitor (the graphical user interface of the VPN Client)

2.6 Establishing the connection



figure 2.6.1: Profile Secure Entry Client Monitor

Seeing as the connection is set to be established manually, click on the **Connection** slider to initiate the tunnel.

A certificate has been defined to be used to authenticate the user, so a dialog prompting for the PIN (passphrase) to enable the use of the private key within the PKCS#12 to be used will be shown. This is required to establish a connection.

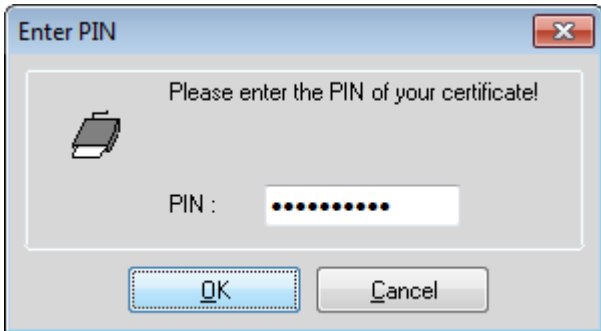


figure 2.6.2: Enter PIN

Enter the passphrase/PIN and then click on **OK** to continue...

The client will now proceed to build up the connection. When the connection has successfully been established, this is shown by the bar turning green and the different items denoting the different stages within the negotiation to create the tunnel are also green.

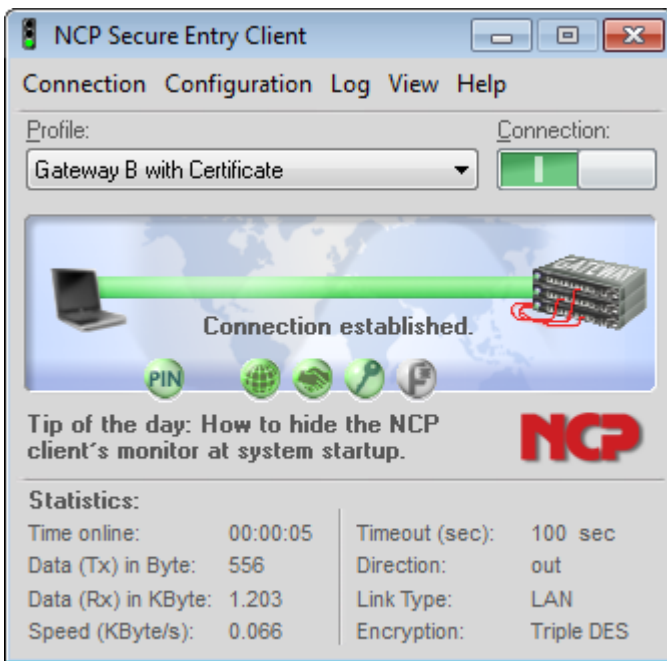
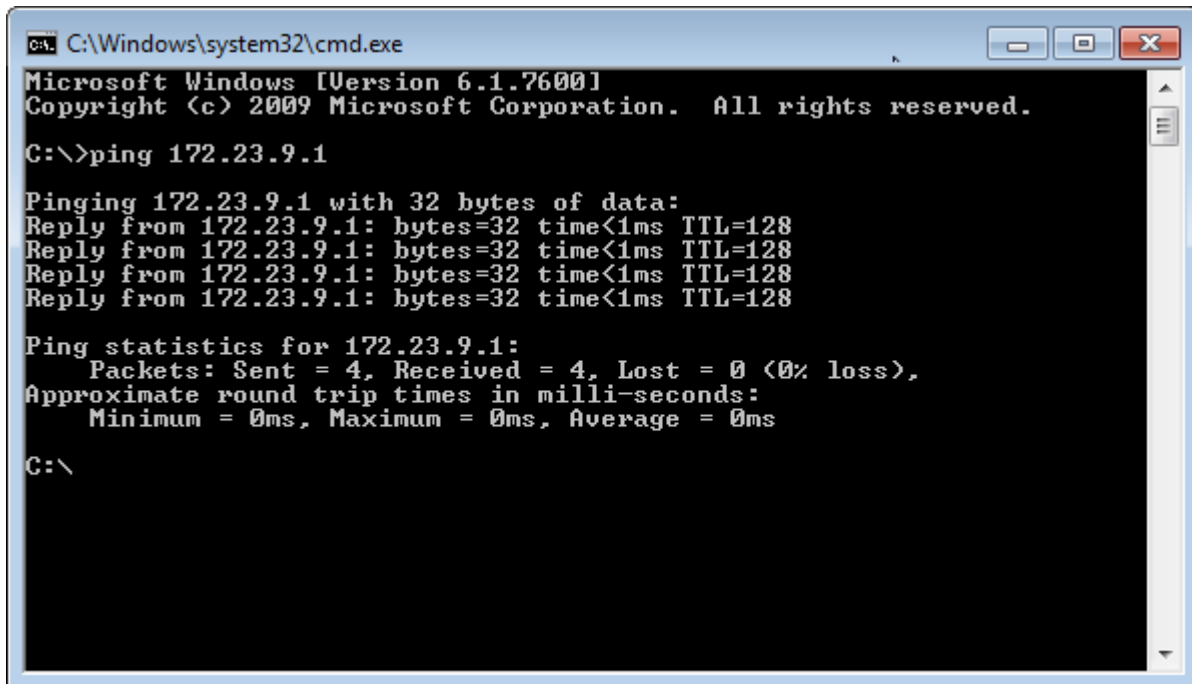


figure 2.6.3: Established connection

Then open a dos box, and ping the internal network interface of the VPN Gateway to confirm the connection has been successfully established. Depending on the VPN Gateway's configuration other hosts on the Gateway B's internal LAN can be reached



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ping 172.23.9.1

Pinging 172.23.9.1 with 32 bytes of data:
Reply from 172.23.9.1: bytes=32 time<1ms TTL=128
Reply from 172.23.9.1: bytes=32 time<1ms TTL=128
Reply from 172.23.9.1: bytes=32 time<1ms TTL=128
Reply from 172.23.9.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.23.9.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

figure 2.6.4: Command Prompt: Ping response

2.7 Verifying the defined certificate

In order to verify that the certificate has correctly been located and loaded, please go to **Connection** -> **Enter PIN**



figure 2.7.1: Entering PIN to open user certificate

Enter the **PIN**, and this then allows you to view the client certificate in **Connection** -> **Certificates** -> **View Client Certificate**.

NOTE: If this option is not available, then one may not have defined (or selected) a connection profile that requires certificates, or has a certificate profile associated with it; see fig. 2.5.15

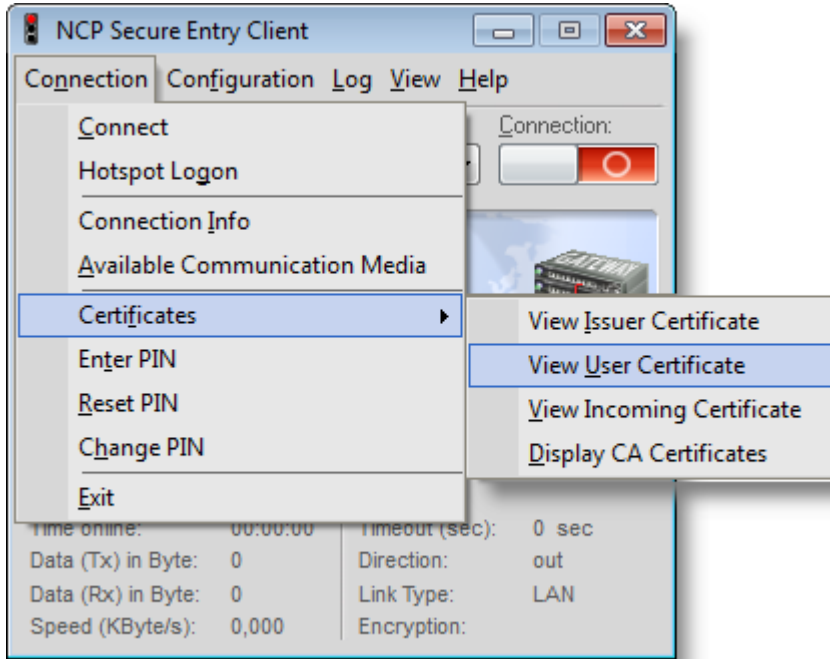


figure 2.7.2: Connection -> Certificates -> View Client Certificate

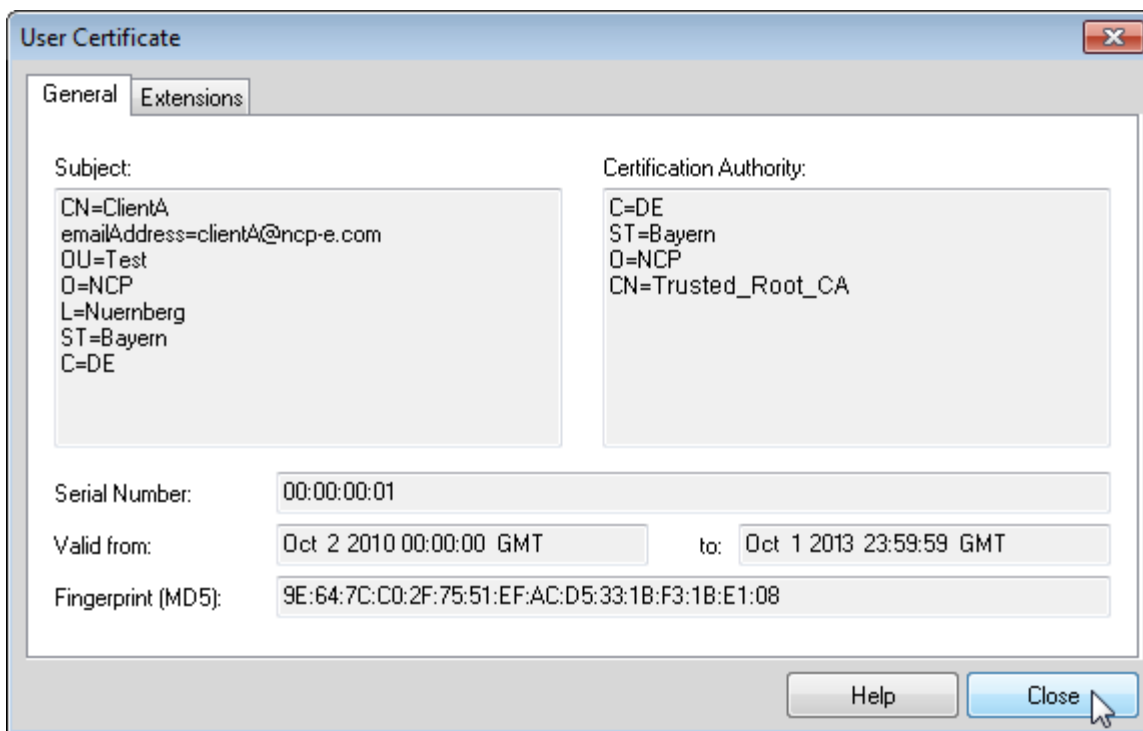


figure 2.7.3: Verify user certificate

If there is any problem this will be highlighted in bright red. The example above shows a client certificate generated by the **Trusted_Root_CA** used in this example.