



SECURE COMMUNICATIONS ■

Secure Entry CE Client & Watchguard Firebox 700

A quick configuration guide to setting up the NCP Secure Entry CE Client in a simple VPN scenario

PDA Client-to-Gateway using pre-shared secrets

Typical client-to-gateway VPN using a pre-shared secret for authentication.

Document version 2.00

Using **NCP Secure Entry CE Client** v2.11 (build 2)

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.

© 2004 NCP Engineering GmbH. All rights reserved.

1. Configuring the Watchguard Firebox

Please refer to the manual/documentation for a comprehensive explanation and procedures to follow when configuring the Firebox for remote user access. This document serves merely as a simple guide to assist in the configuration. It is by no means complete; and therefore highly recommended to consult the respective product's manuals.

1.0 Configuring a Remote User

In the Watchguard **Policy Manager**, select **Remote User** from the **Network** menu.

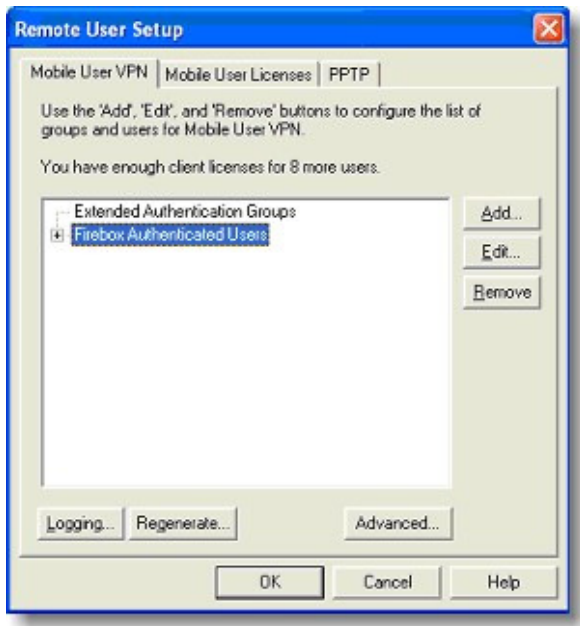


Figure 1.0.1: Remote User Setup

Bring up the **Mobile User VPN** tab, and highlight the **Firebox Authenticated Users** option. Then select **Add...** to start the **Mobile User VPN Wizard**.

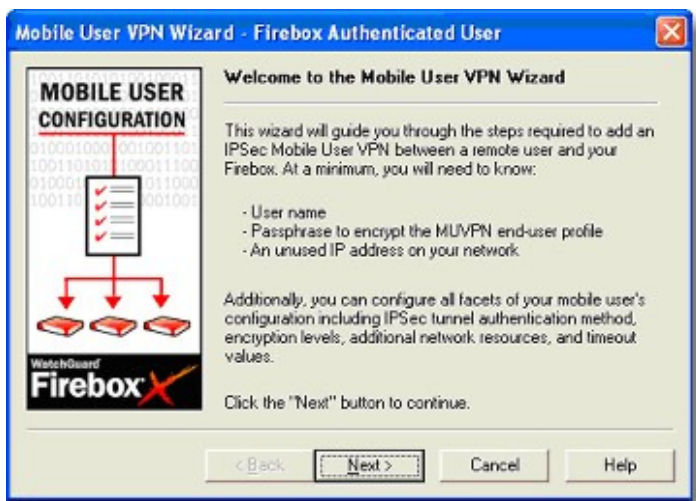


Figure 1.0.2: Mobile User VPN Wizard

Click **Next >** to continue...

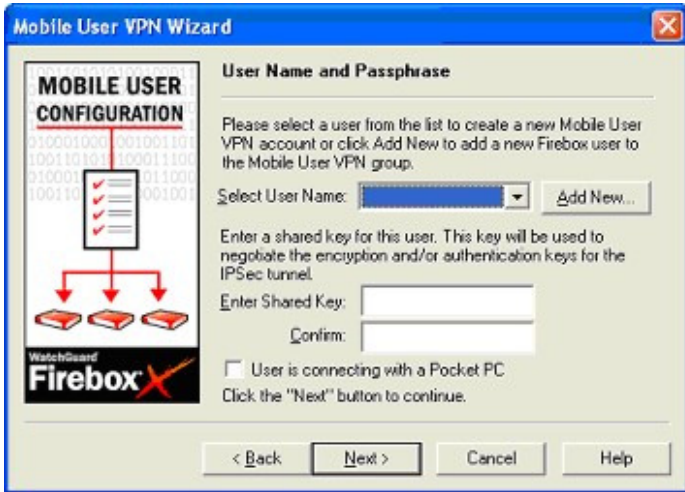


Figure 1.0.3: Username and Passphrase

Click on **Add New...**, to create a new user with a given username and password.

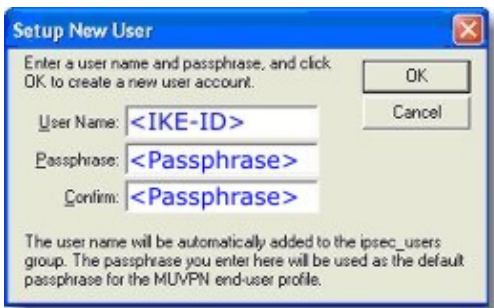


Figure 1.0.4: New User

The WatchGuard Firebox expects the IKE-ID type to be a **ID_USER_FQDN**. Create a user by entering in the **User Name**, which will be referred to as **<IKE-ID>**, further on in the document. The **<Passphrase>** is not used.

Click **OK** to continue...

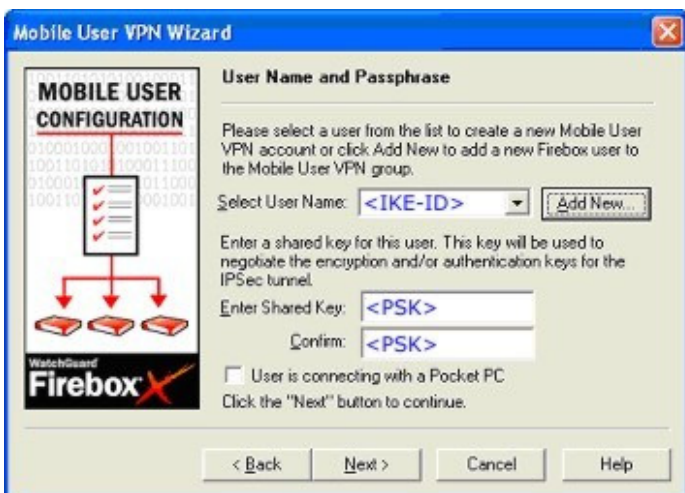


Figure 1.0.5: Username and Passphrase

Select a Pre-Shared Key or secret that will be referred to as **<PSK>** further on in this document.

NOTE: Regardless of whether the NCP Secure Client is running on Windows or on an PDA, do **NOT** select **User is connecting with a Pocket PC**.



Figure 1.0.6: IPSec Tunnel Authentication Method

Enable **Use the passphrase of the end-user profile (the .wgx or .exp file) as the pre-shared key.**

Then click on **Next >** to continue...

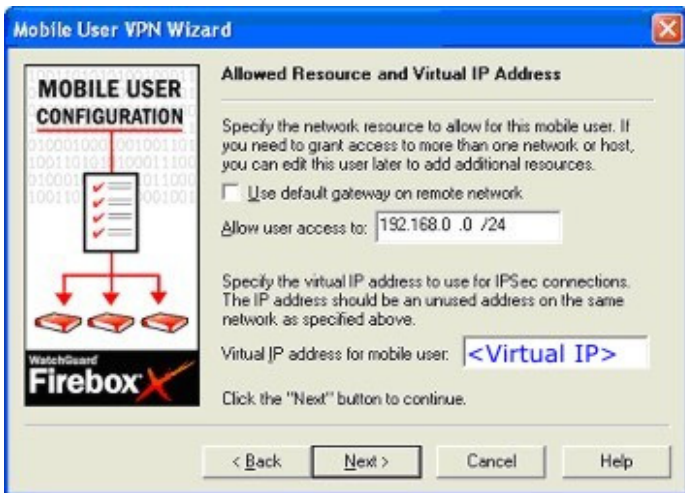


Figure 1.0.7: Allowed Resource and Virtual IP Address Assignment

Define which network the remote user is allowed to gain access to. Also designate a free IP address in the same network segment to the remote user. This will be referred to as the **<Virtual IP>** further on in this document. (Suggestion: it would be a good idea to create a separate network segment entirely devoted to the remote users).

Click **Next >** to continue...

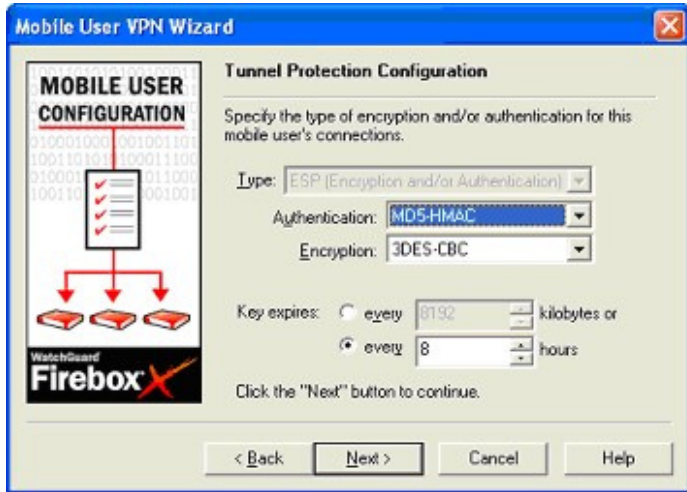


Figure 1.0.8: Tunnel Protection Configuration

Select which parameters are to be used for **Authentication** and **Encryption**, and set the SA lifetimes.

Click **Next >** to continue...

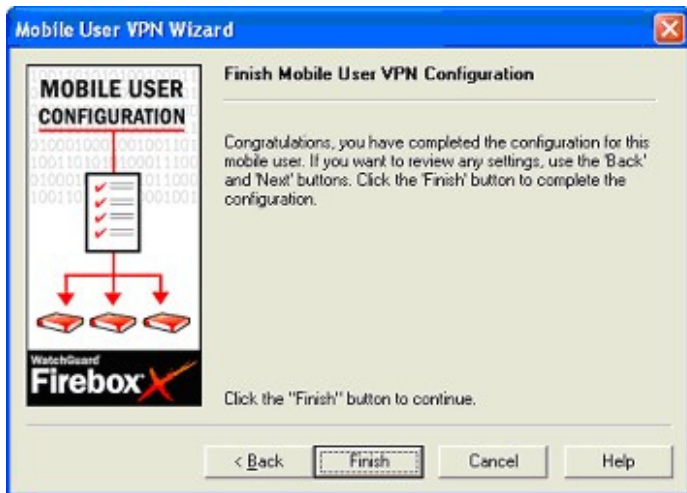


Figure 1.0.9: Completing the configuration

Select **Finish** and save the configuration.

2. Setting up the Client

This section will outline the configuration of the NCP Secure Entry Client for PDAs running WindowsCE. The configuration differs only slightly from using the NCP Secure Entry Client for Windows. The first section 2.0 shows screenshots of the configuration being made with the help of the **Configuration Assistant**. Section 2.1 outlines how to modify an existing profile.

2.0 Using the Configuration Assistant

The first time you start up the NCP Entry CE Client you will be prompted to create a profile. You can either use the assistant or modify an existing profile as shown in section 2.1.

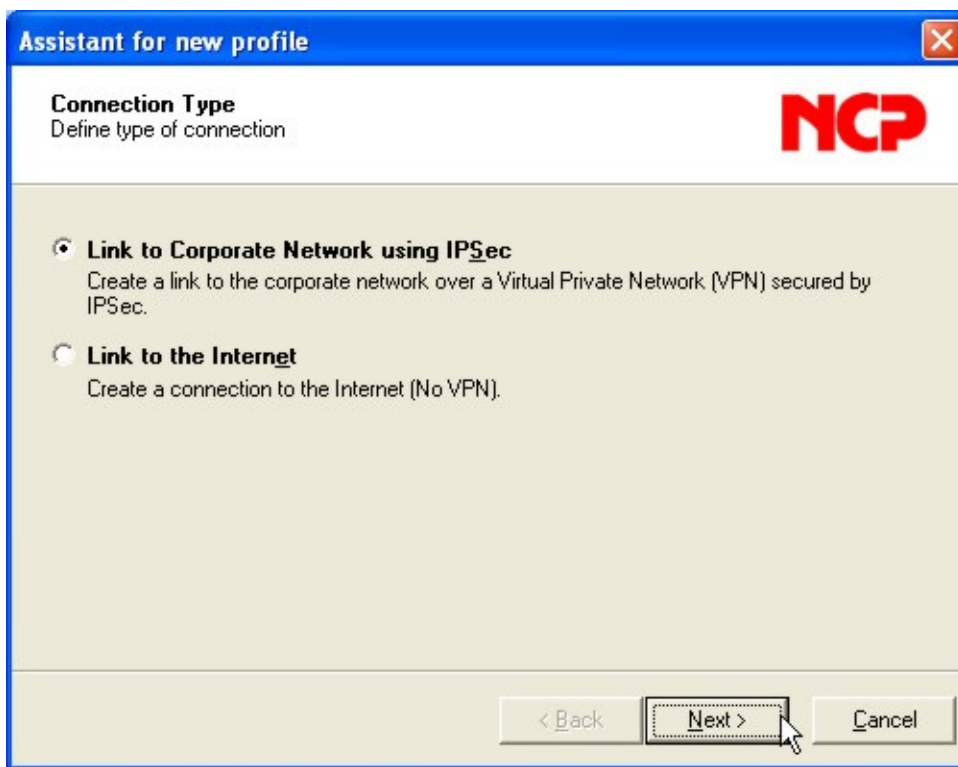


Figure 2.0.1: Define type of connection

Select **Link to Corporate Network using IPsec** to create a profile with the parameters needed to establish a connection to the Watchguard Firebox.

Click **Next >**.

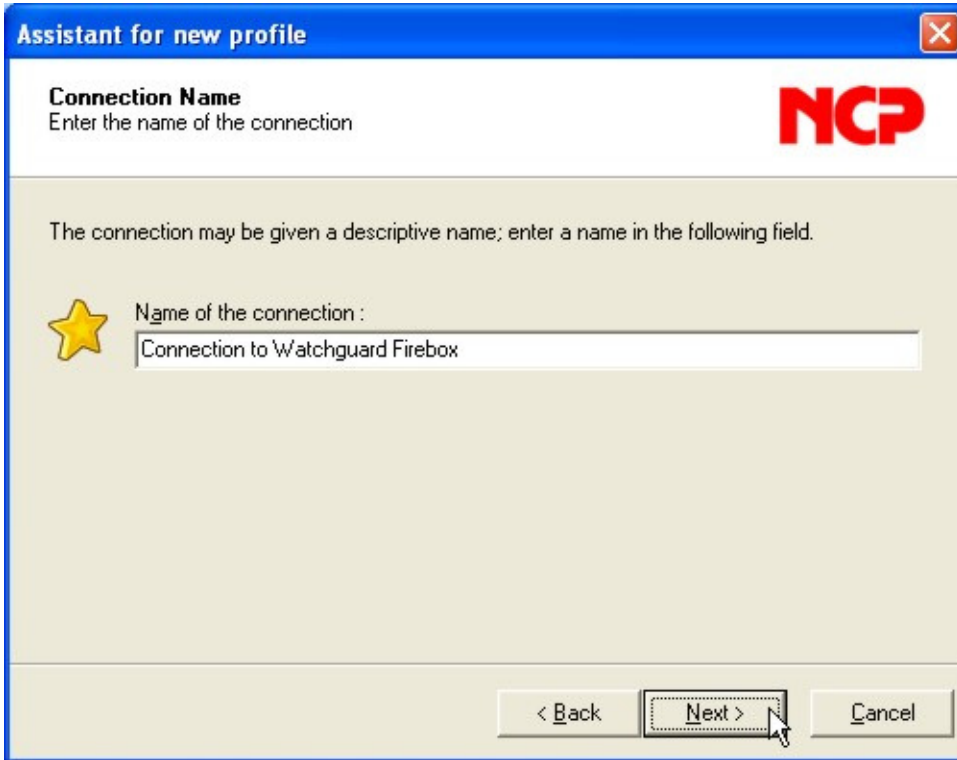


Figure 2.0.2: Connection Name

Several profiles can be created and each given different name. In this example, this profile is created and given the name **Connection to Watchguard Firebox**. Click **Next >**.



figure 2.0.3: Link type (Dial up configuration)

The NCP Secure Entry CE 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 **Modem** and then click **Next >**.

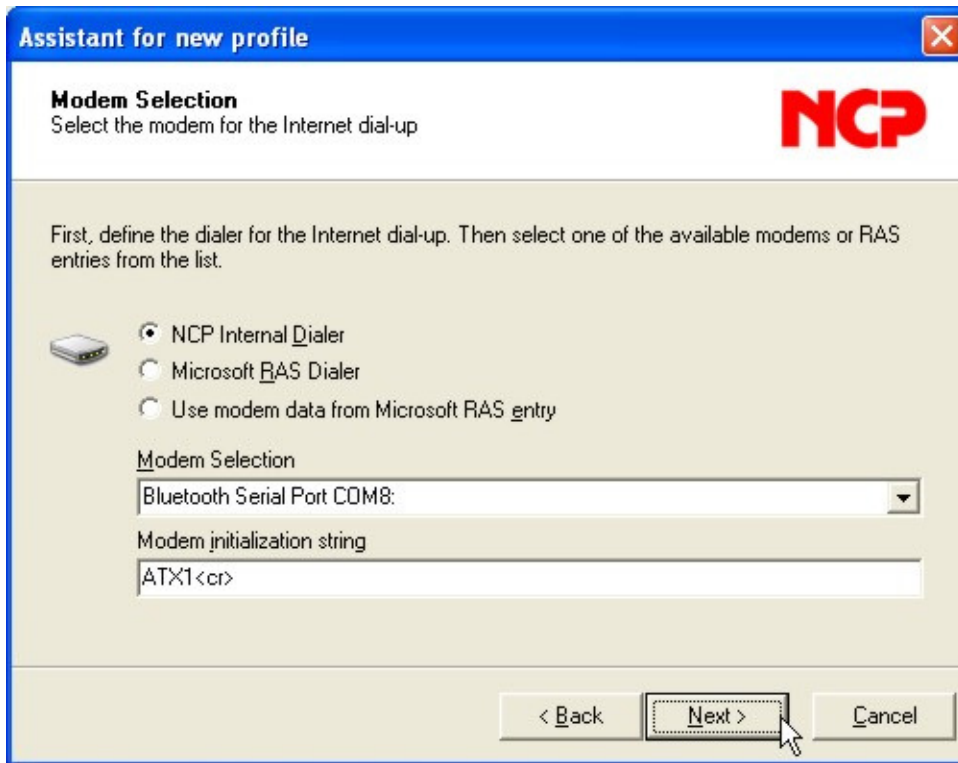


figure 2.0.4: Modem Selection

In this example the internal dialer will be used to establish a connection to the Internet. The PDA in this example has a Bluetooth partnership (**Bluetooth Serial Port COM8**) with a mobile phone. Click **Next >**.



figure 2.0.5: Access information to the internet service provider

Enter in the access information required by the ISP to establish a connection to the Internet.

Click **Next >** to continue...

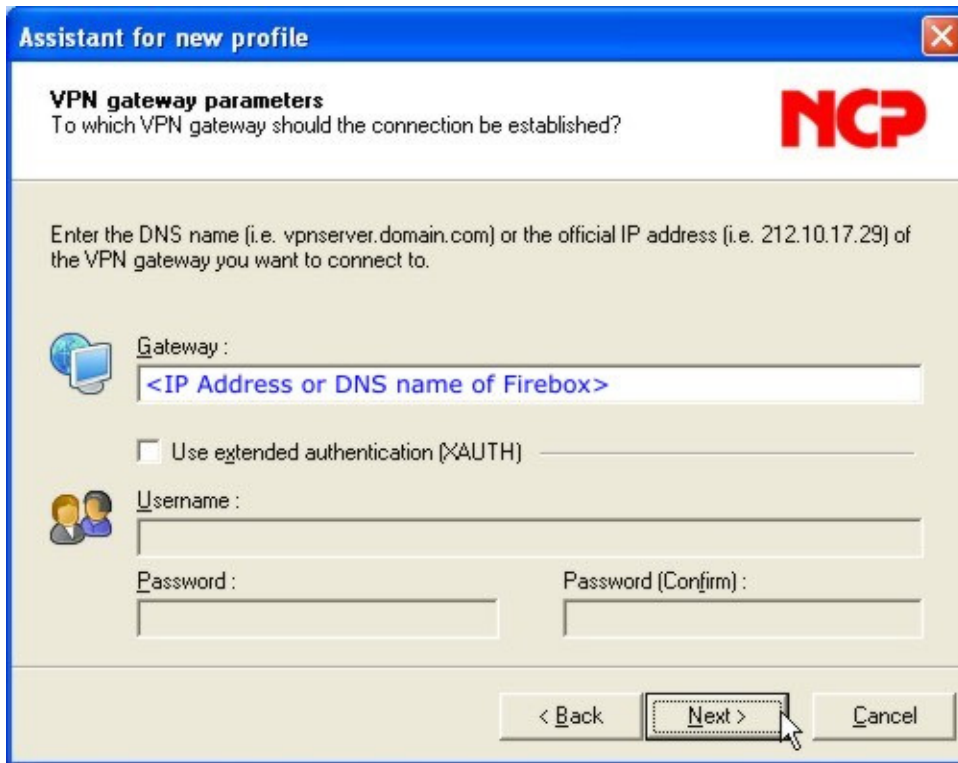


figure 2.0.6: VPN gateway parameters

Enter in the Firebox'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 >**.

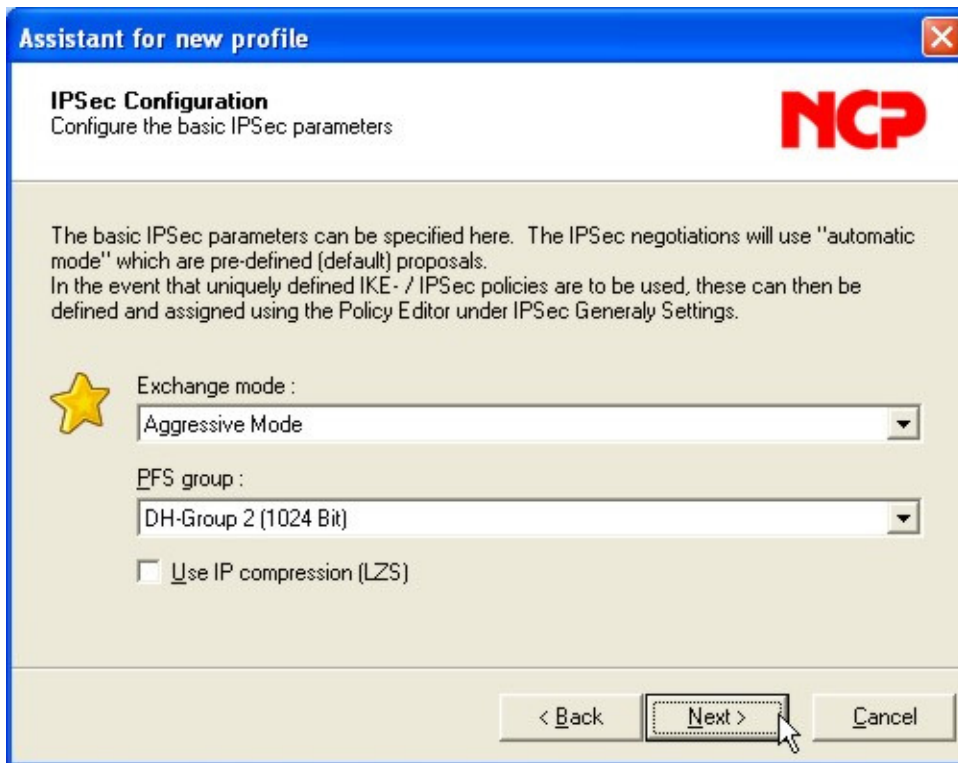


figure 2.0.7: Basic IPSec Configuration

This example will use **Aggressive Mode** and **Perfect Forward Secrecy** seamless re-keying, employing **DH-Group2 (1024 Bit)**. (If the VPN Gateway supports LZS compression, then this can be enabled here). Click **Next >**.

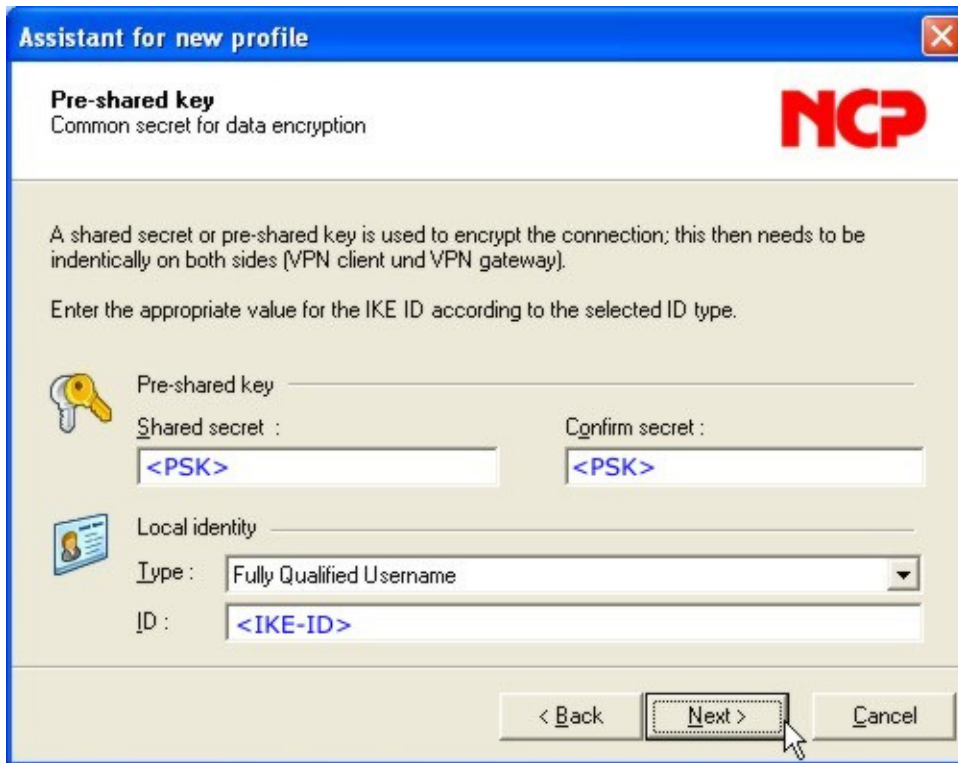


figure 2.0.8: Pre-shared keys

In this example, a pre-shared key or shared secret is used, identical passwords on the IPSec communicating peers. The Firebox expects **ID_USER_FQDN** as **Local Identity** so therefore select **Fully Qualified Username** as IKE-type (as shown above) and enter in the values **<IKE-ID>**, and **<PSK>** used (see figure 1.0.5) and confirm this to ensure that it is correctly entered in.

The **Next >** button will not be available until the **Shared Secrets** have been entered in, confirmed and match.

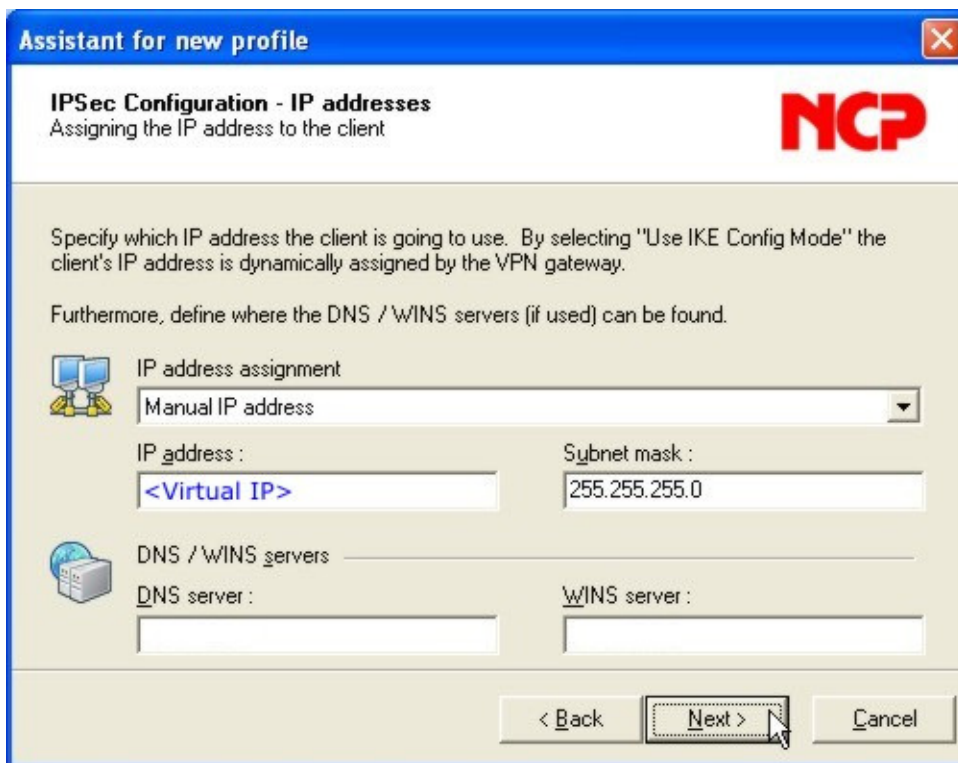


figure 2.0.9: IPSec Configuration – IP addresses

The Firebox is configured to assign a Virtual IP Address to the incoming 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). Optionally enter in the addresses where the (internal/external) DNS and WINS servers can be found.

Click **Next >** to continue.

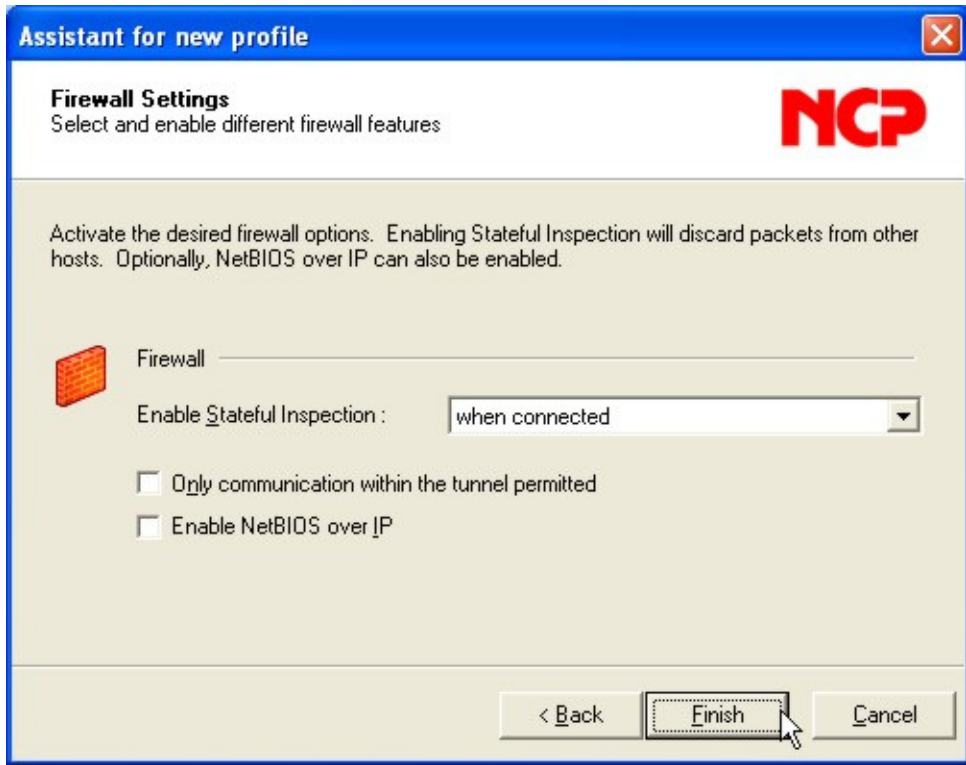


figure 2.0.10: Firewall settings

The NCP Secure Entry Client also comes with a (stateful inspection) personal firewall that can be enabled to provide protection against attacks from the local LAN (for example an environment at a public wlan hotspot). Click **Finish** to save the setting to this profile.

2.1 Checking/Modifying the Configuration



figure 2.1.1: Configuration -> Profile Settings

Open the **Profile Settings** to review/modify the connection parameters.

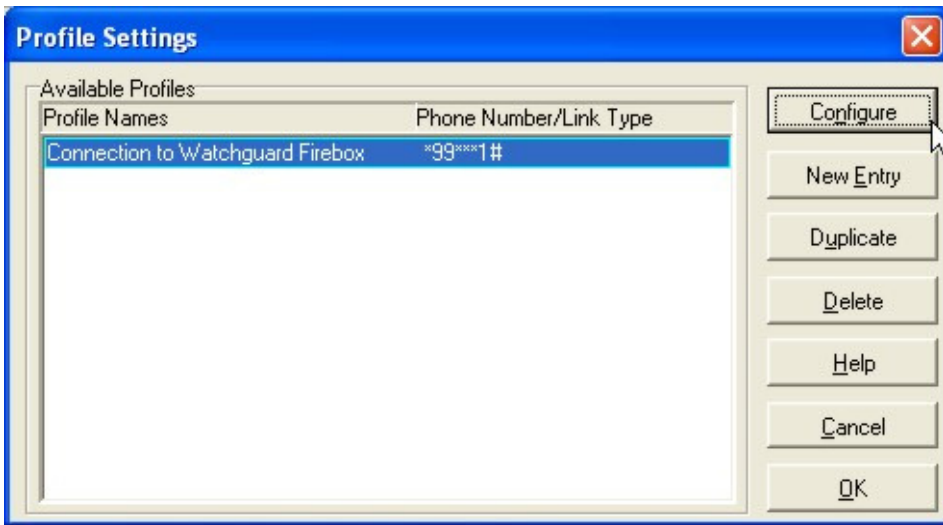


figure 2.1.2: Profile Settings

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

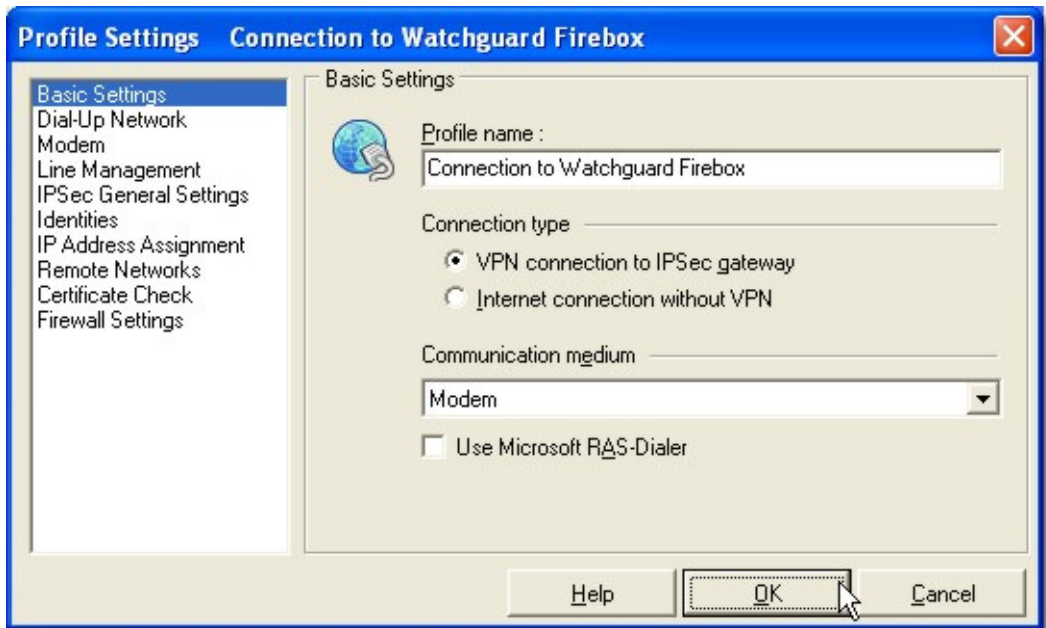


figure 2.1.3: Profile Settings: Basic Settings

Review the parameters and ensure they are correct.
 Select **Dial-Up Network** to continue...



figure 2.1.4: Profile Settings: Dial-Up Network Settings

Confirm the **Username**, **Passwords** and access **number** to the ISP's POP are correct.
 Select **Modem** to review the modem settings...

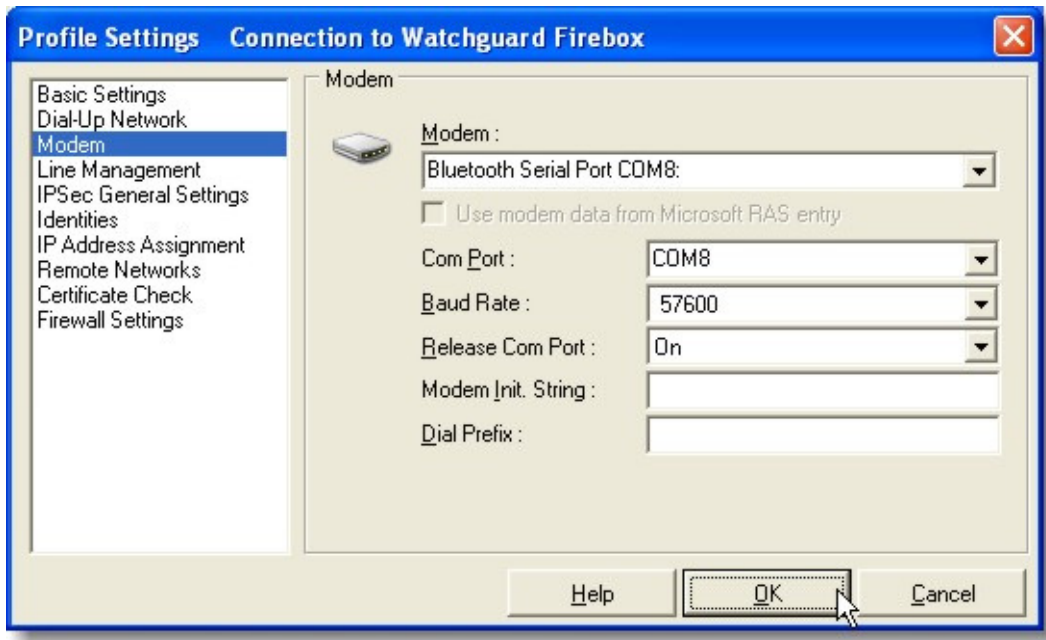


figure 2.1.5: Profile Settings: Modem Settings

Verify the correct Modem is selected.
Select **Line Management** to continue...



figure 2.1.6: Profile Settings: Line Management

The **Connection Mode** can be set to connect automatically, meaning that any time a packet is destined for Firebox's Internal 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...

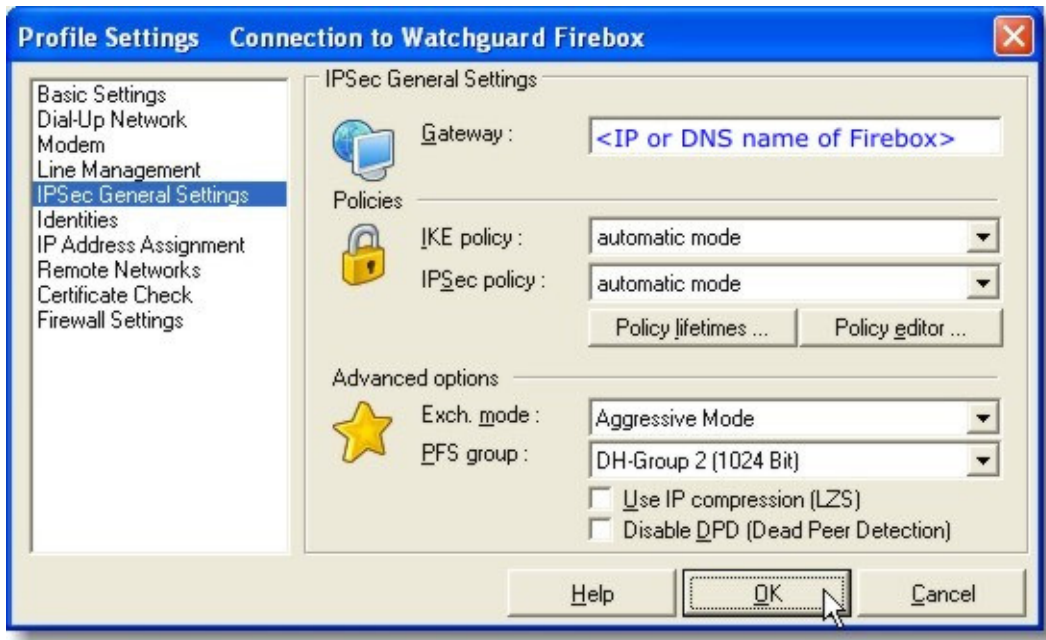


figure 2.1.7: Profile Settings: IPSec General Settings

Verify the IP address or DNS name of the Watchguard Firebox is correctly configured.

When **automatic mode** is selected for both the **IKE** (Phase 1) and **IPSec** (Phase 2) **Policies**, the client will submit a range of different commonly used proposals and the Firebox can then select one to use for the connection. The select settings as shown in figure 1.0.8 will work automatically, thereby not necessitating the definition of custom proposals.

Click on **Identities** to move to the next dialog box.



figure 2.1.8: Profile Settings: Identities

The Firebox is expecting a **Fully Qualified Username**; enter in the same values as in figure 1.0.5. Other IKE-ID types can be used, but are beyond the scope of this quick guide; please refer to the manual for more details.

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

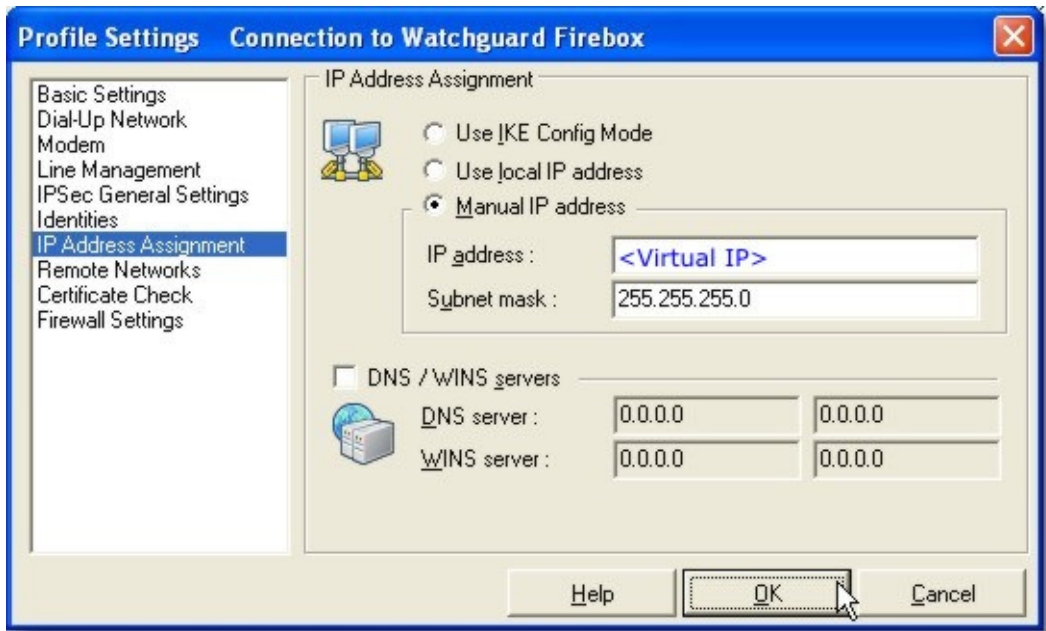


figure 2.1.9: Profile Settings: IP Address Assignment

Confirm the settings as entered in figure 1.0.7. Then click on **Remote Networks** to move to the next dialog box.

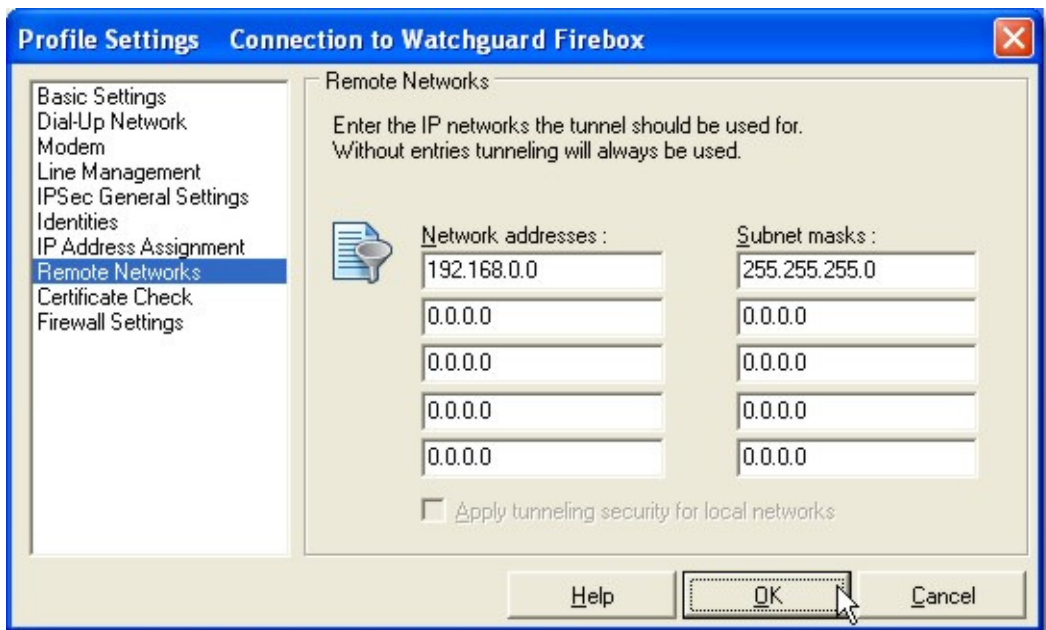


figure 2.1.10: Profile Settings: Remote Networks

Enter in the **Network address(es)** (depending on the subnet masks defined, these can be individual hosts or network segments) that are to be reached. This is used in the Phase 2 negotiation and often the cause for configuration mistakes. In this scenario, the Firebox's LAN segment, **192.168.0.0/24** (or netmask **255.255.255.0**) is to be reached, so that can be defined here (see figure 1.0.7).

Skip **Certificate Check**, because this example does not call for the use of certificates, select the **Firewall Settings** instead...



figure 2.1.11: Profile Settings: Firewall Settings

Confirm the settings here as entered in figure 2.0.10.

Click on **OK** to return to the main **Profile Settings** dialog box.

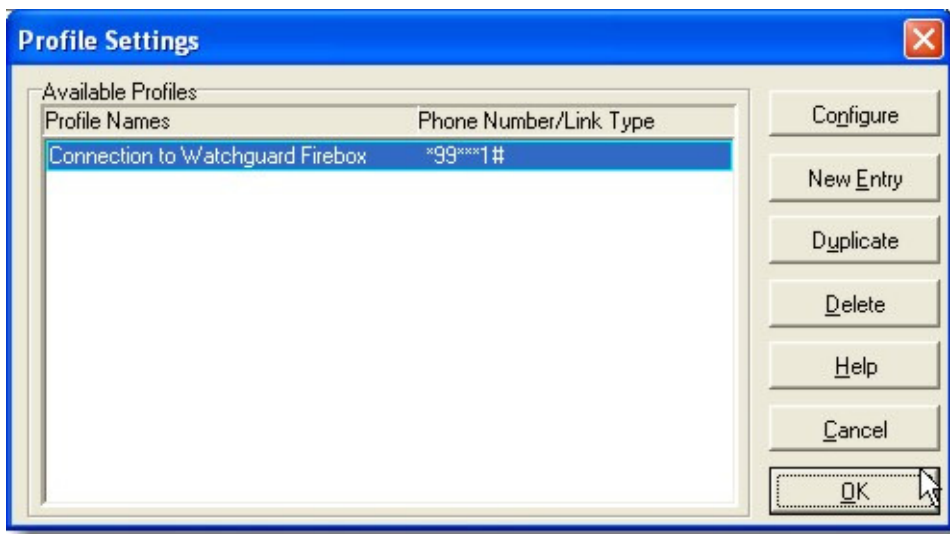


figure 2.1.12: Profile Settings

Select **OK** to return to the configurator (the graphical user interface to configure the VPN CE Client)



figure 2.1.13: Upload Profile Settings to PDA

Upload the configuration to the connected PDA.