



D-Link NetDefend VPN Client (DS-601/605)

A quick installation guide to setting up the D-Link NetDefend VPN Client in a VPNC scenario

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.

Document version 1.00

Using **D-Link NetDefend Client v1.0**

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. 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 pre-shared secret for authentication.

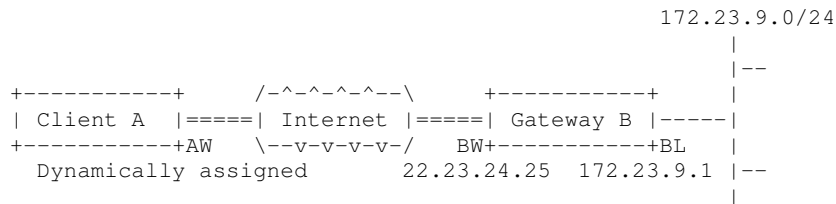


Figure 1.1.1: Scenario

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 Configuration Assistant



Figure 1.2.1: Configuration Assistant

The first time you start up the D-Link VPN Client you may be prompted to create a profile if one doesn't already exist. You can either use the assistant as outlined in section 1.2, or modify an existing profile as in section 1.3.



Figure 1.2.2: Configuration Assistant: Connection 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 Pre-Shared Key**. Click **Next >**.

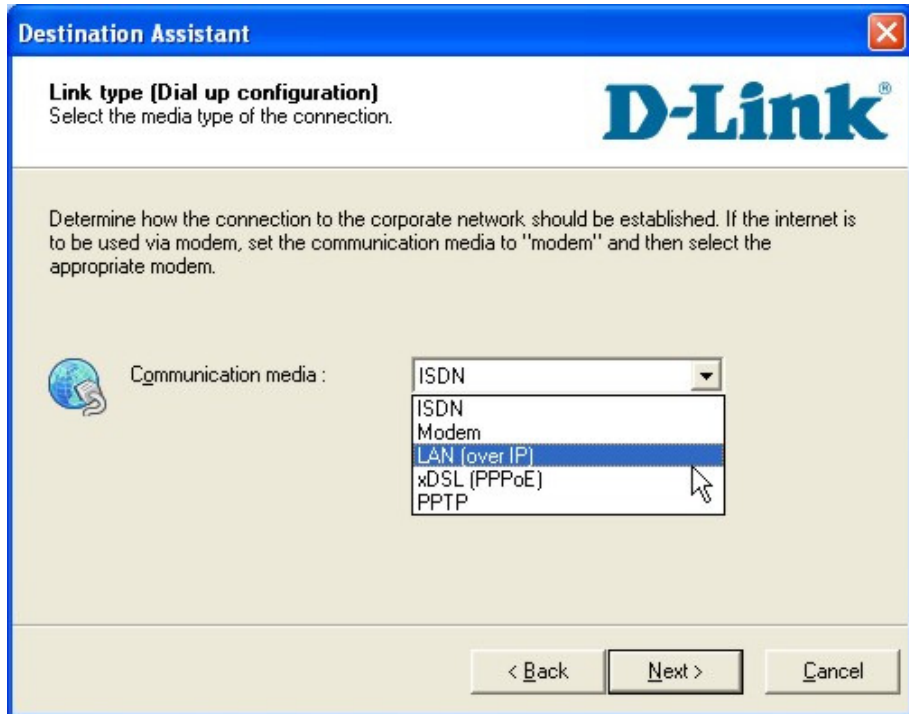


figure 1.2.3: Configuration Assistant: Link type (Dial up configuration)

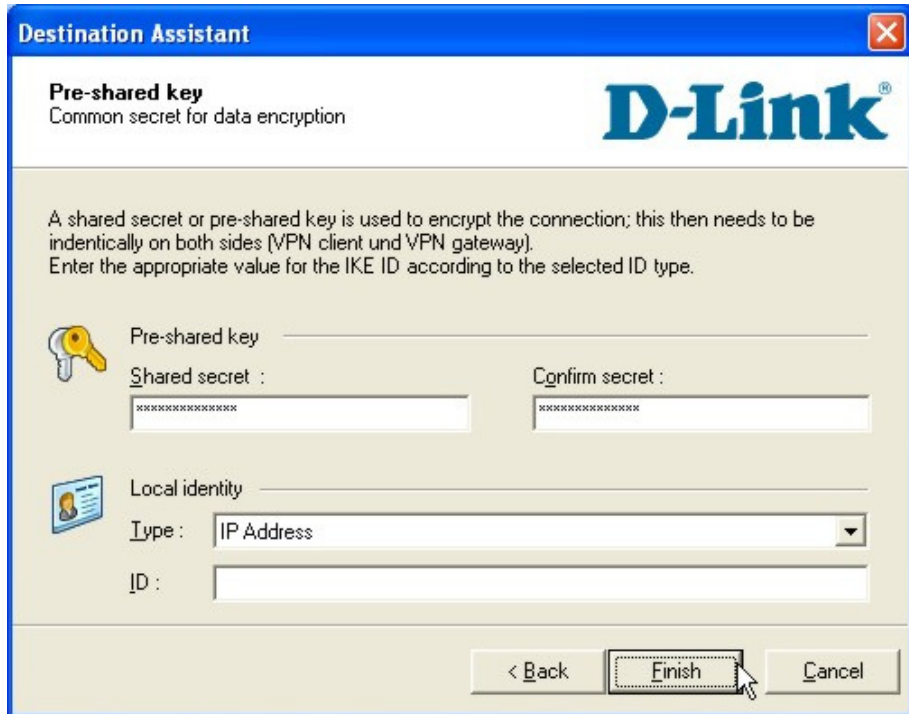
The VPN Client supports different media types; the integrated dialer for example, can be used to establish a connection to the ISP with a modem (if available to the system) prior to building the VPN Tunnel. In this example, select **LAN (over IP)**. Click **Next >**.



The screenshot shows a window titled "Destination Assistant" with a blue header and a red close button. Below the header, the text reads "VPN gateway parameters" and "To which VPN gateway should the connection be established?". The D-Link logo is in the top right. The main area contains instructions: "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." There are three input fields: "Gateway" with the value "22.23.24.25", "Username" (empty), and "Password" (empty). A checkbox "Use extended authentication (XAUTH)" is unchecked. Below the password fields are "Password (Confirm)" (empty). At the bottom are buttons for "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.

figure 1.2.4: Configuration Assistant: VPN gateway parameters

Enter in the gateway's IP address or DNS name.
Click **Next >**.



The screenshot shows a window titled "Destination Assistant" with a blue header and a red close button. Below the header, the text reads "Pre-shared key" and "Common secret for data encryption". The D-Link logo is in the top right. The main area contains instructions: "A shared secret or pre-shared key is used to encrypt the connection; this then needs to be identically on both sides (VPN client und VPN gateway). Enter the appropriate value for the IKE ID according to the selected ID type." There are three input fields: "Pre-shared key" (empty), "Shared secret" (masked with asterisks), and "Confirm secret" (masked with asterisks). Below these is a "Local identity" section with a "Type" dropdown menu set to "IP Address" and an "ID" input field (empty). At the bottom are buttons for "< Back", "Finish", and "Cancel". A mouse cursor is pointing at the "Finish" button.

figure 1.2.5: Configuration Assistant: Pre-shared keys

In this example, a pre-shared key or shared secret is used, identical passwords on the IPSec communicating peers. Enter in the given **hr5xb8416aa9r6** (see section 1.1) and confirm this to ensure that it is correctly entered in. The **Finish** button will not be available until the values have been correctly entered in and match.

1.3 Checking/Modifying the Configuration



figure 1.3.1: Configuration -> Profile Settings

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

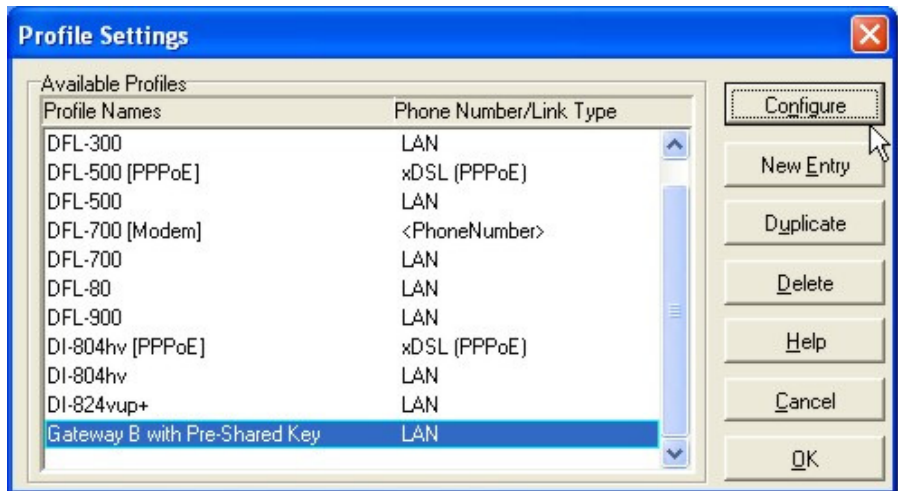


figure 1.3.2: Profile Settings

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

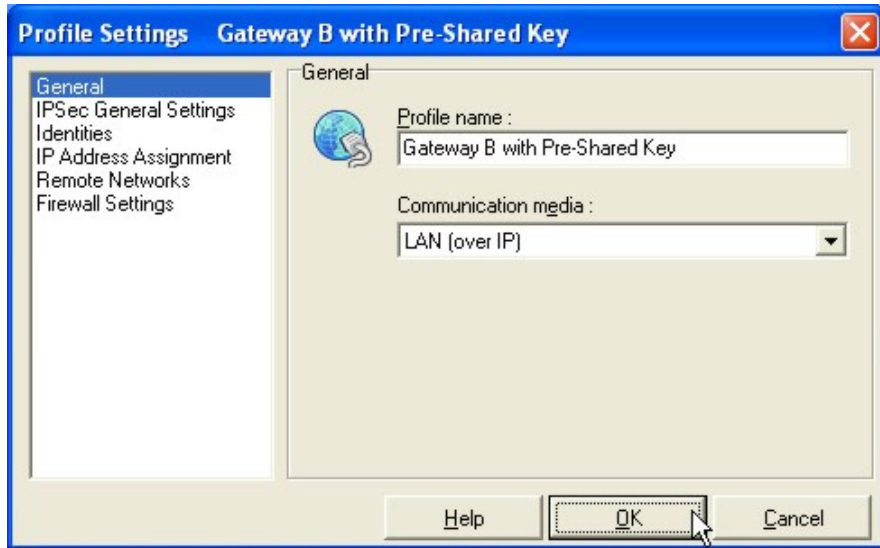


figure 1.3.3: Profile Settings: General

Review the parameters and ensure they are correct. Select **IPSec General Settings** to continue...

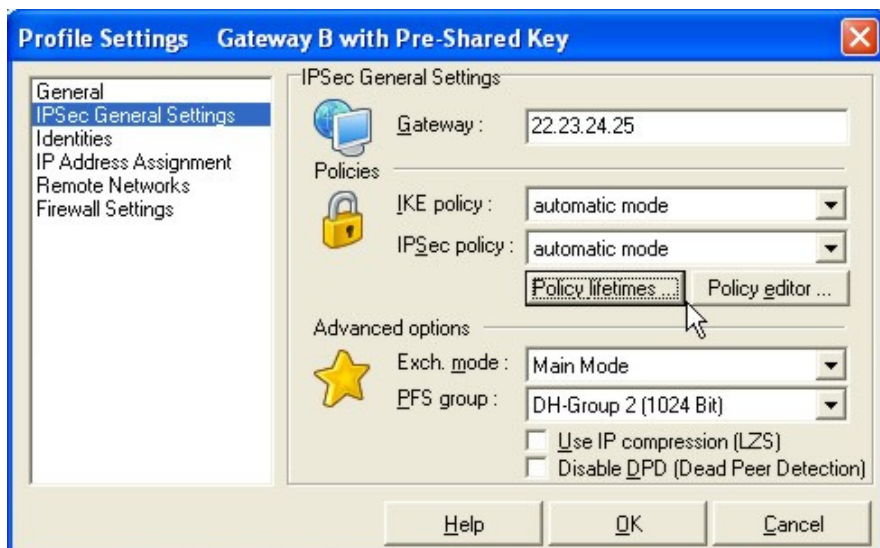


figure 1.3.4: Profile Settings: IPSec General Settings: Policy Lifetimes

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, (although automatic mode works) both the IKE and IPSec policies will be manually defined in accordance to section 1.1; so select **Policy lifetimes...**

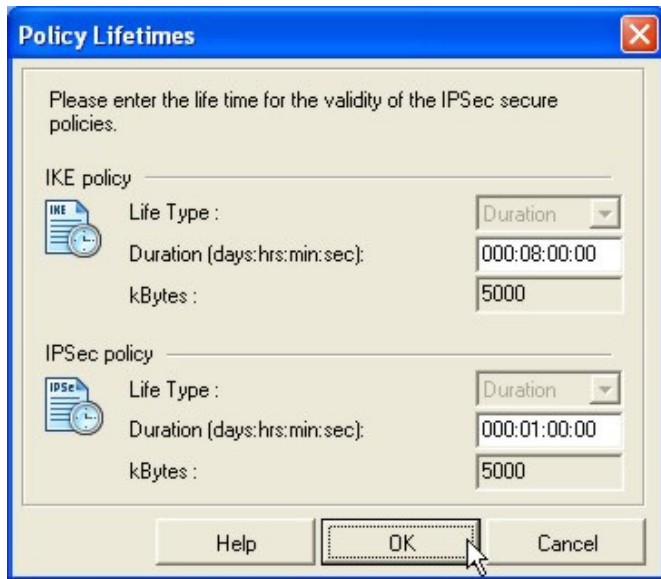


figure 1.3.5: Policy Lifetimes

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...

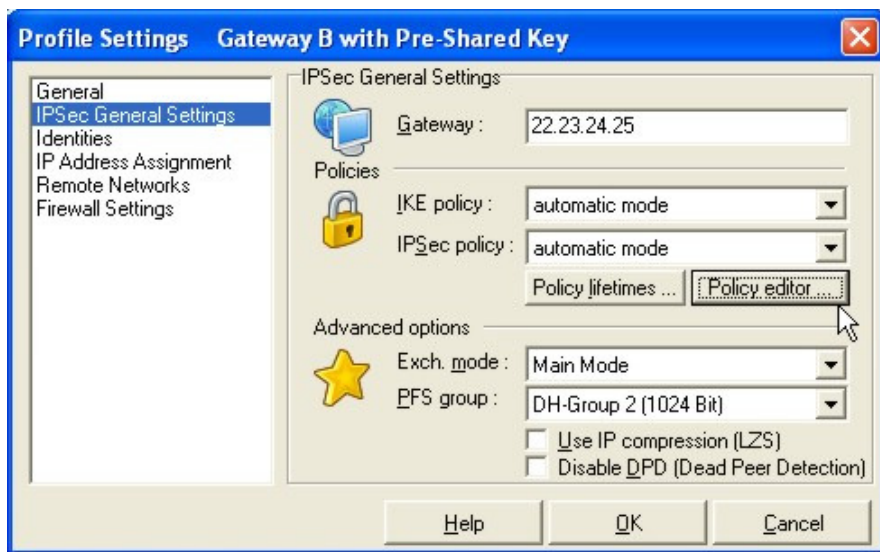


figure 1.3.6: Profile Settings: IPSec General Settings: Policy Editor

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

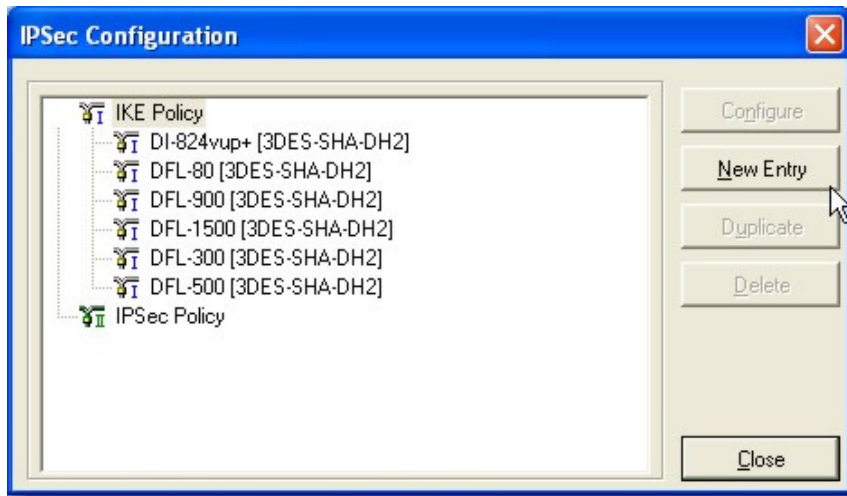


figure 1.3.7: Proposal Definitions: IKE Policy

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

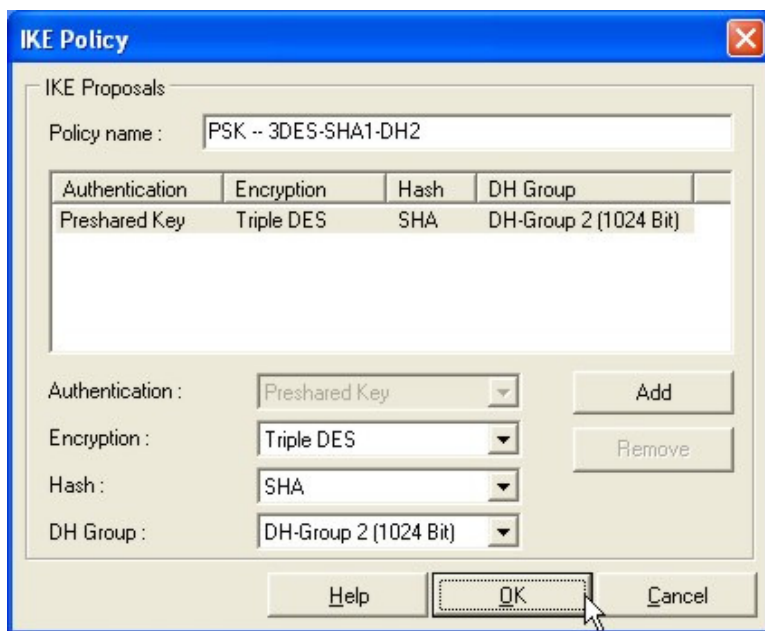


figure 1.3.8: Defining an IKE Policy

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 **Preshared Key** 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.

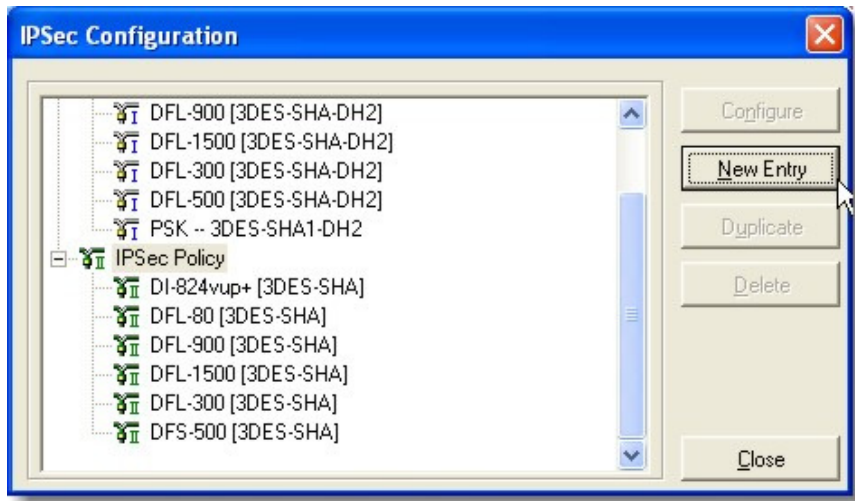


figure 1.3.9: Proposal Definitions: IPsec Policy

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

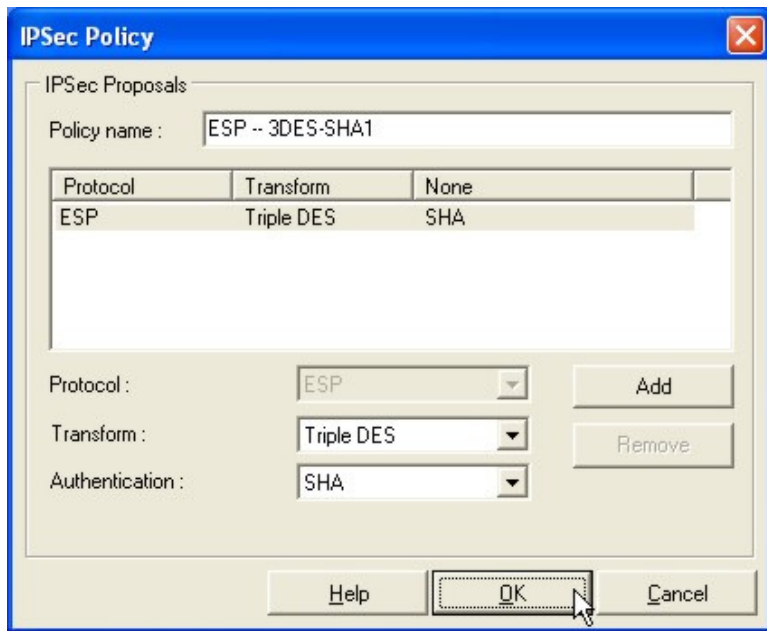


figure 1.3.10: Defining an IPsec Policy

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...

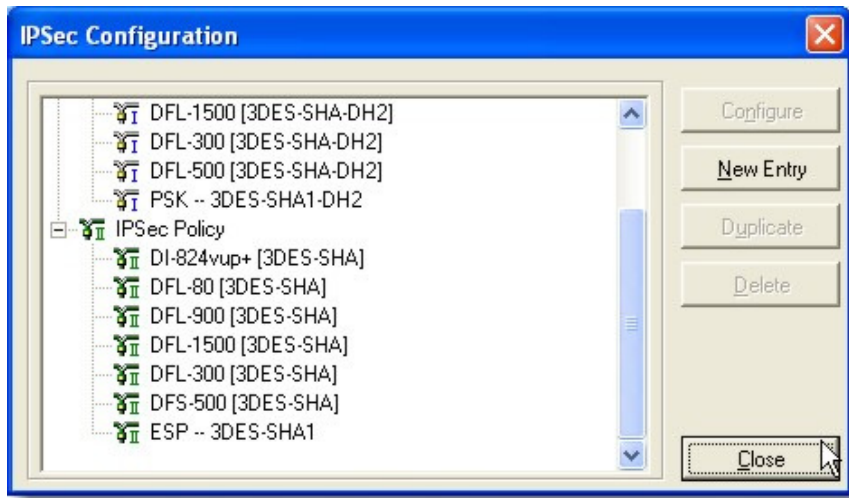


figure 1.3.11: IPSec/IKE (ISAKMP) parameters defined

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

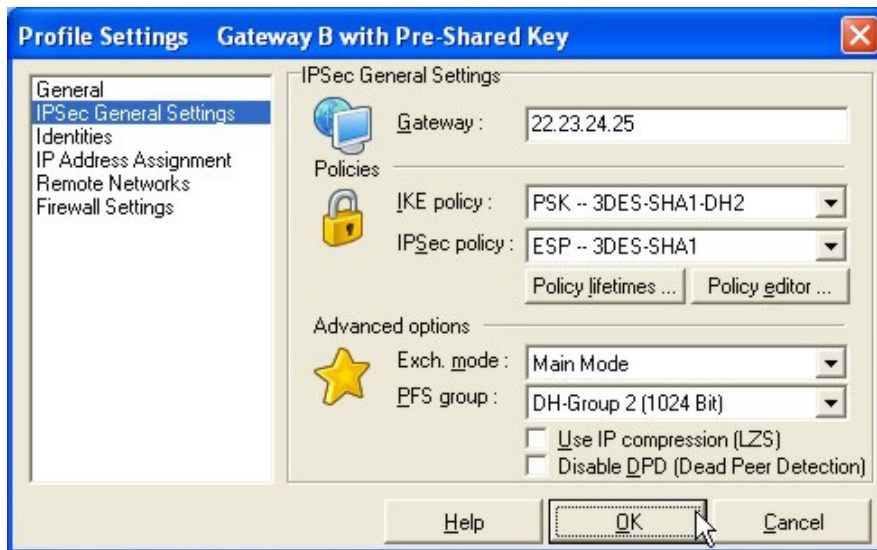


figure 1.3.12: Profile Settings: IPSec General Settings

Select the newly defined **IKE-** (ISAKMP) and **IPSec Policies**, and click on **Identities** to move to the next dialog box.



figure 1.3.13: 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 beyond the scope of this document; please refer to the manual for more details. Click on **IP Address Assignment** to continue...

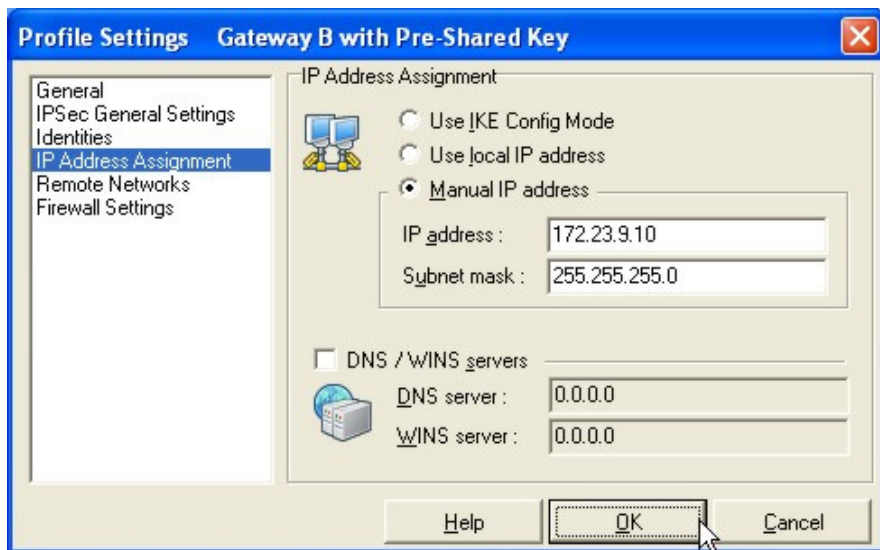


figure 1.3.14: Profile Settings: IP Address Assignment

In this example, the client is known to the VPN Gateway by a virtual IP address which has to be manually entered into the client.

Click on **Remote Networks** to move to the next dialog box.

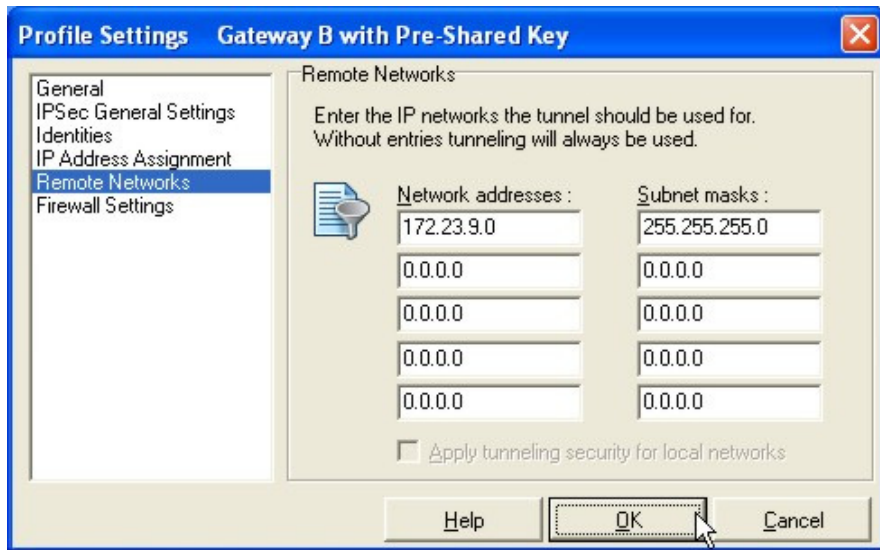


figure 1.3.15: Profile Settings: Remote Networks

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, Gateway B's LAN segment, **172.23.9.0/24** (or netmask **255.255.255.0**) is to be reached, so that can be defined here.

Select the **Firewall Settings** to continue...

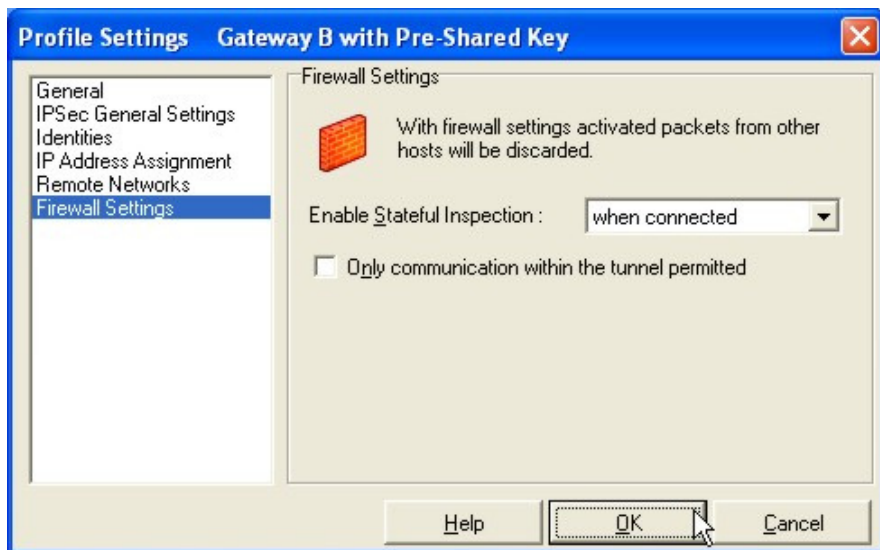


figure 1.3.16: Profile Settings: Firewall Settings

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

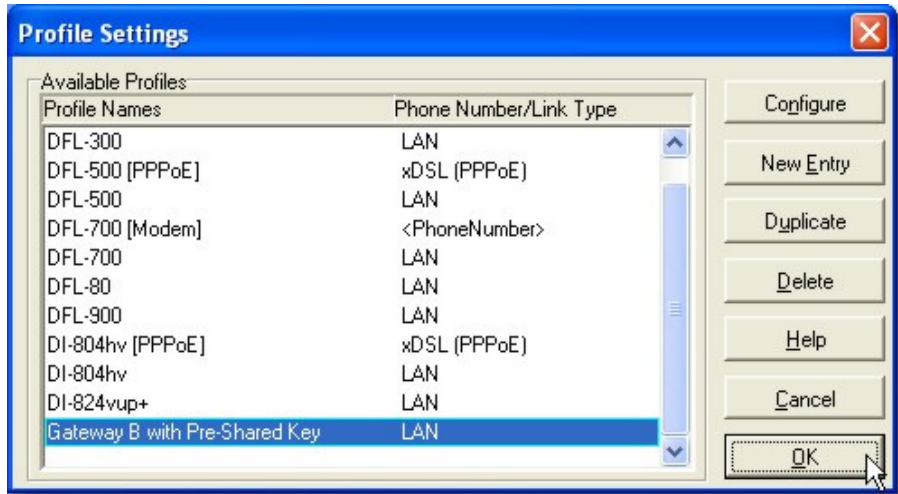


figure 1.3.17: Profile Settings

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

1.4 Establishing the connection



figure 1.4.1: D-Link VPN Client Monitor

Seeing as the connection is set to be established manually, click on **Connect** to create the tunnel. 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.

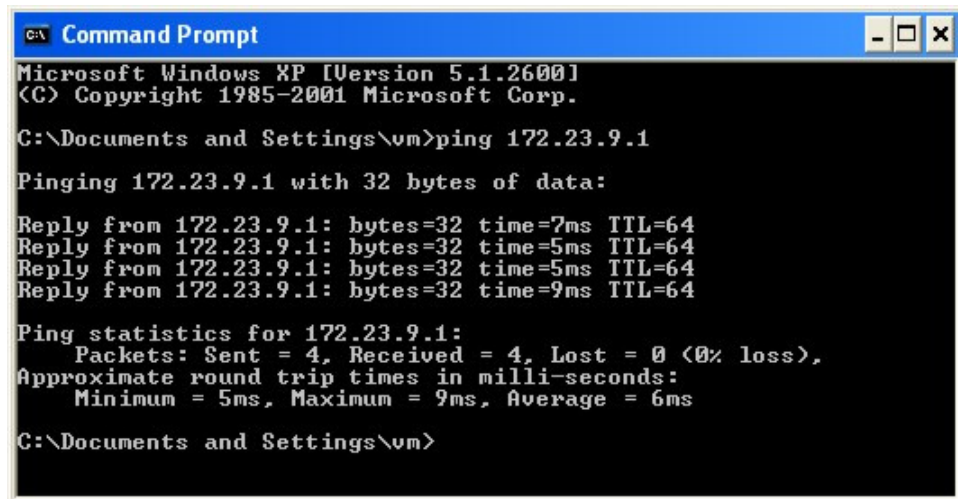


figure 1.4.2: Command Prompt: Ping response