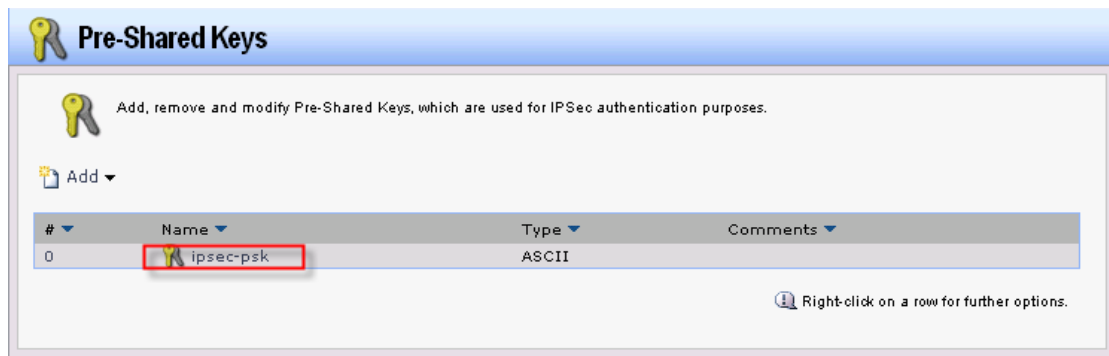
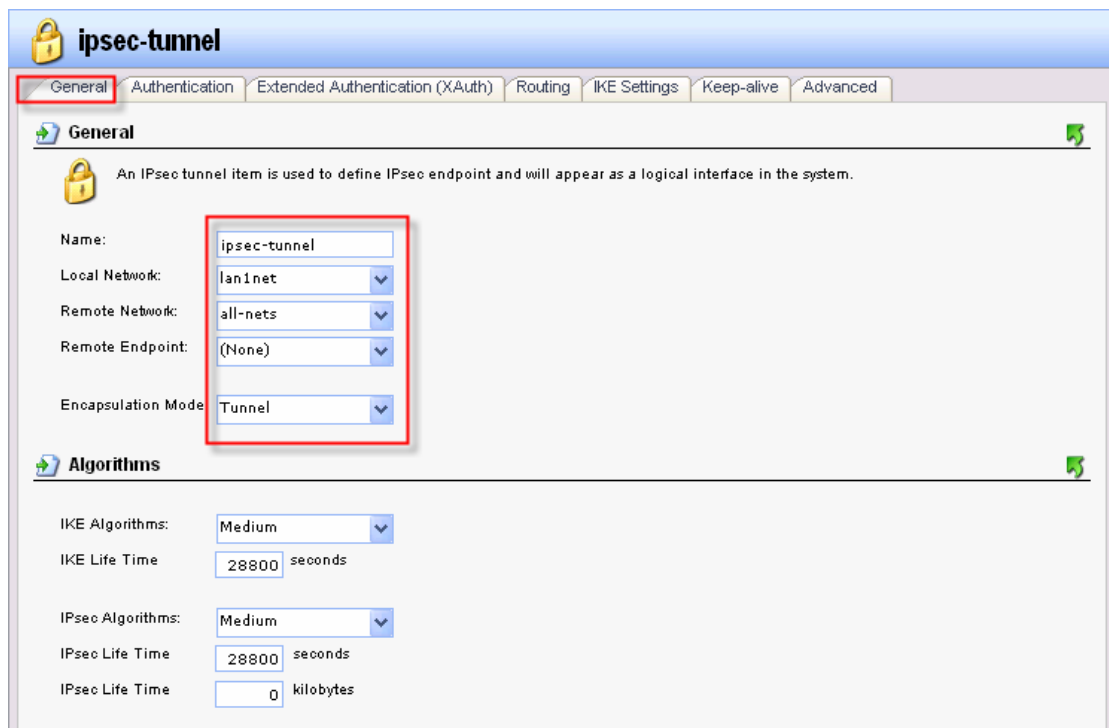


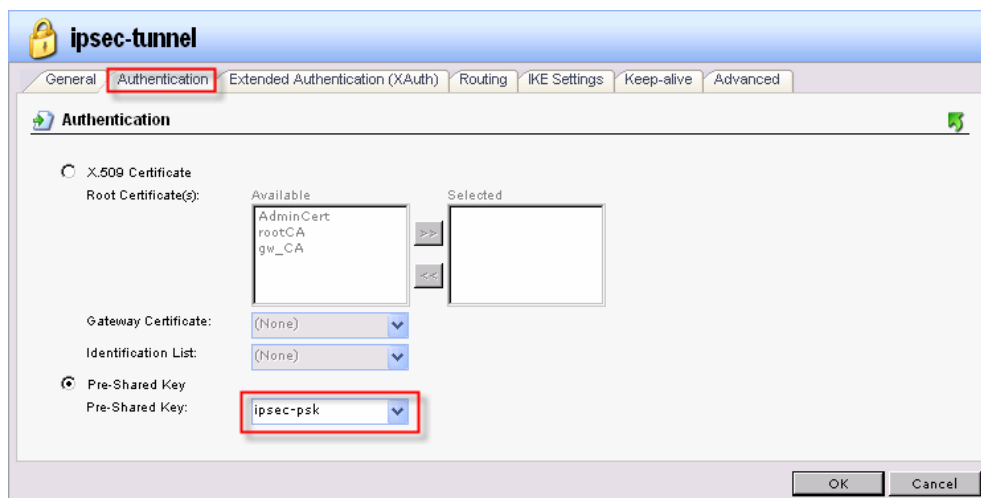
1. Create the pre-shared key first.



2. IPSec tunnel setting (general page): this is for remote clients to dial in



3. select the pre-shared key you created.



4. Enable the option shown below.

The screenshot shows the 'ipsec-tunnel' configuration window with the 'Routing' tab selected. The 'Automatic Routing' section has the option 'Dynamically add route to the remote network when a tunnel is established' checked. The 'Packet Sizes' section shows 'Plaintext MTU' set to 1424. The 'IP Addresses' section has 'Automatically pick the address of a local interface that corresponds to the local net' selected. The 'OK' and 'Cancel' buttons are at the bottom right.

ipsec-tunnel

General Authentication Extended Authentication (XAuth) **Routing** IKE Settings Keep-alive Advanced

Automatic Routing

☐ Allow DHCP over IPsec from single-host clients
☒ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).
Plaintext MTU:

IP Addresses

IP address to use as source IP of the tunnel

☒ Automatically pick the address of a local interface that corresponds to the local net
☐ Specify address manually:
IP Address:

OK Cancel

5. Choose the IKE and PFS at your will.

The screenshot shows the 'ipsec-tunnel' configuration window with the 'IKE Settings' tab selected. The 'IKE' section has 'Main' selected and 'DH Group' set to 2. The 'Perfect Forward Secrecy' section has 'PFS' selected and 'DH Group' set to 2. The 'Security Association' section has 'Per Net' selected. The 'Compatibility Flags' section has 'Do not verify padding' unchecked. The 'NAT Traversal' section has 'On if supported and NATed' selected. The 'OK' and 'Cancel' buttons are at the bottom right.

ipsec-tunnel

General Authentication Extended Authentication (XAuth) Routing **IKE Settings** Keep-alive Advanced

IKE

☒ Main ☐ Aggressive DH Group:

Perfect Forward Secrecy

PFS: DH Group:

Security Association

☒ Per Net ☐ Per Host

Compatibility Flags

☐ Do not verify padding

NAT Traversal

☐ Off ☒ On if supported and NATed ☐ On if supported

OK Cancel

6. Disable this option shown below. This isn't necessary for remote dial in clients.

The screenshot shows the 'ipsec-tunnel' configuration window with the 'Advanced' tab selected. The 'Automatic Route Creation' section has the option 'Add route for remote network' unchecked. The 'Route Metric' is set to 90. The 'OK' and 'Cancel' buttons are at the bottom right.

ipsec-tunnel

General Authentication Extended Authentication (XAuth) Routing IKE Settings Keep-alive **Advanced**

Automatic Route Creation

Automatically add route for remote network.

☐ Add route for remote network

Route Metric:

OK Cancel

7. Combine the ipsec and lan interface

ipsec-lan

General

Use an interface group to combine several interfaces for a simplified security policy.

Name:

☐ Security/Transport Equivalent

Interfaces

Available	Selected
wan1	lan1
wan2	ipsec-tunnel
dmz	
lan2	
lan3	
ipsec-tunnel-2	

Comments

Comments:

OK Cancel

8. create the necessary rule.

ipsec-allow

General Log Settings NAT SAT SAT Server Load Balancing

General

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

Name:

Action:

Service:

Schedule:

Address Filter

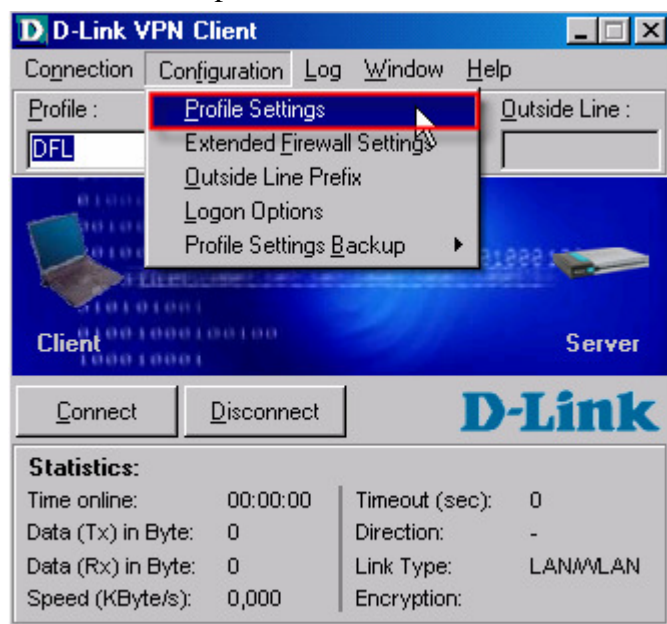
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Source	Destination
Interface:	<input type="text" value="ipsec-lan"/>	<input type="text" value="ipsec-lan"/>
Network:	<input type="text" value="all-nets"/>	<input type="text" value="all-nets"/>

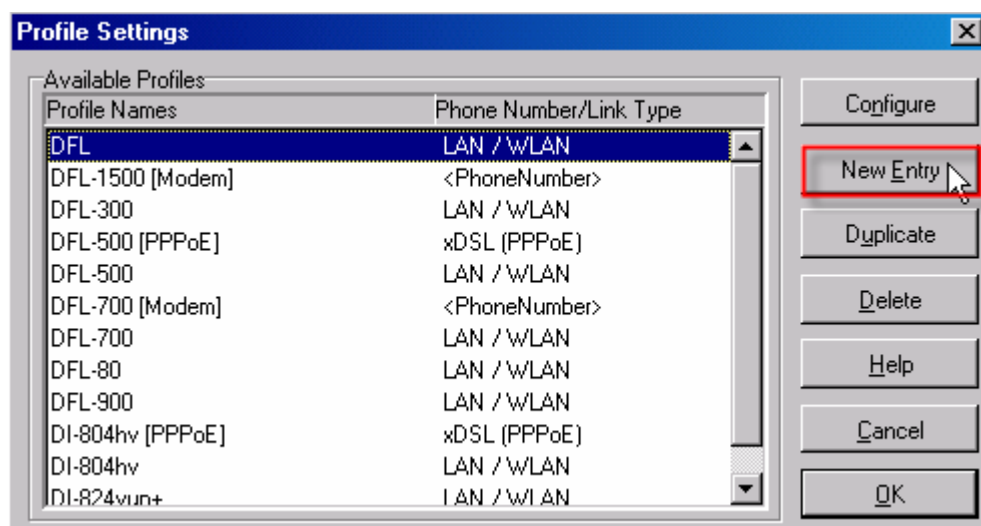
Comments

OK Cancel

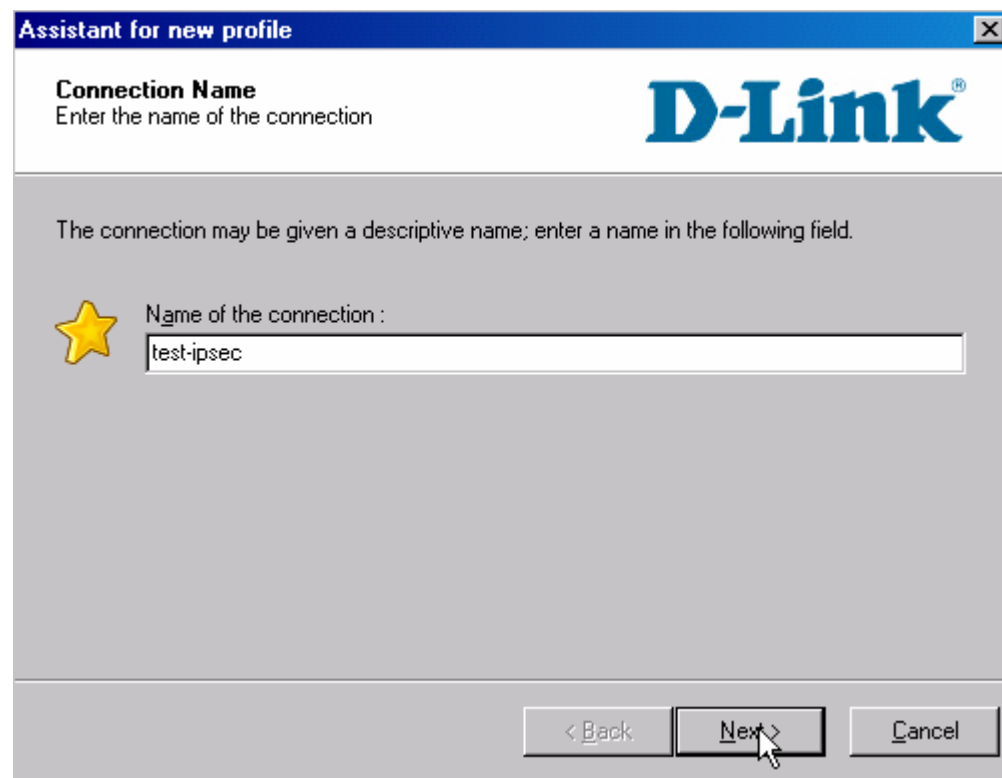
1. Create a new profile.



2.



3.



Assistant for new profile

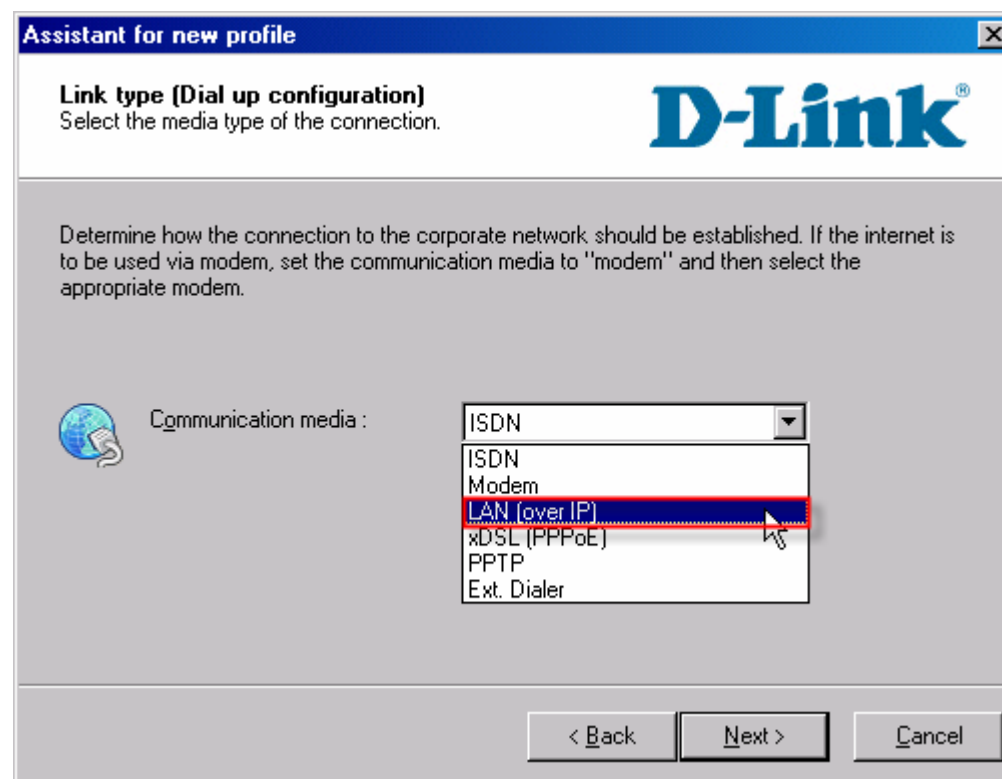
Connection Name
Enter the name of the connection

The connection may be given a descriptive name; enter a name in the following field.

Name of the connection :
test-ipsec

< Back Next > Cancel

4.



Assistant for new profile

Link type (Dial up configuration)
Select the media type of the connection.

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.

Communication media :
ISDN
Modem
LAN (over IP)
xDSL (PPPoE)
PPTP
Ext. Dialer


< Back Next > Cancel

5.


Assistant for new profile [X]

VPN gateway parameters
To which VPN gateway should the connection be established **D-Link®**

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 Username and Password for the authentication. If no authentication data are entered they will be requested when establishing the connection.

 Gateway : **firewall WAN IP**

☐ Use extended authentication (XAUTH) _____

 Username :

Password : Password (Confirm) :


< Back **Next >** Cancel

6.


Assistant for new profile [X]

Pre-shared key
Common secret for data encryption **D-Link®**

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 **Pre-shared key**

Shared secret : Confirm secret :

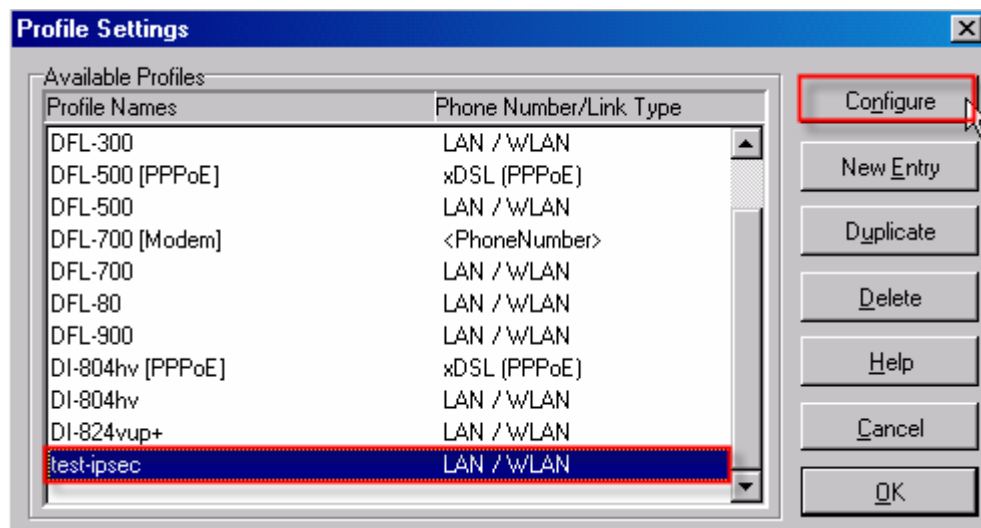
 Local identity _____

Type : [v]

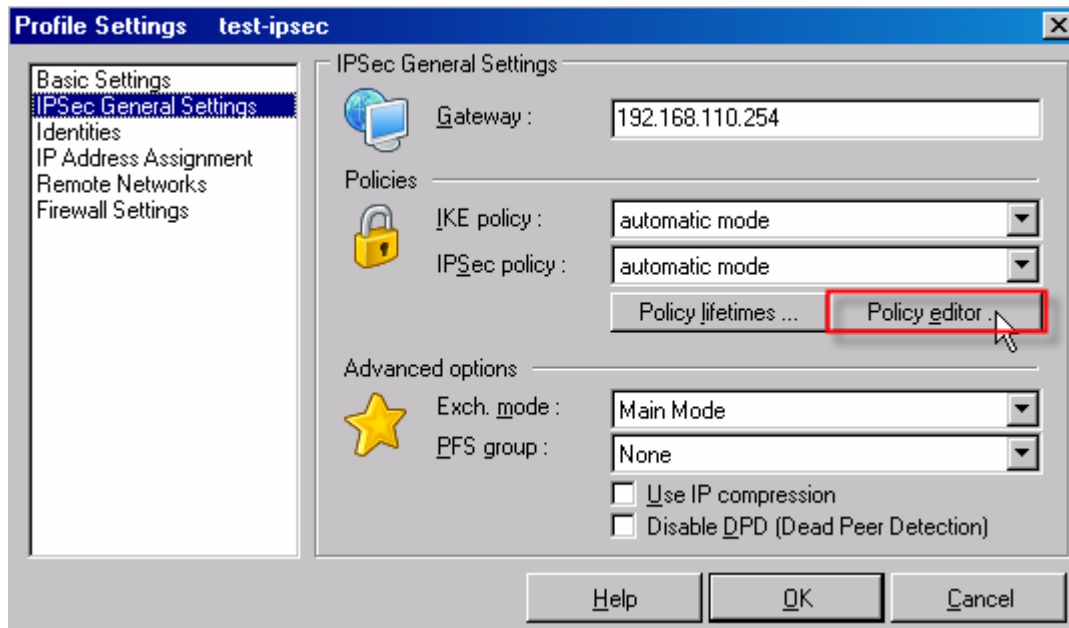
ID :

< Back **Finish** Cancel

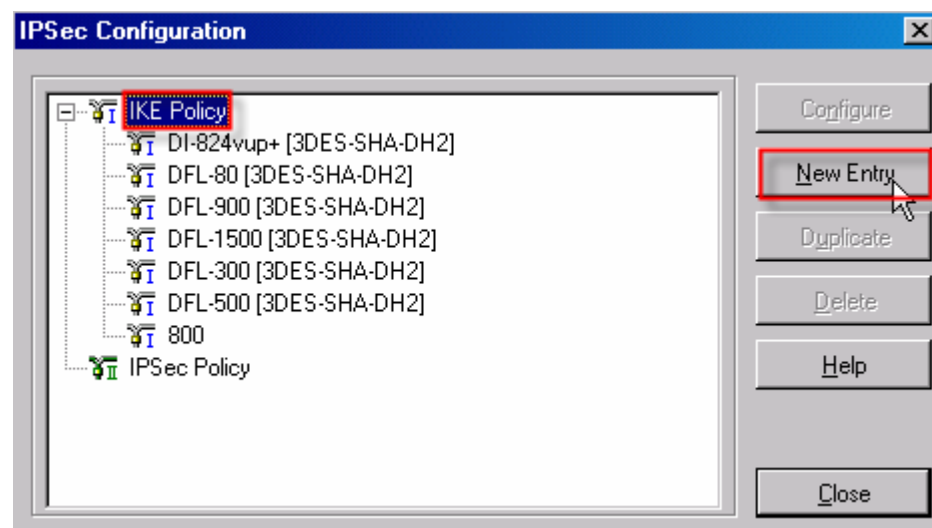
7.



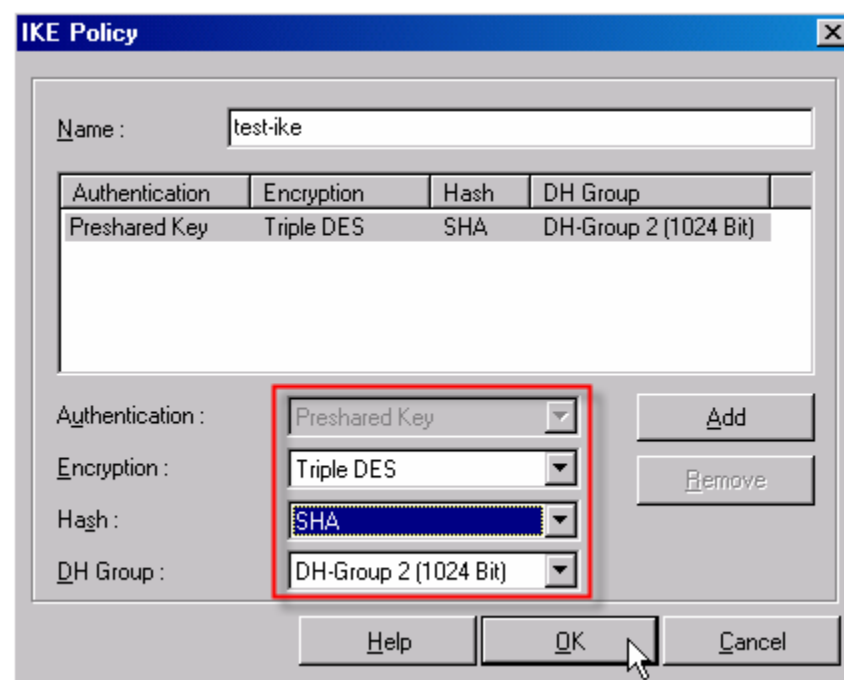
8. Create IKE (phase 1) and IPSec (phase 2) policy. They need to match what you set in the firewall.



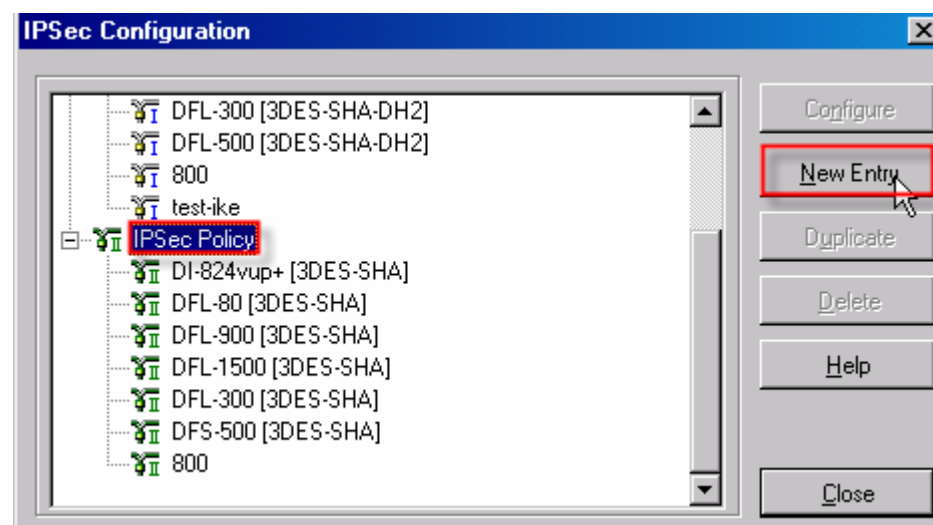
9.



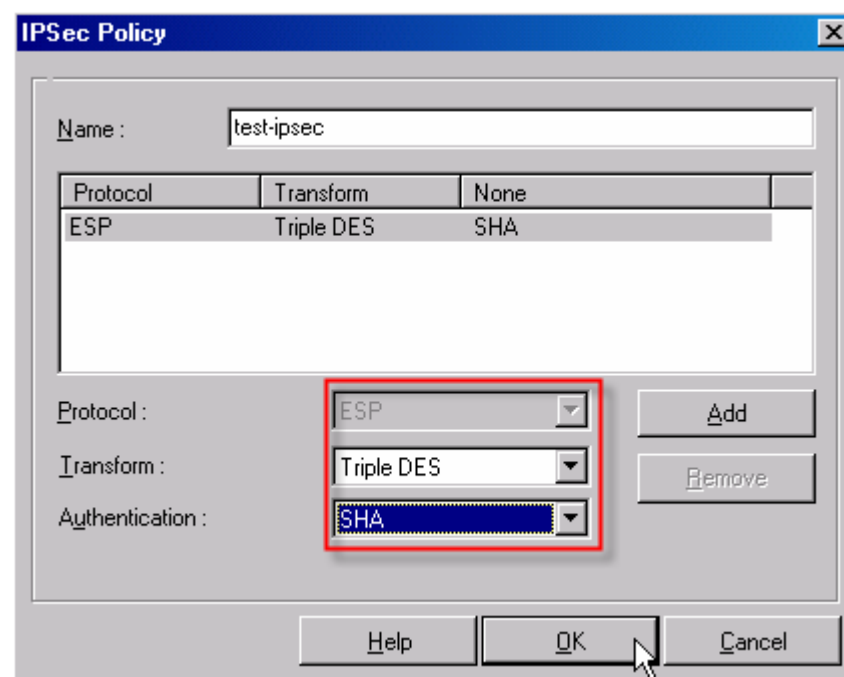
10.



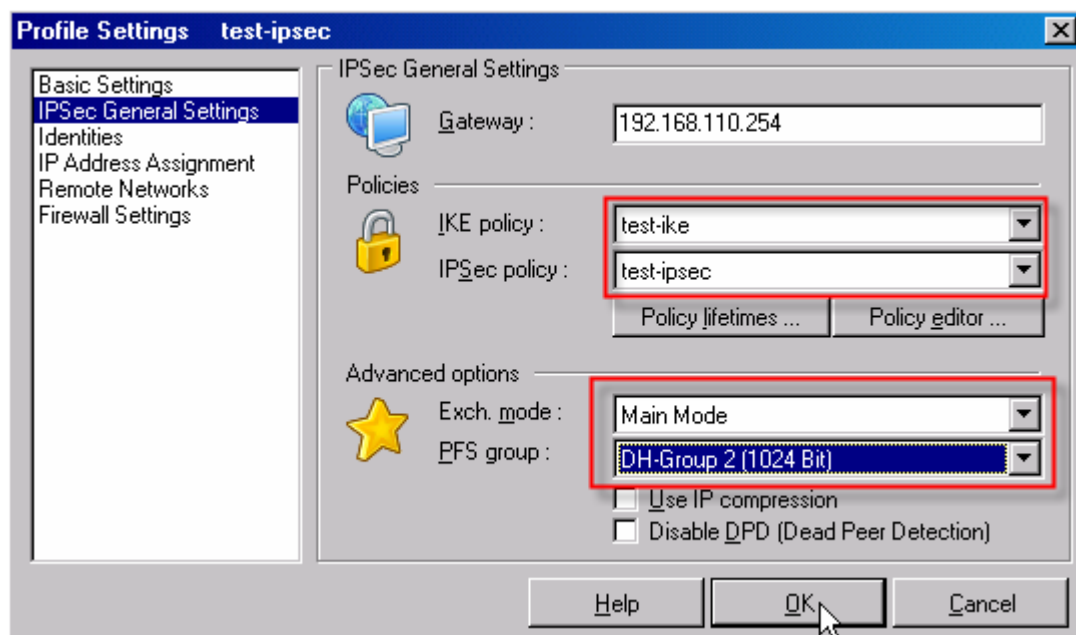
11.



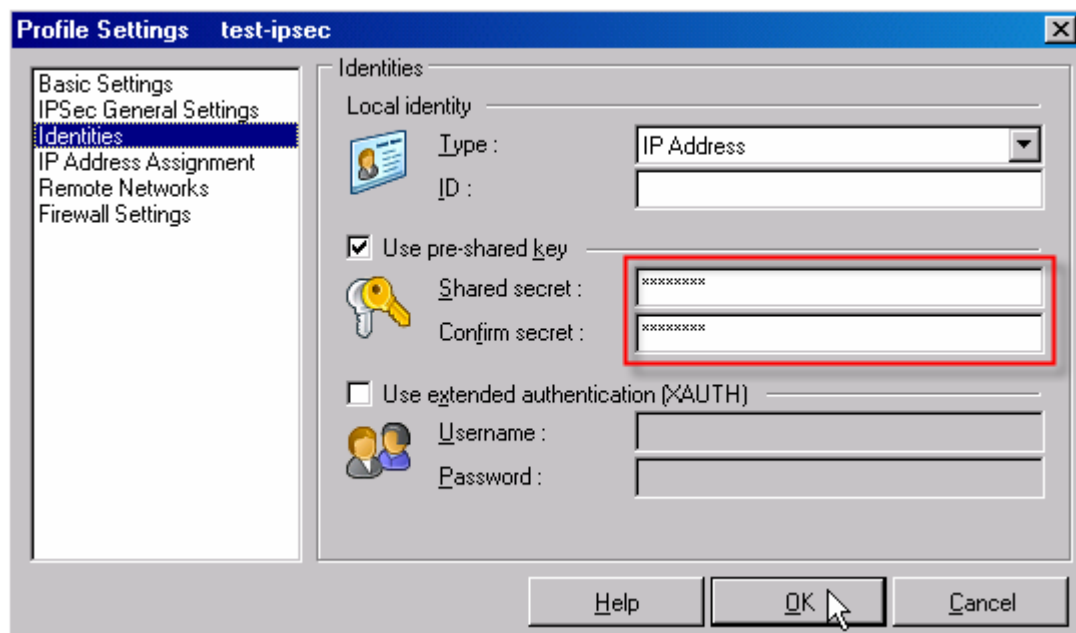
12.



13. Again, these settings have to match what you set in the firewall.



14.



15. Firewall local-net

