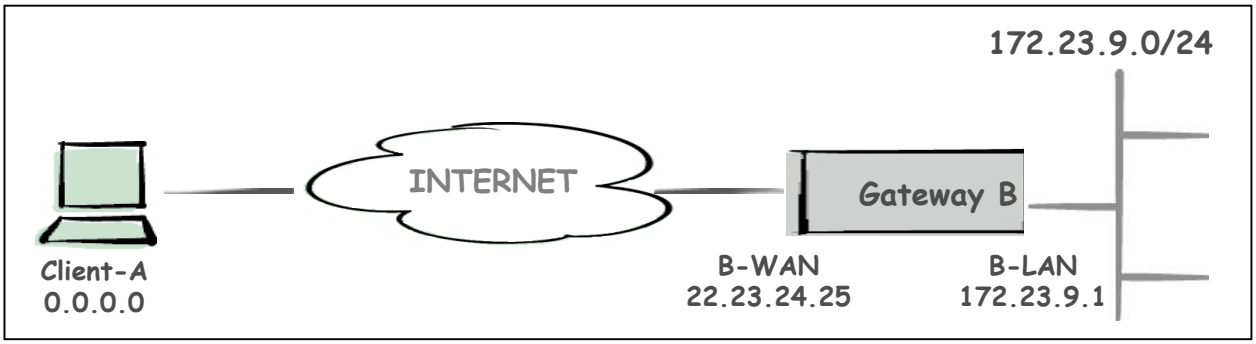
Interoperability Profile for FortiGate-50 with SSH Sentinel VPN Client

The purpose of this document is to provide you with necessary steps to configure SSH Sentinel with remote Fortigate-50 VPN Gateway. This document is based on VPN Consortium's Profile of Interoperability and should help to understand VPN setup scenario. All these configurations has been installed and verified by myself and is for information only.

VPN Client-to-Gateway with pre-shared secrets

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



Client connects to the internal LAN 172.23.9.0/24 via the Internet through Gateway B's WAN Interface 22.23.24.25. Gateway B is configured for RAS clients with dynamic IP addressing. In other configurations static IP addressing could be used, such as LAN, PPPoE and NT RAS connections.

The **IKE Phase 1 parameters** used this Scenario 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 this Scenario 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 0.0.0.0 and 172.23.9.0/24, using IPv4 subnets

Assuming, you have VPN Gateway already configured. If you run this setup from scratch, go the section "VPN GATEWAY CONFIGURATION" and complete installation & configuration before configuring Client.

Products:

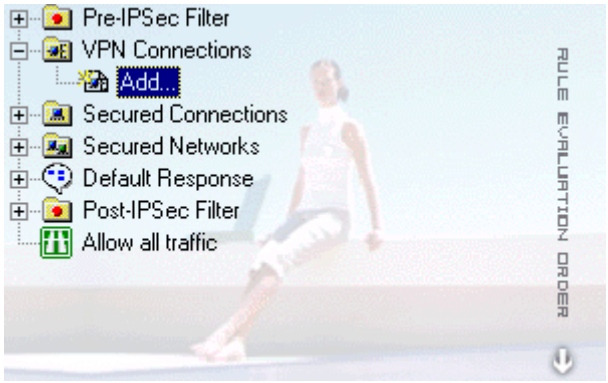
- CLIENT: WIN 2000 Professional & SSH Sentinel 1.4.0.178-30-EVAL
- VPN Gateway: Fortinet FortiGate-50 (Firmware 2.50 Maintenance Release 5)

SSH Sentinel Configuration

The installation of the SSH Sentinel software is easy and straightforward. Start the SSH Sentinel setup program (Fortinet1.4.0.178-30-EVAL.exe) by double-clicking the icon and follow the instructions on the screen. The installation procedure is also well documented in the SSH Sentinel User Manual (available from SSH Sentinel documentation web page).

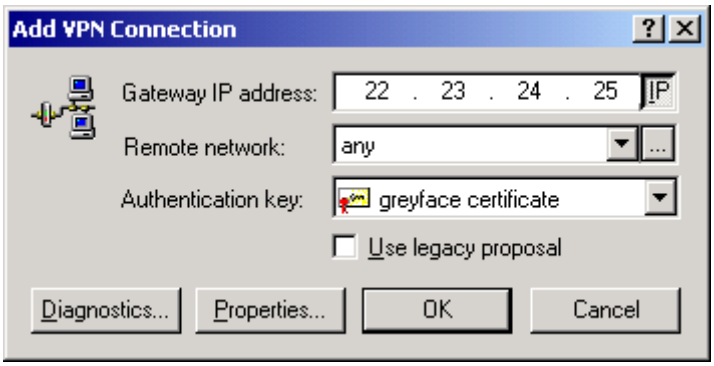
Create a new VPN Connection

1. Right-click on the SSH icon and select Run Policy Editor



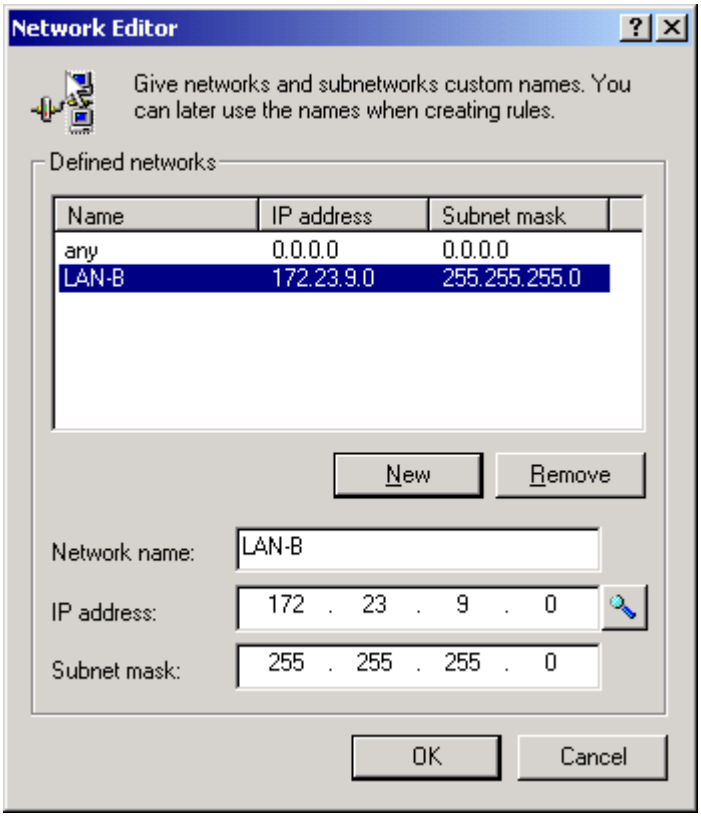
2. Expand VPN Connections by clicking on + , select Add… and click on **ADD**

3. In the add VPN Connection dialog box, click on IP. Gateway Name will change to Gateway IP Address



4. In the Gateway IP address, enter 22.23.24.25 (Gateway-B WAN Address)

5. Select ... to add a new remote network

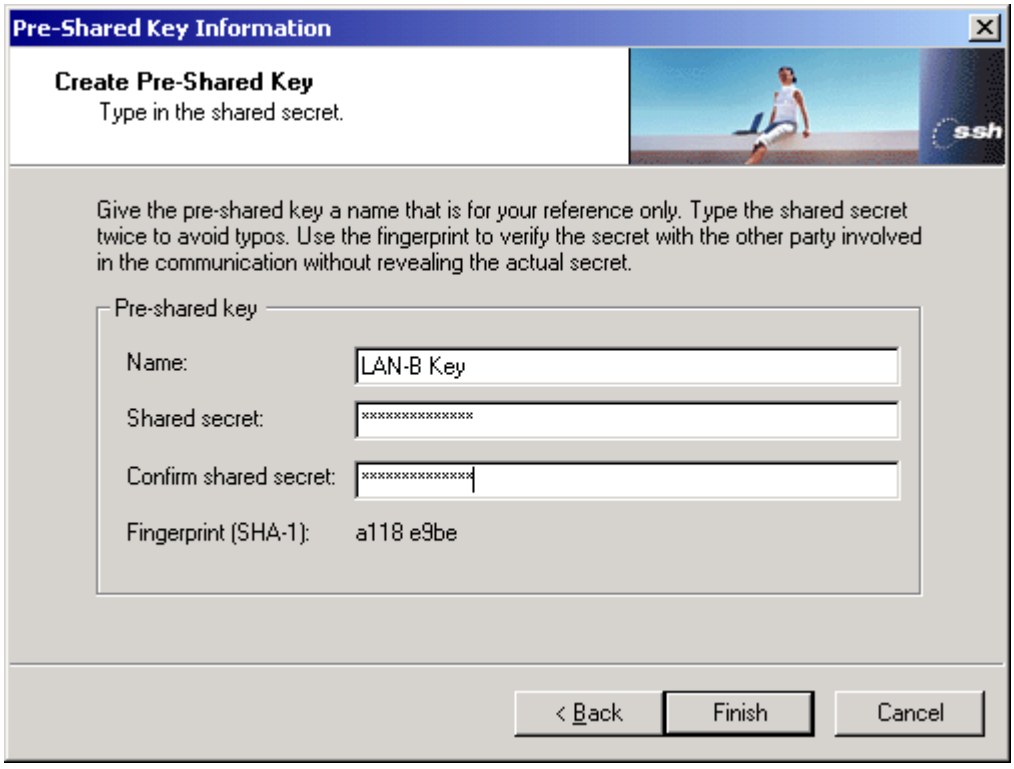


Add pre-shared key to be used during Phase-1 negotiations. The client pre-shared key must match the VPN Gateway authentication key. Typos or different key won't be able to complete Phase-1

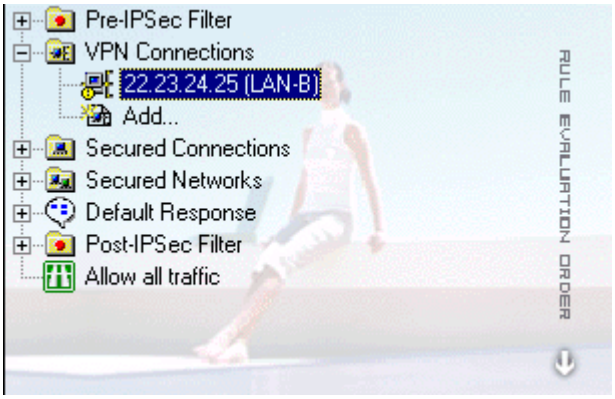
Go to SSH Sentinel Policy Editor -> Key Management -> My Keys

Select **Add**.

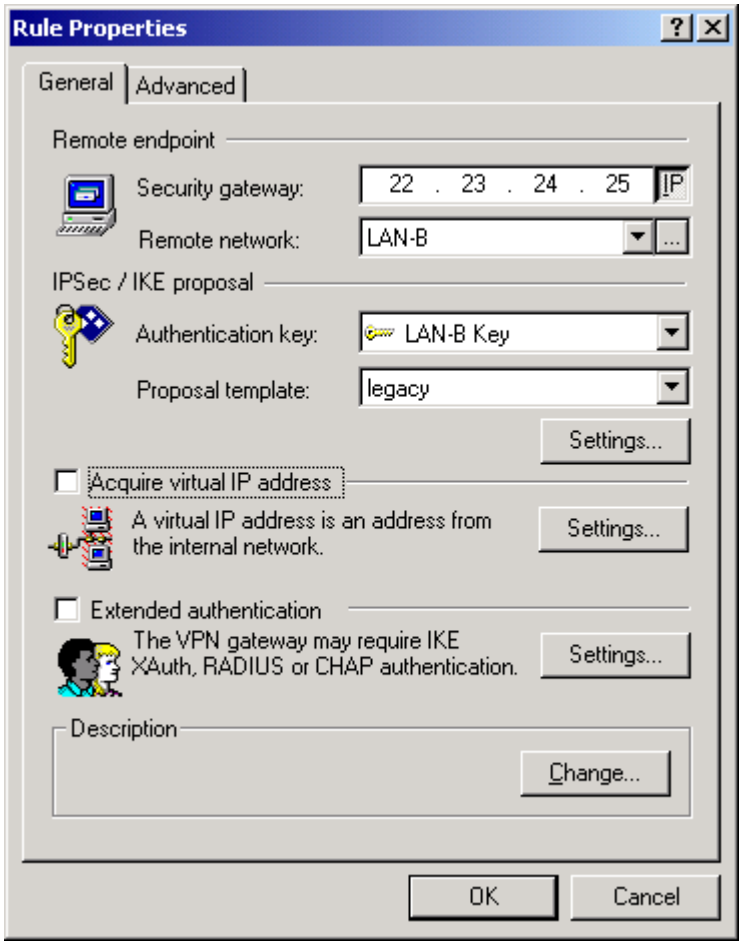
On the New Authentication Key wizard, select Create a pre-shared key. Type a unique name and use the same shared secret, as stated at the first page VPN Consortium's requirement (IKE Phase-1 parameters)



Apply pre-shared key to VPN policy and policy will be updated. Go back to Security Policy and select a newly added VPN Connection (LAN-B)



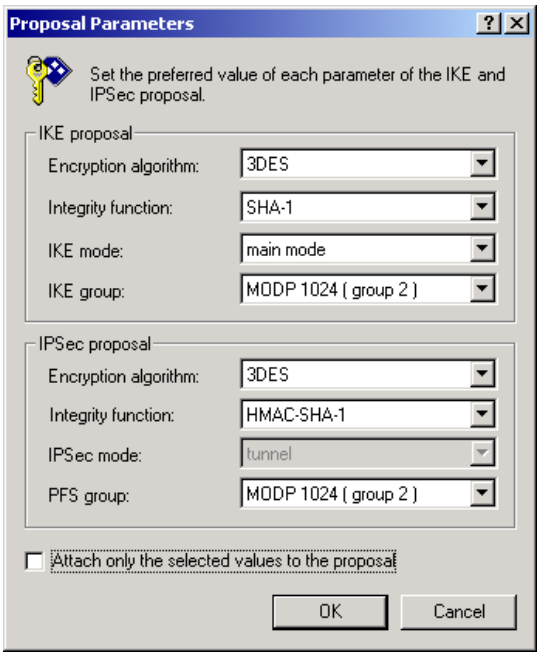
Click on **Properties**



Select the **LAN-B Key** for Authentication Key

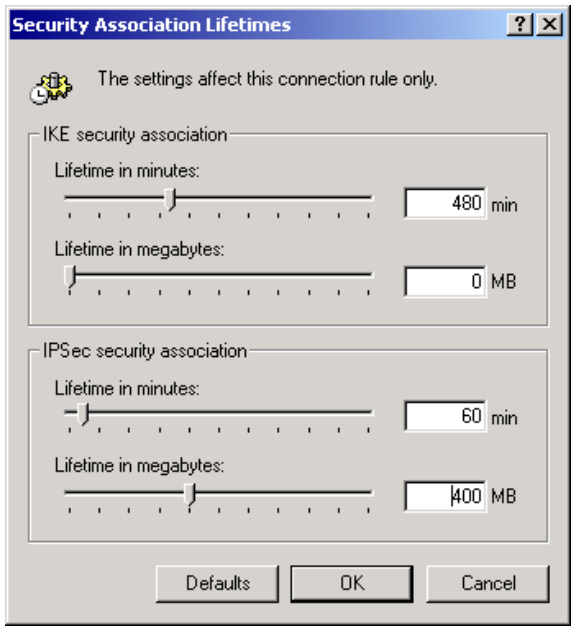
Change Proposal Template to **LEGACY**

Click on SETTINGS under IPSec/IKE Proposal

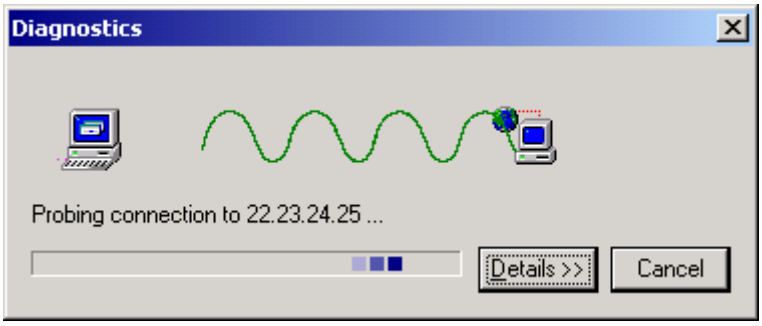


Change the values, based on IKE PHASE-1 requirements.

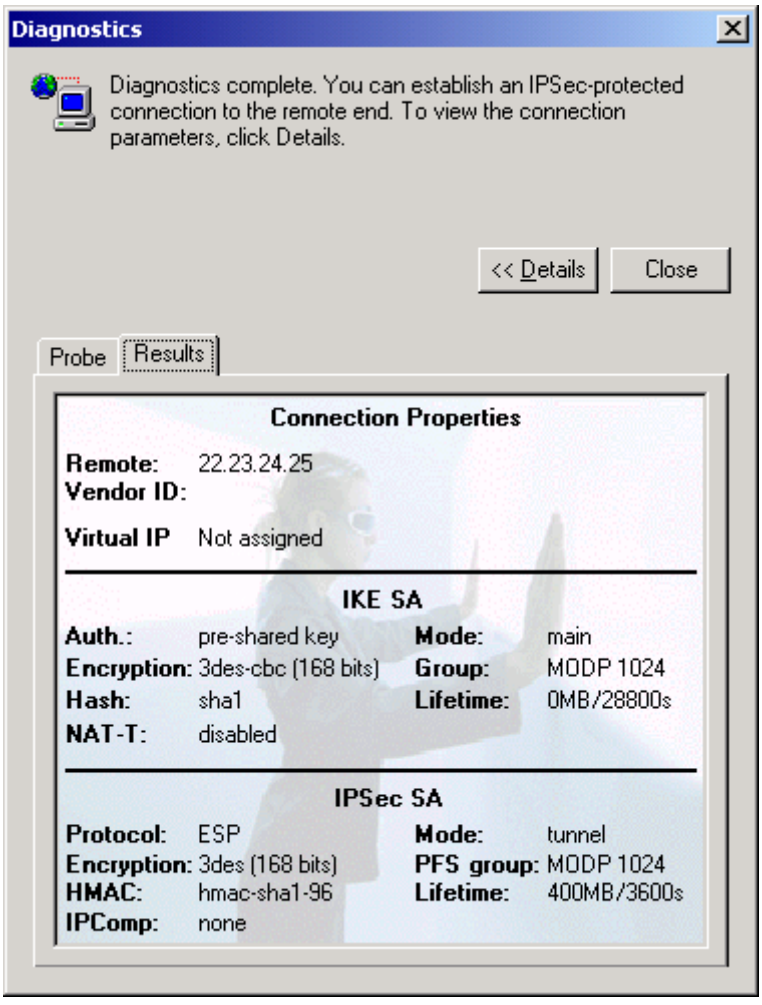
To change the IKE and IPSec re-keying information, select the advanced tab and click on the Settings tab of Security association lifetimes.



Don't forget to Apply, when done. Now you can probe by selecting the VPN Connection and click on Diagnostics.



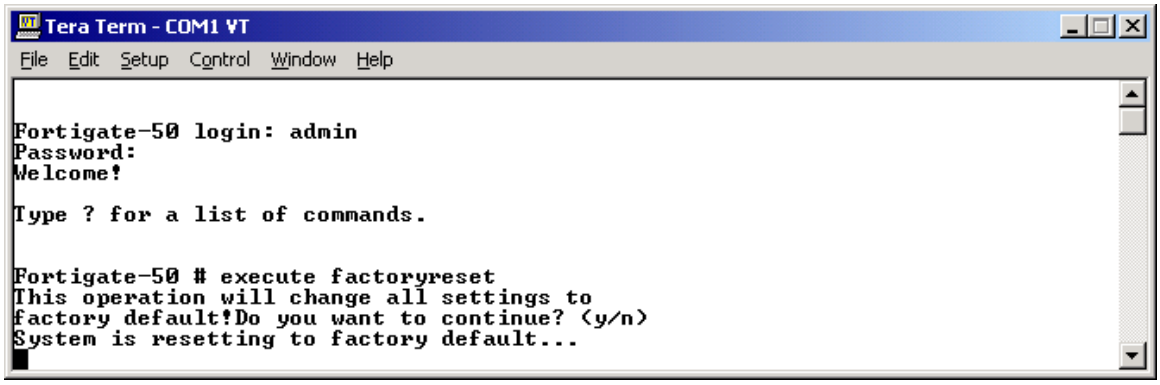
A successful Diagnostics would look like that



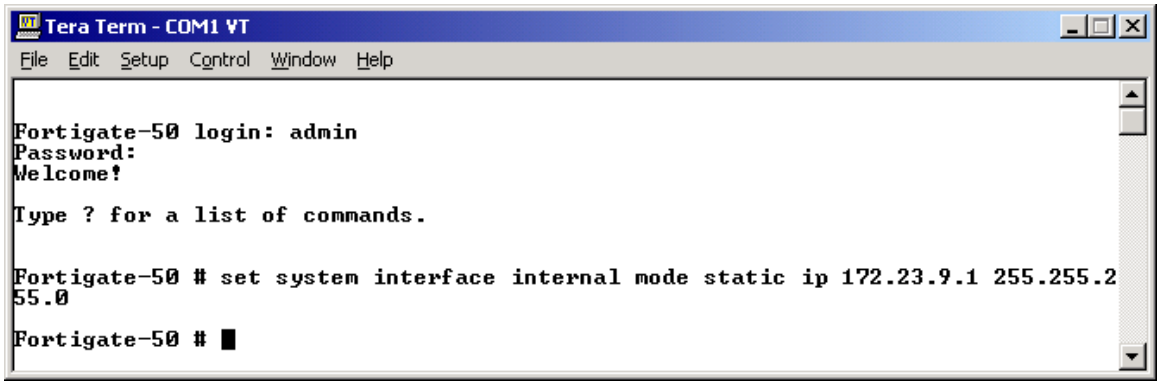
This is a simple setup. You could assign virtual IP and natting as well.

FortiGate-50 Configuration

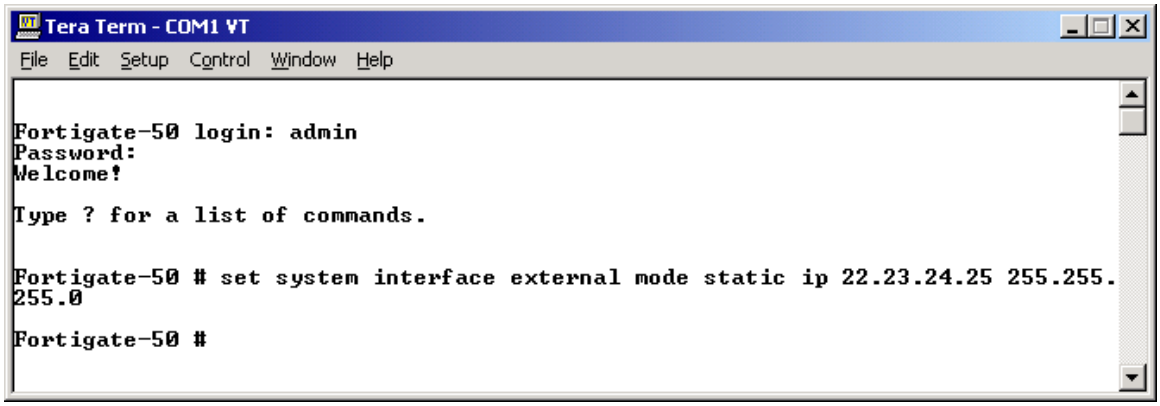
Connect FortiGate with Console Cable, start and logon as admin



When FortiGate has been rebooted, logon and assign internal Interface IP Address (LAN-B)

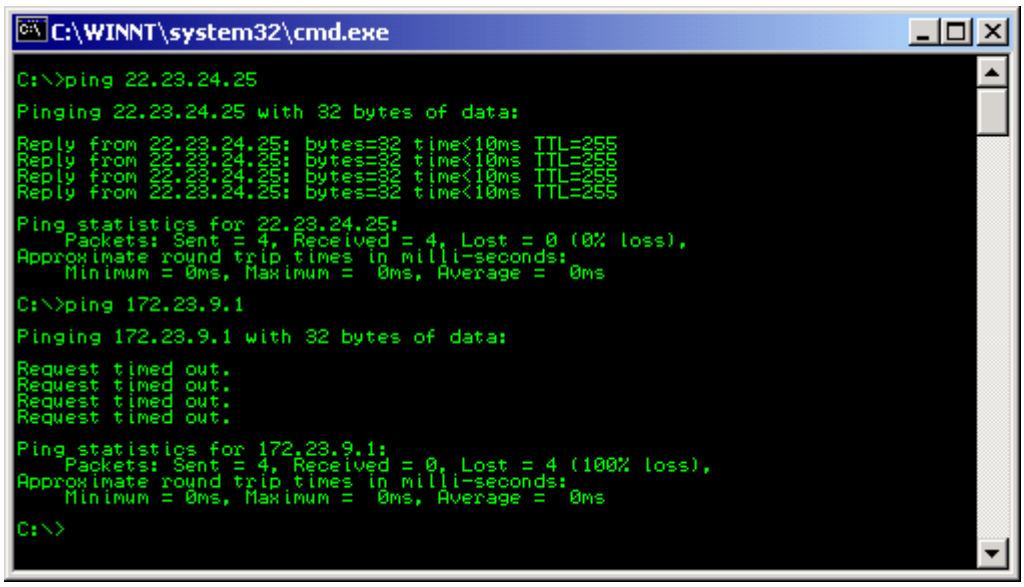


Assign external Interface IP Address (WAN-B)



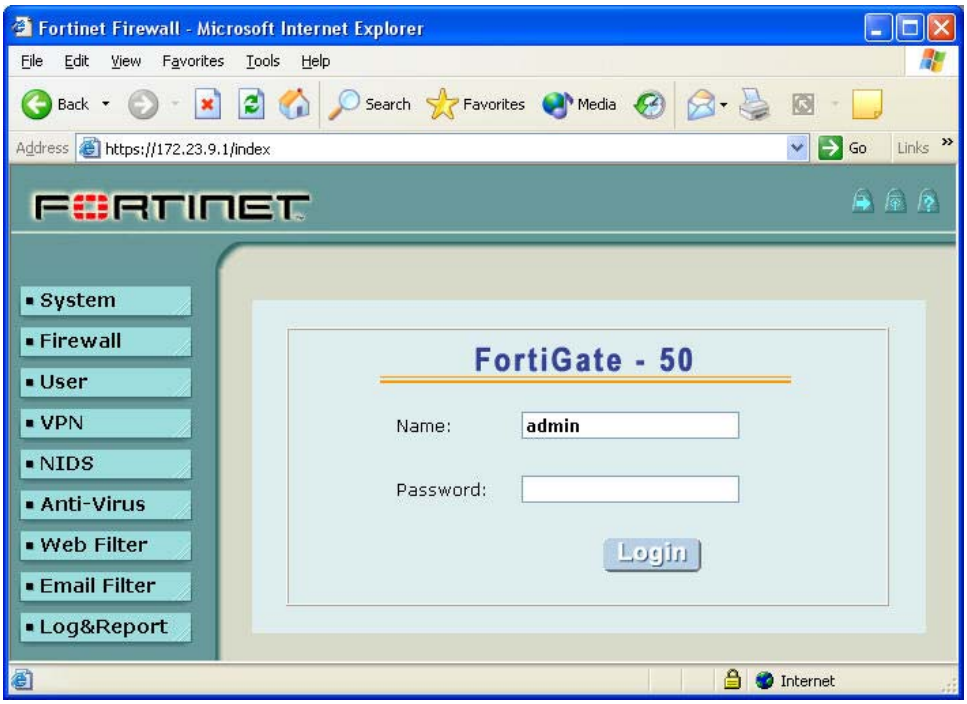
Verify to ping each device to make sure the IP is working.

I have a client connected at WAN interface to see if external interface can be reached and internal interface has been secured.



This is all, you have to do on the console. Everything else can be done via Web Interface.

Configure FortiGate Unit as Dial-Up Server



Logon to FortiGate-50

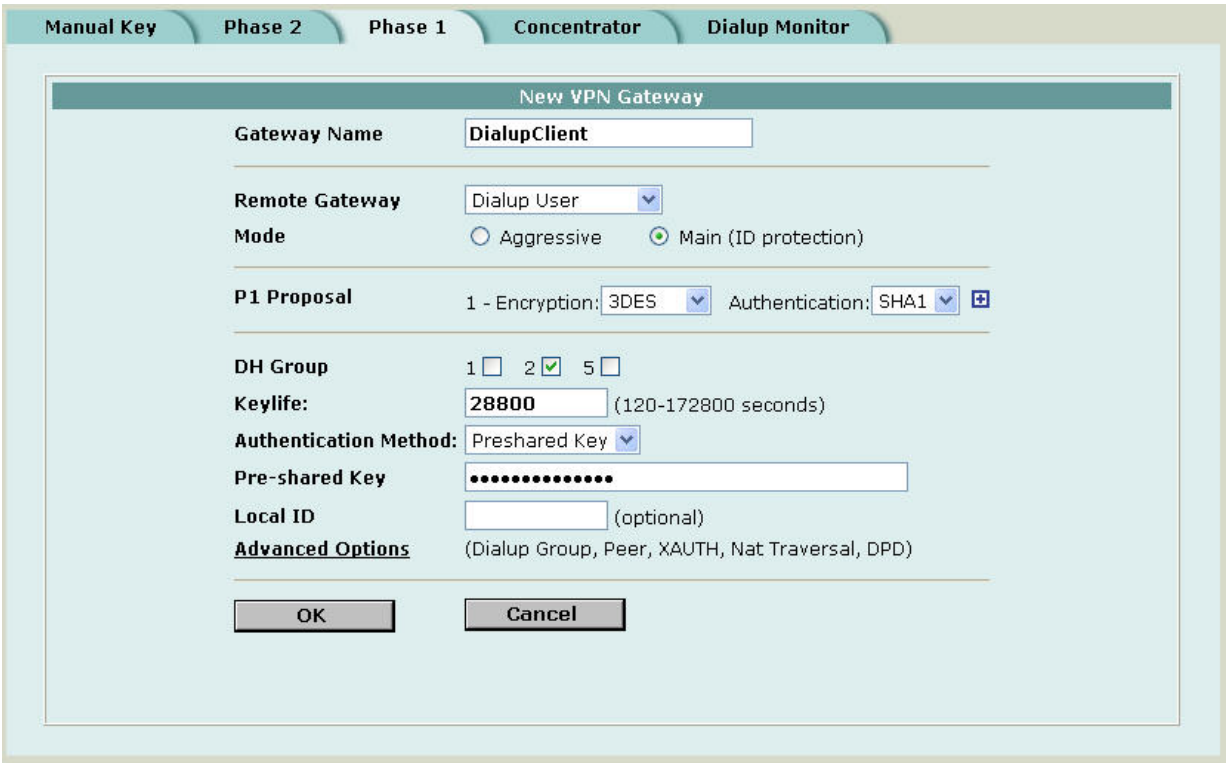
Add a Remote Gateway

1. Go to VPN -> IPSEC -> Phase 1

2. Select New

3. Enter the following information. Everything else can be kept at default

- **Gateway Name:** **DialupClient**
- **Remote Gateway:** **Dialup User**
- **Mode:** **Main (ID Protection)**
- **P1 Proposal:** **1-Encryption 3DES, Authentication SHA1**
- **DH Group:** **2**
- **Keylife:** **28800**
- **Authentication Mode:** **Preshared Key**
- **Pre-shared Key:** **hr5xb84l6aa9r6**



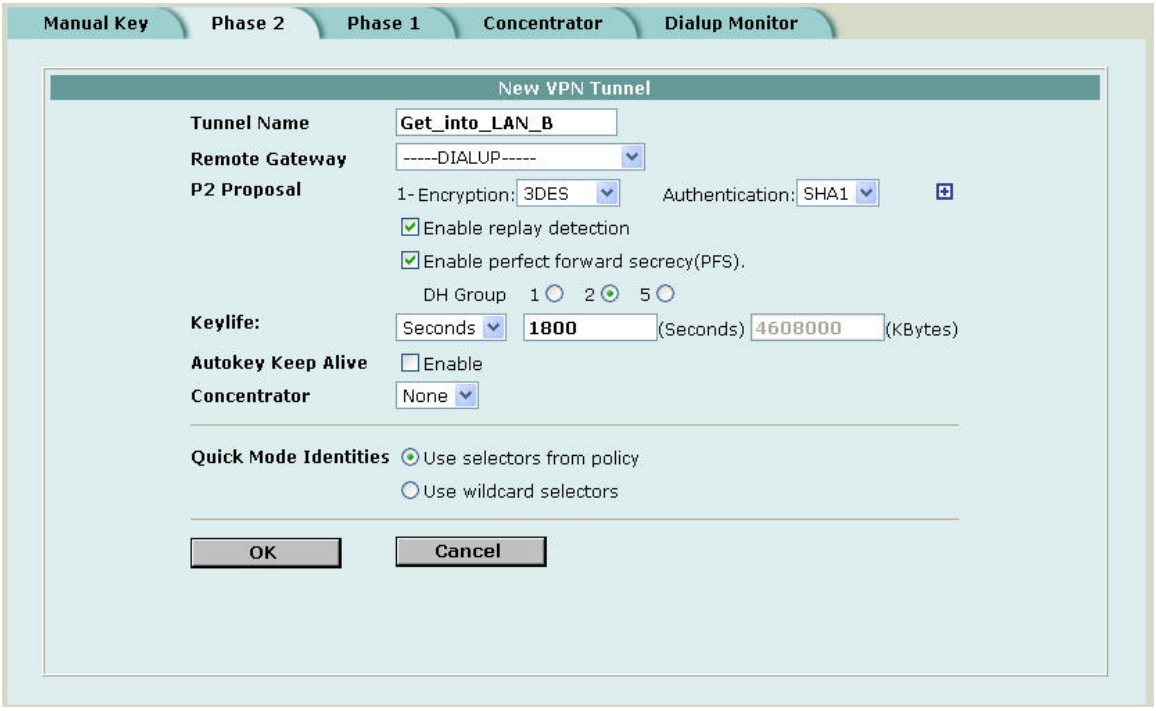
4. Click on **OK**

Add an AutoIKE VPN Tunnel

5. Go to VPN -> IPSEC -> Phase 2

6. Enter the following information. Everything else can be kept at default

- **Tunnel Name:** **Get_into_LAN_B**
- **Remote Gateway:** **----DIALUP----**
- **P2 Proposal:** **1-Encryption 3DES, Authentication SHA1**
- **Replay Detection:** **Disabled**
- **PFS:** **Enabled**
- **DH Group:** **2**
- **Keylife:** **3600**
- **Autokey Keep Alive:** **Disabled**
- **Concentrator:** **None**
- **Quick Mode Identities:** **Use selectors from policy**



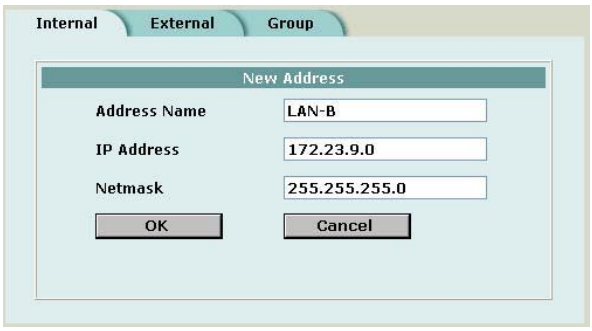
Add a source address to specify the address or address range on the FortiGate internal network that is part of the VPN

7. Go to Firewall -> Address -> Internal

8. Select New

9. Enter the following information

- **Address Name:** **LAN-B**
- **IP Address:** **172.23.9.0**
- **Netmask:** **255.255.255.0**



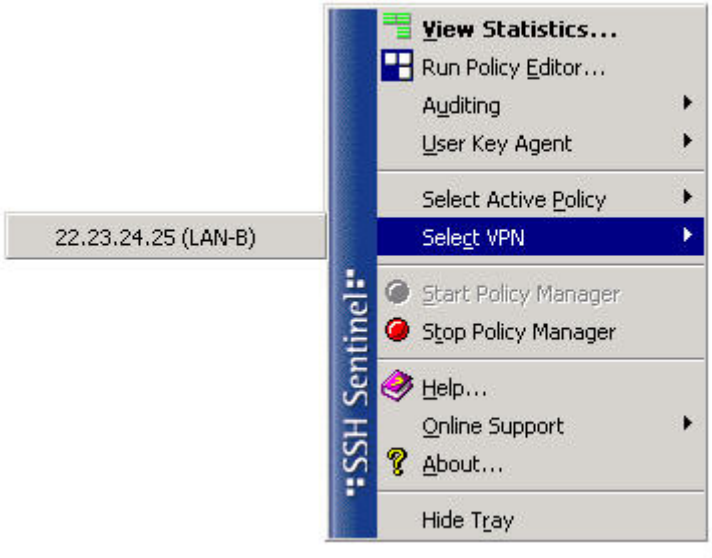
Add an internal to external encrypt policy that includes the source address, the destination address External_All, and the Dial-Up VPN Tunnel

10. Click on **OK**
11. Go to Firewall -> Policy -> Int->Ext.
12. Enter the following information

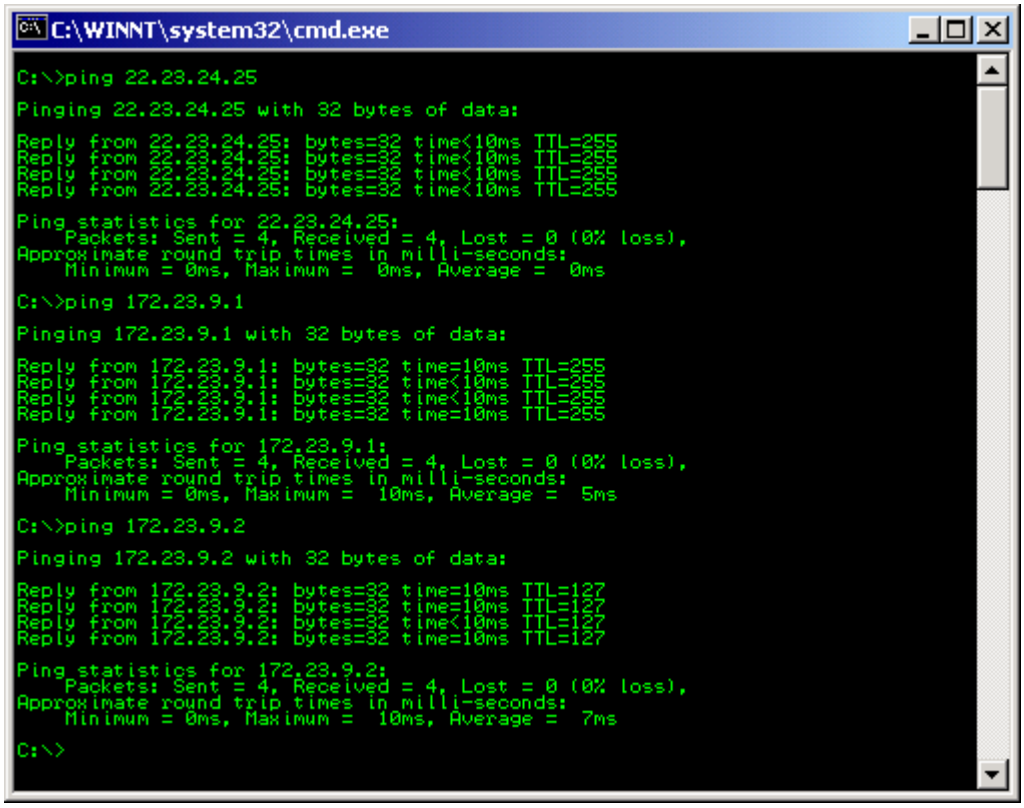
- **Source:** **LAN-B**
- **Destination:** **External_All**
- **Schedule:** **Always**
- **Service:** **Any**
- **Action:** **Encrypt**
- **VPN Tunnel:** **Get_into_LAN_B**
- **Allow inbound:** **Check Allow Inbound to enable inbound users to connect to the source address**
- **Allow outbound:** **Check Allow Outbound to enable outbound users to connect to the destination address**
- **Inbound NAT:** **Uncheck Inbound NAT**
- **Outbound NAT:** **Uncheck Outbound NAT**
- **Traffic Shaping:** **Disabled**
- **Anti-Virus & Web Filter:** **Disabled**
- **Log Traffic:** **Enabled**
- **Comments:** **(none)**

Establish a VPN Connection

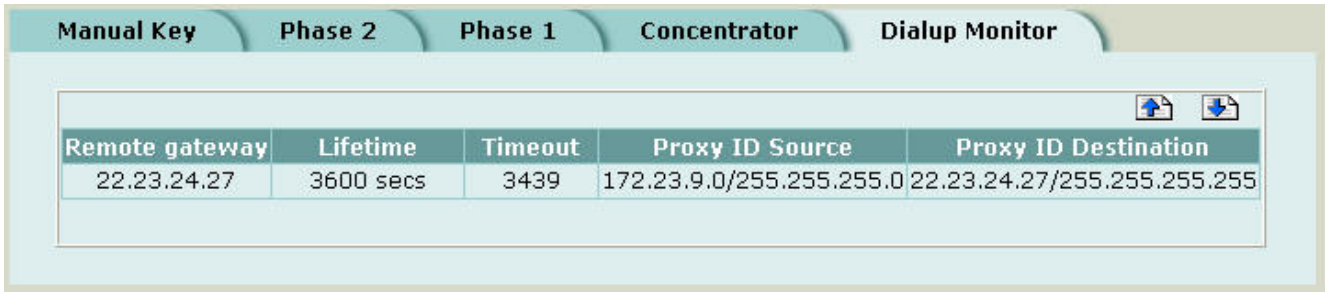
13. Right click on and select VPN "22.23.24.25 (LAN-B)



14. Verify again, if ping works. This time, a host located in LAN B should be positively pinged as well.



On FortiGate's Dialup Monitor, you should see a successful VPN connection



That's pretty much all to do for a successful Client-Gateway VPN with shared Secret.