

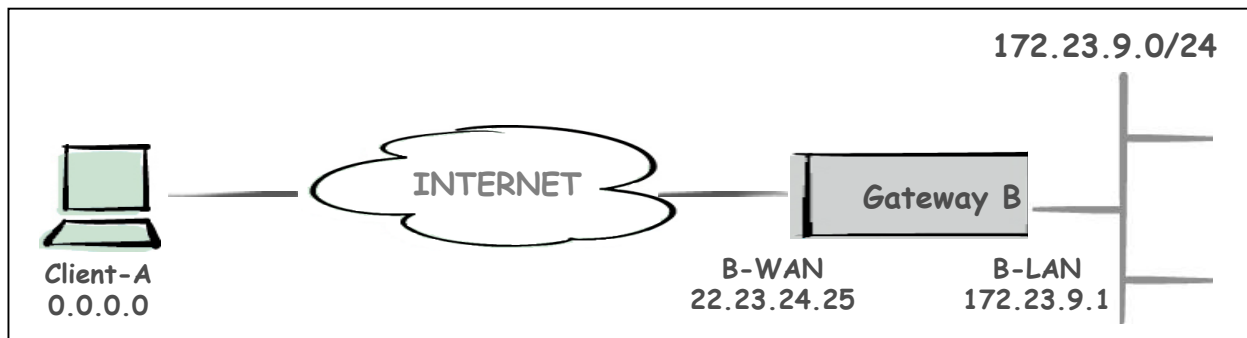


Interoperability Profile for FortiGate-50 with Equinux VPN Tracker

The purpose of this document is to provide you with necessary steps to configure Equinux VPN Tracker 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



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user.

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

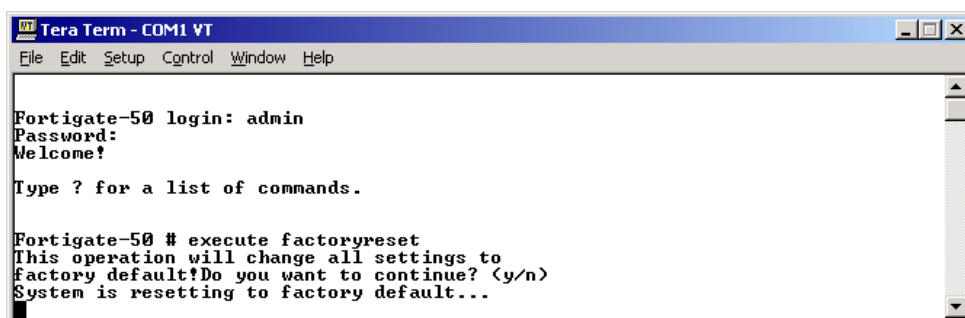
Assuming, you have VPN Gateway already configured. If you run this setup from scratch, go the section “VPN GATEWAY CONFIGURATION” and complete installation & configuration before configuring Client.

Products:

- CLIENT: VPN Tracker 2.2.3 for MAC OS X 10.2 & 10.3
- VPN Gateway: Fortinet FortiGate-50 (Firmware 2.50 Maintenance Release 5)

FortiGate-50 Configuration

Connect FortiGate with Console Cable, start and logon as admin



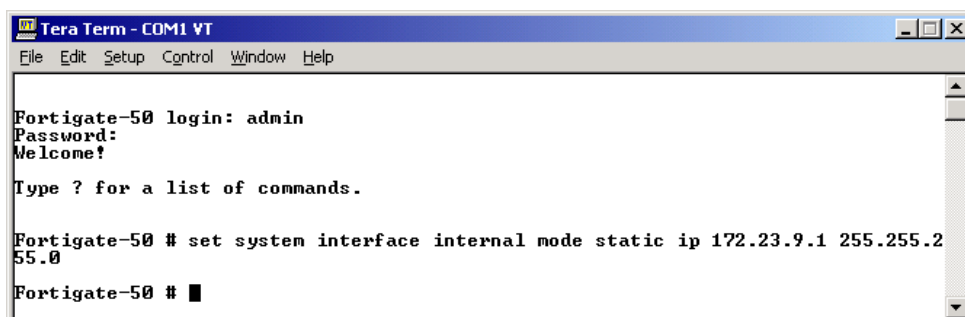
```
Tera Term - COM1 VT
File Edit Setup Control Window Help

Fortigate-50 login: admin
Password:
Welcome!

Type ? for a list of commands.

Fortigate-50 # execute factoryreset
This operation will change all settings to
factory default!Do you want to continue? (y/n)
System is resetting to factory default...
```

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



```
Tera Term - COM1 VT
File Edit Setup Control Window Help

Fortigate-50 login: admin
Password:
Welcome!

Type ? for a list of commands.

Fortigate-50 # set system interface internal mode static ip 172.23.9.1 255.255.2
55.0
Fortigate-50 #
```



Assign external Interface IP Address (WAN-B)

```
Tera Term - COM1 VT
File Edit Setup Control Window Help

Fortigate-50 login: admin
Password:
Melcome!

Type ? for a list of commands.

Fortigate-50 # set system interface external mode static ip 22.23.24.25 255.255.
255.0
Fortigate-50 #
```

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.

```
C:\WINNT\system32\cmd.exe

C:\>ping 22.23.24.25
Pinging 22.23.24.25 with 32 bytes of data:
Reply from 22.23.24.25: bytes=32 time<10ms TTL=255
Reply from 22.23.24.25: bytes=32 time<10ms TTL=255
Reply from 22.23.24.25: bytes=32 time<10ms TTL=255
Reply from 22.23.24.25: bytes=32 time<10ms TTL=255
Ping statistics for 22.23.24.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

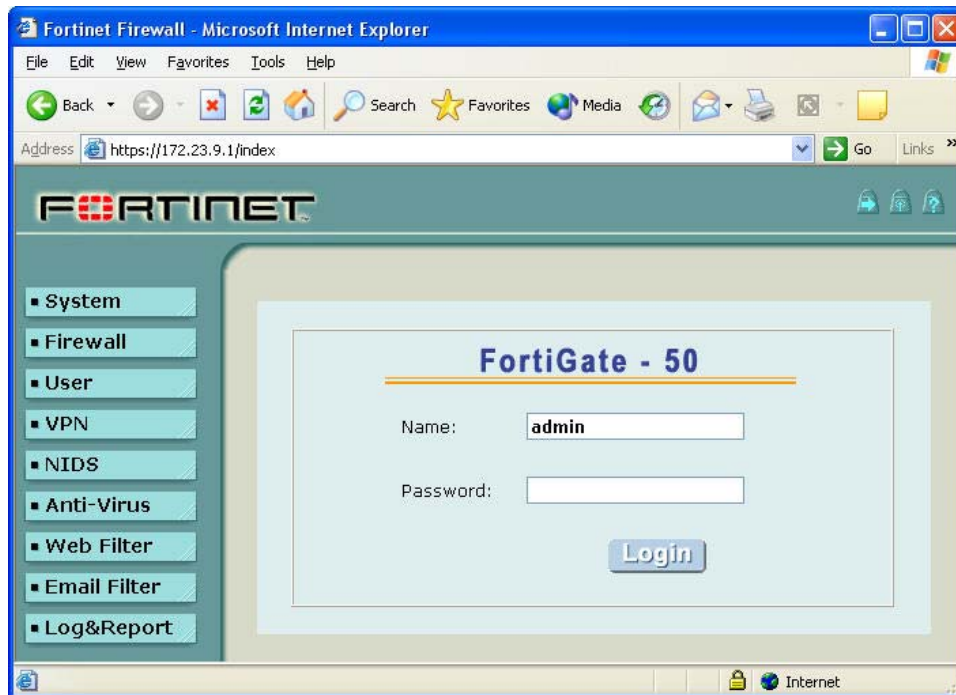
C:\>ping 172.23.9.1
Pinging 172.23.9.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.23.9.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

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



Manual Key Phase 2 Phase 1 Concentrator Dialup Monitor

New VPN Gateway

Gateway Name:

Remote Gateway:

Mode: Aggressive Main (ID protection)

P1 Proposal: 1 - Encryption: Authentication:

DH Group: 1 2 5

Keylife: (120-172800 seconds)

Authentication Method:

Pre-shared Key:

Local ID: (optional)

Advanced Options (Dialup Group, Peer, XAUTH, Nat Traversal, DPD)

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



New VPN Tunnel

Tunnel Name:

Remote Gateway:

P2 Proposal: 1-Encryption: Authentication:

Enable replay detection

Enable perfect forward secrecy(PFS).

DH Group: 1 2 5

Keylife: (Seconds) (KBytes)

Autokey Keep Alive: Enable

Concentrator:

Quick Mode Identities: Use selectors from policy
 Use wildcard selectors

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

New Address

Address Name:

IP Address:

Netmask:



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)

The screenshot shows the 'New Policy' configuration window for an Int->Ext policy. The configuration is as follows:

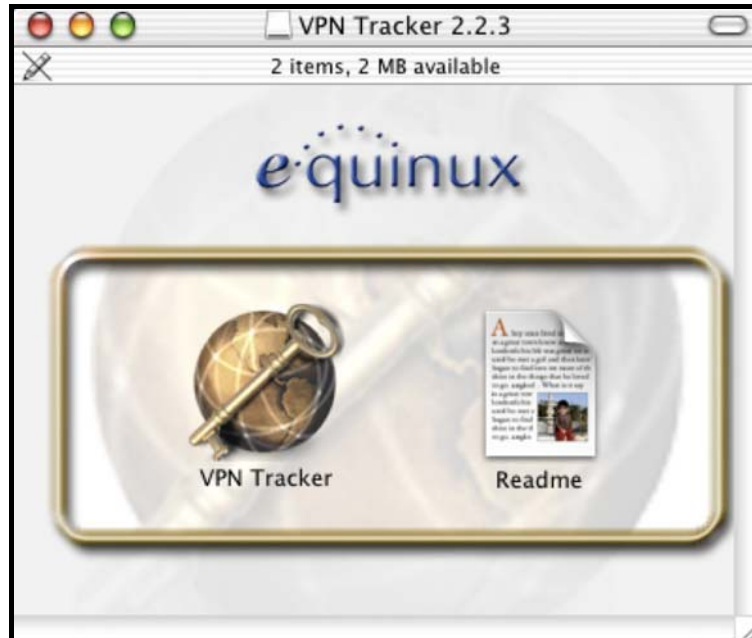
Field	Value
Source	LAN-B
Destination	External_All
Schedule	Always
Service	ANY
Action	ENCRYPT
VPN Tunnel	Get_into_LAN_B
Allow inbound	<input checked="" type="checkbox"/>
Allow outbound	<input checked="" type="checkbox"/>
Inbound NAT	<input type="checkbox"/>
Outbound NAT	<input type="checkbox"/>
Traffic Shaping	<input type="checkbox"/>
Guaranteed Bandwidth	0 (KBytes/s)
Maximum Bandwidth	0 (KBytes/s)
Traffic Priority	High
Anti-Virus & Web filter	<input type="checkbox"/>
Content Profile	Strict



Installing VPN Tracker

If you haven't downloaded the evaluation package, go to www.equinux.com.

Double-click on VPN_Tracker__2.2.3.dmg



Click on **VPN Tracker**

Authenticate to have proper right to install the application



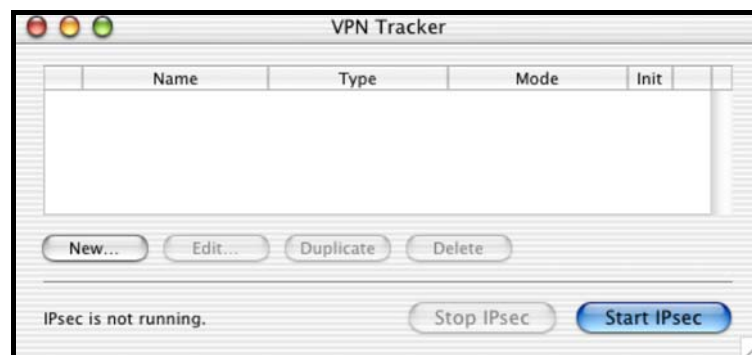
Enter Password or phrase and click on **OK**




If you are running the demo version, you should get following notification.



Click on **DEMO**



Next, you will have to add a new connection. Click on **NEW**.

All settings are greyed out. Click on  to unlock for making changes. You will be asked to Authenticate with your passphrase.

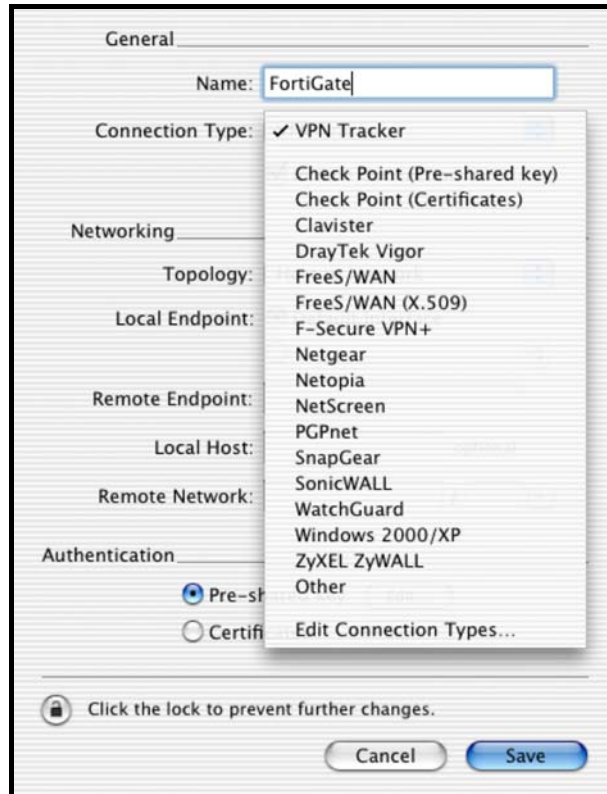


You are now ready to add values for the new connection type.

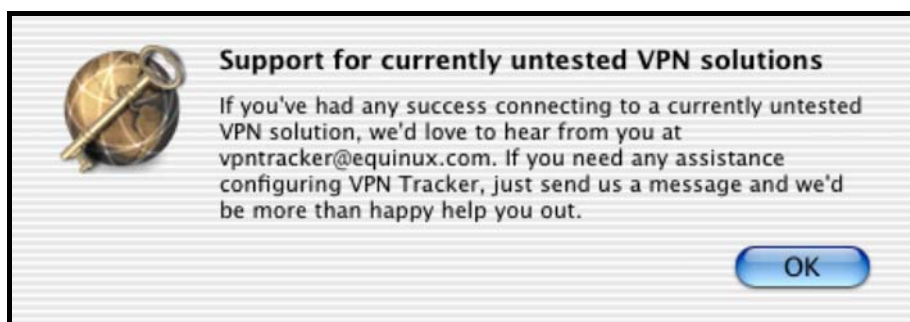


Add New Connection

Type a Name of your new connection and choose from Connection Type “**Other**” from the Pull-Down Menu.



This is for all untested VPN solutions. With VPN Tracker 2.2.3, there is no predefined setting for Fortigate.



Click on **OK**



Type IP Address of Remote Endpoint and Remote Network

General

Name: FortiGate

Connection Type: Other

Initiate connection

Networking

Topology: Host to Network

Local Endpoint: Default Interface

Remote Endpoint: 22.23.24.25

Local Host: optional

Remote Network: 172.23.9.0 / 24

Authentication

Pre-shared key Edit...

Certificates Edit...

Click the lock to prevent further changes.

Cancel Save

Click on **EDIT** of Pre-shared key. By removing the checkmark of “**HIDE TYPING**”, you can see real values, as VPN Tracker does not offer a **COMPARE** feature

Pre-shared Key

hr5xb8416aa9r6

Hide typing

Enter key when establishing connection
The key will not be saved on disk.

Local Identifier

Local endpoint IP address

Remote Identifier

Remote endpoint IP address

Verify remote identifier

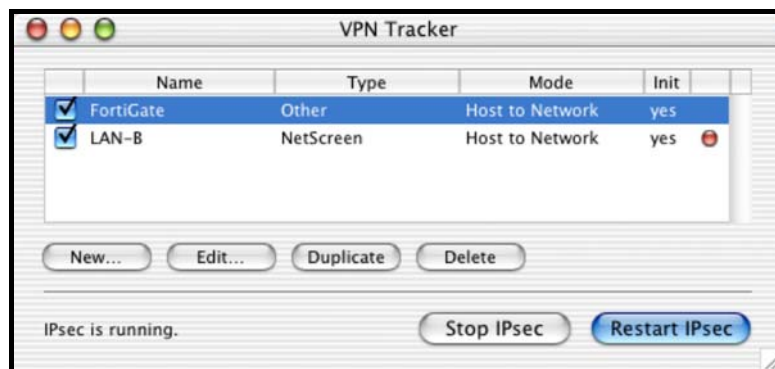
Cancel OK

Click on **OK** and **SAVE**. You might be asked again to authenticate for saving this connection



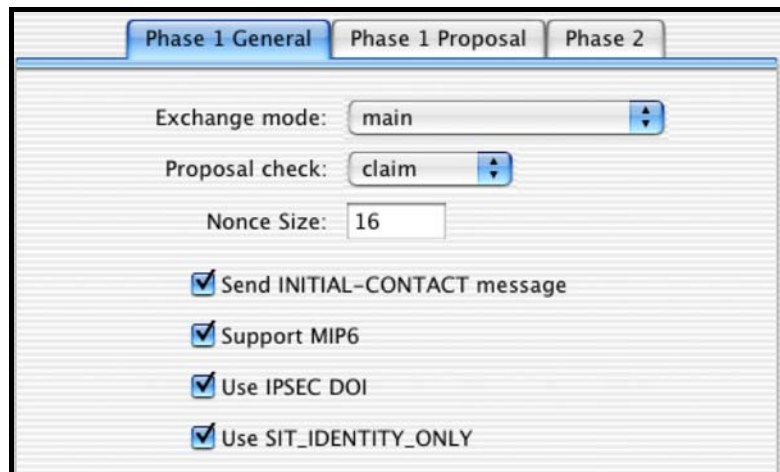


There are some settings you have to change to make sure all parameters are equal between Client and VPN Gateway



Highlight the new Connection and click on **EDIT**

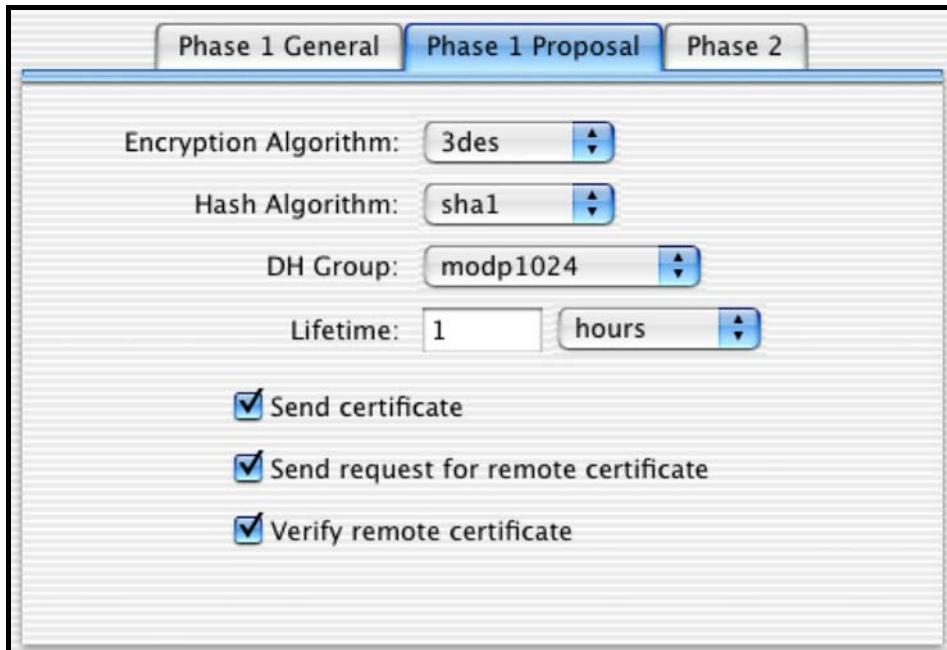
Go to Connection Type and choose from Pull Down Menu **EDIT CONNECTION TYPE**



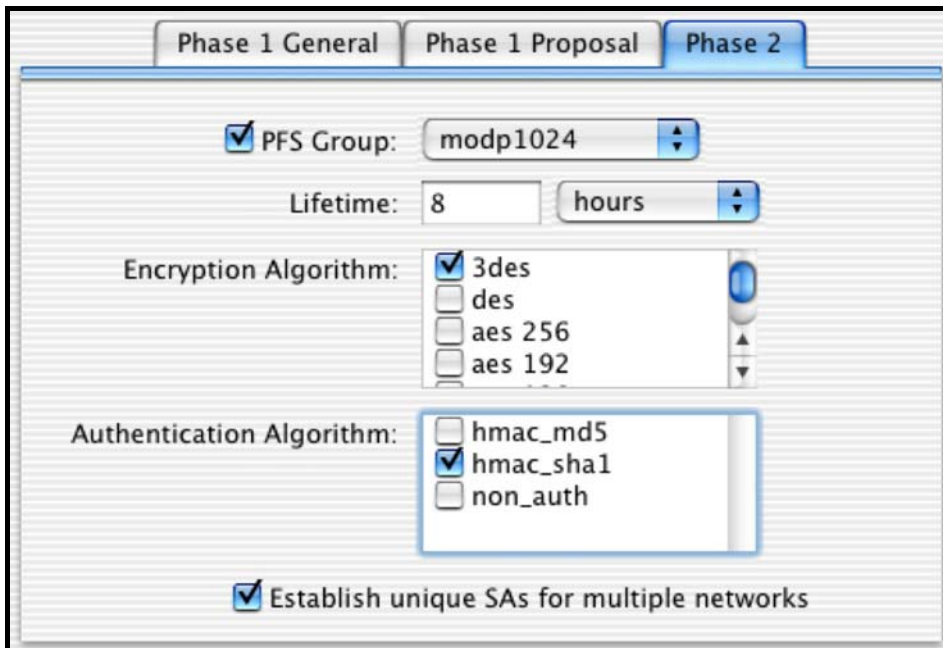
Change Exchange Mode to **MAIN** on Phase 1 General



On Phase 1 Proposal, change Encryption Algorithm to **3des** , Hash Algorithm to **sha1** and DH Group to **modp1024**



On Phase 2 make sure, that only **3des** & **hmac_sha1** is check-marked

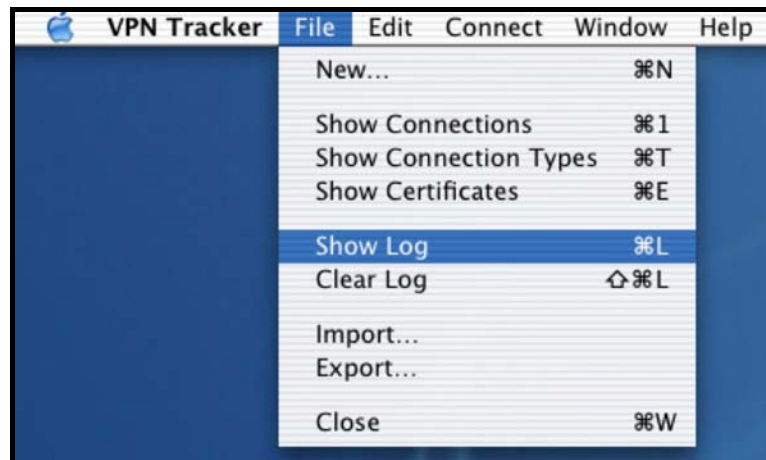


Click on SAVE and  to close the window

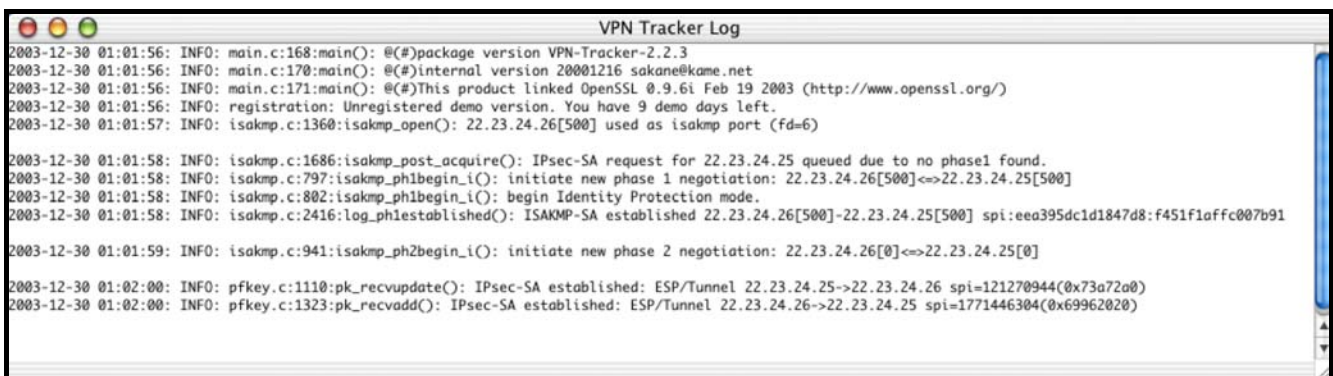


Finally click on **SAVE** again

Open Log Window from **FILE**

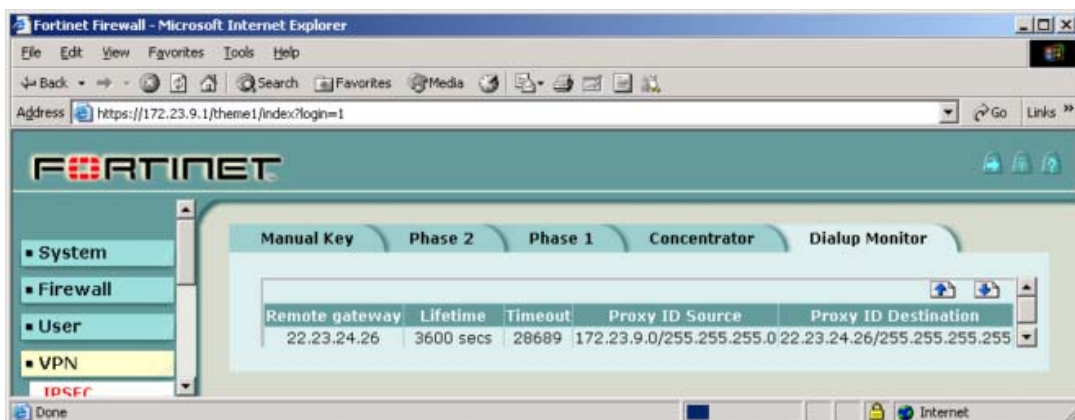


Checkmark FortiGate Connection only and click on **RESTART IPsec**



On Fortigate Web Interface, log on and click on VPN – IPSEC – Dialup Monitor.

You should see an entry of the new remote gateway (in this case 22.23.24.26, which is my VPN Client)



On MAC OS X Dock, you should see a lock which indicates an established IPsec connection.



That's pretty much all to do for a successful Client-Gateway VPN with shared Secret. Check out my website for more Sample Instructions to come.

www.bemsel.com/techtips

