

Official Tech Documents
The better way to get your HotBrick product up and running

HotBrick VPN Client

How To

How to establish a VPN tunnel using the HotBrick VPN client with a 401VPN

USA

7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

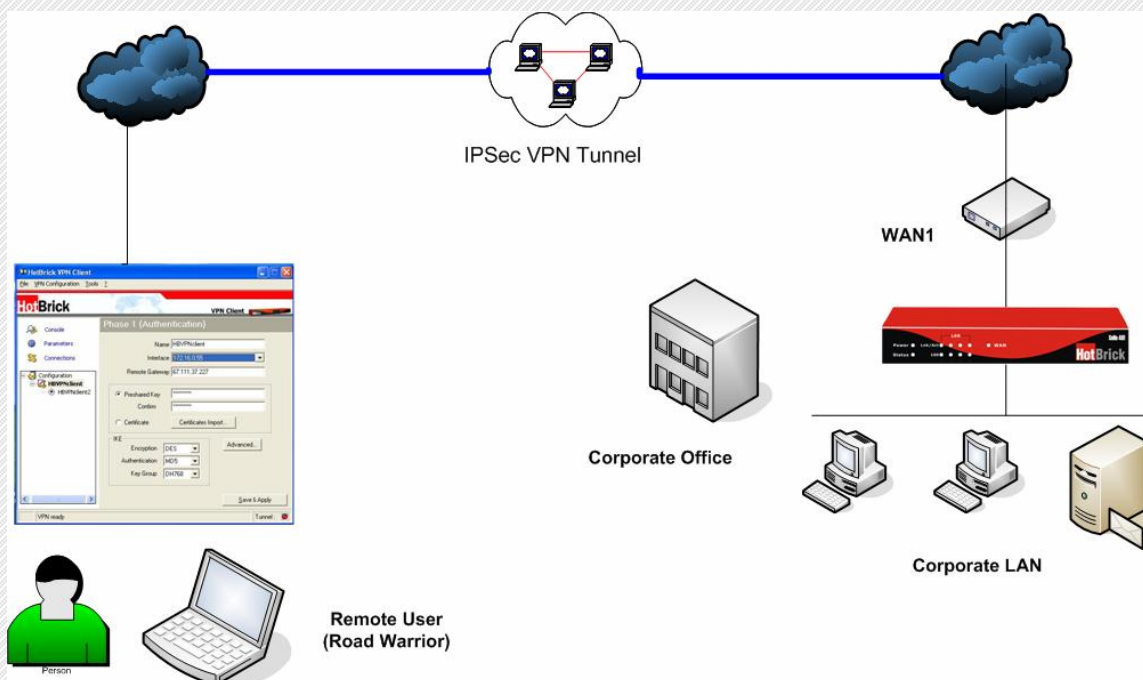
EUROPE

Generatorstraat 26
Hengelo (Ov), 7556 RC
Amsterdam - Netherlands
www.hotbrick.nl
support@hotbrick.nl

BRAZIL

Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

How to establish a VPN tunnel using the HotBrick VPN client with a 401VPN



This setup guide will let a client use the HotBrick VPN to connect to the 401VPN from any location with an internet connection. This is accomplished by using a Fully Qualified Username (example: support@hotbrick.com) for the remote user.

HotBrick VPN Client Setup

1. After you launch the HotBrick VPN client right on the Configuration and select "New Phase 1". Please see figure 1.

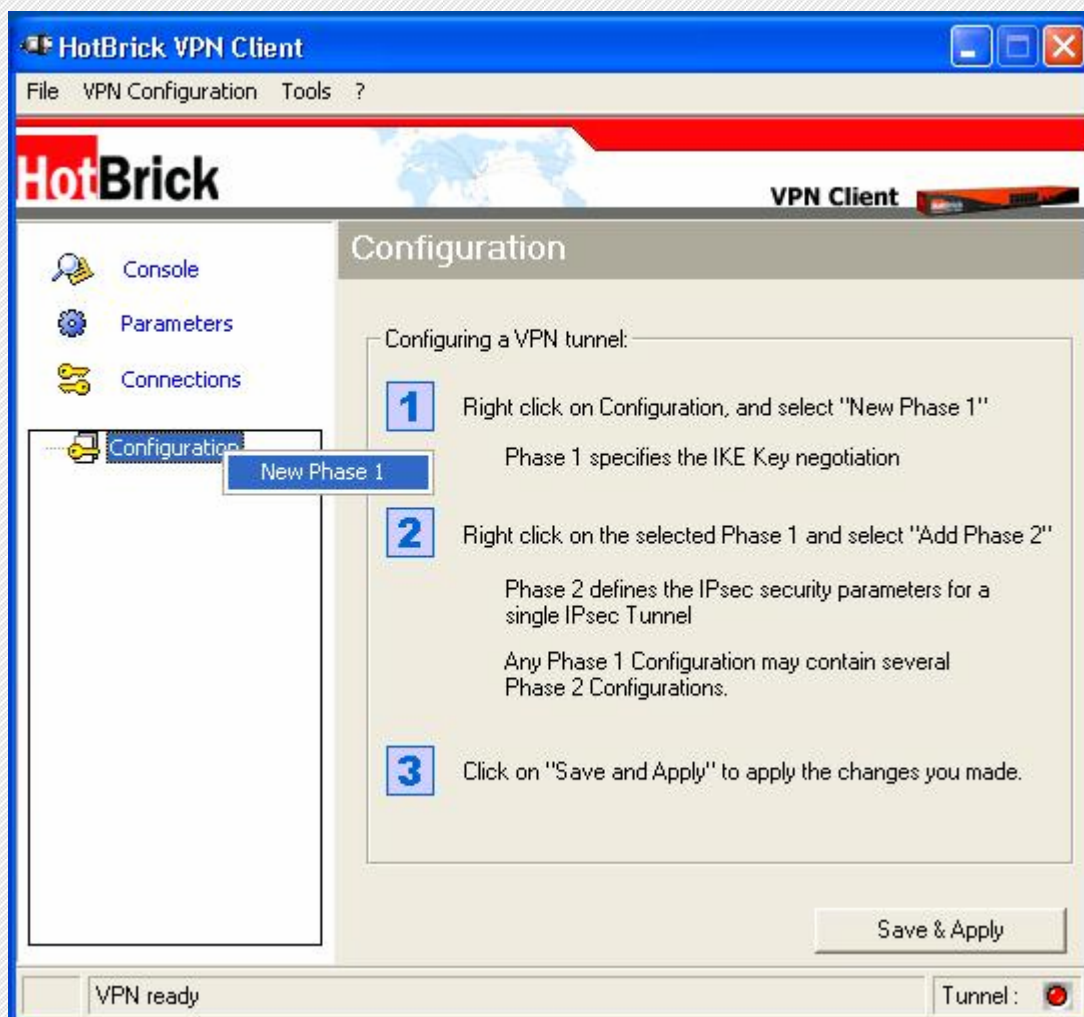


Figure 1 - Configuration Screen

- a. Enter a name for the Phase 1; our example is "test401VPN".
- b. The **Interface** is the Client side IP address (Your PC IP Address ex. 192.168.2.59).
- c. The **Remote Gateway** is the Remote IP address of the LB-2 VPN (67.111.37.232).
- d. Enter the Pre-shared Key for the VPN session.
- e. Enter the IKE parameters (ex. 3DES, MD5, and DH768 which is DHGroup1)
- f. Hit the "Save & Apply" button.
- g. Please see figure 2 below.

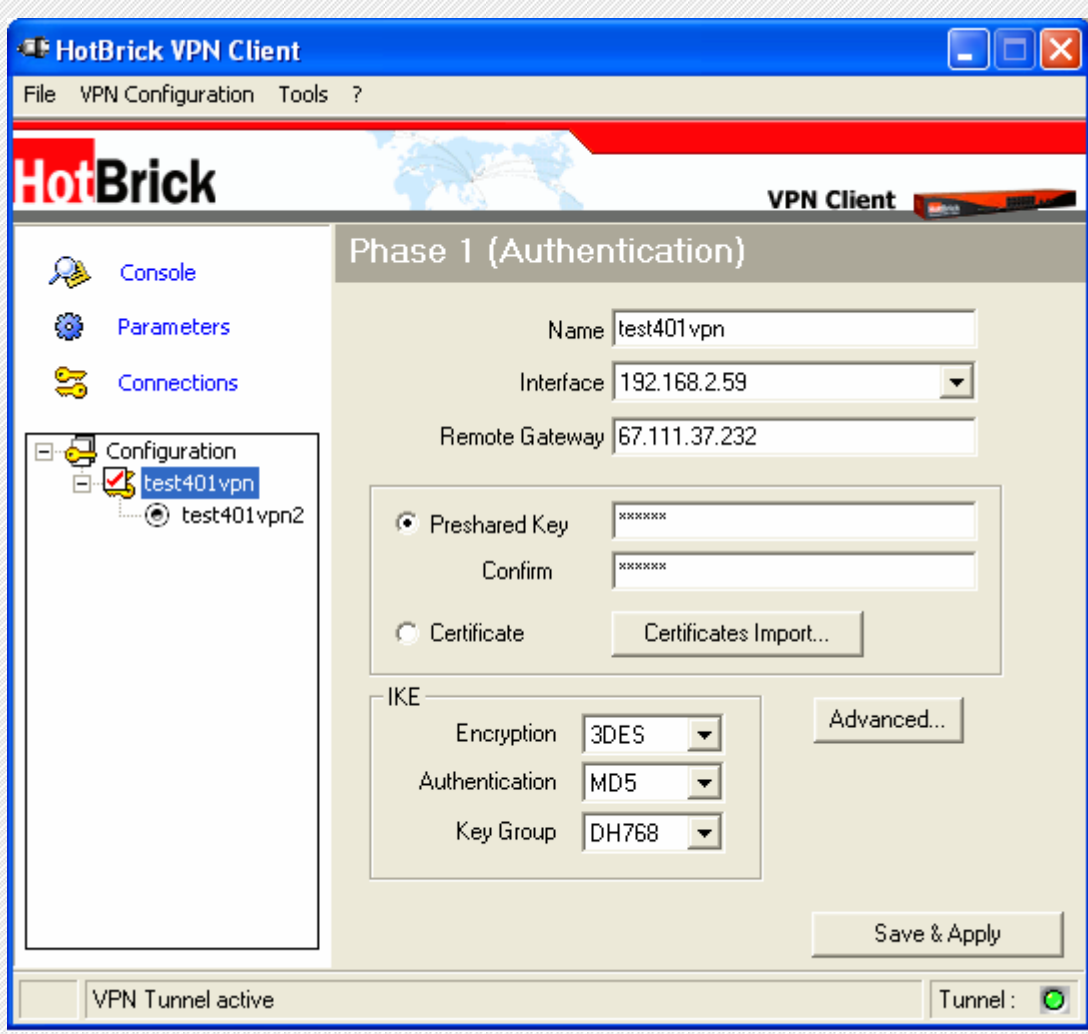


Figure 2 - Phase 1 (Authentication)

2. Now click on the advanced button and check "Aggressive Mode" and under "IKE Port" input 500.
 - a. Under Local ID, Value input your email address. (Ex: support@hotbrick.com)
 - b. Under Type, please select Email
 - c. Under Remote ID, Value input IP address (Ex: 67.111.37.232)
 - d. Under Type, please select IP Address
 - e. When you are finished click OK.
 - f. Hit the "Save & Apply" button.
 - g. Please see figure 3 below.

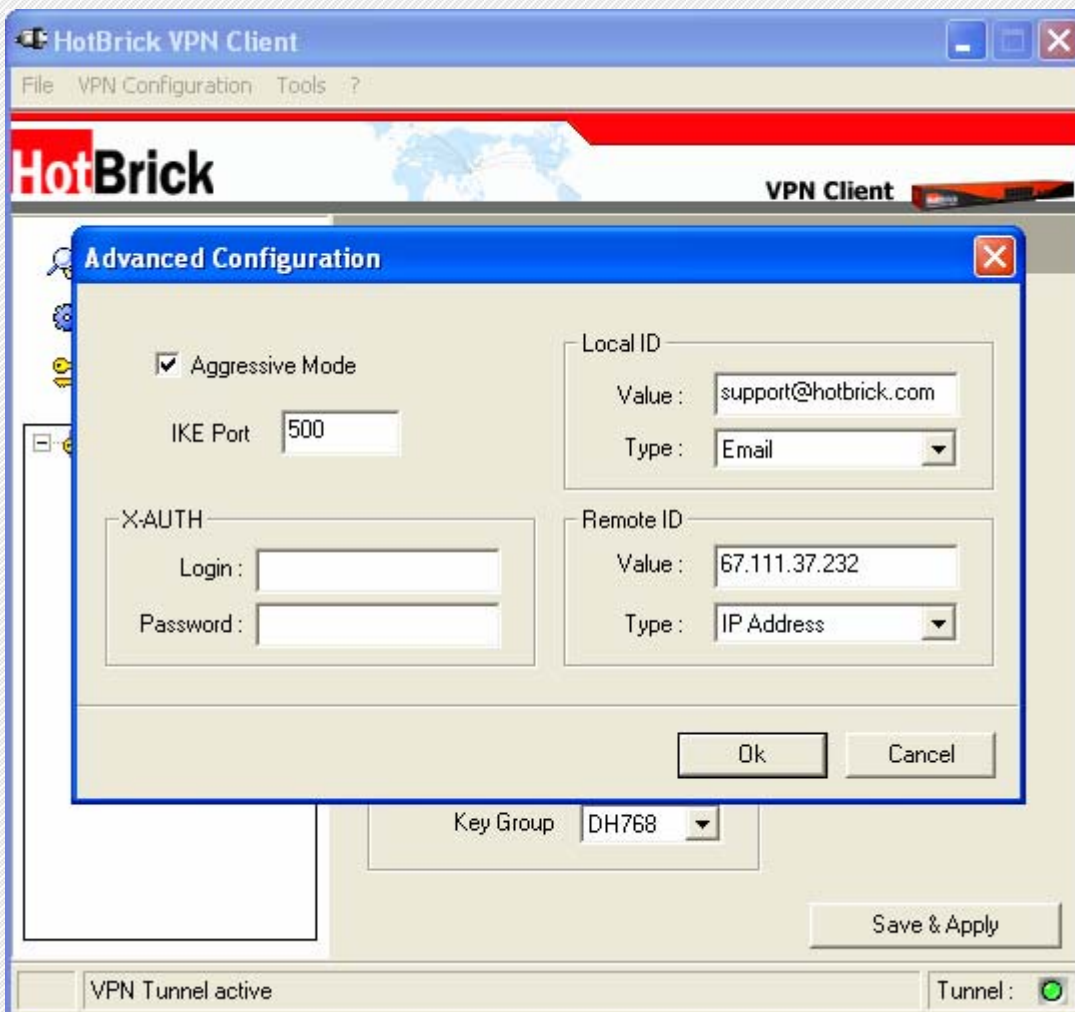


Figure 3 - Advanced Configuration for Phase 1

3. Now right click on your Phase 1 (test401vpn) and select "Add Phase 2"
- h. Enter a name for the Phase 2 (ex: test401vpn2)
- i. The VPN Client address should be IP address of your computer (192.168.2.59)
- j. Next select "Subnet Address" for the Address Type
- k. Next input the Remote LAN address (LAN subnet of the 401VPN)
- l. Next enter the subnet mask, which will most likely be 255.255.255.0
- m. Under ESP, enter the Encryption, Authentication, and mode "Tunnel"
 - 3DES
 - MD5
 - DH1024
- n. Select PFS and DH1024 (DHGroup2)
- o. Hit the "Save & Apply" button.
- p. Please see figure 4 below.

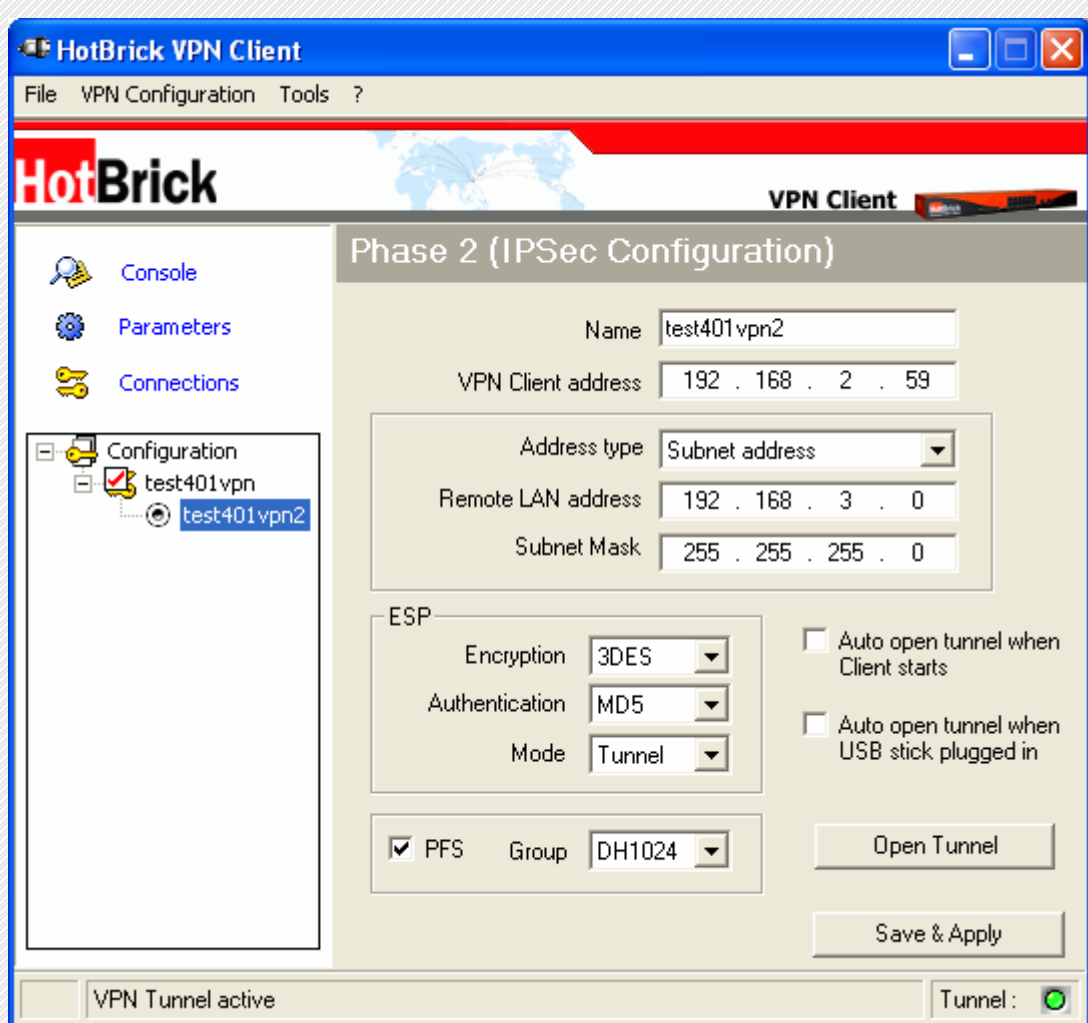


Figure 4 - Phase 2 (IPSec Configuration)

401 VPN Setup

1. Login to you 401VPN and click on *VPN (IPSec)* and then on *VPN policies*.
2. Next click on *Add New Policy* button and this will bring you to the **VPN Wizard**.
3. Click on *Next*. Please see figure 5 below.

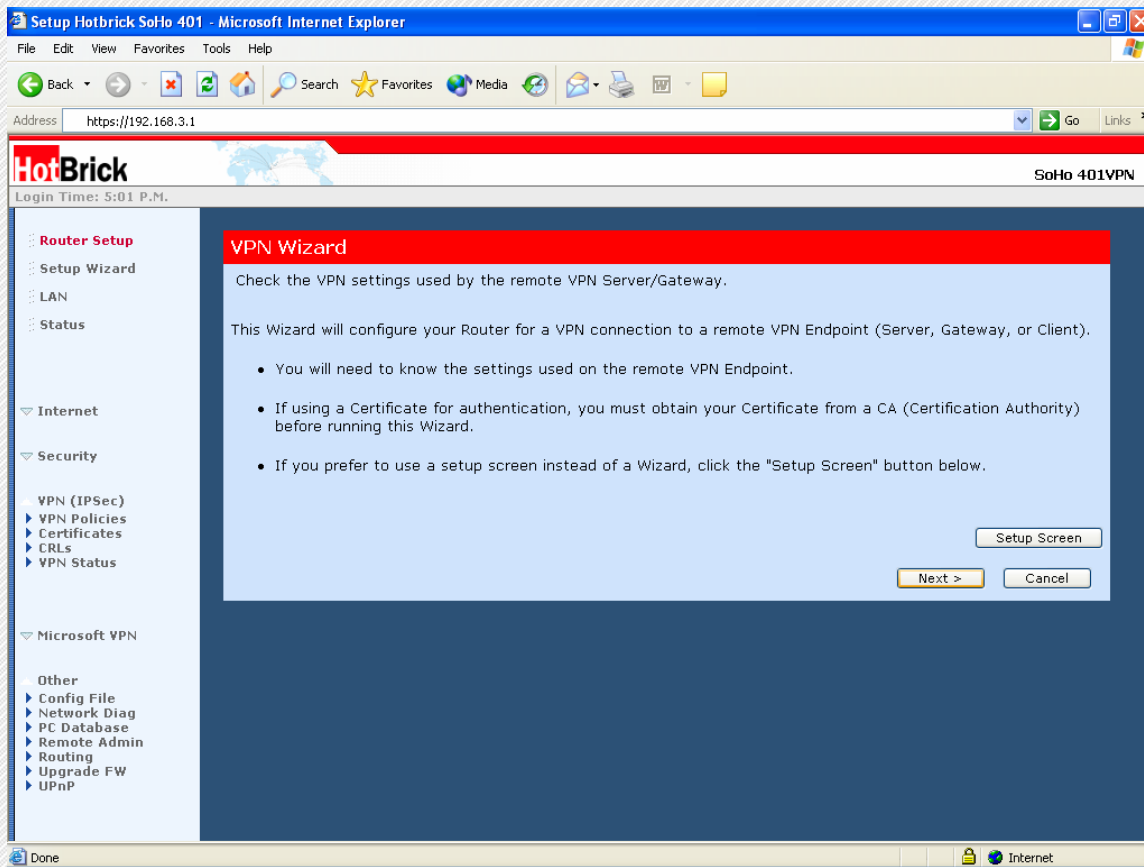


Figure 5 - VPN Wizard

4. This will take you to the **VPN Wizard – General Information** page
- q. Enter the name of the tunnel under *Policy Name* (ex: HBVPNclient)
- r. Make sure *Enable Policy* is checked
- s. *Allow NetBIOS traffic* is optional, but in our example it is selected.
- t. For **Remote Endpoint Address** make sure that *Dynamic IP* is selected.
- u. Click on the **Next** button.
- v. Please see figure 6 below.

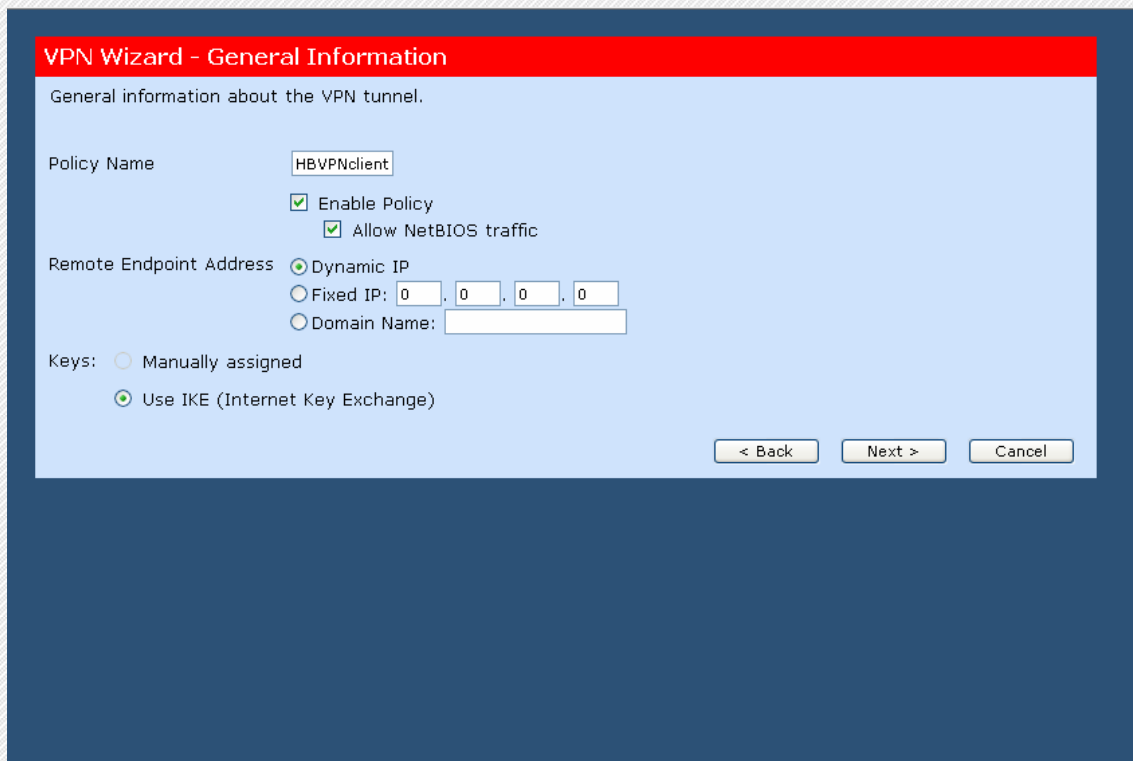


Figure 6 - VPN Wizard - General Information

5. The next page is the VPN Wizard – Traffic Selector. Here you can define both local area network and remote area network within the IPsec tunnel.
 - w. Under **Local IP addresses**, select the *Subnet address* from the drop down box under **Type**.
 - x. Under **IP address** you should see the LAN network address for your 401VPN (ex: 192.168.3.0)
 - y. Under **Subnet Mask** you should see the subnet mask 255.255.255.0
 - z. The **Remote IP addresses** section should be grayed out.
 - aa. When you have finished click on **Next**.
 - bb. Please see figure 7 below.

VPN Wizard - Traffic Selector

This traffic will be sent through a VPN tunnel.

Local IP addresses

Type: Subnet address

IP address: 192 . 168 . 3 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP addresses

Type: Subnet address

IP address: 192 . 168 . 3 . 0 ~ 0

Subnet Mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Figure 7 - VPN Wizard Traffic Selector

6. The next page is the VPN Wizard – IKE Phase 1 (IKE SA). Here we will define the phase 1 encryption and authentication as well as the Local and Remote Identities.
- cc. The **Local Identity Type** should be WAN IP address with the *Data* field grayed out.
- dd. Under **Remote Identity**, please select **Fully Qualified User Name** from the drop box next to *Type*.
- ee. In the *Data* field enter an email address (ex: support@hotbrick.com)
- ff. Under **Authentication**, select *Pre-shared Key* and then enter a phrase, keyword, or number combination (ex: 123456).
- gg. Under **Authentication Algorithm** select *MD5* from the drop down box.
- hh. Under **Encryption Algorithm** select *3DES*.
- ii. Under **IKE SA Life Time** enter 28800
- jj. Under **Diffie-Hellman (DH) Group** select *Group 1 (768 Bit)*.
- kk. Click on the **Next** button
- ll. Hit the “Save & Apply” button.
- mm. See figure 8 below.

VPN Wizard - IKE Phase 1 (IKE SA)

These settings must match the remote VPN Endpoint.

Local Identity
Type: WAN IP Address Data: []

Remote Identity
Type: Fully Qualified User Name Data: support@hotbrick.com

Authentication RSA Signature (requires Certificate)
 Pre-shared Key 123456
Authentication Algorithm: MD5

Encryption Algorithm: 3DES Key Size: n/a (AES only)

IKE Exchange Mode: Aggressive Mode

Direction: Responder

IKE SA Life Time: 28800 (secs)

Diffie-Hellman (DH) Group: Group 1 (768 Bit)

IKE PFS PFS Key Group: Group 2 (1024 Bit)

IKE Keep Alive Ping IP Address: 0 . 0 . 0 . 0

< Back Next > Cancel

Figure 8 - VPN Wizard - IKE Phase 1 (IKE SA)

7. The next page is the VPN Wizard – IKE Phase 2 (IPSec SA). Here we will define the phase 2 IPSec encryption and authentication protocols.

- nn. Under **IPSec SA Life Time** select 28800 seconds
- oo. Make sure the **IPSec PFS** is checked
- pp. Under **Key Group** select *Group 2 (1024 Bit)*
- qq. Make sure that **ESP Encryption** is checked
- rr. Under **Algorithm** select *3DES*
- ss. Make sure that **ESP Authentication** is checked
- tt. Under **Algorithm** select *MD5*.
- uu. Click on the **Next** button
- vv. See figure 9 below.

VPN Wizard - IKE Phase 2 (IPsec SA)

These settings must match the remote VPN Endpoint.

IPsec SA Life Time: 28800 (secs)

IPsec PFS
Key Group: Group 2 (1024 Bit)

AH Authentication
Algorithm: MD5

ESP Encryption
Algorithm: 3DES
Key Size: n/a (AES only)

ESP Authentication
Algorithm: MD5

< Back Next > Cancel

Figure 9 - VPN Wizard - IKE Phase 2 (IPSec SA)

8. Now just click on the Finish tab to create and enable your VPN policy.
ww. See figures 10 and 11 below.

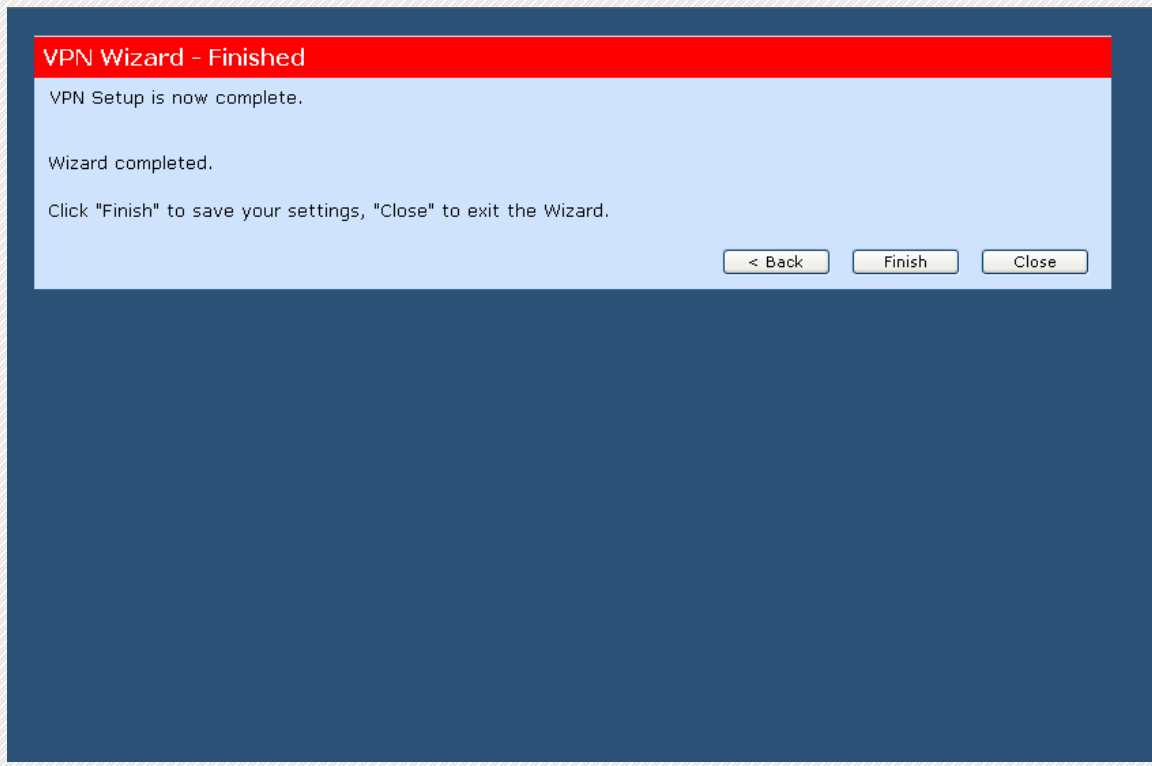


Figure 10 - VPN Wizard Finished

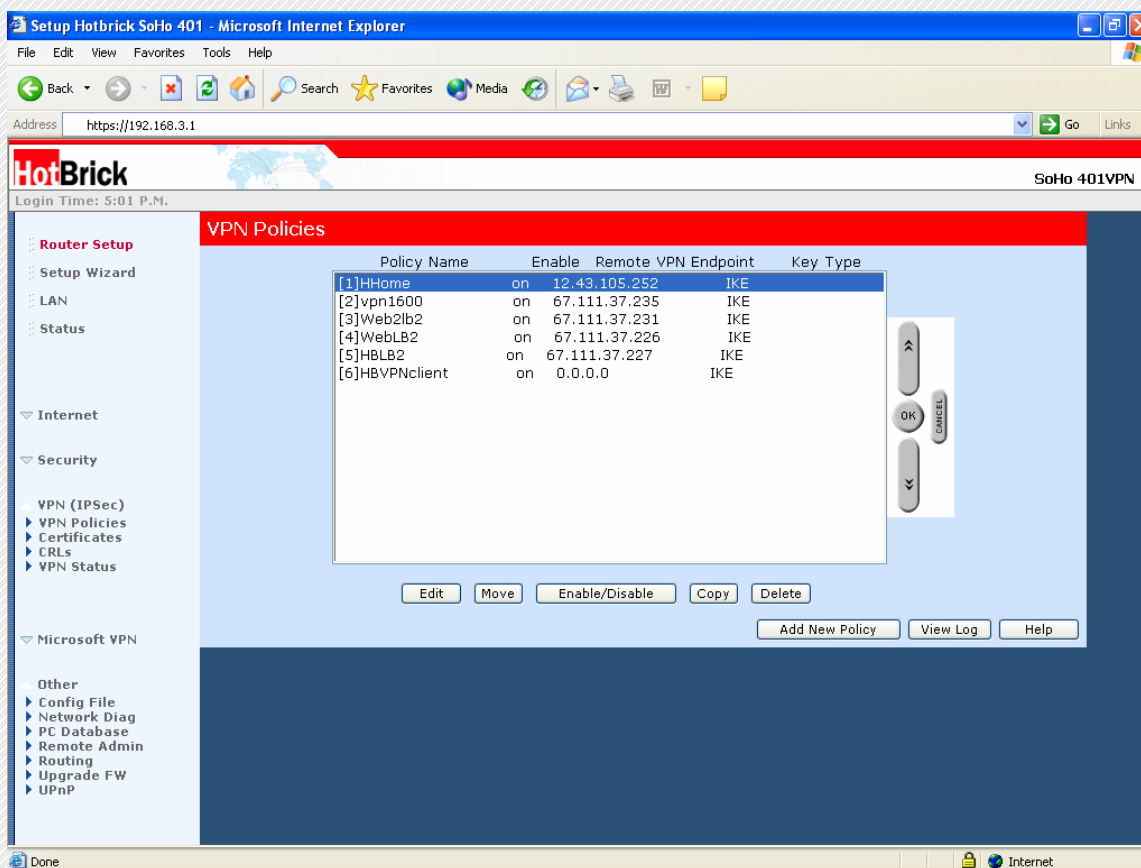


Figure 11 - VPN Policy created

Connecting and Establishing the VPN

1. You will now need to go to the HotBrick VPN client and select your Phase 2 entry (ex: test401vpn2) and click on the Open Tunnel button.
 - a. See figure 12 below.
2. This will initiate and establish the VPN tunnel.
3. We can see in figure 13 that the tunnel is connected on the HotBrick VPN client.
4. In figure 14 we have the VPN status for our tunnel (ex: HBVPNclient) on the 401VPN.
5. Figure 15 and 16 are the logs for the HotBrick VPN client and 401VPN.

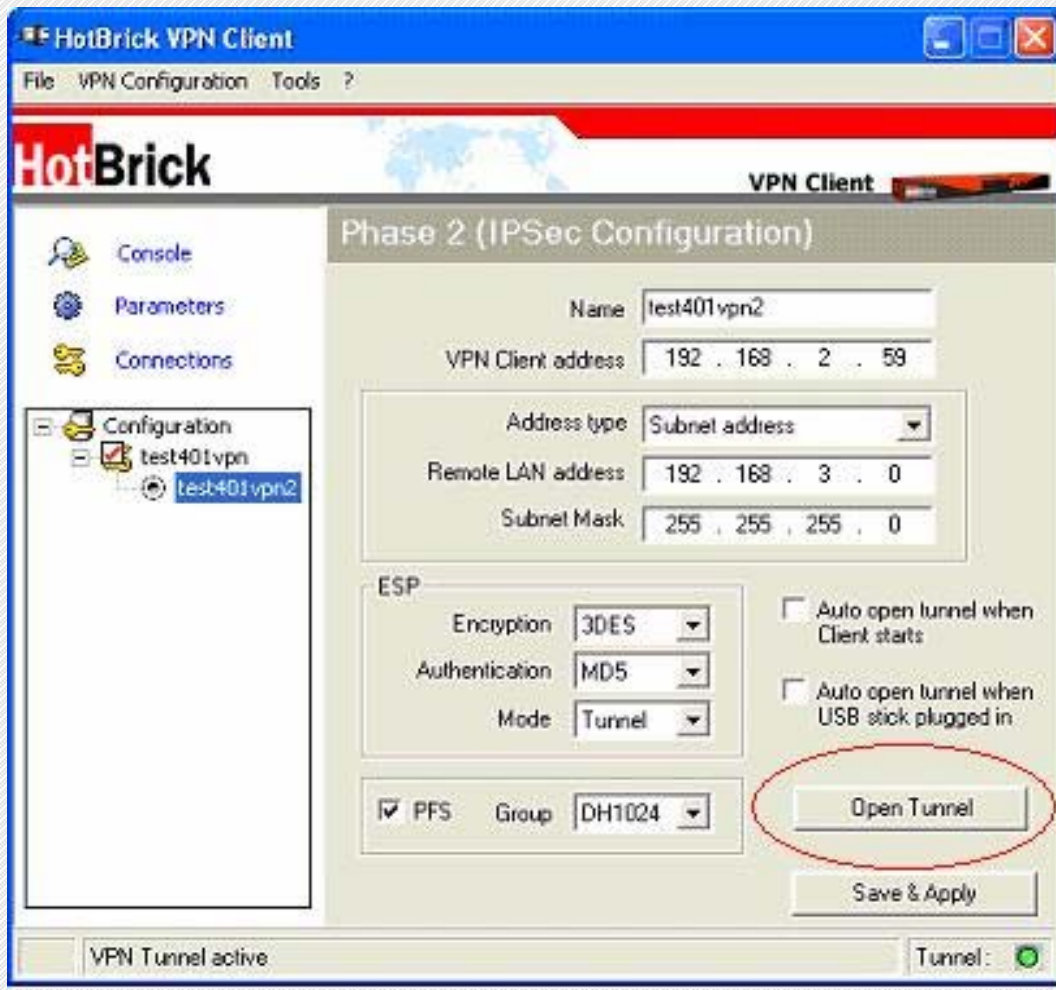


Figure 12 - Open tunnel on HotBrick VPN client

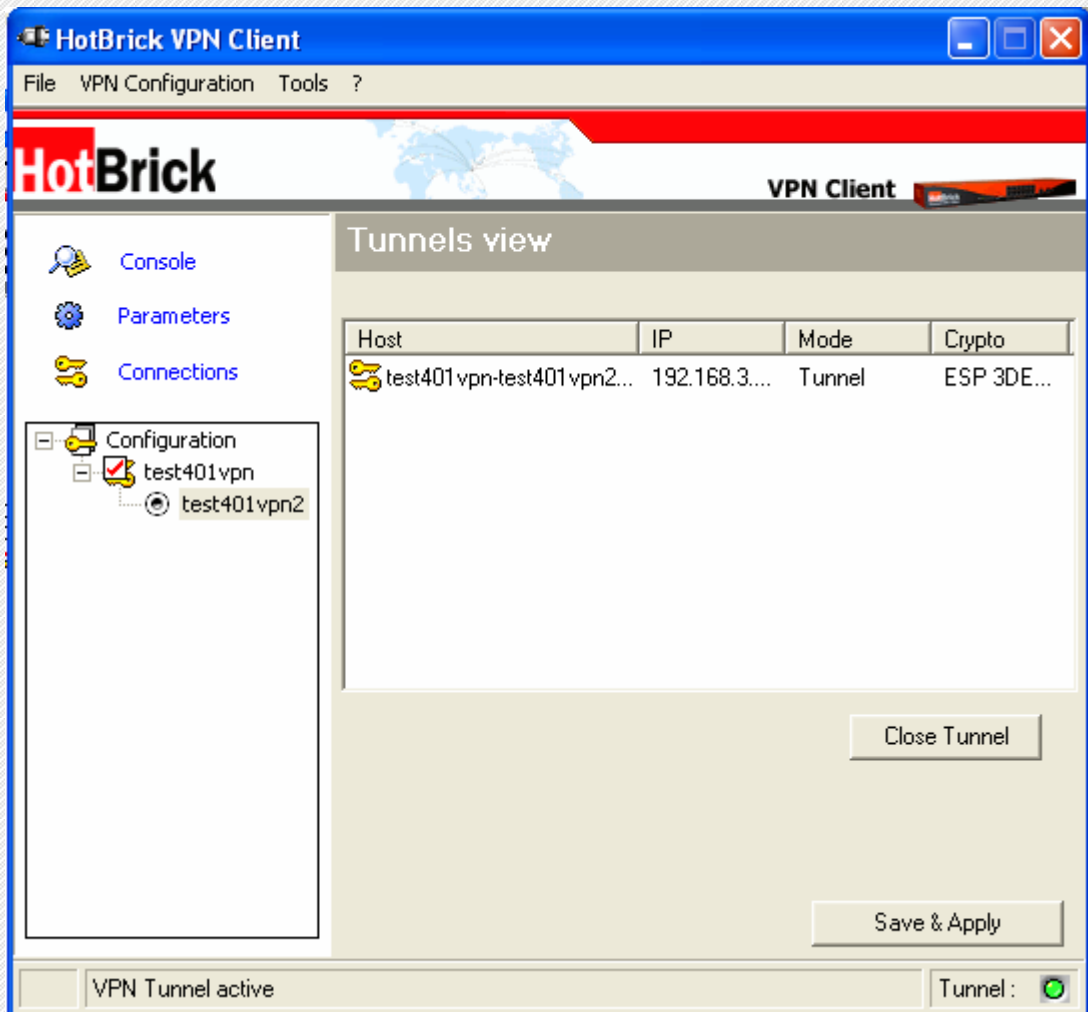


Figure 13 - VPN tunnel connected on Tunnel View

VPN Status

Current VPN SAs

Policy Name	SPI	Type	VPN Endpoint	Data Transferred
HBVPNclient-1	cc7ea322	ESP	67.111.37.228	463
INWebLB2	c695c519	ESP	67.111.37.232	12268
INHBLB2	b29cba54	ESP	67.111.37.232	64301
HBLB2	b1876300	ESP	67.111.37.227	9446
Web2lb2	ef58c4a0	ESP	67.111.37.231	6572
INWeb2lb2	a3233ab4	ESP	67.111.37.232	9340
WebLB2	e00c2ca0	ESP	67.111.37.226	7269
INHBVPNclient-1	c9be5cec	ESP	67.111.37.232	234

Figure 14 - VPN status on 401VPN

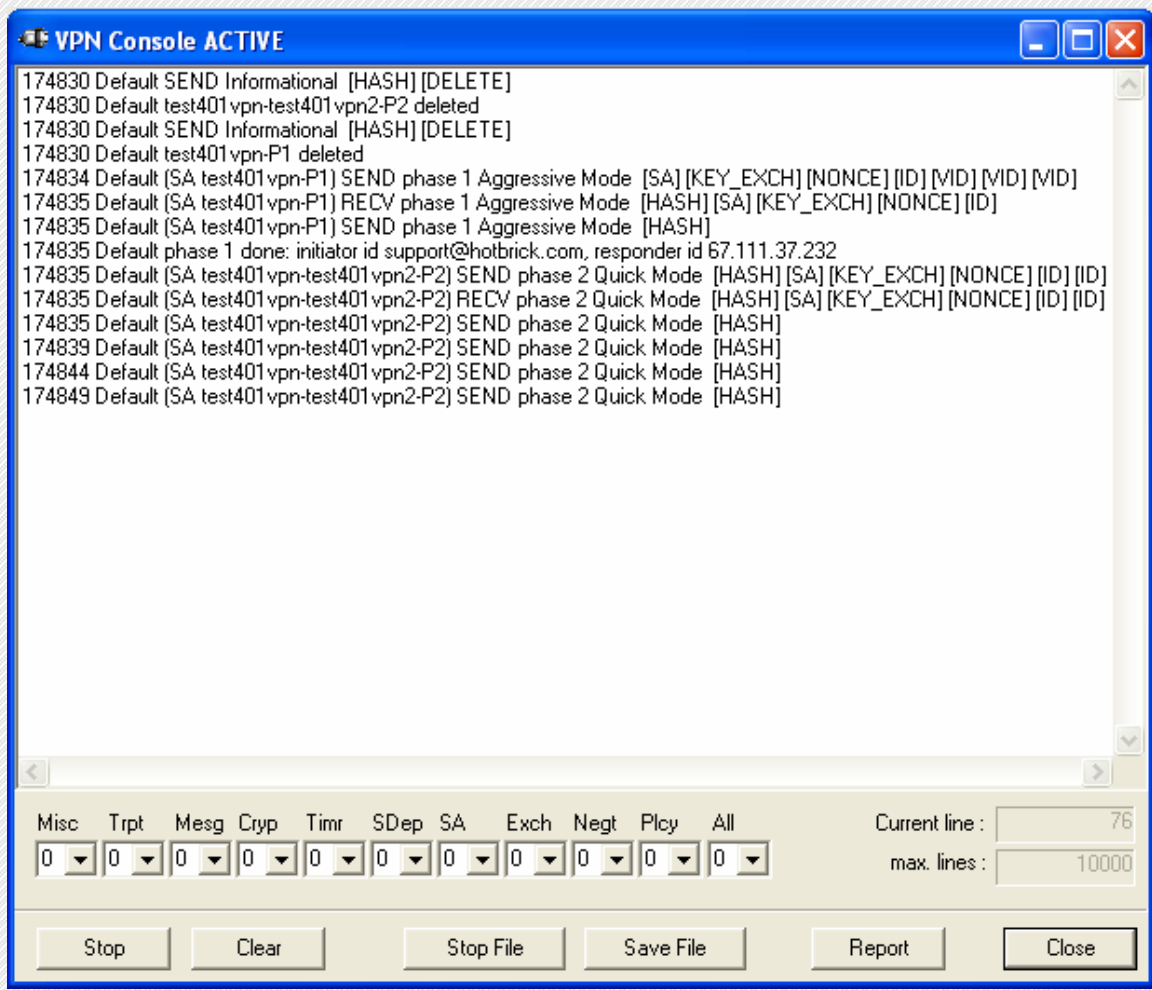


Figure 15 - HotBrick VPN client logs

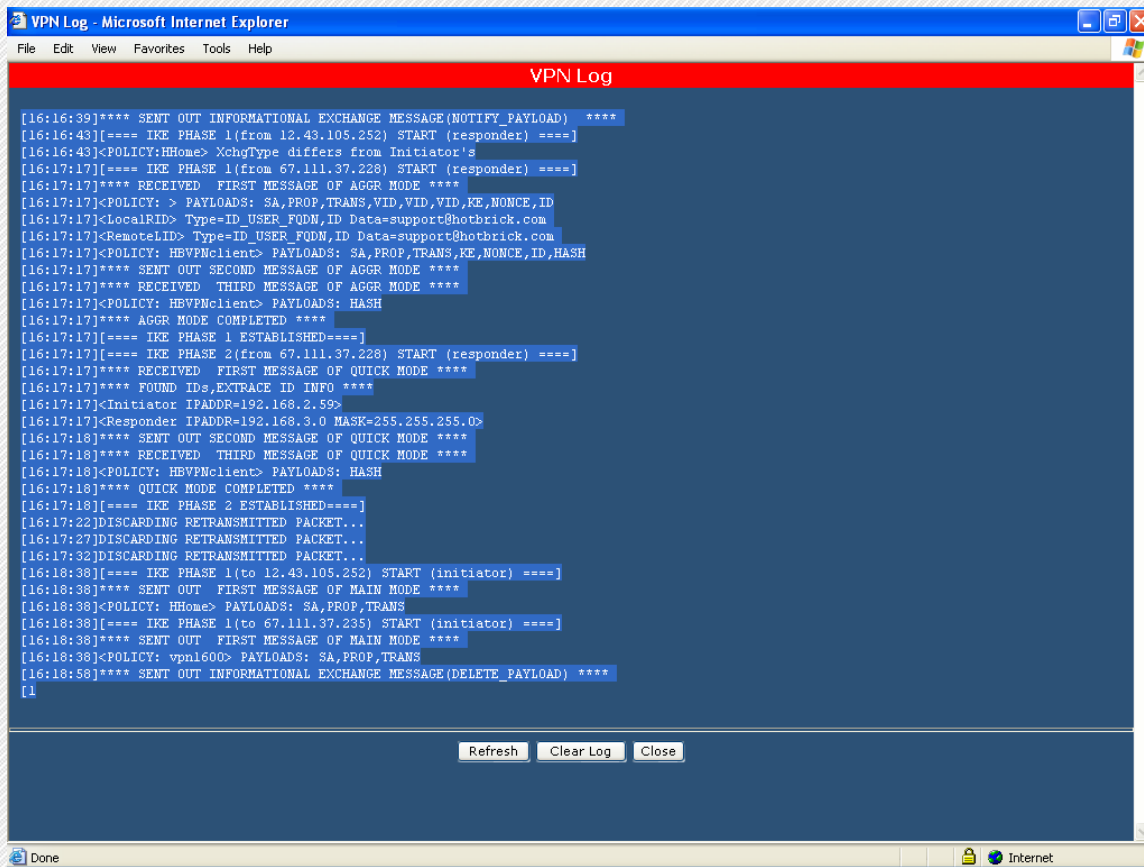


Figure 16 - 401VPN logs