

**Official Tech Documents**

The better way to get your HotBrick product up and running

## Firewall HotBrick SoHo 401 VPN, LB-2 VPN and VPN 800/2

### How To

401 VPN setup guide for IPSec VPN tunnel with LB-2 VPN  
Or VPN 800

#### USA

7243 NW 54th Street  
33166  
Miami, FL  
[www.hotbrick.com](http://www.hotbrick.com)  
[support@hotbrick.com](mailto:support@hotbrick.com)

#### EUROPE

Generatorstraat 26  
Hengelo (Ov), 7556 RC  
Amsterdam - Netherlands  
[www.hotbrick.nl](http://www.hotbrick.nl)  
[support@hotbrick.nl](mailto:support@hotbrick.nl)

#### BRAZIL

Francisco Tramontano, 100  
05686-010  
São Paulo/SP  
[www.hotbrick.com.br](http://www.hotbrick.com.br)  
[suporte@hotbrick.com.br](mailto:suporte@hotbrick.com.br)

## 401 VPN setup guide for IPSec VPN tunnel with LB-2 VPN Or VPN 800

The HotBrick 401VPN, LB-2 VPN, and VPN 800 are all VPN capable router/firewalls with industry standard IPSec encryption. They provide extremely secure LAN to LAN connectivity over the Internet. The 401VPN, LB-2 VPN, and VPN 800 support VPN by encryption, encapsulation, and authentication.

The maximum tunnels allowed on a 401VPN and LB-2VPN is 10 VPN tunnels. The maximum tunnels allowed on a VPN 800 are 50 tunnels. This setup guide will help the user establish an IPSec VPN tunnel between a 401VPN and an LB-2 VPN, or a 401VPN and a VPN800.

### IPSec Tunnel between a 401 VPN and an LB-2 VPN

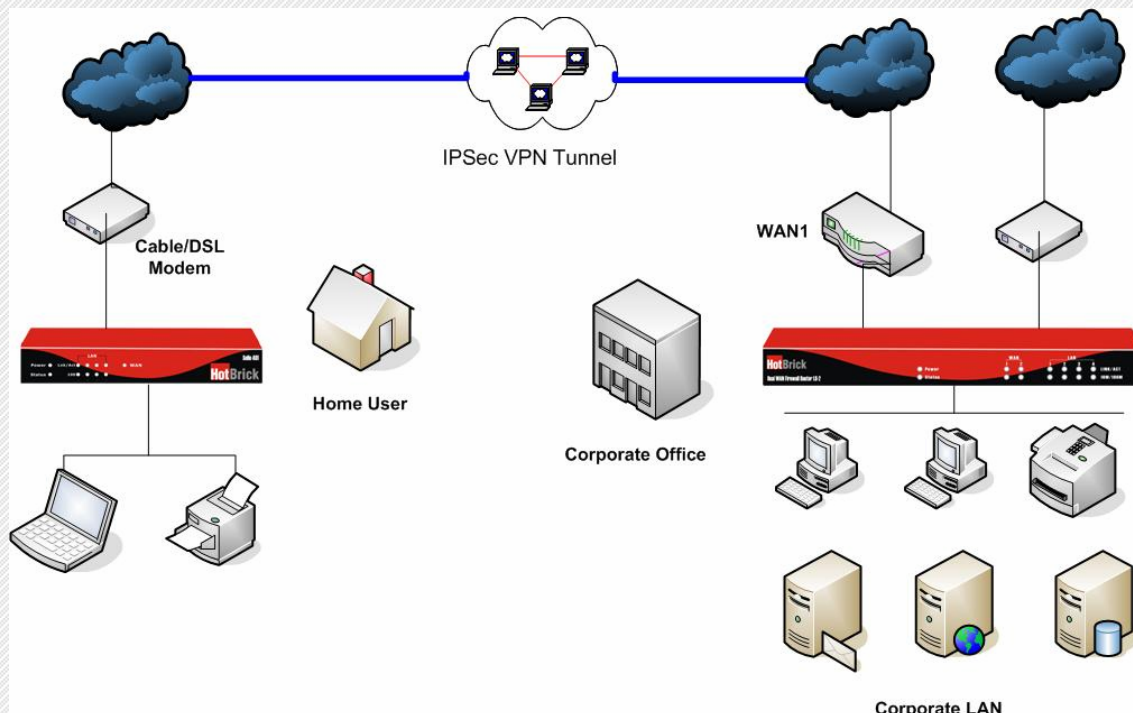


Figure 1 - 401 VPN and LB-2 VPN site to site tunnel

The picture above displays two sites that are joined by a VPN IPSec tunnel using a 401 VPN and an LB-2 VPN. The site on the left is a home user establishing a VPN tunnel to his corporate office on the site on the right.

As you will see below, the IPSec VPN setup for the LB-2 VPN and VPN 800 are exactly the same. We will be describing the setup and showing screenshots for the entire configuration. Here is the setup:

#### Login to the web interface of the 401 VPN

1. Click on VPN (IPSec) and then click on VPN policies
2. A screen shot of the VPN Policies is shown below on Figure 2
3. Next click on the *Add New Policy* button

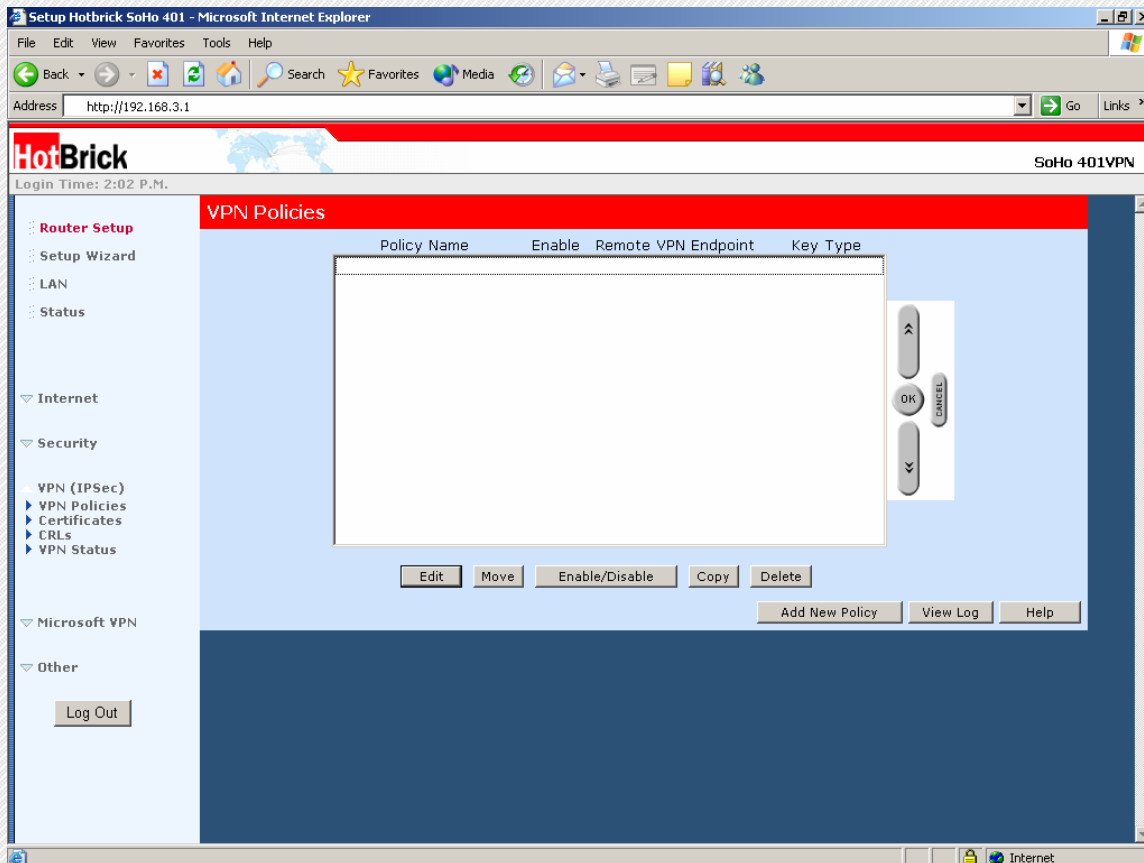


Figure 2 - VPN Policies

4. This brings you to the VPN wizard screen
5. There are two ways to setup an IPsec VPN on a 401VPN:
  - i. VPN Wizard
  - ii. Setup Screen
6. For this setup guide we will use the "VPN Wizard"
7. Click **Next** on the VPN Wizard

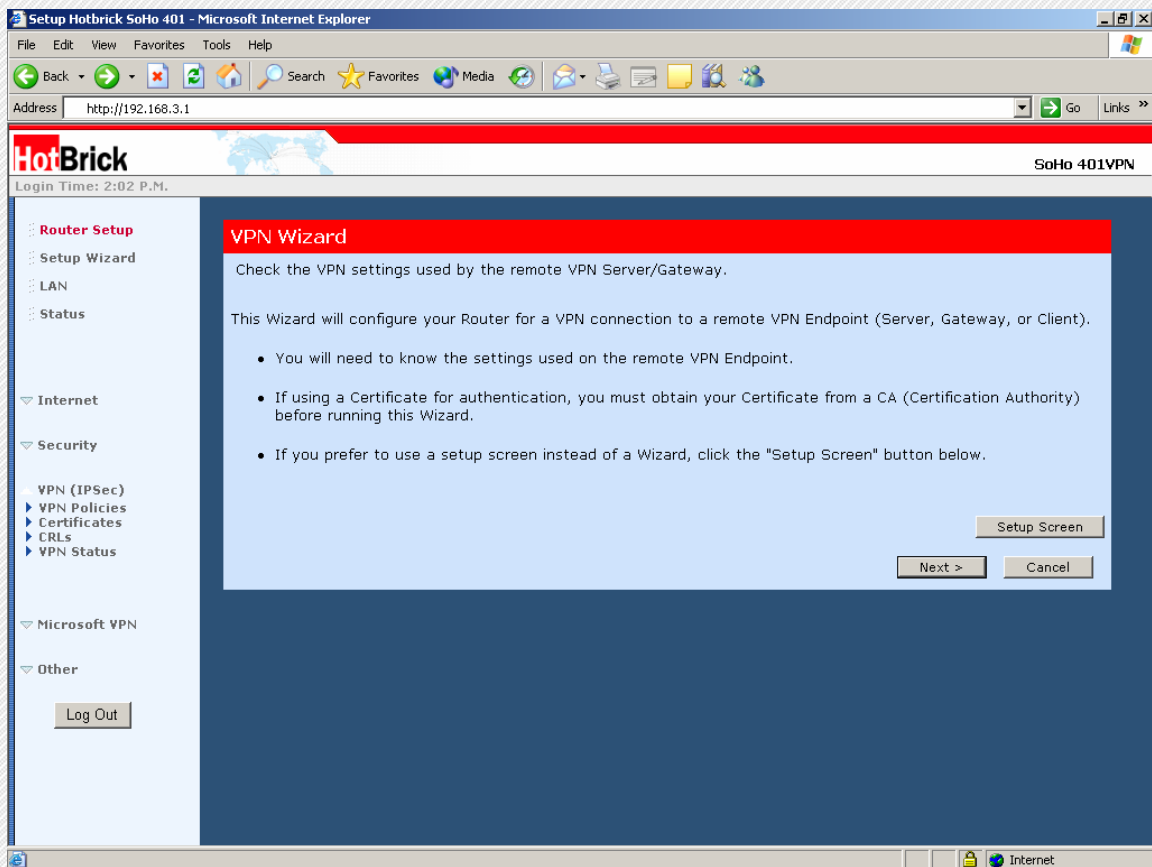


Figure 3 - VPN wizard

8. This brings us to the VPN Wizard – General Information screen. Under *Policy Name* enter a name for the tunnel (ex: LB2VPN)
9. Make sure the box is checked for *Enable Policy*
10. You may also check the enable box to allow NetBIOS traffic (optional)
11. The Remote Endpoint Address can be a:
  - i. Dynamic IP
  - ii. Fixed IP
  - iii. Domain Name
  - iv. In our example it is an WAN IP address of the LB-2 VPN (ex: 67.111.37.228)
  - v. When you are finished click on the **NEXT** button.

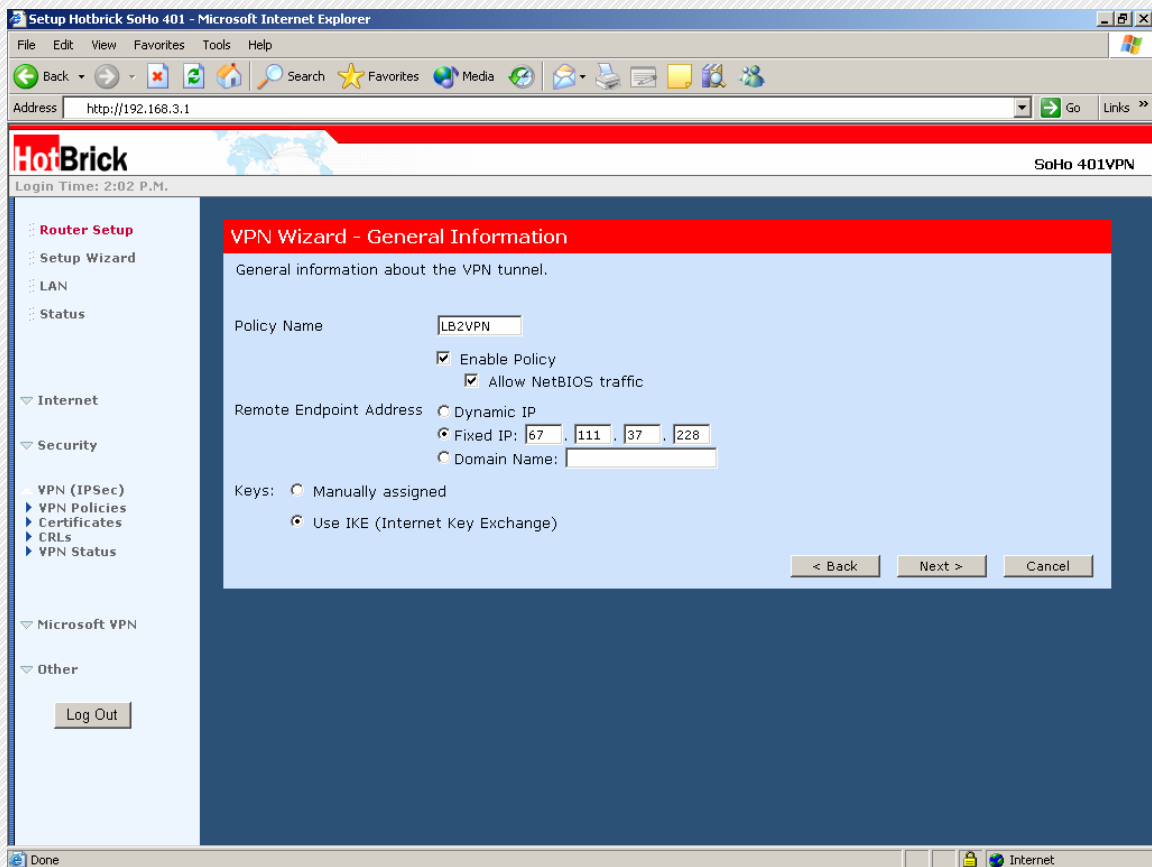


Figure 4 – VPN Policy Definition

12. The next screen is the VPN Wizard – Traffic Selector. Here will be defining the LAN Network and Remote Network under this IPSec policy. Under “Local IP Addresses” make sure that the “Type” is **Subnet address**
13. Under “IP address” input the Local LAN subnet (ex: 192.168.3.0) and “Subnet Mask” (ex: 255.255.255.0)
14. Under “Remote IP Address” also make sure that the “Type” is **Subnet address**. This time under “IP address” input the Remote LAN subnet (ex: 192.168.2.0) and “Subnet Mask” (ex: 255.255.255.0).
15. When you are finished click on the **NEXT** button.

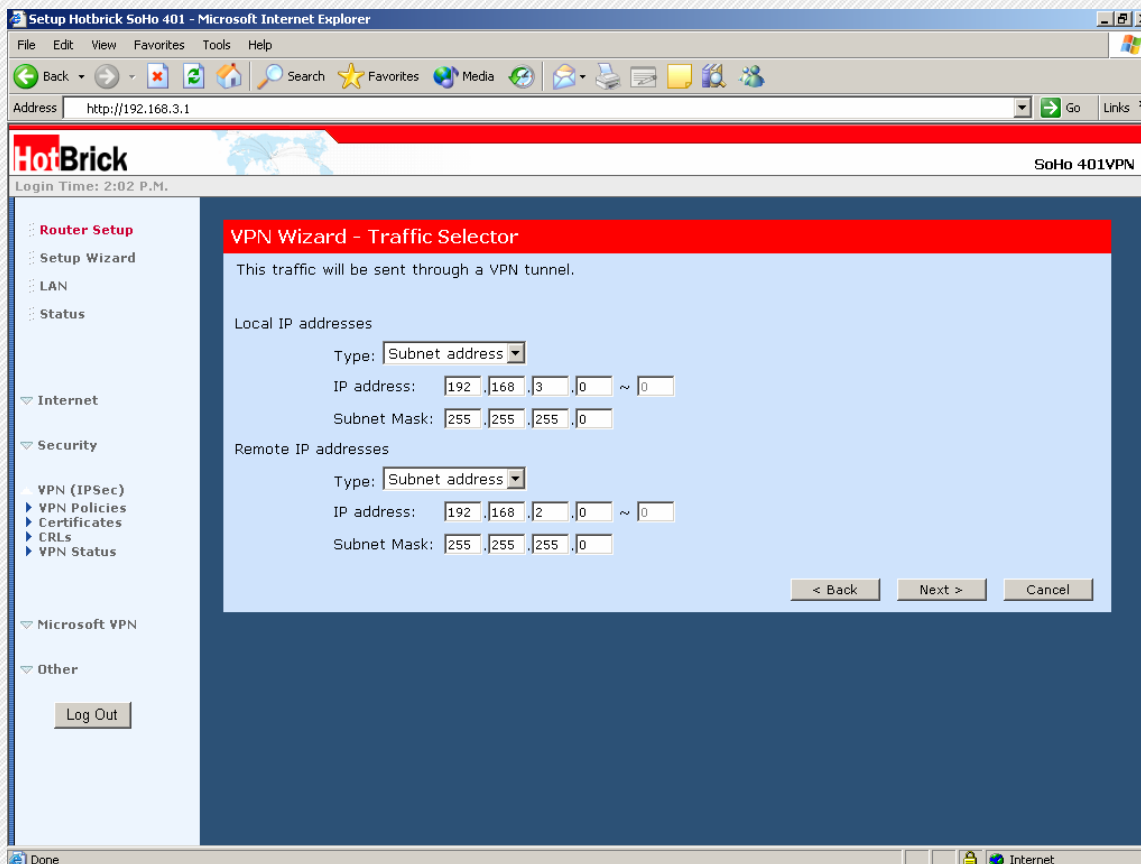


Figure 5 - VPN Wizard Traffic Selector

16. The next screen is the VPN Wizard – IKE Phase 1 (IKE SA). Under “Local Identity Type” make sure **WAN IP address** is selected.
17. Under “Remote Identity Type” make sure **Remote WAN IP** is selected.
18. Under “Authentication” make sure the **Pre-shared Key** is selected. The pre-shared key used in our example is “testlab”.
19. Under “Authentication Algorithm” make sure **MD5** is selected. Under “Encryption Algorithm” select **3DES**
20. Under “IKE Exchange Mode” select **Main Mode**.
21. Under “Direction” make sure it is set for **Both Directions**.
22. Under “IKE SA Life Time” please input **28800**.
23. Under “Diffie-Hellman (DH) Group” select **Group 1 (768 Bit)**. Please do not check the **IKE PFS**.
24. When you are finished click on the **NEXT** button. Please see Figure 6 below.

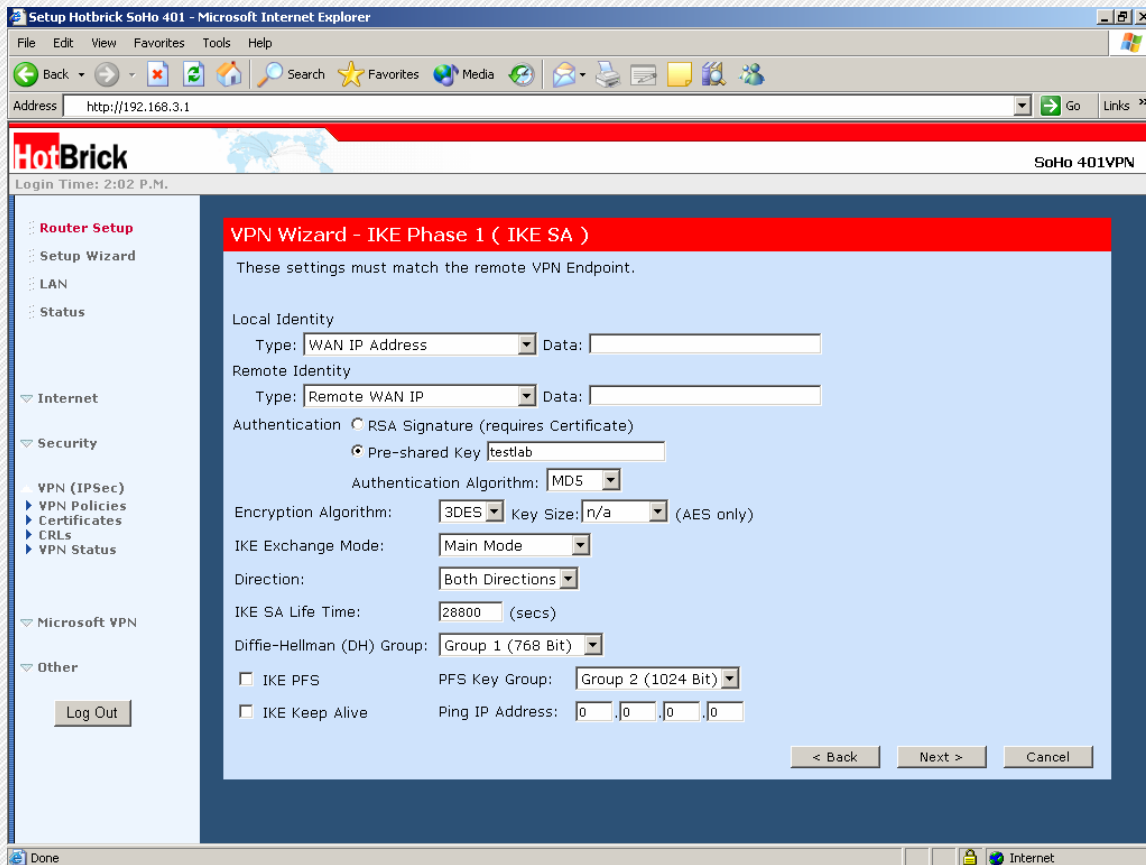


Figure 6 – IKE Phase 1 (IKE SA)

25. The next screen is the VPN Wizard – IKE Phase 2 (IPSec SA). Under “IPSec SA Life Time” input **28800**
26. Under “IPSec PFS” select **Group 2 (1024 Bit)**
27. Under “ESP Encryption” the algorithm in our example is **3DES**.
28. Under “ESP Authentication” the algorithm in our example is **MD5**.
29. When you are finished click on the **NEXT** button. Please see Figure 7 below.

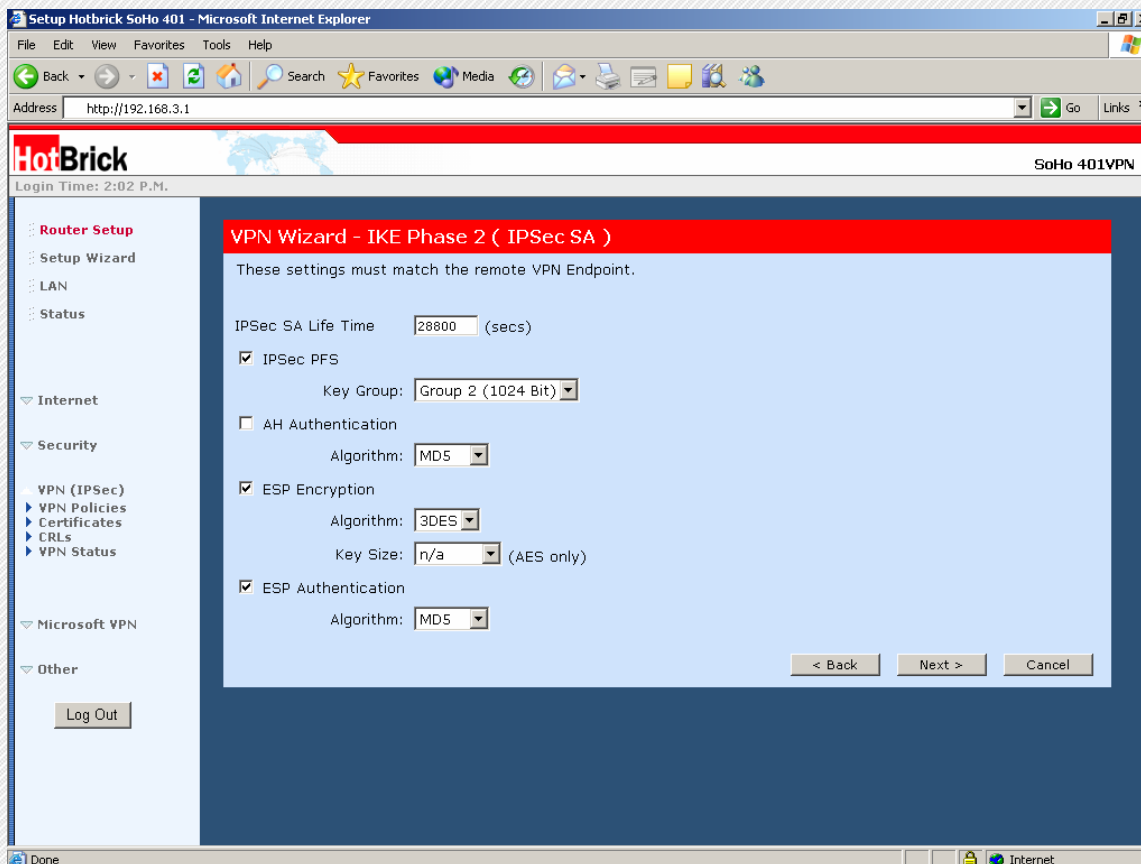


Figure 7 – IKE Phase 2 (IPSec SA)

Now it is time to configure the VPN tunnel on the LB-2 VPN or VPN 800.

1. Click on VPN Configuration and click on Global Setting
2. Make sure you:
  - i. Check the enable box for WAN1 and/or WAN2
  - ii. Under Phase 1 DH Group select **DH Group 1 (768-bit)**
  - iii. Under Phase 1 Encryption Method select **3DES**
  - iv. Under Phase 1 Authentication Method select **MD5**
  - v. Under Phase 1 SA Lifetime select **28800**
  - vi. Hit Submit
  - vii. Figure 8 shows the Global Setting for the LB-2 VPN and Figure 9 shows the Global Setting for the VPN 800.

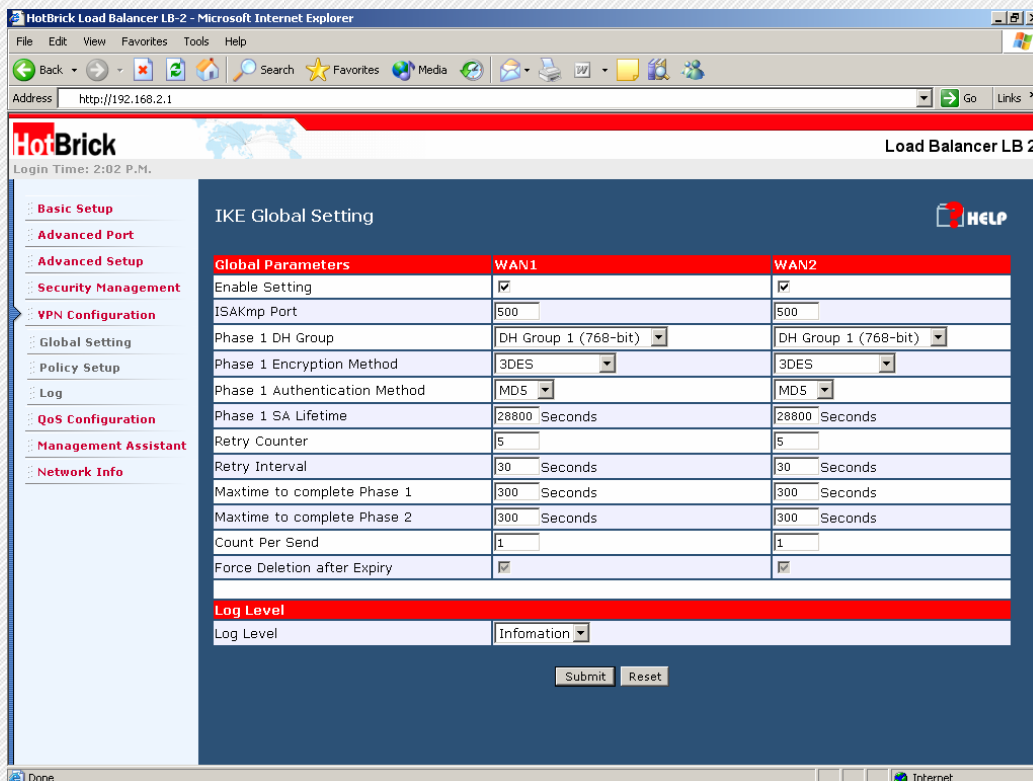


Figure 8 – IKE Global Settings for LB-2 VPN

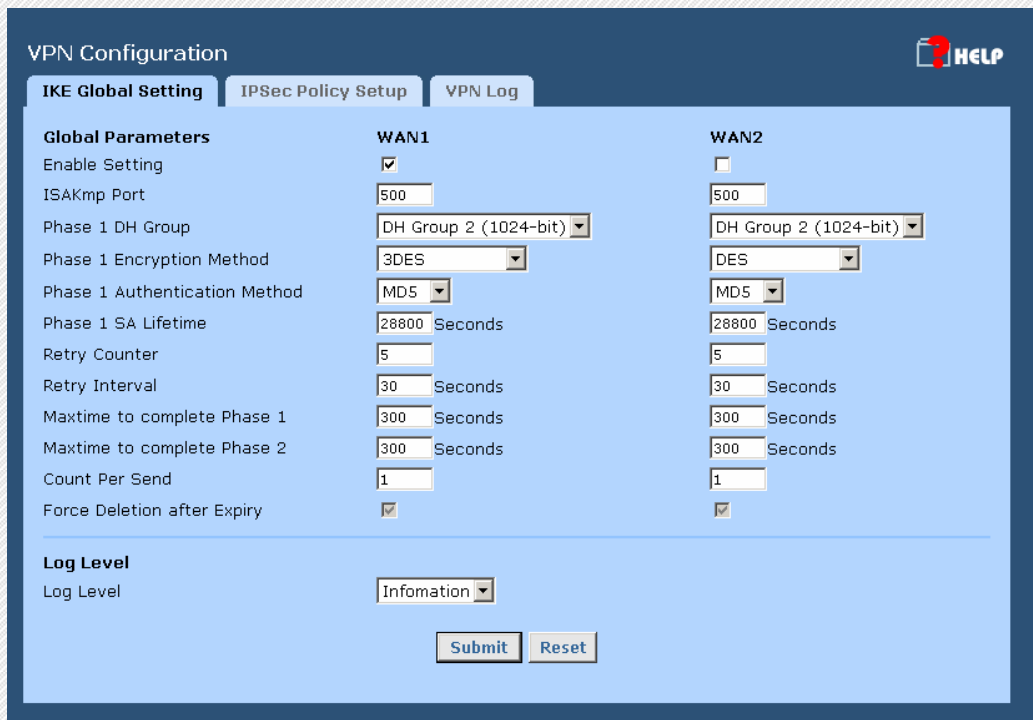
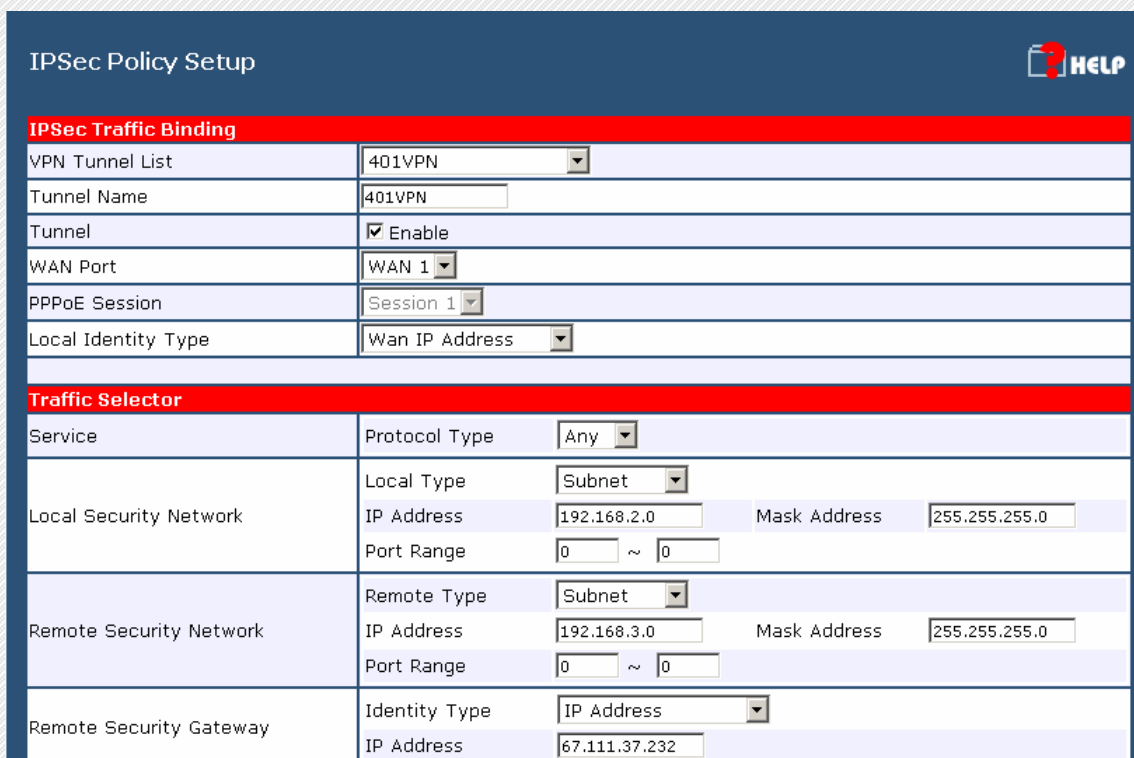


Figure 9 - IKE Global Settings for VPN 800

3. Next click on Policy Setup
  - a. Enter a Tunnel Name (ex: 401VPN)
  - b. Check enable for the tunnel
  - c. Under "WAN port" select **WAN1**
  - d. Under Traffic Selector:
    - i. Under "Service", Protocol Type select **Any**
    - ii. Local Type select **Subnet**
    - iii. Under "Local Security Network", IP address – make sure this is the LAN subnet of LB-2 VPN, in our example it is 192.168.2.0 and subnet mask 255.255.255.0.
    - iv. Port Range should be zero to zero (0 ~ 0)
    - v. Under "Remote Security Network", Remote Type – IP Address, enter the **Interface** IP address of the 401VPN, in our example it is 192.168.3.0 and subnet mask 255.255.255.0.
    - vi. The port range should be zero to zero (0 ~ 0)
    - vii. Under "Remote security Gateway", Select **IP address** for "Gateway Type"
    - viii. Enter the same IP Address as the Remote Security Network IP address (67.111.37.232).



IPSec Traffic Binding	
VPN Tunnel List	401VPN
Tunnel Name	401VPN
Tunnel	<input checked="" type="checkbox"/> Enable
WAN Port	WAN 1
PPPoE Session	Session 1
Local Identity Type	Wan IP Address
Traffic Selector	
Service	Protocol Type: Any
Local Security Network	Local Type: Subnet
	IP Address: 192.168.2.0    Mask Address: 255.255.255.0
	Port Range: 0 ~ 0
Remote Security Network	Remote Type: Subnet
	IP Address: 192.168.3.0    Mask Address: 255.255.255.0
	Port Range: 0 ~ 0
Remote Security Gateway	Identity Type: IP Address IP Address: 67.111.37.232

Figure 10 - LB2 VPN IPsec Policy Setup

**VPN Configuration** HELP

**IKE Global Setting** | **IPSec Policy Setup** | VPN Log

**IPSec Traffic Binding**

VPN Tunnel List: -- Add New Policy --

Tunnel Name: 401VPN

Tunnel:  Enable

WAN Port: WAN 1

PPPoE Session: Session 1

Local Identity Type: Wan IP Address

---

**Traffic Selector**

Service: Protocol Type: Any

Local Security Network: Local Type: Subnet

IP Address: 192.168.2.0 Mask Address: 255.255.255.0

Port Range: 0 ~ 0

Remote Security Network: Remote Type: Subnet

IP Address: 192.168.3.0 Mask Address: 255.255.255.0

Port Range: 0 ~ 0

Remote Security Gateway: Identity Type: IP Address

IP Address: 67.111.37.232

Figure 11 – VPN 800 IPSec Policy Setup

Remote Security Network	Remote Type: Subnet	IP Address: 192.168.3.0	Mask Address: 255.255.255.0
	Port Range: 0 ~ 0		
Remote Security Gateway	Identity Type: IP Address	IP Address: 67.111.37.232	

---

**Security Level**

Encryption Method: 3DES

Authentication Method: MD5

ESP Mode: Tunnel

---

**Key Management**

Key Type: AutoKey (IKE)

Phase 1 Negotiation: Main Mode

Perfect Forward Secrecy: DH Group 2 (1024-bit)

Preshared Key: testlab (Characters / Hex:0x)

Key Lifetime: In Time: 28800 Seconds (Note : 0 for no expiry)

In Volume: 0 Kbytes

---

**Action**

Connect | Flush Tunnel | Reload Policy | Tunnel Status | Set Options ..

Figure 12 - LB2 VPN IPSec Policy Setup Continued

**Security Level**  
Encryption Method: 3DES  
Authentication Method: MD5  
ESP Mode: Tunnel

**Key Management**  
Key Type: AutoKey (IKE)  
Phase 1 Negotiation: Main Mode  
Perfect Forward Secrecy: DH Group 2 (1024-bit)  
Preshared Key: testlab (Characters / Hex:0x)  
Key Lifetime: In Time 28800 Seconds (Note : 0 for no expiry)  
In Volume 0 Kbytes

**Action**  
Connect Flush Tunnel Reload Policy Tunnel Status Set Options ..  
Add Delete Update Reset

Figure 13 - LB2 VPN IPsec Policy Setup Continued

5. Under Security Level, make sure you input the Encryption Method is **3DES** and Authentication Method is **MD5**.
6. Under Key Management and Key Type select **Auto key (IKE)**.
  - i. For phase 1 negotiation select **Main Mode**.
  - ii. Under "Perfect Forward Secrecy" select **DH Group 2(1024-bit)**
  - iii. Under "Pre-Shared key", we must input the same pre-shared key entered in the 401VPN ("testlab")
  - iv. Make sure the key lifetime is **28800** seconds, and you may leave the Key lifetime volume to be zero.
  - v. Once you have verified all these settings click on **Add**.
7. Now under **Action** select **Set Options**
  - i. Make sure that you check the enable box for **Detection**, under Dead Peer Detection Feature.
  - ii. Under "Check Method" make that **DPD (RFC 3706)** is selected.
  - iii. Under "Action" make sure that **Keep Tunnel Alive** is selected.
  - iv. Under the "Options" section, make sure that **NetBios Broadcast** (optional) and **Auto Triggered** are both selected.
  - v. Now click on the **Set** button, and then click on the **Update** button on the "IPsec Policy Setup" page.
  - vi. You are now ready to establish the tunnel. For the Policy Setup

IPSec Policy options HELP

**Tunnel attributes**

State	Name	Security Gateway	Remote Site	Security Policy	Key Type	Physical Status	Negotiation Status
Enable	401VPN	67.111.37.232	192.168.3.0	3DES/MD5	AutoKey (IKE)	WAN 1 Connected	Initiator (Quick) : established

**Dead Peer Detection Feature**

Detection  Enable

Check Method  Heartbeat  ICMP Host   DPD (RFC 3706)

Check After Idle  Seconds

Retry Times

Action  Do Nothing  Remove Tunnel  Keep Tunnel Alive

Logging  Enable

**Options**

NetBIOS Broadcast	<input checked="" type="checkbox"/> Enable	Check ESP Pad	<input type="checkbox"/> Enable
Auto Triggered	<input checked="" type="checkbox"/> Enable	Allow Full ECN	<input type="checkbox"/> Enable
Anti Replay	<input type="checkbox"/> Enable	Copy DF Flag	<input type="checkbox"/> Enable
Passive(Responder) Mode	<input type="checkbox"/> Enable	Set DF Flag	<input type="checkbox"/> Enable

Figure 14 – IPSec Policy Options

IPSec Policy options HELP

**Tunnel attributes**

State	Name	Security Gateway	Remote Site	Security Policy	Key Type	WAN	Status
Enable	401VPN	67.111.37.232	192.168.3.0	3DES/MD5	AutoKey (IKE)	WAN 1 Connected	Idle

**Dead Peer Detection Feature**

Detection  Enable

Check Method  Heartbeat  ICMP Host   DPD (RFC 3706)

Check After Idle  Seconds

Retry Times

Action  Do Nothing  Remove Tunnel  Keep Tunnel Alive

Logging  Enable

**Options**

NetBIOS Broadcast	<input checked="" type="checkbox"/> Enable	Check ESP Pad	<input type="checkbox"/> Enable
Auto Triggered	<input checked="" type="checkbox"/> Enable	Allow Full ECN	<input type="checkbox"/> Enable
Anti Replay	<input type="checkbox"/> Enable	Copy DF Flag	<input type="checkbox"/> Enable
Passive(Responder) Mode	<input type="checkbox"/> Enable	Set DF Flag	<input type="checkbox"/> Enable

Figure 15 – IPSec Policy Options

To establish the VPN tunnel:

1. On the LB-2 VPN or VPN 800 click “Connect” under **Action** in the policy setup.
2. This will initiate and establish the tunnel.
3. On the LB-2 VPN and VPN 800, Under “Security Association List”, you should see the Negotiation Status as **Initiator (Quick) established**.
4. On the 401VPN click on the VPN Status link. If the two policy names listed have values under “Data Transferred” the connection is established. Please see Figure 18 below.

Security Association List							
State	Name	Security Gateway	Remote Site	Security Policy	Key Type	Physical Status	Negotiation Status
Enable	401VPN	67.111.37.232	192.168.3.0	3DES/MD5	AutoKey (IKE)	WAN 1 Connected	Initiator (Quick) : established

Figure 16 – Security Association List on LB-2 with VPN established

Security Association List							
State	Name	Security Gateway	Remote Site	Security Policy	Key Type	WAN	Status
Enable	401VPN	67.111.37.232	192.168.3.0	3DES/MD5	AutoKey (IKE)	WAN 1 Connected	Initiator (Main) : established

Figure 17 – Security Association List on VPN 800 with VPN established

VPN Status				
Current VPN SAs				
Policy Name	SPI	Type	VPN Endpoint	Data Transferred
LB2VPN	3f52cbc1	ESP	67.111.37.228	7153
INLB2VPN	ab89d0b9	ESP	67.111.37.232	20036

Figure 18 – VPN Status on 401VPN with VPN established