Firewall HotBrick LB-2

How To

LB-2 IPSec Tunnel Setup Guide

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

LB-2 IPSec Tunnel Setup Guide

The HotBrick LB-2 is a VPN capable Dual WAN Gateway with industry standard IPsec encryption. It provides extremely secure LAN-to-LAN connectivity over the Internet. The LB-2 supports VPN by encryption, encapsulation, and authentication using the following methods:

DES/3DES/AES
MD-5
SHA-1/SHA-2

The maximum tunnels allowed are 10 VPN tunnels. This setup guide will help the user establish an IPsec VPN tunnel between two LB-2s with VPN.

Note: The LB-2 must have the VPN upgrade to establish an IPSec Tunnel. This will also help you setup an IPSec Tunnel if you have an LB-2 VPN with license key. Please upgrade your LB-2 VPN to the latest version by going to our website and clicking on the Downloads link (http://hotbrick.com/support.asp).

IPsec Tunnel between two LB-2 VPN

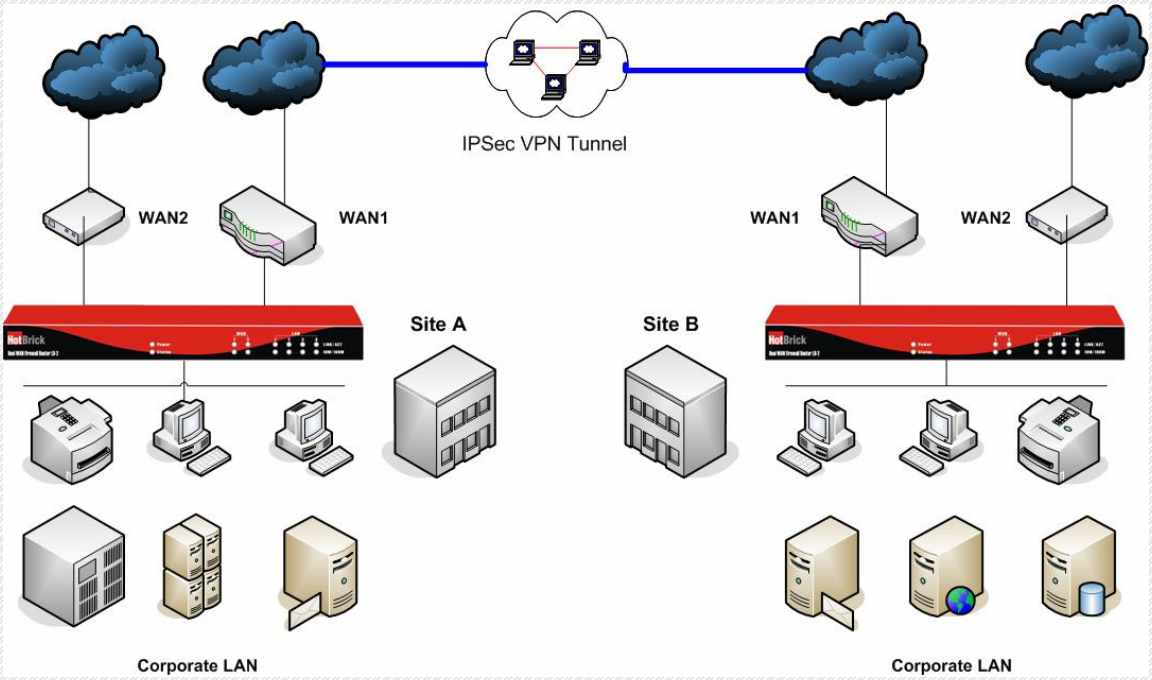

Figure 1 - LB-2 site to site tunnel

The picture above displays two sites that are joined by a VPN IPsec tunnel between two LB-2s with VPN. Here is how to setup the VPN IPSec tunnel:

1. Login to your LB-2
2. Go to Advanced Setup
3. VPN Configuration
4. Click on Global Setting. Please see the picture below for the IKE Global Setting for site A.

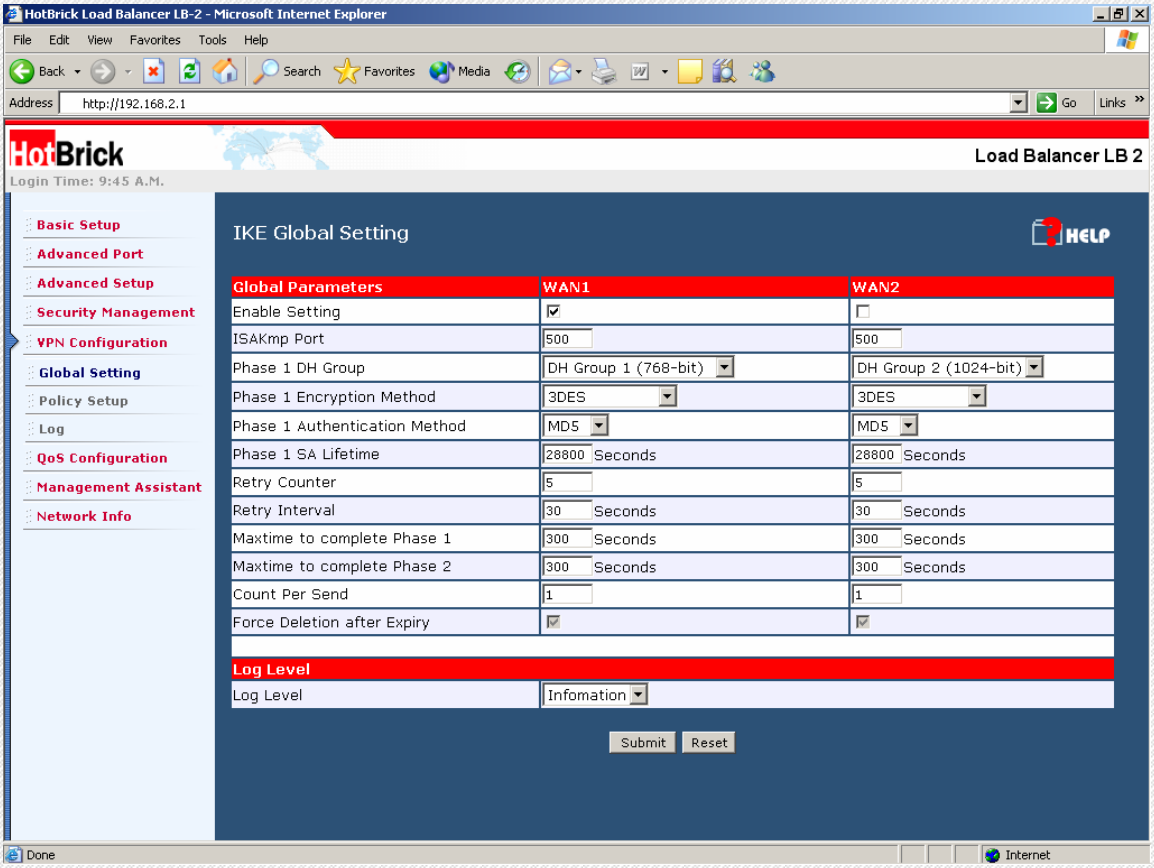

Figure 2 - Global Setting for Site A

5. Under the Global Setting, make sure you enable the WAN interface that you want the VPN IPSec tunnel to establish through.
6. Both WAN1 and WAN2 can initiate and establish VPN Tunnels
7. Figure 2 shows the Global Parameters for WAN1. Remember that these parameters must be identical at both sites. Below are some recommended values:

- Phase 1 DH Group – DH Group 1 (768 bit)
- Phase 1 Encryption Method – 3DES
- Phase 1 Authentication Method – MD5
- Phase 1 SA Lifetime – 28800

8. Once you have selected the Global Parameters then hit **Submit**.
9. The LB-2 will be restarted and refreshed to save the settings.
10. After the settings are refreshed, click on Policy Setup
11. Under IPSec Traffic Binding, input a name for "Tunnel Name". In Figures 3 and 4 below, we have the tunnel name "LB2VPN".
12. Make sure you check the enable box for "Tunnel".
13. For *WAN port* you can bind the tunnel to WAN1, WAN2 or ANY. Since we are building a tunnel on WAN1, we will be specific and select WAN1 on the *WAN Port*.
14. If you have multiple PPPoE sessions on the WAN ports make sure you select the appropriate session.

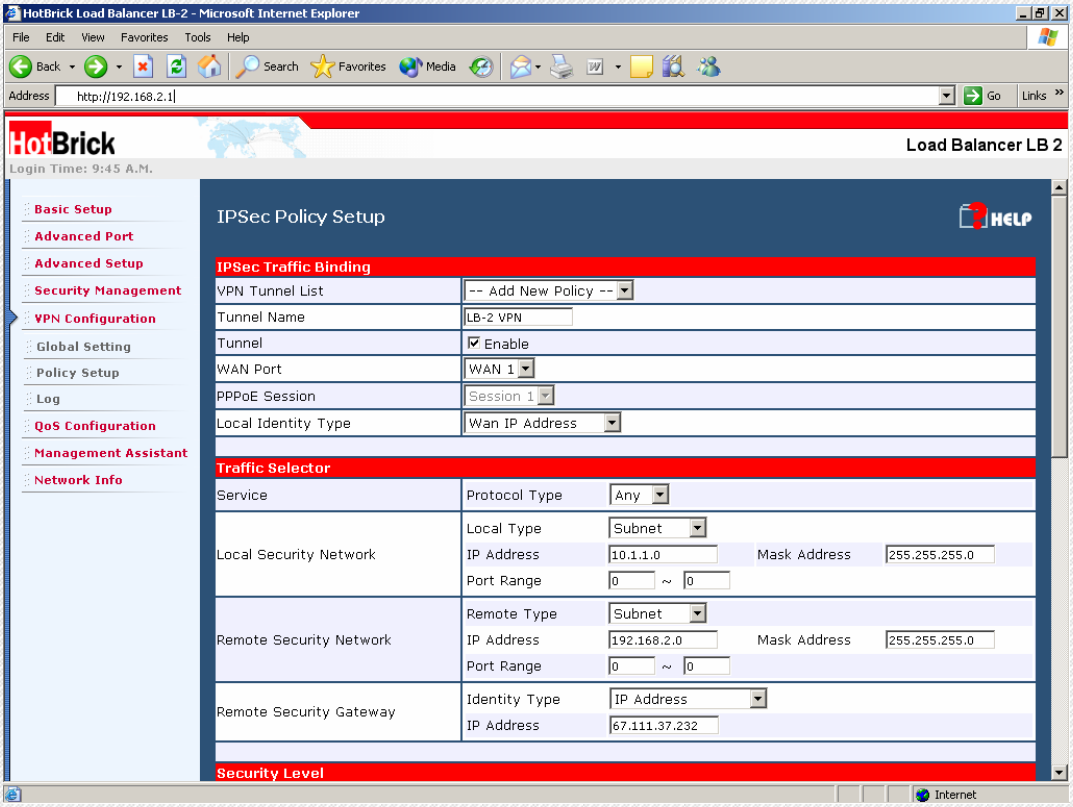

Figure 3 - IPSec Traffic Binding for Site A

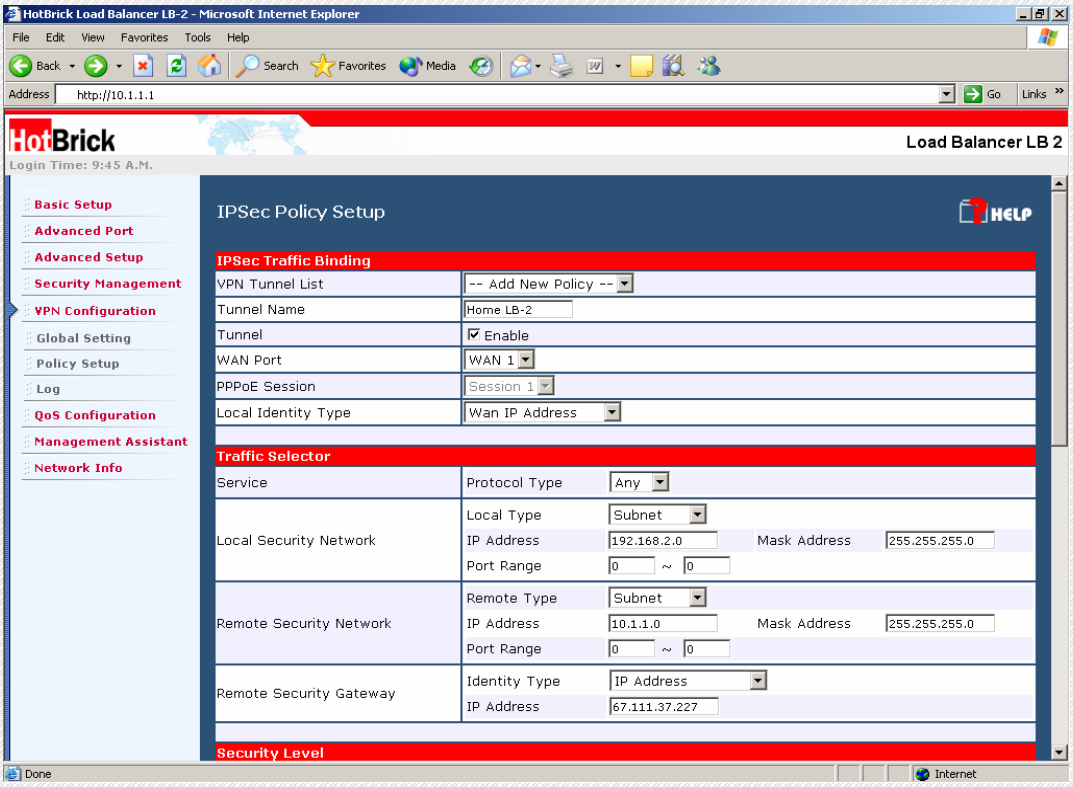

Figure 4 - IPSec Traffic Binding for Site B

15. Under **Traffic Selector**, for **Service** – *Protocol Type* select **ANY**.
16. Under **Local Security Network** , for *Local Type* select **Subnet**.
17. The IP address must reflect the entire subnet. Please see below:
    a. In Figure 3, Site A IP address is 192.168.2.0 and Mask Address 255.255.255.0
    b. In Figure 4, Site B IP address is 10.1.1.0 and Mask Address 255.255.255.0
    c. NOTE – LAN subnets and IP addresses must be different or there will be overlapping.
18. The Port Range can be left at 0 ~ 0.
19. For Remote Security Network, for Remote Type select Subnet.
20. The IP address must again reflect the entire subnet. In Figure 3, the remote security network for Site B is 10.1.1.0. In Figure 4, the remote security network for Site A its 192.168.2.0.
21. For the Remote Security Gateway the gateway type is IP Address. The IP address is the WAN1 IP address of the remote site (Site B).
22. Under Security Level, the VPN IPSec Tunnel will be in ESP (Encapsulating Security Payload) mode.
23. For the Encryption method you can choose from: Null, DES/3DES, or AES. In our example we have chosen 3DES. Please see figure 5 and figure 6.
24. For the Authentication Method you can choose from: Null, MD5, SHA-1/SHA-2. In our example we have chosen MD-5.

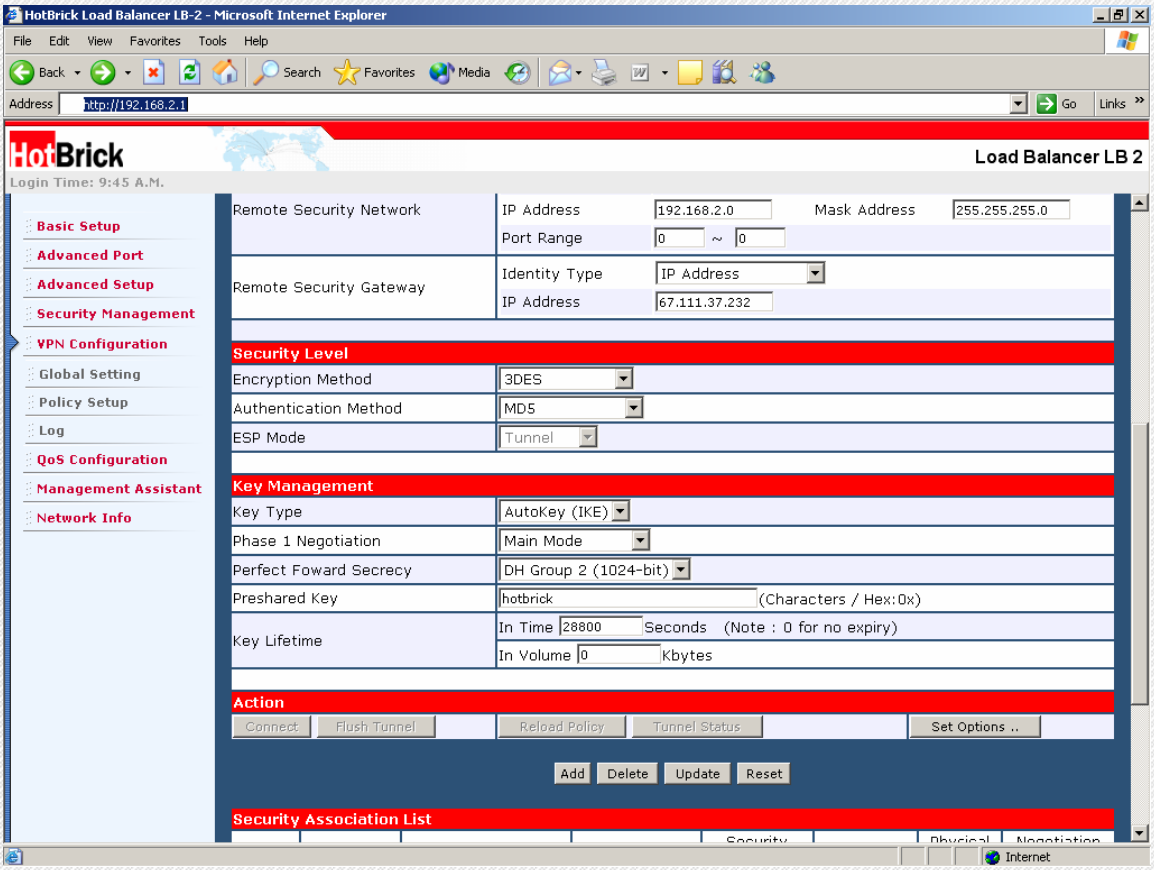

Figure 5 - Policy Setup for Site A

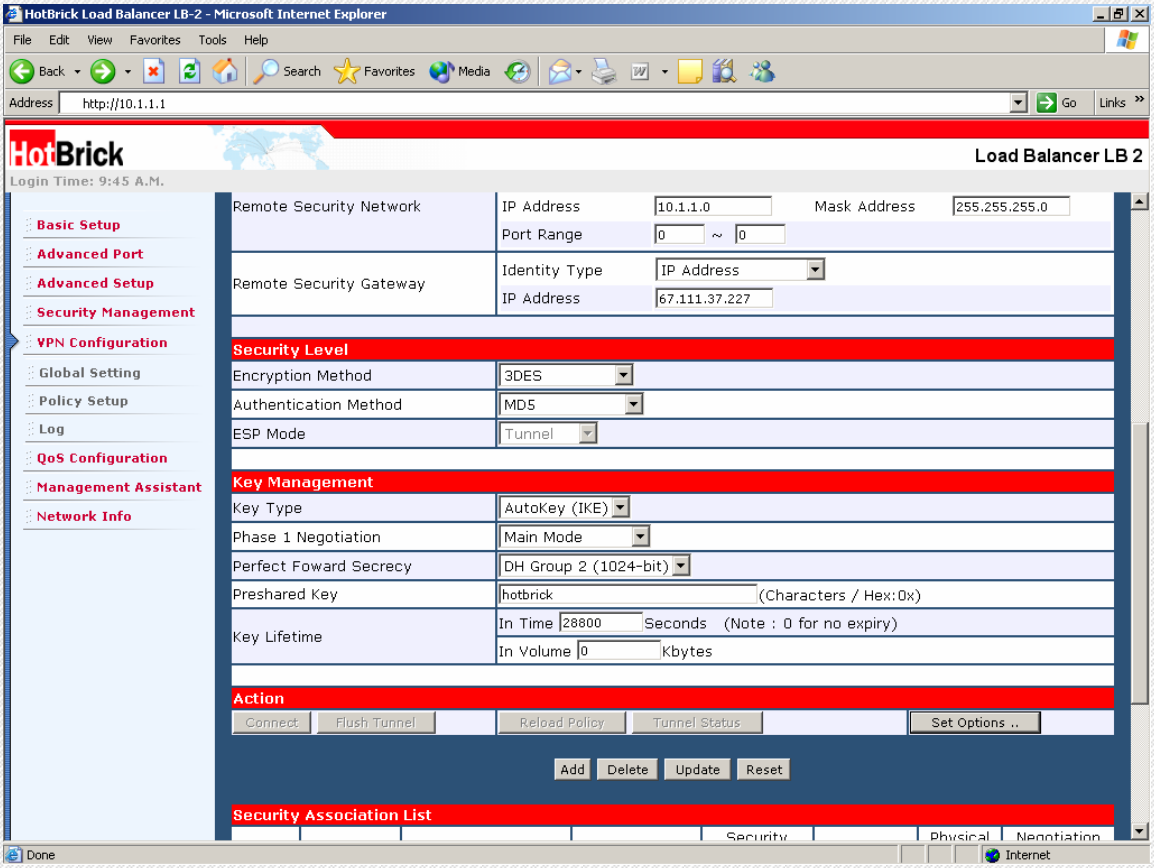

Figure 6 - Policy Setup for Site B

25. Under Key Management there are two types: Autokey (IKE) or Manual Key.
26. If AutoKey (IKE) is selected, your Phase 1 Negotiation can be Main Mode or Aggressive Mode. In our example we used Main Mode.
27. For Perfect Forward Secrecy you can choose to enable it or not. In our example we have used DH Group 2 (1024-bit).
28. The Preshared Key must be characters and/or hexadecimal units. The preshared key entered in our example is “hotbrick”.
29. The Key life time can be set in seconds with zero indicating no expirations. In our example we used 28800 seconds or eight hours.
30. For the service In Volume we left the default 0 Kbytes.
31. If Manual Key was chosen the encryption key and authentication key would have to be entered using characters and/or hexadecimal units. Please see figure 7 below.

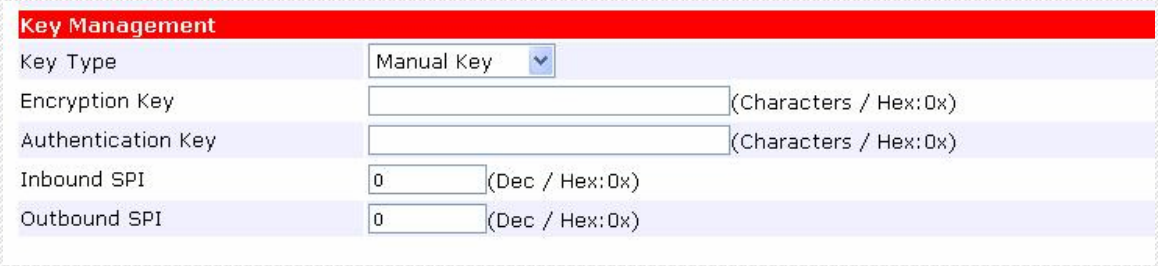

Figure 7- Manual Key.

32. The Inbound and Outbound Stateful Packet Inspection must also be set.
33. Once all these values all entered you click on Add.
34. Now under *Action*, select **Set Options**. This brings you to the **IPSec Policy Options** page. We recommend that you use this section to always keep the tunnels up.
35. Under **Dead Peer Detection Feature**, make sure the enable box is checked.
    Under *Check Method* there are three options:

Heartbeat
ICMP host
DPD (RFC 3706)

In our example we have selected DPD (RFC 3706). Under *Action*, it is important that you select **Keep Tunnel Alive**.

36. Under **Options**, you can enable NetBIOS Broadcast to be able to send NetBIOS traffic through the tunnel. Also enable **Auto Triggered**, to always reconnect the tunnel if the tunnel happens to drop.
37. When you are finished click **Set**. This will take you back to the Policy Setup page, then scroll down to the bottom and under *Action* hit the Update button.
38. You must then configure site two to match the entries in site one.

When you have finished, click on connect on any of the two LB-2s. In our example the connect button was hit on Site A (Initiator) and the tunnel was established to Site B (Responder).

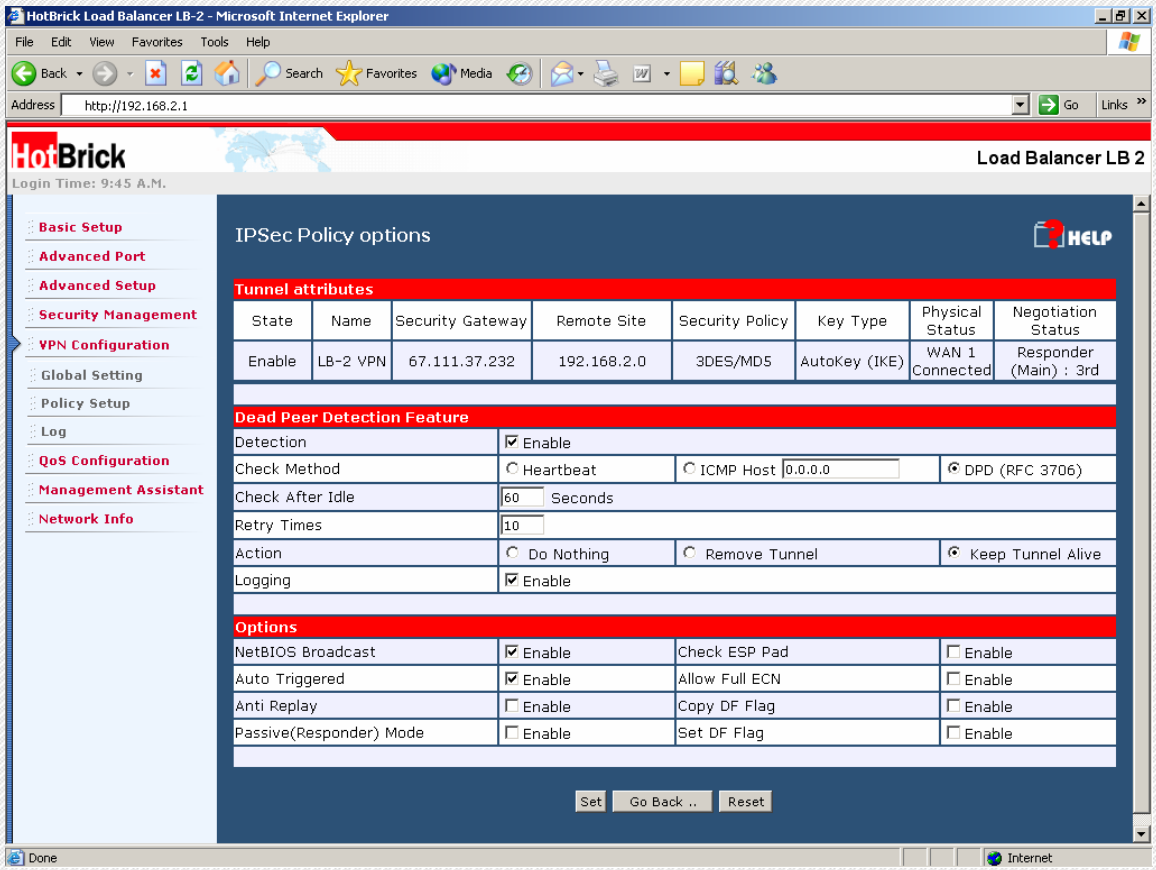

Figure 8 – IPSec Policy Option for Site A

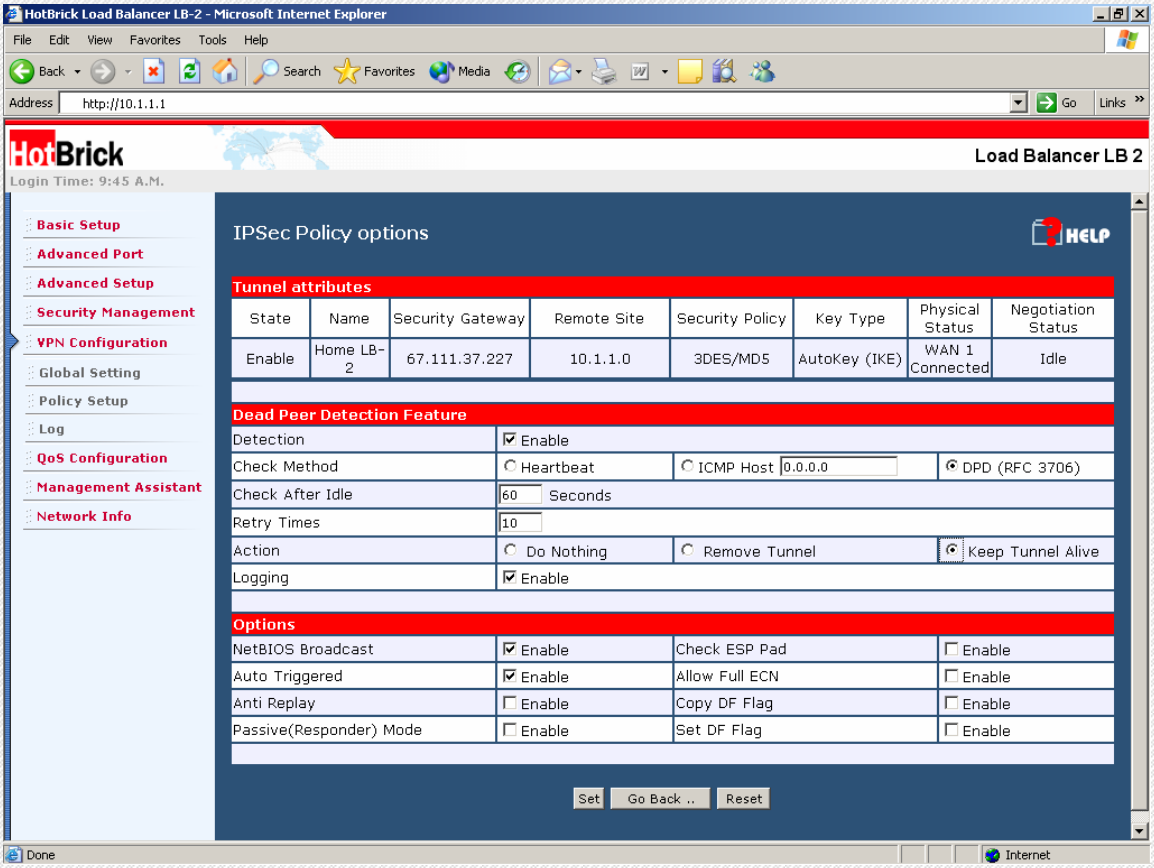

Figure 9 – IPSec Policy Option for Site B

Figures 10 and 11 show the tunnel established under Policy Setup. Figures 11 and 12 show the log with all the phases of the IPSec tunnel established.

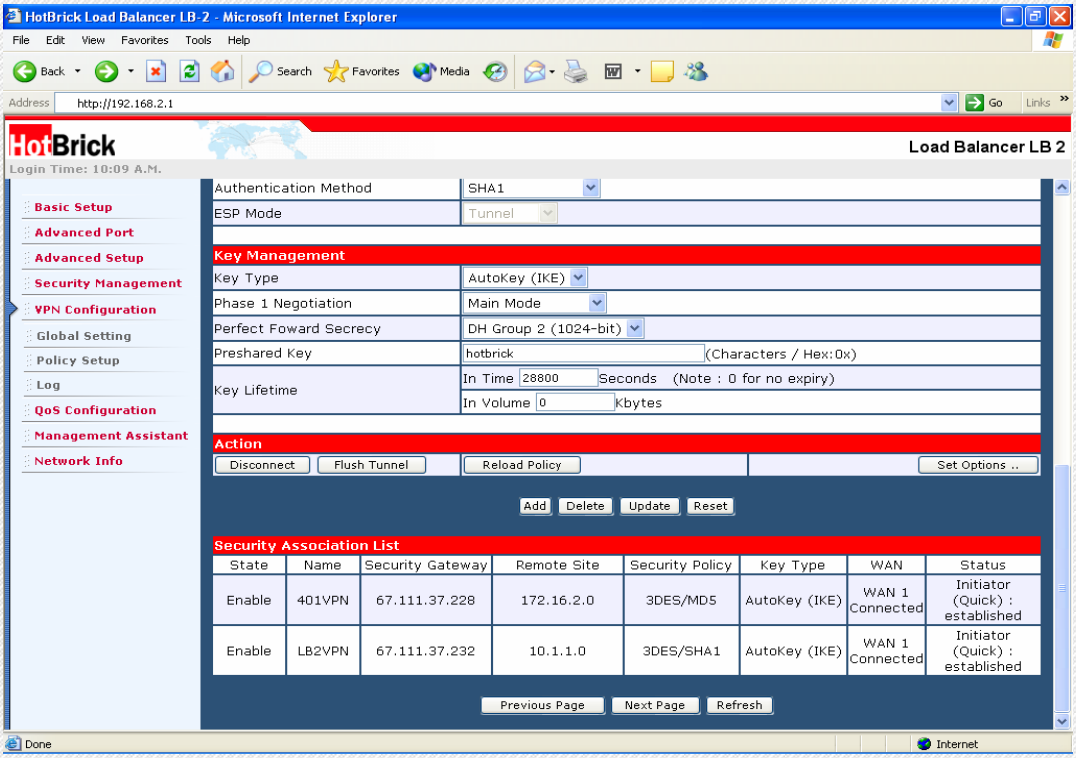

Figure 10 - Site A tunnel established

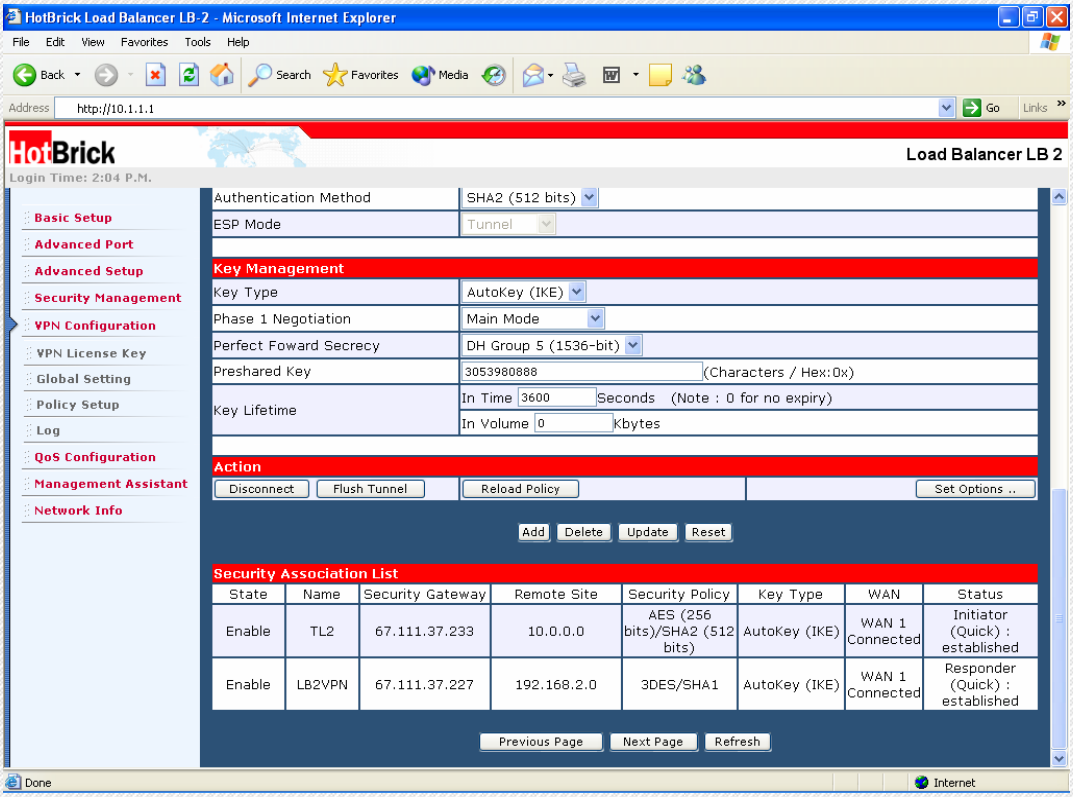

Figure 11 - Site B tunnel established

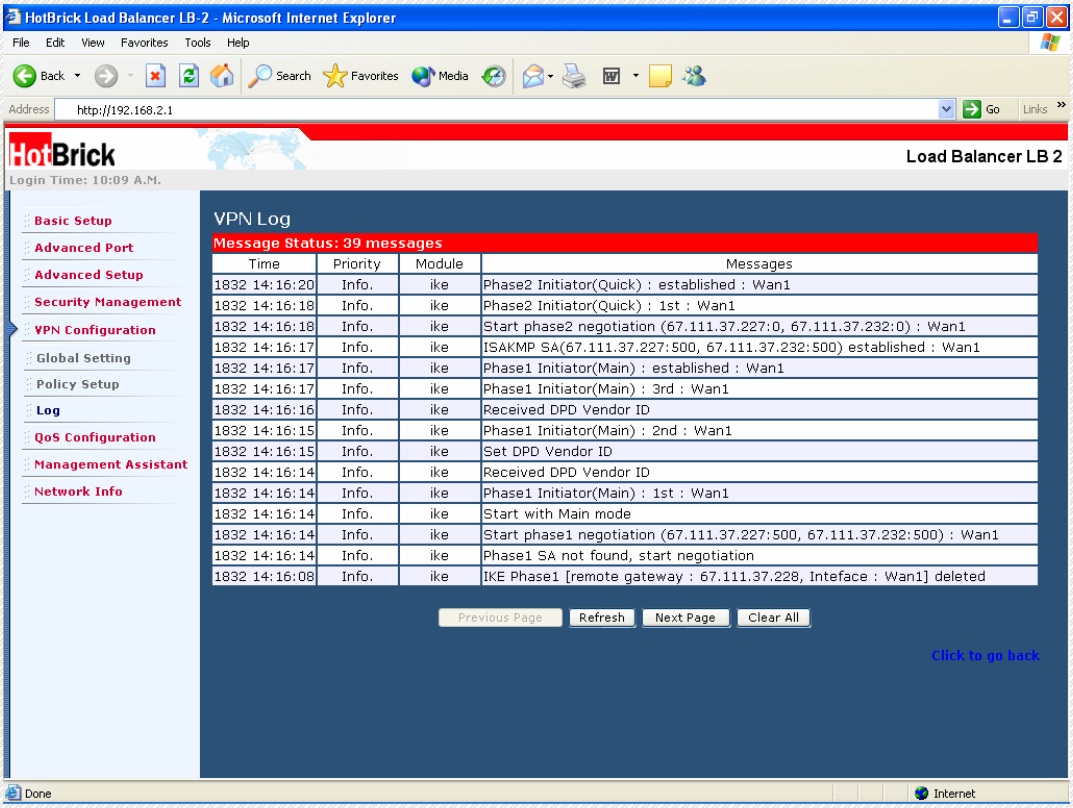

Figure 12 - Logs with tunnel established in Site A

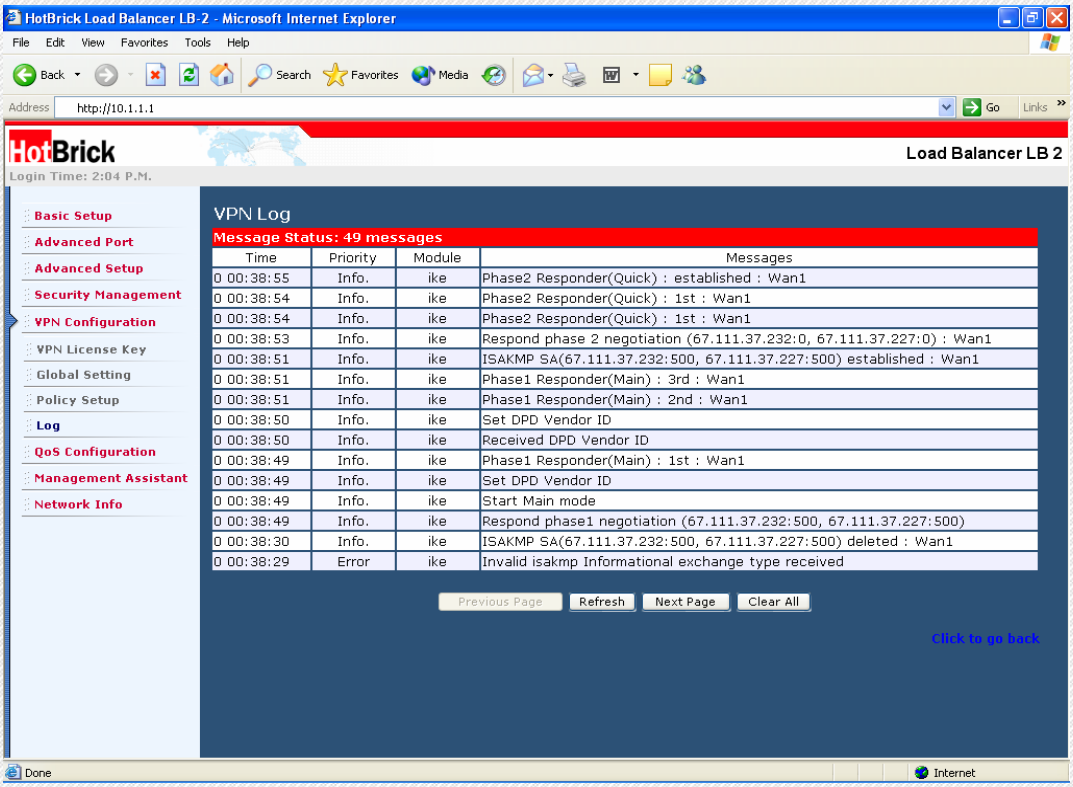

Figure 13 - Logs with tunnel established in Site B

VPN Policy References

IPSec Global Setting

Enable
Enabling WAN 1, WAN 2 or Both will start global setting.

ISAkmp Port
Designed to negotiate, establish, modify and delete security associations and their attributes which was assigned by IANA UDP port 500.

Phase 1 DH Group
Use DH Group 1 (768-bits), DH Group 2 (1024-bits), Group 5 (1536-bits) to generate IP Sec SA Keys.

Phase 1 Encryption Method
There are 3 data encryption methods available: DES, 2DES, and AES.

Phase 1 Authentication Method
There are 2 authentication methods available: MD5 and SHA1 (Secure Hash Algorithm)

Phase 1 SA Life Time
By default the Security Association lifetime is set at 28800 Sec.

Maxtime to complete phase 1
Aim of phase 1 is to authenticate and establish a secure tunnel, which will protect further IKE negotiation. The maximum time default is 30 Sec.

Maxtime to complete phase 2
Maximum time to establish the IPSec SAs. By default the maximum time is 30 Sec.

Log Levels

Select a VPN log level that you like to display on VPN log.

VPN Policy Setup

IPSec Traffic Binding

VPN Tunnel List
Shows tunnels you have entered. The router can be setup to 50 tunnels**.**

Tunnel Name
Distinguishes "tunnels" by names

Tunnel
The tunnel can only be connected when the **ENABLE** check box is selected.

WAN port
You can choose WAN 1, WAN 2 or any to make the VPN connection.

PPPoE Session
Some ISP's offer multiple sessions when using PPPoE to make VPN connections. These PPPoE sessions can be selected to construct VPN tunnels.

Traffic Selector

Service
Protocol Type: Choices are TCP/UDP/ICMP/GRE as your connection protocol. By default the protocol type is "Any".
Local Security Network
These entries identify the private network on the VPN gateway and the hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP Range to make VPN LAN-to-LAN connection.

Remote Security Network
These entries identify the private network on the remote peer VPN router whose hists can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP Range to make VPN connection.

Remote Security Gateway
Select either remote side domain name or remote side IP address (WAN IP Address) as your remote side security gateway.

Security Level

Encryption Method
It specifies the encryption method to use. Data encryption makes the data unreadable if intercepted. There are 3 encryption methods available: DES, 3DES, and AES. The default is null.

Authentication
This specifies the packet authentication mechanism to use. Packet authentication confirms the data's source. There are 3 authentications available: MD5, SHA1 and SHA2.

Key Management

Key – Key Type:
There are 2 key types (manual key and auto key) available for the key exchange management.

Manual Key
If manual key is selected, no key negotiation is needed.

Encryption Key
This field specifies a key to encrypt and decrypt IP traffic.

Authentication Key
This field specifies a key to use to authentication IP traffic

Inbound/outbound
SPI (Security Parameter Index) is carried on the ESP header. Each tunnel must have a unique inbound and outbound SPI and no 2 share the same SPI. Notice that Inbound SPI must match the other router's outbound SPI.

AutoKey (IKE)
There are 2 types of operation modes can be used:
Main Mode accomplishes a phase 1 IKE exchange by establishing a secure channel.
Aggressive Mode is another way of accomplishing a phase 1 exchange. It is faster and simpler than main mode, but does not provide identity protection for the negotiating nodes.

Perfect Forward Secrecy (PFS)
If PFS is enabled, IKE phase 2 negotiation will generate a new key Material for IP traffic encryption & authentication.

Preshared Key
This field is to authenticate the remote IKE peer.

Key Lifetime
This specifies the lifetime of the IKE generated Key. If the time expires or data is passed over this volume, a new key will be renegotiated. By default, 0 is set for no limit.

Options

NetBIOS Broadcast
This is used to forward NetBIOS broadcast across the Internet.

Keep Alive
This is to help maintain the IPSec connection tunnel. It can be reestablished immediately if a connection is dropped.

Anti Replay
This mechanism works by keeping track of the sequence numbers in packets as they arrive.

Passive Mode
When enabled, your PC establishes the data connection.

Check ESP Pad
When checked, this will enable ESP (Encapsulating Security Payload) padding.

Allow Full ECN
Enable will allow full Explicit Congestion Notification (ECN). ECN is a standard proposed by the IETF that will minimize congestion on a network and the gateway dropping packets.

Copy DF Flag
When an IP packet is encapsulated as payload inside another IP packet, some of the outer header fields can be newly written and others are determined by the inner header. Among these fields is the IP DF (Do Not Fragment) flag. When the inner packet DF flag is clear, the outer packet may copy it or set it. However, when the inner DF flag is set, the outer header MUST copy it.

Set DF Flag
If the DF (Do Not Fragment) flag is set, it means the fragmentation of this packet at the IP level is not permitted.