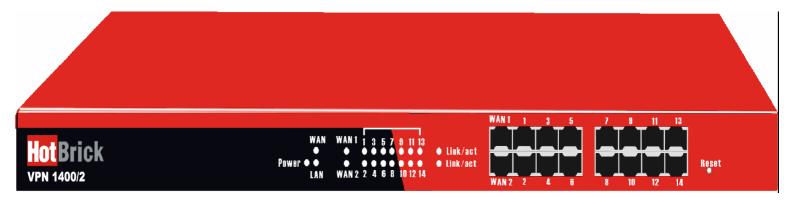
Brick

Dual WAN Firewall VPN 1400/2 User's Guide



Version 1.0 Date : Nov 2006 Please Check www.hotbrick.com for the latest version



-

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

TABLE OF CONTENTS

1: INTRODUCTION		4
Internet Features		4
Physical Details		7
2: QUICK INSTALLATION		
•		
<i>,</i> ,		
		-
PPTP		3
5: ADVANCED CONFIGURATION		4
0		
5		
•		
5		
6: SECURITY MANAGEMENT	40)
Block URL		0
-		
0	44	
	4	
	4	
•		
9: MANAGEMENT ASSISTANT		56
Admin. Setup		6
•		
Syslog		Э



Upgrade Firmware	60
10: DEVICE INFORMATION	
Operation	61
System Status	
WAN Status	
10: DEVICE STATUS	
APPENDIX A SPECIFICATIONS	
APPENDIX B WINDOWS TCP/IP SETUP	
Overview	
TCP/IP Settings	69
APPENDIX C TROUBLESHOOTING	
Overview	
General Problems	
Internet Access	73
APPENDIX D IPSEC TUNNEL EXAMPLES	
Tunnel to HotBrick Unit	74

Copyright HotBrick 2006[®]. All Rights Reserved. Document Version: 1.0

All trademarks and trade names are the properties of their respective owners.



1:Introduction

Congratulations on the purchase of your new Dual WAN VPN Firewall. The Dual WAN VPN Firewall not only provides 2 WAN ports selections – it also provides **Shared Broadband Internet Access** for all LAN users.

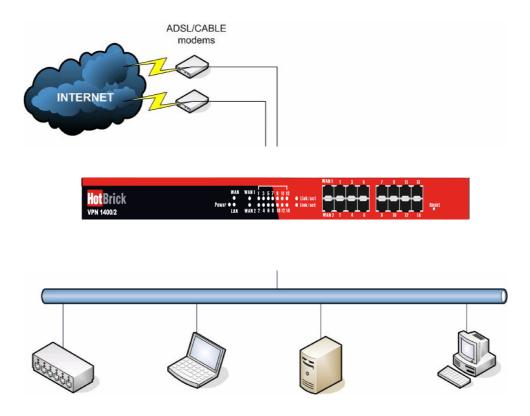


Figure 1-1: Dual WAN VPN Firewall

Internet Features

Dual WAN ports

There are 2 WAN ports available for use on the Dual WAN VPN Firewall. They can function for load-balancing and failover.

Shared Broadband Internet Access

All LAN users can access the Internet through the Dual WAN VPN Firewall by sharing two Broadband modems and connections.

High-Performance multi ADSL Modem Support

The Dual WAN VPN Firewall has two WAN ports, allowing the connection of up to two broadband modems at the same time.

This can provide a greater increase in bandwidth than is allowed by a single modem. Flexible configuration allows each WAN port to use a different type of modem and connection. Additionally, you can determine how the Internet traffic is shared between the 2 modems.



Supports all common Connection Methods

All popular DSL and Cable Modems and connection methods are supported, including Fixed IP, Dynamic IP, PPPoE, and PPTP.

Outbound/Inbound Traffic Load Balancing and Failover

There are many load-balancing methods to allow administrators to manage the traffic from LAN or WAN to maximize bandwidth usage. There are also smart health check methods to protect against connection failure by using failover.

PPPoE Session Management

Multiple PPPoE sessions are supported and you can choose to "map" sessions to individual PCs if desired.

Multiple IP Address Support

If your ISP allocates you multiple public IP addresses, you can "map" them to internal PCs if desired.

Special Application

This feature allows you to use some non-standard applications, where the port number used to reply is not the same port number used by the sender.

Virtual Server

This feature allows Internet users to access your internal Internet servers on your LAN. For standard servers such as Web, FTP or E-Mail servers, only the IP address of the server PC is required. You can also define you own Server types if needed.

Multiple DMZ

A "DMZ" PC will receive incoming connection requests that would normally be blocked. For each IP address allocated by your ISP, a separate "DMZ" PC can be specified. So if your ISP has provided multiple IP addresses, you can have multiple "DMZ" PCs. Each "DMZ" PC has unrestricted 2-way Internet access. This allows you to run programs that are otherwise incompatible with NAT routers like the Multi-WAN VPN Link Balancer.

Access Filter

The network administrator can use the Access Filter to gain fine control over Internet access and applications available to LAN users. Five (5) user groups are available, and each group can be assigned unique access rights.

Block URL

Use this feature to block access to undesirable Web sites by LAN users. You can even have different settings for different groups of PCs.

Session Limit

With the Session Limit feature, when the number of new sessions for the system exceeds the maximum in the sampling time, any new session in the system will be dropped.

System Filter Exception

The firewall rejects every packet with an unrecognized port to avoid port scans by hackers. This requires exception handling in situations where some servers (e.g. SMTP server port 113) or clients need to respond to non-standard packets to indicate aliveness to their communication peers.

VPN (Virtual Private Network)

Up to 50 VPN tunnels are supported, with a fail-over mechanism.



Other Features

16-Port Switching Hub

The Dual WAN VPN Firewall incorporates a 16-port 10 /100BaseT switching hub that allows you to quickly create or extend your LAN.

DHCP Server Support

Dynamic Host Configuration Protocol provides dynamic IP addresses to PCs and other devices upon request. The Dual WAN VPN Firewall can act as a **DHCP Server** for devices on your local LAN.

Multi Segment LAN Support

LANs containing one or more segments are supported, via the Multi-WAN VPN Load Balancer's built-in static routing table or LAN ANY IP settings.

Easy Setup

Use your favorite WEB browser for configuration.

Remote Management

The Dual WAN VPN Firewall can be managed from any PC on your LAN. If the Internet connection is active, the unit can also (optionally) be configured via the Internet.

Password - protected Configuration

Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

HTTP Firmware Upgrade and backup

The web management feature allows you to use HTTP to upgrade new firmware and backup the system configuration from the local or even from the remote site (as long as you enable "Remote Upgrade" and "Remote web-based setup" from the Advanced Feature web page).

Email Alert

A warning email can be sent to the system administrator if one of the WAN ports drops provided two WAN ports are enabled. Also, there is excessive ping notification available.

Syslog

Real time system information can be generated on the web page or a particular machine. This is very useful when monitoring the device.

QoS Configuration.

This function gives specified packets a higher priority for pass-through. This is especially useful if you have real-time applications like Internet phone, video conference etc.

UPnP

If UPnP (Universal Plug & Play) is set to "Enable", the Dual WAN VPN Firewall becomes one of the network devices. This is useful for discovering and controlling network devices, such as the Internet gateway.



Package Contents

The following items should be included:

- □ The Dual WAN VPN Firewall Unit
- □ Power Cord
- □ Quick Installation Guide
- CD-ROM containing the on-line manual.
 Note: If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel

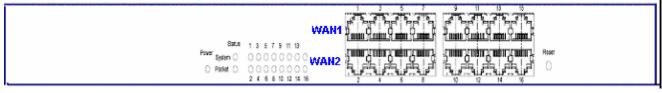


Figure 1-2: Front Panel

Operation of the Front Panel LED's is as follows :

Power	OFF – No Power ON – Normal Operation
Status	ON/OFF – Error
System	Blinking – Normal Operation.
Packets	Blinking – Packets Active ON/OFF – No Packet
Ethernet	Green ON – 100M Linked Yellow ON – 10M Linked Blinking – Data Transmit / Receive. OFF – Not Linked

Ethernet Ports and Reset Bottom

Ethernet Ports	WAN ports: 2 are available for WAN connections. LAN ports: the remaining ports are for LAN (device or hub) usage. Note: Use an Ethernet cable to connect to a normal port or another hub.
Reset Button	When pressed and released, the Dual WAN VPN Firewall will reboot (restart)
	within 1 second. It will reset to factory default settings after you press and hold the reset button over 3 seconds

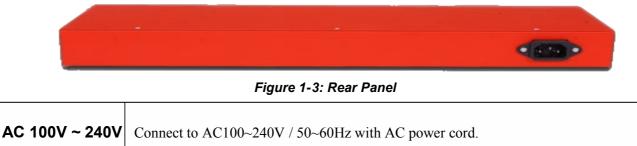


Some Status and Error conditions are indicated by combinations of LED's, as shown below

LED Action	Condition
Status – System & Packets flash alternatively	Firmware Download in progress
Status – System & Packets flash concurrently	MAC address not assigned
Status – System (Solid Off) & Packets (Solid On)	SDRAM error
Status – System (Solid Off) & Packets (Flash once)	Timer/Interrupt error
Status – System (Solid Off) & Packets (Flash twice)	LAN/WAN error



Rear Panel



Default Settings

When the Dual WAN VPN Firewall has finished booting, all configuration settings will initially be set to the factory defaults, including:

- □ *IP Address* set to its default value of 192.168.1.1, with a *Network Mask* of 255.255.255.0
- DHCP Server is enabled
- User Name: admin
- □ Password cleared (no password)

TFTP Download

This setting should be used only if your Dual WAN VPN Firewall interface can't be accessed, and you wish to restore it by uploading new firmware. In that case use the following procedure:

- 1. Power on the Dual WAN VPN Firewall.
- 2. Use the supplied Windows utility or a TFTP client program to apply the new firmware. If you are using the supplied Windows TFTP program, the screen will look like the following example.

😹 TFT	P ¥1.01	K
Local Serve:	BIOW38	
Upgra Statu	ade Firmware Save Configuration Set to Default Help Exit	

Figure 1-4: Windows TFTP utility

- □ Enter the name of the firmware upgrade file on your PC, or click the "Browse" button to locate the file.
- □ Enter the LAN IP address of the Dual WAN VPN Firewall in the "Server IP" field.
- □ Click "Upgrade Firmware" to send the file to the Multi-WAN VPN Link Balancer.
- 3. When uploading is finished the unit should function normally, **using the default settings.**



Note:

The supplied Windows TFTP utility also allows you to perform three (3) additional operations:

- □ Save the current configuration settings to your PC (use the "Save Configuration" button).
- □ Restore a previously saved configuration file to the Dual WAN VPN Firewall (use the "Upgrade Firmware" button).
- □ Set the Dual WAN VPN Firewall to its default values (use the "Set to Default" button).



2: Quick Installation

Overview

Initial Basic Setup of your Dual WAN VPN Firewall involves the following steps:

- 1. Attach a PC to the Dual WAN VPN Firewall in port $3 \sim 16$, and configure your LAN.
- 2. Install your Dual WAN VPN Firewall in your LAN, and connect the Broadband Modem or Modems.
- 3. Configure your Dual WAN VPN Firewall for Internet Access.
- 4. Configure PCs on your LAN to use the Dual WAN VPN Firewall.

Requirements

- □ 1 or 2 WAN connections, each with an active Internet Access account with an ISP.
- □ Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- □ TCP/IP network protocol must be installed on all PCs.

Procedure

1: Configuring the Dual WAN VPN Firewall for your LAN

- 1. Use a standard LAN cable to connect your PC to any LAN port (3 -16) on the Dual WAN VPN Firewall. (Default 2 WAN ports from port 1-2)
- 2. Connect the power cord into a power outlet on the rear panel of Dual WAN VPN Firewall.
- 3. Start your PC. If your PC is already running, restart it. It will then obtain an IP address from the Dual WAN VPN Firewall.
- 4. Start your WEB browser.
- 5. In the *Address* or *Location* box enter: HTTP://192.168.1.1
- 6. You will be prompted for the User Name and password, as shown below.

Enter Ne	twork Passv	vord	<u>?</u> ×
? >	Please type yo	our user name and password.	
4	Site:	192.168.1.1	
	Realm	NeedPassword	
	<u>U</u> ser Name	admin	
	Password		
	□ <u>S</u> ave this pa	assword in your password list	
		OK Cance	

Figure 2-1: Password Dialog

Enter *admin* for the "User Name" and leave the "Password" blank.

- \Box The "User Name" is always *admin*.
- \Box You can and should set a password, using the following *Admin Password* screen.



No Response?

□ Is your PC using a Fixed IP address?

If so, you must configure your PC to use an IP address within the range 192.168.1.2 to 192.168.1.254, with a *Network Mask* of 255.255.255.0. See *Appendix B – Windows TCP/IP Setup* for details.

- □ Check that the Dual WAN VPN Firewall is properly installed, LAN connection is OK, and it is powered ON.
- 7 After the login, you will see the **Admin Password** screen, as shown below. Assign a password by entering it in the "Password" and "Verify Password" Fields.

н	otBrick		HotBri	ck VPN 140	00/2		
Log	in Time: 1:53 P.M.						
		Management Assi	stant				😪 Xelp
		Admin Setup Em	ail Alert SNMP	Syslog Upgrade F	irmware		
	Quick Installation	Remote Access Conf Remote Upgrade	iguration Remote Setup	Access Port		ved Remote IP	
	Load Balancing	Enabled	Enabled	8080	0.0.0.0	~ 0.0.0.0	
	Advanced WAN	Administrator Passw	rord				
	Advanced Configuration	User Name admin	Password	Verify Password			
	Security Management	aumin					
	VPN Configuration	Submit		Cancel			
	QoS Configuration						
	Management Assistant						
	Device Status						
	Device Information						

Figure 2-2: Home Screen (Admin. Setup)



8. Select LAN & DHCP from the menu. You will see a screen like the example below.

otBrick		Hot	Brick VPN 1	1400/2
gin Time: 1:53 P.M.				
	Quick Installat			se ilei
Quick Installation	LAN IP Configura IP Address 192.168.1.1		Subnet Mask 255.255.255.0	(ex. 255.255.25.0)
Advanced WAN Advanced Configuration	Optional Configu DHCP Server	LAN Any IP		
Security Management ¥PN Configuration	DHCP Configura Lease Time	tion DNS Server IP for Cli		Offered IP Range
QoS Configuration Management Assistant Device Status	60 (min.)	1. 192.168.1.1	2. 192.168.1.1 Cancel	192.168.1.2 ~ 192.168.1.100
Device Information				

Figure 2-3: LAN & DHCP Setup

- 9. If your LAN already has a DHCP Server, and you wish to continue to use it, the following configuration is required.
 - □ The DHCP Server function in the Dual WAN VPN Firewall must be **disabled.** This setting is on the *LAN & DHCP* screen.
 - □ Your DHCP Server must be configured to provide the Dual WAN VPN Firewall LAN IP address as the "Default Gateway".
 - □ Your DHCP Server must provide correct DNS addresses to the PCs.

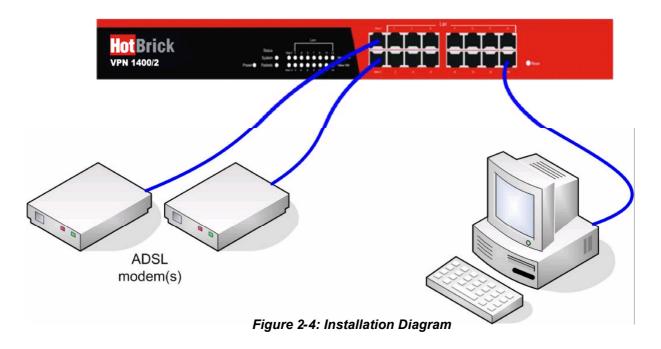
10. Ensure these settings are suitable for your LAN.

- 11. The default settings are suitable for many situations.
- 12. See the following table for details of each setting.

Save your data, then go to Installing the Dual WAN VPN Firewall in your LAN.



HotBrick, Tel: 305-398-0888, Fax: 305-398-5966 Installing the Dual WAN VPN Firewall on your LAN



- 13. Ensure the Dual WAN VPN Firewall and the DSL/Cable modem are powered OFF. Leave the modem or modems connected to their data line.
- 14. Connect the Broadband modem or modems to the Dual WAN VPN Firewall.
 - \Box If using only one (1) Broadband modem, connect it to WAN port 1.
 - □ Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.
- 15. Use standard LAN cables to connect PCs to the LAN ports on the Dual WAN VPN Firewall.
 - □ Both 10BaseT and 100BaseT connections can be used simultaneously.
 - □ If you need to connect the Dual WAN VPN Firewall to another Hub, use a standard LAN cable to connect any LAN port on the Dual WAN VPN Firewall to a standard port on another hub. Any LAN port on the Dual WAN VPN Firewall will automatically act as an "Uplink" port when required.
 - □ If a device is set to 2 WAN ports from port 1 to 2, the others are LAN ports from port 3 to 16.
- 16. Power Up
 - \Box Power on the Cable or DSL modem or modems.
 - □ Connect the supplied power cord to the Dual WAN VPN Firewall and power up.
- 17. Check the LEDs
 - \Box The **Power** LED should be ON.
 - □ The *Link/ACT* LED should be ON, if the corresponding WAN port is connected to a broadband modem.
 - □ For each PC connected to the LAN ports, the corresponding **LAN** LED (either **10/Yellow** or **100/Green)** should be ON.



3. Quick Installation - LAN & DHCP

Select *LAN & DHCP* from the menu. You will see a screen like the example below.

otBrick	HotBrick VPN 1400/2					
gin Time: 1:53 P.M.						
	Quick Installat Primary Setup				se Heip	
Quick Installation	LAN IP Configure	ation	Subnet Mask			
Load Balancing	192.168.1.1	(ex. 192.168.1.1)	255.255.255.0	(ex. 255.255.255.0)		
Advanced WAN Advanced Configuration Security Management	Optional Configu DHCP Server ✓ Enabled	LAN Any IP				
VPN Configuration QoS Configuration	DHCP Configura Lease Time 60 (min.)	tion DNS Server IP for Cl 1. 192.168.1.1	ient 2. 192.168.1.1	Offered IP Range 192.168.1.2 ~ 192.168.1.10	0	
Management Assistant Device Status		Submit	Cancel		OHCP List	
Device Information						

Figure 3-1: LAN & DHCP

Ensure these settings are suitable for your LAN.

- \Box The default settings are suitable for most networks.
- \Box See the following table for setting details.



LAN IP Configuration:

- □ **IP address -** for the Dual WAN VPN Firewall, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
- □ **Subnet Mask** -The default value 255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Dual WAN VPN Firewall is attached (the same value as the PCs on that LAN).

DHCP server configuration :

- □ DHCP Server Setup If enabled, the Dual WAN VPN Firewall will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default and recommended value is "Enable". (Windows Systems, by default, act as DHCP clients. This setting is called *Obtain an IP address automatically.*)
- □ **DHCP Server Setup -** If you are already using a DHCP Server, the DHCP Server setting must be **disabled**, and the existing DHCP server must be set to provide the IP address of the VPN Dual WAN VPN Firewall as the *Default Gateway*.
- □ **Client Lease Time** This is the period of time that a DHCP server leases an IP address to a DHCP client.

DHCP IP address range

- □ Offered Range fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.
- □ **Free Entries** indicates how many DHCP entries are not currently allocated, and available.

ARP Proxy

Enable this ONLY if the LAN port has an IP address in the same address range as the WAN port(s). This means that all PCs using this Gateway must have valid fixed external (Internet) IP addresses. If enabled, enter the IP address range used on your LAN.

LAN Any IP Setup

The default is disabled. If you enable "LAN ANY IP", that means no matter what static IP address your client has, the client does not need to change their IP address to access the Internet. This is normally used when the client is on a different IP segment than the LAN segment.



DHCP Client List

This table shows the IP addresses that have been allocated by the DHCP Server. For each allocated address, the following information is displayed.

□ Name – The ""hostname"" of the PC. In some cases, this may not be known.

□ MAC Address – The physical address (network adapter address) of the PC.

 \Box IP Address – The IP address allocated to this PC.

 \Box Type – Indicates IP address to be dynamic or static.

□ Status – If leased the IP address was allocated by this DHCP Server.

 \Box Time Left – The time left before the lease expires



Quick installation - Primary setup

Connection mode

- **Enable** Select this if you have connected a broadband modem to this port.
- □ **Disable –** Select this if there is no broadband modem connected to this port.

 \Box **Backup** – Use this if you have a broadband modem on each port, and wish to normally use only one. Select *Enable* for the primary port, and *Backup* for the secondary port. The *Backup* port will only be used if the primary port fails.

Connection type (Check the data supplied by your ISP, and select the appropriate option)

- □ **Static IP** Select this if your ISP has provided a Fixed or Static IP address. Then enter the data into the *Address Info* fields.
- □ **Dynamic IP** Select this if your ISP provides an IP address automatically when you connect. You can ignore the *Address Info* fields.
- □ **PPPoE** Select this if your ISP uses this method. (Usually, your ISP will provide some PPPoE software. This software is no longer required, and should not be used.) When this method is selected, you must complete the *PPPoE dialup* fields.
- **Note:** If using the PPTP connection method, select *Static IP* or *Dynamic IP*, as appropriate, according to the IP address method used by your ISP.

Address Info

This is for *Static IP* users only. Enter the address information provided by your ISP. If your ISP provided multiple IP addresses, you can use the *Multi-DMZ*

DNS

This is for *Static IP* users only. Enter the address information provided by your ISP. If your ISP provided multiple IP addresses, you can use the *Multi-DMZ*

Optional

- □ **Host name** This is required by some ISPs. If your ISP provided a Host Name, enter it here. Otherwise, you can use the default value.
- □ **Domain name** This is required by some ISPs. If your ISP provided a Domain Name, enter it here. Otherwise, you can use the default value.
- □ **MAC address** Some ISP's record your MAC address (also called "Physical address" or "Network Adapter address"). If so, you can enter the MAC address required by your ISP in this field. Otherwise, this should be left at the default value.



3 : Loadbalancing

This screen is only operational if using Internet connections on both WAN ports

	tBrick			Hoti	Brick [°]	VPN 1	.40	0/2				
	Time: 1:53 P.M.											
		Load Balan	_									- Salel
		Load Balanc										
	uick Installation	Load Balanci Enabled	ng Configuratio	m								
	.oad Balancing	Load Balancing	a Base on			rtes Tx + Rx		~				
•	dvanced WAN				_,		AN 1			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	AN 2	
A	dvanced Configuration	Loading Share				5	96			5	96	
-	curity Management											
_			Subm	it		Ca	rcel					
_	N Configuration											
Qo	S Configuration	Current Stati		Loading	1 Share	Curre	ntloa	adina		Current	Bandy	width
ча	nagement Assistant	Interface	Status	Default	Current	Session	Byte	Packe		Download		Upload
De	vice Status	WAN 1 WAN 2	Disconnected Disconnected	50 % 50 %	50 % 50 %	1	3		1	0 bytes/sec 0 bytes/sec		0 bytes/sec 0 bytes/sec
Dev	ice Information											
		Overall Statis						Overa	п ву	tes Statistics		
		Interfac	3	Loading Sha	re	Rece				Transmitted		Total
		WAN 1 WAN 2		0%				о кв о кв			окв	

Figure 3-2: Load Balance

Load balancing – Load Balancing

□ **Enable** – Use this to enable your Load Balance settings. Unless this is checked, the other settings on this screen have no effect.

□ **Balance Type –** Select the desired option:

Bytes rx+tx – Traffic is measured by Bytes. Packets rx+tx – Traffic is measured by Packets. Sessions established – Traffic is measured by Sessions. IP Address – Traffic is measured by IP Address.

□ Loading Share on WAN 1 – Enter the percentage (%) of traffic to be sent over WAN 1. If one WAN port connection has greater bandwidth than the other, the one with the greater bandwidth should be given a higher percentage of traffic than the other.

NAT statistics This section displays the current data about WAN 1 and WAN 2. You can use this information to help you "fine-tune" the settings above.

Interface statistics This section displays cumulative statistics. Use the "Restart Counters" button to restart these counters when required.



4 : Advanced WAN

Advanced WAN Port Options PPpc PTP uad Balancing Advanced Configuration Security Management WAN port WAN 1 MTU 1500 Bytes Connection Health Check Bridge Option Bridge Option Bridge Option Bridge Option Bridge Options (For all interfaces) Transparent Bridge Options (For all interfaces) ARP Tables Size 22 Entries Clear ARP Tables View ARP Tables.	Login Time: 1:53 P.M.			k VPN 1400/2	
Unick Instantion WAN Port WAN 1 MTU 1500 Bytes Load Balancing Connection Health Check Method Advanced Configuration ICMP HTTP Traffic Interval Alive Indicator Security Management 60 sec. Fransparent Bridge Option Bridge Mode NetBIOS Broadcast VPN Configuration Enabled Enabled Oos Configuration Transparent Bridge Options (For all interfaces) Transparent Assistant Traffic Management Strict Binding Device Status AP Tables Size 32 Entries			РОЕ РРТР		<i>≈</i> . <mark>#</mark> 18
Advanced WAN Method Interval Alive Indicator Advanced Configuration ICMP HTTP Traffic Interval Alive Indicator Security Management 60 sec. Interval Interval Interval VPN Configuration Bridge Mode NetBIOS Broadcast Interval Interval QoS Configuration Bridge Mode NetBIOS Broadcast Interval Interval Management Assistant Transparent Bridge Options (For all interfaces) Interval Interval Device Status AP Tables Size 32 Entries Clear ARP Tables View ARP Tables.		WAN Port		0 Bytes	
Security Nanagement Bridge Option Bridge Mode NetBIOS Broadcast VPN Configuration Enabled QoS Configuration Transparent Bridge Options (For all interfaces) Nanagement Assistant Traffic Management Device Status ARP Tables Size Device Information View ARP Tables.	Advanced WAN	Method	Interval	Alive Inc	licator
Security Management Bridge Mode NetBIOS Broadcast VPN Configuration Enabled Enabled QoS Configuration Transparent Bridge Options (For all interfaces) Load Balancing Management Assistant District Binding Close Binding Load Balancing Device Status ARP Tables Size 32 Entries Clear ARP Tables View ARP Tables.	Advanced Configuration				
Viccompanyance Transparent Bridge Options (For all interfaces) Nanagement Assistant Traffic Management Device Status ARP Tables Size Device Information View ARP Tables	Security Management	Bridge Mode			
Management Assistant Traffic Management Strict Binding Loose Binding Load Balancing Device Status ARP Tables Size 32 Entries Clear ARP Tables View ARP Tables	¥PN Configuration	Enabled	Enabled		
Nanagement Assistant Traffic Management No IP Translation Device Status ARP Tables Size 32 Entries Clear ARP Tables View ARP Tables Device Information Image: Clear ARP Tables View ARP Tables Image: Clear ARP Tables View ARP Tables	QoS Configuration	Transparent Bridge			
evice Information	anagement Assistant	Traffic Management	 Strict Binding 		CLoad Balancing
	evice Status	ARP Tables Size	32 Entries	Clear ARP Tables	View ARP Tables
Submit Cancel	Device Information				
		Submit		Cancel	

Port options

Connection validation

- □ Health Check If disabled, the Alive Indicator Check is not performed. The default is enabled. Health checking is performed by ICMP echo request and HTTP packets to the specified destination that could be either: the Name or IP Address the user specified in the "Alive Indicator" input box or the gateway of the WAN interface used if "Alive Indicator" input box is blank.
- □ Alive Indicator This is the IP address used to check if the WAN connection is operating. The Dual WAN VPN Firewall will contact this system to check if the WAN connection is working. Change this address if you wish. Default is the gateway IP. Note: This is not used for PPPoE connections.
- □ **MTU** The Maximum Transmission Unit determines the packet size to be used on the WAN interface. Normally, this does not need to be changed, but if your ISP advises you to use a specific MTU, enter it here.



Transparant bridge option

- □ **Bridge Mode** If set to Enable, this WAN port does not use NAT or the Load Balance function when both the LAN and WAN have real IP addresses on the same network segment.
- □ **NetBIOS Broadcast** This function allows you to access files through Microsoft Network Neighborhood if it is enabled.

□ Traffic Management

Strict Binding: traffic from bridged hosts (eg. transparent to WAN 1) can only go through that specified WAN(eg. WAN 1) interface.

Loose Binding: Traffic from bridge hosts (eg. transparent to WAN 1) can go thru the alternative WAN (eg.WAN 2) interface when bind interface (eg. WAN 1) is down, it acts like a fail over mechanism for transparent bridge mode.

Load Balancing: Traffic from bridge hosts (eg. transparent to WAN 1) can go thru either WAN (eg. WAN 1 or WAN 2) interface based on loading mechanism specified in the load balance section, it's acting like as a load balancing mechanism for transparent bridge mode.

ARP Table – the ARP table is used by the device to determine the bridge hosts' location (eg. inside/outside WAN and which WAN). Its size can be adjusted if needed. View ARP
 Tables displays ON/OFF for bridge mode on each WAN port. Clear ARP Tables disables bridge mode on all WAN ports.



The screen is required in order to use multiple PPPoE sessions on the same WAN port. It can also be used to manually connect or disconnect a PPPoE session.

Advanced WAN – PPPoE

Time: 1:53 P.M.							
	Advanced		_				Ŵ
	Port Option	IS PPPOE	РРТР				
Juick Installation		Port & Sessio		_			
.oad Balancing	WAN Port		_	~			
	PPPoE Sessio		S	ession 1 🚩			
Idvanced WAN	PPPoE Sessio	in MTU		Bytes			
dvanced Configuration	WAN IP Acc	ount					
ecurity Management	User Name						
PN Configuration	Password						
PN configuration	Verify Passw	ord					
loS Configuration	Options		-				
1anagement Assistant	Specified Fix Assigned Hos		0.	0.0.0	(ex. xxx.xxx.xxx.xx	0	
evice Status	Assigned Hos	it Name					
	PPPoE Auto	Dialup					
evice Information	Cor	Auto Dialup inect-on-dema	nd	Disco	onnect After Idle	Echo Time	Echo Retr
	Cur	Enabled	114	min	utes(-1:Always-on)	seconds	times
	Add	Delete		Update	Cancel		Connect
	Connection WAN		WAN IP /	v d d e	Host Name	PPPoE MTU	Ctatur
	WAN	Session	WAN IP 3	adur.	HUSCINAME	PPPUE MITO	Status

Select WAN port & Session

WAN Port - Selected WAN port using the PPPoE connection

PPPOE Session – Usually the ISP provides multiple floating real IPs for PPPOE. Each WAN port can have up to 8 PPPoE sessions with different IP addresses, if your WAN port is using a PPPoE connection.

PPPOE Session MTU – The Maximum Transfer Unit for PPPoE packet data. Leave it at the default, unless the ISP specifies a different PPPoE packet data size. The default value of MTU is 1492 bytes.

WAN IP Account

- □ **User Name** Enter the PPPoE user name assigned by your ISP.
- □ **Password** Enter the PPPoE password assigned by your ISP.
- □ **Verify Password** Re-enter the PPPoE password assigned by your ISP.



Advanced WAN PPTP

Brick ne: 1:53 P.M.		 	HotBrick VP	N 1400/2		
	Advanced Wi	AN PPPoe PPT	P			⊗a<mark>He</mark>
k Installation	WAN Port					
Balancing	PPTP MTU		Bytes			
inced WAN	WAN IP Accour	nt	_			
nced Configuration	Password					
rity Management	Verify Password					
configuration	Server IP Addre		0.0.0.0 (ex. xxx.xxx.xxx.xxx)		
Configuration			dress 0.0.0.0			
igement Assistant			Mask 0.0.0.0			
ce Status	PPTP Auto Dial					
e Information	Au	uto Dialup	Disconne	ect After Idle	Echo Time	Echo Retry
		ct-on-demand Enabled	minute	s(-1:Always-on)	seconds	times
	Update		Cancel	I		Connect
	Connection Sta WAN W	atus AN IP Addr.	PPTP IP Address	PPTP Server	PPTP MTU	Status

Advanced WAN

WAN Port - Select the desired WAN port (click desired WAN on Connection Status). The data of the selected port will then be displayed in the *WAN IP Account* section. **PPTP MTU** – Maximum transfer unit for PPTP. The default value is 1460

WAN IP Account

- □ **User Name** The PPTP user name (login name) assigned by your ISP.
- □ **Password** The PPTP password associated with the *User Name* above. This is assigned by your ISP, and used to login to the PPTP Server.
- □ **Verify Password** Re-enter the PPTP password assigned by your ISP.
- □ Server IP Address Enter the IP address of the PPTP Server, as provided by your ISP.
- □ **Static IP Adress –** If you have a fixed IP address enter it here. Otherwise this field should be left at 0.0.0.0

Connection Status – This displays the current PPTP connection status.



5 : Advanced Configuration

	Advanced Configuration		X
		I Application Advanced Feature NS Multi DMZ NAT Setting	
Quick Installation		NS Multi DMZ INAT Setting	
Load Balancing	Host Network Identity Host Name [Required]		
Advanced WAN	MAC Address [Required]	00-00-00-00-00 MAC	
	Select Group	Default V	
Advanced Configuration	Reserve in DHCP	Enabled	
Security Management	Reserved IP Address	0.0.0.0 DHCP List	
VPN Configuration		0.0.0.0	
QoS Configuration	Host Network Binding Option		
Que configuration	Binding WAN Port / Session	Enabled	
Management Assistant	Binding method	OStrict Binding OLoose Binding	
Device Status	Select WAN Port	WAN 1 V	
Device Information	Select PPPoE Session	Session 1 💌	
	Add Delete	Update Cancel	
	Host & Group List		
	Name MAC Address	Group Reserve IP in DHCP Port/Session(PP	PoE) Binding
		Status IP Address Status Method	Port Ses

This feature is used in the following situations:

- □ You have Multi-Session PPPoE, and wish to bind each session to a particular PC on your LAN.
- □ You wish to use the *Access Filter* feature. This requires that each PC is identified by using the *Host IP* screen.
- □ You wish to have different **Block URL** settings for different PCs. This requires that each PC is identified by using the **Host IP** screen. (You do not have to use the Host IP feature to apply the same **Block URL** settings to all PCs.)
- □ You wish to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "Obtain an IP address automatically") while gaining the benefits of a fixed IP address. The PC's IP address will never change, so it can be accessed by other people and applications.

Host IP – Host Network Identity

Host network identity

This section identifies each Host (PC)

- □ **Host name** Enter a suitable name. Generally, you should use the "Hostname" (computer name) defined on the Host itself.
- □ MAC Address Also called *Physical Address* or *Network Adapter Address*. Enter the MAC address of this host.
- □ Select Group Select the group you want this host to join.



- Reserve in DHCP Select Enable to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "obtain an IP address automatically") while having an IP address that never changes.
- □ **Reserved IP Address** Enter the IP address you wish to reserve, if the setting above is *Enable*. Otherwise, ignore this field.

Host Network Binding

- □ **Binding WAN Port / Session** Select *Enable* if you wish to associate this PC with a particular PPPoE session. All traffic for that PC will then use the selected PPPoE port and session.
- □ **Binding Method** Suppose your PC is bound to WAN1 port, now you are selecting "Strict Binding". If WAN1 port is disconnected, your packets cannot go out through the other WAN port, if it is still alive. If you select "Loose Binding" then when the WAN1 port is disconnected, your packets will automatically go to the other WAN port, if it is active.
- □ Select WAN Port / Select PPPoE session If the setting above is *Enable*, select the desired Port and Session. Otherwise, ignore these settings.
- □ **Note:** Multiple PPPoE sessions are defined on the *Advanced PPPoE* screen.

Buttons

- □ Add Use this to add a new entry to the database, using the data shown on screen.
- □ **Delete** Click this to delete the selected entry.
- □ **Update** Use this to update the selected entry, after making the desired changes.
- □ **Reset** Reset changes you have made since loading the data from the Multi-WAN VPN Load Balancer.

Host & Group list – This table shows the current binding.



HotBrick		HotBrick	VPN 1400,	/2	
	Advanced Configu	ration			se alle
	Virtual Server UP	nP Special Application	Advanced Featu	ire	
Quick Installation	Host IP Routing	Dynamic DNS Multi I	OMZ NAT Setting		
Load Balancing	Dynamic Routing				
Advanced WAN	RIP v2	Enabled			
Advanced Configuration	Interface	LAN	-	WAN 2	
Security Management		WAN 1	L	WAN 2	
	Submit		Cancel		
VPN Configuration	Static Routing				
QoS Configuration	Network Address	Subnet Mask	Gateway	Interface	
Management Assistant	0.0.0.0	255.255.255.0	0.0.0	LAN 💌	(2~15)
Device Status	Add	elete	Update	Can	cel
Device Information					
	Routing List Destination IP	Subnet Mask	Gateway	Interface	Metric Type

Routing

This section is only relevant if your LAN has other Routers or Gateways.

- □ If you don't have other Routers or Gateways on your LAN, you can ignore the **Static Routing** page completely.
- □ If your LAN has other Gateways and Routers, you must configure the Static Routing screen as described below. You also need to configure the other Routers.

Note:

If there is an entry or entries in the Routing table with an Index of zero (0), these are System entries. You cannot modify or delete these entries.

Dynamic routing

- \Box **RIP v2** This acts as a "master" switch. If enabled, the selected WAN or LAN will run RIPv1/v2. Otherwise the RIP function is not available.
- □ Interface LAN, WAN1 n, is enabled, any WAN or LAN can execute the RIP function.

Static routing

- Network Address The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0.
- □ **Netmask** –The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0



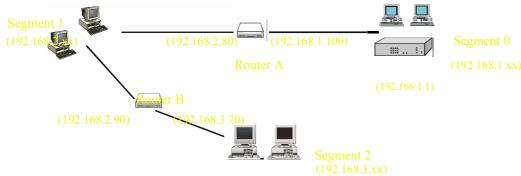
- □ **Gateway** The IP Address of the Gateway or Router that the Dual WAN VPN Firewall must use to communicate with the destination above. (NOT the router attached to the remote segment.)
- □ Interface Select the correct interface, usually "LAN". The "WAN" interface is only available if NAT (Network Address Translation) is disabled.
- □ **Metric** The number of "hops" (routers) pass through to reach the remote LAN segment. The shortest path will be used.

Routing list – This shows the current routing table set by users.

Configuring Other Routers on your LAN

All traffic for devices not on the local LAN must be forwarded to the Dual WAN VPN Firewall, so that they can be forwarded to the Internet. This is done by configuring other Routers to use the Dual WAN VPN Firewall as the *Default Route* or *Default Gateway*, as illustrated by the example below.

Static Routing – example



The Dual WAN VPN Firewall Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Dual WAN VPN Firewall requires 2 entries as follows.

Entry 1 (Segment 1)
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	2
Entry 2 (Segment 2	
Destination IP Address	192.168.3.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	3



HotBrick, Tel: 305-398-0888, Fax: 305-398-5966 For Router A's Default Route

Destination IP	0.0.0.0
Address	
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.1
Metric	2

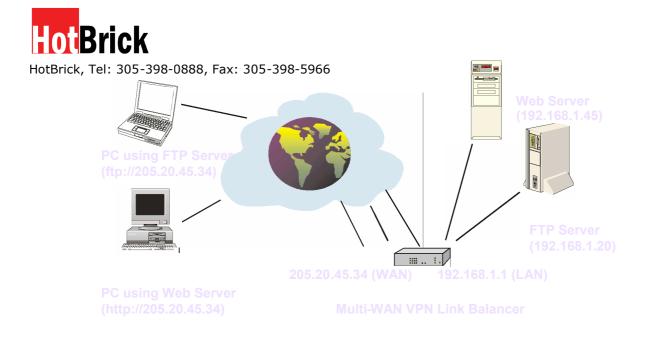
For Router B's Default Route

Destination IP	0.0.0.0
Address	
Network Mask	0.0.0.0
Gateway IP	192.168.2.80
Address	
Interface	LAN
Metric	3

Virtual Server

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users are not able to access a server on your LAN because:

- □ Your Server's IP address is only valid on your LAN, not on the Internet.
- □ Attempts to connect to devices on your LAN are blocked by the firewall in the Dual WAN VPN Firewall. The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.



Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

Connecting to the Virtual Server

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Dual WAN VPN Firewall Internet IP Address (the IP Address allocated by your ISP). e.g.

http://205.20.45.34 ftp://205.20.45.34

- □ To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.
- □ This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use the *Dynamic DNS* feature (explained later in this chapter) to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

e.g.

This screen allows you to define your own Server types:

	Advance	d Configuration				se alle
	Host IP	Routing Dyna	mic DNS	lulti DMZ	AT Setting	
uick Installation	Virtual S	erver UPnP S	Special Applica	ation Adva	nced Feature	
	Virtual Se	rver Configuration				
oad Balancing	Enabled	Server_Name	Protocol	IP Address	s Port Range	Allowed Remote IP
dvanced WAN				N 0.0.0.0	53 ~ 53	From 0.0.0.0
		ONS	W VOD	AN ALL 💙	53 ~ 53	To 0.0.0.0
dvanced Configuration						
ecurity Management	Add	Delete		Update		Cancel
PN Configuration						
9	Virtual Se					
oS Configuration	State	Server_Name	Protocol	Server IP	WAN Port Range	Interface Binding
	Disabled Disabled	DNS	TCP, UDP	0.0.0.0	53~53	ALL
lanagement Assistant	Disabled	FINGER FTP	UDP	0.0.0.0	79~79 21~21	ALL
evice Status	Disabled	GOPHER	TCP TCP	0.0.0.0	21~21 70~70	ALL
Sevice status	Disabled	IPSEC	UDP	0.0.0.0	500~500	ALL
evice Information	Disabled	POP3	TCP	0.0.0.0	110~110	ALL
	Disabled	SMTP	тср	0.0.0.0	25~25	ALL
	Disabled	NNTP	TCP	0.0.0.0	119~119	ALL
	Disabled	PPTP	TCP	0.0.0.0	1723~1723	ALL
	Disabled	TELNET	TCP	0.0.0.0	23~23	ALL
	Disabled	HTTP	TCP	0.0.0.0	80~80	ALL
	Disabled	WHOIS	TCP	0.0.0.0	6677~6677	ALL
				0.0.0.0		

Virtual Server Configuration

- **Enable** The enable checkbox enables or disables each Virtual server as required.
- □ Server Name Enter a name for this server. (By default, there are 12 well-known virtual servers on the Custom Virtual Server List that you may use.)
- □ **Protocol** Select the network protocol (TCP/UDP) used by this sever.
- IP Address LAN, Enter the IP address of the server on your LAN which is running the required Server software.
 Each Host (server) should have a fixed IP address, or a reserved IP address. (See the *Host IP* section earlier in this Chapter for details on reserving an IP address.)
 Each Host (server) must be running the appropriate Server software
- □ **WAN** This selection allows this server to bind to any selected WAN port, or to bind all WAN ports together.
- □ **LAN Port Range** Enter the range of port numbers used for outgoing traffic from this Server. If only a single port is required, enter it in both fields.
- □ **WAN Port Range** -- Enter the range of port number used for incoming traffic to this Server. If only a single port is required, enter it in both fields
- □ Allowed Remote IP This allows only a range of remote side IP address to access the virtual servers. The default is $0.0.0 \sim 0.0.0.0$, means all remote side IP address can access it.

Buttons

- □ **Add** Create a new Virtual Server entry.
- **Delete** Delete the selected entry.



- **Update** Save any changes you have made to the current entry.
- **Cancel** Cancel any changes you have made since the last save operation.

Virtual Server List - This table shows the detail for all Custom Virtual Server configuration data. You can modify this configuration data by clicking the specific row you want to change.



If you use Internet applications that use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Dual WAN VPN Firewall. In this case, you must define the application as a "Special Application" in order for the application to work.

Note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

otBrick gin Time: 1:53 P.M.		HotBric	k VPN 1400/	2	
Quick Installation	Advanced Configurat Host IP Routing I Virtual Server UPnP Special Application Confi	Oynamic DNS Mul	ti DMZ NAT Setting	 'e	se iie
Load Balancing Advanced WAN			tgoing Port Range Inco	TCP 🔽	Incoming Port Range
Advanced Configuration	Add Delet	-	Update	Ca	ncel
Security Management VPN Configuration	Special Application List State Name	Outgoing Protocol	Outgoing Port Range	Incoming Protocol	Incoming Port Range
QoS Configuration		Protocol		Protocol	
Management Assistant Device Status					
Device Information					

Advanced configuration - Special Application.

- **Enable** Use this to Enable or Disable this Special Application as required
- □ **Name** Enter a descriptive name to identify this Special Application.
- □ **Outgoing Protocol** –Select the protocol used by this application, when sending data to the remote server or PC.
- □ **Outgoing Port Range** Enter the beginning and end of the range of port numbers used by the application server for data you send. If the application uses a single port number, enter it in both fields.
- □ **Incoming Protocol** Select the protocol used by this application when receiving data from the remote server or PC.
- □ **Incoming Port Range** –Enter the beginning and end of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both fields.

Buttons

- □ **Add** Create a new Special Application entry.
- **Delete** Delete the selected entry.
- □ **Update** Save any changes you have made to the current entry.
- **Cancel** Cancel any changes you have made since the last save operation.



Special Application List - This list shows the details for all currently defined Special Applications. You can modify its configuration data by mouse clicking the appropriate row.

Using a Special Application on your PC

- □ When the *Special Applications* screen is configured correctly, you can use the application on your PC normally. Remember that only one (1) PC can use each Special application at any time.
- □ Also, when 1 PC is finished using a particular Special Application, a "Time Out" period may be required before another PC can use the same Special Application.
- □ If an application still cannot function correctly, try using the "DMZ" feature instead.

Advanced configuration – Dynamic DNS

Dynamic DNS is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address on your WAN port. With a dynamic IP your IP address may change whenever you connect to your ISP, which makes it difficult for visitors to connect to your web site.

You must register for the Dynamic DNS service. The Dual WAN VPN Firewall supports 3 types of service providers:

- □ Standard client, available at http://www.dyndns.org Other sites may offer the same service, but can not be guaranteed to work.
- □ TZO at http://www.tzo.com
- □ 3322 is available in China at http://www.3322.org

To use the Dynamic DNS feature

- □ Register for the service from your preferred service provider.
- □ Follow the service provider's procedure to have a Domain Name (Host name) allocated to you.
- □ Configure the *Dynamic DNS* screen, as described below.
- □ The Dual WAN VPN Firewall will then automatically update your IP Address recorded by the Dynamic DNS service provider.
- □ From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.



D tBrick Time: 1:53 P.M.	HotBrick VPN 1400/2	
Quick Installation	Advanced Configuration Virtual Server UPNP Special Application Advanced Feature Host IP Routing Dynamic DNS Multi DMZ NAT Setting	se the
Load Balancing	Dynamic DNS Service Service Disabled	
Advanced WAN	Server Name	
Advanced Configuration	User Name Password	
ecurity Management	Verify Password	
PN Configuration	Domain Name	
oS Configuration	Additional Settings	
lanagement Assistant	Enable Wildcard Enable Backup MX	
evice Status	Mail Exchanger	
evice Information	WAN Port Binding WAN 1 V Force Update	
	Submit	

Dynamic DNS Service

This pull-down menu can Enable/Disable the Dynamic DNS feature, and select the required service provider.

- Disable Dynamic DNS is not used.
- \Box **TZO** Select this to use the TZO service (www.tzo.com). You must configure the *TZO* section of this screen.
- □ **DynDNS** Select this to use the standard service (from www.dyndns.org or another provider). You must configure the *Standard Client* section of this screen.
- □ **3322(in China)** This service is available in China. It is similar to "DynDNS"
- □ **User Defined DDNS Server** This is the user defined DDNS server. If the DDNS is not TZO, dyndns.org and 3322.

Additional settings

These options are available if using the standard client.

- □ **Enable Wildcard** If selected, traffic sent to sub-domains (of your Domain name) will also be forwarded to you.
- □ Enable backup MX If enabled, you must enter the *Mail Exchanger* address below.
- □ **Mail Exchanger** If the setting above is enabled, enter the address of the backup Mail Exchanger.

WAN Port Binding

- □ Select the WAN port used by the Dynamic DNS service.
- □ The "Force Update" button will update your record on the Dynamic DNS Server immediately.

This feature allows each WAN port IP address to be associated with one (1) computer on your LAN. All outgoing traffic from that PC will be associated with that WAN port IP address. Any traffic sent to that IP address will be forwarded to the specified PC, allowing unrestricted 2-way communications between the "DMZ PC" and other Internet users or Servers.

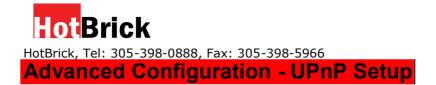
Note:

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

ogin Time: 1:53 P.M.		HotBrick	VPN 1	1400/2		
Quick Installation	Advanced Configurat Virtual Server UPnP Host IP Routing			ced Feature		se Hel l
Load Balancing	Multi DMZ Edit Enabled WAN WAN 1 Y	Name	DHCP	Private IP (LAN) 0.0.0.0	Access Group Default V	Direction Outgoing Y
Advanced Configuration	Add Dele	te	Update		Cancel	
VPN Configuration	Multi DMZ List State WAN Name	Session / Public IP (W	'AN) I	Private IP (LAN)	Access Group	Direction
QoS Configuration Management Assistant						
Device Status Device Information						

Multi DMZ

- **Enable** Use this to enable or disable the DMZ setting, as required.
- □ **WAN** there is 1 WAN port. Its connection type may change based on your WAN connection type (Static/DHCP/PPPoE).
- □ **Name** Enter a name for this setting. This name has no effect on the functionality.
- □ **Private IP Address (LAN)** Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed, or reserved. (See the *Host IP* section for details on reserving an IP address.)
- □ Access Group –You can define the users who have authority to use the DMZ by defining the group/s (Host IP web page)
- Direction –For the DMZ, you can allow inbound only, outbound only, or both inbound and outbound traffic.
- □ **Multi DMZ List** Multi DMZ List shows the details of all DMZ configuration data that is currently defined. You can modify configuration data by mouse-clicking on the row.



With the UPnP (Universal Plug & Play) function, it is easy to setup and configure an entire network to enable discovery and control of networked devices and services.

	Brick		HotBrick	VPN 140	00/2	
Out	ick Installation		n namic DNS Multi D Special Application	MZ NAT Set		steip 😪
Loc	ad Balancing vanced WAN	UPnP Option UPnP Advertisment Interval	O Enabled 30 Minut	 Disabled es (2~1440) 		
Ad	vanced Configuration	Outgoing Interface	WAN 1 ¥			
	curity Management N Configuration	Submit		Cancel		
_	S Configuration	Enabled Application Name	Protocol	Internal IP	Internal Port	External Port
	vice Status vice Information					
De	vice information					

UPnP Option - If UPnP is enabled, then this device will become one of the local network devices. You can then find an icon for it in Network Neighborhood on a Windows XP computer on your LAN.

Every time you add a new service with port mapping, the new service will appear on the mapping list.

UPnP Port Mapping List – With UPnP enabled, the table shows the details of all Custom Virtual Server configuration data.

Hot<mark>Brick</mark>

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

Advanced Configuration – NAT Setting

otBrick in Time: 1:53 P.M.		HotBrick	VPN 1400/2	
		PnP Special Application	-	se te
Quick Installation	Host IP Routing	Dynamic DNS Multi	OMZ NAT Setting	
Load Balancing	NAT Configuration NAT Routing	🗹 Enabled		
Advanced WAN	TCP Timeout	300 seconds	UDP Timeout	120 seconds
Advanced Configuration	TCP Window Limit	0 (0 for no limit)	TCP MSS Value	0 (0 for no change)
Security Management	NAT Port Options Port Range	Port Translation		Timeout
	1025 ~ 61439	Disabled	Enabled	0 seconds
VPN Configuration	0 ~ 0	Disabled	Enabled	0 seconds
QoS Configuration	0 ~ 0	Disabled	Enabled	0 seconds
	0 ~ 0	Disabled	Enabled	0 seconds
Management Assistant	0 ~ 0	Disabled	Enabled	0 seconds
Device Status				
Device Information		ubmit Cancel	NAT Status	
		ubmit Cancer	NAT Status	View Connections
	NAT Alias			
	Enabled	Local Lan IP	Wan IP	WAN
	Allow	Inbound(Virtual Server)	Port Range	Protocol
		0.0.0.0	0.0.0.0	WAN 1 🗸
			~	ALL 🗸
	Add	elete	Update	Cancel
		Jelete	opuate	Cancer
	NAT Alias List			

NAT Configuration

- □ **NAT Routing** You can enable or disable NAT by using the checkbox. If you disable the NAT checkbox, it will act as a bridge or Static Router. Most features will be unavailable.
- **TCP Timeout** Enter the desired value to use for the WAN port. The default is 300.
- **UDP Timeout** Enter the desired value to use for the WAN port. The default is 120.
- \Box **TCP Window Limit** Enter the desired value to use for each WAN port. The default is 0 (no limit).
- □ **TCP MSS Limit** Enter the required MSS (Maximum Segment Size) to use for each WAN port. The default is 0 (no limit),

Non Translation Port Range - If some packets have port numbers that cannot be translated for special applications, you must set the status to "Enable" and input the value in port range. Otherwise its port cannot be translated in the specified time period so you must set Enable and specify seconds in Timeout.

NAT alias - For each alias entry, the WAN IP acts as an alias IP for the host (with the Local LAN IP) for the Internet via the specified WAN port for the specified protocol packets, i.e. 1-1 NAT.

NAT alias list - NAT Alias List shows the list of all currently-defined NAT alias configuration data. You can modify its configuration data by mouse-clicking the list of rows.

Check NAT detail - This displays all detailed information on NAT configuration data

NAT Connection List - This displays the current details of all NAT entries including interface, protocol, state, destination IP, WAN IP, local IP, idle time and in/out packets.



Advanced Configuration – Advanced Feature

HotBrick VPN 1400/2 lotBrick _ogin Time: 1:53 P.M. **Welp Advanced Configuration** Host IP Routing Dynamic DNS Multi DMZ NAT Setting Virtual Server UPnP Special Application Advanced Feat Quick Installation External Filters Configuration Load Balancing 💌 Echo Request Timestamp Request Block Selected ICMP Types Information Request Address Mask Request Advanced WAN Advanced Configuration **DNS Loopback** main Nami Private IP Domain Name Private IP Security Management 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Management Assistant 0.0.0.0 0.0.0.0 **Device Status** Application IDENT Port Make it seem closed, not stealth Enabled SMTP Binding Enabled WAN 1 🔽 IPSec Passthrough 💌 Enabled Αυτο 🔽 Max Tunnels 10 PPTP Passthrough Enabled Δυτο 🗸 Max Tunnels 10 Submit Cancel Protocol & Port Binding Source Type Single IP Protocol Port Range Enabled Destination Type IP Address Subnet Mask WAN Strict Binding

External Filters Configuration

- □ **IDENT Port** Port 113 is associated with the Internet's (Identification / Authentication) service. When a client program in your computer contacts a remote server for services such as POP, IMAP, SMTP, that remote server sends back a query to the "Ident" server running in many systems listening for these queries on port 113. This means that hackers can probe port 113 as a rich source of your personal information. The default value of this check box is "Disable"
- □ **Block Selected ICMP Types** These settings determine whether or not this device should respond to ICMP requests received from the WAN port. If Checked, the selected packet types are blocked. Otherwise, they are accepted.

DNS Loopback - When you have some servers on the LAN and their domain names have already been registered on a public DNS you can avoid a DNS loop back problem by entering the following fields.

- **Domain Name** Enter the domain name specified by you for local server.
- □ **Private IP** Enter the private IP address of your local server.

Interface Binding - SMTP (Simple Mail Transport Protocol) Binding

Unless you are using E-mail accounts from different ISPs on each port, you can ignore these settings.

Some ISPs configure their E-mail Servers so they will not accept E-mail from IP addresses not allocated by them. If you are using accounts from different ISPs, sending E-mail over the wrong WAN port may result in non-acceptance of the mail. In this case, you can use these



settings to correct the problem.

- □ **Enable** If enabled, the WAN port you specify will be used for all outgoing SMTP traffic. If disabled, either WAN port will be used.
- □ **WAN** Select the desired WAN port to be bound.

Protocol and Port Bindings - Use these settings if you wish to ensure that particular traffic is sent by a particular WAN port, and thereby a particular ISP account.

- **Enable** Enable or disable each item as required.
- **Source IP** IP address of the source sending the packets.
- **Destination IP** IP address of the destination receiving the packets.
- □ **Subnet Mask** With a subnet mask other than 255.255.255, you can make an IP subnetwork your destination.
- □ **Protocol** Select protocol type used by the traffic you wish to configure.
- □ **Port Range** Enter the beginning and end of the port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields.
- □ **WAN** Select the WAN port you wish this traffic to use.

Protocol and Port Binding List - This list shows the details of all protocol and port configuration data that are currently defined. You can modify them by mouse clicking the correct row.



6 – Security Management

Security Management – Block URL

Hot <mark>Brick</mark>		HotBrick VPN 1400/2	
ogin Time: 1:53 P.M.			
	Security Management	-	😪 Help
	URL Filter Access Filt	er Session Limit SysFilter Exception	
Quick Installation	Access Group	Default 💙	
Load Balancing	Select Group URL Filter Type	Block Internet Access	
Advanced WAN	Set Type		
Advanced Configuration	Access Item		
Security Management		/ Keyword On Web Site	
VPN Configuration	1		
QoS Configuration	Add Delete	Update Cancel	
Management Assistant	Internet Access List		
Device Status	Index Status	URL / IP / Keyword	
Device Information	1		
	-		

This feature allows you to block access to undesirable Web sites. You can block by URL, IP address, or Keyword. You can also have different blocking settings for different groups of PCs.

- □ Every URL is searched to see if it matches or contains any of the URLs or keywords entered here. Then, after a DNS lookup, it determines the IP address of the requested site; the site's IP address is checked against IP address entries on this screen.
- □ Note that a single IP address may host many Web sites. Entering the address on this screen will block all Web sites hosted at that IP address.

Access Group - This allows you to have different blocking rules for different Groups of PCs.

- All PCs (users) are in the *Default* Group unless moved to another group on the *Host IP* screen.
- □ If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the *Host IP* screen.
- □ If you wish to apply different restrictions to different Groups, select the desired Group, and click the "Select" button. The screen will update data for the selected Group.

Block internet access – When this setting is enabled ,all internet access is allowed; there are no restrictions in place. When a rule is added it will prohibit access to the website.

Allow Internet Access – When this setting is active, all internet access is prohibited by default. An entry here will enable access to the specific allowed site while all other sites are blocked.



Security Management – Access Filter

	otBrick n Time: 1:53 P.M.			HotBr	ick VPN 1400/	2
		Security URL Filt	/ Manage er Acce	ment ss Filter Session Li	mit SysFilter Exception	se Heip
F	Quick Installation Load Balancing	Access (Select Gr		Default 💌		
	Advanced WAN Advanced Configuration	Filter Se No Filt Block			 Allow Selected Access Block Selected Access 	· · · · · · · · · · · · · · · · · · ·
	Security Management VPN Configuration	ICMP Filt	t ers ed Packet T	'ypes	✓ Echo Request ✓ Information Request	✓ Timestamp Request ✓ Address Mask Request
Ē	QoS Configuration Management Assistant	Submit			Cancel	
	Device Status Device Information	User-De Index 1	fined Filter Enabled	Filter Name Archie	Protocol Type	Port Range 1525 ~ 1525
		Add	I	Delete	Update	Cancel
		User-De Index	f <mark>ined Filter</mark> Status	List Name	Protocol Ty	ype Port Range
		1 2 3 4	Disabled Disabled Disabled Disabled Disabled	Archie DNS FTP Command FTP Data Gonber TCP		1525 ~ 1525 53 ~ 53 21 ~ 21 20 ~ 20 70 ~ 70

The network administrator can use the Access Filter to control the Internet access and applications available to LAN users.

- \Box Five (5) user groups are available, and each group can have different access rights.
- □ All PCs (users) are in the *Default* group, unless assigned to another group on the *Host IP* screen.

Access Group - This allows you to create different access rights for different Groups of PCs.

- □ If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the *Host IP* screen.
- □ If you wish to apply different restrictions to different Groups, select the desired Group. The update will apply to the selected Group only.

ICMP – Filters - If you enable ICMP Filter, the ICMP request packet types specified will be blocked from the local host to the remote side.



Port Blocking – There are two possible settings :

- □ **No Filtering** all ports are open
- □ **Block All Access** All ports are closed. When you make a new rule, the port will be opened for that entry (maximum number of rules you enter are 50).
- **Filter Name** Enter a meaningful name for this filter.
- □ **Protocol Type** Select a protocol type you wish to block.
- □ **Port No. Range** Enter the range of port numbers you wish to block. If only a single port is required, enter it in both fields.

HotBrick Login Time: 1:53 P.M.	HotBrick VPN 140	0/2
Quick Installation	Security Management URL Filter Access Filter Bession Limit SysFilter Excep Outgoing New Session Session Limit Sampling Time	tion • Enabled • Disabled 400 msec.
Advanced WAN Advanced Configuration Security Nanagement VPN Configuration QoS Configuration Nanagement Assistant	Maximum of Total New Sessions Maximum of New Sessions for Host Maximum of Dropped New Sessions for Host Pause Time for Host while exceeding limit on Dropped New Sessions Submit Cancel	05535 sess., per sec. 100 sess., per sec. 25 sess. per sec. 5 min.
Device Status Device Information		

This new feature allows you to drop new sessions from both the WAN and LAN side. This occurs when the number of new sessions exceeds the maximum value set by you in a sampling time.

- □ **Sampling time** The time interval specified by you to count the new sessions. Only new sessions are counted in the sampling time to check. (The default is 400 mil-sec.)
- □ **Maximum total of new sessions -** The maximum number of new sessions in the system that is acceptable in the sampling time. Any new incoming sessions will be dropped after the number of new sessions exceeds it. (Default: 65535 session/sec)
- □ **Maximum new Sessions for Host** The maximum number of new sessions from the host that is acceptable in the sampling time. Any new incoming sessions will be dropped from this host after the number of new sessions exceeds it. (Default: 100 session/sec)
- □ **Maximum dropped sessions for host -** If the number of dropped new sessions from the host exceeds the Maximum in the sampling time, any new session from the host will be dropped in the pause time period. (Default: 25 session/sec)
- □ **Pause time for host while exceeding limit on dropped new sessions -** Within the pause time period, no new session from the suspended host can be served by the system when the number of dropped new sessions exceeds the defined Maximum. (Default is 5 minutes)



Security Management – System Filter Exeption



Sysfilter exception - System Filter Exception – will reject every packet with an unrecognized port to avoid port scan programs run by hackers but this also incurs problems when servers (e.g. SMTP server port 113) or clients from the WAN need to respond to packets to verify their availability to their communication peers.

- **Enable** If the check box is checked, the System Filter Exception is enabled.
- □ **Interface** You can select LAN, any WAN port, or ALL interfaces through which a packet passes.
- □ **Protocol** The packet type that will be processed via the above interface by this device.
- □ **Foreign Port Range** Enter the beginning and end of the foreign port range used for the traffic you are configuring. If a single port is used instead of a range, enter the port number in both fields.
- □ **Device Port Range** Enter the beginning and end of the device port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields.

System Filter Exception Rules List - The list will display the details of all System Filter Exception Rule data that you have setup. You can modify it by mouse-clicking each row.



7: VPN Configuration

Virtual Private Network (VPN) uses encryption and authentication to create the connection between two end points (computers or networks). It allows private data to be sent securely over a public network or Internet without the risk of unauthorized access from outside intruders. VPNs establish a private network that can send data securely between two networks. We call this creating a "tunnel". A VPN tunnel connects the two PCs or networks.

Note: The Dual WAN VPN Firewall uses industry standard IP Sec encryption. However, due to the variations in how manufacturers interpret this standard, many VPN products are not interoperable. Although the Dual WAN VPN Firewall can interoperate with many other VPN products, it is not possible to provide specific technical support for every other product on the market.

Planning the VPN

When planning your VPN, you must make following choices first.

1. If the remote end is a network, the two-endpoint networks must have different LAN IP address ranges. If the remote endpoint is a single PC running a VPN client, its destination address must be a single IP address, with a subnet mask of 255.255.255.255

2. You can use the Internet Key Exchange (IKE) setup, or Manual Keying that requires you to specify each phase of the connection. IKE has become the standard for automatic keying.

3. Decide what encryption level you are going to use (DES, 3DES or AES)?

The settings you have to make to connect to another HotBrick product are basic. Some Standard settings that we use for tunnels between our products are SHA1 authentication, AES 128 bits encryption and DH group 2 as hash algorithm. This is a basic setting that ensures good speed and very secure encryption and authentication so your data will be safely transported via the IPSec tunnel.

There are two basic settings:

Tunnel to HotBrick Unit - This describes how to setup an IPSec tunnel to a HotBrick VPN 401 VPNX2, LB-2 VPN, 1400/2, 800/8 F and HSS 6000.

	VPN Configuration Tunnel to HotBrick client	Tunnel to 3rd P	arty SA lis	t VPN Log		≈ ≉ <mark>⊞</mark>
Juick Installation	Tunnel to HotBrick unit	Advanced setting	gs VPN pr	eset		
.oad Balancing	VPN Tunnel List	Add New P	olicy 🔽			
dvanced WAN	Tunnel Name					
	Tunnel WAN Port	WAN 1 🗸				
vanced Configuration	Local Security Network	IP Address	0.0.0	Netmask	0.0.0.0	1
curity Management	Remote Security Network	IP Address	0.0.0.0	Netmask		
N Configuration	Remote Security Gateway	IP Address	0.0.0.0	Nethidsk	0.0.010	
S Configuration	Negotiation Type	Main Mode	~			
nagement Assistant	Preshared Key	Main Mode	·	(Characte	rs / Hex:0x)	
vice Status						
	Action			Sta	itus	
vice Information	Connect	Set Options .				
		-	Submit Re	ot		
		-	Subline Ke	,et		

VPN Configuration – Tunnel to HotBrick Unit

- □ **VPN Tunnel List** here you can add a new tunnel or change an existing one from the list. The router allows a maximum of 50 tunnels.
- **Tunnel Name–** In order to distinguish the tunnels, you have to give the "Tunnel" a unique name.
- **Tunnel –** The tunnel can be connected only after the tunnel check box is enabled.
- □ **WAN port** You can choose WAN1, WAN2 or Any to make the VPN connection.
- □ Local Security Network- These entries identify the private network on this VPN router. The Network hosts can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make a VPN LAN-to-LAN connection.
- □ **Remote Security Network** These entries identify the private network on the remote peer VPN router whose hosts can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make a VPN connection
- □ **Remote Security Gateway** You can select the remote-side IP address (WAN IP address) as your remote security gateway
- □ **Preshared Key –** Choose a shared secret for this entry, this must be the same on both units.
- Action

Connect – this button will initiate the tunnel

Submit Query – this button will add the policy

VPN Configuration – Tunnel to HotBrick Client

Brick me: 1:53 P.M.		HotBrick	VPN 1	400/2		
		vanced settings unnel to 3rd Par		et VPN Log		😪 Help
iick Installation				WHICE COG		
ad Balancing	VPN Tunnel List Tunnel Name	Add New Pol	icy 🚩			
Ivanced WAN	Tunnel	Enable				
vanced Configuration	WAN Port	WAN 1 Y				
-	Local Security Network		0.0.0.0	Netmask	0.0.0.0	
urity Management	Distinguished Name Remote client	neer ID	0.0.0	(Name string /	ID Address)	
Configuration	Negotiation Type	Main Mode	~	(Name string)	IF Address)	
i Configuration	Preshared Key	Main Mode		(Character	s / Hex:0x)	
agement Assistant						
-						
ice Status	Action Connect	Set Options	-	Sta	us	
ce Information						
		s	ubmit Rese	1		



Tunnel to HotBrick Client – This describes an IPSec tunnel from a the VPN 1400/2 to the HotBrick Client Software.

- □ **VPN Tunnel List** allows you to add a new tunnel or change an existing one on the list. The router can support a maximum of 50 tunnels.
- **Tunnel Name** In order to distinguish the tunnels, you have to give the "Tunnel" a unique name.
- **Tunnel –** Only after you enable the tunnel check box, the tunnel can be connected.
- □ **WAN port –** You can choose WAN1, WAN2 or Any to make the VPN connection.
- □ Local Security Network- These entries identify the private network on this VPN router. The Network hosts 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.
- □ **Distinguished name remote client –** this is an email format address. For example: pete@HotBrick.com
- **Preshared key -** Choose a shared secret for this entry. They must be the same on both units.
- □ Action

Connect – this button will initiate the tunnel

Submit Query – this button will add the policy

VPN Configuration – Advanced settings

When you use the **tunnel to HotBrick unit** or **tunnel to HotBrick client** configurations the **Advanced Settings** a ren't required. They are only required for configuring an IPSec tunnel to a third party unit.



Time: 1:53 P.M.		HotBrick VPN 1400/2	
Tille, 1.33 P.M.	VPN Configuration		e alleip
	Tunnel to HotBrick client	Tunnel to 3rd Party SA list VPN Log	
uick Installation	Tunnel to HotBrick unit	Advanced settings VPN preset	
.oad Balancing	VPN Tunnel		
.oau barancing	Tunnel List	✓	
Advanced WAN	PPPoE Session	Session 1 🔽	
Advanced Configuration	Enable Setting		
ecurity Management	Key Management		
PN Configuration	Кеу Туре	AutoKey (IKE) 💌	
oS Configuration	Phase 1		
	Negotiation Type	Main Mode 👻	
lanagement Assistant	DH Group	DH Group 2 (1024-bit) 💌	
evice Status	Encryption Method	AES (128 bits) 💙	
evice Information	Authentication Method	SHA1 🕶	
evice information	SA Lifetime	28800 Seconds	
	Phase 2		
	Encapsulation Format	ESP 👻	
	Encryption Method	AES (128 bits) 🕶	
	Authentication Method	SHA1	
	Perfect Foward Secrecy	DH Group 2 (1024-bit) 💌	
	Key Lifetime	In Time 3600 Seconds (Note : 0 for no expiry) In Volume 0 Kbytes	
	ESP Mode	Tunnel	

- **Tunnel Name–** In order to distinguish the tunnel, you have to give the "Tunnel" a unique name.
- □ **PPPoE Session** If you are using PPPoE to make the connection, and your ISP offers multiple PPPoE sessions, you can select these PPPoE sessions to construct VPN tunnels.
- **Enable setting –** The tunnel can only be connected if enabled.
- □ Phase 1 DH Group Use DH Group 1(768-bits), DH Group 2(1024-bits), or Group 5 (1536-bits) to generate IPSec SA keys.
- □ **Phase 1 Encryption Method** Three data encryption methods are available: DES, 3DES, AES.
- □ **Phase 1 Authentication Method** There are two authentication methods available: MD5 and SHA1 (Secure Hash Algorithm).
- □ Phase 1 SA Life Time- By default the Security Association lifetime is 3600 Sec.
- □ **Force Deletion after Expiring** Once SA expires, tunnel will be removed and related resources will be released to the system.

Security level

- □ **Encryption Method** specifies the encryption mechanism to use. Data encryption makes the data unreadable if intercepted. There are three encryption method available; DES, 3DES and AES. The default is null.
- □ Authentication specifies the packet authentication mechanism to use. Packets authentication proves the data comes from the source you think it comes from. There are three authentications available: MD5, SHA1 and SHA2.

Hot<mark>Brick</mark>

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

Key management

- □ **Key Key Type:** there are two key types (manual key and auto key) available for key exchange management.
- □ **Manual Key:** If manual key is selected, no key negotiation is needed.
- □ **AutoKey (IKE)-** There are two types of operation modes that can be used.
- □ **Main mode** accomplishes a phase one IKE exchange by establishing a secure channel.
- □ **Aggressive Mode** is another way of accomplishing a phase one 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 new key values for IP traffic encryption & authentication. Preshared Key This field authenticates the remote IKE peer.
- \Box Key Lifetime- This is specified the lifetime of the IKE generated Key. If the time expires or data is passed over this volume, a new key will be renegotiated. No limit 0 is the default.



IPSec policy options

	IPSec Policy options			A A
	Tunnel Attributes			
	State Name Security Gateway	Remote Network	Security Level Key Type	Interface Negotiation Status
uick Installation	Enabled gbbhlijjh 68.143.210.81	192.168.2.0/255.255.255	AES (128 Autokey	WAN 1 Jdle
ad Balancing	1		bits)/SHA1 (IKE) D	isconnected Tule
Ivanced WAN	Dead Peer Detection Feature			
	Detection	Enabled		
lvanced Configuration	Check Method	O Heartbeat	OICMP Host 0.0.0.0	 OPD (RFC 3706)
curity Management	Check After Idle	60 Seconds		
	Retry Times	10		
N Configuration	Action	 Failover 	ORemove Tunnel	OKeep Tunnel Alive
S Configuration	Logging	🗹 Enabled		
anagement Assistant	NAT Traversal Feature			
	NAT Traversal	Enabled		
vice Status	Keep Alive Interval	60 Seconds	UDP Checksum	Enabled
vice Information				
	Options NetBIOS Broadcast	Enabled	Check ESP Pad	Enabled
	Auto Triggered		Allow Full ECN	Enabled
	Anti Replay		Copy DF Flag	Enabled
	Passive(Responder) Mode		Set DF Flag	Enabled

- **Tunnel Attribute –** The defined attributes for the tunnel.
- □ **Dead Peer Detection -** This setting allows you to use a WAN port for backup or for WAN failover in the event of a connection failure.
- □ **Check Method** You can choose ICMP, Heartbeat or DPD protocol. This detects if the remote end of the VPN tunnel is alive or not.

Options :

- □ NetBIOS Broadcast- This is used to forward NetBIOS broadcasts across the Internet.
- □ **Auto Trigger**—This helps keep the IPSec tunnel connection us so it can be re-established immediately, if a connection is dropped and detected.
- □ Anti Replay This keeps IP packet-level security in order.
- □ **Passive mode** This means that your PC establishes the data connection (if you enable passive mode).
- □ **Check ESP Pad –** If enabled, ESP (Encapsulating Security Payload), it will check ESP padding.
- □ Allow Full ECN Enable will allow full Explicit Congestion Notification (ECN). ECN is a standard proposed by the IETF that will cut down on network congestion and routers 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 rewritten, and others are determined by the inner header. Among these fields is the IP DF (don't 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 this DF (Do not Fragment) flag is set, it means the fragmentation of this packet at the IP level is not permitted.

Quick Installation Think to Holdshick fill a Worked Settings Load Balancing WaN Port WaN Port WaN 1 × Advanced WAN Activate IPSec Task Advanced configuration ISAkmp Port Security Nanagement Per Configuration VPN Configuration Maxtime to complete Phase 1 100 Seconds Maxtime to complete Phase 2 120 120 Seconds	
Advanced WAN WAN Port WAN 1 M Advanced Configuration Advanced Configuration Security Nanagement Security Nanagement Retry Interval Seconds VPN configuration Maxtime to complete Phase 1 100 Seconds	
Advanced Configuration ISAKinp Port Soo Security Nanagement ISAKinp Port Soo VPN Configuration Retry Interval 10 Seconds VPN Configuration Maxime to complete Phase 1 100 Seconds	
Security Management Retry Counter 5 VPN configuration Maxtime to complete Phase 1 100 Seconds Maxtime to complete Phase 2 120 Seconds	
VPN Configuration Maxtime to complete Phase 1 100 Seconds Maxtime to complete Phase 2 120 Seconds	
Maxtime to complete Phase 2 120 Seconds	
QoS Configuration Count Per Send 1	
Management Assistant NAT Traversal Port 4500	
Device Status	
Device Information Logging Level	
Log Level Infomation 💌	

- □ **ISAkmp Port** Internet Security Association and Key Protocol Management (ISAkmp) is designed to negotiate, establish, modify and delete security associations and their attributes. In particular, it was assigned UDP port 500 by the IANA.
- □ **WAN Port –** Choose the WAN port that you want these settings to be applied to.
- □ **Retry Counter** It indicates how many times the process of Phase 1 will be restarted if it's unsuccessful. There is an error message in VPN log once it is expired.
- □ **Retry Interval** It is the time period between two consecutive retries.
- □ Maxtime to complete Phase 1 It indicates the maximum time allowed to be negotiated in Phase 1. If it expires often, it's recommended to increase the Maxtime period or reduce DH group level. Default value is 30 sec.
- □ Maxtime to complete Phase 2 It indicates the maximum time allowed to be negotiated in Phase 2. If it expires often, it's recommended to increase the Maxtime period or reduce DH group level. Default value is 30 sec.
- □ **Count Per Send** It indicates the maximum amount of duplicate packets to be resent if the remote side does not respond to the first packet.
- □ **Logging Level -** This function allows you to select which information you want to see on the VPN log. It has six different levels of messages: None, Critical, Error, Warning, Information, Debug.



VPN Configuration – SA

otBrick gin Time: 1:53 P.M.	HotBrick VPN 1400/2
	VPN Configuration Tunnel to HotBrick unit Advanced settings VPN preset Tunnel to HotBrick client Tunnel to 3rd Party SA list VPN Log
Quick Installation	Security Association List
Load Balancing	State Name Security Remote Site Security Policy Key Type Physical Negotiation Gateway Remote Site Security Policy Key Type Status Status
Advanced WAN	Prev Page Next Page Refresh
Advanced Configura	tion
Security Manageme	nt
VPN Configuration	
QoS Configuration	
Management Assista	ant
Device Status	
Device Information	

VPN configuration – **SA**

The list will display the details of all Policy Setup configuration data that you have setup. You can modify it by mouse-clicking each row.



Hot <mark>Brick</mark> Login Time: 1:53 P.M.	HotBrick VPN 1400/2
	VPN Configuration Tunnel to HotBrick unit Advanced settings VPN preset
Quick Installation	Tunnel to HotBrick Client Tunnel to 3rd Porty SA list VPN Log Message Status: 0 message(s)
Load Balancing	Time Priority Module Messages
Advanced WAN	Prev Page Refresh Next Page Clear All
Advanced Configurat	
Security Managemen	
QoS Configuration	
Management Assista	and a second
Device Status	
Device Information	

You can monitor the VPN status through the VPN log web page. The log level (priority) can be chosen from VPN IKE Global Setting web page.

Message Status

- □ **Priority** It This indicates the severity level of a message for analysis.
- **Time** This indicates when this message is created using the system time.

Undefined messages

- □ **Module** The module that is responsible for the message being sent in IPSec architecture.
- □ **Messages** The message displays information describing the event that occurred.



8: QoS Configuration

QoS Configuration – overview

The Dual WAN VPN Firewall provides QoS, which supports high quality network service. By prioritizing outgoing packets based on user-defined policies, the Quality of Service feature can result in real-time applications achieving better response or performance

otBrick		HotBrick VPN 1400/2	
	QoS Configuration	iguration	& Heij
Quick Installation	QoS Features Enable QoS Queuing Method	Enabled	
Advanced WAN Advanced Configuration Security Management	IP TOS(Type of Service) Fe Process TOS Field Overwrite Policy Priority	Enabled	
¥PN Configuration QoS Configuration	Submit	Cancel	
Management Assistant Device Status			
Device Information	l		

QoS Features :

- **Enable QoS –** This enables the QoS function.
- Queuing Method Theses methods determine how to manage your queue. Priority
 Queuing is one of the first queuing variations to be widely implemented.

IP TOS (Type of Service Feature)

- □ **Process TOS Field** An 8-bit field in the IP Packet header designed to contain values indicating how each packet should be handled in the network. If you choose "enable" it will enable this function to process this IP Type of service field.
- □ **Overwrite policy priority -** Choose "yes" to set the priority of the TOS field in the IP packet to overwrite the priority defined in the policy configuration.



otBrick in Time: 1:53 P.M.		HotBrick VPN 1400/2	
	QoS Configuration QoS Setup Policy Configuration	iguration	‰ ∺lei p
Quick Installation	QoS Features Enable QoS	Enabled	
Advanced WAN Advanced Configuration	Queuing Method 	Enabled	
Security Management VPN Configuration	Overwrite Policy Priority	Tes Cancel	
QoS Configuration Management Assistant			
Device Status Device Information			

QoS Setup

QoS Feature

- **Enable QoS –** This will allow users to enable the QoS function.
- □ **Queuing Method -** The method used to manage your queue. Priority queuing is one of the first queuing solutions to be widely implemented.

IP TOS

- Process TOS Field An 8 bits field in the IP packet header designed to contain values indicating how each packet should be processed in the network. Enable this function to process the IP Type of Service field.
- Overwrite policy priority Choose "yes" to set the priority of the TOS field in IP the packet

to overwrite the priority defined in the policy configuration.

	QoS Configura	tion		20
		olicy Configuration		×6.11
Quick Installation	Policy Priority			
	Policy Name			
Load Balancing	Source Address	IP Address 💌		
Advanced WAN	1	From 0.0.0.0	To 0.0.0.0	
Advanced Configuration	Destination Addres	ss IP Address 🕑		
		From 0.0.0.0	To 0.0.0.0	
Security Management	Protocol Type	тср 💌		
VPN Configuration	Source Port	From 0 To 0		
QoS Configuration	Destination Port	From 0 To 0		
gos comigaración	Priority Queue	High 🔽		
Management Assistant				
Device Status	Add	Delete	Update	Cancel
Device Information		Delete		
Device Information	Policy List			
	Policy Name So	ource Address / Port	Destination Address / Port	Protocol Que

QoS Configuration – Policy Configuration



- □ Policy Name List When adding a new Policy, ignore this list. To edit an existing entry, select it from the list and then click the "Select" button. The data fields will be updated with data for the selected entry.
- □ Policy Name Enter a suitable name. Generally, you should use the "Policy Name" for the network traffic type for ease of identification.
- Source Address Define the source address of packets here. It has two types: IP address or MAC address. If you select IP address you can define the IP address range; otherwise you can define up to four MAC addresses.
- □ Destination Address Define the destination address of packets here. The explanation is as the same as above.
- □ Protocol Type The field defines traffic packet type, i.e. IP, TCP and UDP.
- \Box Source Port Define the source port of the packets here.
- □ Destination Port Define the destination port of the packets here.
- □ Priority Queue Determines if a packet meets all conditions defined above and will be serviced with a defined priority level.



9 : Management Assistant

Management assistant – Admin Password

	lotBrick		HotBri	ick VPN 140	00/2	
Qurck Installation Admin Setup Email Allert SNMP Syslog Upgrade Firmware Qurck Installation Remote Access Configuration Remote Setup Access Port Allowed Remote IP Load Balancing Enabled Enabled B080 0.0.0.0 ~ 0.0.0 Advanced WAN Administrator Password User Name Password Verify Password Administrator Possword User Name Password Verify Password QoS Configuration Submit Cancel	ogin Time: 1:53 P.M.					
Load Balancing Remote Upgrade Remote Setup Access Port Allowed Remote IP Load Balancing Enabled B080 0.0.0.0 0.0.0.0 Advanced WAN Administrator Password Verify Password 0.0.0.0 Advanced Configuration User Name Password Verify Password VPN Configuration Submit Cancel				Syslog Upgrade I	Firmware	2 <mark>He</mark> l
Load Balancing Enabled B080 0.0.0.0 0.0.0.0 Advanced WAN Administrator Password User Name Password Verify Password Advanced Configuration User Name Password Verify Password VPN Configuration Submit Concel	Quick Installation					
Advanced Configuration Security Management VPN Configuration QoS Configuration Management Assistant	Load Balancing					
Security Management admin VPN Configuration Submit QoS Configuration Cancel	Advanced WAN					
Security Management VPN Configuration Management Assistant	Advanced Configuration		Password	Verify Password	_	
QoS Configuration Management Assistant	Security Management	dumm				
Management Assistant	¥PN Configuration	Submit		Cancel		
	QoS Configuration					
Device Status	Management Assistant					
	Device Status					
Device Information	Device Information					

Enter the desired password, re-enter it in the Verify Password field, then save it.

When you connect to the Load Balancer with your Browser, you will be prompted for the password as shown below.

Enter Ne	twork Pass	word	Y ×
20	Please type y	ourusername and password.	
- T.	Site:	192.168.1.1	
	Realm	NeedPassword	
	Quer Name	admin	
	Esseword	[
	E Severthis p	assword in your password list	
		OK. Cano	la

Figure 8-5: Password Dialog

- Enter "Admin" for the User Name.
- □ Enter the password for the Dual WAN VPN Firewall, as set on the *Admin Password* screen above. (The default is blanks.)



Manageme

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

HotBrick Login Time: 1:53 P.M.	HotBrick VPN 1400/2	
	Management Assistant	~ #
	Admin Setup Email Alert SNMP Syslog Upgrade Firmware	
Quick Installation	Global Settings: Notification on Enable & Link Down Excessive Ping	
Load Balancing	Enabled Enabled MAX. Pings Before Notification 120 times / min.	
Advanced WAN	Email Alert Configuration LAN	
Advanced Configuration	Email (SMTP) Server Address	
Security Management	User Name	
VPN Configuration	Password Sender Address	
QoS Configuration	Recipient Address	
Management Assistant	Validate Settings Send Test E-mail	
Device Status		
	Submit	
Device Information	Email Alert Configuration List	
	Interface Mail Server User Name Sender Addr. Recipient Ad	ldr.
	LAN WAN 1	
	WAN 2	

This feature will send a warning Email to inform the system administrator that one of the WAN ports is disconnected.

Enable/Disable Email Alert

- **Enable –** This enables Email Alert to send a warning email when a WAN port disconnects.
- Disable This disables Email Alert so no warning email is sent when a WAN port disconnects.

Email Alert Configuration

- □ **Email Sender Address-** This is the email address that sends a warning email to a recipient. The email informs the recipient to check if there is a problem with a WAN port or not.
- Email (SMTP) Server Address This is the email server a warning email will be sent to If the setting is enabled. For example: mail.domain.com.
- □ **Email(SMTP) Server User Name** This is the user name of the email sender for authentication (optional).
- **Email(SMTP)Server Password -** This is the user password.
- □ **Email Recipient Address -** This is the email recipient address (ex.admin@yourdomain.com). If one of the WAN port disconnects, the email message will be sent to this recipient.

Excessive Ping Notification - This function prevents ICMP packet attacks from either the WAN or LAN on the unit. These packets will be dropped if the ping times exceed the threshold value, Ping Before Notification, and will send an e-mail to notify the administrator if Email Alert is enabled.

Ping Attack Notification - By default this feature is Disabled.



□ **Ping Before Notification -** A threshold value for the maximum Pings allowed to each interface on this device in a minute. The valid values range from 0 to 9999.

Management Assistant – SNMP

This section is only useful if you have SNMP(Simple Network Management Protocol) software on a PC or server. If you have SNMP software, you can use a standard MIB 2 file with the VPN 1400/2.

		ail Alert <mark>SNMP</mark> Sys	log Upgrade Firmware	
uick Installation	System Information Contact Person	Supervisor		
oad Balancing	Device Name	Supervisor HotBrick VPN 1400/2	-	
dvanced WAN	Physical Location	Head Office	-	
dvanced Configuration	Community			
ecurity Management	Community Name 1	private	Access Control 1 Read	i/Write 🔽
PN Configuration	Community Name 2	public	Access Control 2 Read	i Only 🔽
oS Configuration	Trap Targets			
	Target IP Address 1	0.0.0.0 (ex.	xxx.xxx.xxx.xxx)	
anagement Assistant	Target IP Address 2	0.0.0		
evice Status	Target IP Address 3	0.0.0.0		
evice Information	Submit		Cancel	

System Information

- **Contact Person –** The contact information for the person responsible for this device.
- Device name The name of the Dual WAN VPN Firewall.
- **Physical Location –** The location of the Dual WAN VPN Firewall.

Community – A relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

Trap Targets - Enter the IP address of any targets (PCs running SNMP software) that you want to receive traps. All traps are level 1.

Hot<mark>Brick</mark>

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

Management Asssistant – Syslog

tBrick Time: 1:53 P.M.			HotBrick V	PN 1400/2	
	Management A Admin Setup	ssistant Email Alert	SNMP Syslog	Upgrade Firmware	**
uick Installation	Syslog Delivery				
oad Balancing	Sending Out	Enabled	Enabled IP Address	Keep Sent Message	Enabled
	Syslog Server 1		0.0.0.0	Port (Default:514) 514	Log Priority Level Emerg. 👻
dvanced WAN	Syslog Server 2		0.0.0.0	514	Emerg. V
dvanced Configuration	Syslog Server 3		0.0.0.0	514	Emerg.
ecurity Management			0.0.0.0	314	
	Log Priority for M	odules			Expand
PN Configuration	SNTP Configuratio	on			
oS Configuration	Time Zone	(GMT+01	L:00) France, Germany	, Italy 🔽	
anagement Assistant	System Time	2000 / 1	/ 1 0 : 22 :	18	
anagement Assistant	SNTP Server 1				
evice Status	SNTP Server 2				
evice Information	SNTP Server 3				
		Submit	Cancel		View Syslo

This feature can send real time system information on the web page or to the specified PC.

Syslog Delivery

- **Sending out –** Check this, if you want to send syslog messages to another machine.
- □ **Keep Sent messages –** Check this if you want to keep sent messages; otherwise the sent message will be deleted.
- Syslog Server IP address: Up to 3 syslog servers can be used.
- **Enable:** You can enable or disable each server temporarily.
- **Port:** If your syslog does not use the default port, change it here.
- □ Log Priority for modules The messages are grouped into 8 priority levels, from Emergency to Debug. The lower the level, the fewer messages will be generated. Emergency is the lowest priority level, and Debug is the highest. Setting the priority to Debug will send all generated messages.

SNTP Configuration

□ **Time Zone** - You can setup system time using SNTP (**Simple Network Time Protocol**), and you can define 3 SNTP servers on the SNTP configuration.



Management Assistant - Upgrade Firmware

	Management					_		A THE
	Admin Setup	Email Alert	SNMP	Syslog	Upgrade Firm	ware		
Quick Installation	Save System Config		Save				Factory Set	ings
Load Balancing			_					
Advanced WAN	Upgrade Firmv User Name	are	admin					
Advanced Configuration	Password		Gammi					
Security Management	Upgrade Softwa Configuration	re or				Browse	Upgrade	
VPN Configuration								
Qo5 Configuration								
Management Assistant								
Device Status								
Device Information								
	_							

This Upgrade Firmware Screen allows you to upgrade firmware on the system, to enable remote administration, and FTP upgrade.

- You can backup your system configuration by selecting "Save" next to "Save System Configuration".
 This will allow you to save and store the system configuration file and use it as a backup. (Note: You have to refresh the browser after you saved the system configuration file).
- □ If you have password protection you'll be require to enter your password before making any changes to the system configuration files. **Important! Do not Reset or Restart the device while updating the firmware or unit may Crash.**



10: Device Status

Once both the Dual WAN VPN Firewall and the PCs are configured, operation is automatic. However, some additional Internet configuration may be required for your specific network.

Refer to Chapter 6 - Advanced Features for further details.

	Brick ime: 1:53 P.M.			HotBrick	VPN 1400/2	
		Device St	atus			a
		System S	tatus WAN S	tatus		
Qu	ick Installation	Interface	Connection Typ	16	Status	MAC Address
	ad Balancing	WAN 1	DHCP Force I	Renew	Disconnected	00-09-A3-00-AE-23
	-	WAN 2	DHCP Force I	Renew	Disconnected	00-09-A3-00-AE-24
Ad	vanced WAN	Tubartaan	IP Address	Subnet Mask	0-+	DNS IP Address
Ad	vanced Configuration	WAN 1	0.0.0.0	0.0.0.0	Gateway 0.0.0.0	0.0.0.0
Se	curity Management	WAN 2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
VPI	N Configuration		IP Address	Subnet Mask	MAC Address	DHCP Server
Qo	S Configuration	LAN	192.168.1.1	255.255.255.0	00-09-A3-00-AE-22	Enabled
Ma	nagement Assistant					
De	vice Status					
De	vice Information					

- □ **Connection Status –** Current status either "Connected" or "Disconnected".
- □ **Connection Type –** The type of connection used DHCP, Fixed IP, PPPoE or PPTP.
- □ **"Force Renew"** button– Only available when using a dynamic IP address (DHCP). Clicking this button will perform a DHCP "Renew" transaction with the ISP's DHCP server. This will extend the allocation period for your current WAN IP.
- □ **IP Address –** The public WAN address of the Dual WAN VPN Firewall, as seen from the Internet. This IP Address is allocated by the ISP (Internet Service Provider)
- □ **Subnet Mask –** The Network Mask (Subnet Mask) for the above IP Address.
- **Gateway** The default gateway for this subnet.
- DNS IP Adress The DNS server address is supplied by your ISP if needed.
- □ **MAC address –** The MAC address of the WAN 1 interface.

LAN Information

- □ **IP Address –** The LAN IP Address of the VPN 1400/2 Firewall Router.
- □ **Subnet Mask –** The Network Mask (Subnet Mask) for the IP Address above.
- □ MAC Address The MAC (physical) address of the Dual WAN VPN Firewall.



DHCP Server – The status of the DHCP Server function - either "Enabled" or "Disabled".

	Device Stat	us							Se al le
	System Stat	us WAN Sta	tus						
Quick Installation	Current Stati	stics							
Load Balancing	Interface	Status	Loadin Default	g Share Current	Currei Session	nt Load Byte		Current B Download	andwidth Upload
Advanced WAN	WAN 1 WAN 2	Disconnected Disconnected	50 % 50 %	50 % 50 %	1 1	1	1 1	0 bytes/sec 0 bytes/sec	0 bytes/se 0 bytes/se
Advanced Configuration	Overall Stati	stice							
Security Management	Interfac		oading Shi	are				/tes Statistics	
¥PN Configuration	WAN 1		0 %		Rece		кв	Transmitted	Total ЭКВ ОК
QoS Configuration	WAN 2		0 %				КВ		окв ок
Management Assistant		_	_			_		_	
Device Status		Refre	sh	Restart	Counters				NAT Status
Device Information									

Device Status - WAN status

NAT Statistics

This section displays data for each WAN port.

- **Connection status –** This will display either *Connected* or *Not Connected*.
- **Default Loading Share -** The default traffic loading between the WAN ports.
- □ **Current Loading Share –** The current traffic loading between the WAN ports.
- □ **Current Loading** The number of sessions, Bytes and Packets currently being processed on each port.
- Current Bandwidth The current Download and Upload speeds on each WAN port.
 "Check NAT Detail" will display the NAT Status screen, described below.

Brick				-lotBrick \	/PN 1400	/2		
ne: 9:55 A.M.			-			7 –		
	NAT Status							
	Active Interfac	e IP Info						
k Installation	Interface LAN			idress 168.1.1		onet Mask 5.255.255.0		
d Balancing			192.	100.1.1	200	.200.200.0		
-	NAT Timeouts							
anced WAN	TCP			300	UDP			120
anced Configuration	TCP Property							
irity Management	Max. Segment S	ize		1460	Max. Window	s Size		0
Configuration	NAT Traffic			Local	To Internet	Inter	net To Li	ocal
	Bytes			0		0		
Configuration	Packets			0		0		
igement Assistant	Connection Lis	t						
ce Status	ТСР	0		UDP	0	ICMP	0	
	Overall Connect	ons		Created	0	Deleted	0	
e Information	View	Dele	te	Criteria Filter	Interface	IP Address		Port Range
				Set Clear Al	ALL 💌	0.0.0	0	~ 0
	Errors							
	Checksum	0		Retries	0	Bad Packets	0	
	Misc.							
	Total IP Packets	:	420		Reserved Addr	ess O		
				lefresh				Ge Back

Download from Www.Somanuals.com. All Manuals Search And Download.



Data – NAT Status

LAN IP info

- □ **IP Address –** The LAN IP Address of the Dual WAN VPN Firewall.
- □ **Mask Address –** The Network Mask (Subnet Mask) for the IP Address above.

Active WAN IP Info – There is one (1) row for each active connection. The

following data is displayed for each connection:

- □ **IP Address –** The WAN (Internet) IP Address of the VPN1400/2 Firewall Router.
- □ **Mask Address –** The Network Mask (Subnet Mask) for the IP Address.
- NAT Timeouts This displays the current timeout values for TCP and UDP connections. TCP Prosperity - This displays the MSS (Maximum Segment Size) and Maximum Windows size for TCP packets.

NAT Traffic - This section displays statistics for both outgoing (LAN to Internet) and incoming (Internet to local) traffic.

NAT Connections - This displays the current number of active connections. For further details, click the "View Connection" list button.

Errors - Statistics are displayed for Checksum errors, number of retries, and number of bad packets.

Misc - This displays the total IP packets and reserved address.

Interface Statistics - This section displays cumulative statistics. Use the "Restart Counter" button to restart these counters when required.



Device information – Device Information

	Device Information Device Information	Exit				×.
Quick Installation	Device Information Hardware ID Firmware Version	Exit	03212104200001 Ver 2.0 Rel 23 Bu			
Advanced WAN	NAT Special Application	Enabled Disabled	Load Balance Multi DMZ	Enabled Disabled	Virtual Server URL Filter	Disabled Disabled
Advanced Configuration	Device Statistics					
Security Management VPN Configuration	System UpTime CPU Usage 1 %		26m 10s Memory Heap 1 %		Packet Queue 1 %	
- QoS Configuration						
Management Assistant	1	Refresh		J	Factory Settings	Restart
Device Status						
Device Information						
	-					

Device Information

- **Firmware Version –** Version of the Firmware currently installed.
- □ **NAT –** Status of the *NAT* feature either "Enable" or "Disable".
- □ Load Balance Status of the Load Balance feature –either "Enable" or "Disable".
- □ Virtual Server Status of the Virtual Server feature either "Enable" or "Disable".
- □ **Special Applications –** Status of the *Special Applications* feature either "Enable" or "Disable".
- □ **DMZ** Status of the *DMZ* feature either "Enable" or "Disable".
- □ Block URL Status of the *Block URL* feature either "Enable" or "Disable".
- □ Hardware ID The manufacturer's ID for this specific device.

Device Statistics

- **System UpTime –** The time since the system of a device was last initialized.
- □ **CPU Usage –** The current CPU usage percentage.
- □ **Memory Usage –** The current usage percentage of Memory (Heap & Queue).

Buttons

- □ **Refresh** Update the data on screen.
- **Restart –** Restart (reboot) the Dual WAN VPN Firewall.

Restore Factory Defaults – This will delete all existing settings, and restore the factory default settings. See below for details.



HotBrick	HotBrick VPN 1400/2
Login Time: 10:44 A.M.	
	Reset To Factory Default Values To restore the factory default setting values, you can click on the RESTORE button. You have to be careful of doing this, it will erase all settings you did previously, and reset them to factory
Quick Installation	default values.
Load Balancing	Restore
Advanced WAN	
Advanced Configuration	
Security Management	
VPN Configuration	
QoS Configuration	
Management Assistant	
Device Status	
Device Information	

If the "Restore Default Value" button on this screen is clicked:

- □ All your current settings will be erased.
- □ The default IP address, password and ALL other settings will be restored to the default values.
- □ The DCHP server function will be enabled.

These changes mean that your prior configuration is invalid, and you will have to re-connect to the Dual WAN VPN Firewall using its default IP address (192.168.1.1).



Appendix A

Specifications

Model Dimensions Operating Temperature	HotBrick VPN 1400/2 Dual WAN Firewall 120mm (W) x 427mm (D) x 43.4mm (H) 0° C to 40° C
Storage Temperature	-10° C to 70° C
Network protocol T Protocol:	CP/IP
Network Interfaces	16 Ethernet:
	14 * 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices
2 * 10/100BaseT (F	RJ45) for WAN
LEDs	14 LAN
	2 WAN
	2 Status
	1 Power
Power Input	AC 110V-230V @ 0.5A

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause improper operation.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Hot<mark>Brick</mark>

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

Appendix B

Windows TCP/IP Setup

Overview TCP/IP Settings

If using the default Load Balancer settings, and the default Windows 95/98/ME/2000 settings, no changes need to be made.

□ By default, the Dual WAN VPN Firewall will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.

- □ For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.
- □ If you wish to check your TCP/IP settings, the procedure is described in the following sections.
- □ If your LAN has a Router, the LAN Administrator must re-configure the Router itself.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

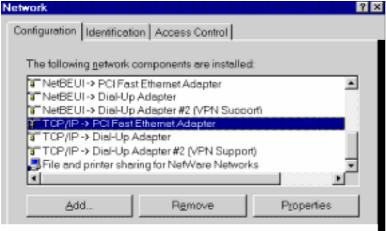


Figure B-1: Network Configuration

- 2. Select the *TCP/IP* protocol for your network card.
- 3. Click on the *Properties* button. You should then see a screen like the following.



ties					<u> </u>
Advanz	ced	NetBl	0S	DNS Co	nfiguration
	WINS C	onfigura	tion	IP /	Address
does not a inistrator to	automatic or an add	colly as: Iress, ar	sign IP (nd then	addresses,	esk.your
an IP add	ress:				
fress.					
et Mask:		1	1		
	is can be a does not o inistrator to an IP addre ran IP add gress	an IP address automatic inistrator for an add an IP address autor ran IP address	WINS Contigural ss can be automatically ass does not automatically ass inistrator for an address, an an IP address automatically ran IP address:	WINS Configuration Is can be automatically assigned to does not automatically assign IP of inistrator for an address, and then an IP address automatically r an IP address: gress	WINS Contiguration IP / is can be automatically assigned to this comp does not automatically assign IP addresses, inistrator for an address, and then type it in the an IP address automatically ren IP address: gress

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the VPN 1400/2 Firewall Router.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- □ If the *DNS Server* fields are empty, select *Use the following DNS server addresses,* and enter the DNS address or addresses provided by your ISP, then click *OK*.
- □ On the *Gateway* tab, enter Dual WAN VPN Firewall IP address in the *New Gateway* field and click *Add*, as shown below. (Your LAN administrator can advise you of the IP Address they assigned to the Dual WAN VPN Firewall.)

Statistics

TCP/IP Proper	ties		? ×
Bindings Gateway	Advanced WINS	NetBIOS Configuration	DNS Configuration
address ard are used. <u>N</u> ew gatew	erinî the list will be vey: 68 . 0 . 1		vill be the default. The ch these machines
		Eems	VE

Figure B-3: Gateway Tab (Win 95/98)



On the DNS Configuration tab, ensure Enable DNS is selected. If the DNS Server Search Order list is empty, enter the DNS address provided by your ISP in the fields beside the Add button, then click Add.

TCP/IP Properties	8		? ×
Gateway Bindings	MINS Advanced	Configuration NetBIOS	IP Address DNS Configuration
C Djsable Di	NS		
G Enable DN	15	D <u>o</u> main:	
DNS Server S	earch Order		Add
			Bemave

Figure B-4: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows 2000:

6. Select Control Panel - Network and Dial-up Connection.

□ Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

Local Area Connection Properties	? ×
General	
Connect using:	
SMC EZ Card 10/100 (SMC1211TX)	
	Configure
Components checked are used by this connect	ion:
	etworks
Install Uninstall	Properties
eneral Connect using: SMC EZ Card 10/100 (SMC1211TX) Configure Components checked are used by this connection: Components checked are used by this checked are used by this connection: Components checked are used by this connection: Components checked are used by this checked are used	
OK	Cancel

Figure B-5: Network Configuration (Win 2000)

- □ Select the *TCP/IP* protocol for your network card.
- □ Click on the *Properties* button. You should then see a screen like the following.



Internet Protocol (TCP/IP) Propertie	25	? ×
General		
You can get IP settings assigned autor this capability. Otherwise, you need to the appropriate IP settings.		
Obtain an IP address automatical	lly	
C Use the following IP address:		- I
IP address:		
Subnet mask:		
Default gateway:		
Obtain DNS server address autor	matically	_
_⊂ Use the following DNS server ad	-	- I
Preferred DNS server:		
Alternate DNS server:		
		-
	Advanced	
	OK Cano	el

Figure B-6: TCP/IP Properties (Win 2000)

□ Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting.

Restart your PC to ensure it obtains an IP Address from the Dual WAN VPN Firewall.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes:

- Enter Dual WAN VPN Firewall IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Multi-WAN VPN Link Balancer.)
- □ If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.



Checking TCP/IP Settings - Windows XP:

7. Select Control Panel - Network Connection.

□ Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.B)
<u>C</u> onfigure
This connection uses the following items:
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol (TCP/IP)
Install Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Sho <u>w</u> icon in notification area when connected
OK Cancel

Figure B-7: Network Configuration (Windows XP)

- □ Select the *TCP/IP* protocol for your network card.
- □ Click on the *Properties* button. You should then see a screen like the following:



Internet	Protocol (TCP/IP) Prope	erties 🔹 💽 🔀							
General	Alternate Configuration								
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.									
00	Obtain an IP address automatically								
00	\underline{s} e the following IP address: —								
ĮP a	ddress:	· · ·							
Sub	net mask:								
Def	ault gateway:	· · ·							
00	<u>b</u> tain DNS server address auto	matically							
-OU	s <u>e</u> the following DNS server ad	Idresses:							
Pref	erred DNS server:								
Alte	mate DNS server:	· · ·							
		Ad <u>v</u> anced							
		OK Cancel							

Figure B-8: TCP/IP Properties (Windows XP)

□ Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *obtain an IP Address automatically.* This is the default Windows setting.

Restart your PC to ensure it obtains an IP Address from the Multi-WAN VPN Link Balancer.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- □ Enter the Dual WAN VPN Firewall IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Dual WAN VPN Firewall.)
- □ If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Hot<mark>Brick</mark>

HotBrick, Tel: 305-398-0888, Fax: 305-398-5966

Appendix C

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Dual WAN VPN Firewall and some possible solutions for them. If you follow the suggested steps and the Dual WAN VPN Firewall still does not function properly, contact your dealer for further advice.

General Problems

Problem : Can't connect to the Dual WAN VPN Firewall to configure it.

Solution : Check the following:

- □ The Load Balancer is properly installed, LAN connections are OK, and it is powered ON.
- □ Ensure that your PC and the Dual WAN VPN Firewall are on the same network segment. (If you don't have a router, this must be the case.)
- □ If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with the Dual WAN VPN Firewall default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match the VPN 1400/2 Mask.

Internet Access

Problem : When I try to reach an URL or IP address I get a time out error.

Solution : A number of things could be causing this. Try the following troubleshooting steps.

- □ Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- □ If the PCs are configured correctly, but still not working, check the VPN 800/2 Firewall Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- □ If the Dual WAN VPN Firewall is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem : Some applications do not run properly when using the VPN 1400/2 Dual WAN Firewall.

Solution :

The Dual WAN VPN Firewall processes the data passing through it, so it is not transparent. Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly. If this does not solve the problem use the *DMZ* function. This should work with most applications, but:

- It is a security risk, since the firewall is disabled for the *DMZ* PC.
- \Box Only one (1) PC can use this feature.



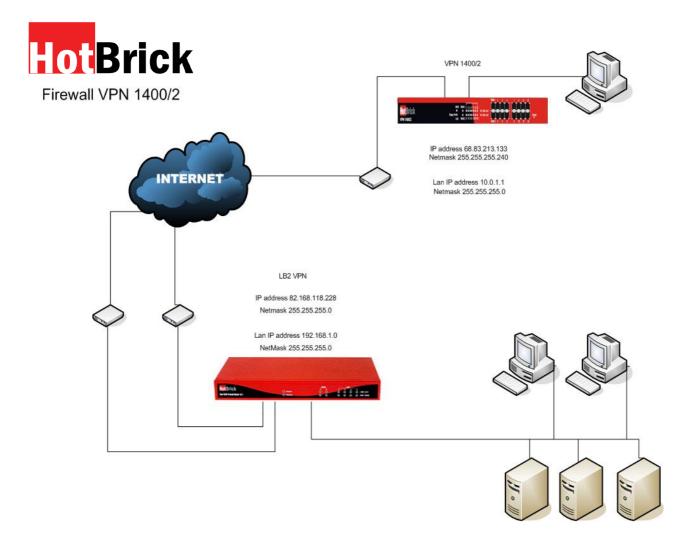
Appendix D : IPSec Tunnel Examples

VPN Configuration – Examples

Tunnel to HotBrick Unit

VPN 1400/2 To: 401VPNX2 or LB-2

The HotBrick units in the following example use registered IP addresses. You have to replace these addresses with IP addresses that are available to you. These settings are only possible if you have a static IP address available on one or both of your WAN ports.



This example takes a tunnel between a VPN 1400/2 and a LB-2 VPN. This example applies to the HotBrick 401VPN X2, LB-2 VPN and 1400/2 series, you can use either unit at both sides. You can use the IP addresses from the network diagram above.

This type of tunnel is named a LAN to LAN IPSec tunnels.



First we will make settings in the VPN 1400/2

-	otBrick		HotBri	ck VPN	1400/2	
	gin Time: 1:53 P.M.					
		VPN Configuration Tunnel to HotBrick unit Adv	vanced setti	ngs VPN pr	eset	se <mark>Heip</mark>
	Quick Installation	Tunnel to HotBrick client	unnel to 3rd	Party SA li	st VPN Log	
	Load Balancing	VPN Tunnel List Tunnel Name	Add New	Policy 👻		
	Advanced WAN	Tunnel	Enable			
	Advanced Configuration	WAN Port	WAN 1 🚩			
	Security Management	Local Security Network	IP Address	0.0.0	Netmask 0.0.0.0	
	VPN Configuration	Distinguished Name Remote client Negotiation Type	Main Mode	0.0.0.0	(Name string / IP Address)	
	QoS Configuration	Preshared Key	Main Mode	~	(Characters / Hex:0x)	
	Management Assistant					
	Device Status	Action			Status	
	Device Information	Connect	Set Options	·		
				Submit Re	set	

Next we will make settings for the LB-2 VPN

Hot Brick										LB-2 \
ogin Time: 10:32 A.M.										
Basic Configuration	IPSec Policy Setu)								🚺 HELP
Advanced Configuration	Policy Entry				Binding		Local Iden	itity Optio	n	
	New Policy Name		State	Interfa	ce Session		Туре			
Security Management	test		📃 Enable	WAN	. 😽 Sessior	n 1 🗠	IP Address	; 💙		
§ VPN Configuration										
IKE Global Setup	Traffic Selector									
IPSec Policy Setup	Protocol Type	Any 🌱								
VPN Logs		Local Ty	.ocal Type		IP Address		Subnet Mask		Port Rang	je
QoS Configuration	Local Security Network	Subnet 🎽		1	192.168.1.0		255.255.255	.0	~	
Management Assistant	Remote Security	Remote	emote Type		IP Address		Subnet Mask		Port Rang	je
	Network	Subnet	*	1	92.168.2.0		255.255.255	.0	~	
Network Info	Remote Security	Identity	dentity Type							
	Gateway	IP Addr	Address 😽 68.143.210.1							
	Security Level									
	Encapsulation Format	E	SP 🗸							
	Encryption Method	D	ES	*						
	Authentication Method	м	D5	~						
	111									
	Key Management									
	Кеу Туре		utokey (IK	E) 🗸						
	ксу турс		atokoy (In	-/	-					

Note : you need different subnets at both ends of the tunnel. This is because the IPSec tunnel will connect the two subnets so they need to be different in order to avoid IP address conflicts.

These are all the settings you need to setup the tunnel. You can push the connect buttons at one of the locations, this unit will be initiator of the tunnel, the other unit will be the responder. You can check the tunnel status in the SA list. Information about key lifetimes and these kind of things you can find by pushing the tunnel status button in **VPN Configuration – Advanced settings**.



Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com