Brick

Firewall VPN 800/8 F User's Guide



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

Copyright HotBrick 2006®. AllRights Reserved. Document Version: 1.0

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

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



TABLE of CONTENTS

1:	Introduction	. 4
	Internet Features 4	
	Other Features 4	
	Package Contents5	
	Pysical Deatails5	
2:	Quick Installation	
	Overview	
	Procedure7	
	Requirements8	
	Installing8	
	LAN & DHCP	
	Primary Setup9	
3:	Load Balancing	. 20
4:	Advanced WAN	. 21
	Port Options	
	PPPoE	
	PPTP	
5:	Advanced Configuration	. 25
	Host IP	
	Routing	
	Virtual Server	
	Special Application	
	Dynamic DNS 31	
	Multii DMZ 32	
	UPnP Setup	
	NAT Setting	
	Advanced Feature	
6:	Security Management	. 41
	URL Filter	
	Access Filter	
	Session Limit	
	SysFilter Excepmtion	



7: VPN Configuration	45
Tunnel to Hotbrick Unit	
Tunnel to Hotbrick Client 47	
Advanced Settings 48	
IPsec Policy Options 49	
VPN Preset 50	
SA List	
VPN Log	
8: QOS Configuration	55
Overview	
QOS Setup56	1
QOS Policy 57	,
9: Management Assistant	58
Admin. Setup	,
Email Alert	
SNMP	I
Syslog)
Upgrade Firmware61	
10: Device Information	63
Operation	\$
System Status64	1
WAN Status65	, ,
11: Device Status	66
Appendix A Specifications	. 68
Appendix B Windows TCP/IP Setup	69
Overview	
TCP/IP Settings)
Appendix C Troubleshooting	75
Overview	
General Problem75	
Internet Access	; ;
Appendix D IPsec Tunnel Example	. 76
Tunnel to Hotbrick Unit	

Copyright HotBrick 2006®. AllRights 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 VPN 800/8 F Firewall. The VPN 800/8 F Firewall provides 2 up to 8 WAN ports selections – it also provides **Shared Broadband** *Internet Access* for all LAN users.

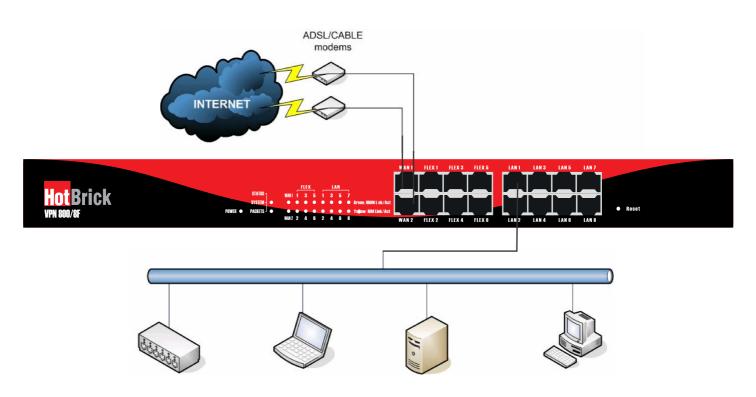


Figure 1-1: VPN 800/8 F Firewall

Internet Features

WAN ports

There are 2 up to 8 WAN ports available for use on the VPN800/8 F Firewall. They can function for load-balancing and failover.

Shared Broadband Internet Access

All LAN users can access the Internet through the VPN800/8 F Firewall by sharing two up to eight Broadband connections.

□ High-Performance multi ADSL Modem Support

The VPN800/8 F Firewall has two up to eight WAN ports, this can provide a greater increase in bandwidth than is allowed by a single connection by making use of the additional 6 flex ports that can either become LAN or WAN ports. Additionally, you can determine how the Internet traffic is shared between 2 and up to 8 connections using several different load-balacing methods.



Supports all common Connection Methods

All Popular DSL, Cable Modems and T1 Connections are supported, including Fixed IP, Dynamic IP, PPPoE, and PPTP.

Outbound Traffic Load Balancing and Failover

There are many load-balancing methods like Outbound load balance by least load(byte/packet/session/IP), Auto-learning, Priority, Round robin, Weight Round Robin, and Auto Backup Connection. These methods allow administrators to manage the 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.

URL Filter

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

WAN Ports: 2 Up to 8 10/100 Mbps

The VPN 800/8 F has 2 up to 8 WAN 10/100Mbps ports with a combination of any of the flex ports.

Flex Ports

The VPN 800/8 F has a total of 6 Flex ports that can be configured to be addditional WAN Ports or additonal LAN ports by default the Flex Ports are LAN ports .

LAN Switch Ports: 8 Up to 16 10/100 Mbps Switch

The VPN 800/8 F is an 8 up to 14 LAN 10/100 Mbps switch port with a combination of any of the flex ports, for you to share your cable/DSL connection with up to 253 users, class C subnet, on your LAN (using additional switches and/or hubs), if there are less than 14 PCs/Nodes in your network there is no need of a switch or hub.

DHCP Server Support

Dynamic Host Configuration Protocol provides dynamic IP addresses to PCs and other devices upon request. The VPN800/8 F 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 VPN800/8 F 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 VPN800/8 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 VPN800/8 F 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

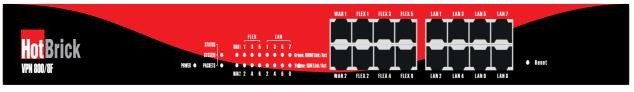


Figure 1-2: Front Panel

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

Power	OFF – No Power ON – Normal Operation
Status System	ON/OFF – Error 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 up to 8 are available for WAN connections. LAN ports: 8 up to 14 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 VPN800/8 F 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

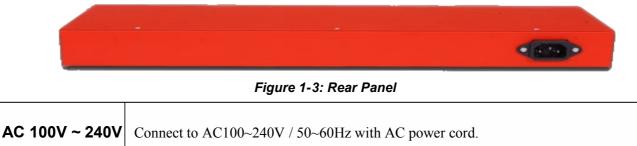


Some Status and Error conditions are indicated by combinations of LED s, as shown below

LED Action	Condition
Status - System & Packets flash concurrently	MAC address not assigned
Status - System & Packets Flash alternatively	Firmware Download in progress
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 VPN800/8 F 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 VPN800/8 F 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 VPN800/8 F 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.

🍇 TFTP V1.01			×
Local File			Browse
Upgrade Firmware Status	Save Configuration	Set to Default	Help

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 VPN800/8 F 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 VPN800/8 F Firewall (use the "Upgrade Firmware" button).
- □ Set the VPN800/8 F Firewall to its default values (use the "Set to Default" button).



2: Quick Installation

Overview

Initial Basic Setup of your VPN800/8 F Firewall involves the following steps:

- 1. Attach a PC to the VPN800/8 F Firewall in port $3 \sim 14$, and configure your LAN.
- 2. Install your VPN 800/8 F Firewall in your LAN, and connect the Broadband Modem or Modems.
- 3. Configure your VPN800/8 F Firewall for Internet Access.
- 4. Configure PCs on your LAN to use the Drewall.

Requirements

- □ 1 or up to 8 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 VPN 800/8 F Firewall for your LAN

- 1. Use a standard LAN cable to connect your PC to any LAN port (Default LAN ports 3 -14) on the VPN800/8 F Firewall. (Default 2 WAN ports from port 1-2)
- 2. Connect the power cord into a power outlet on the rear panel of VPN800/8 F Firewall.
- 3. Start your PC. If your PC is already running, restart it. It will then obtain an IP address from the VPN800/8 F 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	ur user name and password.	
•	Site:	192.168.1.1	
	Realm	NeedPassword	
	<u>U</u> ser Name	admin	
	Password		
	□ <u>S</u> ave this pa	ssword in your password list	
		OK Cance	9

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 VPN800/8 F 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.

H	otBrick		HotBi	rick VPN 80	0/8	
Lo	gin Time: 11:42 A.M.					
		Management Assi	stant			se Heip
L		Admin Setup Em	ail Alert SNMP	Syslog Upgrade I	Firmware	
	Quick Installation	Remote Access Confi Remote Upgrade	guration Remote Setup	Access Port	Allowed F	Remote IP
	Load Balancing	Enabled	Enabled	8080		- 0.0.0.0
	Advanced WAN	Administrator Passw	ord			
	Advanced Configuration	User Name admin	Password	Verify Password		
	Security Management	admin	1		!	
	VPN Configuration	Submit		Cancel		
	QoS Configuration					
Þ	Management <mark>Assistant</mark>					
	Device Status					
	Device Information					
L						
L						
L						
L						

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	800/8	
Log	gin Time: 11:42 A.M.					
		Quick Installa	and a second		ŝ	e Heip
	Quick Installation	LAN IP Configu		Subnet Mask		
	Load Balancing	192.168.1.1	(ex. 192.168.1.1)	255.255.255.0	(ex. 255.255.255.0)	
	Advanced WAN	Optional Confid	uration			
	Advanced Configuration	DHCP Server	LAN Any IP			
	Security Management					<u> </u>
	VPN Configuration	DHCP Configura Lease Time	ation DNS Server IP for Cl	ient	Offered IP Range	
	QoS Configuration	60 (min.)	1.192.168.1.1	2.192.168.1.1	192.168.1.2 ~ 192.168.1.100	
	Management Assistant	-				
	Device Status		Submit	Cancel	ВНСР L	.ist
	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 VPN800/8 F Firewall must be **disabled.** This setting is on the *LAN & DHCP* screen.
 - □ Your DHCP Server must be configured to provide the VPN800/8 F Firewall LAN IP address as the "Default Gateway".
 - □ Your DHCP Server must provide correct DNS addresses to the PCs.

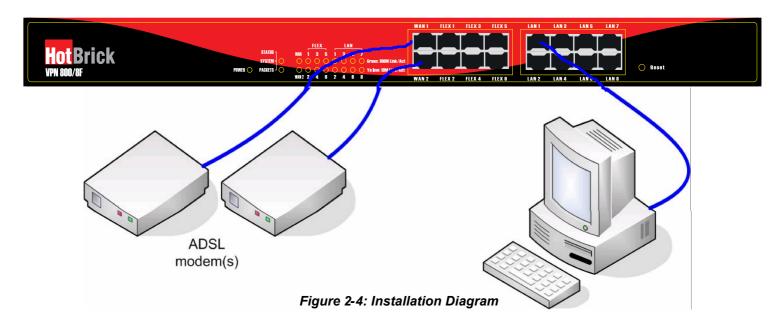
10. Ensure these settings are suitable for your LAN.

- 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 VPN800/8 F Firewall in your LAN.



HotBrick, Tel: 305-398-0888, Fax: 305-398-5966 Installing the VPN800/8 F Firewall on your LAN



- 13. Ensure the VPN800/8 F 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 VPN800/8 F 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 VPN800/8 F Firewall.
 - □ Both 10BaseT and 100BaseT connections can be used simultaneously.
 - □ If you need to connect the VPN800/8 F Firewall to another Hub, use a standard LAN cable to connect any LAN port on the VPN800/8 F Firewall to a standard port on another hub. Any LAN port on the VPN800/8 F 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 VPN800/8 F 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 - MAX WAN

HotBrick	HotBrick VPN 800/8	
Login Time: 11:42 A.M.		
	Quick Installation MAX WAN Primary Setup LAN & DHCP	%Heip
Quick Installation	Number of WAN Port	
Load Balancing	Use Port 1 ~ Port 3 a WAN port. DMZ Port Setting	
Advanced WAN	Port 15 setting as LAN Port 16 setting as LAN	
Advanced Configuration	Port 16 setting as	
Security Management	Submit	
VPN Configuration		
QoS Configuration		
Management Assistant		
Device Status		
Device Information		

Figure 3-0: MAX WAN

Flex Ports:

Here you will be able to configure how many flex ports you want to change into WAN Ports. Using the the drop down list you can choose the range of ports you want to change into WAN ports. **Note: The unit will restart inself when you submit your changes.**

DMZ Port Setting:



3. Quick Installation - LAN & DHCP

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

Ŀ	lotBrick	HotBrick VPN 800/8	
Lo	ogin Time: 11:42 A.M.		
		Quick Installation Image: Constant of the second	elp
Þ	Quick Installation	LAN IP Configuration IP Address Subnet Mask	
	Load Balancing	192.168.1.1 (ex. 192.168.1.1) 255.255.255.0 (ex. 255.255.255.0)	
	Advanced WAN	Optional Configuration	
	Advanced Configuration	DHCP Server LAN Any IP	
	Security Management		_
	VPN Configuration	DHCP Configuration Lease Time DNS Server IP for Client Offered IP Range	
	QoS Configuration	60 (min.) 1,192.168.1.1 2,192.168.1.1 192.168.1.2 ~ 192.168.1.100	
	Management Assistant		
	Device Status	Submit Cancel DHCP 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 VPN800/8 F 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 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the VPN800/8 F Firewall is attached (the same value as the PCs on that LAN).

DHCP server configuration :

- □ DHCP Server Setup If enabled, the VPN800/8 F 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 VPN800/8 F 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		
		LAN & DHCP	L.46
uick Installation	Connection		
.oad Balancing	Interface Connect Mode	WAN 1 💌 Connect Type	PPTP Connection
Idvanced WAN	O Disabled O Enabled	Dynamic IP	
dvanced Configuration	PPTP Dialup		
ecurity Management	PPTP Server IP Address 0.0.0.0	User Name	Password
PN Configuration			
oS Configuration	DNS (Optional for dynamic IP) Server 1	Server 2	Server 3
lanagement Assistant	0.0.0.0	0.0.0.0	0.0.0
evice Status	Optional		
evice Information	Host Name DBG00D63A	Domain Name	MAC Address 00-09-A3-00-D6-3A
	Update	mit and Reboot	Cancel

Quick Installation - Primary Setup

(See Below)



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. Load Balance

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

D tBrick n Time: 11:42 A.M.			1101	BHCK	VPN 8	00/			
	Load Balan	cina							
	Load Balance								760 1101
Quick Installation		ing Configuratio	n						
Load Balancing	Enabled	_					-		
Advanced WAN	Load Balancin	g Base on		B)	tes Tx + Rx WAN 1	-		N 2	WAN 3
	Loading Share	3			34 96			96	33 96
dvanced Configuration									
ecurity Management			_		_	_			
PN Configuration		Subm	it		Can	cel			
oS Configuration	Current Stat	istics							
anagement Assistant	Interface	Status	Loadin Default	g Share Current		t Loadin Byte – P		Current Ba Download	ndwidth Upload
anagement Assistant	WAN 1	Disconnected	34 %	33.96	1	1 syte	acket	0 bytes/sec	0 bytes/sec
evice Status	WAN 2	Disconnected	33 %	33.96	1	1	1	0 bytes/sec	0 bytes/set
vice Information	WAN 3	Disconnected	33.96	33.96	1	1	1	0 bytes/sec	0 bytes/se
	Overall Stati	stics							
	Interfac	e	Loading Sha	are				tes Statistics Transmitted	Total
	WAN 1		0 %		Recei	/ea O K			KB OKI
	WAN 2		0.96			ОК			кв ок
	WAN 3		0.96			0 К	в	0	кв окі

Figure 3-2: Load Balance

Load Balance

- □ **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

HotBrick		HotBri	ck VPN 800/8	
Login Time: 11:42 A.M.				
	Advanced WAN			seatteip 😪 🕹
	Port Options PPPoE	рртр		
Quick Installation	Interface			
Load Balancing	WAN Port V Connection Health Chee		0 Bytes	
Advanced WAN	Method ICMP HTTP Traffic	Interval	Alive Indic	ator
Advanced Configuration		60 sec.		
Security Management	Transparent Bridge Opt Bridge Mode	ion NetBIOS Broadcast		
VPN Configuration	Enabled	Enabled		
QoS Configuration	Transparent Bridge Opt	ions (For all interfa	ces)	
Management Assistant	• Traffic Management	Strict Binding	⊂Loose Binding ☑ No IP Translation	C Load Balancing
Device Status	ARP Tables Size 32	Entries	Clear ARP Tables	View ARP Tables
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 VPN800/8 F F irewall 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

HotBrick		HotBrick	VPN 800/8		
Login Time: 11:42 A.M.					
	Advanced WAN Port Options PPPoE P	РТР			≈≈Help
Quick Installation	Select WAN Port & Session	 1			
Load Balancing	WAN Port PPPoE Session	Session 1]		
Advanced WAN	PPPoE Session MTU	Bytes			
Advanced Configuration	WAN IP Account				
Security Management	User Name				
VPN Configuration	Password Verify Password				
QoS Configuration	Options Specified Fix IP Address	0.0.0.0	<u> </u>		
Management Assistant	Assigned Host Name	0.0.0.0	(ex. xxx.xxx.xxx.xxx)		
Device Status	PPPoE Auto Dialup				
Device Information	Auto Dialup Connect-on-demand	Disc	connect After Idle	Echo Time	Echo Retry
	Enabled	mi	inutes(-1:Always-on)	seconds	times
	Add Delete	Update	Cancel		Connect
	Connection Status WAN Session	WAN IP Addr.	Host Name	PPPoE MTU	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

	otBrick			HotBrick	XPN 800	/8		
Lo	gin Time: 11:42 A.M.	Advanced W/ Port Options		ртр			se He l	lp -
	Quick Installation	WAN Port PPTP MTU		Bytes	;			
	Load Balancing	WAN IP Accour	nt					-
Þ	Advanced WAN	User Name						
	Advanced Configuration	Password Verify Password						
	Security Management	Server IP Addres		0.0.0.0	(ex. xxx.xxx.xx	x.xxx)		
	VPN Configuration	Use Static IP		Address 0.0.0.0	_			
	QoS Configuration			et Mask 0.0.0.0	_			
	Management Assistant		Default G	ateway 0.0.0.0	_			
	Device Status	PPTP Auto Dial	up					
	Device Information	Au Connec	ito Dialup ct-on-demand		connect After Idle	Echo Ti	ime Echo Retry	
			Enabled	n	ninutes(-1:Always-c	on) seco	onds times	
		Update		Ca	ncel		Connect	
		Connection Sta WAN W	atus AN IP Addr.	PPTP IP Add	ress PPTF	Server PP	PTP 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

otBrick	ŀ	lotBrick VPN 800/8	
in Time: 11:42 A.M.			
	Advanced Configuration Virtual Server UPnP Speci Host IP Routing Dynamic	ial Application Advanced Feature DNS Multi DMZ NAT Setting	% Hel
Quick Installation	Host Network Identity		
Load Balancing	Host Name [Required]		
Advanced WAN	MAC Address [Required]	00-00-00-00-00 MAC	
Advanced Configuration	Select Group	Default 💌	
Security Management	Reserve in DHCP	Enabled	
	Reserved IP Address	0.0.0.0 DHCP List	
¥PN Configuration			
QoS Configuration	Host Network Binding Option Binding WAN Port / Session	Enabled	
Management Assistant	Binding method	○ Strict Binding SLoose Binding	
Device Status	Select WAN Port	WAN 1	
	Select PPPoE Session	Session 1 💌	
Device Information	Add Delete	Update Can	cel
	Host & Group List		
	Name MAC Address	Group	ssion(PPPoE) Binding Method Port Sess.

Advanced configuration – Host IP

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 **URL Filter** 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 **URL Filter** 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.
- \Box 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.



Advanced configuration – Routing

1	Quick Installation	Advanced Configur Virtual Server UP Host IP Routing				<i>≈</i> #e
Î	Load Balancing	Dynamic Routing RIP v2	Enabled			
Ĩ	Advanced WAN	Interface				
ÞĨ	Advanced Configuration		WAN 1	wan 2	 w	AN 3
Î	Security Management					
Ī	VPN Configuration	Submit		Cancel		
Ĩ	QoS Configuration	Static Routing Network Address	Subnet Mask	Gateway	Interface	Metric
ſ	Management Assistant	0.0.0.0	255.255.255.0	0.0.0.0	LAN	
ĺ	Device Status	Add De	lete	Update	Can	cel
Ī	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



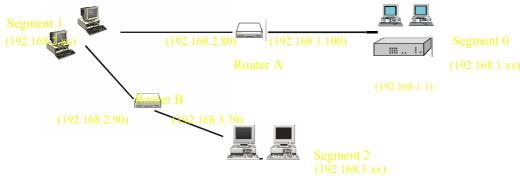
- □ **Gateway** The IP Address of the Gateway or Router that the VPN800/8 F Firewall must use to communicate with the destination above. (NOT the router attached to the remote segment.)
- □ Interface Select the correct interface, usually "LAN". The "WAN" interface is only available if NAT (Network Address 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 VPN800/8 F Firewall, so that they can be forwarded to the Internet. This is done by configuring other Routers to use the VPN800/8 F Firewall as the *Default Route* or *Default Gateway*, as illustrated by the example below.

Static Routing – example



The VPN 800/8 F Firewall Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the VPN800/8 F Firewall requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP	192.168.2.0
Address	
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	2
Entry 2 (Segment 2)	
Destination IP	192.168.3.0
Address	
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 Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.1
Metric	2

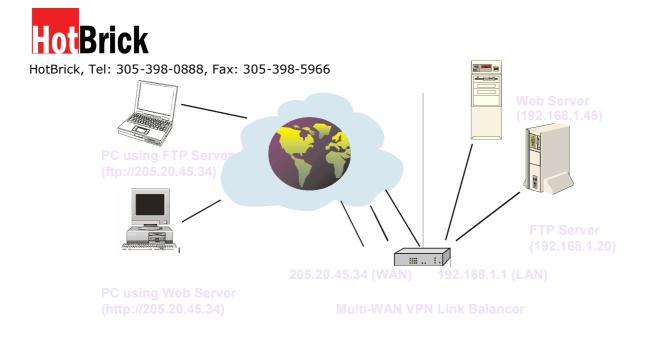
For Router B's Default Router

Destination IP Address Network Mask	0.0.0.0 0.0.0.0
Gateway IP Address	192.168.2.80
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 VPN800/8 F 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 VPN800/8 F 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.

Advanced Configuration Virtual Server

This screen allows you to define your own Server types:

otBrick jin Time: 11:42 A.M.			HotBr	ick VPN	800/8	
	Advance Host IP		mic DNS		NAT Setting	s≥, <mark>Xe</mark> l
Quick Installation						
Load Balancing	Enabled	rver Configuration Server Name	Protocol	IP Address	Port Range	Allowed Remote IP
Advanced WAN					53 ~ 53	From 0.0.0.0
		ONS		AN ALL	53 ~ 53	To 0.0.0.0
Advanced Configuration						
Security Management	Add	Delete		Update		Cancel
¥PN Configuration	Virtual Se	montist				
QoS Configuration	State	Server_Name	Protocol	Server IP	WAN Port Range	Interface Binding
yos configuration	Disabled	DNS	TCP, UDP	0.0.0.0	53~53	ALL
		ETHIOPE .	UDP	0.0.0.0	79~79	ALL
Management Assistant	Disabled	FINGER				
Management Assistant	Disabled Disabled	FINGER	тср	0.0.0.0	21~21	ALL
Management Assistant Device Status			ТСР ТСР	0.0.0.0 0.0.0.0	21~21 70~70	
- Device Status	Disabled	FTP				ALL
	Disabled Disabled	F T P GOPHER	тср	0.0.0.0	70~70	ALL ALL
- Device Status	Disabled Disabled Disabled	FTP GOPHER IPSEC	TCP UDP	0.0.0.0 0.0.0.0	70~70 500~500	ALL ALL ALL
- Device Status	Disabled Disabled Disabled Disabled	FTP GOPHER IPSEC POP3	TCP UDP TCP	0.0.0.0 0.0.0.0 0.0.0.0	70~70 500~500 110~110	ALL ALL ALL ALL
Device Status	Disabled Disabled Disabled Disabled Disabled	FTP GOPHER IPSEC POP3 SMTP	TCP UDP TCP TCP	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	70~70 500~500 110~110 25~25	ALL ALL ALL ALL ALL
- Device Status	Disabled Disabled Disabled Disabled Disabled Disabled	FTP GOPHER IPSEC POP3 SMTP NNTP	TCP UDP TCP TCP TCP	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	70~70 500~500 110~110 25~25 119~119	ALL ALL ALL ALL ALL ALL
Device Status	Disabled Disabled Disabled Disabled Disabled Disabled Disabled	FTP GOPHER IPSEC POP3 SMTP NNTP PPTP	TCP UDP TCP TCP TCP TCP	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	70~70 500~500 110~110 25~25 119~119 1723~1723	ALL ALL ALL ALL ALL ALL ALL

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.

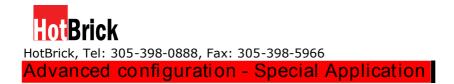
Buttons

- \Box Add Create a new Virtual Server entry.
- \Box **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 VPN800/8 F

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

				k VPN 800/8		
Quick Installation	Advanced Cor Host IP Rou Virtual Server	ting Dynamic	DNS Mult	i DMZ NAT Setting		& 1 10
Load Balancing	Enabled Nam		otocol Out		ing Protocol	Incoming Port Range
Advanced WAN Advanced Configuration	Add	Delete		Update		ncel
Security Management	Special Applicat	t ion List Name	Outgoing Protocol	Outgoing Port Range	Incoming Protocol	Incoming Port Range
QoS Configuration 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 VPN800/8 F 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 VPN800/8 F 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.



HotBrick	HotBrick VPN 800/8	
Login Time: 11:42 A.M.		
Quick Installation	Advanced Configuration Virtual Server UPP Special Application Advanced Feature Host IP Routing Dynamic DNS Multi DMZ NAT Setting	se Help
Load Balancing	Dynamic DNS Service Service V	
Advanced WAN Advanced Configuration	Server Name User Name	
Security Management	Password Verify Password Domain Name	
VPN Configuration QoS Configuration	Additional Settings	
Management Assistant	Enable Wildcard Enable Backup MX	
Device Status Device Information	Mail Exchanger	
	WAN 1 V Force Update	
	Submit Cancel	

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.

	HotBrick VPN 800/8	
Quick Installation	Advanced Configuration Virtual Server UPnP Special Application Advanced Feature Host IP Routing Dynamic DNS Multi DMZ NAT Setting	se Help
Load Balancing Advanced WAN		Direction Dutgoing 💌
Advanced Configuration	Add Celete Update Cancel	
VPN Configuration	Multi DMZ List State WAN Name Session / Public IP (WAN) 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.



Advanced Configuration - UPnP Setup

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.

	otBrick		HotBrick	VPN 80	0/8	
	gin Time: 11:42 A.M. Quick Installation	Advanced Configuratio	n namic DNS Multi D Special Application	MZ NAT Set		se Heip
	Load Balancing Advanced WAN Advanced Configuration	UPnP Option UPnP Advertisment Interval Outgoing Interface	C Enabled 30 Minut WAN 1 T	● Disabled es (2~1440)	·	
ſ	Security Management VPN Configuration QoS Configuration	Submit UPNP Port Mapping List Enabled Application Name	e Protocol	Cancel	Internal Port	External Port
	Management Assistant Device Status Device Information					

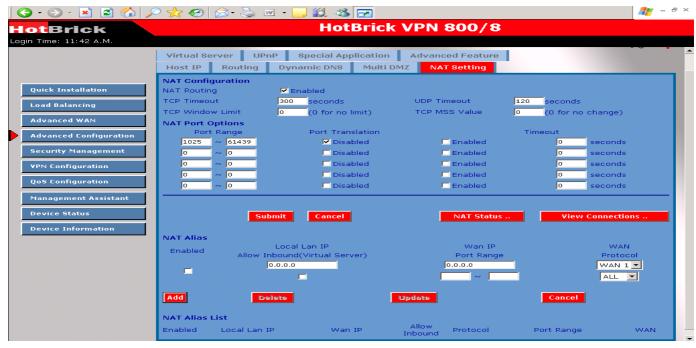
UPnP Option - If UPnP is enabled, then this device will become one of the local network devices. You can then find an icon for it in Network Neighborhood on a Windows XP computer on your LAN.

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.



Advanced Configuration – NAT Setting



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

] (3 • 🕞 - 💌 🖻 🏠 🔎	े 🏡 🚱 😒 ।	w • 🔜 🛍 🦓 🖻			🥂 – & ×
	otBrick		HotBi	ick VPN 800,	/8	
Lo	jin Time: 11:42 A.M.					
		Advanced Configu	ration			😪 🕷 🗧
		Host IP Routing	Dynamic DNS	lulti DMZ NAT Settin	g	
		Virtual Server UP	nP Special Applic	ation Advanced Feat	ture	
	Quick Installation	External Filters Confi	guration			
	Load Balancing	Block Selected ICM	P Types	Echo Request	I Timestamp Request	
	Advanced WAN			Information Request	🗹 Address Mask Requ	est
	Advanced Configuration	DNS Loopback				
		Domain Name	Private IP	Domain Name	Private IP	
	Security Management		0.0.0		0.0.0.0	-
	VPN Configuration		0.0.0.0		0.0.0.0	-
	QoS Configuration		0.0.0.0		0.0.0.0	-
	Management Assistant		0.0.0		0.0.0.0	-
	Device Status	Application				
	Device Information	IDENT Port SMTP Binding	Enabled	Make it seem clo WAN 1 💌	sed, not stealth	
		IPSec Passthrough	Enabled	AUTO V	Max Tunnels 10	
		PPTP Passthrough	Enabled	AUTO V	Max Tunnels 10	
						-
		Submit		Cancel		
		Protocol & Port Bindir	na			
			rce Type	Single IP	Protocol Po	rt Range
		Destin		Address Subnet Mas		ct Binding
		Sin	gle IP 💌		ALL 🔽	~

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.

	otBrick gin Time: 10:20 A.M.			HotBric	k VPN 80	0/8	
	gin fine. 10:20 A.M.		0.0.0.)		0.0.0.0	
	Quick Installation		0.0.0.1			0.0.0.0	_
Þ	Load Balancing Advanced WAN Advanced Configuration Security Management	Application IDENT Port SMTP Binding IPSec Passthrough PPTP Passthrough		Enabled Enabled Enabled Enabled	Make it seem WAN 1 ¥ AUTO ¥ AUTO ¥	closed, not stealth Max Tunnels 10 Max Tunnels 10	
	YPN Configuration QoS Configuration	Submit			Cancel		
	Management Assistant Device Status	Protocol & Port B Enabled	inding Source Type estination Type	From	Single IP To	Protocol WAN	Port Range Strict Binding
	Device Information		Single IP 💌 IP Range 🛩	0.0.0.0	192.168.1.0 0.0.0.0	TCP 🛩 WAN 1 💌	443 ~ 443 V
		Protocol & Port B	1976	Delete	Update	Cancel	
		State Enabled 192.168.1	Source IP .0	0.0.0.0~	Destination IP (0.0.0.0	Protocol Port Range TCP 443~443	WAN Strict



6 – Security Management

Security Management - URL Filter

HotBrick			HotBrick VPN 800/8	
Login Time: 11:42 A.M.				
	Security Ma	anagement		Setter
	URL Filter	Access Filter	Session Limit SysFilter Exception	
Quick Installation	Access Grou			
Load Balancing	Select Group URL Filter Typ		Default 💌 Block Internet Access 💌	
Advanced WAN	Set Type			
Advanced Configuration	Access Item			
Security Management	Index St	atus – URL / IP / Ke	yword On Web Site	
VPN Configuration	1			
QoS Configuration	Add	Delete	Update Cancel	
Management Assistant	Internet Acc	cess List		
Device Status	Index	Status	URL / IP / Keyword	
Device Information				
	—			

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) 🔎 🛠 🏵 🔗 🛬		rick VPN 800/8	3	
n Time: 11:42 A.M.					
	Security Manager	nent			Setter
	URL Filter Acces	s Filter Session L	imit SysFilter Exception		
	Access Group				
Quick Installation	Select Group	Default 💌			
Load Balancing					
	Filter Setting				
Advanced WAN	No Filtering		Allow Selected Access	only	
Advanced Configuration	O Block All Access		© Block Selected Access	only	
Security Management	ICMP Filters				
security management			🔽 Echo Request	🔽 Timestamp Request	
¥PN Configuration	Selected Packet T	ypes	Information Request	Address Mask Request	
QoS Configuration					
Management Assistant	Submit		Cancel		
Device Status	User-Defined Filter				
Device Information	Index Enabled	Filter Name	Protocol Type	Port Range	
Device Information		Archie	UDP -	1525 ~ 1525	
			·		
	Add	Delete	Update	Cancel	
	User-Defined Filter I	_ist			
	Index Status	Name	Protocol T	ype Port Range	
	1 Disabled	Archie	UDP	1525 ~ 1525	
	2 Disabled	DNS	UDP	53 ~ 53	
	3 Disabled	FTP Command	ТСР	21 ~ 21	
	4 Disabled	FTP Data	TCP	20 ~ 20	
	5 Disabled	Gopher TCP	ТСР	70 ~ 70	
	6 Disabled	Gopher UDP	UDP	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.

Security Management - Session Limit

	otBrick	HotBrick VPN 800/8	
Lo	gin Time: 11:42 A.M.		
		Security Management URL Filter Access Filter Session Limit SysFilter Exception	Help
	Quick Installation	Outgoing New Session	
	Load Balancing	Session Limit © Enabled © Disabled Sampling Time 400 msec.	
	Advanced WAN	Maximum of Total New Sessions 65535 sess. per sec.	
	Advanced Configuration	Maximum of New Sessions for Host 100 sess. per sec. Maximum of Dropped New Sessions for Host 25 sess. per sec.	
	Security Management	Pause Time for Host while exceeding limit on Dropped New Sessions 5 min.	
	VPN Configuration	Submit	
	QoS Configuration		
	Management Assistant		
	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

ot Brick in Time: 11:42 A.M.		HotBric	CVPN 800/8	
		cess Filter Session Limit	SysFilter Exception	~ #ei
Quick Installation Load Balancing	System Filter Exc Index Enabled	eption Rules Interface Protocol LAN ICMP	Foreign Port Range	Device Port Range
Advanced WAN Advanced Configuration	Add	Delete	Update	Cancel
Security Management ¥PN Configuration	System Filter Exc Index Status	eption Rules List Interface Protocol	Foreign Port Range	Device Port Range
QoS Configuration				
Management Assistant Device Status	1			
Device Information				

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 VPN800/8 F Firewall uses industry standard IPSec encryption. However, due to the variations in how manufacturers interpret this standard, many VPN products are not interoperable. Although the VPN800/8 F 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, LB-2, 1400/2, 800/8 F, 800/2 G and HSS 6000.

	otBrick		HotBrick VPN 800/8	
LO	gin Time: 11:42 A.M.			
		VPN Configuration		Salein
		Tunnel to HotBrick client	Tunnel to 3rd Party VPN preset SA list	144
	Quick Installation	Tunnel to HotBrick unit	Advanced settings Mesh Group VPN Log	
	Load Balancing	VPN Tunnel List	Add New Policy 💌	
		Tunnel Name		
	Advanced WAN	Tunnel	Enable	
	Advanced Configuration	WAN Port	WAN 1	
	Security Management	Local Security Network	IP Address 0.0.0.0 Netmask 0.0.0.0	
		Remote Security Network	IP Address 0.0.0.0 Netmask 0.0.0.0	
	VPN Configuration	Remote Security Gateway	IP Address 0.0.0.0	
	QoS Configuration	Negotiation Type	Main Mode	
	Management Assistant	Preshared Key	(Characters / Hex:0x)	
	Device Status			
	Device status	Action	Status	
	Device Information	Connect	Set Options	
			Submit Reset	

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

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

	VPN Configuration		e al e l
Quick Installation	Tunnel to HotBrick unit Tunnel to HotBrick client	Advanced settings Mesh Group VPN Log Tunnel to 3rd Party VPN preset SA list	
Load Balancing	VPN Tunnel List	Add New Policy 💌	
Advanced WAN	Tunnel Name Tunnel	Enable	
Advanced Configuration	WAN Port	WAN 1 -	
Security Management	Local Security Network Distinguished Name Remote	IP Address 0.0.0.0 Netmask 0.0.0.0	
¥PN Configuration	client	peer ID 0.0.0.0 (Name string / IP Address)	
QoS Configuration	Negotiation Type Preshared Key	Main Mode 🔽 (Characters / Hex:0x)	
Management Assistant	1		
Device Status	Action	Status	
Device Information	Connect	Set Options	
		Submit Reset	



Tunnel to HotBrick Client – This describes an IPSec tunnel from a the VPN 800/8 F 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.



	J • 🕑 • 본 😢 	🔎 🧙 🚱 😒 🌭 💌 •		🥂 – 8 ×
	otBrick		HotBrick VPN 800/8	
Lo	gin Time: 11:42 A.M.			
		VPN Configuration		😪 😪 🖌 🖕
		Tunnel to HotBrick client	Tunnel to 3rd Party VPN preset SA list	
		Tunnel to HotBrick unit	Advanced settings Mesh Group VPN Log	
	Quick Installation	VPN Tunnel		
	Load Balancing	Tunnel List		
		PPPoE Session	Session 1 🔽	
	Advanced WAN	Enable Setting		
	Advanced Configuration	Key Management		
	Security Management	Кеу Туре	AutoKey (IKE)	
	VPN Configuration	Phase 1		
	QoS Configuration	Negotiation Type	Main Mode	
		DH Group	DH Group 2 (1024-bit) 💌	
	Management Assistant	Encryption Method	AES (128 bits)	
	Device Status	Authentication Method	SHA1	
	Device 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 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.

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.



VPN Configuration - Tunnel to 3rd Party

	3 • 🕑 • 💌 🖻 🏠 🍃	후 🛠 😧 😒	🔤 🛛 📜 鑬 🦓 🛃	🥂 - 8 ×
-	lotBrick		HotBrick VPN 800/8	
Lo	gin Time: 11:42 A.M.			
		VPN Configuratio	n	😪 Help 🔺
		Tunnel to HotBrick	unit Advanced settings Mesh Group VPN Log	
		Tunnel to HotBrick	client Tunnel to 3rd Party VPN preset SA list	
	Quick Installation	IPSec Traffic Bindin		
	Load Balancing	VPN Tunnel List	Add New Policy 💌	
	Advanced WAN	Tunnel Name Tunnel	Enable	
	Advanced Configuration	WAN Port	WAN 1	
	Security Management	Local Identity Type	Wan IP Address 💌 Local ID/Email	<u> </u>
	¥PN Configuration	Traffic Selector		
	QoS Configuration	Service	Protocol Any 💌	
	Management Assistant Device Status	Local Security Network	Local Type Subnet IP Address 0.0.0.0 Mask Address 0.0.0.0 Port Range 0 ~ 0	
	Device Information	Remote Security Network	Remote Type Subnet 💌 IP Address 0.0.0.0 Mask Address 0.0.0.0 Port Range 0 ~ 0	
		Remote Security Gateway	Identity Type IP Address T IP Address 0.0.0.0	
		Key Management Negotiation Type	Main Mode	
		Preshared Key	(Characters / Hex:0x)	

Tunnel to 3rd Party - This describes an IPsec tunnel from a VPN800/8 F with a non-Hotbrick certified 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. They must be the same on both units.
- Action
 Connect this button will initiate the tunnel
 Submit Query this button will add the policy



IPSec policy options

Time: 1:14 P.M.			Hotbrie	« VPN 800	, •			
	IPSec Policy	options					e He	
	Tunnel Attribut	es						
uick Installation	State Name	Security Gateway	Remote Network	Security Level	Кеу Туре	Interface	Negotiation Status	
oad Balancing	Enabled 6565	, 115.365.18.9	0.0.0.0/0.0.0.0	AES (128 bits)/SHA1	Autokey (IKE)	WAN 1 Disconnected	Idle	
dvanced WAN	Dead Peer Det	ection Feature	,					
dvanced Configuration	Detection		Enabled					
ecurity Management	Check Method		C Heartbeat	CICMP Host 0.0.0.0		• DPD	PD (RFC 3706)	
ecurity Planagement	Check After Idle		60 Seconds					
PN Configuration	Retry Times		10					
oS Configuration	Action		Failover	C Remove Tu	unnel	С Кеер	Tunnel Alive	
	Logging		💌 Enabled					
1anagement Assistant	NAT Traversal	Feature						
evice Status	NAT Traversal	cuture	Enabled					
evice Information	Keep Alive Inter	val	60 Seconds	UDP Checksur	m	E Enab	led	
	Options							
	NetBIOS Broadc	ast	🔽 Enabled	Check ESP Pa	id	🗖 Enab	oled	
	Auto Triggered		🗖 Enabled	Allow Full ECN		🗖 Enab		
	Anti Replay		🗖 Enabled	Copy DF Flag		🗖 Enab		
	Passive(Respond	der) Mode	🔽 Enabled	Set DF Flag		🗖 Enab	led	

- **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 Tunnel to HotBrick unit Advanced settings Mesh Group VPN Log Quick Installation Tunnel to HotBrick client Tunnel to 3rd Party VPN preset SA list Load Balancing WAN Port WAN 1 Kativate IPSec Task I Advanced Configuration Retry Counter 500 Retry Counter Sa	e e e e e e e e e e e e e e e e e e e
Load Balancing Preset Parameters Advanced WAN WAN Port WAN 1 Advanced Configuration Activate IPSec Task I ISAKmp Port 500 Retry Counter 5	
Advanced WAN Activate IPSec Task Image: Configuration Advanced Configuration ISAKmp Port 500 Retry Counter 5	
Retry Counter 5	
Retry Counter 5	
Security Management Retry Interval 10 Seconds	
VPN Configuration Maxime to complete Phase 1 180 Seconds	
QoS Configuration Maxtime to complete Phase 2 120 Seconds	
Count Per Send 1	
Management Assistant NAT Traversal Port 4500	
Device Status	
Device Information Logging Level	
Log Level Infomation 💌	
submit submit	

- 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 in Time: 11:42 A.M.	HotBrick VPN 800/8
		VPN Configuration Tunnel to HotBrick unit Advanced settings Mesh Group VPN Log Tunnel to HotBrick client Tunnel to 3rd Party VPN preset SA list
ĺ	Quick Installation Load Balancing	Security Association List State Name Security Remote Site Security Policy Key Type Physical Negotiation Status Status Status
-	Advanced WAN Advanced Configuration	Prev Page Next Page Refresh
	Security Management	
	¥PN Configuration QoS Configuration	
i	Management Assistant	
ļ	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.

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

VPN Configuration – VPN Log

	HotBrick VPN 800/8
Login Time: 11:42 A.M. Quick Installation Load Balancing Advanced WAN Advanced WAN Advanced Configuration Security Nanagement VPN Configuration QoS Configuration Nanagement Assistant Device Status Device Information	VPN Configuration Tunnel to HotBrick client Tunnel to 3rd Party VPN preset SA list Tunnel to HotBrick unit Advanced settings Mesh Group VPN Log Message Status: 0 message(s) Messages Time Priority Module Messages Prev Page Refresh Next Page Clear All

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 VPN800/8 F 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 inreal-time application achieving better response or performan

	otBrick		HotBrick VPN 800/8	
LO	gin Time: 11:42 A.M.			
		QoS Configuration		se Help
		QoS Setup Policy Confi	iguration	-
	Quick Installation	QoS Features		
	Load Balancing	Enable QoS Queuing Method	Enabled Priority Queuing	
	Advanced WAN			
	Advanced Configuration	IP TOS(Type of Service) Fe Process TOS Field	Enabled	
	Security Management	Overwrite Policy Priority	T Yes	
	VPN Configuration			
	Qos Configuration	Submit	Cancel	
	Management Assistant			
	Device Status			
	Device Information			

QoS Features :

- □ **Enable QoS** This enables theQoS function.
- Queuing Method Thesesmethodsdeterminehow 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 choese ble 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.



	lotBrick		HotBrick VPN 800/8	
La	ogin Time: 11:42 A.M.			
		QoS Configuration	figuration	% Help
	Quick Installation	QoS Features Enable QoS	Enabled	
	Load Balancing	Queuing Method	Priority Queuing	
	Advanced WAN	IP TOS(Type of Service) F	eatures	
	Advanced Configuration	Process TOS Field Overwrite Policy Priority	Enabled	
	Security Management	Overwrite Policy Priority	Yes	
	VPN Configuration	Submit	Cancel	
₽	Qos Configuration			
	Management Assistant Device Status			
	Device Information			



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 Overwrite policy priority - Choose "yes" to set the priority of the TOS field in IP the packet to overwrite the priority to overwrite the priority of the policy configuration.

otBrick gin Time: 11:42 A.M.		HotB	rick VPN 800	/8	
	QoS Configura QoS Setup	tion blicy Configuration			se tel
Quick Installation	Policy Priority				
Load Balancing	Policy Name Source Address	IP Address 🔽			
Advanced WAN		From 0.0.0.0	То 0.0.0.0		
Advanced Configuration	Destination Addres				
Security Management	Protocol Type	From 0.0.0.0	То 0.0.0.0		
VPN Configuration	Source Port	From 0 To 0			
QoS Configuration	Destination Port Priority Queue	From 0 To 0			
Management Assistant	Phoney Quede	Thigh 💽			
Device Status	Add	Delete	Update	Cano	cel -
Device Information					
	Policy List Policy Name So	urce Address / Port	Destination A	ddress / Port	Protocol Queue
	Policy Name Sc		Destination A		FISCOLOF QUEL

QoS Configuration – Policy Configuration

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



Policy Priority

- □ 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.
- □ 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

HotBrick	HotBrick VPN 800/8	
Login Time: 11:42 A.M.	Management Assistant Admin Setup Email Alert SNMP Syslog Upgrade Firmware	Melp
Quick Installation Load Balancing	Remote Access Configuration Remote Upgrade Remote Setup Access Port Allowed Remote IP Enabled Enabled 8080 0.0.0.0 ~ 0.0.0.0	
Advanced WAN Advanced Configuratio	Administrator Password User Name Password Verify Password admin	
Security Management VPN Configuration QoS Configuration	Submit Cancel	
Management Assistant Device Status		
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 ×
	Please type y	ourusername and password.	
- T.	Site:	192.168.1.1	
	Realm	NeedPassword	
	<u>U</u> ser Name	admin	
	Esseword		
	E Serve this p	assword in your password list	
		OK. Care	la

Figure 8-5: Password Dialog

- Enter "Admin" for the User Name.
- □ Enter the password for the VPN800/8 F Firewall, as set on the *Admin Password* screen above. (The default is blanks.)



otBrick		H	otBrick V	PN 800/8	
gin Time: 11:42 A.M.					
	Management As	sistant			
	Admin Setup	mail Alert SN	IMP Syslog	Upgrade Firmware	
Quick Installation	Global Settings: No				
Load Balancing	Enable & Link Down	Excessive		Before Notification 120 tim	voc (min
Advanced WAN		Enabled	MAX. Pings i		
	Email Alert Configu		1		
Advanced Configuration	Email (SMTP) Server	Address			
Security Management	User Name				
¥PN Configuration	Password				
VPN Configuration	Sender Address				
QoS Configuration	Recipient Address				_
Management Assistant			Validate Settings	Send Test E-mail	
Device Status		Submit		Cancel	
Device Information		Jubinit		Current	
	Email Alert Configu	ration List			
	Interface	Mail Server	User Name	Sender Addr.	Recipient Addr.
	LAN				
	WAN 1				

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.

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

□ **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 800/8 F.

HotBrick		HotBrick \	/PN 800/8	
Login Time: 11:42 A.M.				
	Management Assis	tant iil Alert <mark>SNMP</mark> Syslog	Upgrade Firmware	e Help
Quick Installation	System Information			
Load Balancing	Contact Person Device Name	Supervisor HotBrick VPN 4000		
Advanced WAN	Physical Location	Head Office		
Advanced Configuration	Community			
Security Management	Community Name 1	private	Access Control 1 Read/Write	
VPN Configuration	Community Name 2	public	Access Control 2 Read Only	⊻
QoS Configuration	Trap Targets Target IP Address 1	0.0.0.0 (ex. xxx.x	xx.xxx.xxx)	
Management Assistant	Target IP Address 2	0.0.0.0		
Device Status	Target IP Address 3	0.0.0.0		
Device Information	Submit		Cancel	

System Information

- **Contact Person** The contact information for the person responsible for this device.
- Device name The name of the VPN800/8 F Firewall.
- Dependence of the Physical Location The location of the VPN800/8 F 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 addressof any targets (PCs running SNMP software) that you want to receive traps.All traps are level 1.

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

Management Asssistant – Syslog

otBrick			HotBrick V	PN 800/8			
gin Time: 11:42 A.M.							
	Management 4	ssistant			⊗aHelp		
	Admin Setup	Email Alert	SNMP Syslog	Upgrade Firmware			
Quick Installation	Syslog Delivery						
Load Balancing	Sending Out	Enabled	Enabled	Keep Sent Message Port (Default:514)	Enabled		
Advanced WAN	Syslog Server :		0.0.0	514	Emerg. 💌		
Advanced Configuration	Syslog Server : Syslog Server :		0.0.0.0	514	Emerg. 💌 Emerg. 💌		
Security Management					Expand		
VPN Configuration		Log Priority for Modules					
QoS Configuration	SNTP Configurati		L:00) France, German	y, Italy 💌			
Management Assistant	System Time	2000 / 1	/ 1 0 ; 51 ;	37			
-	SNTP Server 1						
Device Status	SNTP Server 2						
Device Information	SNTP Server 3						
		Submit	Cancel		View Syslog		
				-			

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.

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

Management Assistant - Upgrade Firmware

H	otBrick			HotB	rick V	/PN 800/8	8		
Log	jin Time: 11:42 A.M.								
		Management	Assistant					đ	e Heip
		Admin Setup	Email Alert	SNMP	Syslog	Upgrade Firmv	vare		_
	Quick Installation	System Config Save System Co		Save				Factory Settin	as
	Load Balancing								
	Advanced WAN	Upgrade Firmw User Name	are	admin					
	Advanced Configuration	Password							
	Security Management	Upgrade Softwar Configuration	re or				Browse	Upgrade	
	VPN Configuration								
	QoS 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 VPN800/8 F 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.

Device status – System status HotBrick VPN 800/8 **Hot**Brick ogin Time: 11:42 A.M **Melp** Device Status WAN Status Interface Connection Type Quick Installation Status MAC Address 00-09-A3-00-D6-3A WAN 1 DHCP Disconnected Load Balancing WAN 2 Disconnected 00-09-A3-00-D6-3B DHCP Advanced WAN WAN 3 Disconnected 00-09-A3-00-D6-30 DHCP Advanced Configuration Interface IP Address Subnet Mask Gateway **DNS IP Address** ity Managen WAN 2 WAN 3 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Interface IP Address LAN 192.168.1.1 Subnet Mask 255.255.255.0 MAC Address 00-09-A3-00-D6-39 DHCP Server agement Assista Enabled Device Status Device Informatio

- □ **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 VPN800/8 F 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 800/8 F Firewall Router.
- □ **Subnet Mask –** The Network Mask (Subnet Mask) for the IP Address above.
- □ **MAC Address –** The MAC (physical) address of the VPN800/8 F Firewall.



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

	Manageme	nt Assistant							e stel
	Admin Setu	Email Alert	SNMP	Syslog	g Upgi	ade Fi	rmware		140
Quick Installation	Current Stati	stics							
Load Balancing	Interface	Status	Loading Default	Share Current	Curre Session	ent Load		Current I Download	Bandwidth Upload
Load balancing	WAN 1	Disconnected	34 %	33.96	Session 1		Packet		
Advanced WAN	WAN 2	Disconnected	33.96	33 %	1				
Advanced Configuration	WAN 3	Disconnected	33 %	33 %	1	1			
Security Management	Overall Stati	stics							
VPN Configuration	Interface	e L	oading Shai	re			Overall	Bytes Statistics	
VPN Configuration	WAN 1		0.96		Rece	eived	кв	Transmitted	Total OKB OKE
QoS Configuration	WAN 1 WAN 2		0%				КВ		0 KB 0 KB
Management Assistant	WAN 3		0 %				КВ		
-									
Device Status						_		_	
Device Information		Refre	sn	Restart (ounters			_	NAT Status

Device Status - V	VAN status	5
--------------------------	------------	---

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.

ime: 9:51 A.M.						
	NAT Status					÷,
ick Installation	Active Interface IP I Interface LAN	n fo. IP Addres 192.168.			et Mask 55.255.0	
ad Balancing vanced WAN	NAT Timeouts		300	UDP		120
vanced Configuration	TCP Property Max. Segment Size		1460	Max. Windows !	Size	0
N Configuration	NAT Traffic			To Internet		net To Local
5 Configuration	Bytes Packets	0			0	
nagement Assistant	Connection List					
vice Status	TCP 0 Overall Connections	c	IDP reated	0	ICMP Deleted IP Address	0
vice Information	View D	elete –	riteria Filter Set Clear Al	Interface	0.0.0.0	WAN Port Range
	Errors Checksum 0	R	etries	0	Bad Packets	0
	Misc. Total IP Packets	496		Reserved Addres	s O	

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



Data – NAT Status

LAN IP info

- □ **IP Address –** The LAN IP Address of the VPN800/8 F 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 VPN 800/8 F 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					
Load Balancing	Hardware ID Firmware Version		03212104200001 Ver 8.0 Rel 13 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	System UpTime		54m 42s			
VPN Configuration	CPU Usage 1 %		Memory Heap 1 %		Packet Queue 1 %	
QoS Configuration		Refresh			Factory Settings	Restar
Management Assistant				-		_
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 VPN800/8 F Firewall.

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



) • 🕑 • 본 🙆 🔒	🔎 🏡 🚱 🙆 • 🥃 🔟 • 🧾 🏭 🕸 🖃	A -
otBrick	HotBrick VPN 800/8	
n Time: 10:07 A.M.		
		<u> </u>
Quick Installation	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 default values.	n to factory
Load Balancing	Restore	
Advanced WAN		
Advanced Configuration		
Security Management		
¥PN 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 VPN800/8 F Firewall using its default IP address (192.168.1.1).



Appendix A

Specifications

Model Dimensions Operating Temperature	HotBrick VPN 800/8 F 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 (H	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.

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 VPN800/8 F 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:

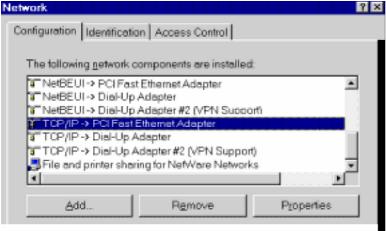


Figure B-1: Network Configuration

- 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>
Advan	ced	NetBI	0S	DNS Co	nfiguration
	WINS Co	onfigura	tion	IP.4	vddress
does not (inistrator to	automatic or an add	colly as: Iress, ar	sign IP (ad then	addresses,	ask.your
an IP add	ness:				
fress.					
efikiasko		1	1		
	s can be a does not i inistrator to an IP addr ren IP add fress	s can be automatic does not automatic inistrator for an add an IP address autor ran IP address:	WINS Configural s 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 t does not automatically assign IP inistrator for an address, and then an IP address automatically ran IP address: fress.	WINS Configuration IP A s 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 ran IP address:

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 800/8 F 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 VPN800/8 F 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 VPN800/8 F Firewall.)

Statistics

TCP/IP Propertie	is .		? ×
Bindings Gateway	Advanced WINS C	NetBIOS Configuration	DNS Configuration IP Address
address order are used.	in the list will be		vill be the default. The ch these machines
<u>N</u> ew gotewey 192 . 168	y: 3.0.1	Add	
Installed gate	wøys:	Eams	VE
Figu	ire B-3: Gat	eway Tab (M	Vin 95/98)

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 Propertie	98		? ×
Gateway		Configuration	IP Address DNS Configuration
C Disable D	Advanced	NetBIOS	Divid Comiguration
C Disable D			
in Euglie D	140		
Host:		D <u>o</u> main:	
DNS Server	Search Order		
		\supset _	Add
		1	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 connection:
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks Thtemet Protocol (TCP/IP)
Install Uninstall Properties
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Show icon in taskbar when connected
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	_
_⊂ O 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 VPN800/8 F 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 VPN800/8 F 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) Properties 🛛 🔹 🔀								
Gene	eral	Alternate Configuration						
this	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.							
⊙ <u>O</u> btain an IP address automatically								
-	O Use the following IP address:							
	P ad	dress:	· · ·					
	6 <u>u</u> bn	et mask:						
	<u>)</u> efa	ilt gateway:	· · ·					
⊙ O <u>b</u> tain DNS server address automatically								
6	O Use the following DNS server addresses:							
Preferred DNS server:								
	Alterr	ate DNS server:	· · ·					
			Advanced					
			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 VPN800/8 F 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 VPN800/8 F 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*.

ARri

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

Appendix C

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while us/AFN1600/8 F Firewall and some possible solutions for them. If you follow the suggested steps and the VPN 800/8 F Firewall still does not function properly, contact your dealer for further advice.

General Problems

Problem : Can't connect to the VPN800/8 F 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 VPN800/8 F Firewall are on the same network segment. (If you
- dont 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 192.168.12 to 192.1681.254 and thus compatible with the VPN800/8 F Firewall default IP Address of 192.1681.1. Also, the Network Mask should be set to 255.255255.0 to match the VPN 800/8 F 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 If is a second 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 800Firewall Router. Ensure that it is comected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections)
- If the VPN800/8 F Firewall is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is workinorrectly.

Problem : Some applications do not run properly when using the VPN800/8 F Firewall.

Solution :

The VPN800/8 F 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 doesnot solve the problem use the MZ function. This should work with most applications, but:

- It is a security risk, since the firewall is disabled for tDe/Z PC.
- Only one (1) PC can use this feature.



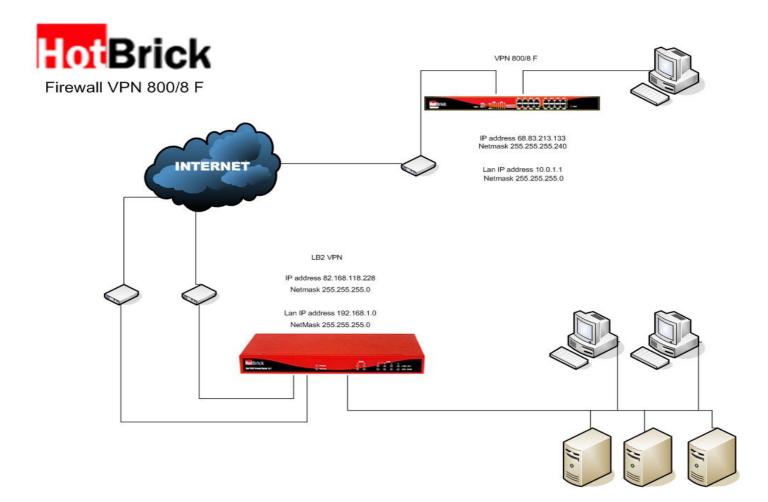
Appendix D : IPSec Tunnel Examples

VPN Configuration – Examples

Tunnel to HotBrick Unit

VPN 800/8 F 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 800/8 F and a LB-2 VPN. This example applies to the HotBrick 401VPN X2, LB-2 VPN and 800/8 F 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 800/8 F

	lotBrick		HotBrick VPN 800/8		
	ngin Time: 11:42 A.M.	VPN Configuration	Tunnel to 3rd Party VPN pr	reset SA list	% Help
	Quick Installation	Tunnel to HotBrick unit	Advanced settings Mesh Gro	oup 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 0.0.0.0	Netmask 0.0.0.0	
Þ	VPN Configuration	Remote Security Network Remote Security Gateway	IP Address 0.0.0.0	Netmask 0.0.0.0	
	QoS Configuration	Negotiation Type	Main Mode		
	Management Assistant	Preshared Key		(Characters / Hex:0x)	
	Device Status				
	Device Information	Action Connect	Set Options	Status	
			Submit Reset	3	

Next we will make settings for the LB-2 VPN

Hot <mark>Brick</mark>					LB-2 \	
Login Time: 10:32 A.M.						
Basic Configuration	IPSec Policy Setup					
Advanced Port	Policy Entry		Traffic Binding	Local Identity Optic	n	
Advanced Configuration	New Policy test	State	Interface Session	Туре		
§ Security Management		Enable	WAN 1 💙 Session 1 💙	IP Address 😽		
VPN Configuration		I				
IKE Global Setup	Traffic Selector					
IPSec Policy Setup	Protocol Type	Any 🎽				
VPN Logs	Local Security Networ	Local Type	IP Address	Subnet Mask	Port Range	
QoS Configuration	Local Security Networ	Subnet 🌱	192.168.1.0	255.255.255.0	~	
Anagement Assistant	Remote Security	Remote Type	IP Address	Subnet Mask	Port Range	
Network Info	Network	Subnet 🌱	192.168.2.0	255.255.255.0	~	
	Remote Security	Identity Type				
	Gateway	IP Address	68.143.210.1			
	Security Level					
	Encapsulation Format	ESP 🗠				
	Encryption Method	DES	*			
	Authentication Method	I MD5	*			
	Key Management					
	Кеу Туре	Autokey (Ik	(E) 🔽			

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