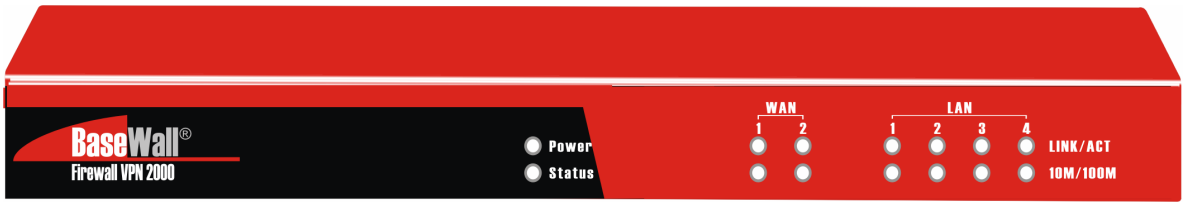
Dual WAN VPN Firewall VPN 2000
User's Guide



Version 1.0 Date : 1 July 2005

Please check www.basewall.com for the latest version

TABLE OF CONTENTS

Document Version: 1.4

1:Introduction

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

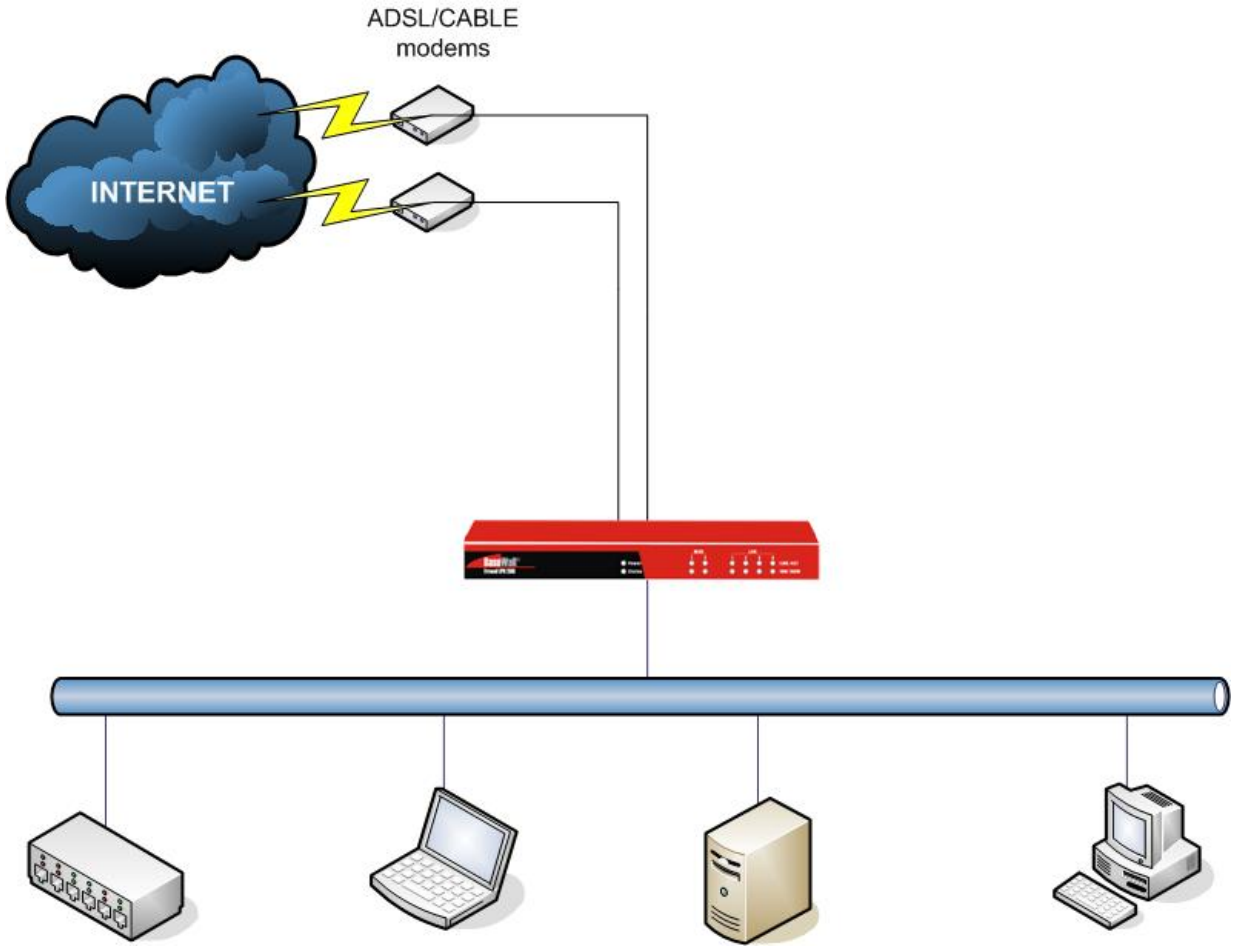


Figure 1-1: Dual WAN VPN Firewall

Internet Features

- ***Dual WAN ports***

  There are 2 WAN ports available for use on the Dual WAN VPN Firewall. They can function as a loadbalancer or as failover.

- ***Shared Broadband Internet Access***

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

- ***High-Performance multi ADSL Modem Support***

  The Dual WAN VPN Firewall has two WAN ports, allowing the connection of up to two broadband modems at the same time.
  This can provide a greater increase in bandwidth than is allowed by a single modem.
  Flexible configuration allows each port to use a different type of modem and connection methods. Also, you can determine how the Internet traffic is shared between the 2 modems.

- ***Supports all common Connection Methods***

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

- ***Outbound/Inbound Traffic Load Balancing and Failover***

  There are many load balancing methods to allow administrators to manage the traffic from LAN or WAN to maximize the bandwidth and smart health check methods to against connection failure or failover.

- ***PPPoE Session Management***

  Multiple PPPoE sessions are supported and you can choose to “mapping” sessions to individual for PCs if desired.

- ***Multiple IP Address Support***

  If your ISP allocates you multiple IP addresses, these are also supported and you can “map” IP addresses to individual PCs if desired.

- ***Special Application***

  This feature allows you to use some non-standard applications, where the port number used for the response is different to the port number used by the sender.

- ***Virtual Server***

  This feature allows Internet users to access 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 required.

- ***Multiple DMZ***

  A "DMZ" PC will receive incoming connection requests, which would otherwise be blocked. For each IP address allocated by your ISP, a separate "DMZ" PC can be specified. So if your ISP has given you multiple IP addresses, you can have multiple “DMZ” PCs. Each “DMZ” PC has unrestricted 2-way Internet access, providing the ability 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 the Internet access and applications available to LAN users. Five (5) user groups are available, and each group can be assigned different access rights.

- ***Block URL***

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

- ***Session Limit***

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

- ***System Filter Exception***

  It will reject every packet with an unrecognized port to avoid port scan program from hackers, but this also invokes problems on situation that some servers (e.g. SMTP server port 113) or client from WAN need to response packet to justify aliveness of their communication peers.

- ***VPN (Virtual Private Network)***

  Support up to 10 VPN tunnels, with a fail-over mechanism.

Other Features

- ***4-Port Switching Hub***

  The Dual WAN VPN Firewall incorporates a 4-port 10 /100BaseT switching hub, making it easy to create or extend your LAN.

- ***DHCP Server Support***

  Dynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Dual WAN VPN Firewall can act as a **DHCP Server** for devices on your local LAN.

- ***Multi Segment LAN Support***

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

- ***Easy Setup***

  Use your favorite WEB browser for configuration.

- ***Remote Management***

  The Dual WAN VPN Firewall can be managed from any PC on your LAN. And, if the Internet connection exists, it 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 upgrade new firmware and backup system configuration from local or even from remote site. As long as you enable “Remote upgrade” and “Remote web-based setup” from Advanced feature web page.

- ***Email Alert***

  It will send a warning email to the system administrator, if one of the WAN ports was disconnected when over two WAN ports are enabled or there is excessive ping notification.

- ***Syslog***

  It can generate real time system information on the web page or a particular machine. It is useful to monitor the device.

- ***QoS Configuration.***

  This function will make some specified packets with higher priority for pass-through. Especially you use real-time applications like Internet phone, video conference etc.

- ***UPnP***

  To “Enable” UPnP (Universal Plug & Play), the Dual WAN VPN Firewall will become one of the network devices. It is useful to discover and control network devices, such as Internet gateway.

Package Contents

The following items should be included:

- The Dual WAN VPN Firewall Unit
- Power Cord
- Quick Installation Guide
- CD-ROM containing the on-line manual.

Note: If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel

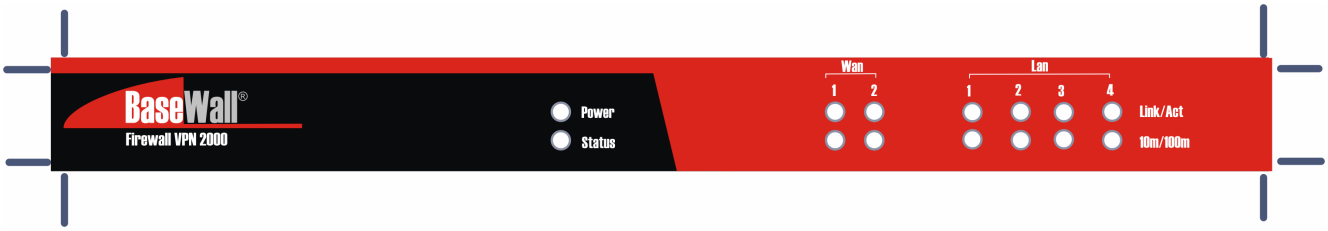


Figure 1-2: Front Panel

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

Power	OFF – No Power ON – Normal Operation
Status **System** **Packets**	 Blinking – Normal Operation. ON/OFF – Error Blinking – Packets Active ON/OFF – No Packet
Ethernet	Green ON – 100M Linked Yellow ON – 10M Linked Blinking – Data Transmit / Receive. OFF – No Linked

Ethernet Ports and Reset Bottom

Ethernet Ports	WAN ports: 2 connected to Modem here. LAN ports: the other ports which are connected to PC or Hub Note: You can use a normal LAN cable connecting to a normal port on another hub.
Reset Button	When pressed and released, the Dual WAN VPN Firewall will reboot (restart) within 1 second. It will reset to default factory settings after you press and hold the reset button over 3 seconds

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

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

Default Settings

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

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

TFTP Download

This setting should be used only if your Dual WAN VPN Firewall is unfit for use, and you wish to restore it by uploading new firmware you should use the following procedure:

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

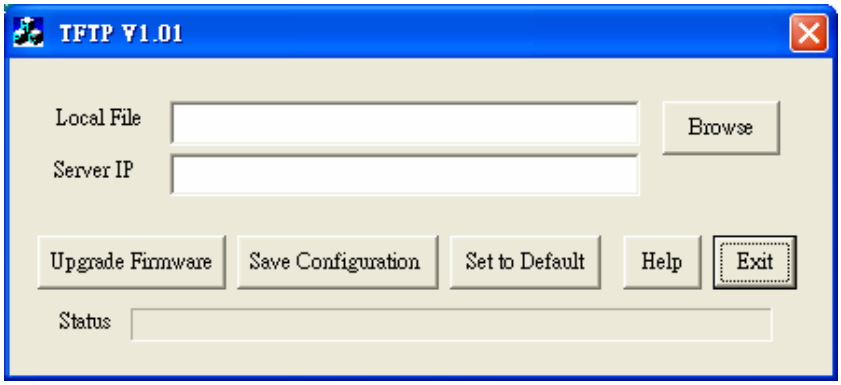


Figure 1-4: Windows TFTP utility

- Enter the name of the firmware upgrade file on your PC, or click the "Browse" button to locate the file.
- Enter the LAN IP address of the Dual WAN VPN Firewall in the "Server IP" field.
- Click "Upgrade Firmware" to send the file to the Dual WAN VPN Firewall.

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) other operations:

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

2: Quick Installation

Overview

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

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

Requirements

- One up to 2 DSL or Cable modems, each with an Internet Access account with an ISP.
- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors
- TCP/IP network protocol must be installed on all PCs.

Procedure

1: Configuring the Dual WAN VPN Firewall for your LAN

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

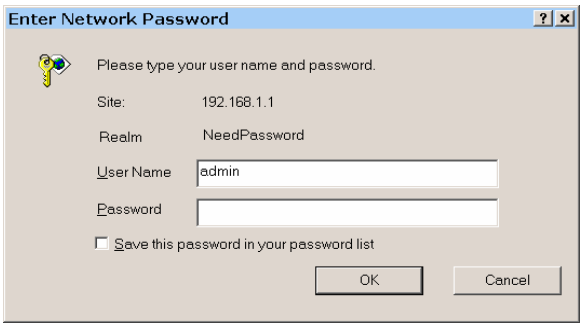


Figure 2-1: Password Dialog

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

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

No Response?

- Is your PC using a Fixed IP address?

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

- Check that the Dual WAN VPN Firewall is properly installed, LAN connection is OK, and it is powered ON.

7 After the login, you will then see the ***Admin Password*** screen, as shown below. Assign a password by entering it in the "Password" and "Verify Password" Fields.

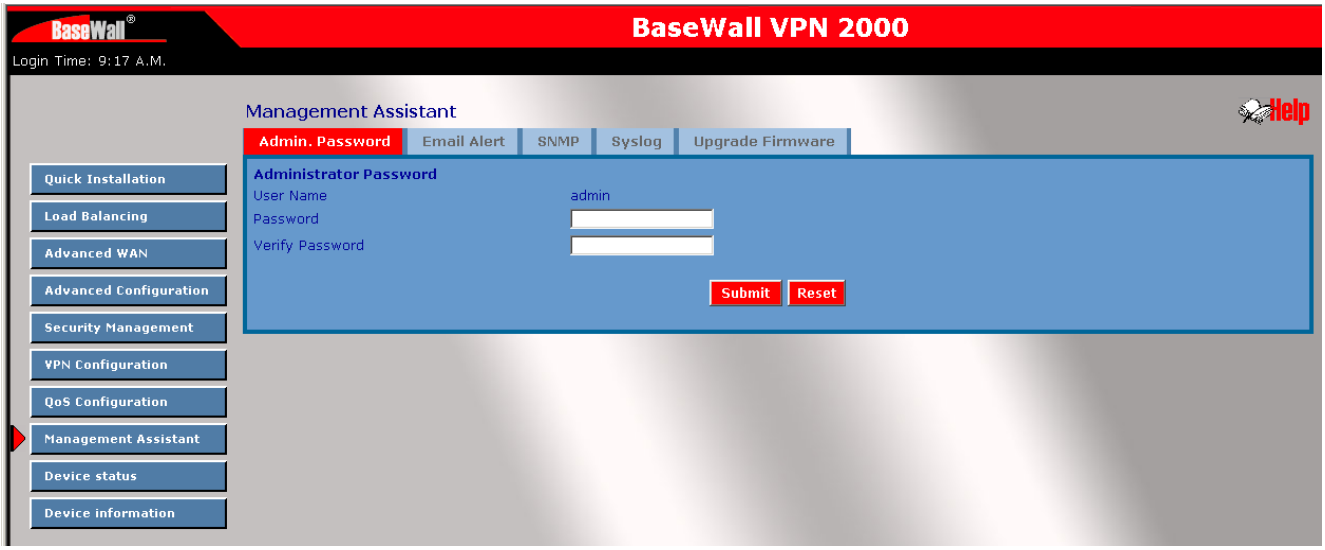


Figure 2-2: Home Screen (Admin. Setup)

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

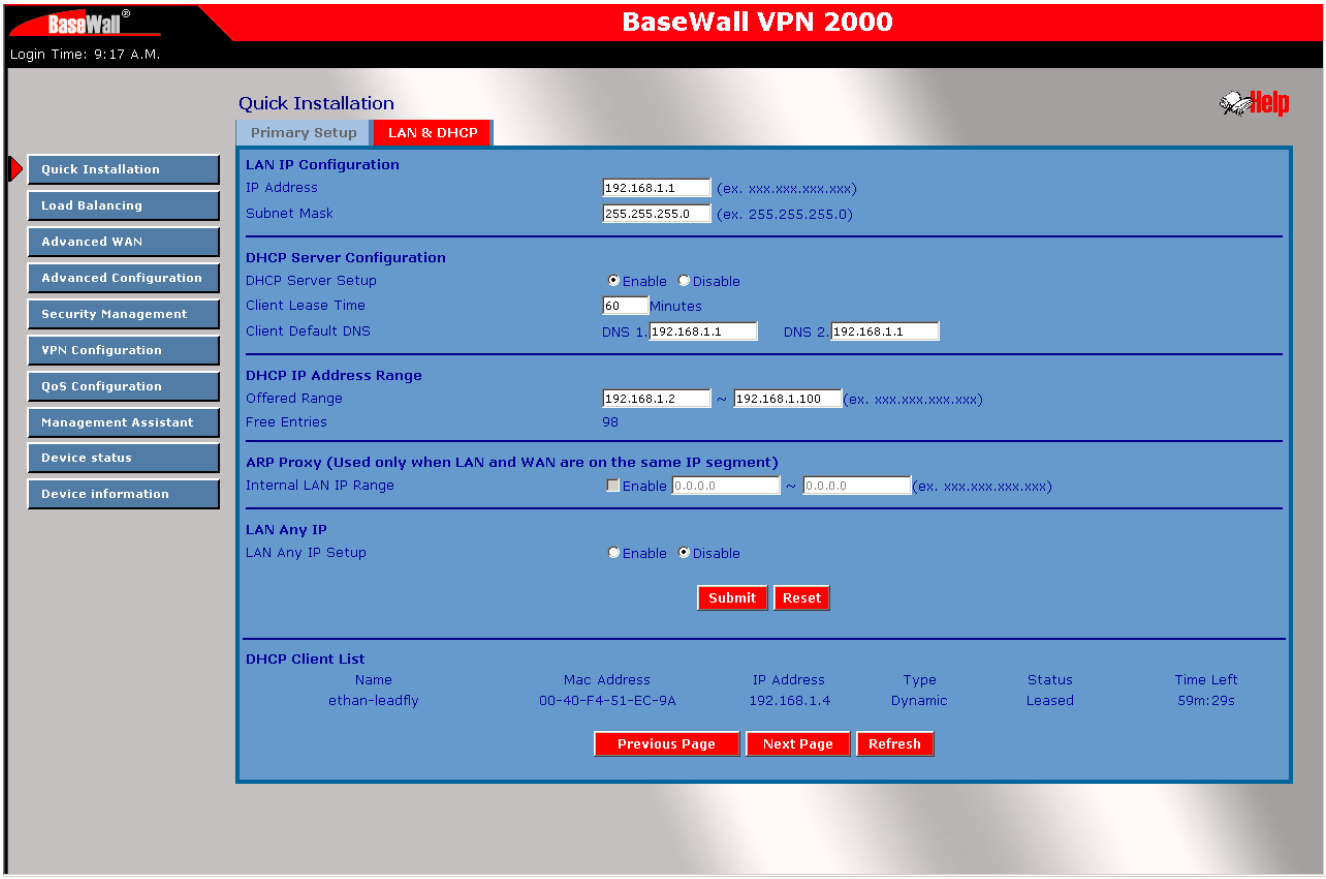


Figure 2-3: LAN & DHCP Setup

9. If your LAN already has a DHCP Server, and you wish to continue to use it, the following configuration is required.
   - The DHCP Server function in the Dual WAN VPN Firewall must be **disabled**. This setting is on the ***LAN & DHCP*** screen.
   - Your DHCP Server must be configured to provide the Dual WAN VPN Firewall LAN IP address as the "Default Gateway".
   - Your DHCP Server must provide correct DNS addresses to the PCs.
10. Ensure these settings are suitable for your LAN:
11. The default settings are suitable for many situations.
12. See the following table for details of each setting.

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

2. Installing the Dual WAN VPN Firewall in your LAN

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

3. Quick Installation - LAN & DHCP

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

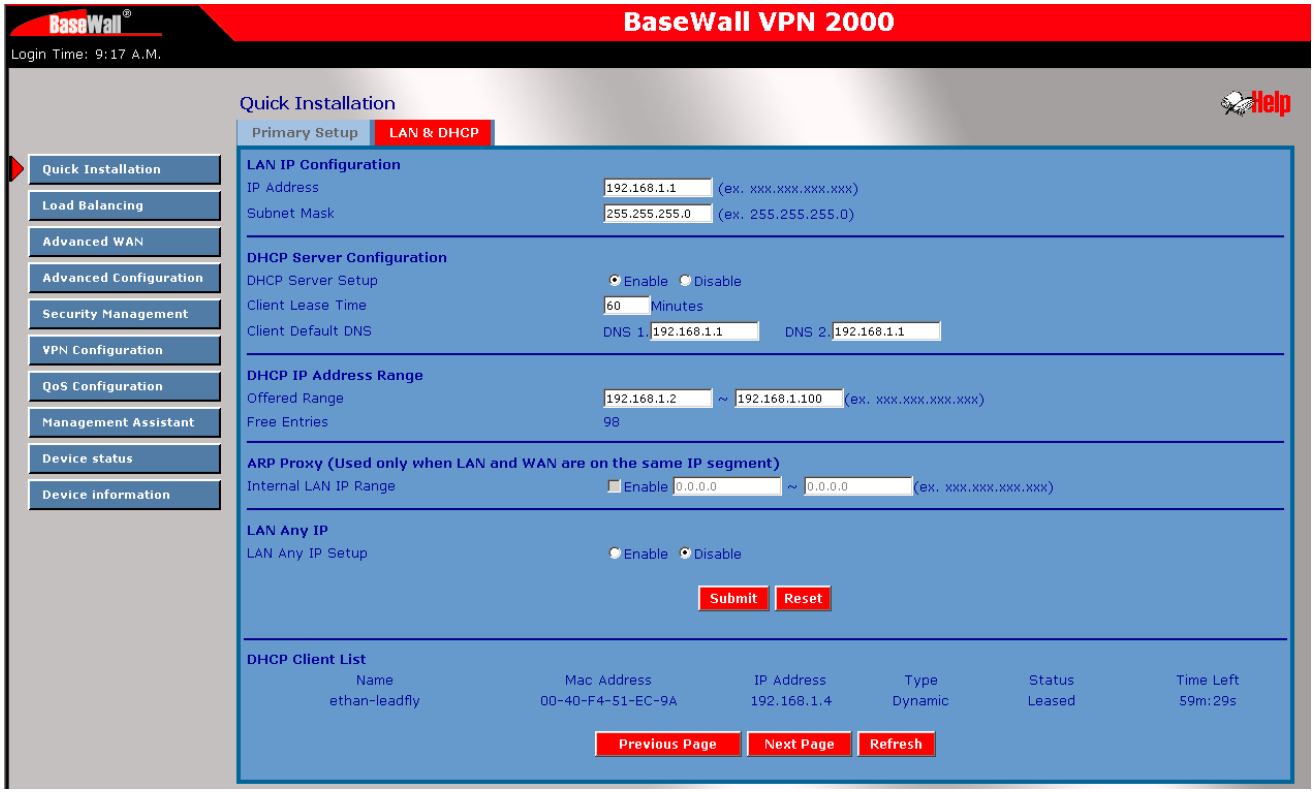


Figure 3-1: LAN & DHCP

Ensure these settings are suitable for your LAN

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

Quick installation – LAN & DHCP

LAN IP Configuration:

- **IP address -** for the Dual WAN VPN Firewall, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
- **Subnet Mask** -The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Dual WAN VPN Firewall is attached (the same value as the PCs on that LAN.

DHCP server configuration :

- **DHCP Server Setup -** If **enabled,** the Dual WAN VPN Firewall will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default and recommended value is "Enable". (Windowssystems, 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 Dual WAN VPN Firewall as the *Default Gateway*
- **Client Lease Time –** It is a certain 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 DHCPclients. This range also determines the number of DHCP clients supported.
- **Free Entries** indicates how many DHCP entries are not currently allocated, and still 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

By default is disabled. If you enable “LAN any IP”, that means no matter what static IP address hold on the client (your PC). The clients do not need to change the IP address, even though it has different IP segment than LAN segment, it still can access Internet through NAT.

DHCP Client List

This table shows the IP addresses which have been allocated by the DHCP Server function. For each address, which has been allocated, the following information is shown.

- 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.
- IP Address – The IP address allocated to this PC.
- Type – Indicates IP address to be dynamic or static.
- Status – If leased the IP address was allocated by this DHCP Server.
- Time Left – The time left before the lease expires

Quick installation - Primary setup

Connection mode

- **Enable** Select this if you have connected a broadband modem to this port.
- **Disable –** Select this if there is no broadband modem connected to this port.
- **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 address, 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 address, 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 expected by your ISP in this field. Otherwise, this should be left at the default value.

3 : Loadbalancing

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

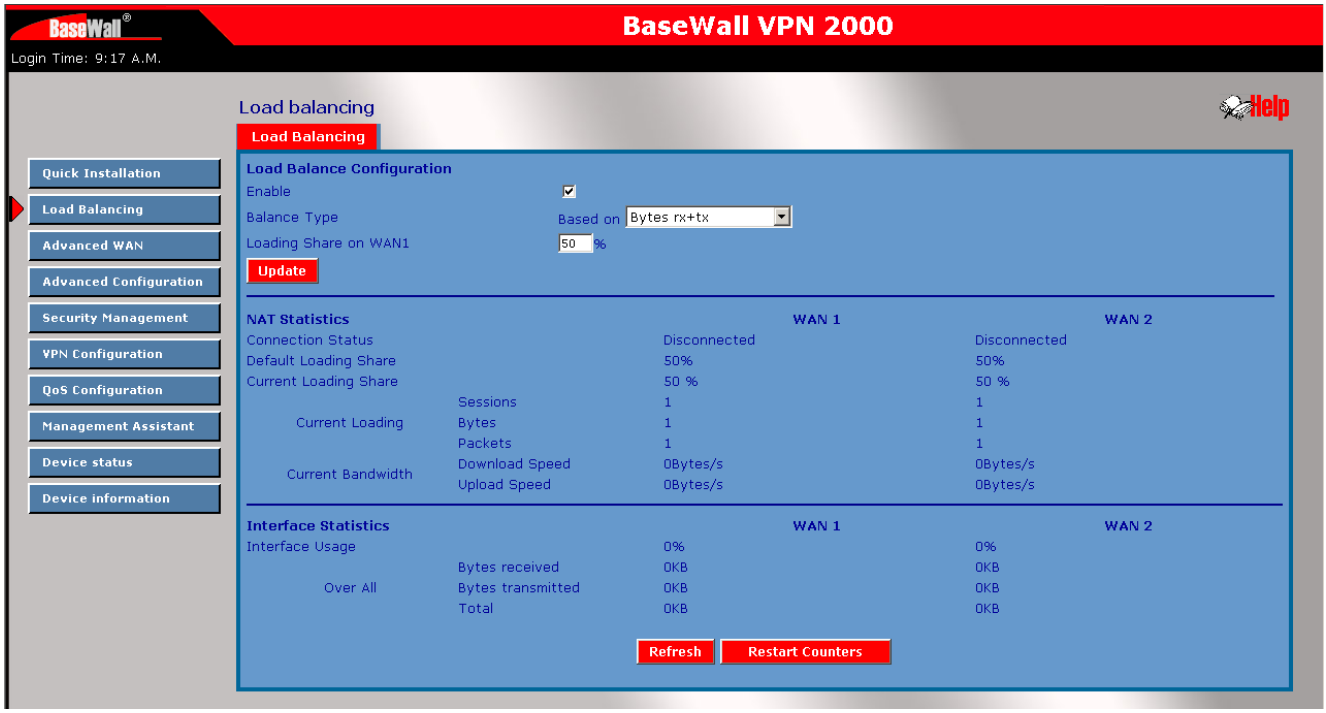


Figure 3-2: Load Balance

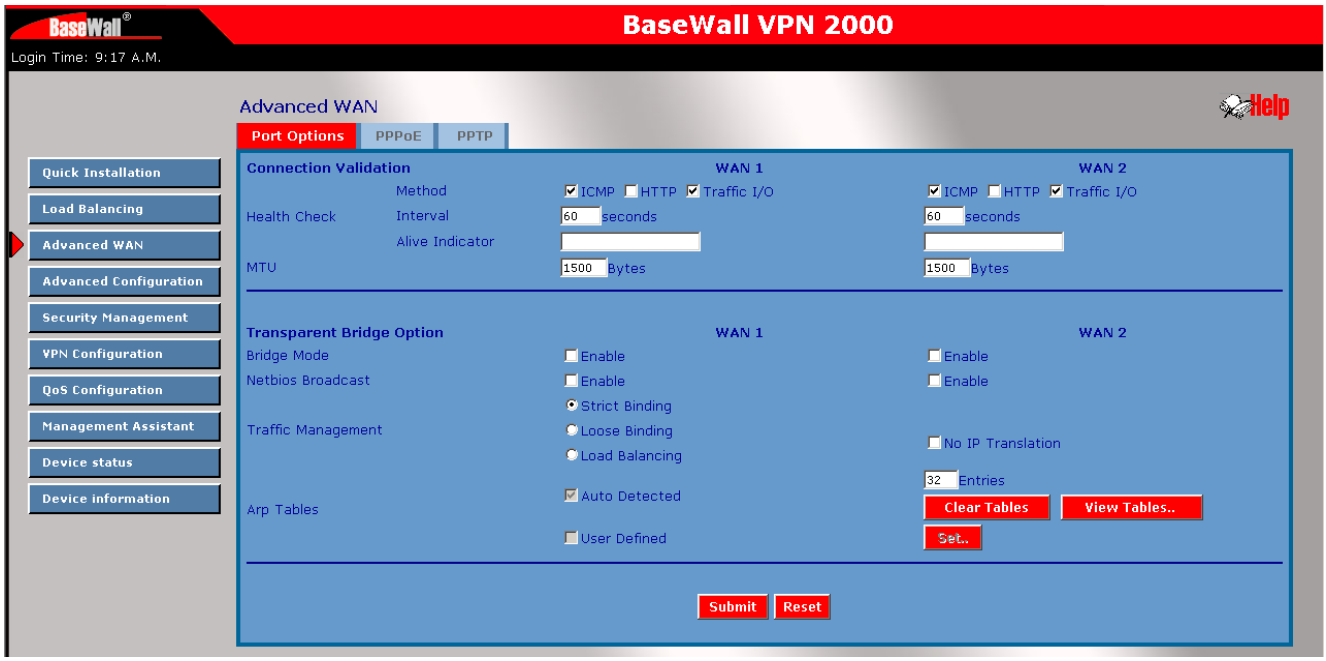
Load balancing – Load Balance

- **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



Port options

Connection validation

- **Health Check –** Disable will not do Alive Indicator Check. By default health check is enable. Health checking is performing an ICMP echo request and HTTP packets to the specific destination that could be either: 1. Name or IP Address user specified in the “Alive Indicator” input box or gateway of WAN interface if “Alive Indicator” input box is left blank.
- **Alive Indicator –** This is the IP address used to check if the WAN connection is operating. The VPN 800/2 Firewall Router 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 is used when determining 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 particular MTU, enter it here.

Transparant bridge option

- **Bridge Mode –** If set to Enable, this WAN port does not use NAT & Load Balance function when LAN/WAN IP have the real IP addresses on the same network segment.
- **NetBIOS Broadcast –** This function can allow you access files through Microsoft network neighborhood. If you enable the NetBIOS Broadcast function.

- **Traffic Management**

  Strict Binding: traffic from bridged hosts (eg. transparent to wan1) can only go through that specified wan(eg. wan1) interface.

  Loose Binding: Traffic from bridge hosts (eg. transparent to wan1) can go thru alternative wan (eg.wan2) interface when bind interface (eg. wan1) is down, it's acting like a fail over mechanism for transparent bridge mode.

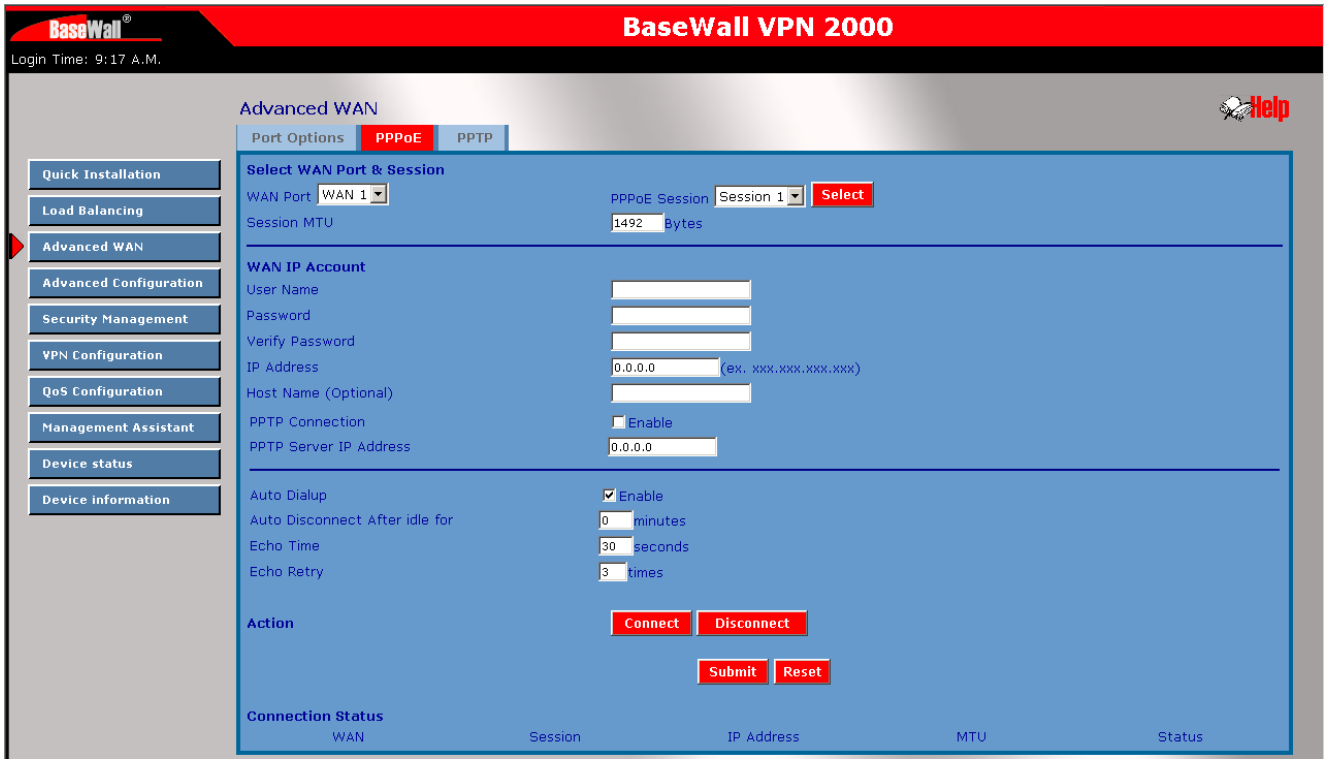
  Load Balancing: Traffic from bridge hosts (eg. transparent to wan1) can go thru either wan(eg. wan1 or wan2) interface based on loading mechanism specified in the load balance section, it's acting like as a load balancing mechanism for transparent bridge mode.

- **ARP Table** – 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 of bridge mode on each WAN port. **Clear ARP Tables** disables bridge mode on all WAN ports.

PPPoE

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



Select WAN port & Session

WAN Port – Selected WAN port only using PPPoE connection

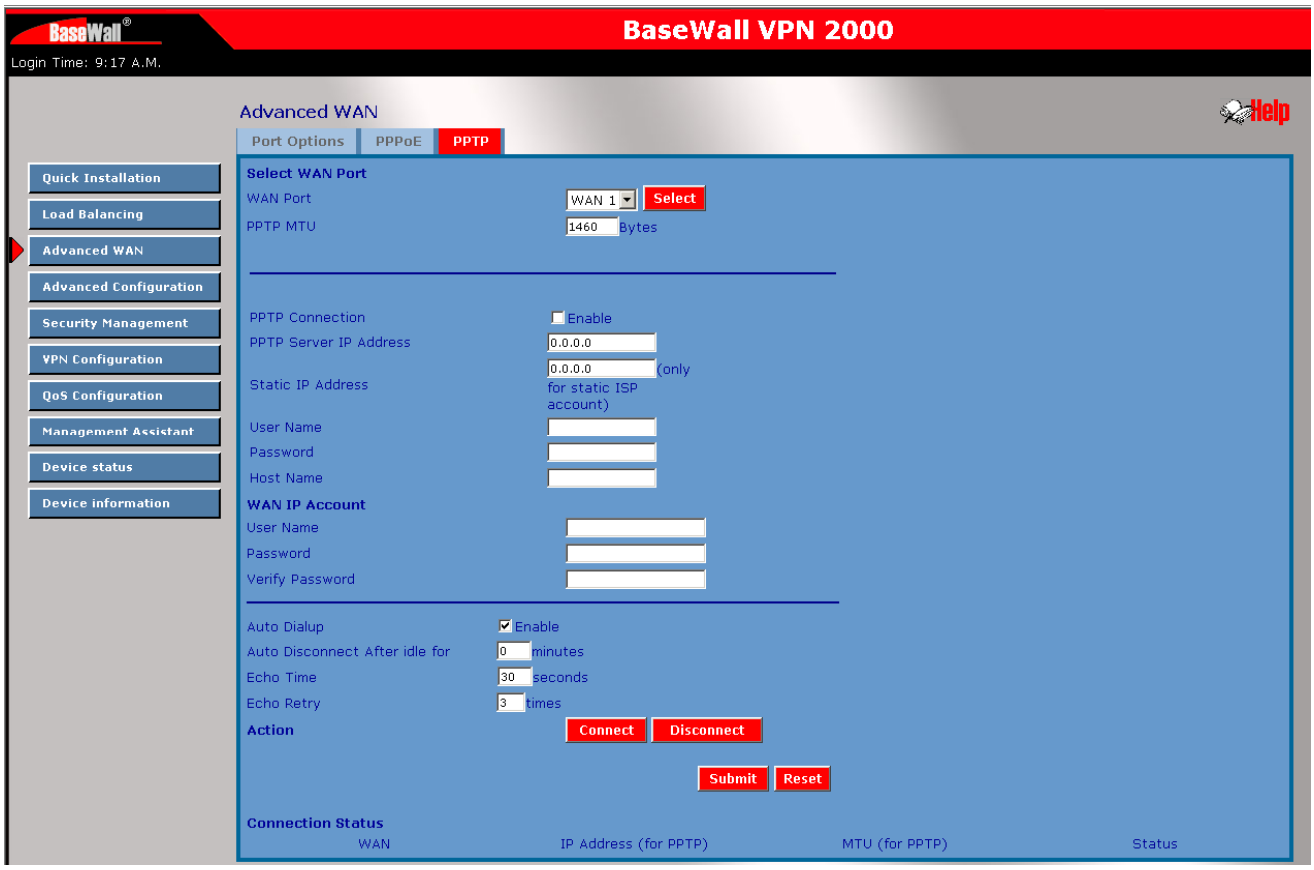
PPPoE Session – Usually ISP provides multiple floating real IP for PPPoE. Each WAN port can have up to 8 PPPoE sessions with different IP address, if your WAN port is using PPPoE connection.

PPPoE Session MTU – The Maximum Transfer Unit for PPPoE packet data. Leave it as default, unless the
ISP provides different PPPoE packets 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



Advanced WAN

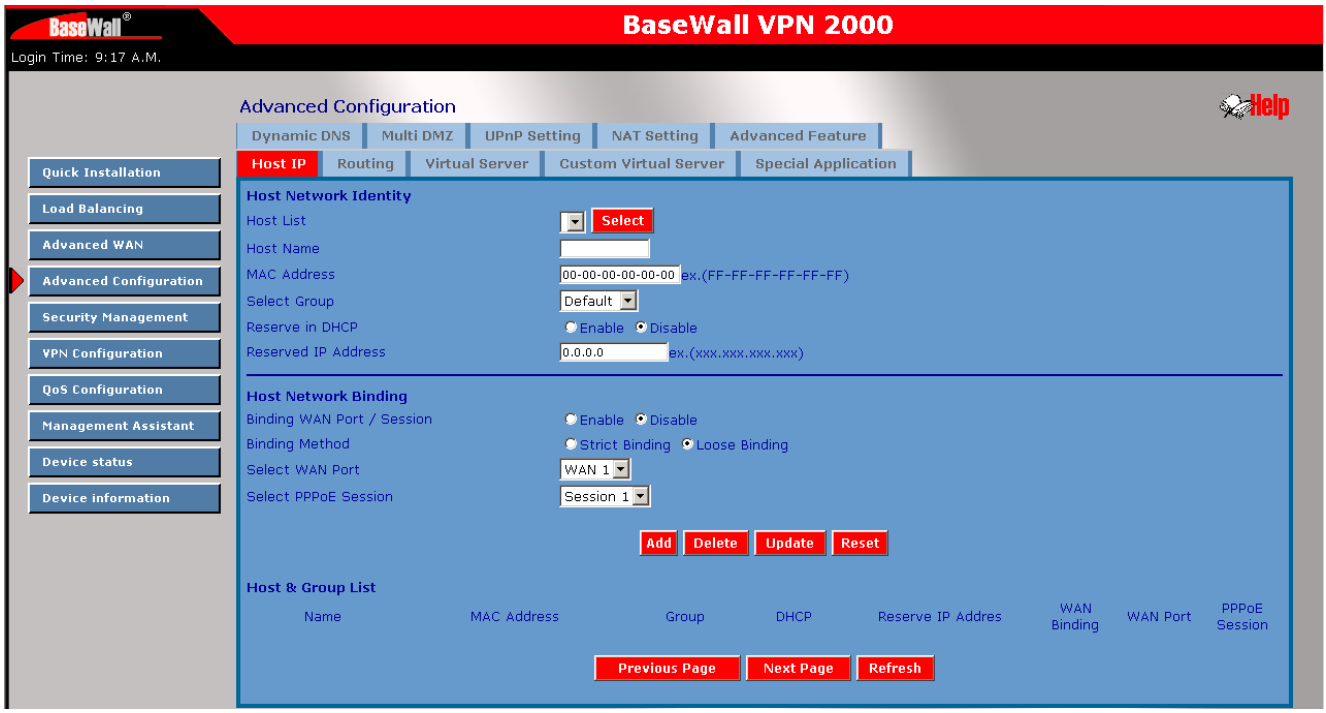
WAN Port - Select the desired WAN port (click desired WAN on Connection Status). The data of the selected port will then be displayed in the *WAN IP Account* section.
PPTP MTU – Maximum transfer unit for PPTP. The default value is 1460

WAN IP Account

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

Connection Status – This displays the current PPTP connection status.

5 : Advanced Configuration



Advanced configuration – 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 ***Block URL*** settings for different PCs. This requires that each PC is identified by using the ***Host IP*** screen. (You do not have to use the Host IP feature to apply the same ***Block URL*** settings to all PCs.)
- You wish to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "Obtain an IP address automatically") while gaining the benefits of a fixed IP address. The PC's IP address will never change, so it can be provided to 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 wish to put this host into.
- **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

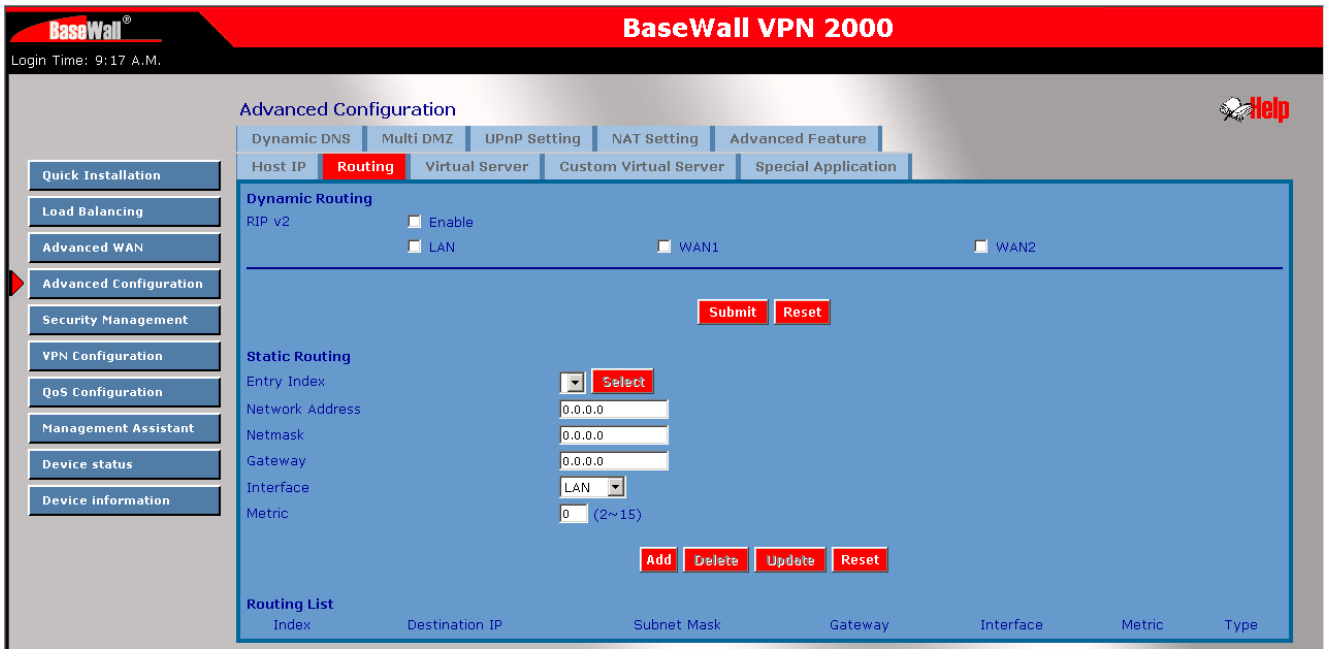
- **Binding WAN Port / Session** – Select *Enable* if you wish to associate this PC with a particular PPPoE session. All traffic for that PC will then use the selected PPPoE port and session.
- **Binding Method** – Suppose your PC is bound to WAN1 port, now you are selecting “Strict Binding”. If WAN1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

Buttons

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

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

Advanced configuration – Routing



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

- **RIP v2** – This acts as a “master” switch. If enabled, the selected WAN or LAN will run RIPv1/v2, otherwise they don’t have RIP function.

- **Interface** – LAN, WAN1 – n, is enabled, any WAN or LAN can execute RIP function.

Static routing

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

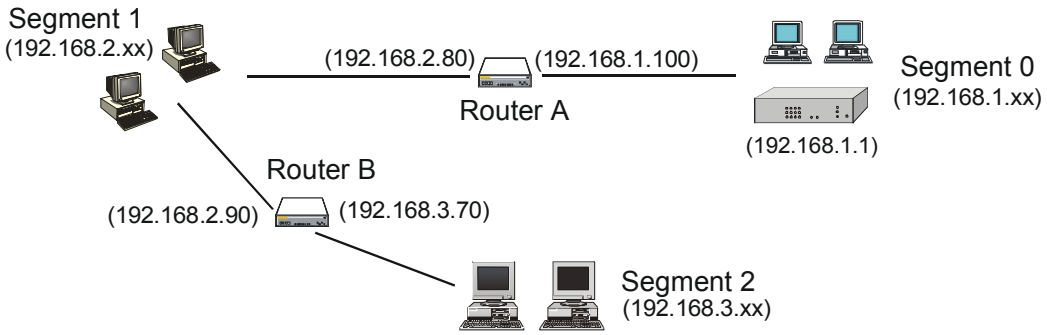
- **Netmask** –The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0
- **Gateway** – The IP Address of the Gateway or Router that the Dual WAN VPN Firewallmust use to communicate with the destination above. (NOT the router attached to the remote segment.)
- **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) to pass through to reach the remote LAN segment. The shortest path will be used.

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

Configuring Other Routers on your LAN

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

Static Routing – example



The Dual WAN VPN Firewall Gateway's Routing Table

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

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

Metric	3

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

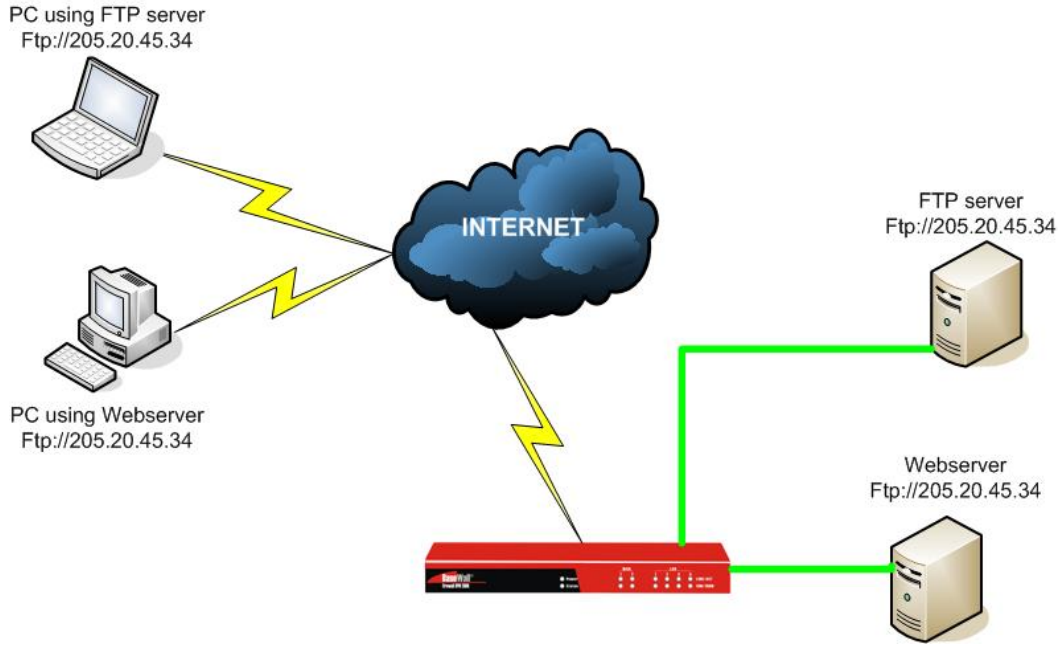
For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	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 would not be able to access a server on your LAN because:

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



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

Connecting to the Virtual Server

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

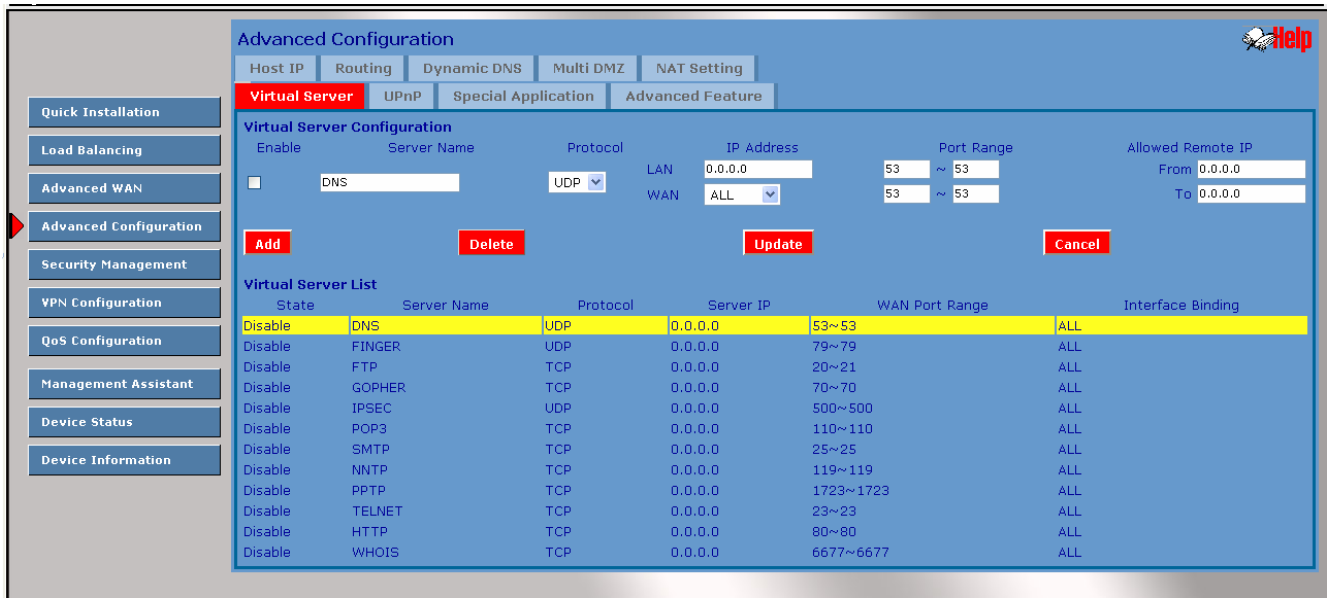
http://205.20.45.34
ftp://205.20.45.34

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

- http://my_domain_name.dyndns.org
- ftp://my_domain_name.dyndns.org

This screen allows you to define your own Server types :

Advanced configuration – virtual server



Virtual Server Configuration

- **Enable** – The enable checkbox is to Enable or Disable each Virtual server as required.
- **Server Name** – Enter a suitable name for this server. (By default, there are 12 well-known virtual servers have been list on the Custom Virtual Server List)
- **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 have 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 on any WAN ports, or even bind all WAN ports together.

- **LAN Port Range** – Enter the range of port number 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** – It allows only a range of remote side IP address to access the virtual servers. The default is 0.0.0.0 ~ 0.0.0.0, means all remote side IP address can access it.

Buttons

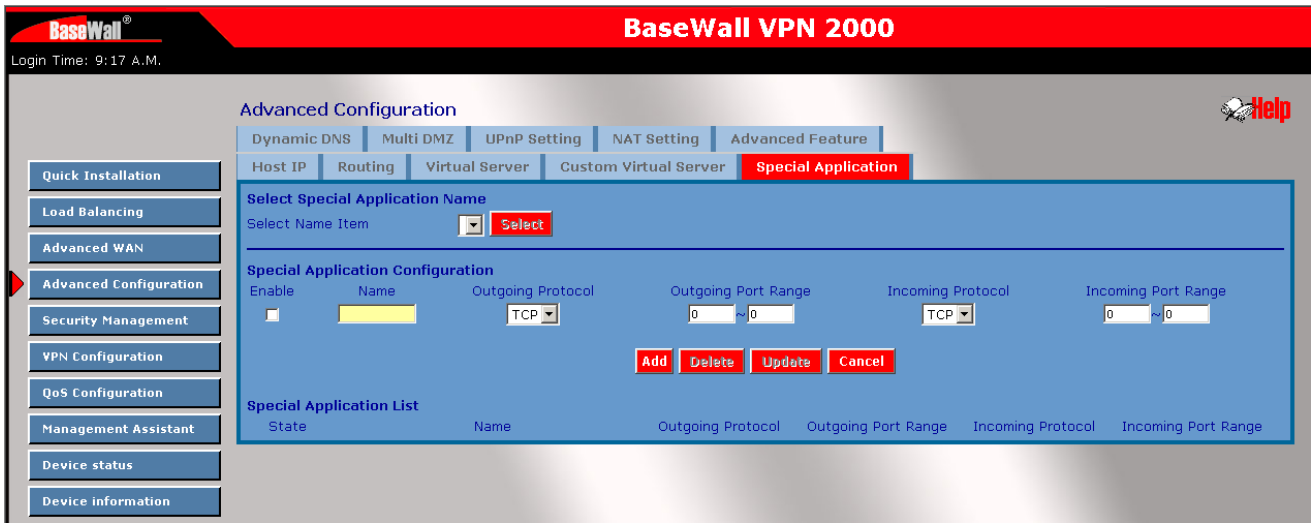
- **Add** – Create a new Virtual Server entry.

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

Virtual Server List - This table shows the details of all Custom Virtual Servers configuration data which have been defined. You can modify their configuration data by mouse clicking some row.

Advanced configuration - Special Application

If you use Internet applications which have non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the firewall in the Dual WAN VPN Firewall. In this case, you can define the application as a "Special Application" in order to make it work.
Note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint



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 shows the details of all Special Applications which are currently defined. You can modify its configuration data by mouse clicking some row.

Using a Special Application on your PC

- Once 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, there may need to be a "Time-out" period before another PC can use the same Special Application.
- If an application still cannot function correctly, try using the "DMZ" feature, if possible.

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.

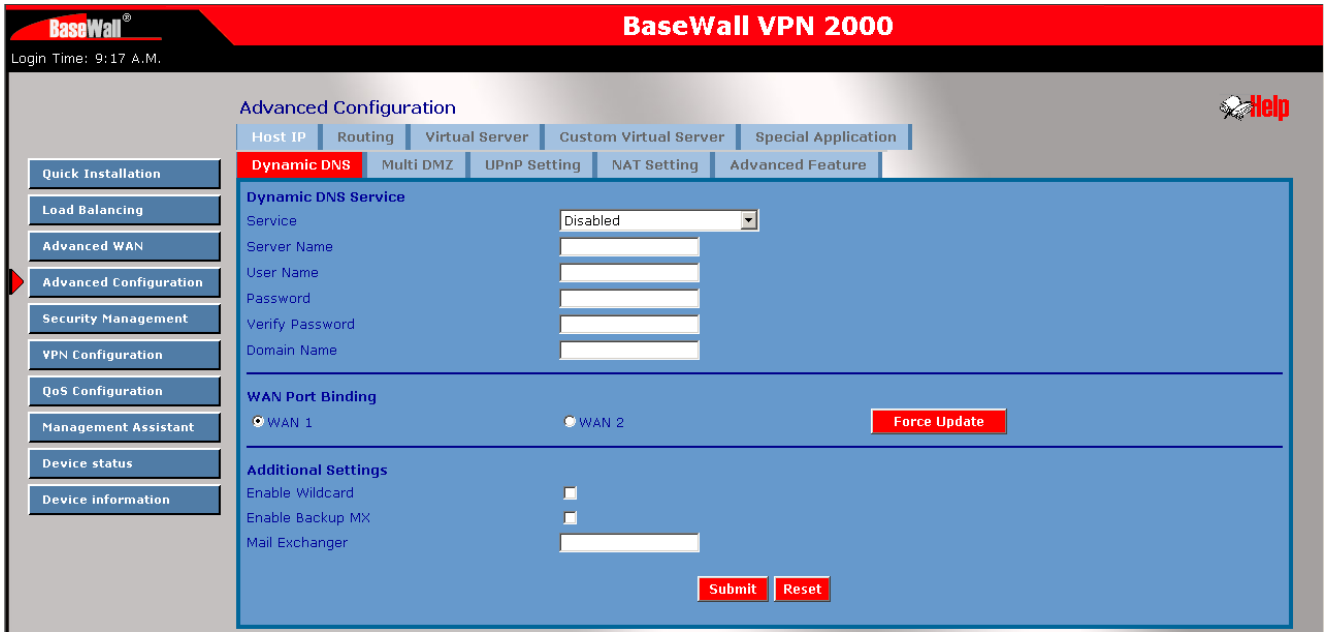
This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect to your ISP, which makes it difficult to connect to you.

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

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

To use the Dynamic DNS feature

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



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.
- **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 other provider). You must configure the *Standard Client* section of this screen.
- **3322(in China)** – This is available in China. It is similar to “DynDNS”
- **User Defined DDNS Server** – This is the user defined DDNS server. If the DDNS other than 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.

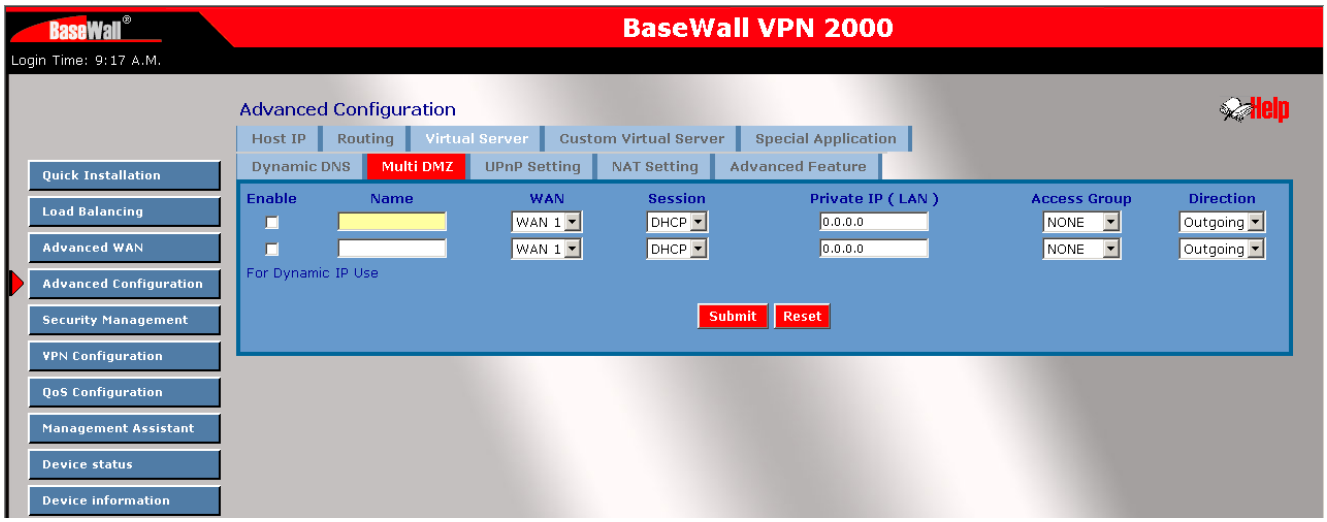
- The "Force Update" button will update your record on the Dynamic DNS Server immediately.

Advanced Configuration - Multi DMZ

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 communication 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.



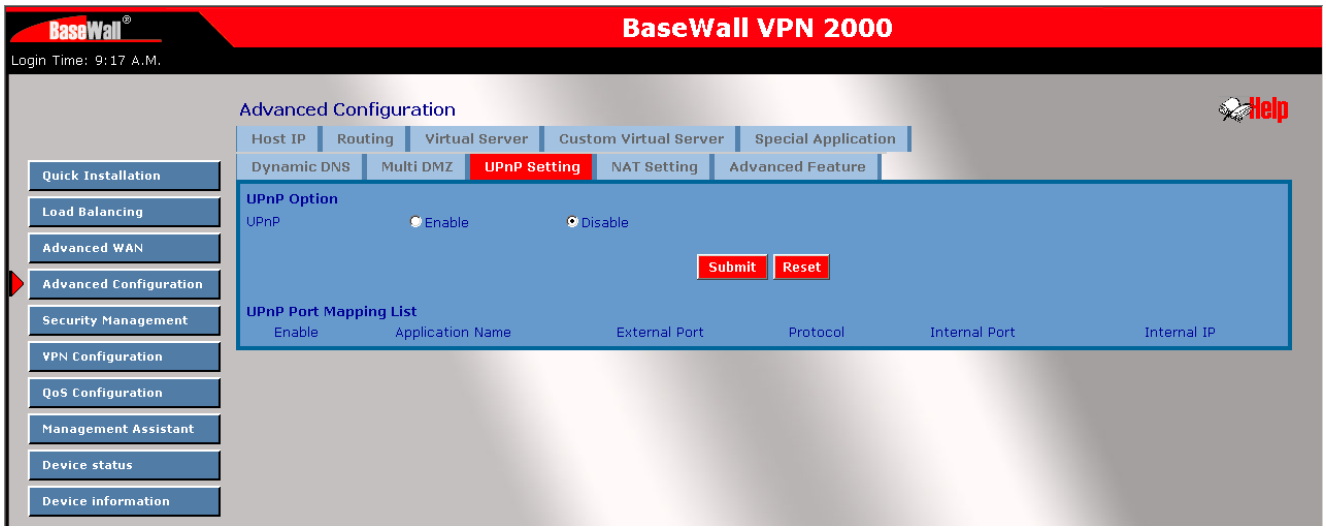
Multi DMZ

- **Enable** – Use this to enable or disable the DMZ setting, as required.
- **WAN** – Select the desired WAN port. (There are 2 WAN ports which can be available.) binding with a particular LAN host. Its connection type may change based on your WAN connection type (Static/DHCP/PPPoE).
- **Name** – Enter a name to assist you to remember this setting. This name has no effect on the operation.
- **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 decide the users to have the authority of using DMZ, by define the groups (Host IP web page)
- **Direction** –For DMZ, you can allow inbound, outbound only, or both inbound and outbound for traffic.

- **Multi DMZ List -** Multi DMZ List shows the details of all DMZ configuration data which are currently defined. You can modify its configuration data by mouse-clicking some row.

Advanced Configuration - UpnP Setup

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

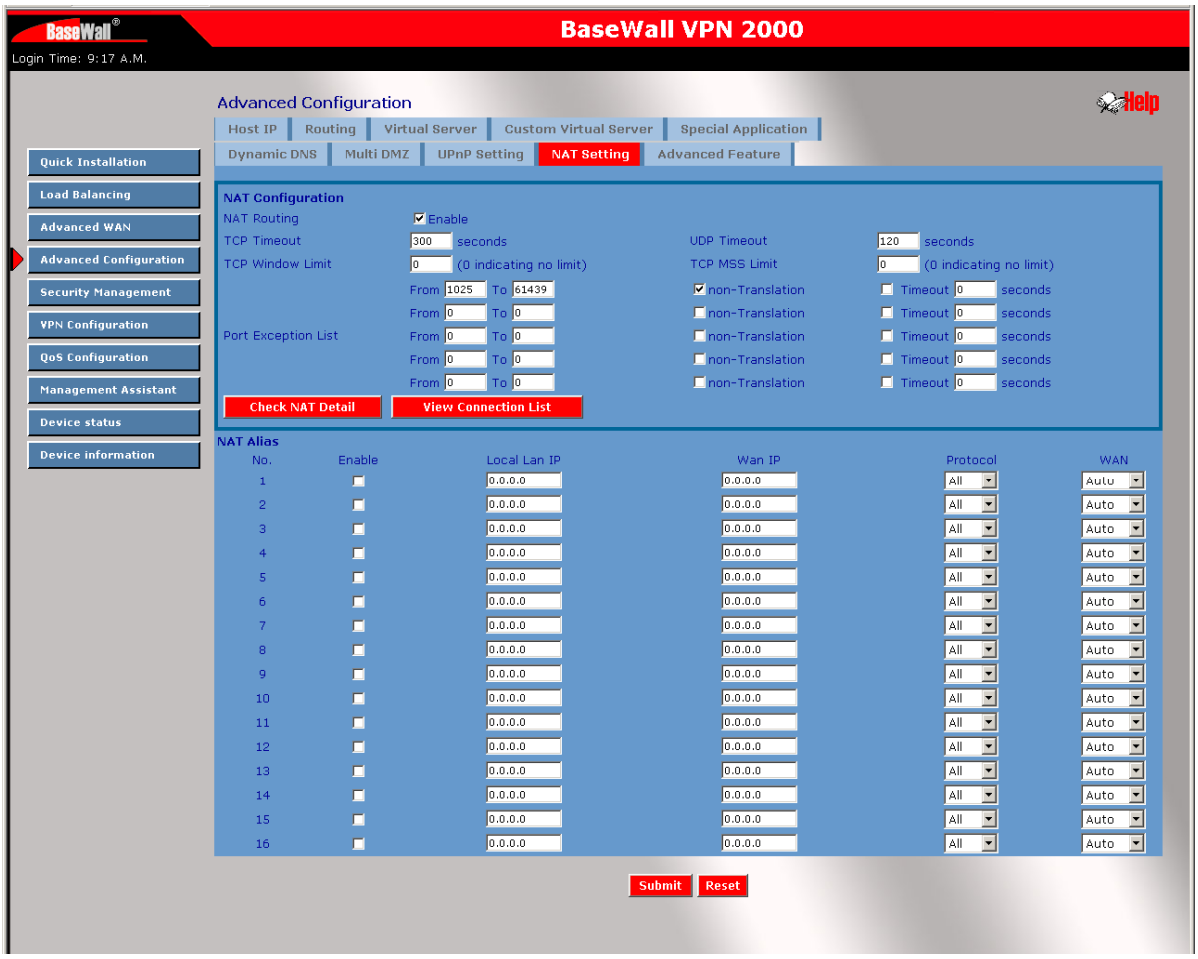


UPnP Option - If Enable UPnP, then this device will become one of the entire local network. You can find out there is an icon shown on the network neighborhood on the Window XP.

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

UPnP Port Mapping List - UPnP is enable, this table shows the details of all Custom Virtual Servers configuration data which have been defined.

Advanced Configuration – NAT Setting



NAT Configuration

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

Non Translation Port Range - If some packets whose port number cannot be translated for special applications, you must set state to “Enable” and input value in port range. Or its port cannot be translated in the specified time period, you must set Enable and some seconds in Timeout.

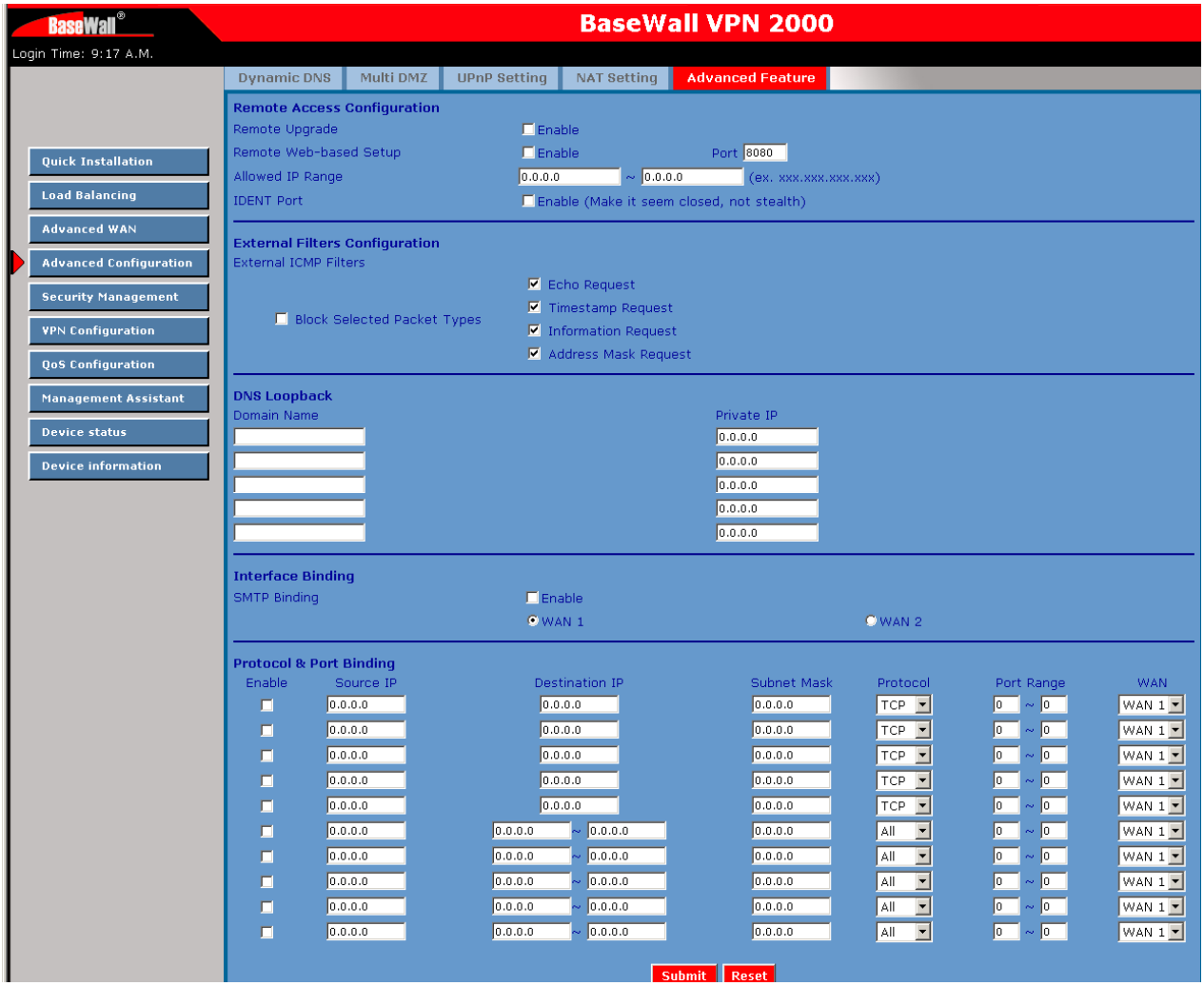
NAT alias - For each alias entry, the WAN IP acts as an alias IP of the host with Local LAN IP to Internet via the specified WAN port for the specified protocol packets, i.e. 1-1 NAT.

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

Check NAT detail - It shows all detailed information on NAT configuration data

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

Advanced Configuration – Advanced Feature



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 LAN and their domain names have already been registered on public DNS. To avoid DNS loop back problem, please enter 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 below will be used for all outgoing SMTP traffic. If not enabled, either WAN port will be used.
- **WAN** – Select the desired WAN port to be bound.

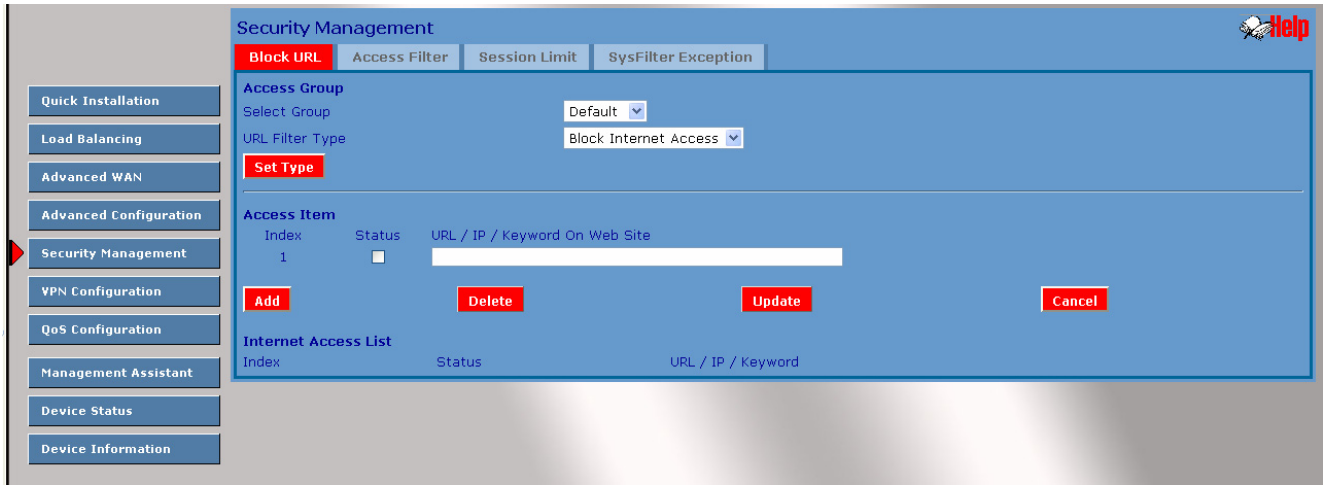
Protocol and Port Bindings - Use these settings if you wish to ensure that particular traffic is sent by a particular WAN port, and thereby a particular ISP account.

- **Enable** - Enable or disable each item as require
- **Source IP** - IP address of source which packets are sent from.
- **Destination IP** – IP address of destination which packets are sent to.
- **Subnet Mask** – With subnet mask other than 255.255.255.255, you can make an IP sub-network as 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 which are currently defined. You can modify them by mouse clicking some row.

6 – Security Management

Security Management – Block URL



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.

- In operation, every URL is searched to see if it matches or contains any of the URL 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 on that IP address.

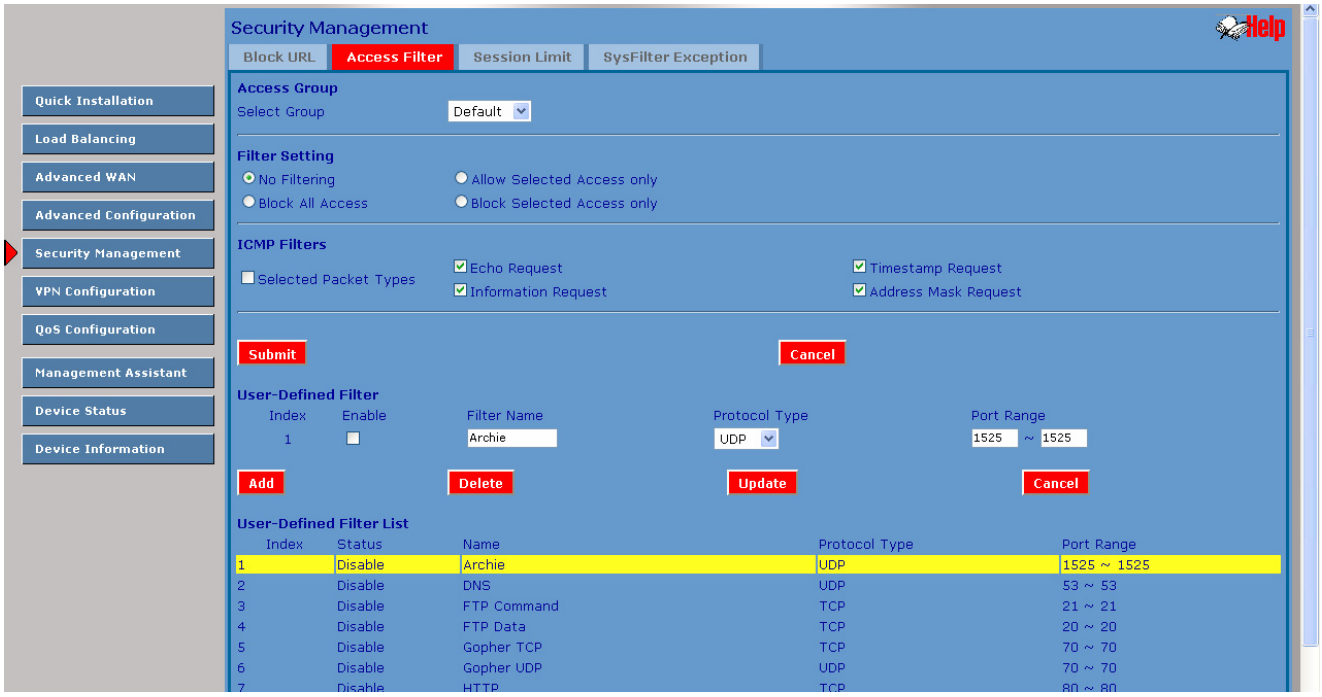
Access Group - This allows you to have different blocking rules for different Groups of PCs.

- 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 on 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 Active ,all internet access is allowed, there are no restrictions in place. When you add a rule here this will prohibit access of the website to which this rule is applied.

Allow Internet Access – when this setting is active, all internet is prohibited by default. An entry here will enable access to that specific site, while the rest is still blocked.

Security Management – Access Filter



The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users.

- 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 have different access rights for different Groups of PCs.

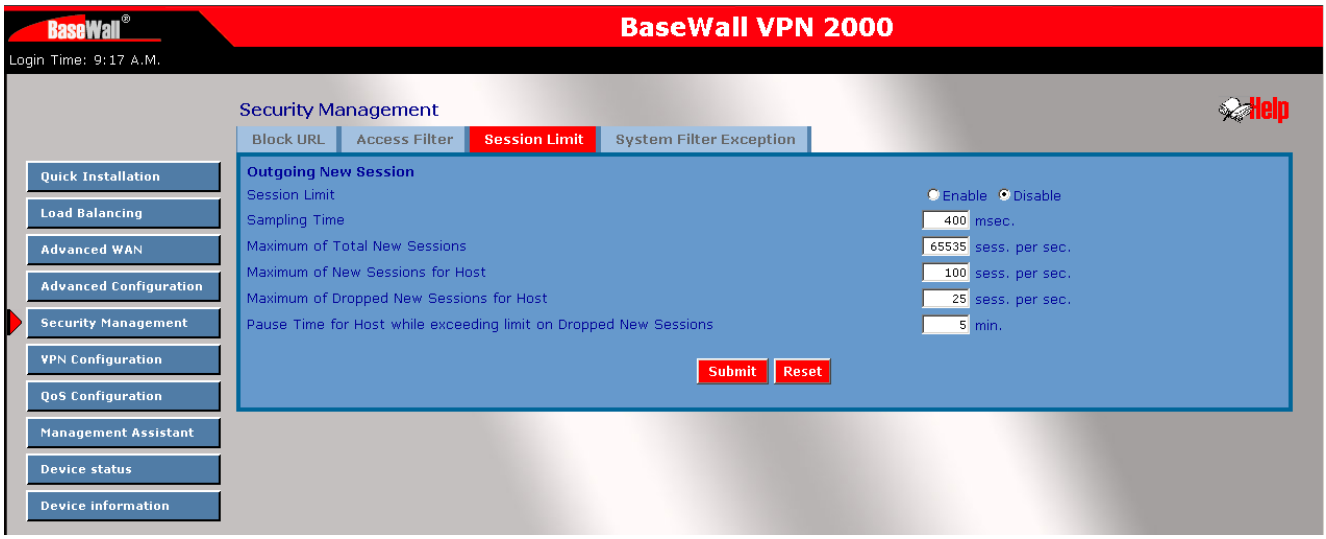
- If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the ***Host IP*** screen.
- If you wish to apply different restrictions on different Groups, select the desired Group. The screen will update data for the selected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

ICMP – Filters - If you enable ICMP Filter that means it will block ICMP request packet type specified by users from local host to 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 used you wish to block. If only a single port is required, enter it in both fields.

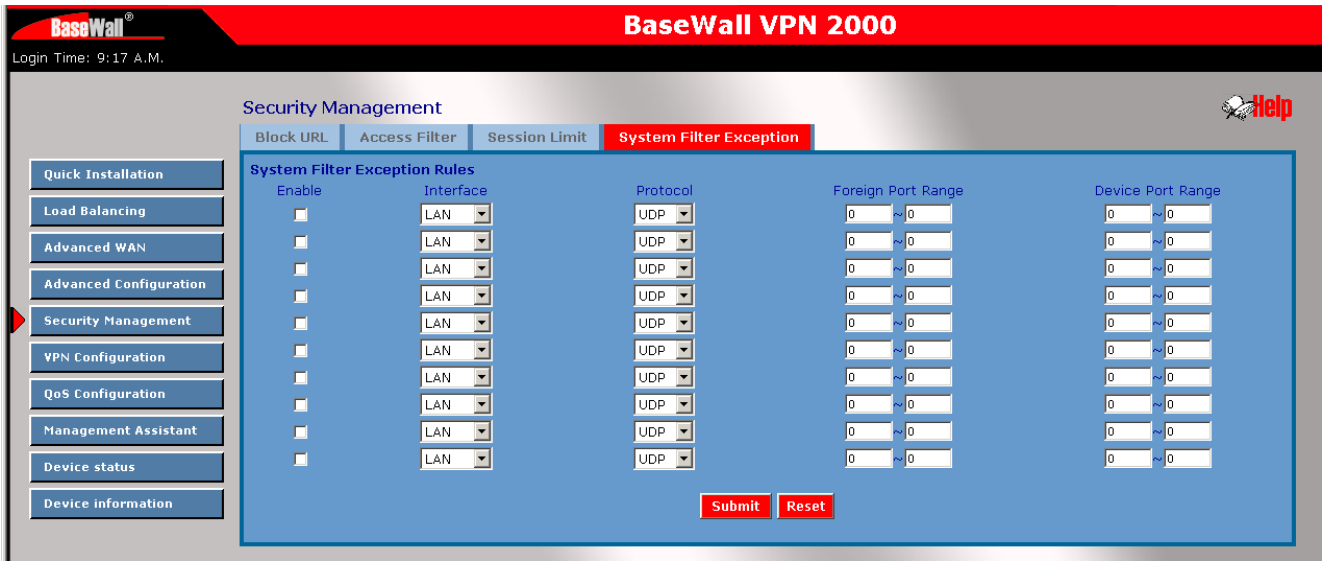
Security Management - Session Limit



This new feature allows to drop the new sessions from both WAN and LAN side. If 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 those new sessions recently occurred is counted in the sampling time to check. (Default is 400 mil-sec)
- **Maximum total of new sessions -** The maximum total number of new sessions in the system which 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 which 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 could be served by system when the number of dropped new sessions exceeds the defined Maximum. (Default is 5 minutes)

Security Management – System Filter Exeption



Sysfilter exeption - System Filter Exception – It will reject every packet with unrecognized port to avoid port scan program from hackers but this also incurs problems on situation that some servers (e.g. SMTP server port 113) or client from WAN need to response packet to justify aliveness of their communication peers.

- **Enable** – If check box is marked, it will enable System Filter Exception
- **Interface** – You can select LAN, any WAN port or ALL interfaces which a packet comes from.
- **Protocol** – The packet type which will be directly processed from above interface by this device.
- **Foreign Port Range** – Enter the beginning and end of the foreign port range used by the traffic you wish to configure. If only a single port is used, 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. VPN establishes a private network that can send data securely between two networks. We call this creating a “tunnel”. A VPN tunnel connects the two PCs or networks.

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

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

1. If the remote end is network, the two-endpoint network 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 subnet mask of 255.255.255.255

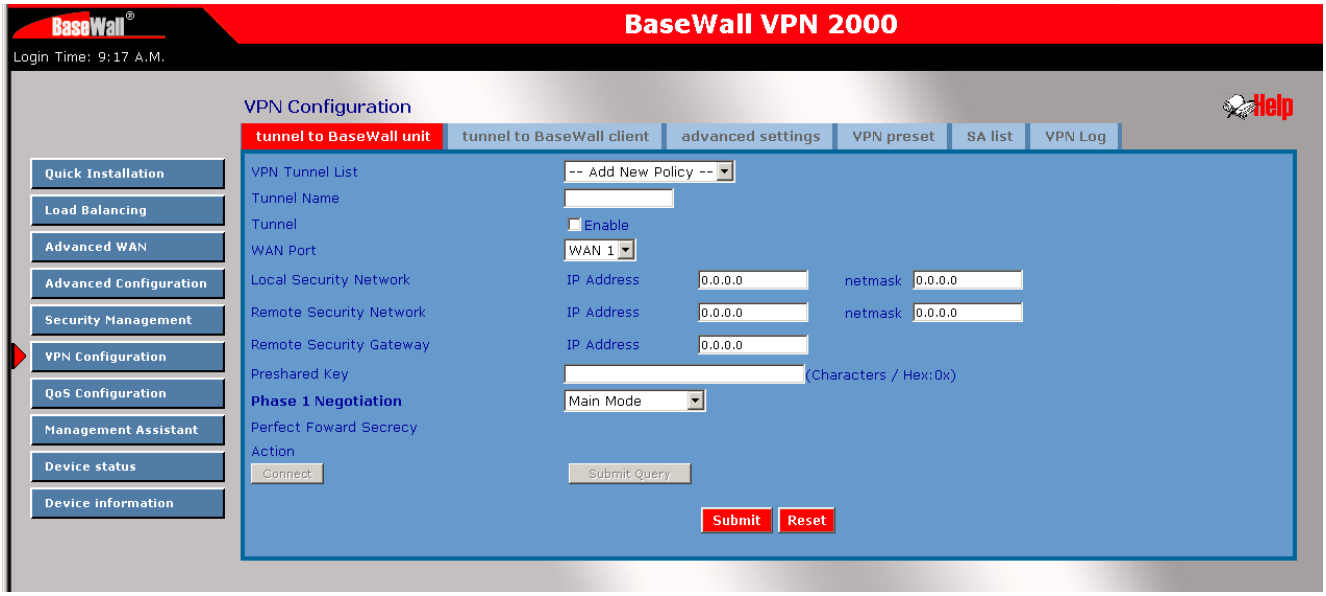
2. Will you be using the Internet Key Exchange (IKE) setup, or Manual Keying, in which you must specify each phase of the connection. IKE has become the standard for automatic keying.

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

The settings that you have to make when connecting to another BaseWall product are kept 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 a very secure encryption and authentication so your data will be safely transported via the IPSec tunnel.

There are two basic settings :

Tunnel to BaseWall Unit - This describes how to setup an IPSec tunnel to a BaseWall VPN 1000,2000,3000,4000,5000 and 6000.



VPN Configuration – Tunnel to Basewall Unit

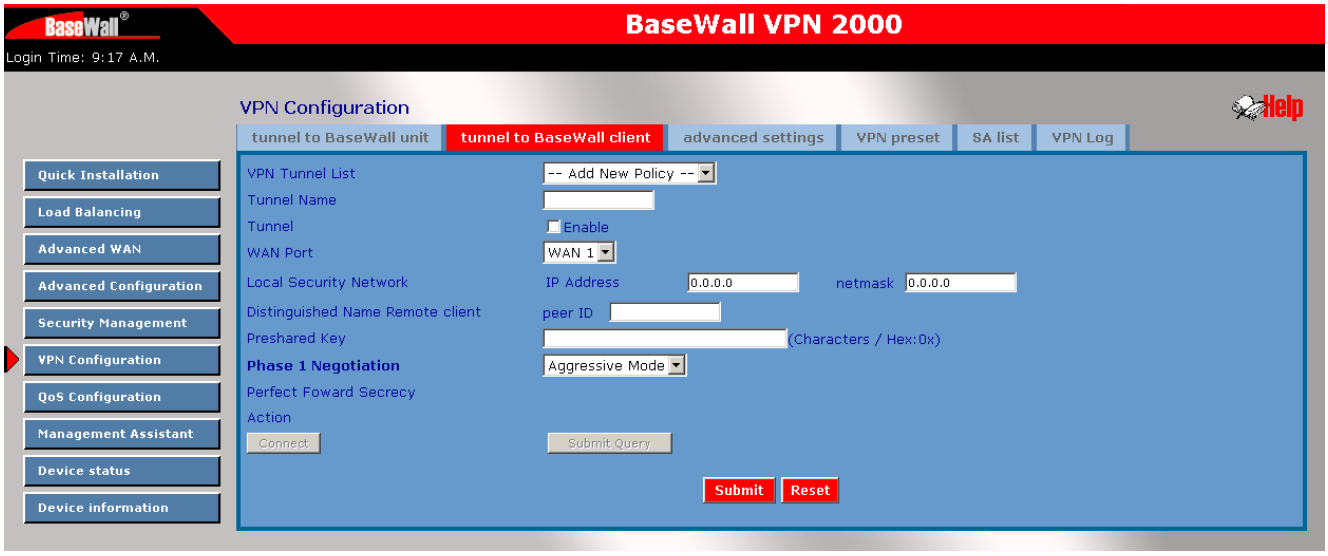
- **VPN Tunnel List–** here you can add a new tunnel or change an existing one from the list The router can setup a maximum of 50 tunnels.
- **Tunnel Name–** In order to distinguish the tunnels, you have to give the “Tunnel” a name..
- **Tunnel –** Only after you enable the tunnel check box, the tunnel 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 hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN LAN-to-LAN connection.
- **Remote Security Network–** These entries identify the private network on the remote peer VPN router whose 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 connection
- **Remote Security Gateway –** You can select the remote side IP address (WAN IP address) as your remote side 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 BaseWall Client



Tunnel to BaseWall Client – This describes an IPSec tunnel from a the VPN 3000 to the BaseWall Client Software.

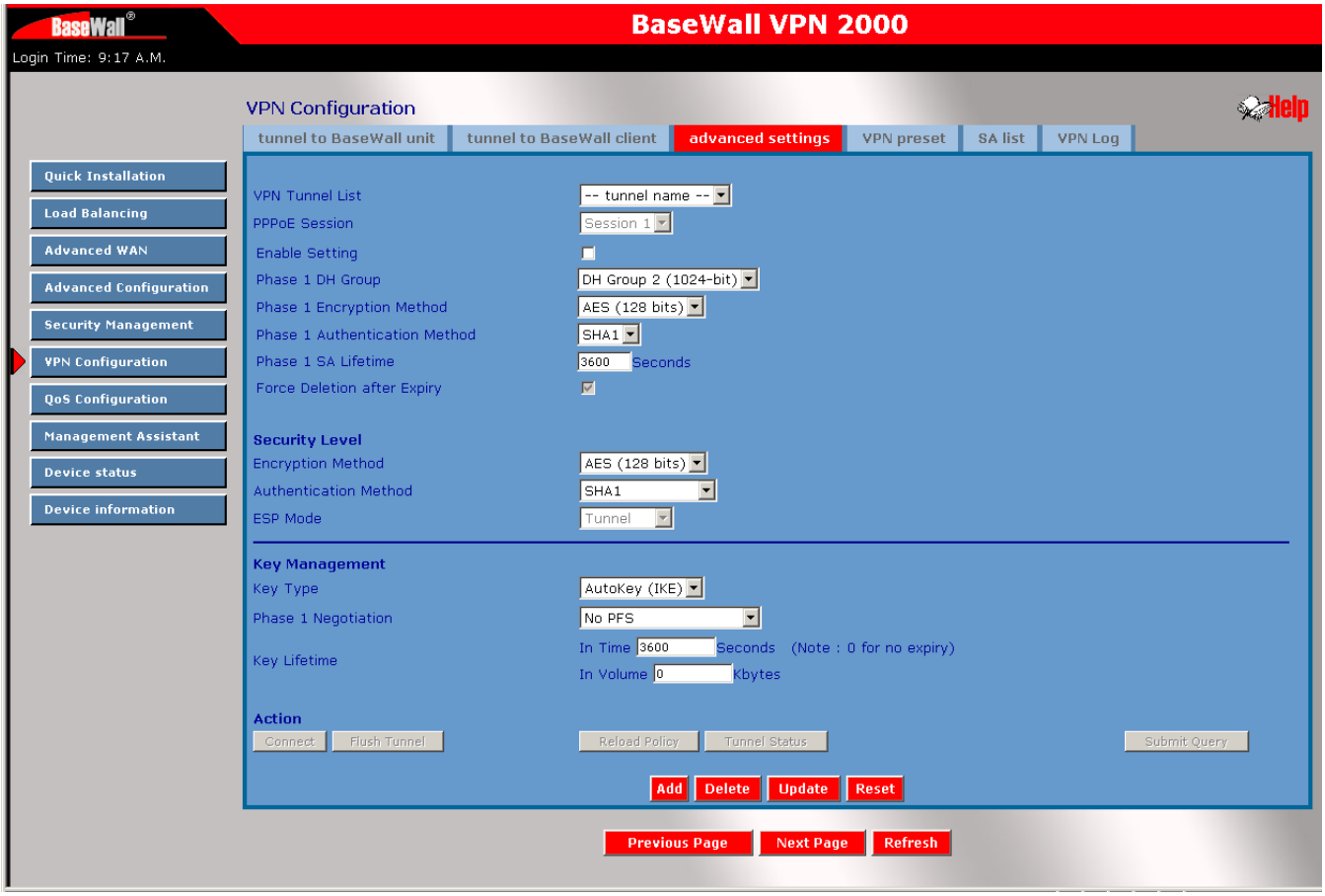
- **VPN Tunnel List–** here you can add a new tunnel or change an existing one from the list The router can setup a maximum of 50 tunnels
- **Tunnel Name–** In order to distinguish the tunnels, you have to give the “Tunnel” a name..
- **Tunnel –** Only after you enable the tunnel check box, the tunnel 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 hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN LAN-to-LAN connection.
- **Distinguished name remote client –** Use for example an email address pete@BaseWall.com
- **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 – Advanced settings

When you use the **tunnel to BaseWall unit** or **tunnel to BaseWall client** configurations you don't need to use the **Advanced Settings.** Only when you want to make adjustments for a IPSec tunnel to a third party unit you can choose here settings that may be required.



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

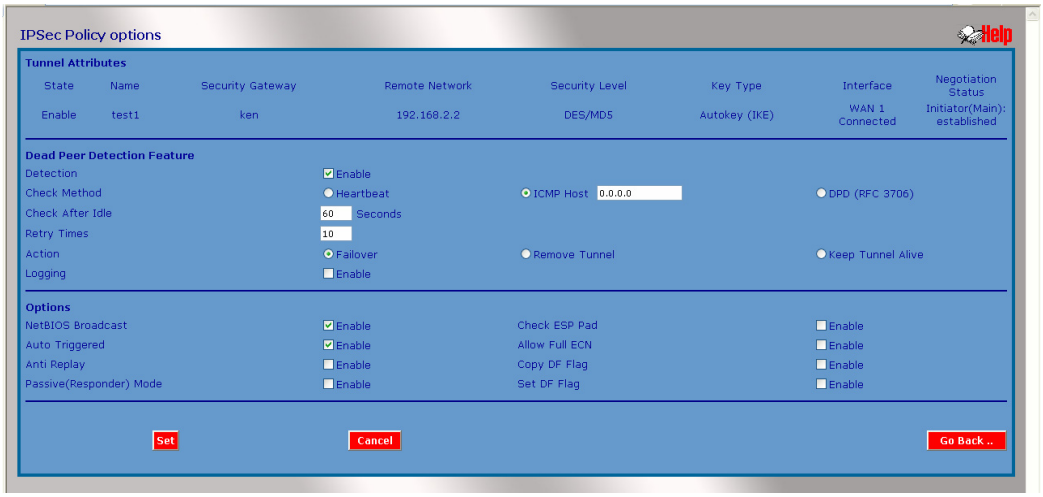
Security level

- **Encryption Method –** It 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 –** It specifies the packets authentication mechanism to use. Packets authentication proves that data comes from source you think it comes from. There are three authentications available. MD5,
  SHA1 and SHA2.

Key management

- **Key – Key Type:** there are two key types (manual key and auto key) available for the key exchange management.
- **Manual Key:** If manual key is selected, no key negotiation is needed.
- **AutoKey (IKE)-** There are two types of operation modes 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 enable, IKE phase 2 negotiation will generate new key material for IP traffic encryption & authentication. Preshared Key – This field is to authenticate the remote IKE peer.
- **Key Lifetime-** This is specified the lifetime of the IKE generated Key. If the time expires or data is passed over this volumn, a new key will be renegotiated, By default, 0 is for no limit.

IPSec policy options



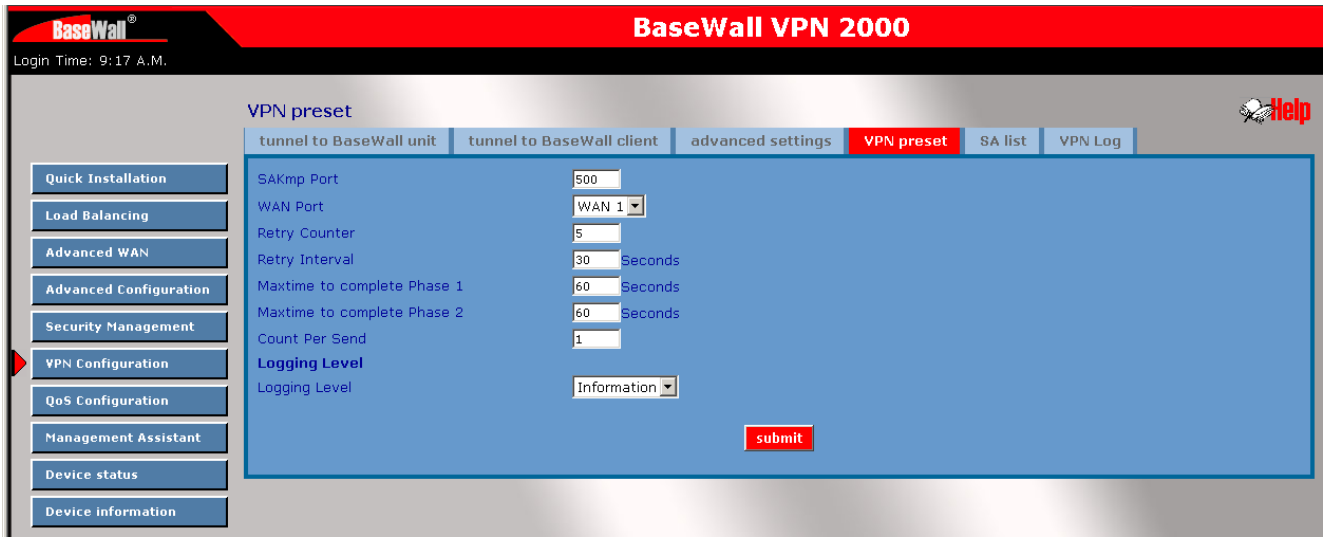
- **Tunnel Attribute –** The attributes for the tunnel that you just setup
- **Dead Peer Detection -** If you like to utilize one of the wan port as a backup or plan the failover function, you can enable Dead Peer Detection function.
- **Check Method –** You can either choose ICMP, Heartbeat or DPD protocol. This will detect if the remote site VPN tunnel is alive or not.

Options :

- **NetBIOS Broadcast-** This is used to forward NetBIOS broadcast across the Internet.
- **Auto Trigger**–This is usefull to keep up the IPSec connection tunnel. It can be re-established immediately, if a connection is dropped and detected.
- **Anti Replay –** It ensures to keep track of 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 enable 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 newly written, 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.

VPN configuration – VPN preset



- **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 for.

- **Retry Counter** – It indicates how many times the process of Phase 1 will be restarted if it's unsuccessful. There is a 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 expired, 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 expired, 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 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 level of messages: None, Critical, Error, Warning, Information, Debug.

VPN Configuration – SA List

VPN configuration – SA list

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

VPN Configuration – VPN Log

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

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

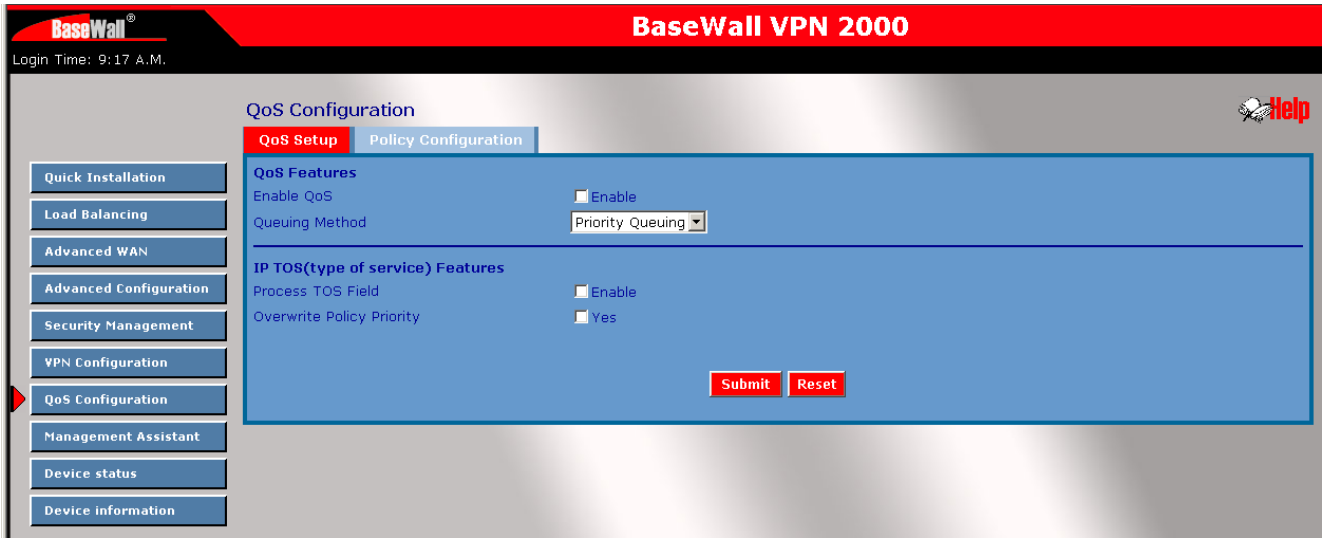
Undefined messages

- **Module** – Which module is responsible for this message to be sent in IPSec architecture.
- **Messages** – this displays some information that describes what event happened.

8: QoS Configuration

QoS Configuration – QoS Setup

The Dual WAN VPN Firewall provides QoS, which supports the high quality of network service. Because it will classify outgoing packets based on some policies defined by users, it can make some real-time applications to get better response or performance.



QoS Features :

- **Enable QoS –** This will allow users enable QoS function.

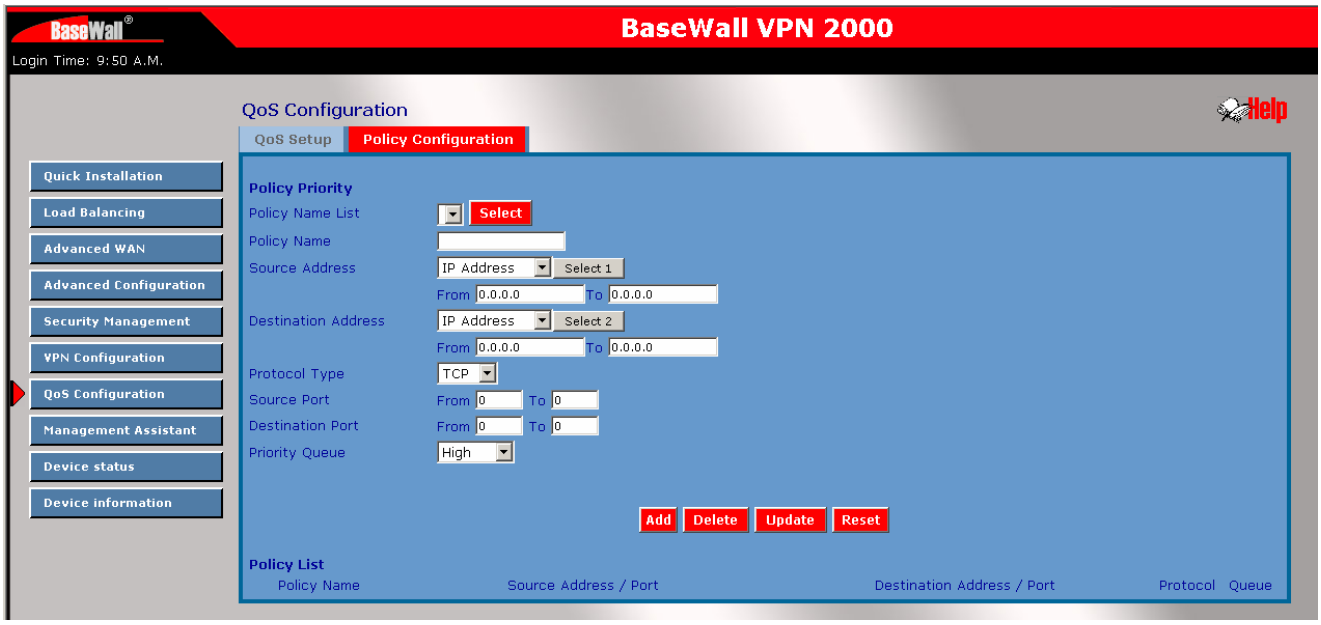
- **Queuing Method –** The methods that how you manage your queue." Priority Queuing is one of the first queuing variations to be widely implemented.

IP TOS (Type of Service Feature)

- **Process TOS Field –** An 8-bit field in the IP Packet header designed to contain values indicating how each packet should be handled in the network. If you choose "enable" it will enable this function to process this IP Type of service field.

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

QoS Configuration – QoS Setup



QoS Setup

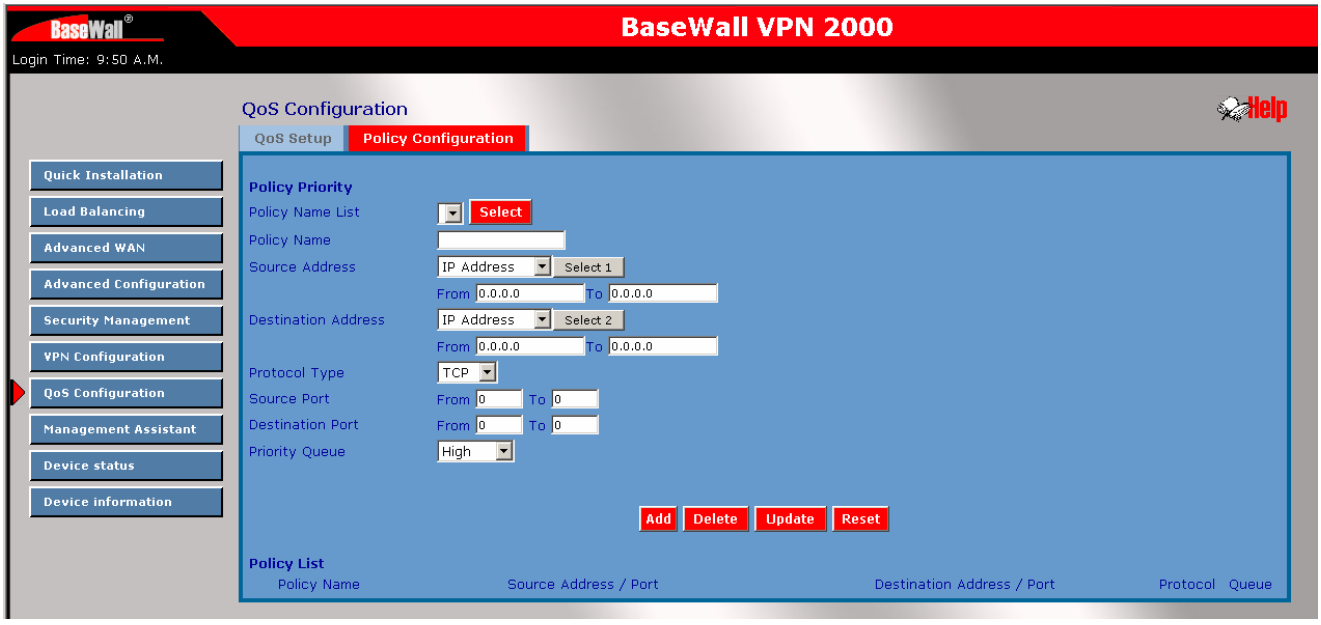
QoS Feature

- **Enable QoS –** This will allow users enable QoS function
- **Queuing Method -** The methods that how you manage your queue. ”Priority queuing. It is one of the first queuing variations to be wildly 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 handled in the network. Enable will enable this function to process IP Type of Service field.
- **Overwrite policy priority –** Choose “yes” to set the priority of TOS field in IP packet to overwrite the priority defined in policy configuration
-

QoS Configuration – Policy Configuration

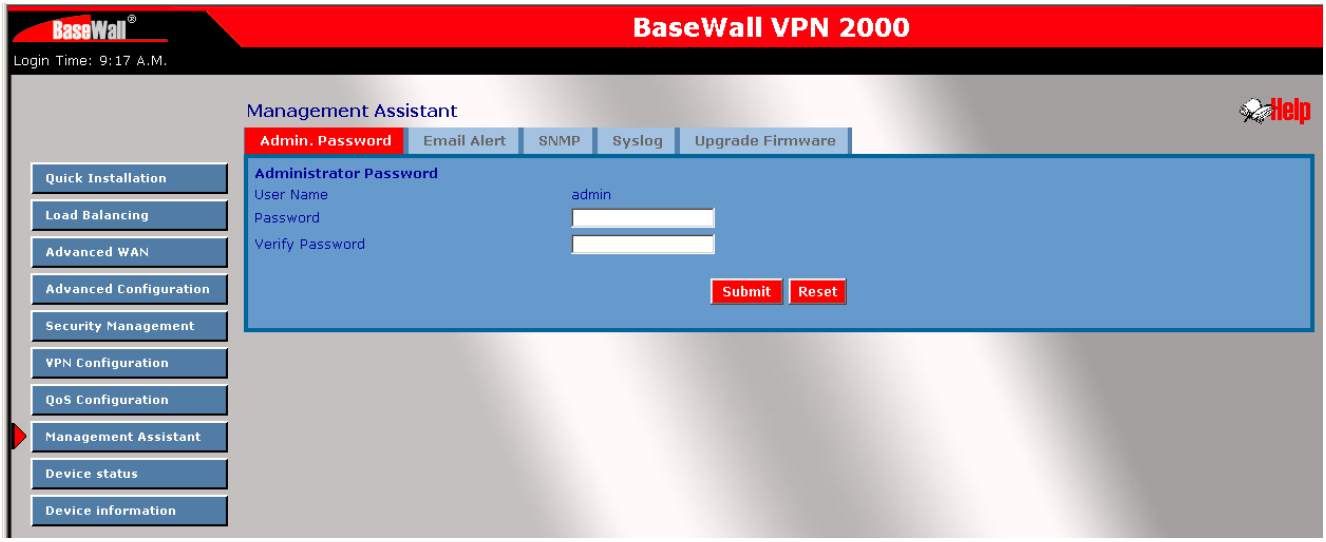


Policy Priority :

- Policy Name List – When adding a new Policy, ignore this list. To edit an existing entry, select it from the list, and click the "Select" button. The data fields will then 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.
- Source Address – Define the source address of packets here. It has two types like IP address or MAC address. If you select IP address, you can define IP address range; otherwise 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 packets here.
- Destination Port – Define the destination port of packets here.
- Priority Queue – It defines a packet if it meets all conditions defined above, it will be serviced with some priority level.

9 : Management Assistant

Management assistant – Admin Password

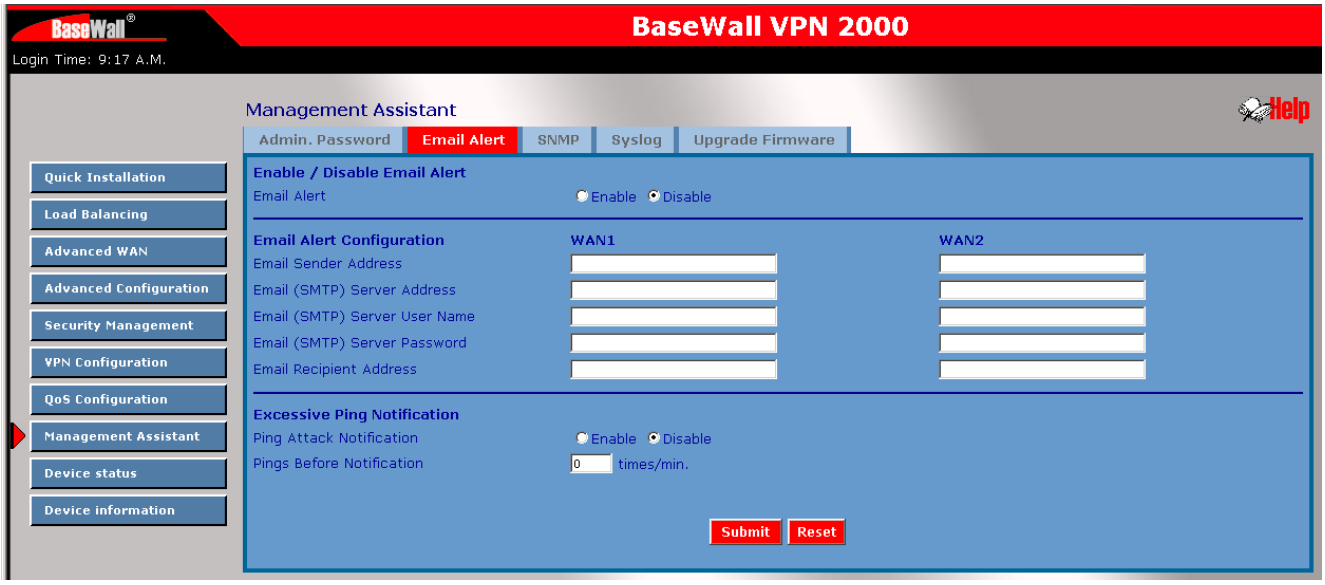


Enter the desired password, re-enter it in the *Verify Password* field, then save it.
When you connect to the Load Balancer with your Browser, you will be prompted for the password when you connect, as shown below.

Figure 8-5: Password Dialog

- Enter "Admin" for the *User Name.*
- Enter the password for the Dual WAN VPN Firewall, as set on the *Admin Password* screen above.

Management Assistant – Email Alert



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

Enable/Disable Email Alert

- **Enable –** This will enable email alert to send a warning email when WAN port was disconnected.
- **Disable –** This will disable email alert not to send a warning email when WAN port was disconnected

Email Alert Configuration

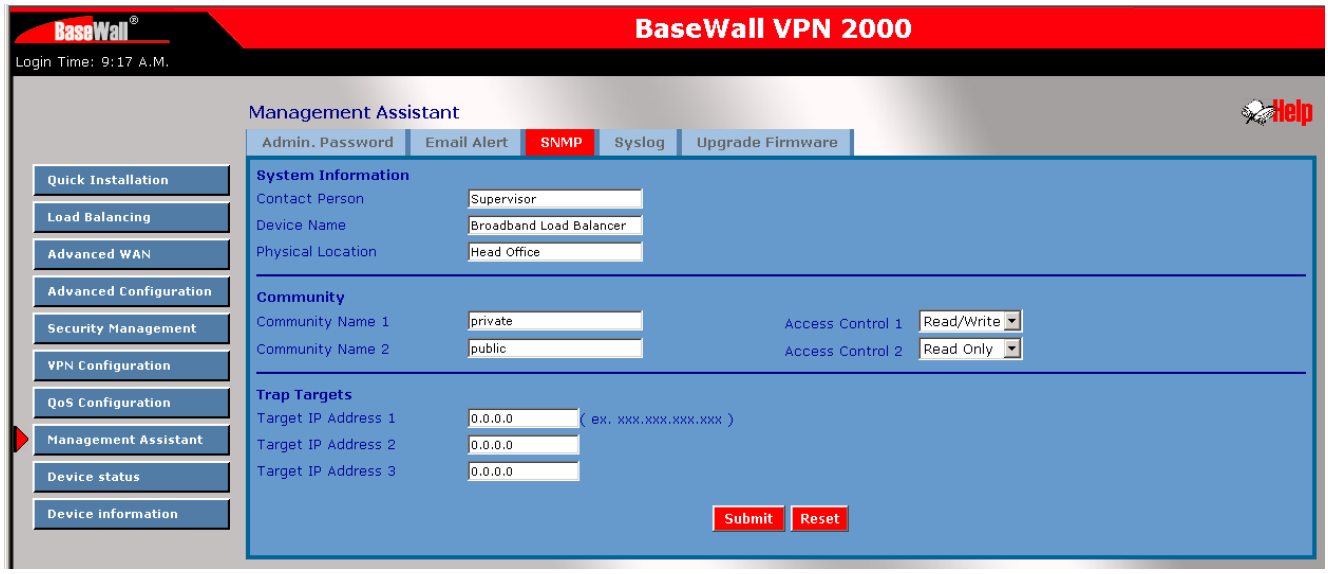
- **Email Sender Address-** It is an email address that sends a warning email to a recipient. Inform that a recipient checks if there is any problem on WAN ports or not.
- **Email (SMTP) Server Address -** It is an email server a warning email will be sent to. If the setting is enabled this is the address we here the email alert will be send to. 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). When if one of the WAN port is disconnected, the email message will be sent to him(her).

Excessive Ping Notification - This function is useful to prevent ICMP packets attacks, from WAN or LAN, on the device. It will drop the packets if the ping times are excessive the threshold value Ping Before Notification. And it will send e-mail to notify the administrator if Email Alert is enabled.

- **Ping Attack Notification -** By default this feature is Disabled.
- **Ping Before Notification -** A threshold value, means the maximum Ping times allowed to each interface on this device in a minute. The valid values ranges from 0 to 9999.

Management Assistant – SNMP

This section is only usefull 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 2000.



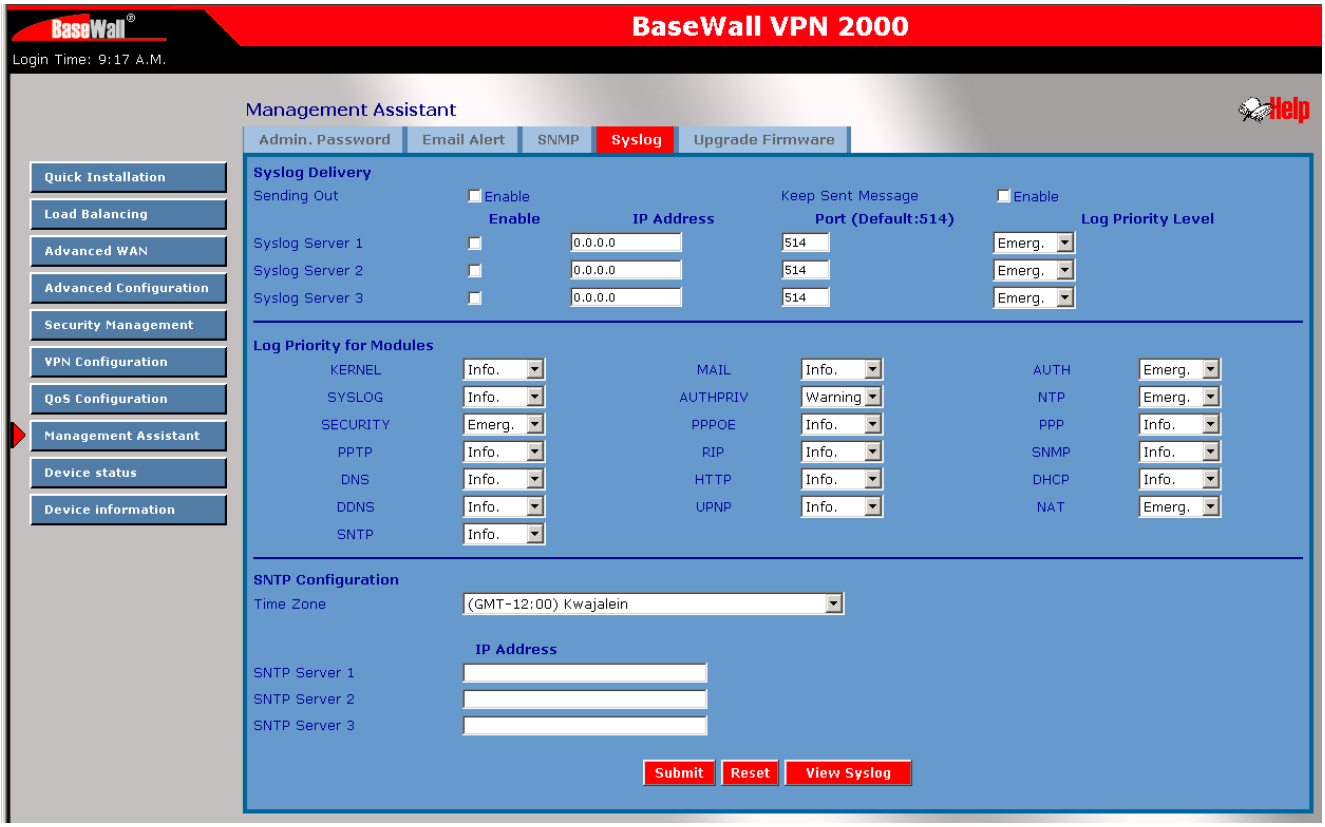
System Information

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

Community - It is a relationship between a SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

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

Management Asssistant – Syslog



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

Syslog Delivery

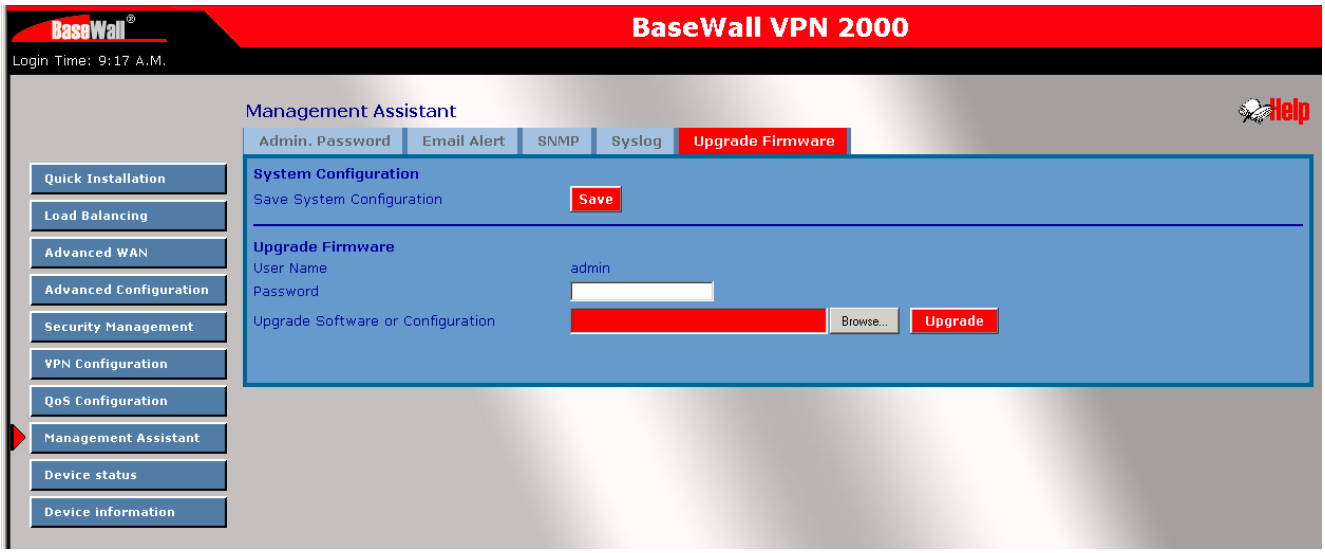
- **Sending out –** Check this, if you want to send syslog messages to other machine.
- **Keep Send messages –** Check this, if you want to keep sent messages, otherwise the sent message will be delete.
- **Syslog Server - IP address:** Up to 3 syslog servers can be used.
- **Enable:** You can enable or disable each server temporarily.
- **Port:** If your syslog does not use the default port, change it.

- **Log Priority for modules -** The messages are grouped into **8** priority levels, from **Emergency** to **Debug**. The lower level it is, the fewer messages it will generate. Emergency is the lowest priority level, and Debug is the highest one. So set priority to **Debug** will send all generated messages.

SNTP Configuration

- **Time Zone -** You can setup system up time using SNTP (**S**imple **N**etwork **T**ime **P**rotocol), and there are 3 SNTP server that you can define on the SNTP configuration.

Management Asssistant - Upgrade Firmware



This Upgrade Firmware Screen allows you to upgrade firmware or backup system configuration by using HTTP upgrade.

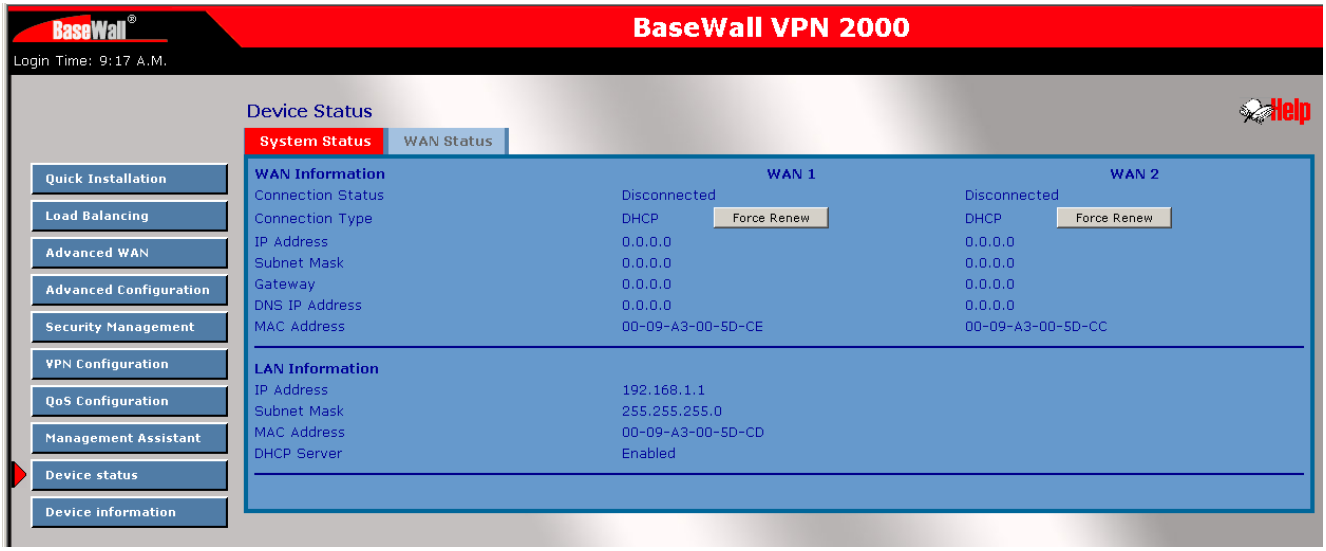
- You can backup your system configuration by press “save” button of Save System Configuration. It will save the system configuration for you. (Notice: You have to refresh the browser after you saved the system configuration file)

- You also can do firmware upgrade by input the correct password and the file name of your firmware. Remember do not Reset or Restart the device while update new firmware, because it may cause system to crash.

10: Device Status

Once both the Dual WAN VPN Firewall and the PCs are configured, operation is automatic. However, there are some situations where additional Internet configuration may be required: Refer to *Chapter 6 - Advanced Features* for further details.

Device status – System status

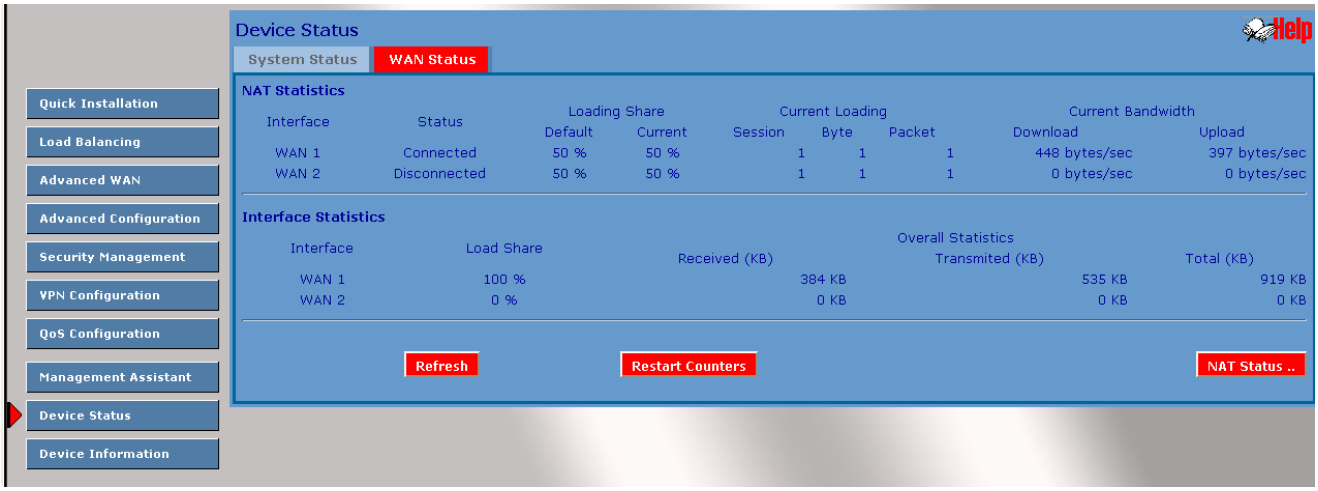


- **Connection Status –** Current status – either "Connected" or "Disconnected".
- **Connection Type –** The type of connection used – DHCP, Fixed IP, PPPoE or PPTP
- **"Force Renew"** button– Only available if using a dynamic IP address (DHCP). Clicking this button will perform a DHCP "Renew" transaction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

LAN Information

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

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



Device Status - WAN status

NAT Statistics

This section displays data for each WAN port.

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

"Check NAT Detail" will display the ***NAT Status*** screen, described below

Data – NAT Status

LAN IP info

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

Active WAN IP Info – There is one (1) row for each active connection, for each connection the following data is shown.

- **IP Address –** The WAN (Internet) IP Address of the Dual WAN VPN Firewall.
- **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.

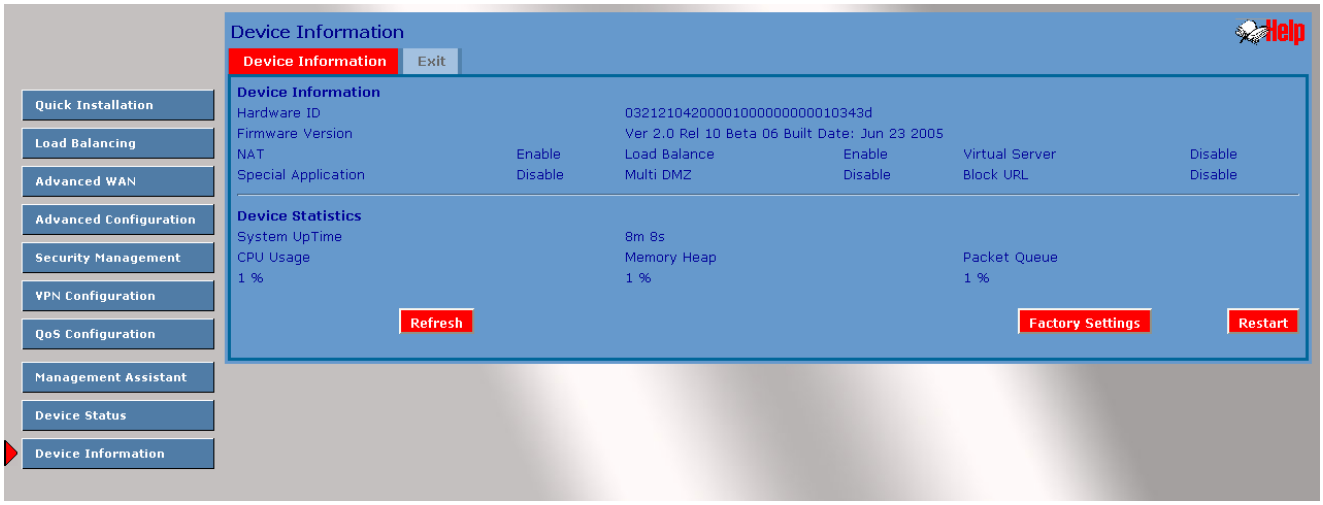
NAT Connections - This displays the current number of active connections. For further details, click the "View Connection" list button.

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

- **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 "Enabled" or "Disabled".
- **Block URL –** Status of the *Block URL* feature - either "Enabled" or "Disabled".
- **Hardware ID -** The manufacturers ID for this particular device

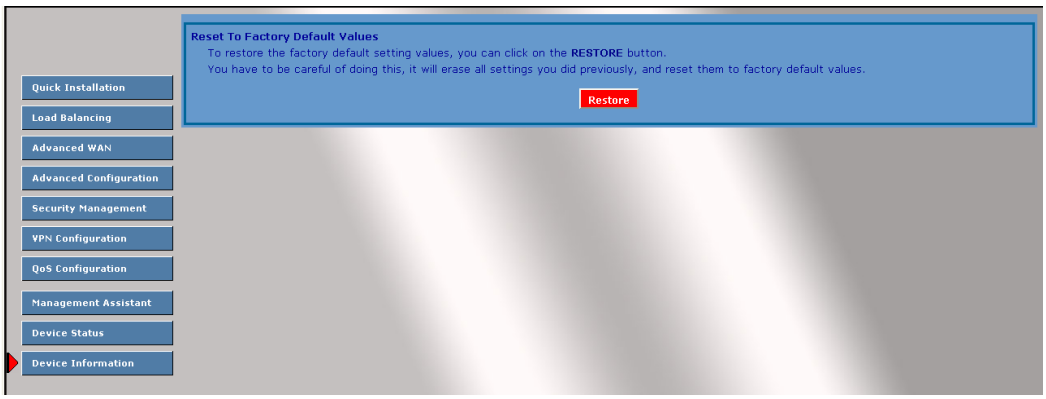
Device Statistics

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

Buttons

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

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



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

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

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

Appendix A

Specifications

Model	BaseWall VPN 2000 Dual WAN Firewall
Dimensions	246mm (W) x 138mm (D) x 30mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network protocol Protocol:	TCP/IP
Network Interfaces	6 Ethernet: 4 * 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices 2 * 10/100BaseT (RJ45) for WAN
LEDs	4 LAN 2 WAN 2 Status 1 Power
Power Input	DC 5V @ 1500 mA

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 undesired 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.

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 TCP/IP settings, no changes need to be made.

- By default, the Dual WAN VPN Firewall will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.
- If you wish to check your TCP/IP settings, the procedure is described in the following sections.
- If your LAN has a Router, the LAN Administrator must re-configure the Router itself.

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

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

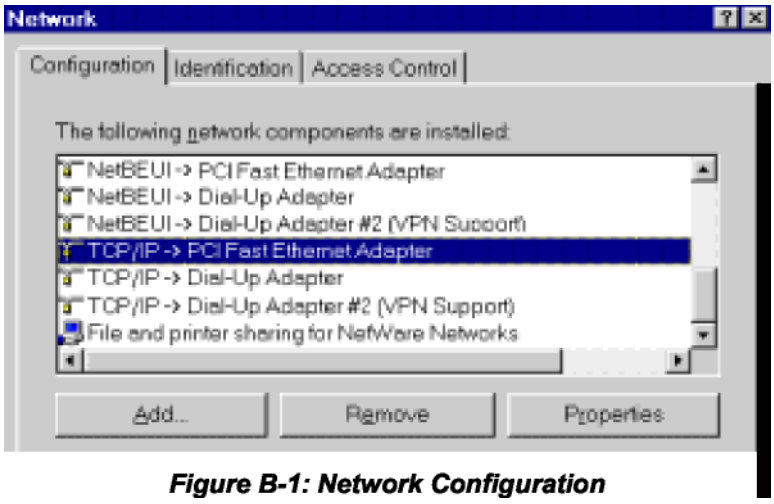
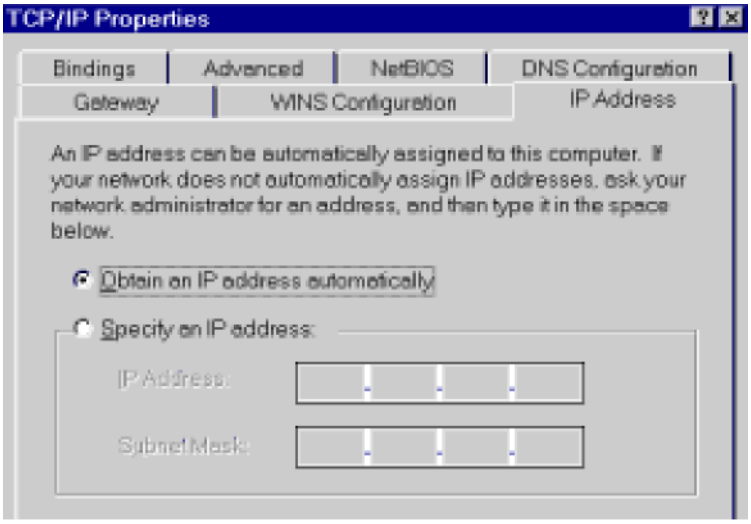


Figure B-1: Network Configuration

2. Select the *TCP/IP* protocol for your network card.

3. Click on the *Properties* button. You should then see a screen like the following.



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 Dual WAN VPN Firewall.

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 the Dual WAN VPN Firewall IP address in the *New Gateway* field and click *Add,* as shown below. (Your LAN administrator can advise you of the IP Address they assigned to the Dual WAN VPN Firewall.)

Statistics

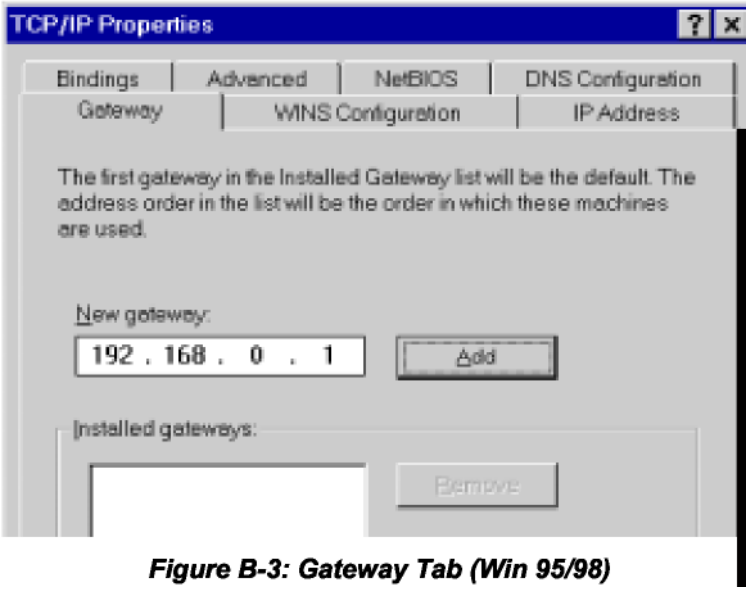


Figure B-3: Gateway Tab (Win 95/98)

- 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.*

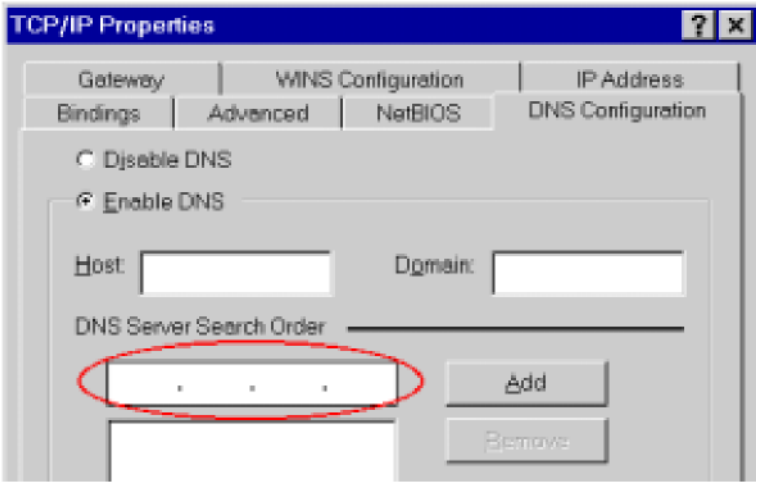


Figure B-4: DNS Tab (Win 95/98)

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:

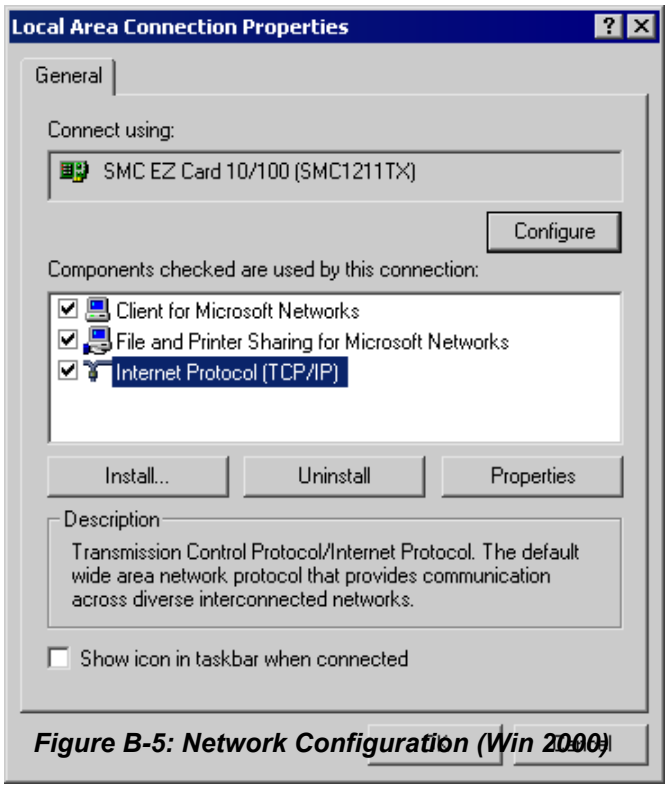


Figure B-5: Network Configuration (Win 2000)

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

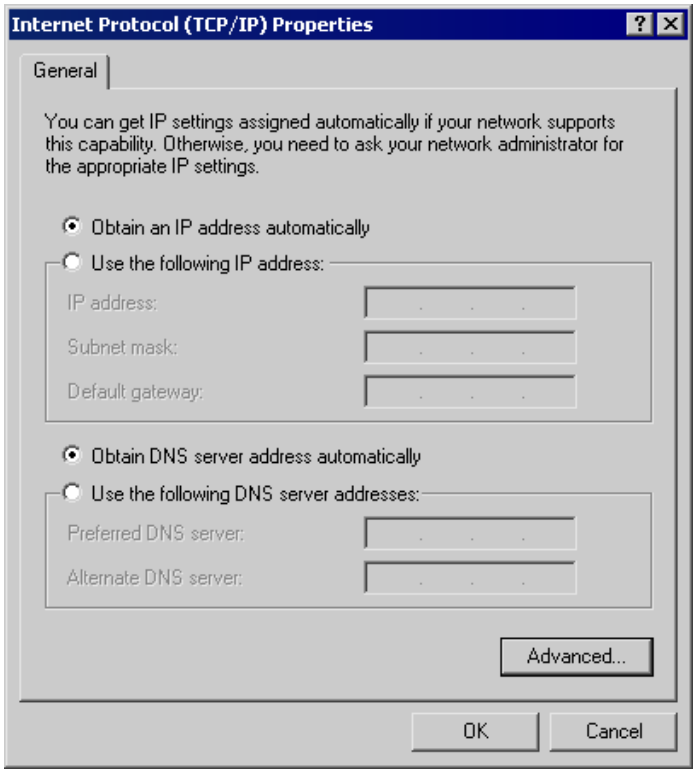


Figure B-6: TCP/IP Properties (Win 2000)

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

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

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

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

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:

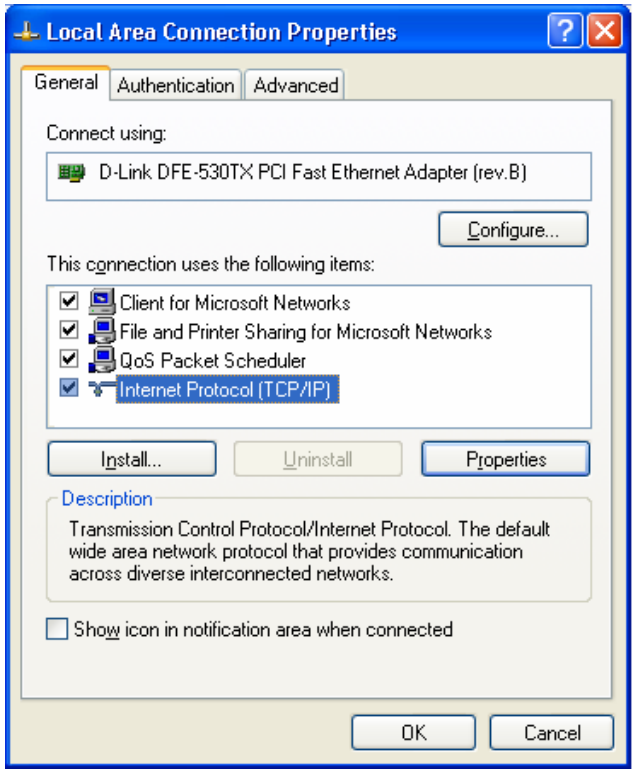


Figure B-7: Network Configuration (Windows XP)

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

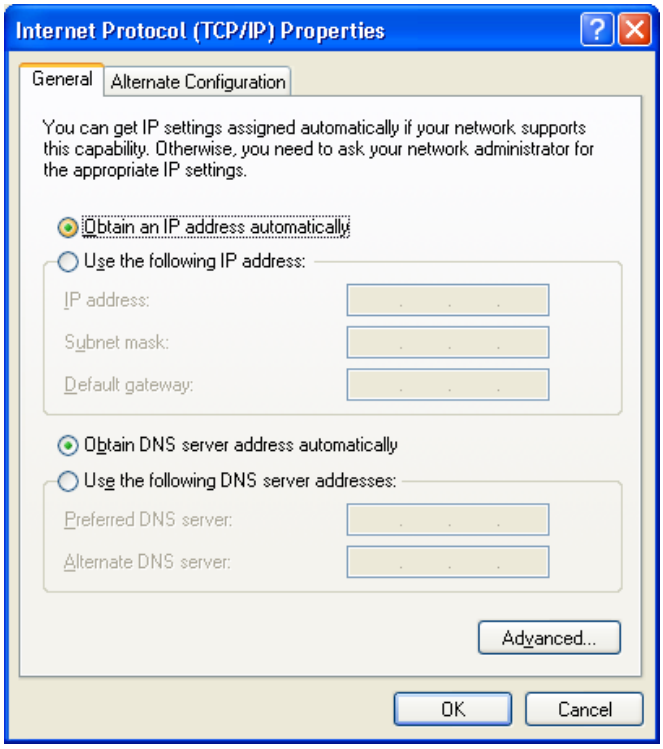


Figure B-8: TCP/IP Properties (Windows XP)

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

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

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

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

Appendix C

Troubleshooting

Overview

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

General Problems

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

Solution : Check the following:

- The Load Balancer is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Dual WAN VPN Firewall are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with the Dual WAN VPN Firewall default IP Address of 192.168.1.1.Also, the Network Mask should be set to 255.255.255.0 to match the VPN 3000 Mask.

Internet Access

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

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

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

Problem 2 : Some applications do not run properly when using the VPN 3000 Dual WAN Firewall.

Solution :

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

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

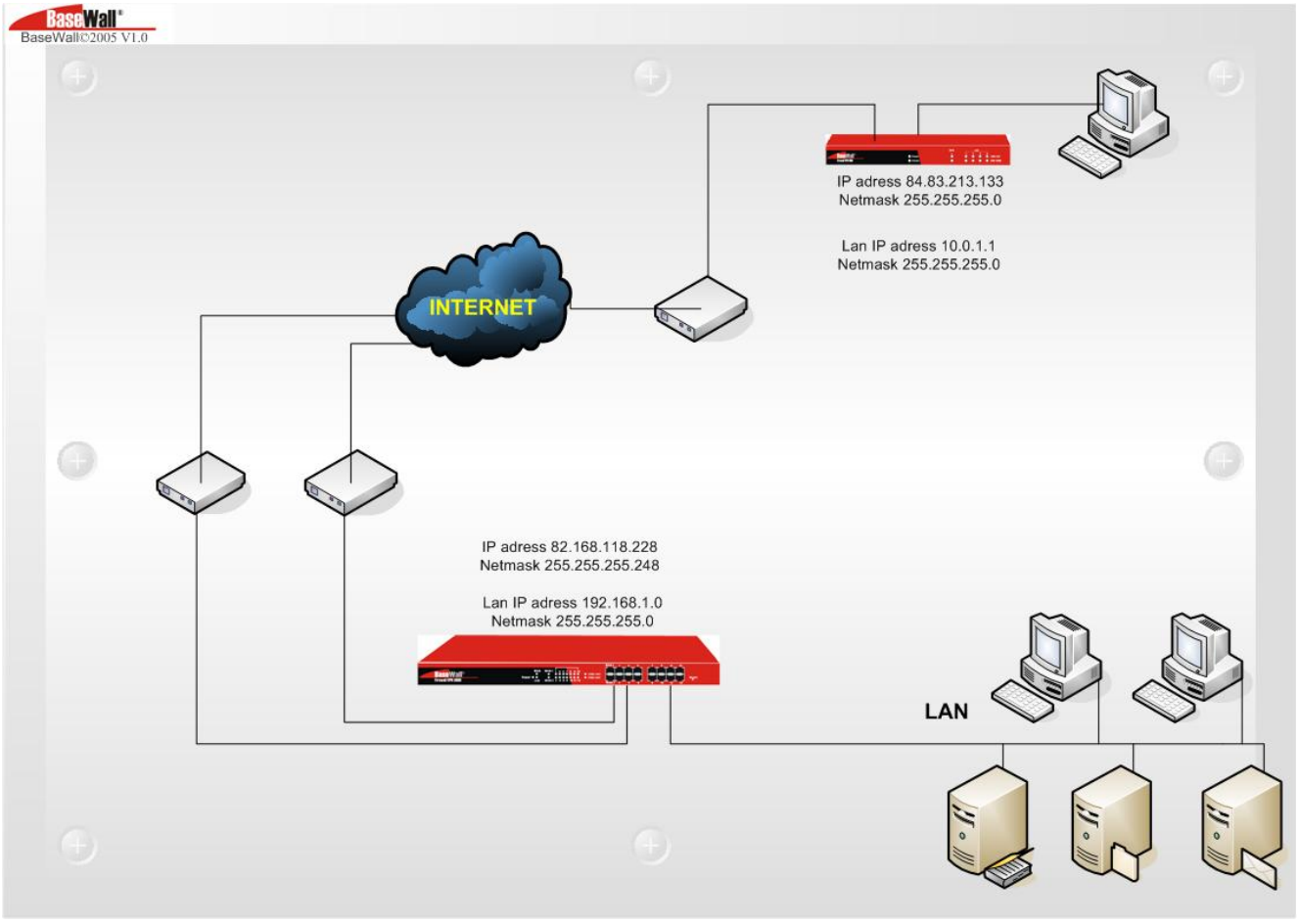
Appendix D : IPSec Tunnel Examples

VPN Configuration – Examples

Tunnel to BaseWall Unit

VPN 3000 TO : VPN 1000 OR VPN 2000 OR VPN 3000

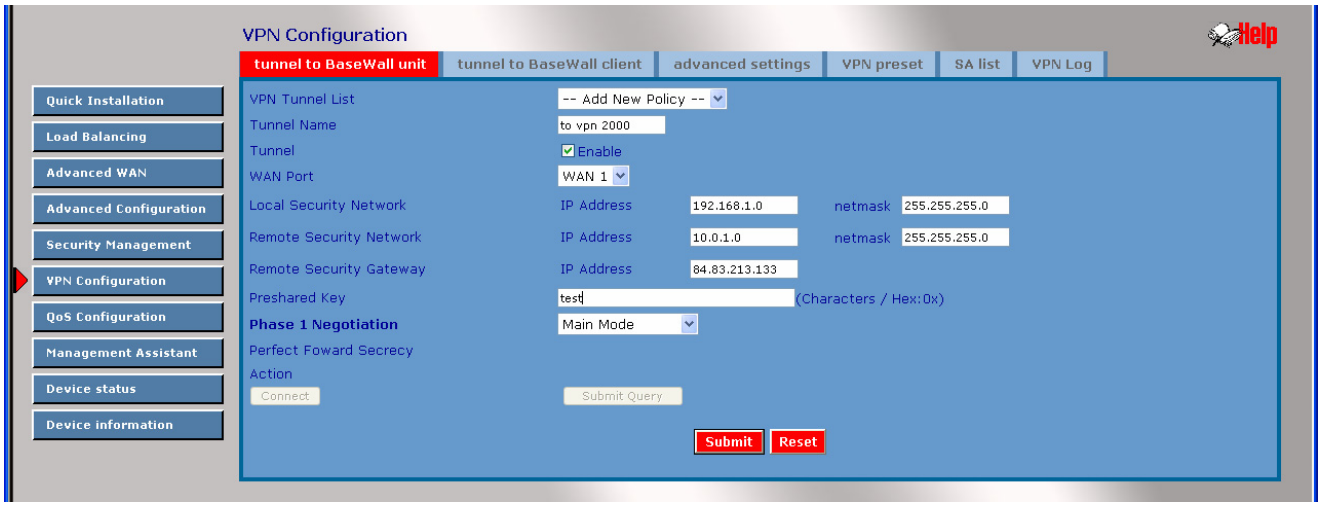
The BaseWall units in the following example use registered IP addresses. You have to replace these addresses with IP addresses that are available to you. These settings are only possible if you have a static IP address available on one or both of your WAN ports.



This example takes a tunnel between a VPN 3000 and a VPN 2000. This example applies to the BaseWall VPN 1000,2000 and 3000 series, you can use eather unit at both sides. You can use the IP addresses from the network diagram above.

These kind of tunnels are named LAN to LAN IPSec tunnels.

First we will make settings in the VPN 3000



Next we will make settings for the VPN 2000

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**.