

# Chapter 2: WEB Configuration

## Network

### 1. LAN

You can activate the DHCP server function for the LAN on this page.

With this function activated, your cable company's DHCP server provides one IP address for your gateway, and your gateway's DHCP server provides IP addresses, starting at the address you set in IP Address on the LAN page, to your PCs. A DHCP server leases an IP address with an expiration time.

To change the lowest IP address that your gateway will issue to your PCs, enter it into the **IP Address** box and then click **Apply**.

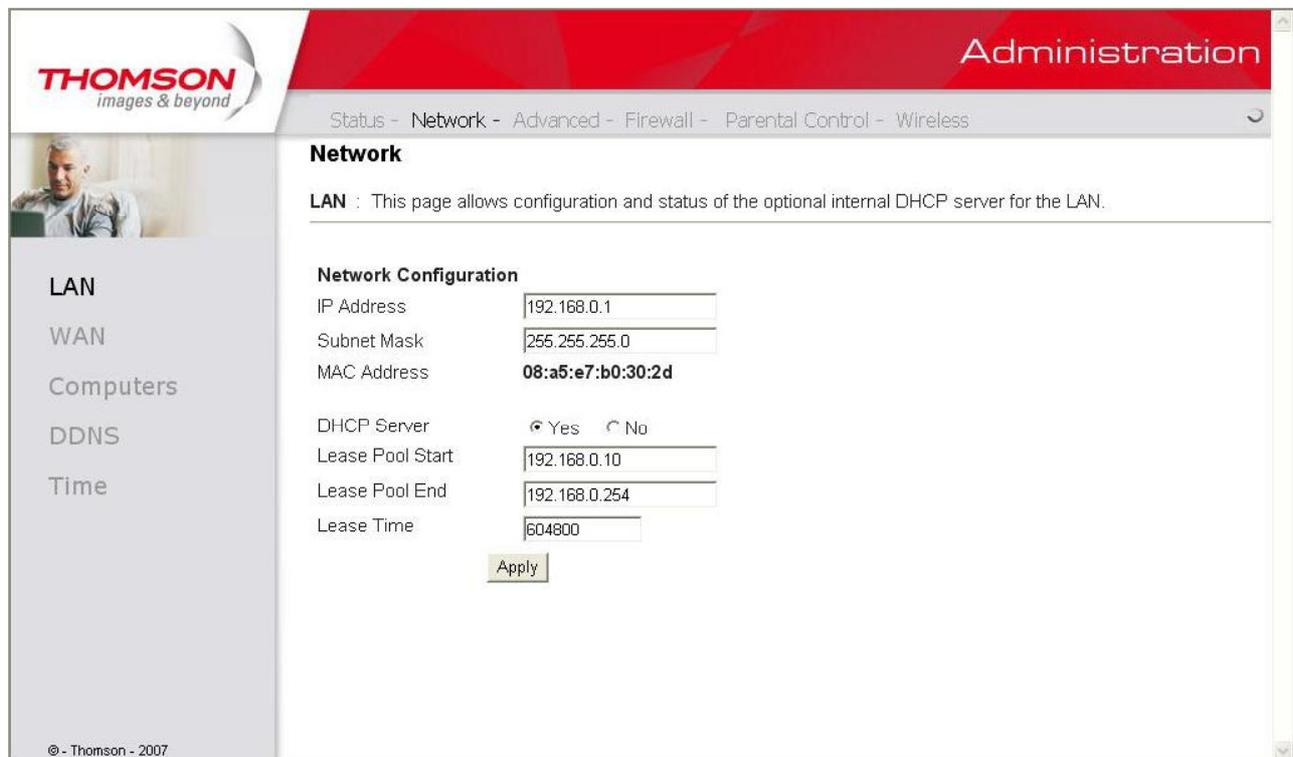


Fig. 13

# Chapter 2: WEB Configuration

## 2. WAN

You can configure the optional internal DHCP server for the WAN on this page. Select different WAN Connection Type will lead to different contents. Take the WAN connection type-DHCP for example, you can release and renew the WAN lease by pressing the buttons.

You can enter a spoofed MAC address that causes your gateway networking stack to use that MAC address when communicating instead of the usual WAN MAC address, e.g., if the MAC address is `00:11:e3:df:66:95`, this spoofed MAC address could be `00:11:e3:df:66:97` or any desired MAC address.

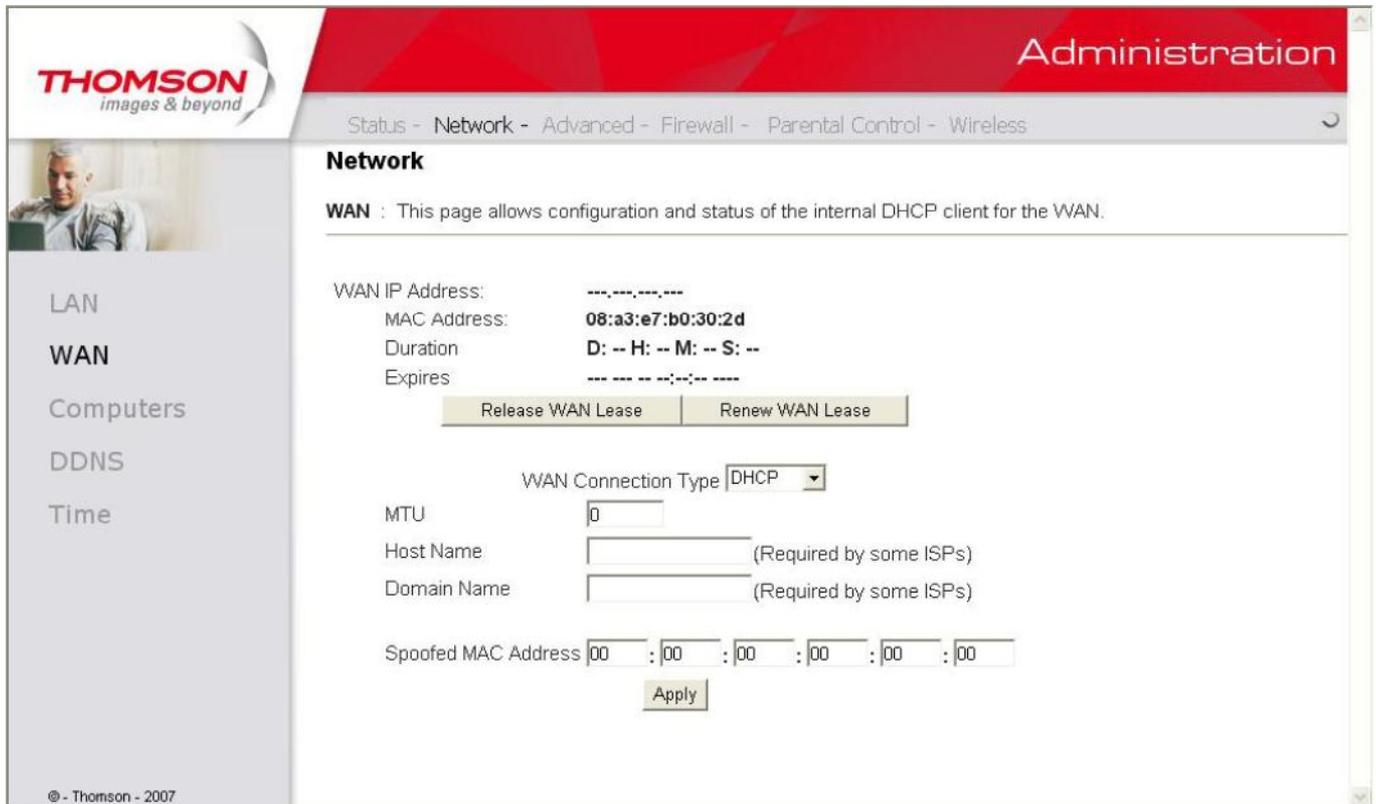


Fig. 14

# Chapter 2: WEB Configuration

## 3. Computers

This page displays the status of the DHCP clients and current system time. You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the **Force Available** button. If you do so, you may have to perform a DHCP Renew on that PC, so that it can obtain a new lease.

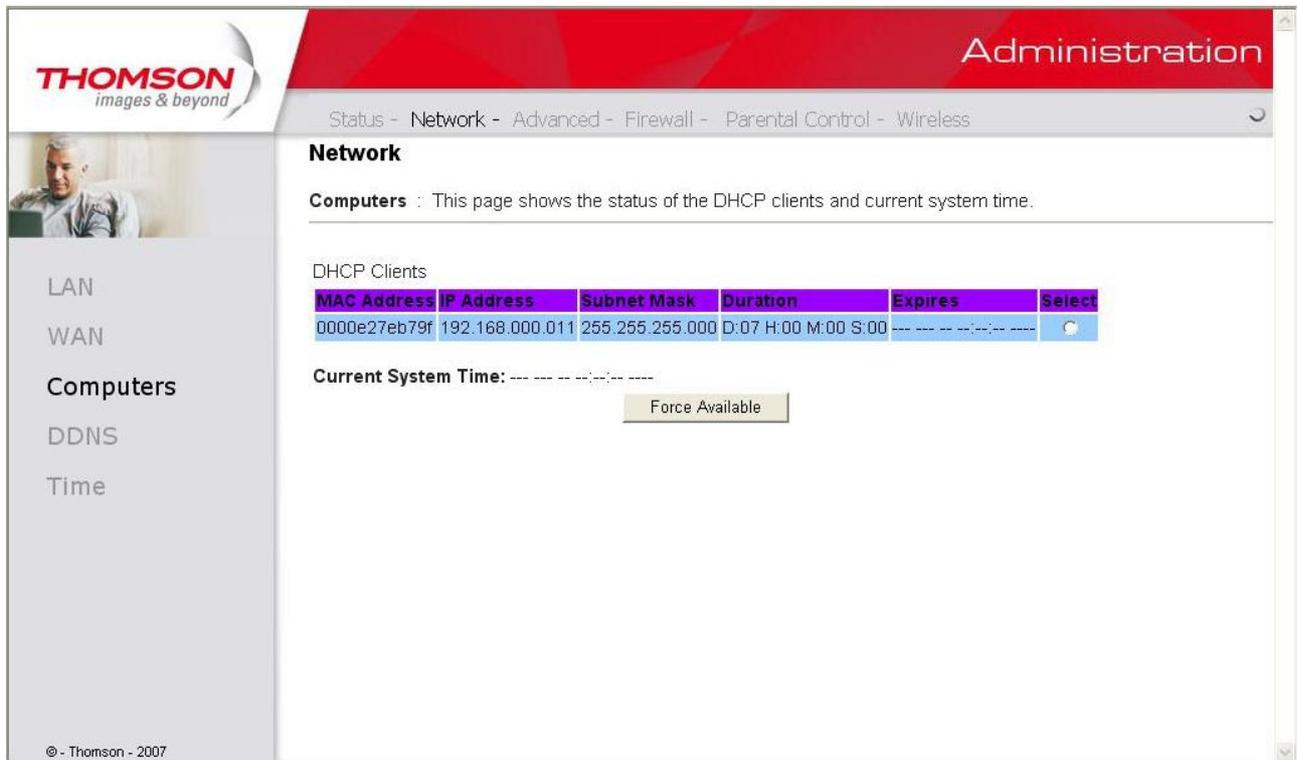


Fig. 15

# Chapter 2: WEB Configuration

## 4. DDNS

This page allows setup of Dynamic DNS service.

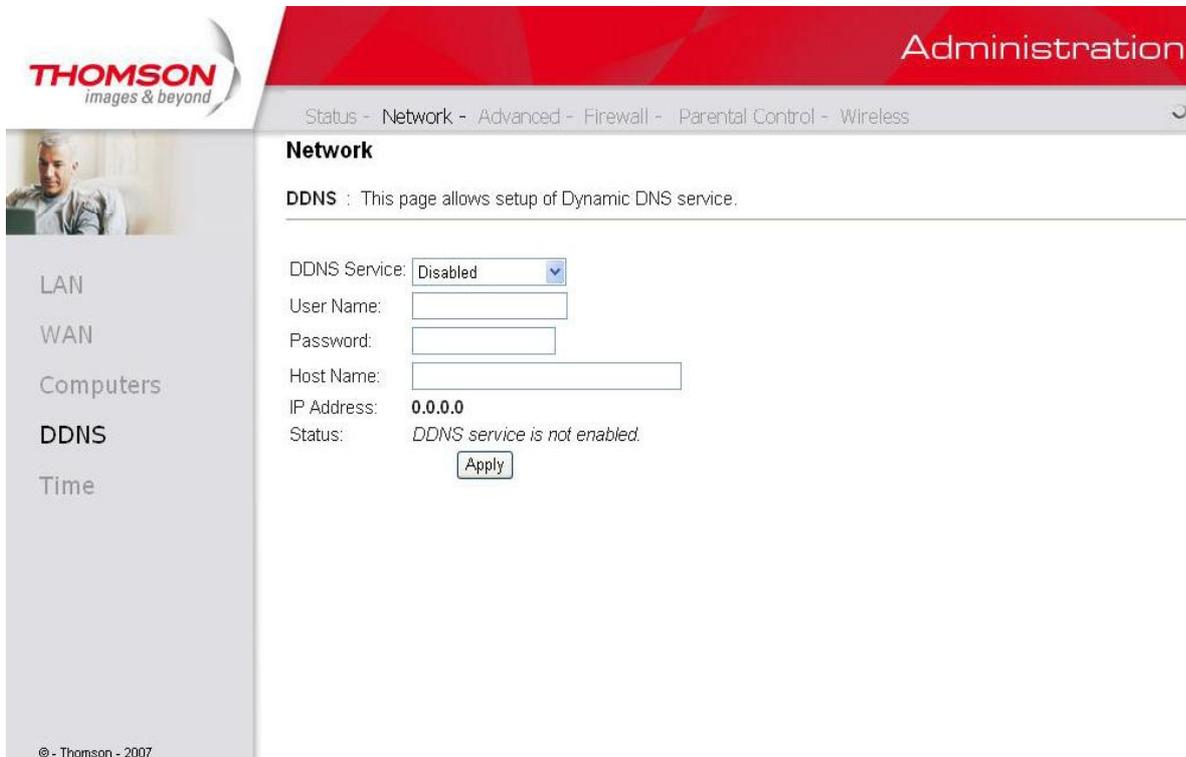


Fig. 16

- **DDNS Service-** Choose Enabled ( [www.DynDNS.org](http://www.DynDNS.org) ) to enable the basic setting. Choose Disabled to close the basic setting.
- **Username-** The username that you registered with your DDNS provider.
- **Password-** The password that you registered with your DDNS provider
- **Host Name-** The domain name or host name that is registered with your DDNS provider
- **Status-** It shows the DDNS service status whether it is enabled or disabled.

Click Apply to save the changes

# Chapter 2: WEB Configuration

## 5. Time

This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.

The screenshot shows the Thomson Administration web interface. The top navigation bar includes the Thomson logo and the word "Administration". Below it is a breadcrumb trail: "Status - Network - Advanced - Firewall - Parental Control - Wireless". The main content area is titled "Network" and contains a "Time" section. This section includes a description: "Time : This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect." Below the description are configuration options: "Enable SNTP" with radio buttons for "Yes" and "No" (where "No" is selected); "Current Time" showing "Thu Jan 01 03:07:27 1970"; "System Start Time" showing "Thu Jan 01 00:00:00 1970"; three "Time Server" fields with values "clock.via.net", "ntp.nasa.gov", and "tick.ucla.edu"; and "Timezone Offset" with "Hours" and "Minutes" dropdown menus both set to "0". At the bottom of the configuration area are "Apply" and "Reset Values" buttons. A left sidebar contains navigation links for LAN, WAN, Computers, DDNS, and Time. The footer of the sidebar shows "© - Thomson - 2007".

## Advanced

### 1. Options

This page allows you to enable/disable some features of the Wireless Gateway.

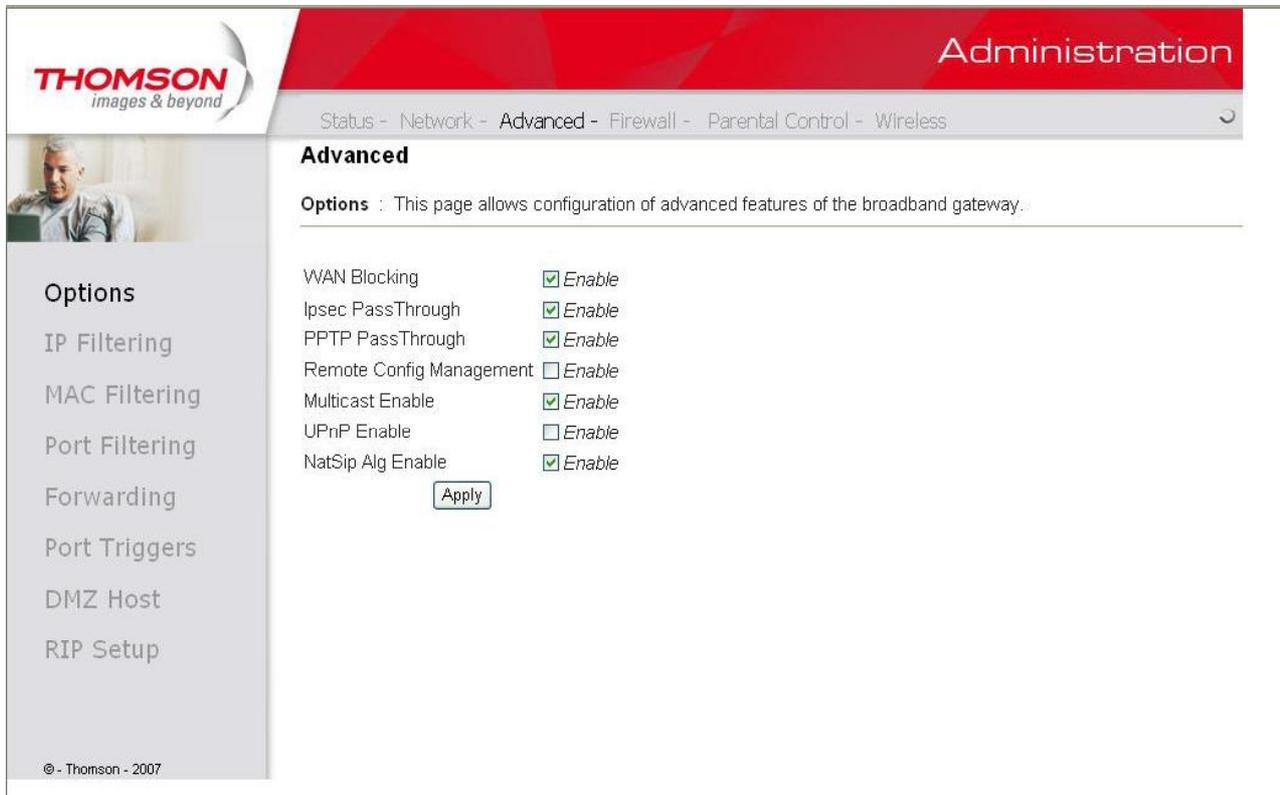


Fig. 17

- **WAN Blocking** prevents others on the WAN side from being able to ping your gateway. With WAN Blocking enabled, your gateway will not respond to pings it receives, effectively “hiding” your gateway.
- **Ipssec PassThrough** enables IpSec type packets to pass WAN ⇔ LAN. IpSec (IP Security) is a security mechanism used in Virtual Private Networks (VPNs).
- **PPTP PassThrough** enables PPTP type packets to pass WAN ⇔ LAN. PPTP (Point to Point Tunneling Protocol) is another mechanism sometimes used in VPNs.
- **Remote Config Management** makes the configuration web pages in your gateway accessible from the WAN side. Note that page access is limited to only those who know the gateway access password. When accessing your gateway from a remote location, you must use HTTP port 8080 and the WAN IP address of the gateway. For example, if the WAN IP address is 157.254.5.7, you would navigate to <http://157.254.5.7:8080> to reach your gateway.
- **Multicast Enable** enables multicast traffic to pass WAN⇔ LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet.
- **UPnP** Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover

# Chapter 2: WEB Configuration

the services from other registered UPnP devices on the network.

- **NatSip Alg Enable** feature enabled by default. While ALG could help in solving NAT related problems in client LAN side. An ALG understands the protocol used by the specific applications that it supports and does a protocol packet-inspection of SIP traffic through it. A NAT router with inbuilt SIP ALG can re-write information within the SIP messages (SIP headers and SDP body) making possible signaling and audio traffic between LAN client and outside SIP endpoint.

## 2. IP Filtering

This page enables you to enter the IP address ranges of PCs on your LAN that you don't want to have outbound access to the WAN. These PCs can still communicate with each other on your LAN, but packets they originate to WAN addresses are blocked by the gateway.

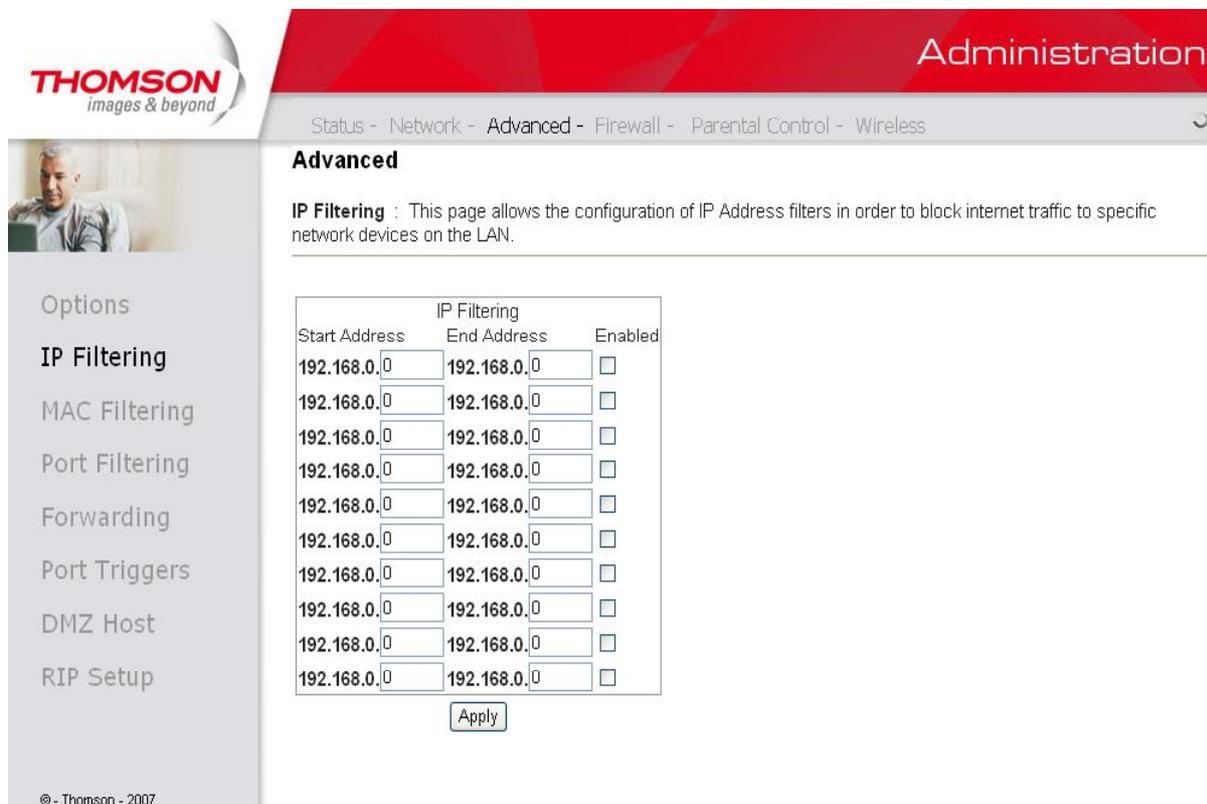


Fig. 18

# Chapter 2: WEB Configuration

## 3. MAC Filtering

This page enables you to enter the MAC address of specific PCs on your LAN that you wish to NOT have outbound access to the WAN. As with IP filtering, these PCs can still communicate with each other through the gateway, but packets they send to WAN addresses are blocked.

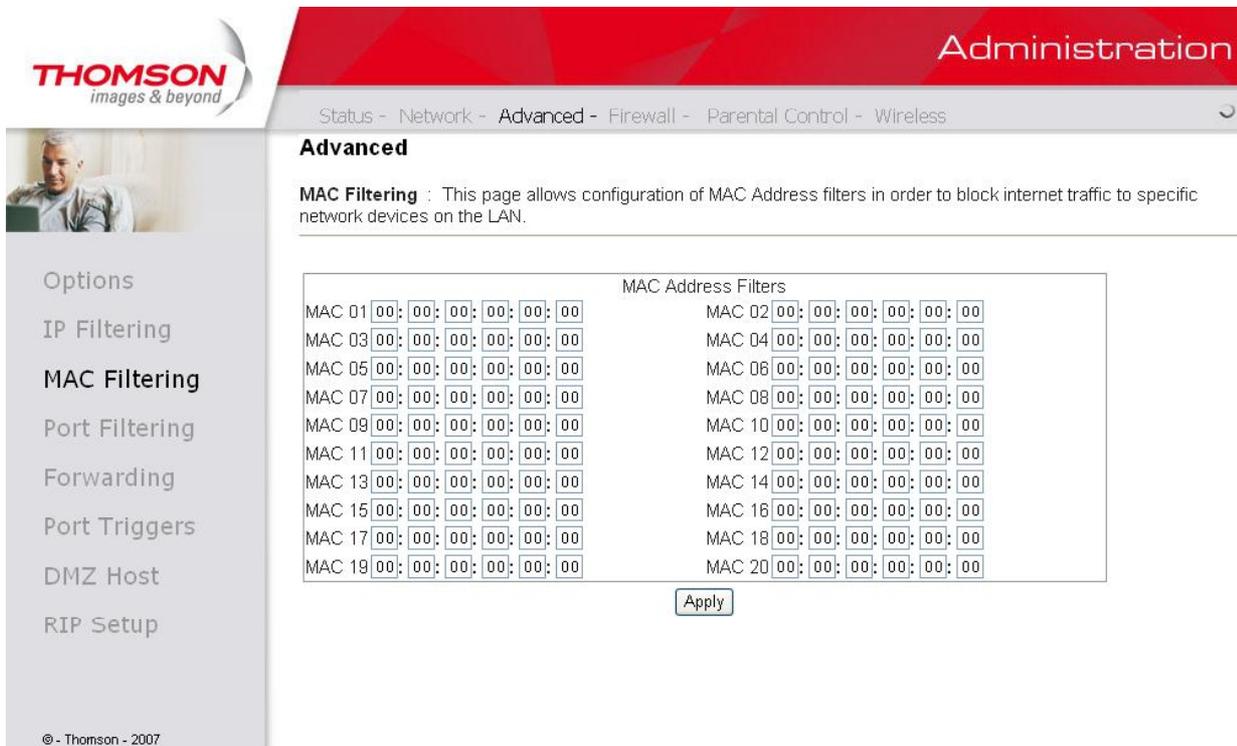


Fig. 19

# Chapter 2: WEB Configuration

## 4. Port Filtering

This page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (http = port 80) but still allow email service (SMTP port 25 and POP-3 port 110). To enable port filtering, set Start Port and End Port for each range, and click Apply. To block only one port, set both Start and End ports the same.

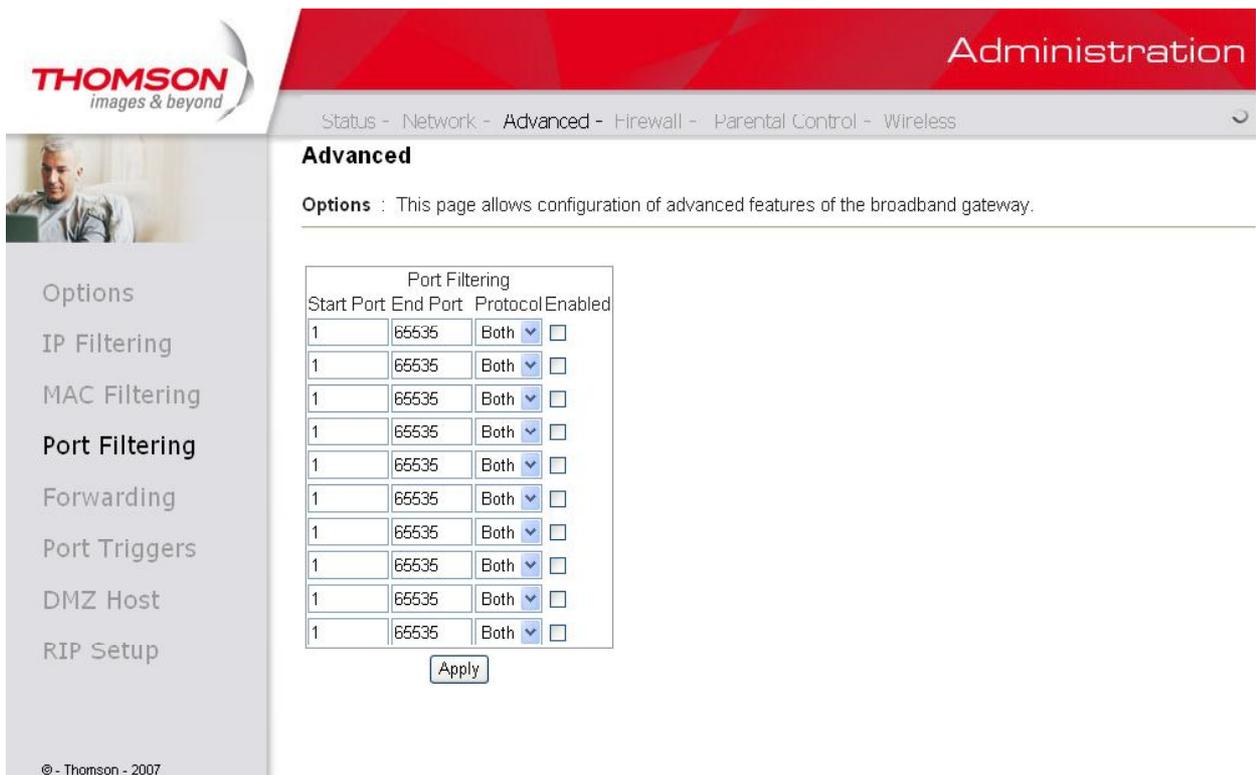


Fig. 20

# Chapter 2: WEB Configuration

## 5. Forwarding

For LAN ↔ WAN communications, the gateway normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.

This page allows you to specify up to 10 such rules. For example, to specify that outsiders should have access to an FTP server you have running at 192.168.0.5, create a rule with that address and Start Port =20 and End Port =21 (FTP port ranges) and Protocol = TCP (FTP runs over TCP and the other transport protocol, UDP), and click Apply. This will cause inbound packets that match to be forwarded to that PC rather than blocked. As these connections are not tracked, no entry is made for them in the Connection Table. The same IP address can be entered multiple times with different ports.

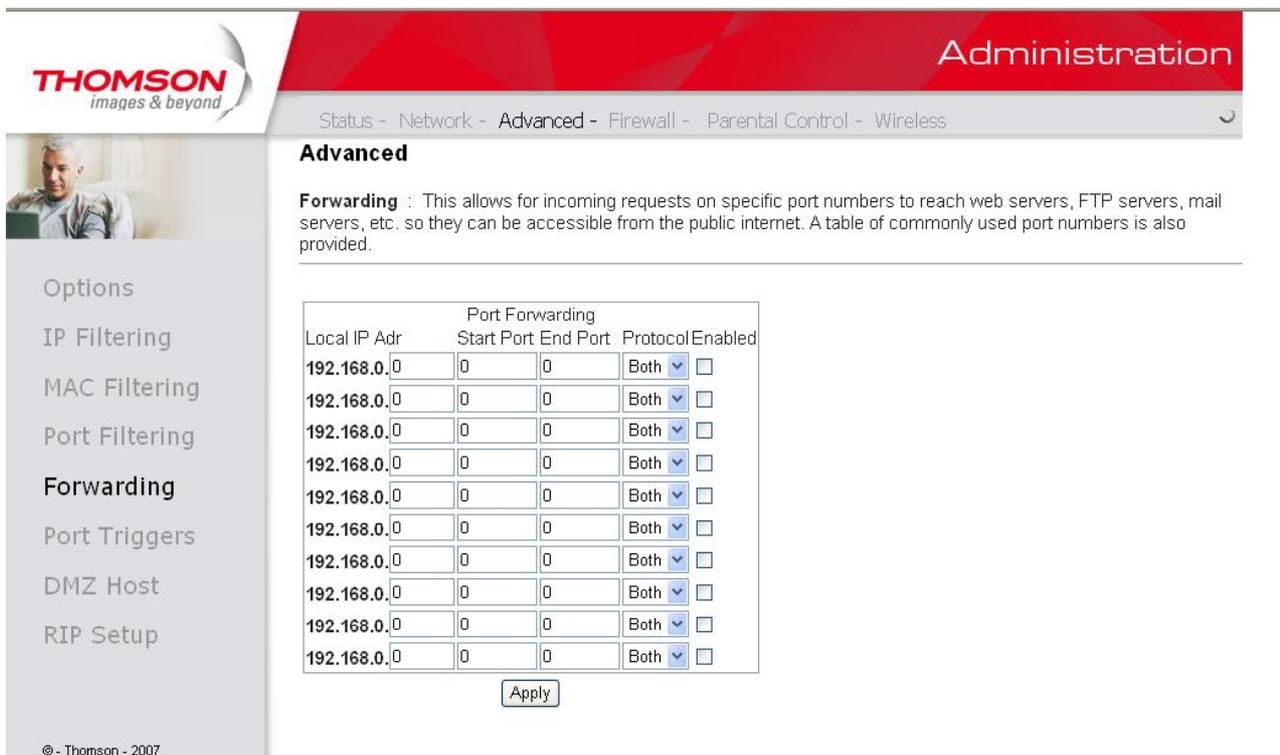


Fig. 21

# Chapter 2: WEB Configuration

## 6. Port Triggers

Some Internet activities, such as interactive gaming, require that a PC on the WAN side of your gateway be able to originate connections during the game with your game playing PC on the LAN side. You could use the Advanced-Forwarding web page to construct a forwarding rule during the game, and then remove it afterwards (to restore full protection to your LAN PC) to facilitate this. Port triggering is an elegant mechanism that does this work for you, each time you play the game.

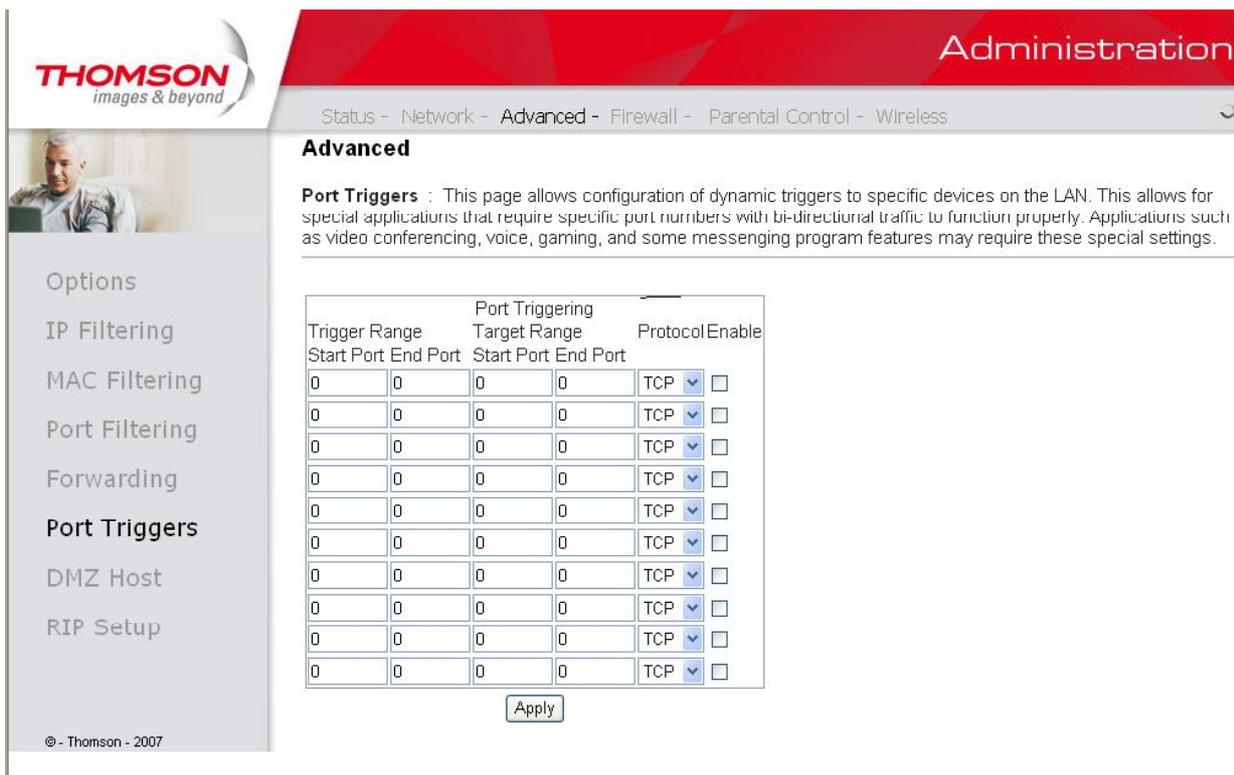


Fig. 22

Port Triggering works as follows. Imagine you want to play a particular game with PCs somewhere on the Internet. You make one time effort to set up a Port Trigger for that game, by entering into **Trigger Range** the range of destination ports your game will be sending to, and entering into **Target Range** the range of destination ports the other player (on the WAN side) will be sending to (ports your PC's game receives on). Application programs like games publish this information in user manuals. Later, each time you play the game, the gateway automatically creates the forwarding rule necessary. This rule is valid until 10 minutes after it sees game activity stop. After 10 minutes, the rule becomes inactive until the next matched outgoing traffic arrives.

For example, suppose you specify Trigger Range from 6660 to 6670 and Target Range from 113 to 113. An outbound packet arrives at the gateway with your game-playing PC source IP address 192.168.0.10, destination port 666 over TCP/IP. This destination port is within the Trigger destined for port 113 to your game-playing PC at 192.168.0.10.

You can specify up to 10 port ranges on which to trigger.

# Chapter 2: WEB Configuration

## 7. DMZ Host

Use this page to designate one PC on your LAN that should be left accessible to all PCs from the WAN side, for all ports. For example, if you put an HTTP server on this machine, anyone will be able to access that HTTP server by using your gateway IP address as the destination. A setting of “0” indicates NO DMZ PC. “Host” is another Internet term for a PC connected to the Internet.

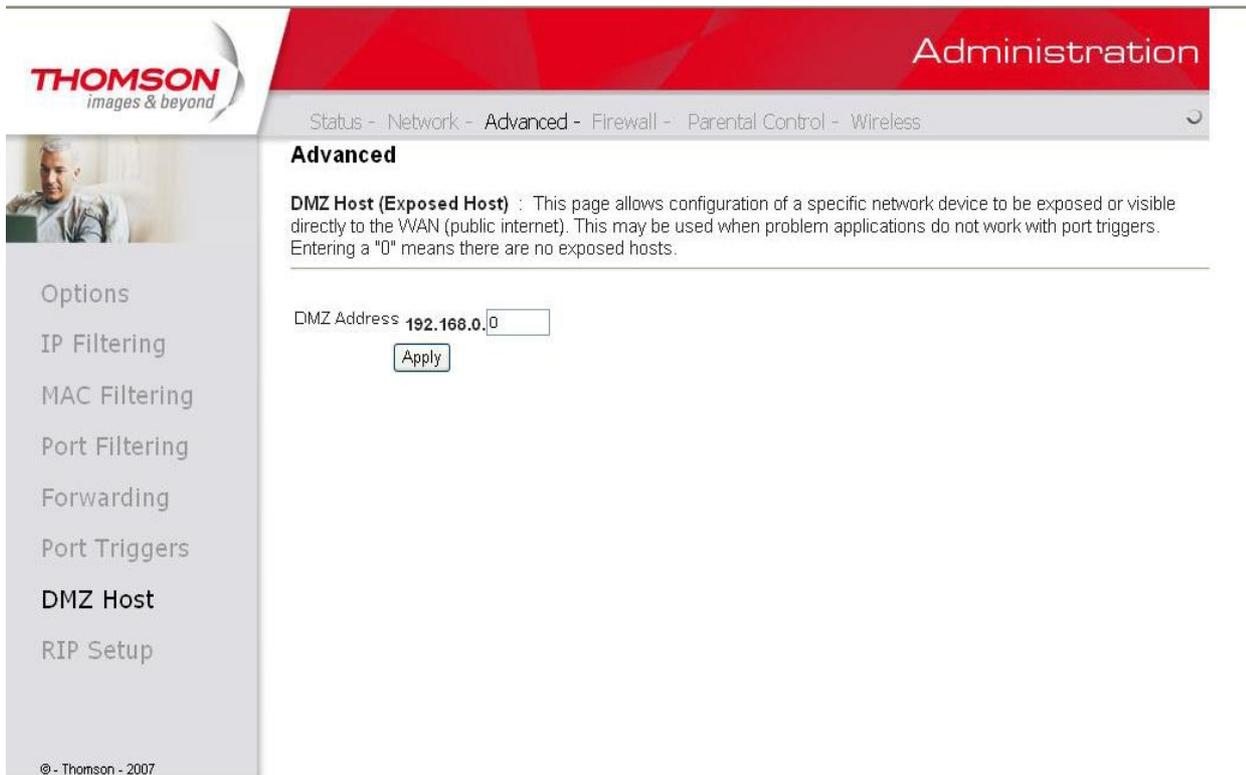


Fig. 23

# Chapter 2: WEB Configuration

## 8. RIP (Routing Information Protocol) Setup

This feature enables the gateway to be used in small business situations where more than one LAN (local area network) is installed. The RIP protocol provides the gateway a means to “advertise” available IP routes to these LANs to your cable operator, so packets can be routed properly in this situation.

Your cable operator will advise you during installation if any setting changes are required here.

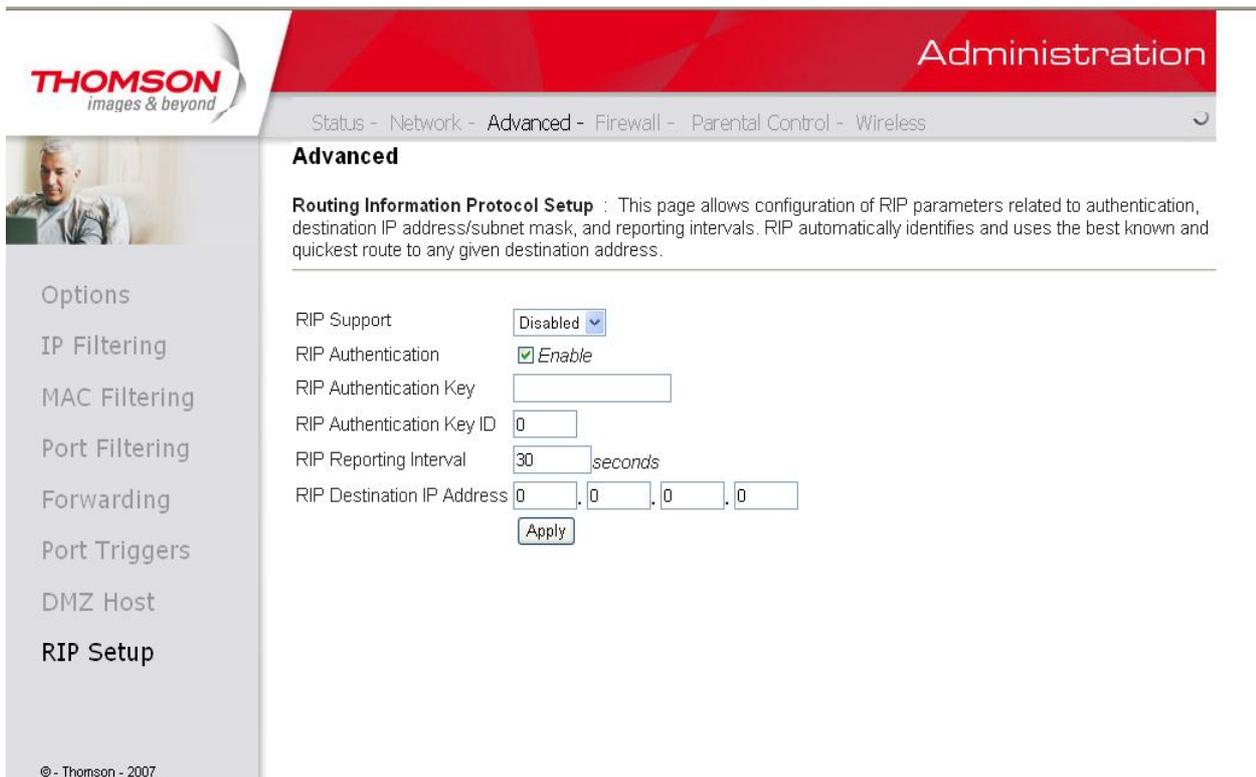


Fig. 24

## Firewall

### 1. Web Filtering

These pages allow you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

The web-related filtering features you can activate from the Web Content Filter page include Filter Proxy, Filter Cookies, Filter Java Applets, Filter ActiveX, Filter Popup Windows, and Firewall Protection.

If you want the gateway to exclude your selected filters to certain computers on your LAN, enter their MAC addresses in the Trusted Computers area of this page.

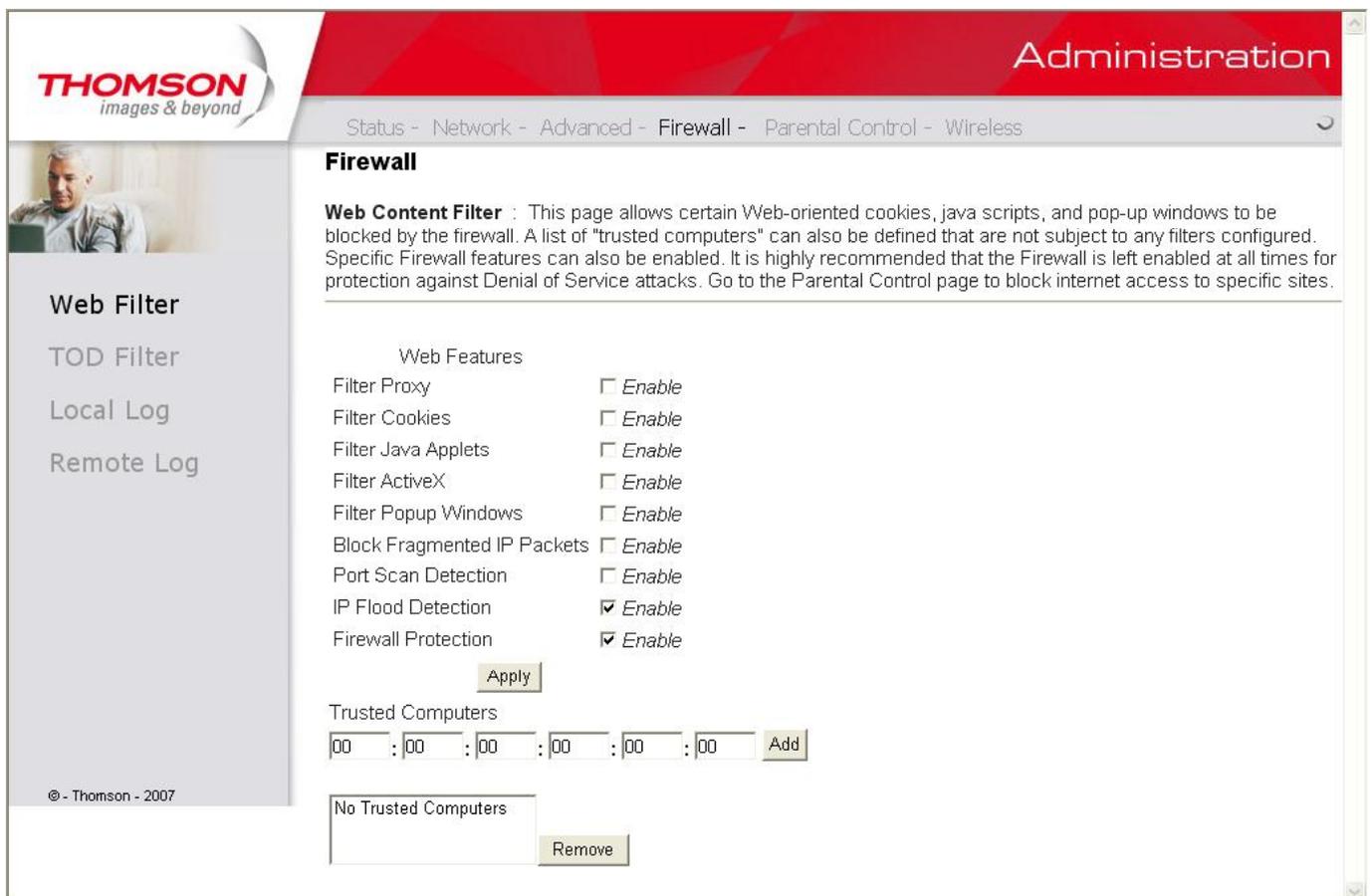


Fig. 25

# Chapter 2: WEB Configuration

## 2. TOD Filtering

Use this page to set rules that will block specific LAN side PCs from accessing the Internet, but only at specific days and times. Specify a PC by its hardware MAC address, and then use the tools to specify blocking time. Finally, click the Apply button to save your settings.

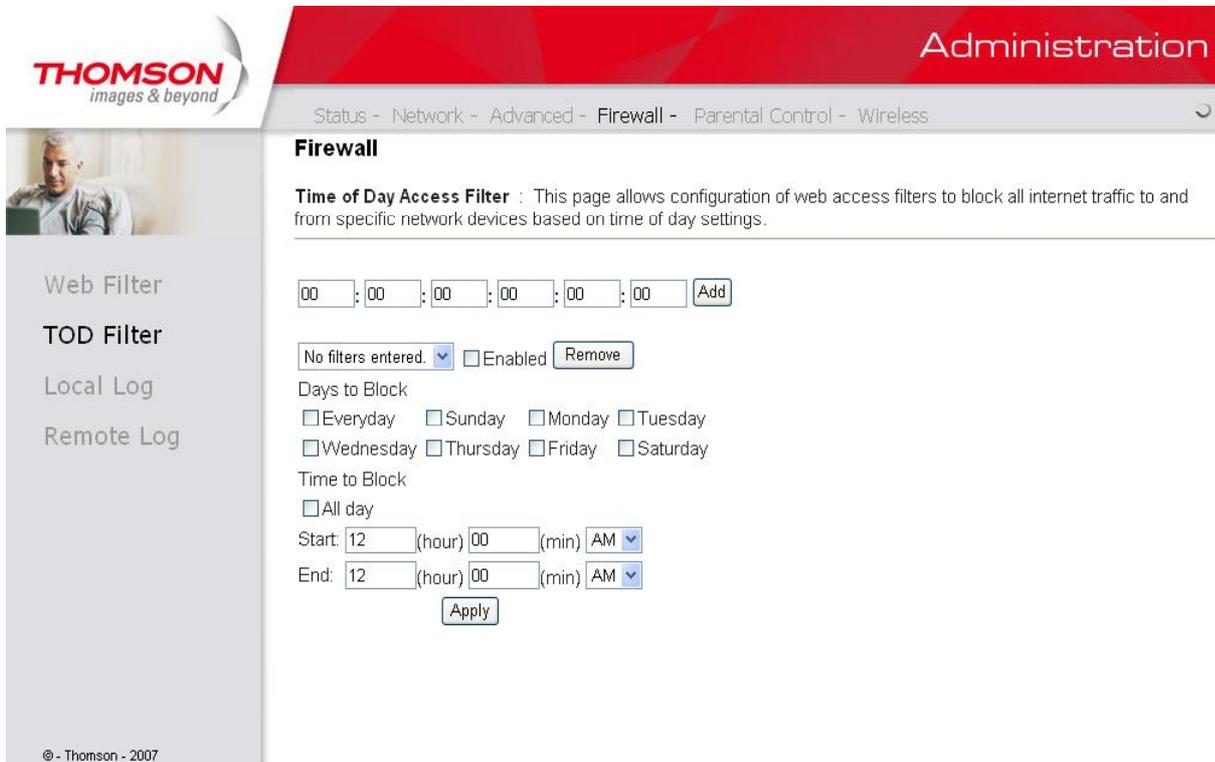


Fig. 26

# Chapter 2: WEB Configuration

## 3. Local Log and Remote Log

The gateway builds a log of firewall blocking actions that Firewall has taken. Using the Local Log page lets you specify an email address to which you want the gateway to email this log. You must also tell the gateway your outgoing (i.e. SMTP) email server's name, so it can direct the email to it. Enable Email Alerts has the gateway forward email notices when Firewall protection events occur. Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

The log of these events is also visible on the screen. For each blocking event type that has taken place since the table was last cleared, the table shows Description, Count, Last Occurrence, Target, and Source.

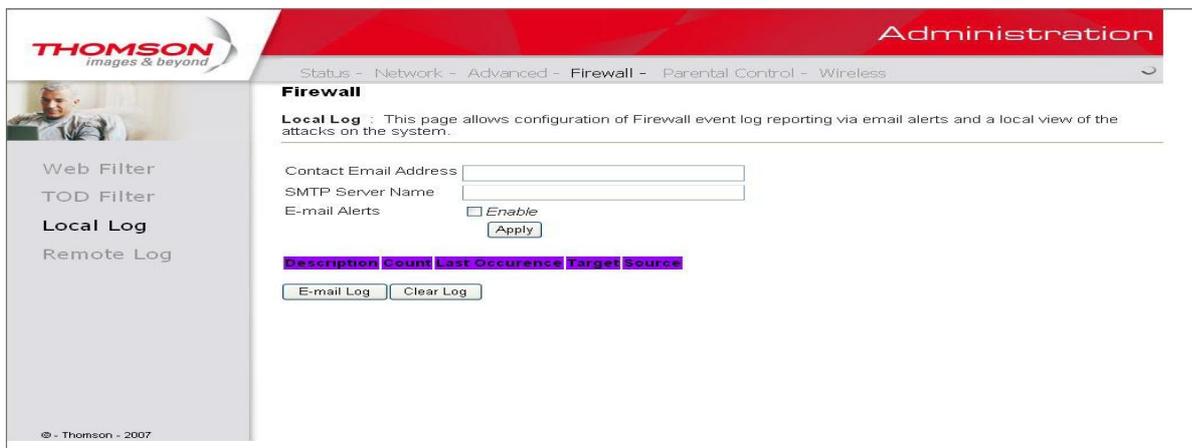


Fig. 27

The Remote Log page allows you to specify the IP address where a SysLog server is located and select different types of firewall events that may occur. Then, each time such an event occurs, notification is automatically sent to this log server.

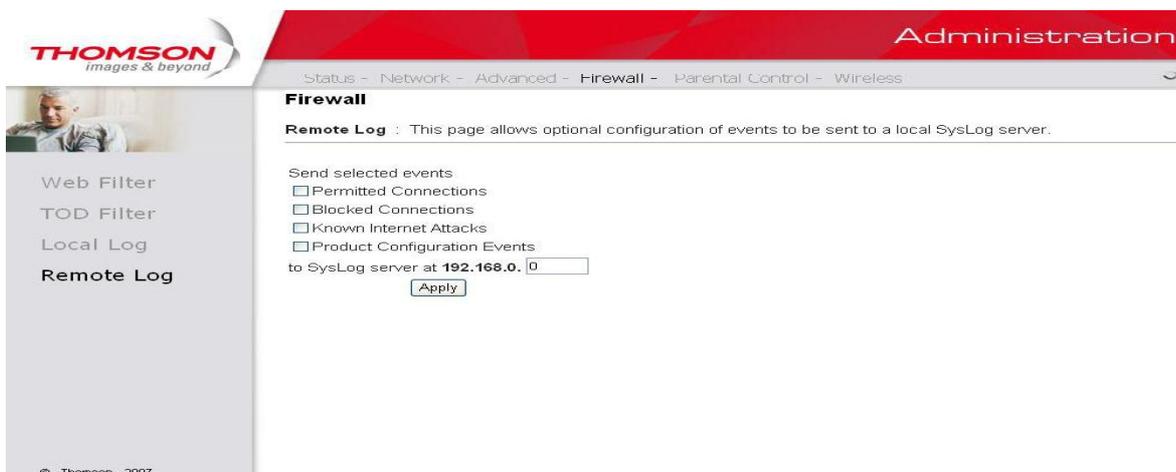


Fig. 28

# Chapter 2: WEB Configuration

## Parental Control

### 1. Basic

This page allows you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking Apply.

Here are some of your choices on the Parental Control page:

- ◆ Activate **Keyword Blocking** and specify some keywords in the Keyword List to cause blocking of web pages on the WAN side with the specified keyword in the content.
- ◆ Activate **Domain Blocking** and specify some Domain Names (e.g. disney.com) in the Domain List.

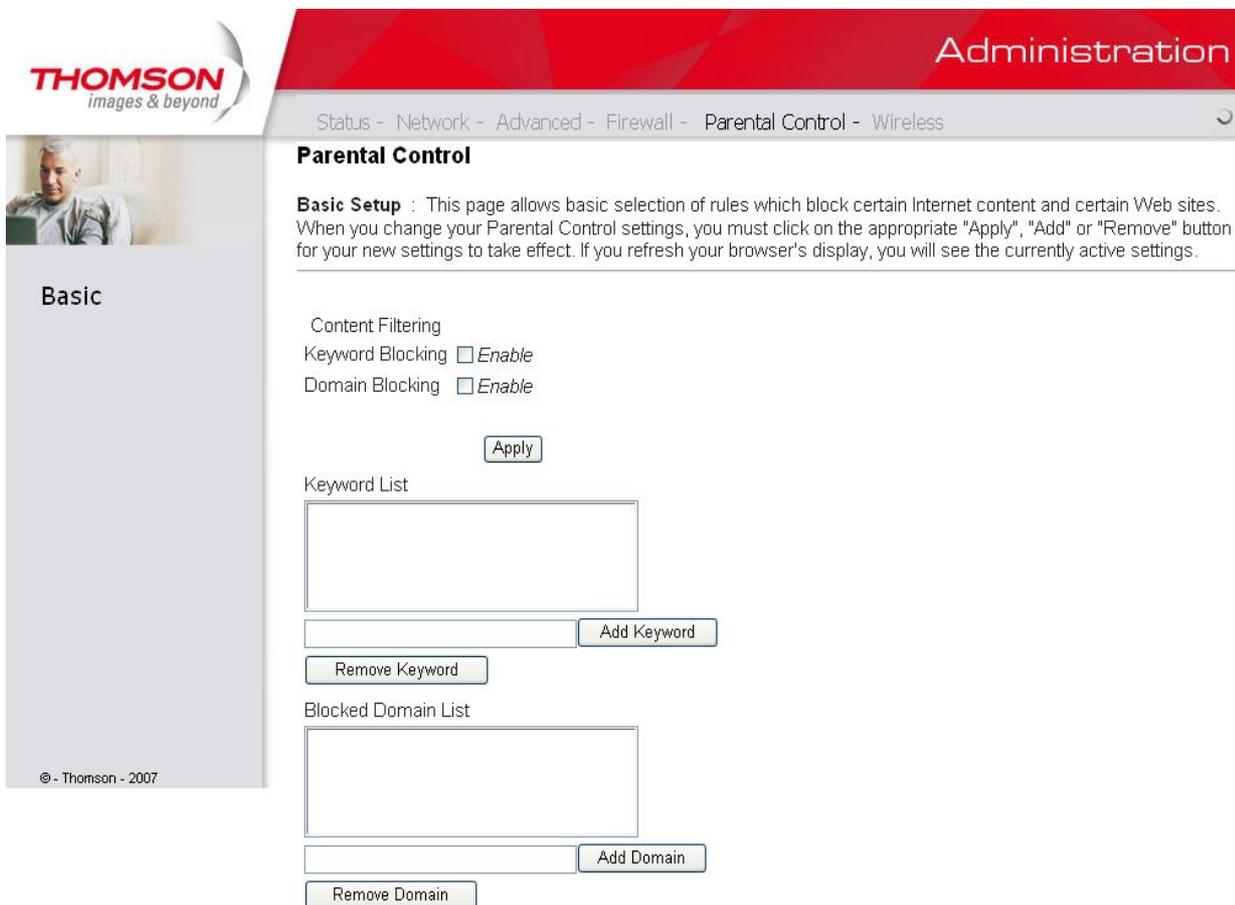


Fig. 29

# Chapter 2: WEB Configuration

## Wireless

---

*Important: Changes to the wireless web pages should be made from a PC that is hard wired to the gateway, i.e. via Ethernet.*

The Wireless web pages group enables a variety of settings that can provide secure and reliable wireless communications for even the most demanding tech-savvy user.

The TCW770 gateway offers a choice of 802.1x, WPA and WPA-PSK authentication of your PCs to the gateway, 64 and 128 bit WEP encryption of communication between the gateway and your PCs to guaranty security, and an Access Control List function that enables you to restrict wireless access to only your specific PCs.

The wireless function will probably work in your home as shipped from the factory. In addition, the factory default wireless channel setting may not provide optimum changes are recommended from the factory defaults, to secure your wireless communications and provide optimum performance.

### **Performance**

Because your wireless communication travels through the air, the factory default wireless channel setting may not provide optimum performance in your home if you or your neighbors have other interfering 2.4GHz devices such as cordless phones. If your wireless PC is experiencing very sluggish or dramatically slower communication compared with the speed you achieve on your PC that is wired to the gateway, try changing the channel number. See the 802.11b/g Radio Web Page discussion below for details.

### **Authentication**

Authentication enables you to restrict your gateway from communicating with any remote wireless PCs that aren't yours. The following minimum authentication-related changes to factory defaults are recommended. See the 802.11b/g Radio and Access Control Web Page discussions below for details.

Network Name (SSID) – Set a unique name you choose

Network Type – Set to Open

Access Control List – Enter your wireless PCs' MAC addresses

### **Security**

Security secures or scrambles messages traveling through the air between your wireless PCs and the gateway, so they can't be observed by others. The following minimum security setting changes to factory defaults are recommended. See the 802.11b/g Primary Network Web Page discussion below for details.

Data Encryption – Set to WEP (64-bit)

PassPhrase – Use this feature to generate security keys