



# HomePortal

## Firewall Monitor Enhanced Service



**User's Guide**

# Contents

<b>Overview</b> .....	1
<b>Getting Started</b> .....	1
<b>Updating Your Firewall Rules</b> .....	2
<b>Viewing Firewall Monitor Attack Alerts</b> .....	2
Viewing Top Attackers .....	3
Understanding the Attacks Blocked Area .....	4
Understanding the Firewall Rule Database Area .....	5
Configuring Attack Alerts .....	6
Enabling Attack Notification .....	6
Configuring Notification Rules .....	7
Email Notification .....	8

## Notice to Users

©2002 2Wire, Inc. All rights reserved. This manual in whole or in part, may not be reproduced, translated, or reduced to any machine-readable form without prior written approval.

2WIRE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR SUCH OTHER INFORMATION, IN NO EVENT SHALL 2WIRE, INC. BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

2Wire, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein is governed by the terms of a separate user license agreement.

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions.

2Wire™, the 2Wire logo, OfficePortal™, and HomePortal™ are trademarks of 2Wire, Inc. All other trademarks are trademarks of their respective owners.

# Firewall Monitor Overview

Your HomePortal™ includes a powerful, professional-grade firewall, featuring two levels of security to help protect your computer(s) from destructive hacker attacks. The firewall actively detects and defends against common Internet threats, such as Distributed Denial of Service attacks using Stateful Packet Inspection, providing exceptional protection. But Internet attacks are created every day. The Firewall Monitor enhanced service helps protect you against these new attacks.

Firewall Monitor enhanced service extends beyond the professional-grade firewall capabilities of your HomePortal. Firewall Monitor provides ongoing software updates assist in protecting your computer(s) from the latest Internet threats while providing detailed logs and notification when attacks are launched against you.

Firewall Monitor:

- Automatically updates your firewall software to help protect against new threats.
- Provides on-screen or email notification to alert you of attacks.
- Provides details about attacks blocked and the source of those attacks.

## Getting Started

The Firewall Monitor service appears as an option on the right-hand side of your HomePortal user interface (<http://homeportal>) (Figure 1).

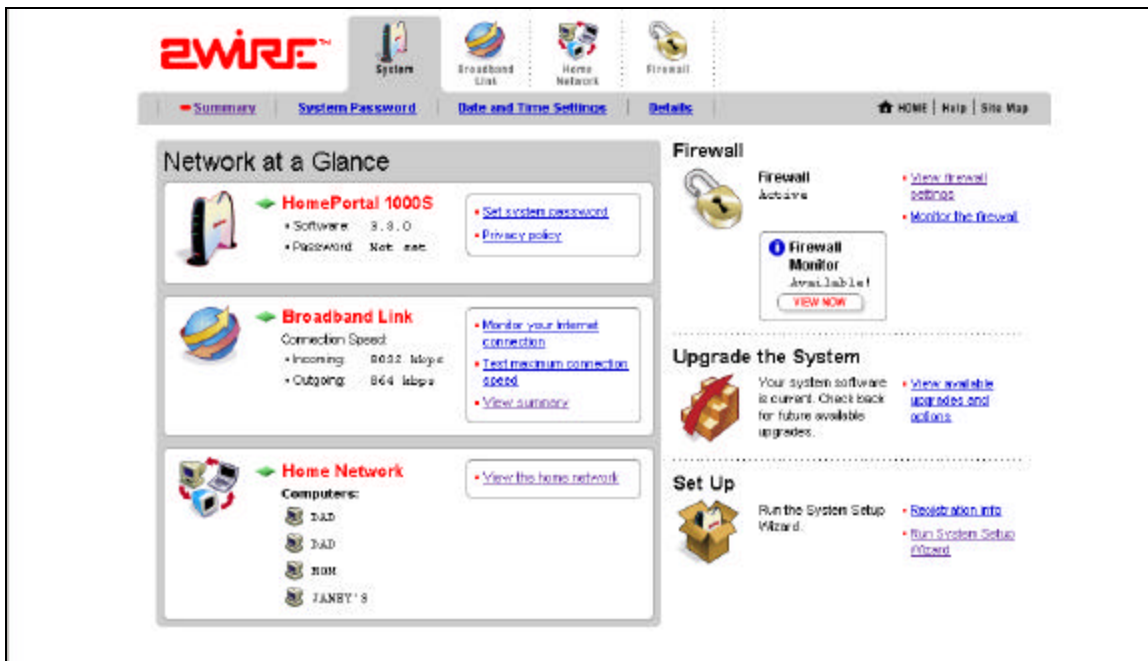


Figure 1

# Updating Your Firewall Rules

Updated firewall rules are automatically downloaded to your HomePortal. The Firewall Monitor application typically checks for new updates every 24 hours.

For more information on how to view the Firewall Rule Database log, see “Understanding the Firewall Rule Database Area” section.

# Viewing Firewall Monitor Attack Alerts

After setting up alert notification, if your firewall is attacked meeting the criteria set, notice of the attack is provided on the HomePortal user interface home page, in the Firewall area.

**Note:** For information on configuring alert notification, see “Configuring Attack Alerts” section.

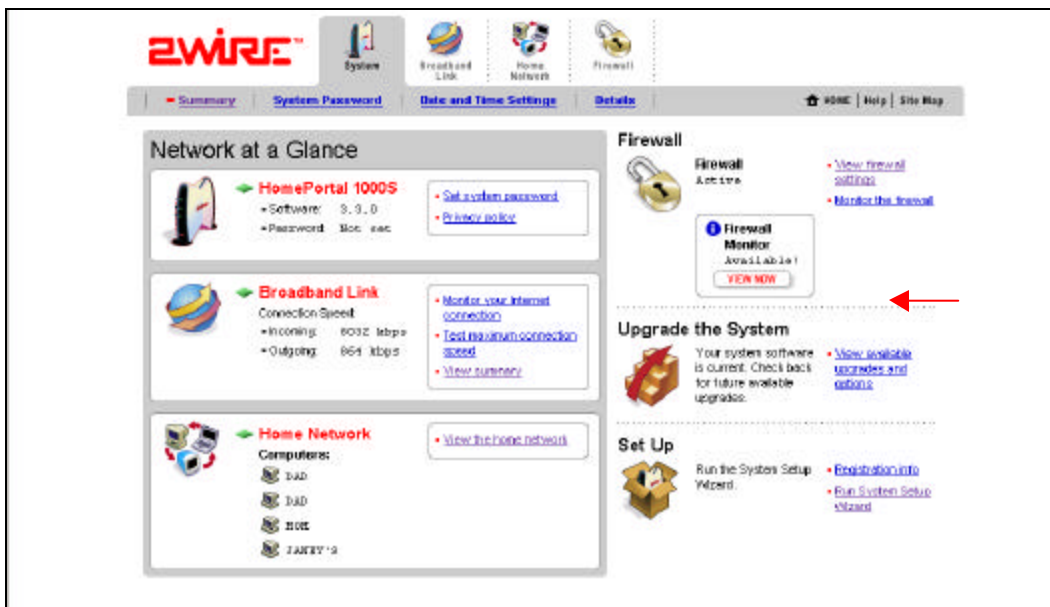


Figure 2

To view the attack alert, click the **VIEW NOW** button (Figure 2).

The *Monitor Your Firewall* page opens (Figure 3).

## Monitor Your Firewall

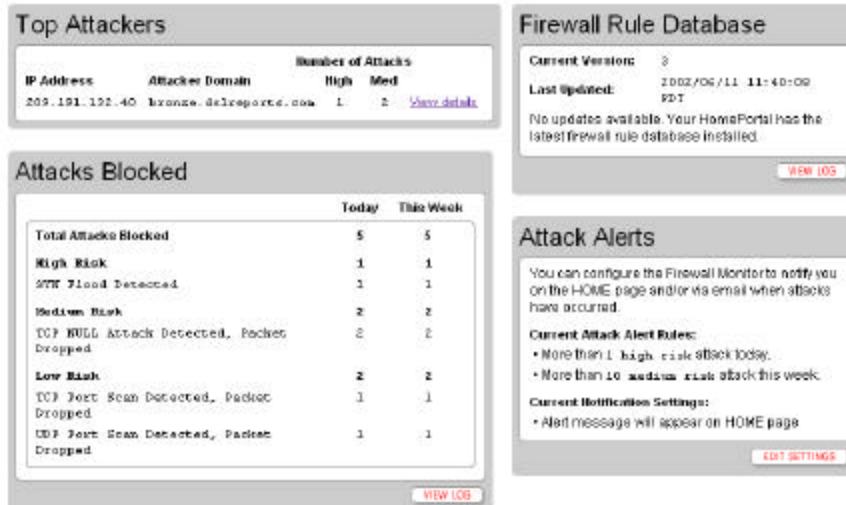


Figure 3

The *Monitor Your Firewall* page contains four areas:

- Top Attackers
- Attacks Blocked
- Firewall Rule Database
- Attack Alerts

### Viewing Top Attackers

The Top Attackers area of the *Monitor Your Firewall* page displays the IP address and domain of each top attacker (Figure 4).



Figure 4

The attackers are ranked based on the number and severity of attacks. To see the details of a particular top attacker, click the **View Details** link of the attacker you wish to view (Figure 4). The *View Attacker Details* page opens (Figure 5).

## View Attacker Details



The screenshot shows a window titled "Details" with the following information:

Internet Domain: bronze.dslreports.com  
Internet Address: 209.191.192.40

	Today	This Week
<b>Total Attacks Blocked</b>	5	5
<b>High Risk</b>	1	1
SYN Flood Detected	1	1
<b>Medium Risk</b>	2	2
TCP NULL Attack Detected, Packet Dropped	2	2
<b>Low Risk</b>	2	2
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

A "DONE" button is visible in the bottom right corner of the window.

Figure 5

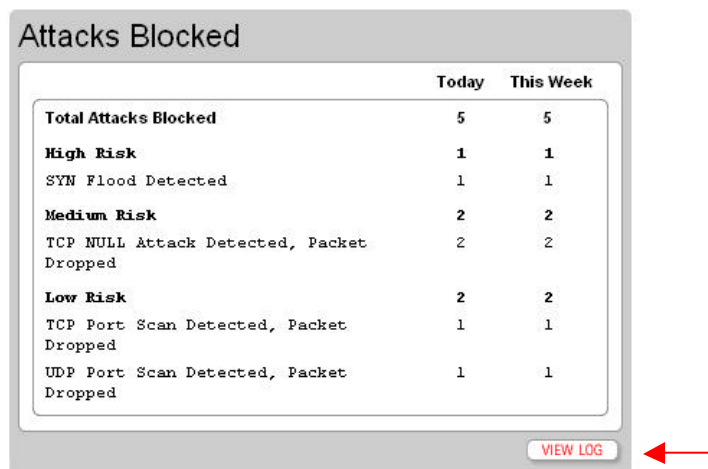
The *View Attackers Details* page shows you the following attack categories and the number of each type of attack that was blocked today and this week:

- Total attacks blocked
- High risk attacks—Indicates blocked attacks that represent a serious attempt by the attacker to disable your firewall protection.
- Medium risk attacks—Indicates blocked attacks that represent a modest level of intent by the attacker to disable your firewall protection.
- Low risk attacks—Indicates blocked attacks that represent no serious threat to disable your firewall protection. Typically, these are probing attacks used by hackers to determine those computers connected to the Internet on which a more serious attack will be conducted.

When you are finished viewing the log, click **DONE** (Figure 5).

## Understanding the Attacks Blocked Area

The Attacks Blocked area of the *Monitor Your Firewall* page displays summary information about all high, medium, and low risk attacks that were blocked today and this week (Figure 6).



The screenshot shows a window titled "Attacks Blocked" with the following information:

	Today	This Week
<b>Total Attacks Blocked</b>	5	5
<b>High Risk</b>	1	1
SYN Flood Detected	1	1
<b>Medium Risk</b>	2	2
TCP NULL Attack Detected, Packet Dropped	2	2
<b>Low Risk</b>	2	2
TCP Port Scan Detected, Packet Dropped	1	1
UDP Port Scan Detected, Packet Dropped	1	1

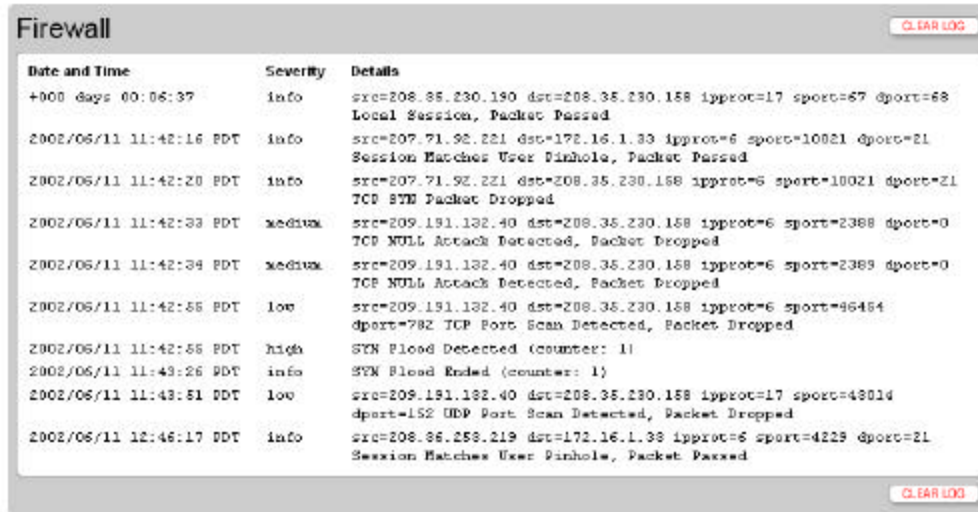
A "VIEW LOG" button is visible in the bottom right corner of the window, with a red arrow pointing to it.

Figure 6

To view details about the blocked attacks, click **VIEW LOG** (Figure 6).

The *View Your Detailed Firewall Log* page opens (Figure 7).

## View Your Detailed Firewall Log



Date and Time	Severity	Details
+000 days 00:06:37	info	src=208.86.230.190 dst=208.35.230.158 ipprot=17 sport=67 dport=68 Local Session, Packet Passed
2002/06/11 11:42:16 PDT	info	src=207.71.92.221 dst=172.16.1.33 ipprot=6 sport=10021 dport=21 Session Matches User Pinhole, Packet Passed
2002/06/11 11:42:20 PDT	info	src=207.71.92.221 dst=208.35.230.158 ipprot=6 sport=10021 dport=21 TCP SYN Packet Dropped
2002/06/11 11:42:33 PDT	medium	src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=2388 dport=0 TCP NULL Attack Detected, Packet Dropped
2002/06/11 11:42:34 PDT	medium	src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=2389 dport=0 TCP NULL Attack Detected, Packet Dropped
2002/06/11 11:42:56 PDT	low	src=209.191.132.40 dst=208.35.230.158 ipprot=6 sport=46454 dport=782 TCP Port Scan Detected, Packet Dropped
2002/06/11 11:42:56 PDT	high	SYN Flood Detected (counter: 1)
2002/06/11 11:43:26 PDT	info	SYN Flood Ended (counter: 1)
2002/06/11 11:43:51 PDT	low	src=209.191.132.40 dst=208.35.230.158 ipprot=17 sport=48014 dport=152 UDP Port Scan Detected, Packet Dropped
2002/06/11 12:46:17 PDT	info	src=208.86.258.219 dst=172.16.1.33 ipprot=6 sport=4229 dport=21 Session Matches User Pinhole, Packet Passed

**Figure 7**

The detail log provides a complete record of firewall activity including additional information about attacks blocked by your firewall. For example, if the Firewall Monitor Summary page indicates that a “SYN Flood” attack has occurred, the detail log will provide information regarding the exact time that the attack began and ended. In addition, the log provides a history of non-attack related actions taken by the firewall. For example, if you configure the firewall to allow specific application data to pass through from the Internet, an entry will be recorded when this type of data is passed to the local network computer.

To clear the log, click **CLEAR LOG** (Figure 7).

To return to the *Monitor Your Firewall* page, click your browser **BACK** button.

## Understanding the Firewall Rule Database Area

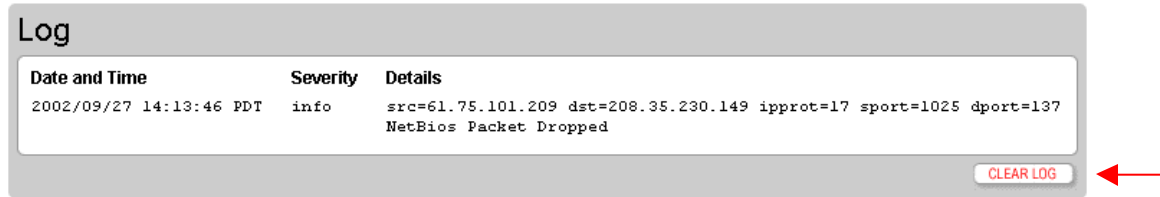
The Firewall Rule Database area of the *Monitor Your Firewall* page shows you the current firewall rules version running on your HomePortal. It also shows you when the rules were last updated (Figure 8).



**Figure 8**

To display the firewall rule database update log, click **VIEW LOG** (Figure 8).

## View Firewall Log



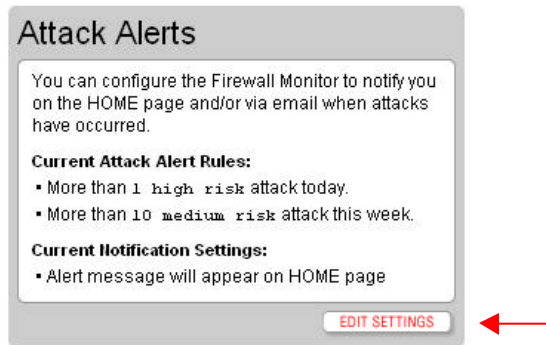
**Figure 9**

The upgrade *Log* page displays information about new downloaded rules including the current version as well as the date and time of the last update.

When you are finished viewing the log, click **CLEAR LOG** (Figure 9).

## Configuring Attack Alerts

The Attack Alerts area of the *Monitor Your Firewall* page shows you the current criteria for posting an alert and how you will be notified of the attack (Figure 10).



**Figure 10**

To configure the Attack Alerts criteria, click **EDIT SETTINGS** (Figure 10).

The *Settings* page for editing attack notification settings opens (Figure 11).

## Edit Attack Notification Settings

The screenshot shows a 'Settings' window with a title bar. Inside, there's a section titled 'Attack Notification' with a red header. Below it is a checkbox labeled 'Enable' which is checked, followed by the text 'Check **ENABLE** for Firewall Monitor attack notification.' Below this is a section titled 'Set Notification Rules' with a red header. It contains the instruction 'Choose up to three situations which will cause a notification message to appear on the HOME page.' followed by three rows of dropdown menus. The first row is 'More than 1 High Risk attack(s) in One day'. The second row is 'More than 10 Medium Risk attack(s) in One week'. The third row is 'More than - Select - - Select - attack(s) in - Select -'. Below this is a section titled 'Email Notification' with a red header. It contains a checkbox labeled 'Enable' which is checked, followed by the text 'Click **ENABLE** to be notified via email when any of the above conditions are met. Then enter the SMTP server information and the email address at which you would like to receive notification messages.' Below this are two text input fields: 'Outgoing SMTP Email Server Name:' and 'Email Address for Alerts:'. A 'TEST' button is located below the second field. At the bottom right of the window are 'SAVE' and 'CANCEL' buttons.

Figure 11

### Enabling Attack Notification

To turn on the attack notification function, make sure the Firewall Monitor attack notification checkbox is checked to enable attack notification (Figure 12). This allows you to be notified of any attacks as determined by your notification rules settings.

If you wish to disable this function, uncheck the checkbox (Figure 12).

#### Attack Notification

**Enable** Check **ENABLE** for Firewall Monitor attack notification.

Figure 12

### Configuring Notification Rules

To be notified of attacks on the home page of the 2Wire HomePortal user interface, you must set up notification rules. You can configure up to three notification rules that will cause a notification message to appear on the HomePortal home page. The following screen shows the default rules (Figure 13).

#### Set Notification Rules

Choose up to three situations which will cause a notification message to appear on the HOME page.

- More than 1 High Risk attack(s) in One day
- More than 10 Medium Risk attack(s) in One week
- More than - Select - - Select - attack(s) in - Select -

Figure 13

Each rule contains the following parameters:

- Number of Attacks—Select the quantity of attacks that have to occur before the notification is sent. Choices include 1, 5, 10, 15, 25, 50, and 100 attacks.
- Type of Attack—Select the type of attack for this notification rule. Choices include high risk, medium risk, and low risk attacks.
- Time Duration—Select the time duration. If the number of attacks specified is exceeded within the chosen duration, you are notified. Choices include one day or one week. A week is defined as Monday at midnight to Sunday at midnight.

When you are finished viewing setting your attack notification criteria, click **SAVE** on the *Settings* page for your notifications rules to take effect (Figure 11).

### Enabling Email Notification

In addition to being notified of attacks on the HomePortal home page, you can be notified via email when one of your attack threshold rules has been exceeded. To receive an email notification when any of the Notification Rule conditions have been met, check the Email Notification Enable checkbox. You must also enter your Outgoing SMTP Email Server Name, mail.bellsouth.net, and the email address that will receive the alerts (Figure 14).

#### Email Notification

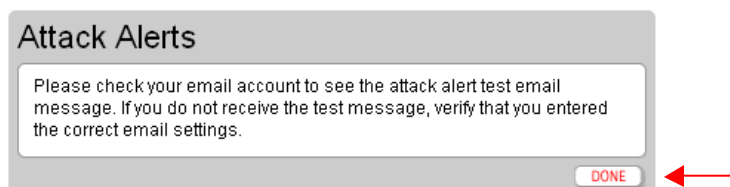
**Enable** Click **ENABLE** to be notified via email when any of the above conditions are met. Then enter the SMTP server information and the email address at which you would like to receive notification messages.

**Outgoing SMTP Email Server Name:**

**Email Address for Alerts:**

Figure 14

To test the email information, click **TEST** (Figure 14). You are prompted with a message indicating that your test message has been sent.



Click **DONE** on the *Settings* page to be returned to the *Monitor Your Firewall* page (Figure 11).