Firewall Monitor

Contents

Notice to Users

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.

5100-000338-000 Rev A 06/05

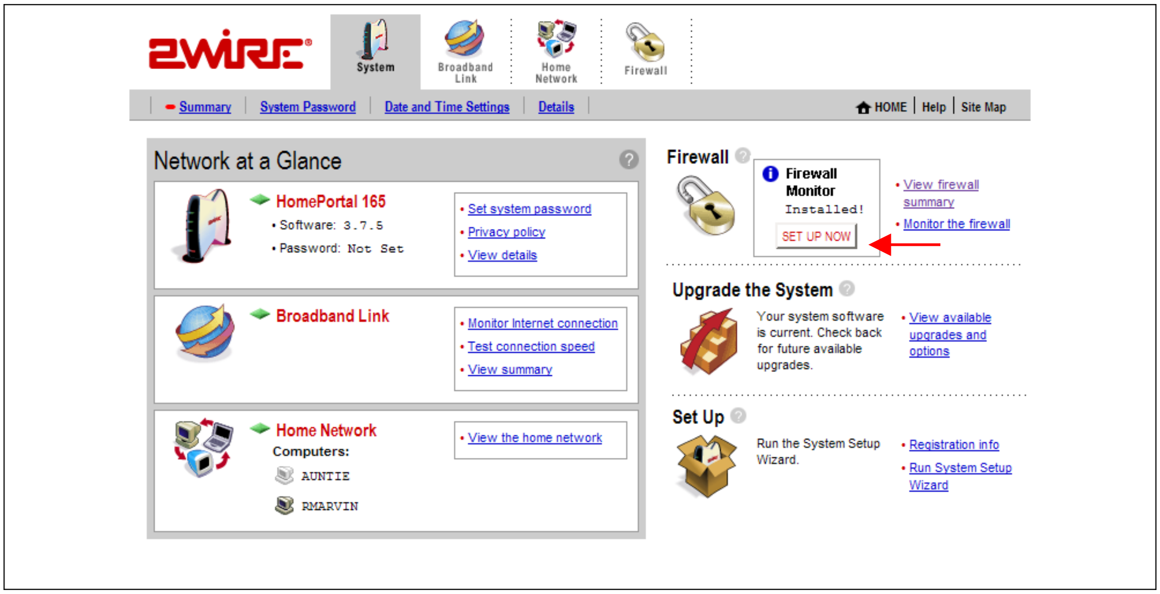
Firewall Monitor Overview

The 2Wire® Firewall Monitor enhanced service extends the professional-grade firewall capabilities of your 2Wire Gateway by continuously assessing threats to your home network. Using the Firewall Monitor service, you can:

- Automatically download updates to your firewall software to protect against new threats.
- Receive on-screen notification to alert you of network attacks.
- Review details about attacks blocked and the source of the attacks.

Getting Started

After you have downloaded the latest firmware version, you can begin configuring the Firewall Monitor by clicking **SET UP NOW**.



- Software: 3.7.5
- Password: Not Set

Computers:
AUNTIE
RMARVIN

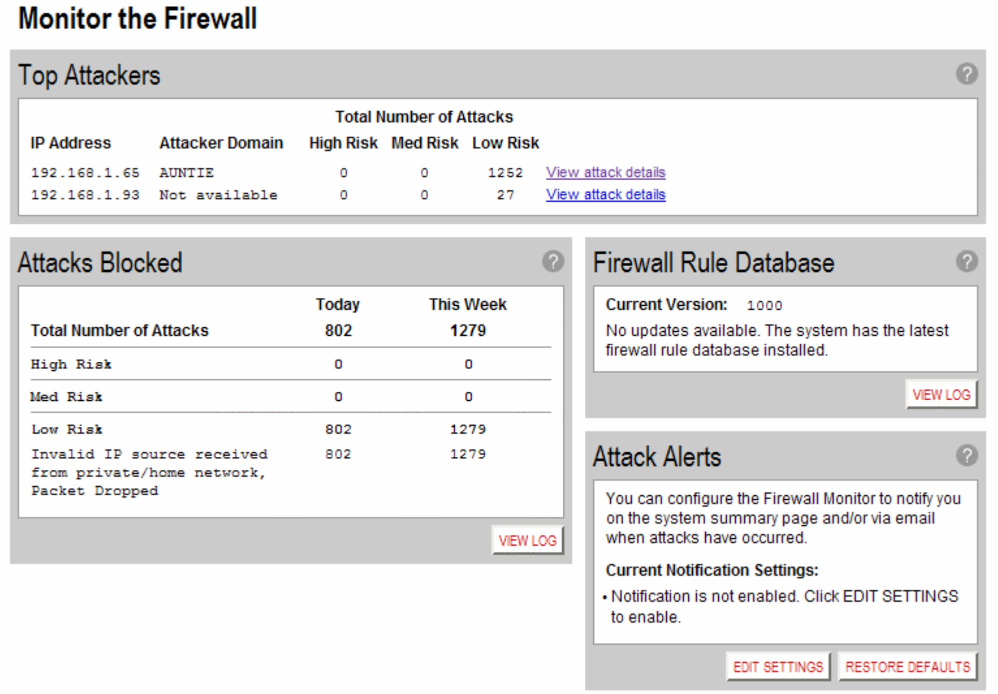
Firewall Monitor Installed!

Your system software is current. Check back for future available upgrades.

Run the System Setup Wizard.

Figure 1

Click the **SET UP NOW** button to display the Monitor the Firewall page (Figure 1) where you can customize these settings for your firewall.



Monitor the Firewall

Top Attackers

		Total Number of Attacks			
IP Address	Attacker Domain	High Risk	Med Risk	Low Risk	
192.168.1.65	AUNTIE	0	0	1252	View attack details
192.168.1.93	Not available	0	0	27	View attack details

Attacks Blocked

	Today	This Week
Total Number of Attacks	802	1279
High Risk	0	0
Med Risk	0	0
Low Risk	802	1279
Invalid IP source received from private/home network, Packet Dropped	802	1279

Firewall Rule Database

Current Version: 1000

No updates available. The system has the latest firewall rule database installed.

Attack Alerts

You can configure the Firewall Monitor to notify you on the system summary page and/or via email when attacks have occurred.

Current Notification Settings:

- Notification is not enabled. Click EDIT SETTINGS to enable.

Figure 2

Setting Up Firewall Monitor Attack Alerts

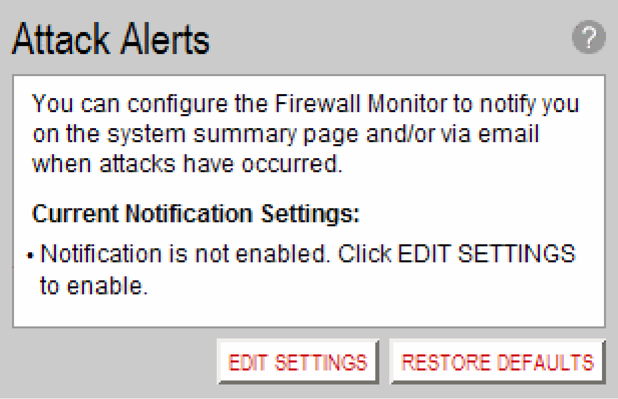
The Attack Alerts area of the Monitor the Firewall page shows you the current criteria for posting an alert and how you will be notified of the attack.

The Monitor the Firewall page contains four areas:

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

Configuring/Editing Attack Alerts

To configure the Attack Alerts criteria, click **EDIT SETTINGS** (Figure 3).



Attack Alerts

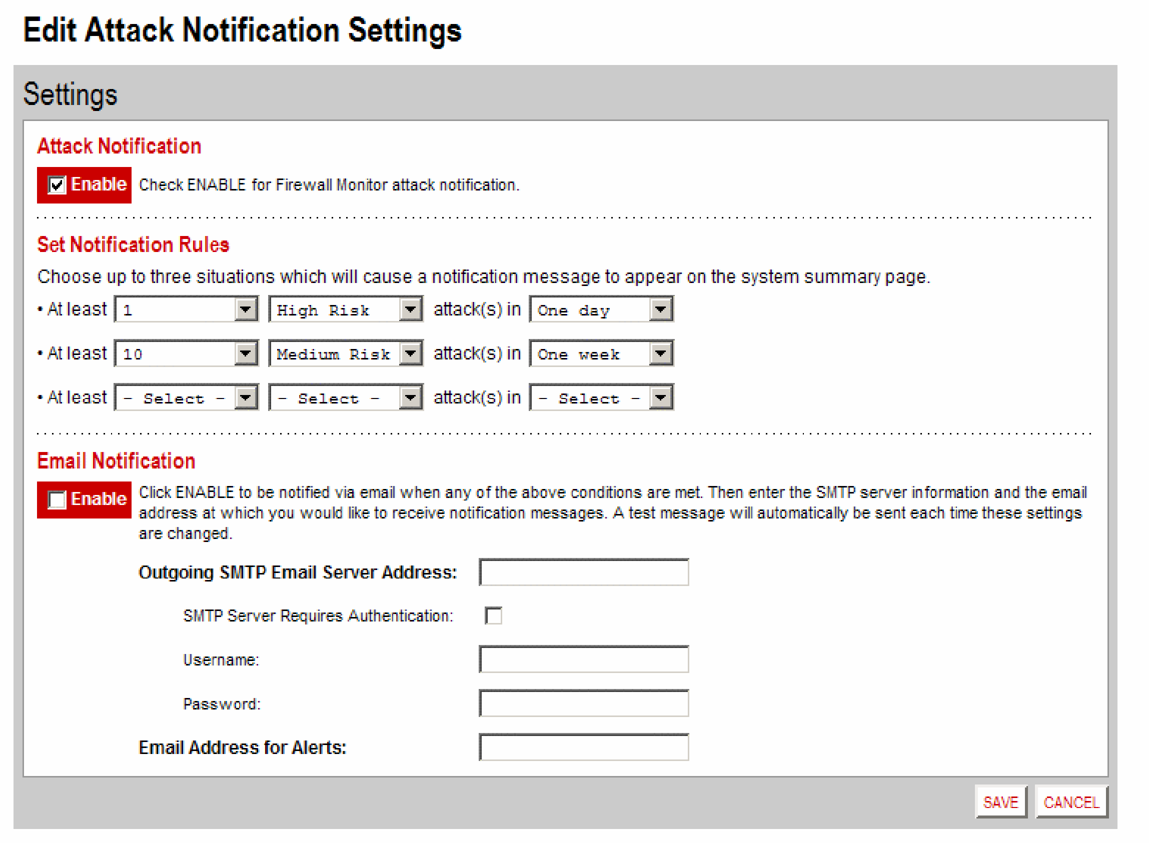
You can configure the Firewall Monitor to notify you on the system summary page and/or via email when attacks have occurred.

Current Notification Settings:

- Notification is not enabled. Click EDIT SETTINGS to enable.

Figure 3

The Edit Attack Notification Settings page opens (Figure 4).



Edit Attack Notification Settings

Settings

Attack Notification

☑ Enable Check ENABLE for Firewall Monitor attack notification.

Set Notification Rules

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

- At least 1 High Risk attack(s) in One day
- At least 10 Medium Risk attack(s) in One week
- At least - Select - - Select - attack(s) in - Select -

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. A test message will automatically be sent each time these settings are changed.

Outgoing SMTP Email Server Address:

SMTP Server Requires Authentication: ☐

Username:

Password:

Email Address for Alerts:

Figure 4

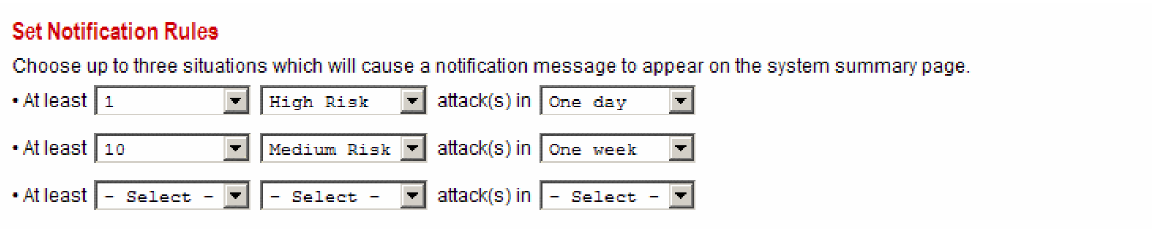
Enabling Attack Notification

To turn on the attack notification function, check the Attack Notification **Enable** checkbox. If you wish to disable this function, uncheck the checkbox.

When you are finished setting your attack notification criteria, click **SAVE** for your notification rules to take effect.

Configuring Notification Rules

To be notified of attacks on the home page of the 2Wire 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 2Wire Gateway home page. The following screen shows the default rules.



Set Notification Rules

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

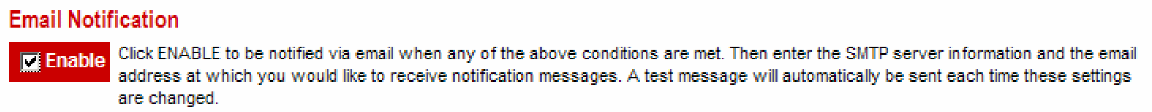
- At least 1 High Risk attack(s) in One day
- At least 10 Medium Risk attack(s) in One week
- At least - Select - - Select - attack(s) in - Select -

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.

Enabling Email Notification

In addition to being notified of attacks on the 2Wire Gateway 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, (which can be found by going to http://help.sbcglobal.net. Go to the “Email” section, click on Set Up, then click on POP, SMTP and NNTP server settings), your SBC/Yahoo member ID, SBC password and the email address that will receive the alerts." .



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. A test message will automatically be sent each time these settings are changed.

Click **SAVE** to return to the Monitor the Firewall page.

Restoring Defaults

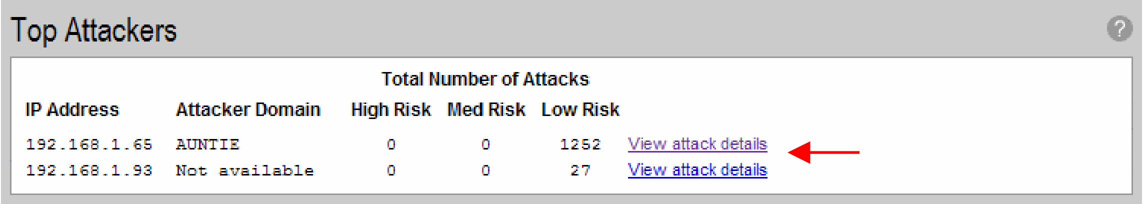
To restore the default settings for Attack Notification and Email Notification, click the **RESTORE DEFAULTS** button in the Attack Alerts area of the Monitor the Firewall page.

Viewing Firewall Monitor Attack Alerts

After setting up alert notification, if your network firewall is attacked meeting the criteria set, notice of the attack is provided on the 2Wire Gateway user interface home page.

Viewing Top Attackers

The Top Attackers area of the Monitor the Firewall page (Figure 5) displays the IP address and domain of each top attacker.



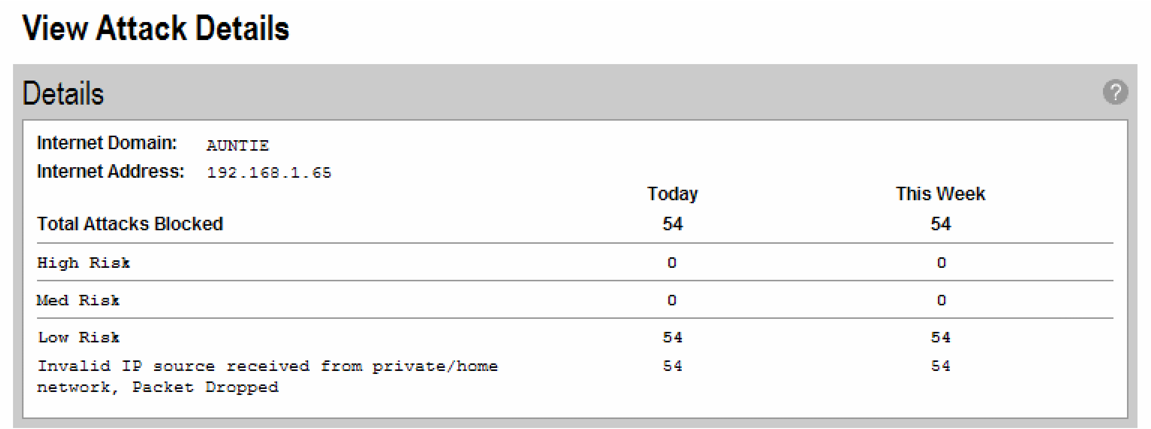
Top Attackers

		Total Number of Attacks			
IP Address	Attacker Domain	High Risk	Med Risk	Low Risk	
192.168.1.65	AUNTIE	0	0	1252	View attack details
192.168.1.93	Not available	0	0	27	View attack details

Figure 5

The attackers are ranked based on the number and severity of attacks. To see the details of a particular top attacker, click the **View attack details** link.

The View Attack Details page opens (Figure 6).



View Attack Details

Details

Internet Domain: AUNTIE

Internet Address: 192.168.1.65

	Today	This Week
Total Attacks Blocked	54	54
High Risk	0	0
Med Risk	0	0
Low Risk	54	54
Invalid IP source received from private/home network, Packet Dropped	54	54

Figure 6

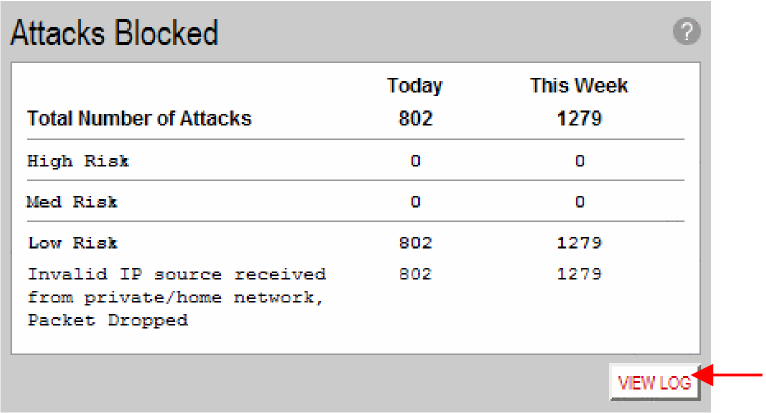
The View Attack Details page shows you the total attacks blocked, and the number of each type of attack that was blocked today and this week:

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

When you are finished viewing the log, click your browser **BACK** button.

Understanding the Attacks Blocked Area

The Attacks Blocked area of the Monitor the Firewall page (Figure 7) displays summary information about all high, medium, and low risk attacks that were blocked today and this week.

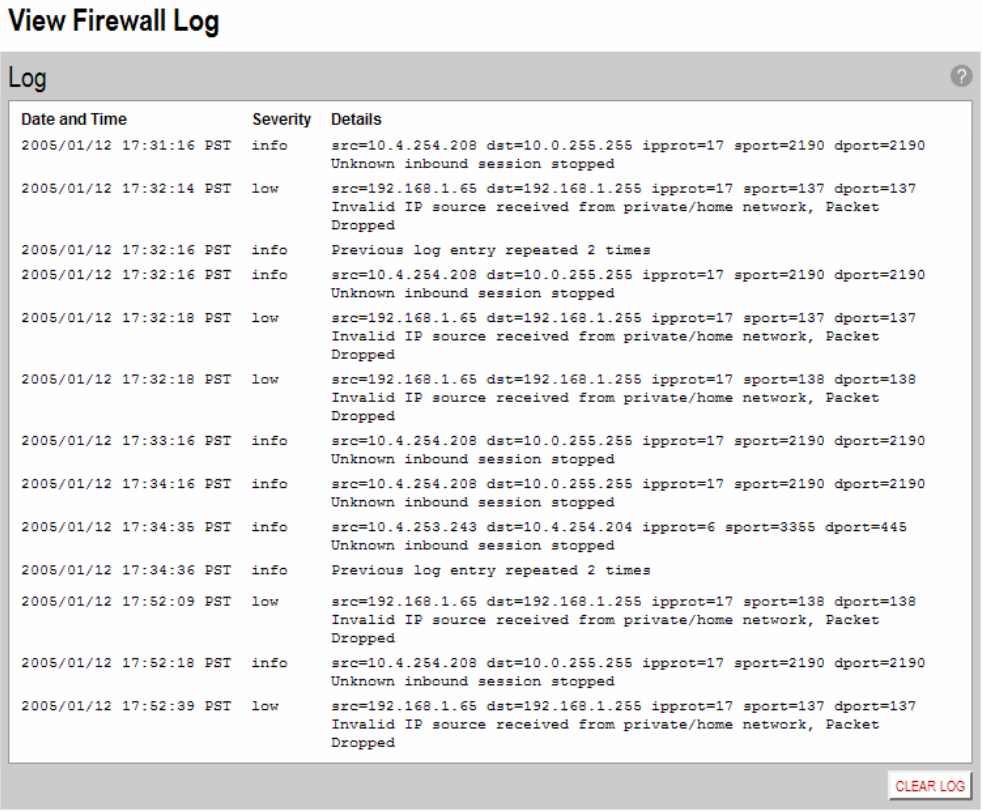


Attacks Blocked

	Today	This Week
Total Number of Attacks	802	1279
High Risk	0	0
Med Risk	0	0
Low Risk	802	1279
Invalid IP source received from private/home network, Packet Dropped	802	1279

Figure 7

To view details about the blocked attacks, click **VIEW LOG**. The View Firewall Log page opens (Figure 8).



View Firewall Log

Log

```
Date and Time            Severity  Details
2005/01/12 17:31:16 PST  info      src=10.4.254.208 dst=10.0.255.255 ipprot=17 sport=2190 dport=2190
                                   Unknown inbound session stopped
2005/01/12 17:32:14 PST  low       src=192.168.1.65 dst=192.168.1.255 ipprot=17 sport=137 dport=137
                                   Invalid IP source received from private/home network, Packet
                                   Dropped
2005/01/12 17:32:16 PST  info      Previous log entry repeated 2 times
2005/01/12 17:32:16 PST  info      src=10.4.254.208 dst=10.0.255.255 ipprot=17 sport=2190 dport=2190
                                   Unknown inbound session stopped
2005/01/12 17:32:18 PST  low       src=192.168.1.65 dst=192.168.1.255 ipprot=17 sport=137 dport=137
                                   Invalid IP source received from private/home network, Packet
                                   Dropped
2005/01/12 17:32:18 PST  low       src=192.168.1.65 dst=192.168.1.255 ipprot=17 sport=138 dport=138
                                   Invalid IP source received from private/home network, Packet
                                   Dropped
2005/01/12 17:33:16 PST  info      src=10.4.254.208 dst=10.0.255.255 ipprot=17 sport=2190 dport=2190
                                   Unknown inbound session stopped
2005/01/12 17:34:16 PST  info      src=10.4.254.208 dst=10.0.255.255 ipprot=17 sport=2190 dport=2190
                                   Unknown inbound session stopped
2005/01/12 17:34:35 PST  info      src=10.4.253.243 dst=10.4.254.204 ipprot=6 sport=3355 dport=445
                                   Unknown inbound session stopped
2005/01/12 17:34:36 PST  info      Previous log entry repeated 2 times
2005/01/12 17:52:09 PST  low       src=192.168.1.65 dst=192.168.1.255 ipprot=17 sport=138 dport=138
                                   Invalid IP source received from private/home network, Packet
                                   Dropped
2005/01/12 17:52:18 PST  info      src=10.4.254.208 dst=10.0.255.255 ipprot=17 sport=2190 dport=2190
                                   Unknown inbound session stopped
2005/01/12 17:52:39 PST  low       src=192.168.1.65 dst=192.168.1.255 ipprot=17 sport=137 dport=137
                                   Invalid IP source received from private/home network, Packet
                                   Dropped
```

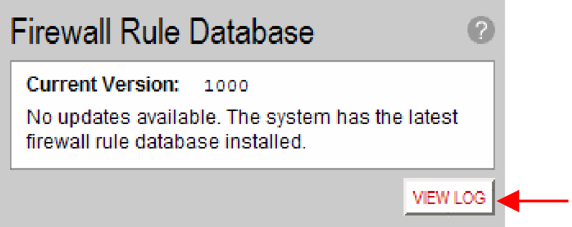
Figure 8

To clear the log, click **CLEAR LOG**.

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

Understanding the Firewall Rule Database Area

The Firewall Rule Database area of the Monitor the Firewall page (Figure 9) shows you the current firewall rules version running on your 2Wire Gateway.



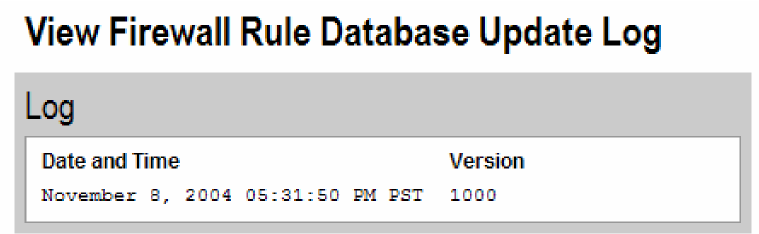
Firewall Rule Database

Current Version: 1000

No updates available. The system has the latest firewall rule database installed.

Figure 9

To display the firewall rule database update log, click **VIEW LOG**.



View Firewall Rule Database Update Log

Log

Date and Time	Version
November 8, 2004 05:31:50 PM PST	1000

Figure 10

The upgrade log (Figure 10) displays the following information about new downloaded rules:

- Date and time
- Version

When you are finished viewing the log, click your browser **BACK** button.

Updating Your Firewall Rules

Updated firewall rules are automatically downloaded to your 2Wire Gateway after you set up the Firewall Monitor service. The Firewall Monitor application typically checks for new updates every 24 hours.