

Chapter 3

Restricting Access From Your Network

This chapter describes how to use the content filtering and reporting features of the Wireless-G Router Model WGR614v9 to protect your network. You can find these features by selecting the items under Content Filtering in the main menu of the browser interface.

This chapter includes the following sections:

- [“Content Filtering Overview”](#)
- [“Blocking Access to Internet Sites”](#)
- [“Blocking Access to Internet Services” on page 3-3](#)
- [“Scheduling Blocking” on page 3-5](#)
- [“Viewing Logs of Web Access or Attempted Web Access” on page 3-7](#)

Content Filtering Overview

The Wireless-G Router Model WGR614v9 provides you with Web content filtering options, plus browser activity reporting and instant alerts through e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as chat rooms or games.

To configure these features of your router, select the items under Content Filtering in the main menu of the browser interface. This chapter describes the screens that display.

Blocking Access to Internet Sites

The Wireless-G Router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL www.zzzyyqq.com/xxx.html is blocked.

- If the keyword **.com** is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.

To block access to Internet sites:

1. Select **Block Sites** under Content Filtering in the main menu. The Block Sites screen displays.

Block Sites

Keyword Blocking

Never
 Per Schedule
 Always

Type keyword or domain name here.

Add Keyword

Block sites containing these keywords or domain names:

discodanny

Delete Keyword Clear List

Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address

Apply Cancel

Figure 3-1

2. Enable keyword blocking by selecting either **Per Schedule** or **Always**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see [“Scheduling Blocking” on page 3-5](#).

Block all access to Internet browsing during a scheduled period by entering a dot (.) as the keyword, and then set a schedule in the Schedule screen.

3. Add a keyword or domain by entering it in the keyword field and clicking **Add Keyword**. The keyword or domain name then appears the **Block sites containing these keywords or domain names** list.

Delete a keyword or domain name by selecting it from the list and clicking **Delete Keyword**.

4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the **Trusted IP Address** fields.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

5. Click **Apply** to save all your settings in the Block Sites screen.

Blocking Access to Internet Services

The Wireless-G Router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To block access to Internet services:

1. Select **Block Services** under Content Filtering in the main menu. The Block Services screen displays.

Figure 3-2

2. Enable service blocking by selecting either **Per Schedule** or **Always**, and then click **Apply**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see “[Scheduling Blocking](#)” on page 3-5.

- Specify a service for blocking by clicking **Add**. The Block Services Setup screen displays.

The screenshot shows the 'Block Services Setup' configuration window. It includes the following fields and options:

- Service Type:** A dropdown menu with 'AIM' selected.
- Protocol:** A dropdown menu with 'TCP' selected.
- Starting Port:** A text input field containing '5190' with a range indicator '(1~65534)' to its right.
- Ending Port:** A text input field containing '5190' with a range indicator '(1~65534)' to its right.
- Service Type/User Defined:** A text input field containing 'AIM'.
- Filter Services For:** A section with three radio button options:
 - Only This IP Address: followed by four input fields containing '192', '168', '1', and an empty field.
 - IP Address Range: followed by two sets of input fields. The first set contains '192', '168', '1', and an empty field. The second set is preceded by 'to' and contains '192', '168', '1', and an empty field.
 - All IP Addresses
- Buttons:** 'Add' and 'Cancel' buttons at the bottom.

Figure 3-3

- From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.
- Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields.
- Click **Add** to enable your Block Services Setup selections.

Configuring a User-Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

- Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

- If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

Blocking Services by IP Address Range

In the Filter Services For area, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking

The Wireless-G Router allows you to specify when blocking is enforced.

To schedule blocking:

1. Select **Schedule** under Content Filtering in the main menu. The Schedule screen displays.

The screenshot shows the 'Schedule' configuration page. It includes the following sections:

- Days to Block:** A list of days with checkboxes: Every Day (checked), Sunday (checked), Monday (checked), Tuesday (checked), Wednesday (checked), Thursday (checked), Friday (checked), and Saturday (checked).
- Time of day to Block:** A section with a checked 'All Day' option and two rows of time pickers. 'Start Blocking' is set to 0 Hour and 0 Minute. 'End Blocking' is set to 24 Hour and 0 Minute.
- Time Zone:** A dropdown menu set to '(GMT-08:00) Pacific Time (US Canada)' and an unchecked checkbox for 'Automatically Adjust for Daylight Savings Time'.
- Current Time:** Thursday, 13 Dec 2007 14:32:27
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

Figure 3-4

2. Configure the schedule for blocking keywords and services.
 - a. **Days to Block.** Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days. Click **Apply**.

b. Time of Day to Block. Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking.

c. Time Zone.

Select the time zone where you are located, and if you prefer to automatically adjust for daylight savings time.



Note: Accurate time zone and daylight savings settings will assure that the scheduling and logging functions operate correctly.

The Wireless-G Router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. To localize the time for your log entries, you must specify your time zone:

- **Time Zone.** Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- **Automatically Adjust for Daylight Savings Time.** Select this check box if your region supports daylight savings time. The router will automatically adjust the time at the start and end of the daylight savings time period.

3. Click **Apply** to save your settings.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **Logs** under Content Filtering in the main menu. The Logs screen displays.

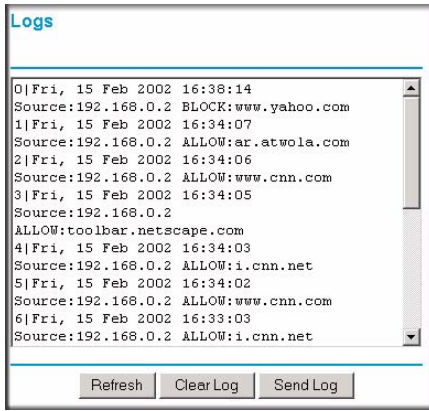


Figure 3-5

[Table 3-1](#) describes the log entries.

Table 3-1. Log Entry Descriptions

Field	Description
Date and time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the website or newsgroup visited or to which access was attempted.
Action	Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

