

Chapter 3

Restricting Access From Your Network

This chapter describes how to use the content filtering and reporting features of the Wireless-N Router Model WNR2000 to protect your network.

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 3-6](#)
- [“Configuring E-mail Alert and Web Access Log Notifications” on page 3-7](#)
- [“Setting the Time Zone” on page 3-9](#)

Content Filtering Overview

The Wireless-N Router Model WNR2000 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.

Blocking Access to Internet Sites

The WNR2000 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 WNR2000 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.

#	Service Type	Port	IP
---	--------------	------	----

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.

Block Services Setup

Service Type: User Defined

Protocol: TCP

Starting Port: (1~65534)

Ending Port: (1~65534)

Service Type/User Defined:

Filter Services For :

Only This IP Address: 192 . 168 . 1 .

IP Address Range: 192 . 168 . 1 . to 192 . 168 . 1 .

All IP Addresses

Apply Cancel

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**. 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**.
- 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.

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 WNR2000 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.

Schedule

Days To Block:

Every day

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Time Of Day To Block: (use 24-hour clock)

All Day

Start Blocking: Hour Min

End Blocking: Hour Min

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. Click **Apply**.

Be sure to select your time zone in the E-mail screen as described in “[Setting the Time Zone](#)” on page 3-9.

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.

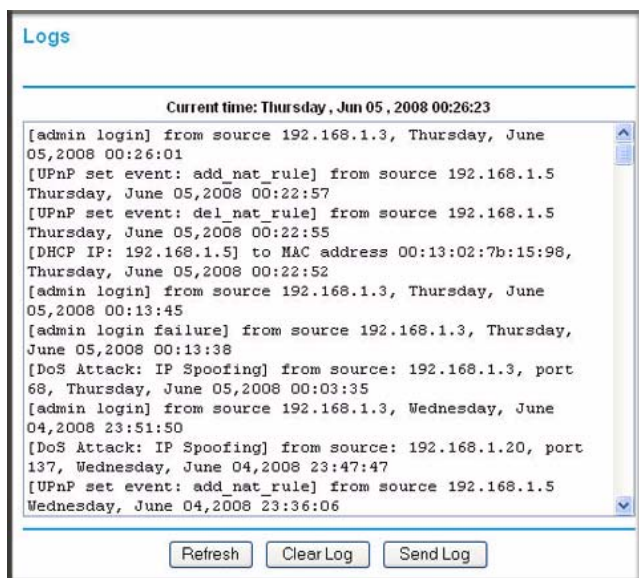


Figure 3-5

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.

Table 3-1. Log Entry Descriptions

Field	Description
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.

To e-mail the log immediately, click the **Send Log** button.

Configuring E-mail Alert and Web Access Log Notifications

To receive logs and alerts by e-mail, you must provide your e-mail account information.

To configure e-mail alert and web access log notifications:

1. Select **E-mail** under Content Filtering in the main menu. The E-mail screen displays.

The screenshot shows the 'E-mail' configuration page. At the top, there is a title 'E-mail' and a checkbox labeled 'Turn E-mail Notification On'. Below this is a section titled 'Send Alerts and Logs Via E-mail' containing several input fields: 'Your Outgoing Mail Server:', 'Send To This E-mail Address:', 'My Mail Server requires authentication' (checkbox), 'User Name', and 'Password'. A second checkbox, 'Send Alert Immediately', is located below these fields, with the text 'When Someone Attempts To Visit A Blocked Site.' underneath it. The next section is 'Send Logs According to this Schedule', which includes a dropdown for 'When Log is Full', a 'Day' dropdown set to 'Sunday', and a 'Time' dropdown set to '0:00' with radio buttons for 'a.m.' and 'p.m.'. Below this is the 'Time Zone' section, featuring a dropdown menu set to '(GMT-08:00) Pacific Time (US & Canada):Tijuana' and a checked checkbox for 'Automatically Adjust for Daylight Savings Time'. At the bottom of this section, it displays 'Current time: Wednesday, Jun 04, 2008 17:46:49'. At the very bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 3-6

2. To receive e-mail logs and alerts from the router, select the **Turn E-mail Notification On** check box.
 - a. Enter the name of your ISP's outgoing (SMTP) mail server (such as **mail.myISP.com**) in the **Your Outgoing Mail Server** field. You might be able to find this information in the configuration screen of your e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail.
 - b. Enter the e-mail address to which logs and alerts are sent in the **Send To This E-mail Address** field. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by e-mail.
3. If your e-mail server requires authentication, select the **My Mail Server requires authentication** check box.
 - a. Enter your user name for the e-mail server in the **User Name** field.

- b. Enter your password for the e-mail server in the **Password** field.
4. You can specify that logs are automatically sent by e-mail with these options:
- **Send alert immediately.** Select this check box for immediate notification of attempted access to a blocked site or service.
 - **Send Logs According to this Schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
 - **Day.** Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
 - **Time.** Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.

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

So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Setting the Time Zone

The WNR2000 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. Localize the time zone so that your log entries and other router functions include the correct time stamp.

To verify and set the time zone (see [Figure 3-6 on page 3-8](#)):

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

