Chapter 5
Protecting Your Network

This chapter describes how to use the basic firewall features of the DG834GT 108 Mbps Super Wireless ADSL Router to protect your network.

Protecting Access to Your DG834GT 108 Mbps Super Wireless ADSL Router

For security reasons, the router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the router User Name and **password** for the router Password. You can use procedures below to change the router's password and the amount of time for the administrator's login timeout.

Note: The user name and password are not the same as any user name or password your may use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

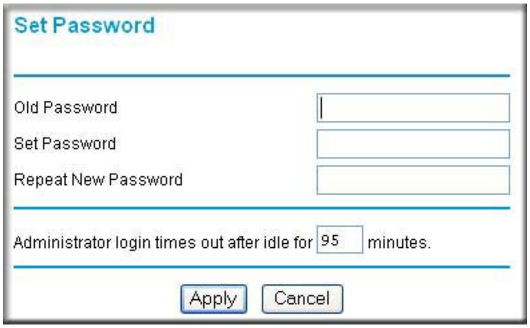
How to Change the Built-In Password

1. Log in to the router at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.

http://192.168.0.1

Figure 5-1: Log in to the router

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in Figure 5-2.



Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for 95 minutes.

Figure 5-2: Set Password menu

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click Apply to save your changes.

Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the router settings previously, you should do a new backup so that the saved settings file includes the new password.

Changing the Administrator Login Timeout

For security, the administrator's login to the router configuration will timeout after a period of inactivity. To change the login timeout period:

1. In the Set Password menu, type a number in ‘Administrator login times out’ field. The suggested default value is 5 minutes.
2. Click Apply to save your changes or click Cancel to keep the current period.

Configuring Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented below.

Blocking Keywords, Sites, and Services

The router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the DG834GT Super Wireless ADSL Router prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

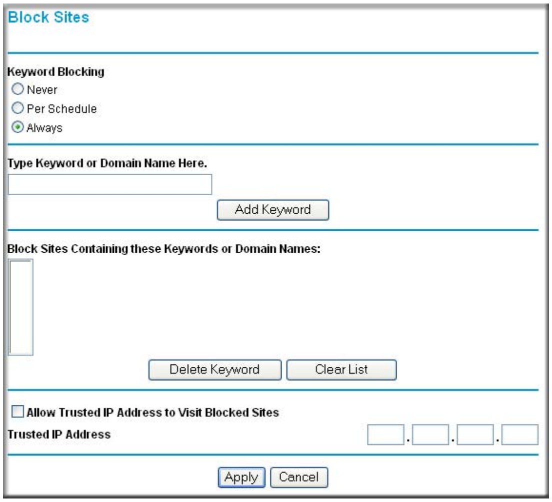
- Keyword blocking of HTTP traffic.
- Outbound Service Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

The section below explains how to configure your router to perform these functions.

How to Block Keywords and Sites

The DG834GT Super Wireless ADSL Router allows you to restrict access to Internet content based on functions such as Web addresses and Web address keywords.

1. Log in to the router at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Block Sites link of the Security menu.



Block Sites

Keyword Blocking

○ Never
○ Per Schedule
● Always

Type Keyword or Domain Name Here.

Block Sites Containing these Keywords or Domain Names:

□ Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address . . .

Figure 5-3: Block Sites menu

3. To enable keyword blocking, select one of the following:
   - Per Schedule—to turn on keyword blocking according to the settings on the Schedule page.
   - Always—to turn on keyword blocking all of the time, independent of the Schedule page.
4. Enter a keyword or domain in the Keyword box, click Add Keyword, then click Apply.

   Some examples of Keyword application follow:
   - If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
   - If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or.gov) can be viewed.
   - Enter the keyword “.” to block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.
5. To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.
6. To specify a trusted user, enter that computer’s IP address in the Trusted IP Address box and click Apply.

   You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

7. Click Apply to save your settings.

Firewall Rules

Firewall rules are used to block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

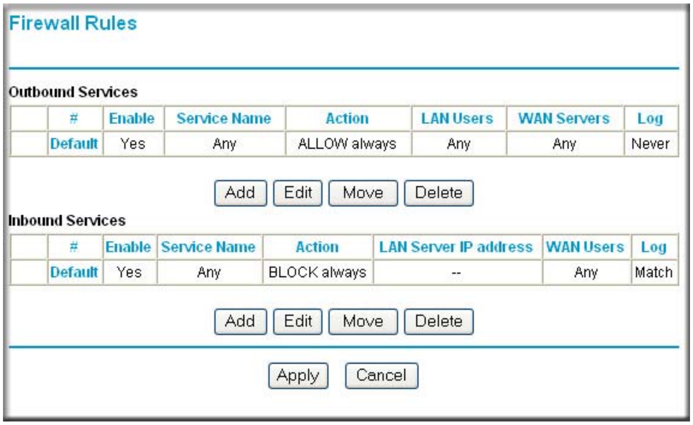
A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the DG834GT are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See "Order of Precedence for Rules" on page 5-11 for more details.

To access the rules configuration of the DG834GT, click the Firewall Rules link on the main menu, then click Add for either an Outbound or Inbound Service.



Firewall Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
	Default	Yes	Any	BLOCK always	--	Any	Match

Figure 5-4: Rules menu

- To edit an existing rule, select its button on the left side of the table and click Edit.
- To delete an existing rule, select its button on the left side of the table and click Delete.
- To move an existing rule to a different position in the table, select its button on the left side of the table and click Move. At the script prompt, enter the number of the desired new position and click OK.

Inbound Rules (Port Forwarding)

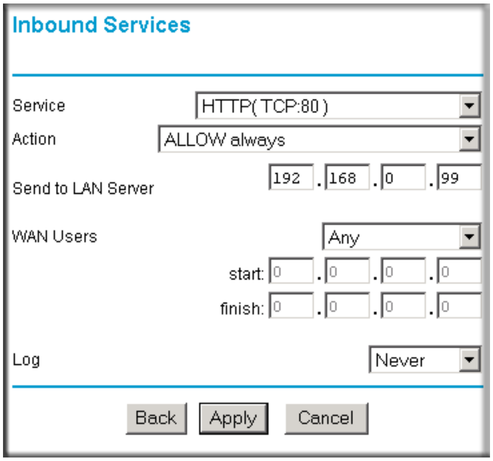
Because the DG834GT uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

> **Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in Figure 5-5:



Inbound Services

Service: HTTP(TCP:80)

Action: ALLOW always

Send to LAN Server: 192 . 168 . 0 . 99

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Never

Figure 5-5: Rule example: A Local Public Web Server

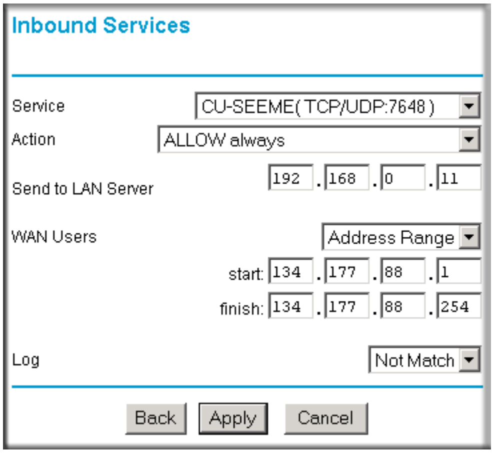
The parameters are:

- Service
  From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- Action
  Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- Send to LAN Server
  Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.

- WAN Users
  These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:
  - Any — all IP addresses are covered by this rule.
  - Address range — if this option is selected, you must enter the Start and Finish fields.
  - Single address — enter the required address in the Start field.
- Log
  You can select whether the traffic will be logged. The choices are:
  - Never — no log entries will be made for this service.
  - Always — any traffic for this service type will be logged.
  - Match — traffic of this type which matches the parameters and action will be logged.
  - Not match — traffic of this type which does not match the parameters and action will be logged.

Inbound Rule Example: Allowing Videoconferencing

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 5-6, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



Inbound Services

Service	CU-SEEME(TCP/UDP:7648)
Action	ALLOW always
Send to LAN Server	192 . 168 . 0 . 11
WAN Users	Address Range
start:	134 . 177 . 88 . 1
finish:	134 . 177 . 88 . 254
Log	Not Match

Figure 5-6: Rule example: Videoconference from Restricted Addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer’s IP address constant.
- Local computers must access the local server using the computer’s local LAN address (192.168.0.11 in the example in Figure 5-6 above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

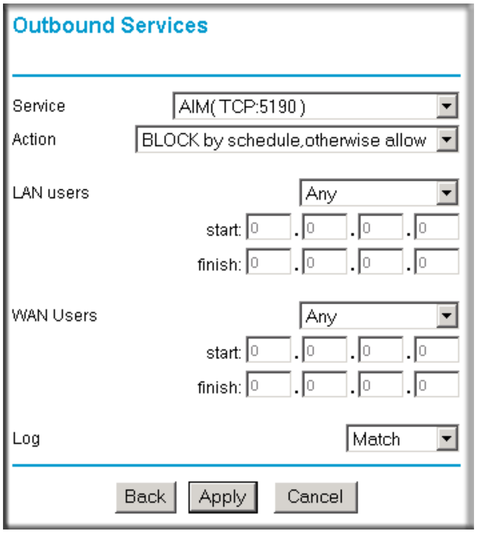
The DG834GT allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the router log any attempt to use Instant Messenger during that blocked period.



Outbound Services

Service: AIM(TCP:5190)

Action: BLOCK by schedule,otherwise allow

LAN users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Match

Figure 5-7: Rule example: Blocking Instant Messenger

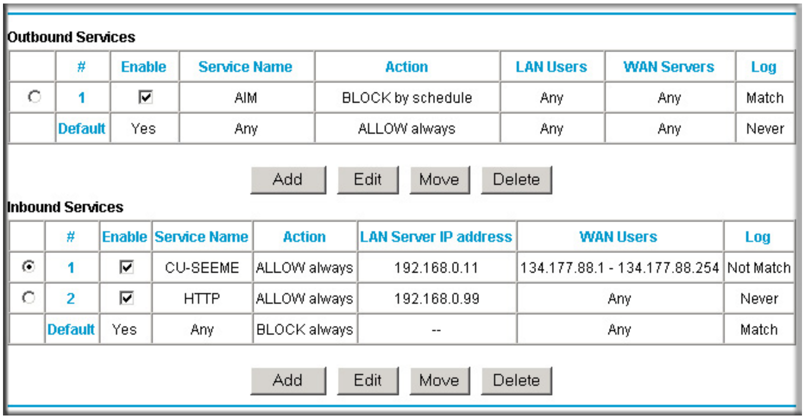
The parameters are:

- Service
  From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Custom Service feature to add any additional services or applications that do not already appear.
- Action
  Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.

- LAN Users
  These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
  - Any — all IP addresses are covered by this rule.
  - Address range — if this option is selected, you must enter the Start and Finish fields.
  - Single address — enter the required address in the Start field.
- WAN Users
  These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
  - Any — all IP addresses are covered by this rule.
  - Address range —if this option is selected, you must enter the Start and Finish fields.
  - Single address — enter the required address in the Start field.
- Log
  You can select whether the traffic will be logged. The choices are:
  - Never — no log entries will be made for this service.
  - Always — any traffic for this service type will be logged.
  - Match — traffic of this type that matches the parameters and action will be logged.
  - Not match — traffic of this type that does not match the parameters and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 5-8:



Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
●	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

Figure 5-8: Rules table with examples

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

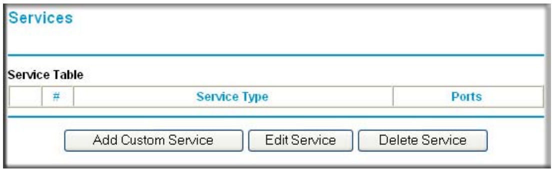
Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, 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.

The service 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.

Although the DG834GT already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

How to Define Services

1. Log in to the router at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Services link of the Security menu to display the Services menu shown in Figure 5-9:



Services

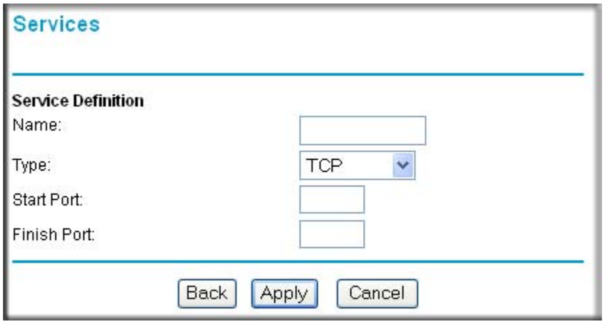
Service Table

	#	Service Type	Ports

Figure 5-9: Services menu

- To create a new Service, click the Add Custom Service button.
- To edit an existing Service, select its button on the left side of the table and click Edit Service.
- To delete an existing Service, select its button on the left side of the table and click Delete Service.

3. Use the page shown below to define or edit a service.



Services

Service Definition

Name:

Type: TCP

Start Port:

Finish Port:

Figure 5-10: Add Services menu

4. Click Apply to save your changes.

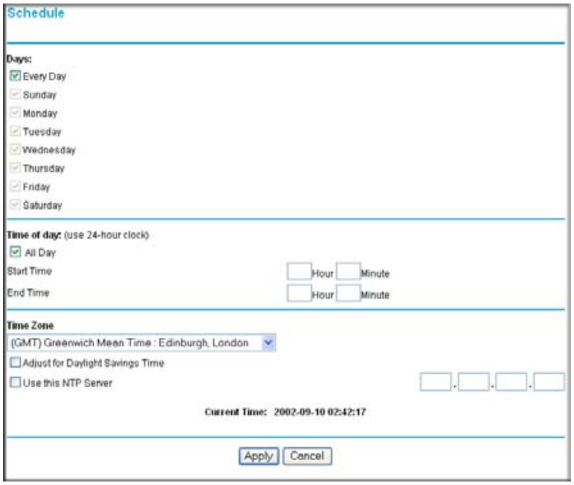
Setting Times and Scheduling Firewall Services

The DG834GT Super Wireless ADSL Router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet.

How to Set Your Time Zone

In order to localize the time for your log entries, you must specify your Time Zone:

1. Log in to the router at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Schedule link of the Security menu to display menu shown below.



Schedule

Days:
☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day: (use 24-hour clock)
☑ All Day
Start Time □ Hour □ Minute
End Time □ Hour □ Minute

Time Zone
(GMT) Greenwich Mean Time : Edinburgh, London
□ Adjust for Daylight Savings Time
□ Use this NTP Server □.□.□.□

Current Time: 2002-09-10 02:42:17

Figure 5-11: Schedule Services menu

3. Select your Time Zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

   Select the Adjust for daylight savings time check box if your time zone is currently in daylight savings time.

Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and clear it at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time.

4. The router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.
5. Click Apply to save your settings.

How to Schedule Firewall Services

If you enabled services blocking in the Block Services menu or Port forwarding in the Ports menu, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the router at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Schedule link of the Security menu to display menu shown above in the Schedule Services menu.
3. To block Internet services based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

   Note: Enter the values in 24-hour time format. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.
4. Click Apply to save your changes.