Content Filtering or Parental Control

The gateway provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the CG814M Gateway prevents objectionable content from reaching the PCs. The CG814M allows access to Internet content to be controlled by screening for keywords within Web addresses. It also has the capability to block access to all sites except those that are explicitly allowed. Key content filtering options include the following:

- Blocking access from the LAN to Internet locations that contain specified keywords.
- Blocking access to web sites that are specified as off-limits.
- Allowing access to only web sites that are specified as allowed.
- Filtering of Proxy servers, Cookies, Java, ActiveX and Popup Windows.

Block Keywords and Domains

Note: The CG814M Gateway allows Internet content access to be restricted based on functions such as web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.NETGEAR.com, the domain name is NETGEAR.com.

To Block Keywords and Domains, complete the following steps:

1. Log in to the gateway 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 chosen for the gateway.
2. Click on the Block Sites link of the Content Filtering menu.
3. To enable keyword blocking or Domain Blocking, check the appropriate Enable box.
4. Enter Keywords into the Keyword List by typing them in the Add Keyword box, then, click Add Keyword. The following are examples of Keyword applications:

- If the keyword “XXX” is specified, the URL is blocked.
- If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
Enter the keyword "." to block all Internet browsing access.

Up to 8 entries are supported in the Keyword list.

5. Enter Domains into the Domain List by typing them in the Add Domain box. Click Add Domain. If the domain “badstuff.com” is specified, the URL is blocked, along with all other URLs in the badstuff.com site. **Note:** Up to 8 entries are supported in the Keyword list.

6. To block access to the domains in the Domain List, select Deny Domains. To allow access to only the domains in the Domain List, select Allow Domains. If the domain “goodstuff.com” is specified, only sites on the goodstuff site will be able to be accessed.

7. To delete a keyword or domain, select it from the list, click Remove Keyword or Remove Domain.

8. Configure the times when access rules apply in the Schedule section.

9. Click the Apply button to save the settings.

**Blocking Services**

The CG814M Gateway allows access to specific traffic such as proxies, cookies, Java Applets, ActiveX and popup windows be blocked.

To enable filtering of services, from the Content Filtering section of the Main Menu, select Services. Check the Enable box for whichever service to be blocked and click the Apply button.

**Proxy**

The proxy filter will prevent PCs from using a proxy server to surf the web. A proxy server can be used to bypass parental control features because the port number for a proxy is usually 8080.

Most web surfing is done on port 80. The parental control feature monitors port 80 so proxy based web surfing would not be inspected by the parental controls. The proxy filter should be used if parental controls are being used.
Cookies
A cookie is a text file saved by the web browser which is sent to a particular web server every time the site is visited. Cookies are used to identify you to the web server automatically.

Back to Top

Java Applets
Java Applets are programs that run from within another application, such as a web browser.

Back to Top

ActiveX
An ActiveX control is a Microsoft Windows program that can be downloaded from a web page and automatically executed by the web browser on the PC.

Back to Top

Popup Windows
Many internet sites open additional browser windows, called popups. They are often used for advertisements. The CG814M can filter out many of these popup windows.

Back to Top

Port Blocking
Firewall rules are used to block or allow specific traffic passing through from one side 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. Instructions for setting up inbound rules can be found in Port Forwarding. Outbound rules (LAN to WAN) determine what outside resources local users can have access to. This section describes how to set up outbound rules.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the CG814M Gateway are the following:

- **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.
Additional rules that will specify exceptions to the default rules may be defined. By adding custom rules, access based on the service or application, source or destination IP addresses, and time of day can be blocked or restricted. In addition, logging traffic that matches or does not match the rule defined is also available.

To configure outbound rules on the CG814M Gateway, click the Port Blocking link on the Advanced section of the main menu.

To block outbound traffic, select the service to be blocked from the drop-down list of predefined services. Click the Add button.

If the service to be blocked is not in the predefined list, add a custom service. Enter the range of ports to block and select whether the ports are TCP, UDP or Both. Click the Add button.

To delete an existing rule, select its button on the left side of the table and click the Delete button.

**Back to Top**