Protecting the Home Network (Firewall)

Protecting Access to the CG814M Gateway
Changing the Built-In Password | Port Forwarding | Port Triggering | Setting Up A Default DMZ Host | Respond to Ping on Internet WAN Port

This section describes how to use the firewall features of the CG814M Wireless Cable Modem Gateway to protect the network.

Protecting Access to the CG814M Gateway

For security reasons, the gateway 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 gateway User Name and password for the gateway Password.

Changing the Built-In Password

To change the built-in password, 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. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password.

3. To change the password, first enter the old password, and then enter the new password twice.

4. To reset the gateway to its factory default settings select Yes for Restore Factory Defaults. This will remove all configuration information you have entered.

5. Click the Apply button to save the changes.

Note: After changing the password, log in again to continue the configuration. If the gateway settings have previously been backed up, do a new backup so that the saved settings file includes the new password.

Port Forwarding

Because the CG814M Gateway uses NAT, the network presents only one IP address to the Internet and outside users cannot directly address any of the local
computers. However, by defining an inbound rule a local server (for example, a web server or game server) can be made visible and available to the Internet. The rule tells the gateway 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.

Remember that allowing inbound services opens holes in the firewall. Only enable those ports that are necessary for the network.

To configure inbound rules on the CG814M Gateway, complete the following steps:

1. Click the Port Forwarding link on the Advanced section of the main menu.

To forward inbound traffic, complete the following steps:

1. Select the service to forward from the drop-down list of predefined services. If the service to forward is not in the predefined list, add a custom service. Enter the range of ports to forward and select whether the ports are TCP, UDP or Both.

2. Enter the IP address of the computer on the network to which to direct the inbound traffic.

3. Click the Add button.

4. To access the local computer from the Internet, use the WAN address of the gateway, which can be found on the Basic Settings page.

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

Considerations for Port Forwarding

If the external IP address is assigned dynamically by the 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 the network.

If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, assign a static IP address to the server outside the range that is assigned by DHCP, but in the same subnet as the rest of the LAN. By default, the IP addresses in the range of 192.168.0.2 through 192.168.0.9 are reserved for this.

Local PCs must access the local server using the PCs’ local LAN address (192.168.0.XXX, by default). Attempts by local PCs to access the server using the external WAN IP address will fail.
Port Triggering

Port Triggering is an advanced feature that allows you to dynamically open inbound ports based on outbound traffic on different ports. This is an advanced feature that can be used for gaming and other internet applications. Port Forwarding can typically be used to enable similar functionality, however, it is static and has some limitations. Ports will be open to traffic from the internet until the port forwarding rule is removed.

Additionally, port forwarding does not work well for some applications when the WAN IP address is assigned by DHCP, and is changed frequently. Port Triggering opens in incoming port temporarily and does not require the server on the internet to track the IP address if it is changed. Port Triggering monitors outbound traffic. When the gateway detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and "triggers" the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

An example of Port Triggering for Internet Relay Chat (IRC) is shown below. When connecting to an IRC server, the server tries to connect back on port 113 to do an Ident lookup. Unless Port Forwarding has been configured to open port 113, the traffic will be blocked. In this example, the initial login to the server in the range of ports 6660 to 6670 will be detected. This will trigger the gateway to temporarily forward port 113 to the PC that initiated the login.

To configure Port Triggering, complete the following steps:

1. In the Trigger Range, enter the outbound ports that will be monitored for activity. This will be the "trigger".
2. In the Target Range, enter the inbound ports that should be forwarded when the trigger occurs.
3. Select the appropriate protocol: TCP, UDP, or Both.
4. Check the Enable box.
5. Click the Apply button.
6. To clear a Port Triggering rule, either remove the check from the Enable box, to temporarily disable the rule, or select the rule and click the Delete button.

Setting Up A Default DMZ Host

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The gateway is programmed to recognize some of these applications and to work properly with them, however, there are other applications that may not function well. In some
cases, one local PC can run the application properly if that PC’s IP address is entered as the Default DMZ Host.

**Note:** For security reasons, avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack the network.

Incoming traffic from the Internet is normally discarded by the gateway unless the traffic is a response to one of the local computers or a service that you have configured in the Port Forwarding or Port Triggering menu. Instead of discarding this traffic, it can be forwarded to one computer on the network. This computer is called the Default DMZ Host.

To assign a computer or server to be a DMZ Host, from the Main Menu, under Advanced, select DMZ Host. Enter the IP address of the computer to assign as a DMZ Host and click the Apply button. To disable the DMZ Host, enter “0” and click the Apply button.

**Back to Top**

**Respond to Ping on Internet WAN Port**

If the gateway should respond to a 'ping' from the Internet, click the 'Respond to Ping on WAN Port' check box. This should only be used as a diagnostic tool, since it allows the gateway to be discovered. Do not check this box unless there is a specific reason to do so.

**Back to Top**