This chapter describes how to use the basic firewall features of the 54 Mbps ADSL Modem Wireless Router Model DG834G to protect your network. It also describes how to configure Trend Micro Home Network Security.

Protecting Access to Your 54 Mbps ADSL Modem Wireless Router Model DG834G

For security reasons, the modem 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 modem router User Name and **password** for the modem router Password. You can use procedures below to change the modem 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 modem 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 modem router.

Figure 4-1

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

Set Password

Old Password	
Set Password	
Repeat New Password	

Administrator login times out after idle for `95` minutes.

[Apply] [Cancel]

Figure 4-2

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 modem 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 modem 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 modem router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the ADSL Modem Wireless Router prevents objectionable content from reaching your PCs. The modem 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 modem router to perform these functions.

How to Block Keywords and Sites

The ADSL Modem Wireless 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 modem 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 modem router.

2. Select the **Block Sites** link of the Security menu.

Figure 4-3

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.

> **Note:** The Block Sites feature is disabled when the Trend Micro Home Security feature is enabled. This is because the Trend security system has incorporates its own site-blocking capability.

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 DG834G v3 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 4-11 for more details.

To access the rules configuration of the DG834G v3, 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

Add Edit Move Delete

Inbound Services

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

Add Edit Move Delete

Apply Cancel

Figure 4-4

- 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 DG834G v3 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 modem 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:
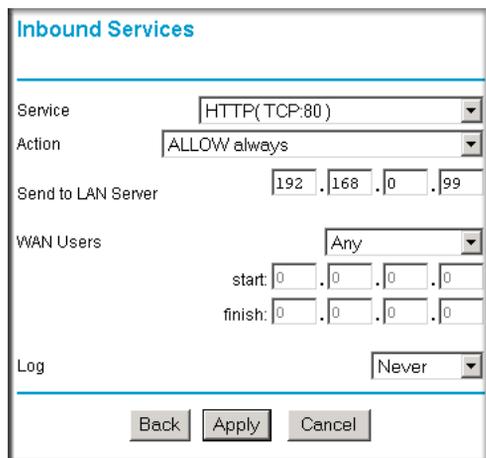
Inbound Services

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

Back   Apply   Cancel

Figure 4-5

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 here, 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

Back   Apply   Cancel

Figure 4-6

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 above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The DG834G v3 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 modem router log any attempt to use Instant Messenger during that blocked period.

Figure 4-7

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:

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

Add   Edit   Move   Delete

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

Add   Edit   Move   Delete

Figure 4-8

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 DG834G v3 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 modem 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 modem router.

2. Select the **Services** link of the Security menu to display the Services menu shown:

Figure 4-9

*   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.
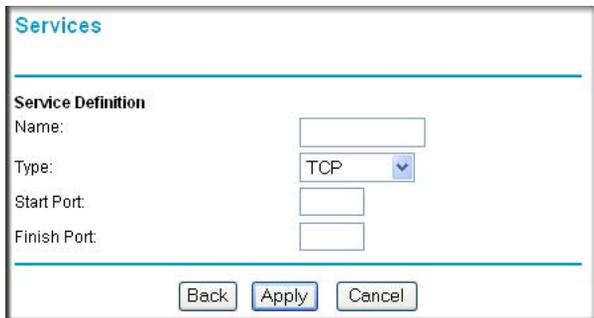
Figure 4-10

4. Click **Apply** to save your changes.

Setting Times and Scheduling Firewall Services

The ADSL Modem Wireless 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 modem 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 modem router.

2. Select the **Schedule** link of the Security menu to display menu shown below.
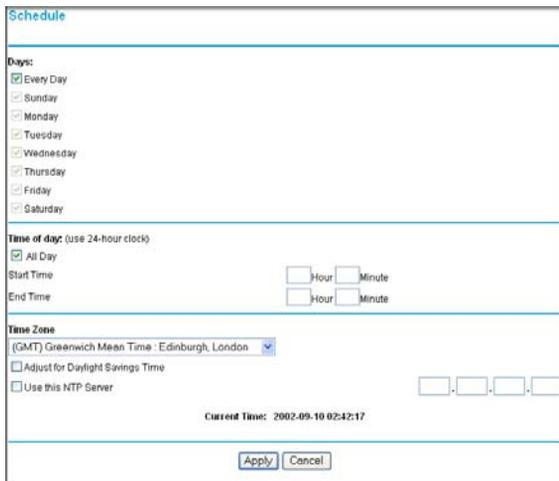

Figure 4-11

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 modem 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 modem 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 modem router.

2. Select the **Schedule** link of the Security menu to display menu shown above.

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.

4. 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.

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

Trend Micro Home Network Security

You can enable Home Network Security as if you didn't do so when you originally set up your router. Home routers provide an enhanced Internet experience, but the likelihood of attacks also increases. Trend Micro Home Network Security addresses the security needs of computers accessing the Internet via home routers.

→	**Note:** The 54 Mbps ADSL Modem Wireless Router Model DG834G supports Home Network Security. To take advantage of this feature you must register an account with Trend Micro. For more information, refer to the Home Network Security *Quick Start Guide* on the NETGEAR Resource CD, or to *http://www.trendmicro.com/offers/netgear*. The Trend Micro software requires Microsoft Internet Explorer 5.5 or higher.

To begin using Home Network Security, configure the Security Service and Parental Controls menus on your ADSL Modem Wireless Router. Each screen has a GUI button to click that will take you to the Trend Micro Web site to open your Trend Micro account.

> **→** **Note:** Because of overlapping functionality, the Block Sites feature, described in "How to Block Keywords and Sites" on page 4-3, is disabled if you enable Trend Micro Home Security.

Security Service Settings

Click **Security Service** under Content Filtering on the Main menu to get the Security Service Settings menu shown below:

Click this banner to install the Trend Micro dashboard and set up your Trend Micro account.

Figure 4-12

To install Home Network Security, click the Trend Micro banner and then follow the on-screen instructions. For assistance, refer to the Home Network Security *Quick Start Guide* included on the NETGEAR Resource CD. (You can download this document and the Home Network Security *User's Guide* at *http://www.trendmicro.com/en/support/tmss/netgear.*)

• **Enable Trend Micro Security Services**. Select this check box and then click **Apply** to enable the Security Service features on this page (automatic updates and Client Virus Protection Status information).

• **Automatically check for update components**. Select this check box to automatically check for updates to Trend Micro scanning components. Choose the desired checking interval from the list, and then click **Apply**.

> **Note:** If your ISP bills by the amount of time or traffic you use, set the update frequency to once a day.

• **Client Virus Protection Status**. Provides information on all computers on your network.

  – **IP Address**: The computer's IP address

  – **Computer Name**: The name of the computer (as shown in Control Panel > System)

  – **Antivirus Software**: The type of antivirus software installed on the computer

  – **Virus Def. File Version**: The version of the virus pattern file in use by the antivirus software

  – **Scan Engine**: The version of the scan engine in use by the antivirus software

  – **Status**: Indicates if the virus pattern file or scan engine require updating (if no recognized antivirus software is found, the status is "Potential Threat")

Parental Controls Settings

Click **Parental Controls** under Content Filtering on the Main menu to get the Trend Micro Parental Controls menu shown below:

Click this banner to install the Trend Micro dashboard and set up your Trend Micro account.

Trend Micro Parental Controls

Enable Parental Controls
- ○ Never
- ○ Per Schedule
- ⊙ Always

Get 1 Year of Parental Controls Free! Enable Trend Micro Home Network Security Now.

Select the Parental Controls Mode
- ⊙ Use General Controls   ○ Use Per-User Controls

        [Parental Control Logs]

General Controls
Parental Controls Bypass Password: ●●●●●●●●●●●●●●●●
Confirm password: ●●●●●●●●●●●●●●●●
Access Control: ○ No Restrictions
                     ⊙ Apply Profile General ▾
                     ○ Use Custom Settings

Parental Controls Access Log

From: September 19, 2005

Category	Access Attempts	Times Accessed
Adult/Mature	0	0
Pornography	0	0
Sex Education	0	0
Intimate Apparel/Swimsuit	0	0
Nudity	0	0
Alcohol/Tobacco	0	0
Illegal/Questionable	0	0
Gambling	0	0
Violence/Hate/Racism	0	0
Weapons	0	0
Illegal Drugs	0	0
Hacking/Proxy Avoidance	0	0

[Refresh]   [Restart Log]

Figure 4-13: Trend Micro Parental Controls menu

To configure Parental Controls:

- Click **Always** to turn on Parental Controls all the time.

- Click **Never** to turn off Parental Controls.

- Click **Per Schedule** to turn on Parental Controls at the times specified on the Schedule page.

→ **Note:** After changing Parental Controls settings, click **Apply** to save changes.

To select Parental Controls Mode:

- Click **Use General Controls** to select General mode. In General mode, one access profile applies to all users.

- Click **Use Per-User Controls** to select Per-User mode. In Per-User mode, each user has an individual access profile.

> **Note:** When in Per-User mode, everyone accessing the Internet through the router is required to log in.

To configure General mode:

1. Enter a password in the Parental Controls Bypass Password box, re-enter it in the Confirm password box, and then click **Apply**. This password allows users to access pages that are blocked by Parental Controls.

2. Select the access profile that will apply to all users, as follows:

   - To select a predefined profile, click **Apply Profile** and then choose a profile from the list.

   - To create a custom profile, click **Use Custom Settings** and then select the check boxes as desired. (For additional choices, click **More Categories**).

   - To allow unrestricted Internet access, click **No Restrictions**.

3. Click **Apply**.

To configure Per-User mode:

The User Account Information table in Per-User mode shows each user's name, access profile, and status. Users with Active status can access the Internet sites permitted by their access profiles. Users with Inactive status cannot log in and cannot access any Internet sites.

To add a new user:

1. Click **Add**. Type the new user's login name and password, and then re-enter the password in the Confirm password box.

2. Select the new user's status. To allow Internet access, click **Active**. To completely disable this user's Internet access, click **Inactive**.

3. Select the access profile that will apply to this user, as follows:

   - To select a predefined profile, click **Apply Profile** and then choose a profile from the list.

- To create a custom profile, click **Use Custom Settings** and then select the check boxes as desired. (For additional choices, click **More Categories**).

- To allow unrestricted Internet access, click **No Restrictions**.

4. Click **Apply**.

To change a user's account information:

1. Select the user's name in the User Account Information table and then click **Edit**.

2. Make the desired changes, and then click **Apply**.

To delete a user, select the user's name in the User Account Information table and then click **Delete**.

Parental Controls Logs

Click **Parental Controls Logs** to view attempts to access restricted sites, and actual accesses.

Blocking criteria for potentially offensive categories

Trend Micro has defined twelve potentially offensive categories of Web sites. Following are the blocking criteria for each category:

- **Adult/Mature Content**: Sites that contain material of an adult nature but without excessive violence, sexual content, or nudity. These sites may include profane or vulgar content not appropriate for children.

- **Alcohol/Tobacco**: Sites that promote or sell alcohol and tobacco products. Includes sites that glamorize or otherwise encourage alcohol or tobacco use. Does not include sites that sell alcohol or tobacco as a subset of another business.

- **Gambling**: Sites where users can place bets or participate in betting pools (including lotteries) online. Also includes sites that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. Does not include sites that sell gambling-related products or machines. Also does not include offline casino and hotel sites, unless meeting one of the foregoing criteria).

- **Hacking/Proxy Avoidance**: Sites providing information on illegal or questionable access to, or use of, communications equipment and software, or that provide information on how to bypass proxy server features or gain unauthorized access to URLs.

- **Illegal Drugs**: Sites that promote, offer, sell, supply, or advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants and chemicals, and related paraphernalia.

- **Illegal/Questionable**: Sites that advocate or advise on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques, and plagiarism. Also includes sites that provide or sell questionable educational materials, such as term papers.

- **Intimate Apparel/Swimsuit**: Sites that contain images of swimsuits, intimate apparel, or other suggestive clothing. Does not include sites selling undergarments as a subset of another business.

- **Nudity**: Sites containing nude or seminude depictions of the human body. Such depictions need not be sexual in intent or effect. May include sites containing nude paintings or photo galleries of an artistic nature. This category includes nudist or naturist sites.

- **Pornography**: Sites that contain sexually explicit material.

- **Sex Education**: Sites that provide information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for better sex as well as products used for sexual enhancement.

- **Violence/Hate/Racism**: Sites depicting or advocating physical harm to people or property. Includes sites that convey hostility or aggression toward, or the denigration of, an individual or group on the basis of race, religion, gender, nationality, ethnic origin, and so forth.

- **Weapons**: Sites that sell, review, or describe guns, knives, martial arts devices, and related accessories. Does not include sites that promote weapons collecting, or groups that either support or oppose weapons ownership.