# CHAPTER 9

# IP Filter/Firewall Setup

## 9.1   Introduction

The IP Filter/Firewall function helps protect your local network against attack from outside. It also provides a way of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

## 9.2   An Overview of the IP Filter/Firewall

The **IP Filter/Firewall Setup** in the Vigor routers mainly consists of the packet filtering, Denial of Service (DoS) defense, and URL (Universal Resource Locator) content filtering facilities. In this chapter, we focus on the introduction of the packet filtering function. In the next two chapters, we will explain more about DoS defense and URL content filtering facilities.

The packet filtering function contains, by default, two types of filter sets: Call Filter set and Data Filter set. The Call Filter is used for users that attempt to establish a connection from LAN side to the Internet. The Data Filter set is used to determine what kind of IP packets is allowed to pass through the router when the WAN connection has been established.

Conceptually, when an outgoing packet is to be routed to the WAN, the IP Filter will decide if the packet should be forwarded to the Call Filter or Data Filter. If the WAN link is down, the packet will enter the Call Filter. If the packet is not allowed to trigger router dialing, it will be dropped. Otherwise, it will initiate a

call to establish the WAN connection.

If the WAN link of the router is up, the packet will pass through the Data Filter. If the packet type is set to be blocked, it will be dropped. Otherwise, it will be sent to the WAN interface. Alternatively, if an incoming packet enters from the WAN interface, it will pass through the Data Filter directly. If the packet type is set to be blocked, it will be dropped. Otherwise, it will be sent to the internal LAN. The filter architecture is shown below.
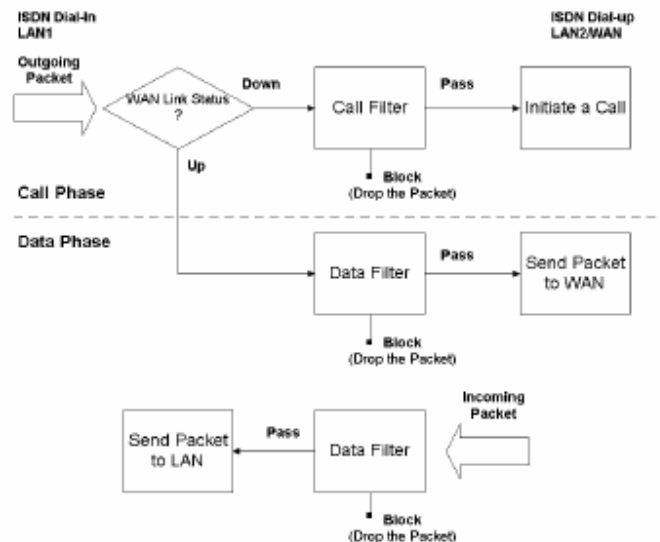


The following sections will explain more about the **General Setup** and **Filter Setup** in the **IP Filter/Firewall Setup** section using the Web Configurator. The Vigor router provides 12 filter sets with 7 filter rules for each set. As a result, there are a total of 84 filter rules for the **Filter Setup**. By default, the Call Filter rules are defined in Filter Set 1 and the Data Filter rules are defined in Filter Set 2.

> Advanced Setup > IP Filter / Firewall Setup

- **General Setup**
- **DoS defense**
- **Content Filter**

- Filter Setup

| Set | Comments |
|-----|----------|
| 1. | Default Call Filter |
| 2. | Default Data Filter |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |
| 11. | |
| 12. | |

**General Setup:** Some general settings are available from this link.

**DoS defense:** Click it to set up the DoS defense facility for detecting and mitigating the DoS attacks. The more details can be found in Chapter 9-A.

**Content Filter:** Here provides the capability of blocking inappropriate web-sites to protect child in school or at home. The more details can be found in Chapter 9-B.

**Filter Setup:** Here are 12 filter sets for IP Filter configurations.

**Set to Factory Default:** Click here to restore the filter rules to default values.

## 9.3 General Setup

In the General Setup page you can enable/disable the Call Filter or Data Filter and assign a Start Filter Set for each, configure the log settings, and set a MAC address for the logged packets to be duplicated to.

3
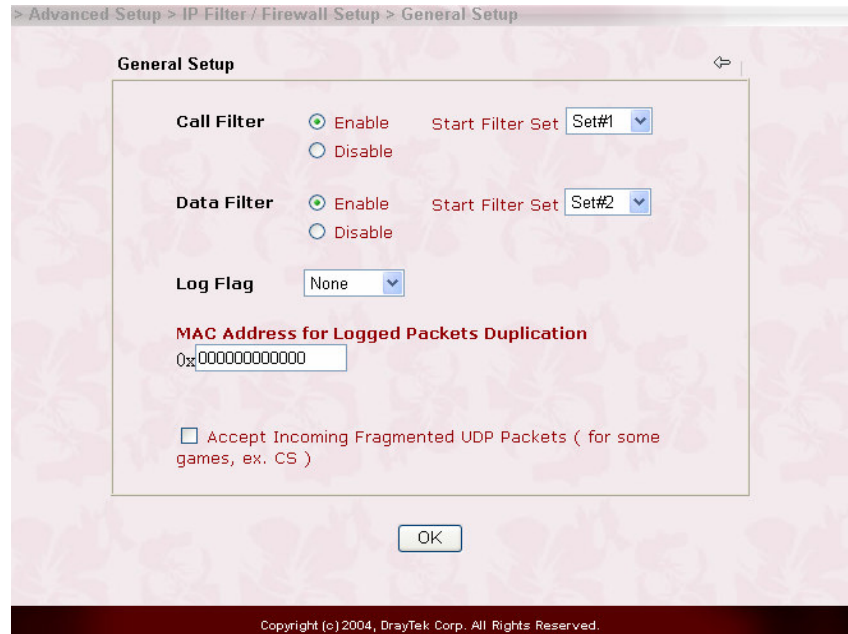
**Call Filter:** Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.

**Data Filter:** Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.

**Log Flag:** For troubleshooting needs you can specify the filter log here.

**None:** The log function is inactive.

**Block:** All blocked packets will be logged.

**Pass:** All passed packets will be logged.

**No Match:** The log function will record all packets which are

nmatched.

**Note:** The filter log will be displayed on the Telnet terminal when you type the "log -f" command.

**MAC Address for Packet Duplication:** Logged packets may also be

4

logged to another location via Ethernet. If you want to duplicate logged packets from the router to another network device, you must enter the other devices' MAC Address (HEX Format). Type "0" to disable the feature. The feature will be helpful under Ethernet environments.

## 9.4    Editing the Filter Sets



**Comments**: Enter filter set comments/description. Maximum length is 23 characters.

**Filter Rule**: Click a button numbered **1 ~ 7** to edit the filter rule.

**Active**: Enable or disable the filter rule.

**Next Filter Set**: Specifies the next filter set to be linked behind the current filter set. The filters cannot be looped.

The following setup pages show the default settings for the Call Filter and the Data Filter. You will see the Call Filter set is assigned to Set 1 and the Data Filter set to Set 2.

5

## 9.5 Editing the Filter Rules

Click the Filter Rule index button to enter the Filter Rule setup page for each filter. The following explains each configurable item in detail.

**Comments:** Enter filter set comments/description. Maximum length is 14 characters.

6

**Check to enable the Filter Rule:** Enables the filter rule.

**Pass or Block:** Specifies the action to be taken when packets match the rule.

> **Block Immediately:** Packets matching the rule will be dropped mmediately.

> **Pass Immediately:** Packets matching the rule will be passed mmediately.

> **Block If No Further Match:** A packet matching the rule, and that does not match further rules, will be dropped.

> **Pass If No Further Match:** A packet matching the rule, and that does not match further rules, will be passed through.



**Branch to Other Filter Set:** If the packet matches the filter rule, the next filter rule will branch to the specified filter set.

**Duplicate to LAN:** If you want to log the matched packets to another network device, check this box to enable it. The MAC Address is

defined in **General Setup > MAC Address for Logged Packets Duplication**.

**Log:** Check this box to enable the log function. Use the Telnet command **log-f** to view the logs.

**Direction:** Sets the direction of packet flow. For the Call Filter, this setting is irrelevant.


For the Data Filter:

**IN:** Specifies the rule for filtering incoming packets.

**OUT:** Specifies the rule for filtering outgoing packets.

**Protocol:** Specifies the protocol(s) this filter rule will apply to.

**IP Address:** Specifies a source and destination IP address for this filter rule to apply to. Placing the symbol **!** before a particular IP Address will prevent this rule from being applied to that IP address. It is equal to the logical NOT operator.

**Subnet Mask:** Specifies the Subnet Mask for the IP Address column for this filter rule to apply to.

**Operator:** The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.

> **=** : If the **End Port** is empty, the filter rule will set the port number to be the value of the **Start Port**. Otherwise, the port number ranges between the **Start Port** and the **End Port** (including the **Start Port** and the **End Port**).

> **!=** : If the **End Port** is empty, the port number is not equal to the

value of the **Start Port.** Otherwise, this port number is not between the **Start Port** and the **End Port** (including the **Start Port** and **End Port**).

**>** : Specifies the port number is larger than the **Start Port** (includes the **Start Port**).

**<** : Specifies the port number is less than the **Start Port** (includes the **Start Port**).

**Keep State**: When checked, protocol information about the TCP/UDP/ICMP communication sessions will be kept by the IP Filter/Firewall (the Firewall **Protocol** option (see page 5-21) requires that TCP or UDP or TCP/UDP or ICMP be selected for this to operate correctly).

**Fragments:** Specifies a fragmented packets action.

**(Do not Care):** Specifies no fragment options in the filter rule.

**Unfragmented:** Applies the rule to unfragmented packets.
**Fragmented:** Applies the rule to fragmented packets.
**Too Short:** Applies the rule only to packets which are too short to contain a complete header.

## 9.6 An Example of Restricting Unauthorized Internet Services

This section will show a simple example to restrict someone from accessing WWW services. In this example, we assume the IP address of the access-restricted user is 192.168.1.10. The filter rule is created in the Data Filter set and is shown as below.

Port 80 is the HTTP protocol port number for WWW services.

> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set > Edit Filter Rule

**Filter Set 2 Rule 2**

**Comments :** WWW          ☑ **Check to enable the Filter Rule**

Pass or Block                          Branch to Other Filter Set
Block Immediately ▾                   None ▾
☐ Duplicate to LAN                    ☐ Log

Direction OUT ▾          Protocol TCP ▾

|  | IP Address | Subnet Mask | Operator | Start Port | End Port |
|---|---|---|---|---|---|
| Source | 192.168.1.10 | 255.255.255.255 (/32) ▾ | = ▾ |  |  |
| Destination | any | 255.255.255.255 (/32) ▾ | = ▾ | 80 |  |

☐ Keep State                          Fragments Don't Care ▾

OK

10

# CHAPTER 9-A

# Prevention of Denial of Service Attacks

## 9-A.1. Introduction

The DoS Defense functionality helps you to detect and mitigate the DoS attacks. Those attacks include the flooding-type attacks and the vulnerability attacks. The flooding-type attacks attempt to use up all your system's resource while the vulnerability attacks try to paralyze the system by offensing the vulnerabilities of the porotocol or operation system.

## 9-A.2. An Overview of DoS Defense Functionality

The DoS Defense Engine inspects ecah incoming packet against the attack signature database. Any packet that may paralyze the host in the security zone is blocked and a syslog message is sent to the client. Also the DoS Defense Enginemonitors the traffic behavior. Any anomaly situation violating the administer's configuration is reported and the corresponding defense function is performed in order to mitigate the attack.
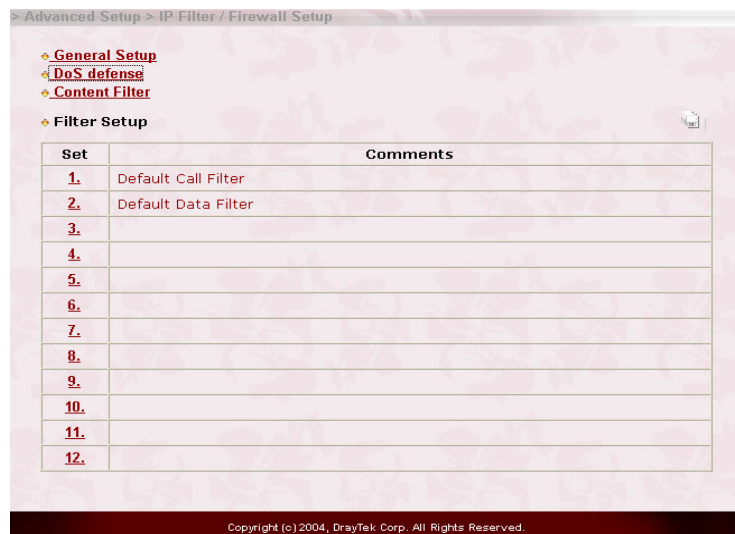
# 9-A.3. Configuration

The following sections will explain in more detail about DoS Defense Setup by using the Web Configurator. It is a sub-functionality of IP Filter/Firewall. There are a total of 15 kinds of defense function for the DoS Defense Setup. By default, the DoS Defense functionality is disabled. Further, once the DoS Defense functionality is enabled, the default values for the threshold and timeout values existing in some functions are set to 300 packets per second and 10 seconds, respectively. A brief description for each item in the DoS defense function is shown below.

> **Enable DoS Defense:** Click the checkbox to activate the DoS Defense Functionality.

> **Enable SYN flood defense:** Click the checkbox to activate the SYN flood defense function. If the amout of the TCP SYN packets from the Internet exceeds the user-defined threshold value, the Vigor2900 router will be forced to discard randomly the sequent TCP SYN packets in the user-defined timeout period. The main goal is to protect the Vigor2900 router against the TCP SYN packets that intend to use up the router's limited-resource. By default, the threshold and timeout values are set to 300 packets per second and 10 seconds, respectively.

> **Enable UDP flood defense:** Click the checkbox to activate the UDP flood defense function. Once the UDP packets from the Internet exceed the user-defined threshold value, the router will be forced to discard all sequent UDP packets in the user-defined timeout period. The default setting for threshold and timeout are 300 packets per second and 10 seconds, respectively.

**Enable ICMP flood defense:** Click the checkbox to activate the ICMP flood defense function. Similar to the UDP flood defense function, the router will discard the ICMP echo requests coming from the Internet, once they exceed the user-defined

threshould (by default, 300 packets per second) in a period of time (by default, 10 second for timeout).

**Enable Port Scan detection:** Port scan attacks occur by sending packets with different port numbers in an attempt to scanning the available services that one port will respond. To examine such an exploration behaviour, please click the checkbox to activate the Port Scan detection function in your Vigor 2900 router. The Vigor2900 router will identify it and report a warning message if the port-scanning rate in packets per second exceeds the user-defined threshold value. By default, the Vigor2900 router sets the threshold as 300 packets per second to detect such a scanning activity.

**Enable Block IP options:** Click it to activate the Block IP options function. The Vigor 2900 router will ignore any IP packets with IP option field appeared in the datagram header. The IP option provides a way for hosts to send some significant information, such as security, compartmentation, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc., which an outsider can analyze to learn details about your private networks.

**Enable Block Land:** Click the associated checkbox and then enforce the Vigor 2900 router to defense the Land attacks. The Lan attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets having the identical source and destination addresses, as well as the port number, with those of the victim.

**Enable Block Smurf:** Click the checkbox to activate the Block Smurf function. The Vigor 2900 router will reject any ICMP echo request destined to the broadcast address.

**Enable Block trace route:** Click the checkbox to activate this function. The Vigor 2900 router will not forward any trace route packets.

**Enable Block SYN fragment:** Click the checkbox to activate the Block SYN fragment function. Any packets having SYN flag and more fragment bit set will be dropped.

**Enable Block fraggle Attack:** Click the checkbox to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

**Enable TCP flag scan:** Click the checkbox to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped.   Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FIN scan*, *Xmas scan* and *full Xmas scan*.

**Enable Tear Drop:** Click the checkbox to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target host will hang once they re-construct the packets. Any packets realizing this attacking activity will be blocked by the Vigor 2900 routers.

**Enable Ping of Death:** Click the checkbox to activate the Block Tear Drop function.   Many machines may crash when receiving ICMP datagrams that exceed the maximum length.   To avoid this type of attack, the Vigor 2900 router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.

**Enable Block ICMP fragment:** Click the checkbox to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

**Enable Block Unknown Protocol:** Click the checkbox to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and

undefined at this time. Therefore, the router should has ability to detect and reject this kind of packets.



# 9-A.4. Warning Message

All the warning messages will be sent to syslog client after you enable the syslog function. The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator. Thus, the administrator can look at the warning messages from DoS Defense functionality through the Draytek Sylsog daemon. The format for this kind of the warning messages is similar to those in **IPFilter/Firewall** except for the preamble keyword "DoS", followed by a name to indicate what kind of attacks is detected.

# IP Filter/Firewall Setup

**DrayTek Syslog**

Controls

192.168.1.1

Vigor2300

**LAN Status**

| TX Packets | RX Packets |
|---|---|
| 5850 | 4517 |

**WAN Status**

| Getway IP (Static) | TX Packets | RX Rate |
|---|---|---|
| 172.16.2.5 | 1190 | 1 |

| WAN IP (Static) | RX Packets | TX Rate |
|---|---|---|
| 172.16.2.84 | 13115 | 1 |

Fire Wall Log | VPN Log | User Access Log | Call Log | WAN Log | Network Infomation | Net State

| Time | Host | Message |
|---|---|---|
| Jan 1 03:46:27 | Vigor | DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328 |
| Jan 1 03:46:24 | Vigor | DoS fraggle Block 172.16.2.83,10752 -> 172.16.2.255,234 PR udp len 20 233 |
| Jan 1 03:46:23 | Vigor | DoS trace_rt Block 192.168.3.1,10752 -> 224.0.0.9,234 PR udp len 20 52 |
| Jan 1 03:46:19 | Vigor | DoS fraggle Block 172.16.2.47,10752 -> 172.16.2.255,234 PR udp len 20 239 |
| Jan 1 03:46:19 | Vigor | DoS fin_wo_ack Block DoS synfin_scan Block 172.16.2.85,1024 -> 172.16.2.84,80 |
| Jan 1 03:46:09 | Vigor | DoS unknown_protocol Block 172.16.2.85 -> 172.16.2.84 PR 105 len 20 20 |
| Jan 1 03:46:03 | Vigor | DoS smurf Block 172.16.2.84 -> 172.16.2.255 PR icmp len 20 32 icmp 0/8 |
| Jan 1 03:46:02 | Vigor | DoS trace_rt Block 172.16.5.5,10752 -> 224.0.0.9,234 PR udp len 20 52 |
| Jan 1 03:45:59 | Vigor | DoS fraggle Block 172.16.2.9,10752 -> 172.16.2.255,234 PR udp len 20 233 |
| Jan 1 03:45:59 | Vigor | DoS land Block 172.16.2.84,80 -> 172.16.2.84,80 PR tcp len 20 40 -S 1 0 |
| Jan 1 03:45:54 | Vigor | DoS trace_rt Block 203.69.175.5,10752 -> 224.0.0.9,234 PR udp len 20 72 |
| Jan 1 03:45:51 | Vigor | DoS fraggle Block 172.16.2.25,10752 -> 172.16.2.255,234 PR udp len 20 78 |
| Jan 1 03:45:52 | Vigor | DoS fraggle Block 172.16.2.1,10752 -> 255.255.255.255,234 PR udp len 20 328 |

**ADSL Status**

| Mode | State | Up Speed | Down Speed | SNR Margin | Loop Att |
|---|---|---|---|---|---|
| ... | ... | ... | ... | ... | ... |

16

# CHAPTER 9-B

# URL Content Filtering

## 9-B.1   Introduction

The Internet contains a wide range of materials, some of which may be offensive or even illegal in many countries.   Unlike traditional media, the Internet does not have any obvious tools to segregate materials based on URL strings or content. URL content filtering systems are seen as tools that would provide the cyberspace equivalent of the physical separations that are used to limit access to some particular materials.   In rating a site as objectionable, and refusing to display it on the user's computer screen, URL content filtering facilities can be used to prevent children from seeing material that their parents find objectionable.   In preventing access, the URL contnet filtering facility acts as an automated version of the convenience-store clerk who refuses to sell adult magazines to high-school students.   The URL content filtering facilities are also used by businesses to prevent employees from accessing Internet resources that are either not work related or otherwise deemed inappropriate.

The name of the URL content filtering comes from checking the content of the URL strings.   Traditional firewall inspects packets based on the fields of TCP/IP headers, while the URL content filtering checks the URL strings or the payload of TCP/IP packets.   In the Vigor 2900 routers, the URL content filtering facility inspects the URL string and some of HTTP data hiding in the payload of TCP packets.

## 9-B.2   An Overview of URL Content Filtering
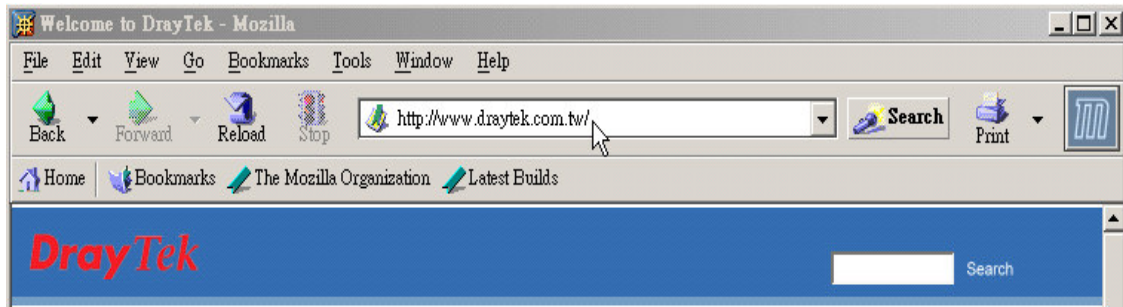


The URL content filtering facility in the Vigor 2900 series of broadband security routers inspects every URL string in the HTTP request initiated inside against the keyword list.   If the entire or part of the URL string (for instance, http://www.draytek.com.tw, as shown above) matches any activated keyword, its associated HTTP request will be blocked by the Vigor 2900 router and a syslog message will be automatically sent to the syslog client.   Also any requst which tries to retrieve the malicious code will be discarded by the Vigor 2900 router. Similarly, a syslog message will be sent to the syslog client.

The URL content filtering facility prevents users from accessing inappropriate websites whose URL strings are identified as prohibition.

Notice that you must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

## 9-B.3   Configuration

The following sections describe the web configuration for setting up the URL content filtering facility, including specific configuration information and any limitation they have.   One can find the entrance of this setting, as depicted in the   following figure, after clicking the **IPFilter/Firewall** in the main menu.

> Advanced Setup > IP Filter / Firewall Setup

◇ **General Setup**
◇ **DoS defense**
◇ **Content Filter**

◇ **Filter Setup**

| Set | Comments |
| --- | --- |
| 1. | Default Call Filter |
| 2. | Default Data Filter |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |
| 10. | |
| 11. | |
| 12. | |

The URL content filtering facility supported in the Vigor 2900 router consists of the *URL Access Control*, *Prevent web access from IP address*, *Restrict Web Feature control*, *Exceptional Subnet handling*, and *Time schedule* functions. The *URL Access Control* aims at controlling the access right of web sites by inspecting the URL string against user-defined keywords. The *Restrict Web Feature control* intends to block the malicious codes hidden in Web pages, such as *Java Applet*, *Active X*, *Cookies*, *Proxy*, *compressed* files, and *executable* files. Also, it is able to block all downloads of *multimedia* files from Web pages in order to control the bandwidth usage.

The function of *Prevent web access from IP address* is used to avoid that inappropriate web sites can be accessed through directly using IP address in the URL locator, even though their URL strings match the user-defined keywords. The function of *Exceptional Subnet handling* allows the administrator to specify a group of hosts that are free from the *URL Access Control*. This group of hosts could be defined as a set of IP addresses or subnets. Finally, the Vigor 2900 router supports the *Time schedule* function to control what time should perform the URL content filtering facility. Now, let us move on the description of each item's usage in more detail.

**Enable URL Access Control:** One checkbox appears giving the choice to activate the *URL Access Control* or not. To enable it, click on the empty

box image and, subsequently, the hook image (☑) will appear.

**Block Keyword List:**   The Vigor 2900 router provides 8 frames for users to define keywords and each frame supports multiple keywords.   The keyword could be a noun, a partial noun, or a complete URL string.   Multiple keywords within a frame are separated by space, comma, or semicolon.   In addition, the maximal length of each frame is 32 characters.   After specifying keywords, the Vigor 2900 router will reject the access right of any website whose whole or partial URL string matched any user-defined keyword.   It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor 2900 router perform.

*Example*:   If you want to filter any website whose URL string contains "sex", "fuck", "gun", or "drug", you should add these words into the frames.   Thus, your Vigor 2900 router will automatically deny any web surfing that its associated URL string contains any one of the list's keywords.   Considering that the user tries to access www.backdoor.net/images/sex /p_386.html, the Vigor 2900 router will cut the connection because this website is prohibited.   But, the user is able to access the website www.backdoor.net/firewall/forum/d_123.html.   Further, the URL content filtering facility also allows you to specify either a complete URL string (e.g., "www.whitehouse.com" and "www.hotmail.com") or a partial URL string (e.g., "yahoo.com") in the blocking keyword list.   Accordingly, the Vigor 2900 router will identify the forbidden URL and perform the blocking action for these websites by cutting the associated connections.

**Prevent Web Access by IP Address:**   One checkbox is available to activate this function that will deny any web surfing activity by directly using IP address.   To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear.

**Enable Excepting Subnets:**   4 entries are available for users to specify some specific IP addresses or subnets so that they can be free from the *URL Access Control*.   To enable an entry, click on the empty checkbox, named as "**ACT**", in front of the appropriate entry.   The hook image (☑) appears to indicate the entry is active.   To disable an entry, click on the hook image (☑).

**Enable Restrict Web Feature:**   It will be of great value to provide the protection mechanism that prohibits the malicious codes from downloading from web pages.   The malicious codes may embed in some executable objects, such as *ActiveX*, *Java Applet*, *compressed files*, and *executable files*, and, if they have been downloaded from websites, would bring a threat of the user's system.   For example, an ActiveX object can be downloaded and run from the web page.   If the ActiveX object has some malicious code in it, it may own unlimited access to the user's system.

*Java***:** Click the checkbox to activate the Block Java object function. The Vigor 2900 router will discard the Java objects from the Internet.

*ActiveX***:** Click the checkbox to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.

*Compressed file***:** One checkbox appears giving the choice to activate the Block Compressed file function to prevent someone from downloading any compressed file.   The following list shows the types of compressed files that can be blocked by the Vigor 2900 router.

   **.zip**          **.rar**          **.arj**          **.ace**          **.cab**          **.sit**

To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear.

*Executable file***:** Similar to the above function, click the checkbox to

enable the Block Executable file function to reject any downloading behavior of the executable file from the Internet. To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear. Accordingly, files with the following extensions will be blocked by the V2900 router.

**.exe .com .scr .pif .bas .bat .inf .reg**

A so-called *cookie* feature introduced by Netscape allows you to keep a close watch on the activities of HTTP request and responses of individual sessions. Many websites use them to create stateful sessions for tracking Internet users, which will violate the users' privacy. Thus, the Vigor2900 router provides the *Cookies filtering facility* that allows you to filter cookie transmission. Similarly, the Vigor2900 router also allows you to filter out all proxy-related transmission in order to support stronger security.

*Cookie:* Click the checkbox to activate the Block Cookie transmission.

The Vigor 2900 router will filter out cookie from any website.

*Proxy:* One checkbox appears giving the choice to activate this function to reject any proxy transmission. To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear.

To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. To enable it, click on the empty box image and, subsequently, the hook image (☑) will appear. Accordingly, files with the following extensions will be blocked by the Vigor 2900 router.

**.mov .mp3 .rm .ra .au .wmv**
**.wav .asf .mpg .mpeg .avi .ram**

**Time Schedule:** Specify what time should perform the URL content filtering facility.

*Always Block:* Click it so that the URL content filtering facility can be executed on the Vigor 2900 router anytime.

*Block from H1:M1 To H2:M2:* Specify the appropriate time duration from *H1*:*M1* to *H2*:*M2* in one day, where *H1* and *H2* indicate the hours. *M1* and *M2* represent the minutes.

*Days of Week:* Specify which days in one week should apply the URL content filtering facility. The Vigor 2900 router supports two exclusive options for users, i.e. everyday or some days in one week. If you expect that the URL content filtering facility is active for whole week, you should click the checkbox "**Everyday**". Otherwise, you should point clearly out the days in one week. For example, if you want the URL content filtering facility to work from Monday to Wednesday, then you should click the appropriate checkboxes (Monday, Tuesday, and Wednesday). Other days the URL content filtering facility will be silent.
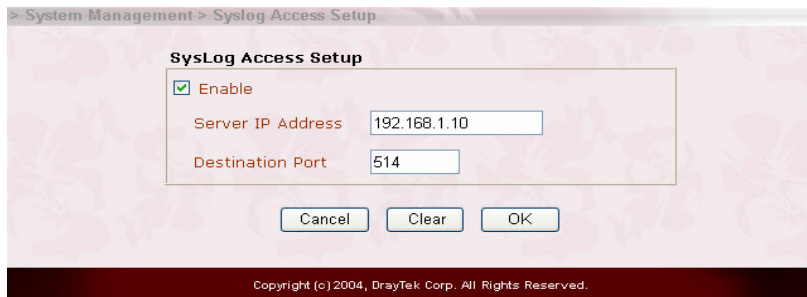
## 9-B.4   Warning Message

When a HTTP reqest is denied, an alert page will appear in your browser, as shown in the following figure.
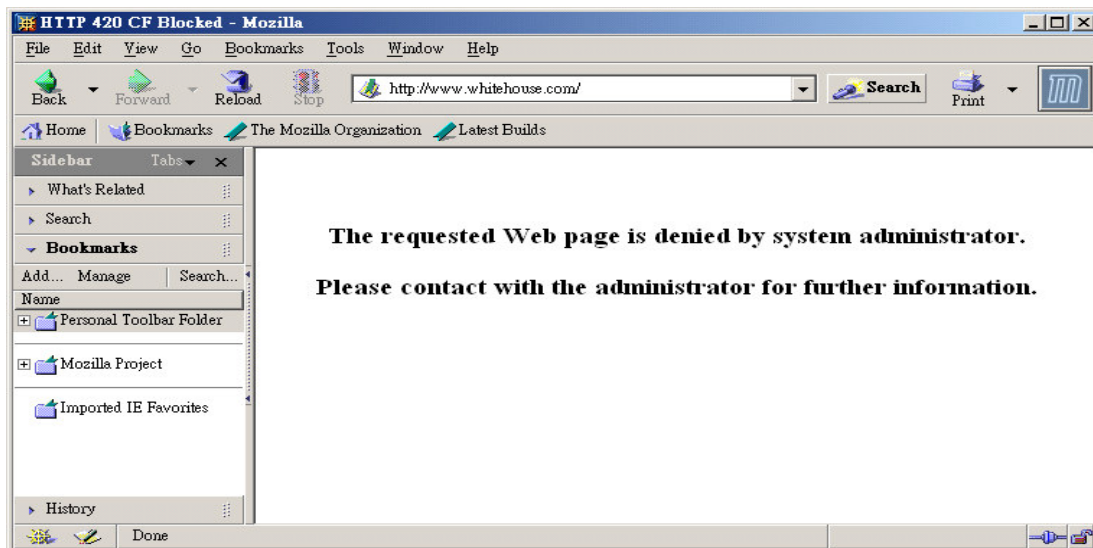
Also, the warning message will be automatically sent to the syslog client after you enable the syslog function.   The administrator can setup the syslog client in the **Syslog Setup** by using Web Configurator.   Thus, the administrator can view the warning messages from the **URL Content Filtering** functionality through the Draytek Sylsog daemon.   The format for this kind of the warning messages is similar to those in the **IPFilter/Firewall** except for the premable keyword "**CF**", followed by a name to indicate what kind of the HTTP request is blocked.