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.

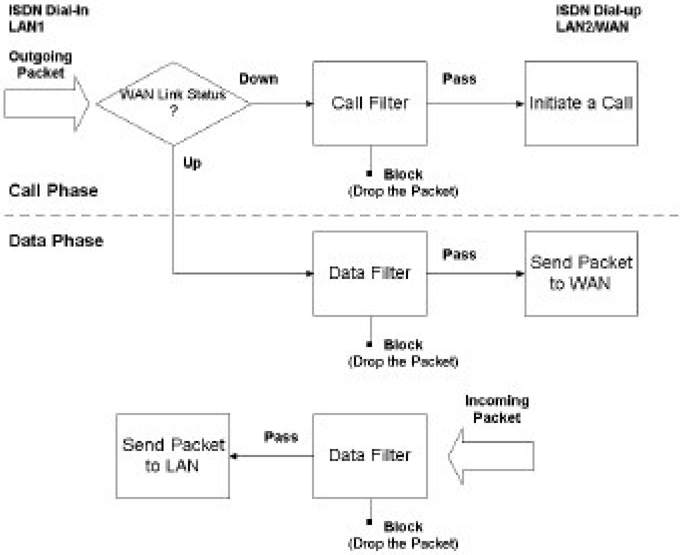
9.2 An Overview of the IP Filter/Firewall

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.

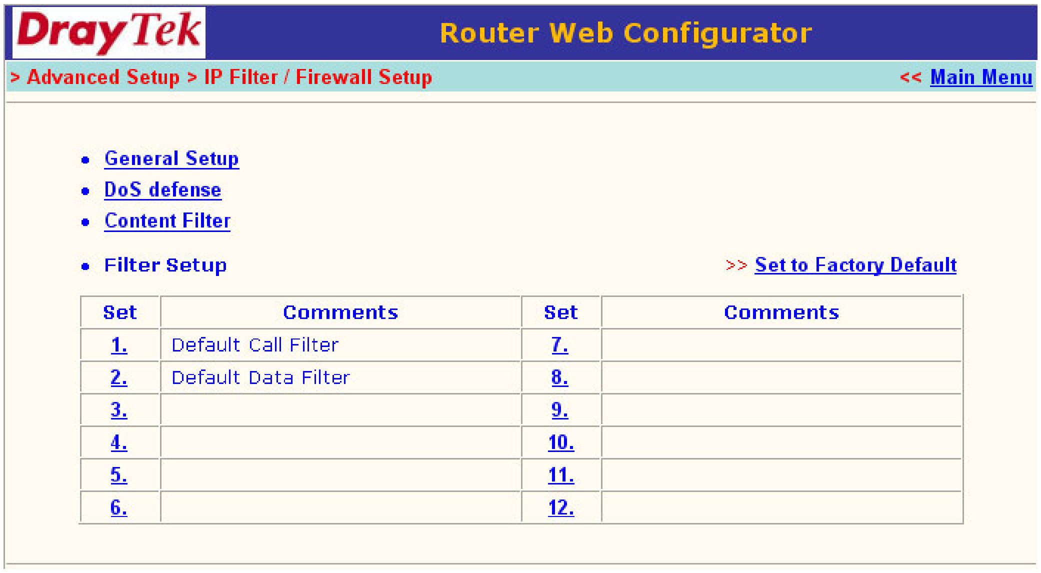
The packet filtering function contains, by default, two types of filter sets: Call Filter set and Data Filter set. The Call Filter is used for users that attempt to establish a connection from LAN side to the Internet. The Data Filter set is used to determine what kind of IP packets is allowed to pass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



DrayTek Router Web Configurator

> Advanced Setup > IP Filter / Firewall Setup << Main Menu

- General Setup
- DoS defense
- Content Filter
- Filter Setup >> Set to Factory Default

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

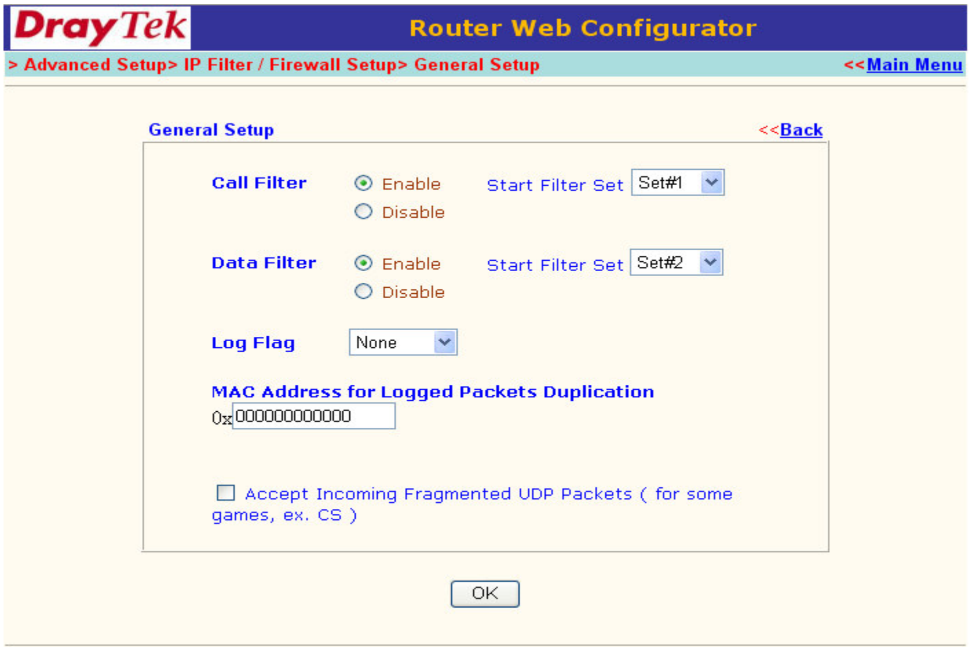
Content Filter: Here provides the capability of blocking inappropriate web-sites to protect child in school or at home. The more details can be found in Chapter 9-B.

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.



Call Filter ● Enable ○ Disable Start Filter Set Set#1

Data Filter ● Enable ○ Disable Start Filter Set Set#2

Log Flag None

MAC Address for Logged Packets Duplication
0x 000000000000

☐ Accept Incoming Fragmented UDP Packets (for some games, ex. CS)

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.

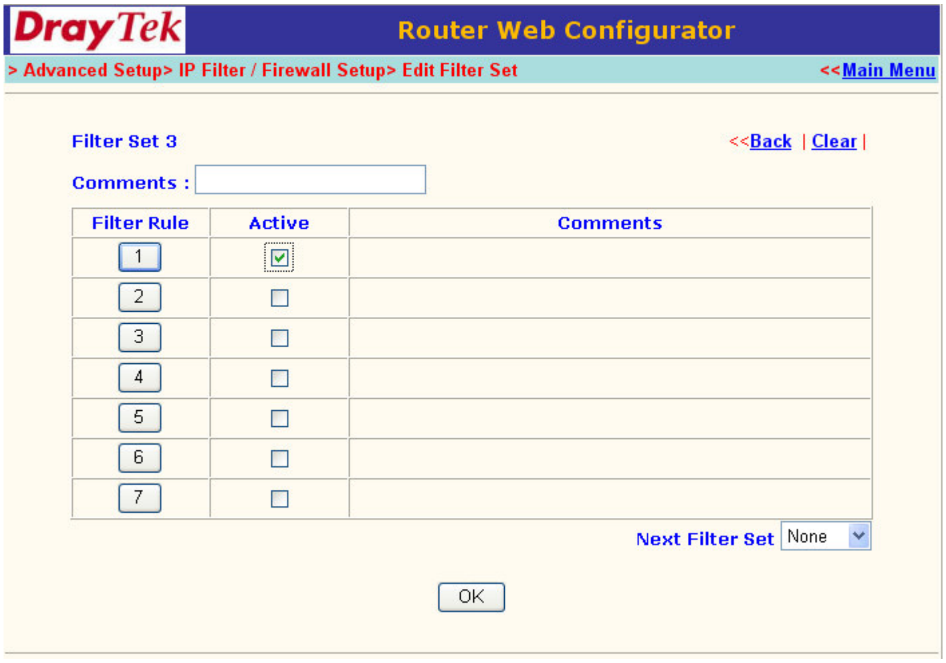
Pass: All passed packets will be logged.

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 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


DrayTek
Router Web Configurator
> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set
<<Main Menu
<<Back | Clear |
OK

Filter Set 3

Comments :

Filter Rule	Active	Comments
1	☑	
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

Next Filter Set None

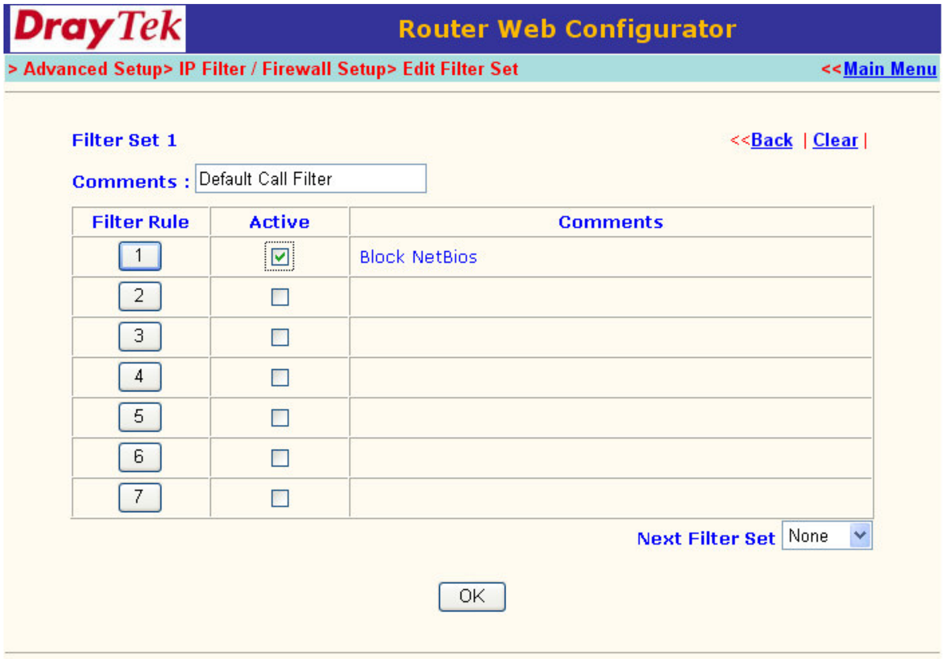
Comments: Enter filter set comments/description. Maximum length is 23 characters.

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.

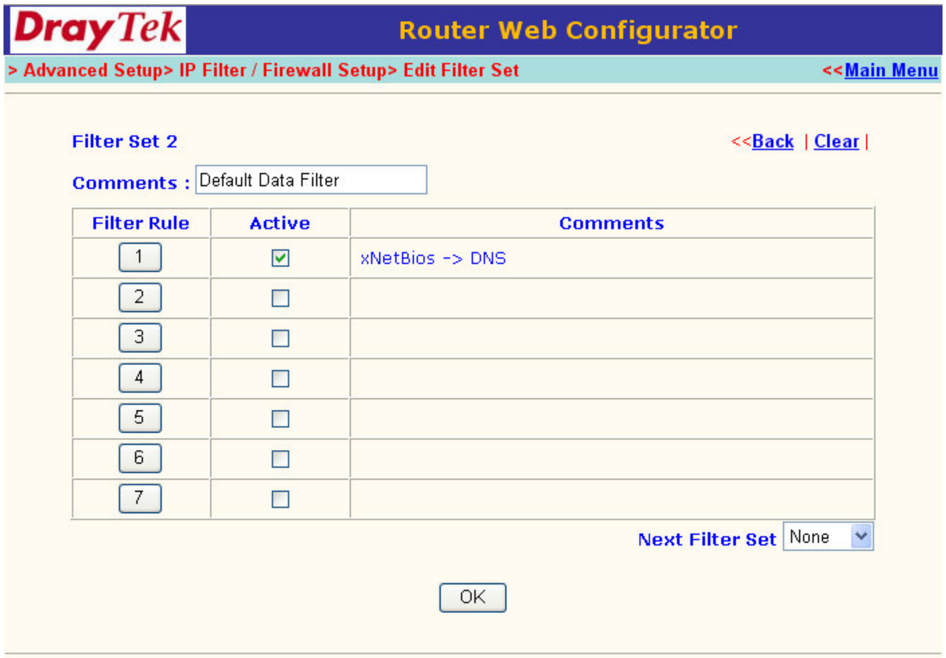

Router Web Configurator
> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set
<<Main Menu
<<Back | Clear |
OK

Filter Set 1

Comments : Default Call Filter

Filter Rule	Active	Comments
1	☑	Block NetBios
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

Next Filter Set None


Router Web Configurator
> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set
<<Main Menu
<<Back | Clear |
OK

Filter Set 2

Comments : Default Data Filter

Filter Rule	Active	Comments
1	☑	xNetBios -> DNS
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

Next Filter Set None

9.5 Editing the Filter Rules

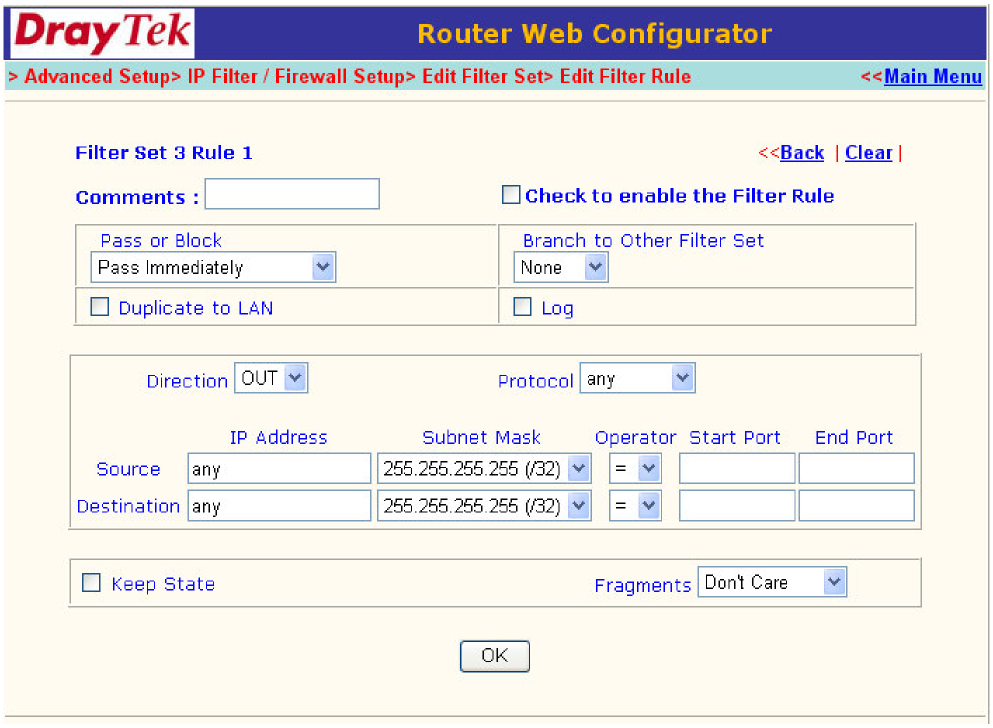
Click the Filter Rule index button to enter the Filter Rule setup page for each filter. The following explains each configurable item in detail.

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

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.


DrayTek
Router Web Configurator
> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set> Edit Filter Rule
<<Main Menu
<<Back | Clear |
OK

Filter Set 3 Rule 1

Comments :

☐ Check to enable the Filter Rule

Pass or Block: Pass Immediately

Branch to Other Filter Set: None

☐ Duplicate to LAN

☐ Log

Direction: OUT

Protocol: any

	IP Address	Subnet Mask	Operator	Start Port	End Port
Source	any	255.255.255.255 (/32)	=		
Destination	any	255.255.255.255 (/32)	=		

☐ Keep State

Fragments: Don't Care

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.

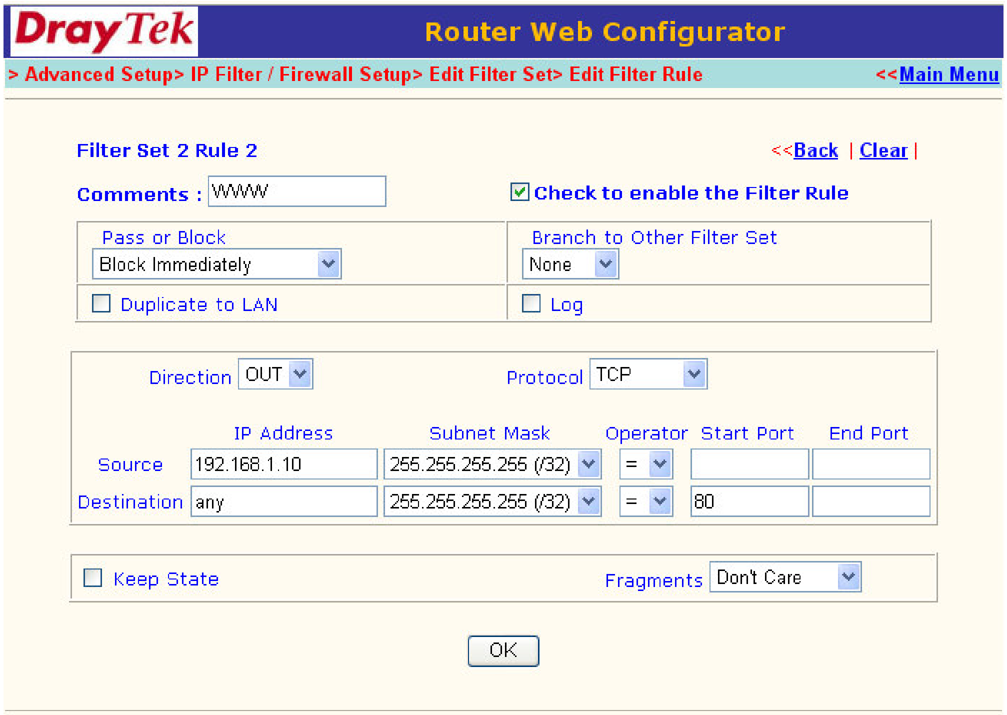
Fragmented: Applies the rule to fragmented packets.

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.


DrayTek
Router Web Configurator
> Advanced Setup> IP Filter / Firewall Setup> Edit Filter Set> Edit Filter Rule
<<Main Menu
<<Back | Clear |
OK

Filter Set 2 Rule 2

Comments : WWW

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: 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

CHAPTER 9-A

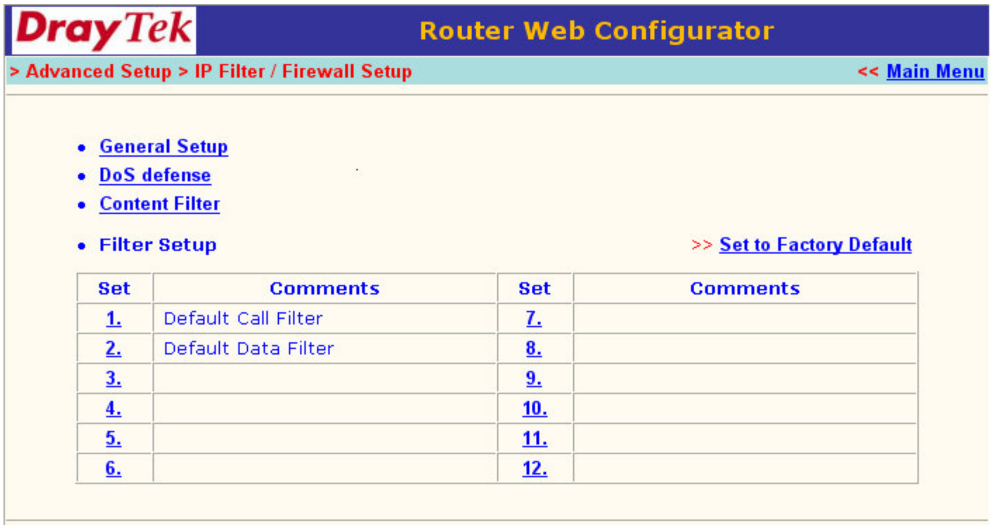
Prevention of Denial of Service Attacks

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.



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

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 Vigor 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 Vigor 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 router. The Vigor 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 Vigor 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 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 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 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 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.

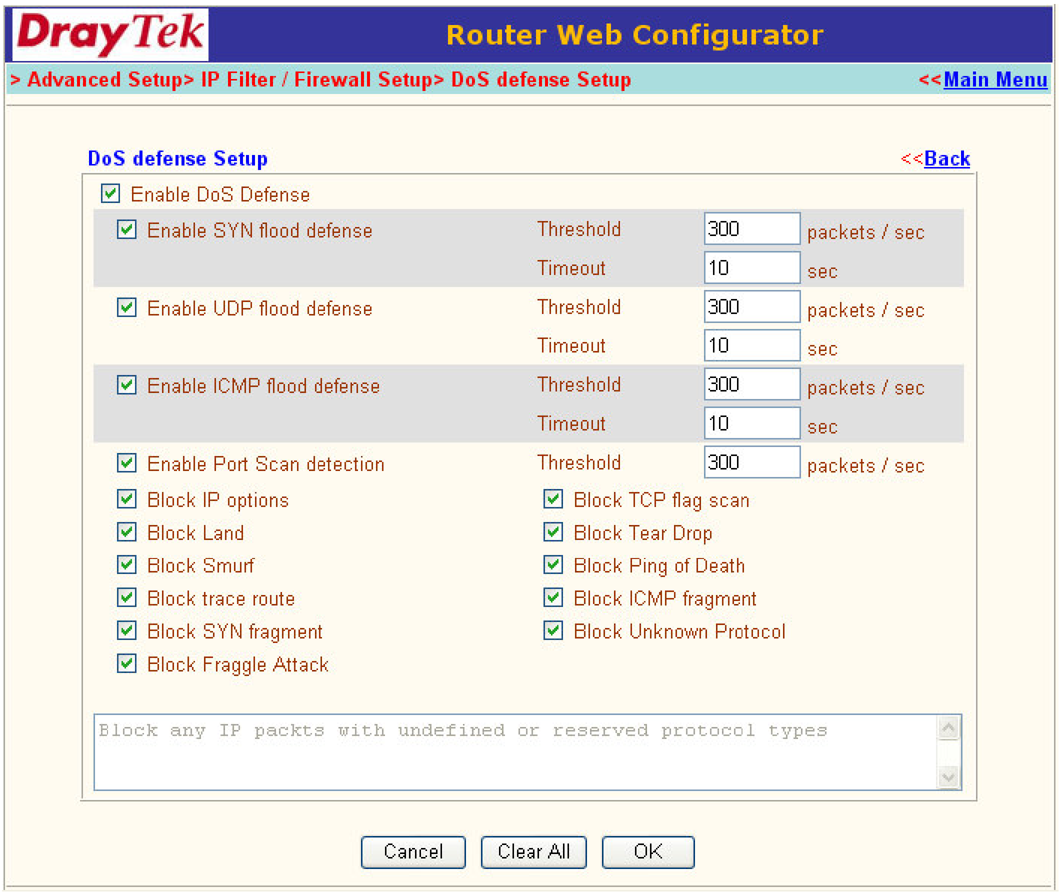
Enable TCP flag scan: Click the checkbox to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include ***no flag scan***, ***FIN without ACK scan***, ***SYN FIN scan***, ***Xmas scan*** and ***full Xmas scan***.

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 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 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.



☑ Enable DoS Defense

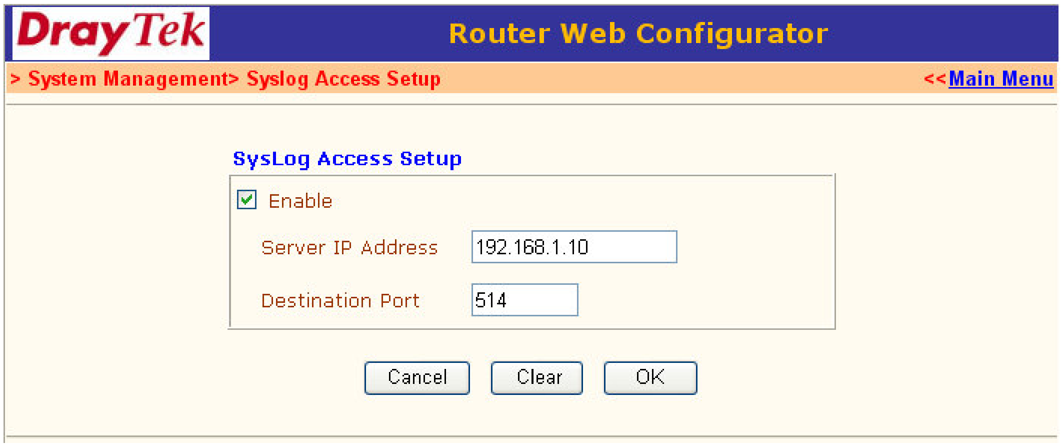
☑ Enable SYN flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable UDP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable ICMP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
☑ Enable Port Scan detection	Threshold	300	packets / sec

☑ Block IP options
☑ Block Land
☑ Block Smurf
☑ Block trace route
☑ Block SYN fragment
☑ Block Fraggle Attack
☑ Block TCP flag scan
☑ Block Tear Drop
☑ Block Ping of Death
☑ Block ICMP fragment
☑ Block Unknown Protocol

```
Block any IP packts with undefined or reserved protocol types
```

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.

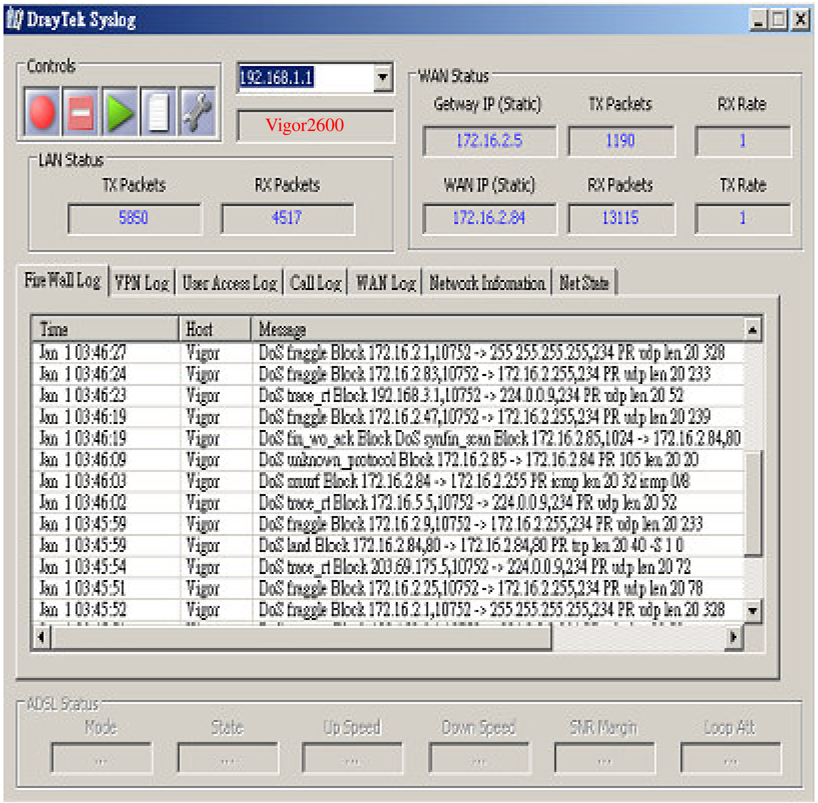


SysLog Access Setup

☑ Enable

Server IP Address: 192.168.1.10

Destination Port: 514



192.168.1.1

Vigor2600

LAN Status: TX Packets 5850; RX Packets 4517

WAN Status: Getway IP (Static) 172.16.2.5; TX Packets 1190; RX Rate 1; WAN IP (Static) 172.16.2.84; RX Packets 13115; TX Rate 1

```
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
```

CHAPTER 9-B

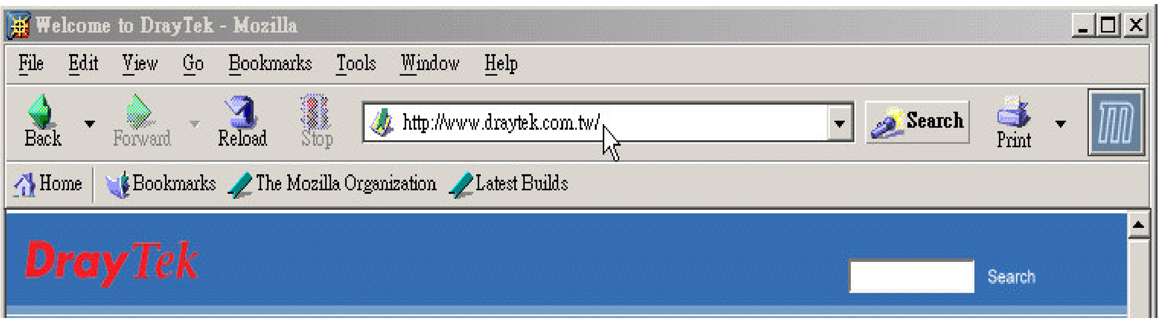
URL Content Filtering

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 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


Welcome to DrayTek - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://www.draytek.com.tw/
Search
Print
Home
Bookmarks
The Mozilla Organization
Latest Builds
DrayTek
Search

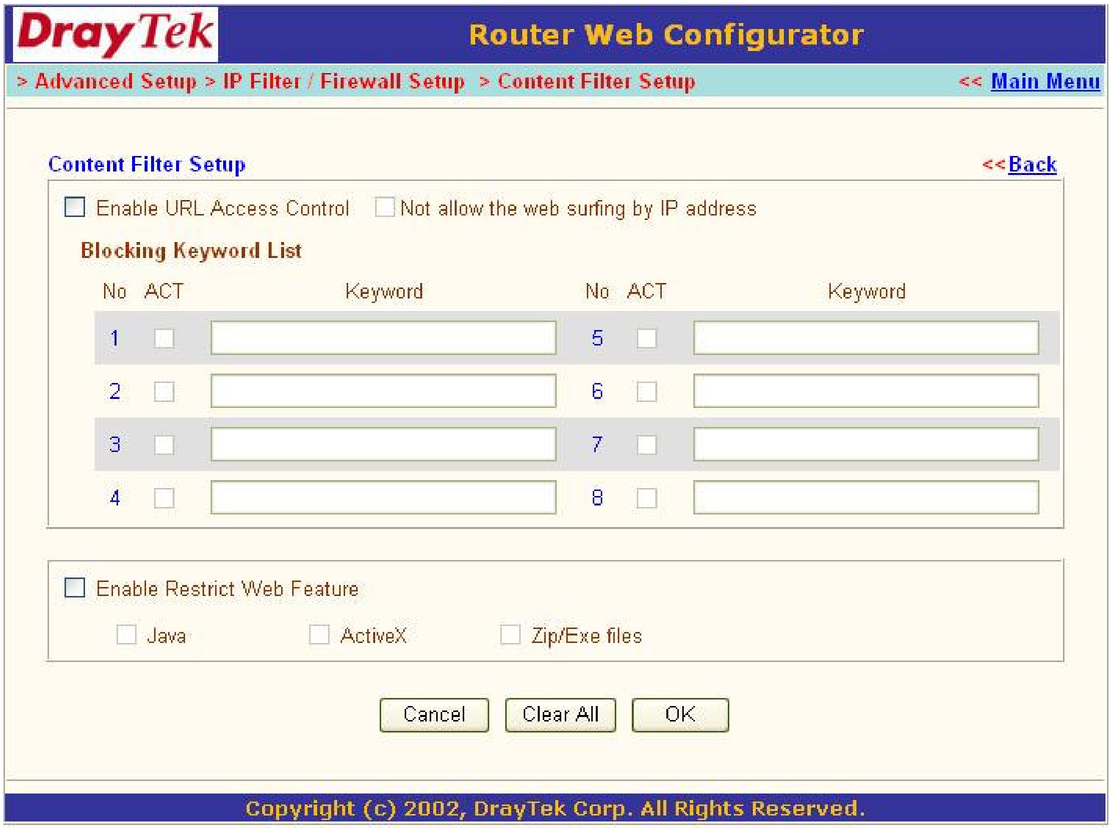
The URL content filtering facility in Vigor routers inspects every URL string in the HTTP request initiated inside against the keyword list. If the entire or part of the URL string (for instance, http://www.draytek.com.tw, as shown above) matches any activated keyword, its associated HTTP request will be blocked by the Vigor 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 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.


DrayTek
Router Web Configurator
> Advanced Setup > IP Filter / Firewall Setup > Content Filter Setup
<< Main Menu
Content Filter Setup
<<Back
☐ Enable URL Access Control
☐ Not allow the web surfing by IP address
Blocking Keyword List
No ACT Keyword No ACT Keyword
1 ☐
2 ☐
3 ☐
4 ☐
5 ☐
6 ☐
7 ☐
8 ☐
☐ Enable Restrict Web Feature
☐ Java
☐ ActiveX
☐ Zip/Exe files
Cancel
Clear All
OK
Copyright (c) 2002, DrayTek Corp. All Rights Reserved.

The URL content filtering facility supported in the Vigor router consists of the ***URL Access Control***, ***Not allow the web surfing by IP address*** and ***Restrict Web Feature*** . 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, ActiveX, Zip/Exe files.

The function of Not allow the web surfing by 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. 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 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 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 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 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 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 router will identify the forbidden URL and perform the blocking action for these websites by cutting the associated connections.

Not allow the web surfing 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 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, Zip/Exe files, 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.

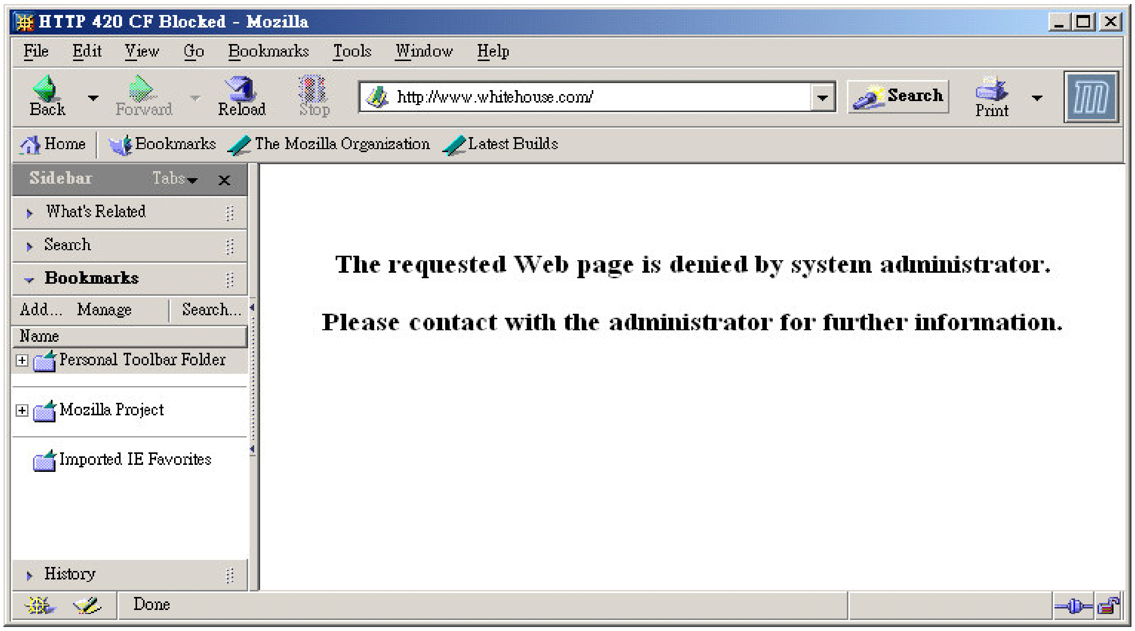
Java: Click the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.

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

Zip/Exe files: Click the checkbox to activate the Block Zip and Exe files function to prevent someone from downloading Zip/Exe files.

9-B.4 Warning Message

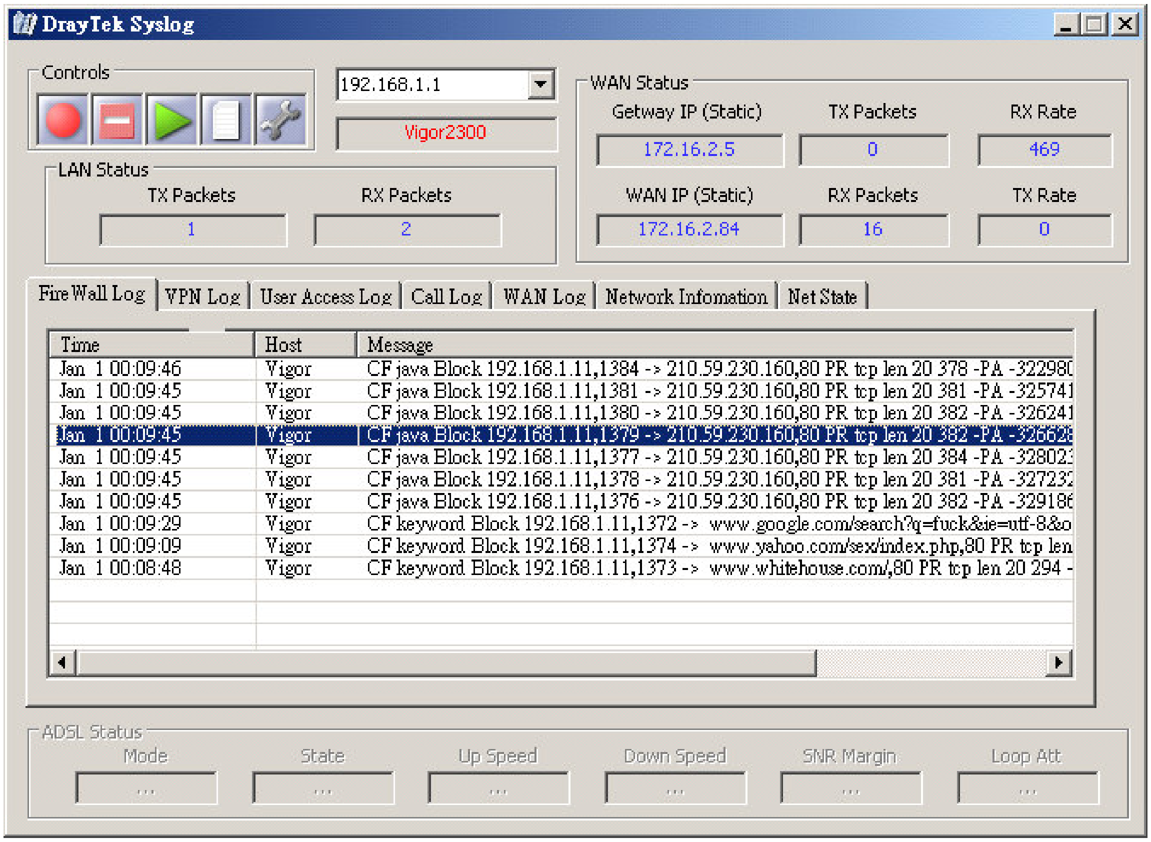
When a HTTP reqest is denied, an alert page will appear in your browser, as shown in the following figure.



The requested Web page is denied by system administrator.

Please contact with the administrator for further information.

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.



192.168.1.1

Vigor2300

LAN Status

TX Packets	RX Packets
1	2

WAN Status

Getway IP (Static)	TX Packets	RX Rate
172.16.2.5	0	469

WAN IP (Static)	RX Packets	TX Rate
172.16.2.84	16	0

```
Time             Host    Message
Jan  1 00:09:46  Vigor   CF java Block 192.168.1.11,1384 -> 210.59.230.160,80 PR tcp len 20 378 -PA -32298
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1381 -> 210.59.230.160,80 PR tcp len 20 381 -PA -325741
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1380 -> 210.59.230.160,80 PR tcp len 20 382 -PA -326241
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1379 -> 210.59.230.160,80 PR tcp len 20 382 -PA -32662
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1377 -> 210.59.230.160,80 PR tcp len 20 384 -PA -32802
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1378 -> 210.59.230.160,80 PR tcp len 20 381 -PA -32723
Jan  1 00:09:45  Vigor   CF java Block 192.168.1.11,1376 -> 210.59.230.160,80 PR tcp len 20 382 -PA -32918
Jan  1 00:09:29  Vigor   CF keyword Block 192.168.1.11,1372 ->  www.google.com/search?q=fuck&ie=utf-8&o
Jan  1 00:09:09  Vigor   CF keyword Block 192.168.1.11,1374 ->  www.yahoo.com/sex/index.php,80 PR tcp len
Jan  1 00:08:48  Vigor   CF keyword Block 192.168.1.11,1373 ->  www.whitehouse.com/,80 PR tcp len 20 294 -
```