IP Filter/Firewall Setup

Introduction

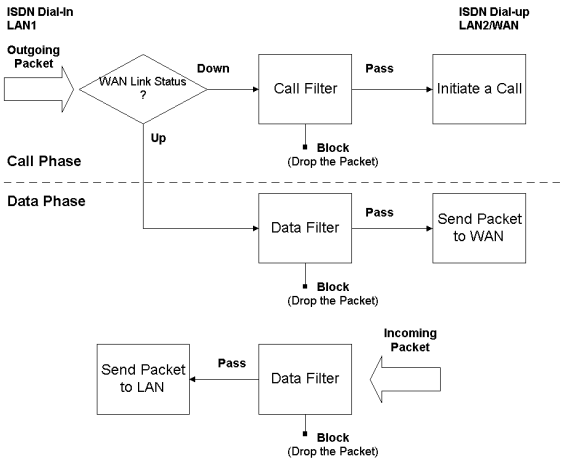
The IP Filter/Firewall function helps protect your local network against attack from outside. It also provides a method of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

An Overview of the Firewall

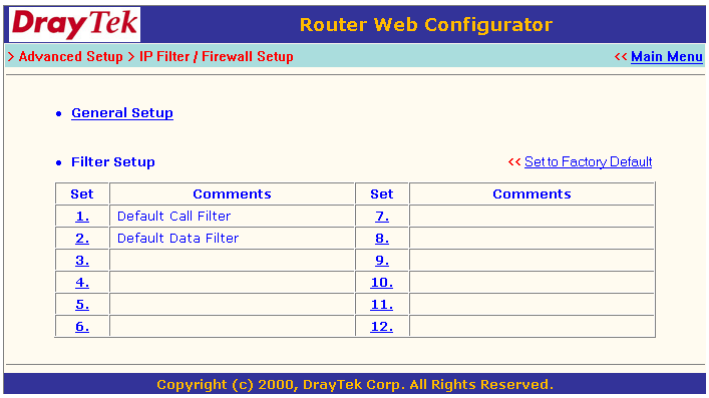
The IP Filter/Firewall includes two types of filter: Call Filter and Data Filter. The former is designed to block or allow IP packets that will trigger the router to establish an outgoing connection. The latter is designed to block or allow which kind of IP packets are allowed to pass through the router when the WAN connection has been established.

In concept, 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 dialling, 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 as below.



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



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

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

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

General Setup

On 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: 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.

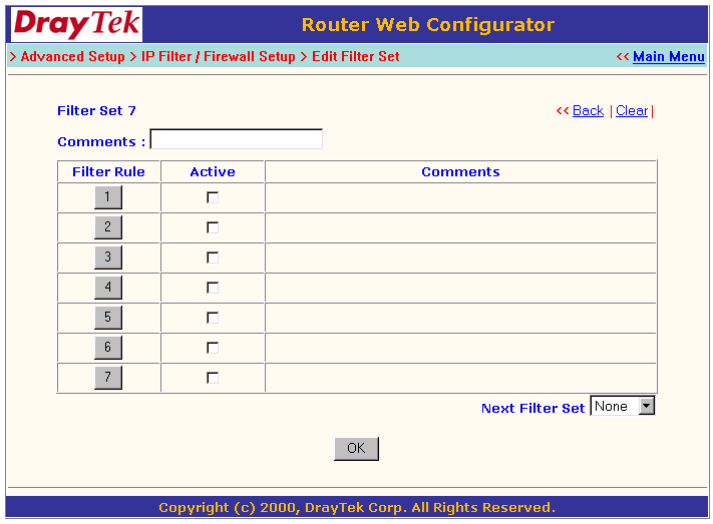
Pass: All passed packets will be logged.

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

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

MAC Adddress 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 (also see "Duplicate to LAN" on page 5-21). The feature will be helpful under Ethernet environments.

Editing the Filter Sets



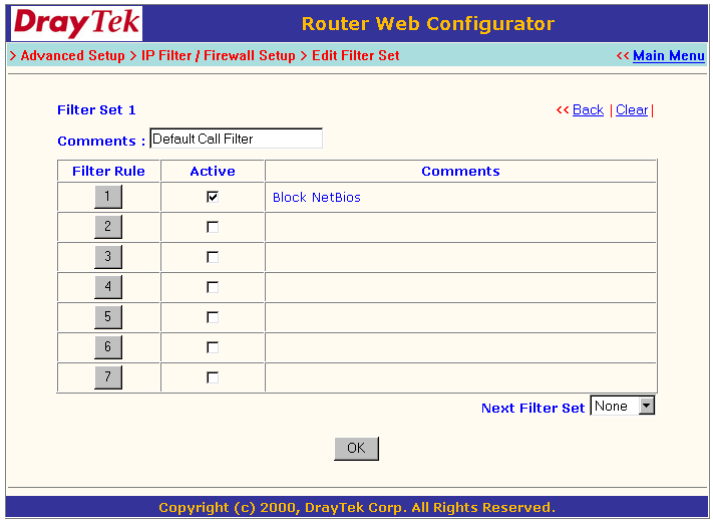
Comments: Enter filter set comments/description. Maximum length is 22 characters.

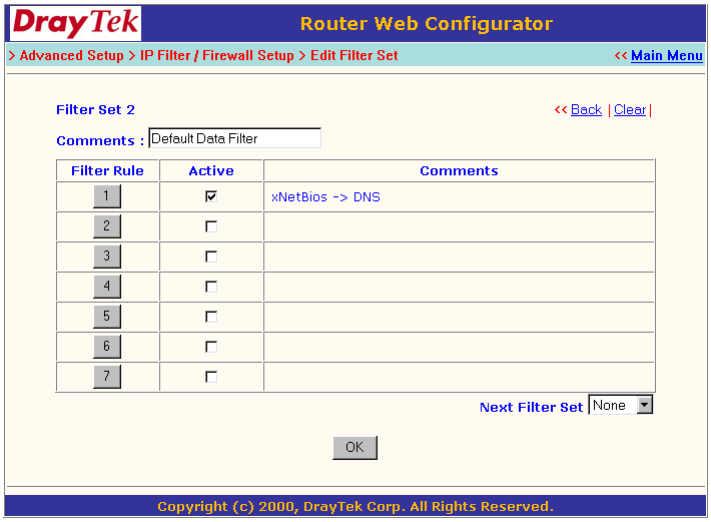
Filter Rule: Click a button numbered **1 ~ 7** to edit the filter rule.

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.





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.

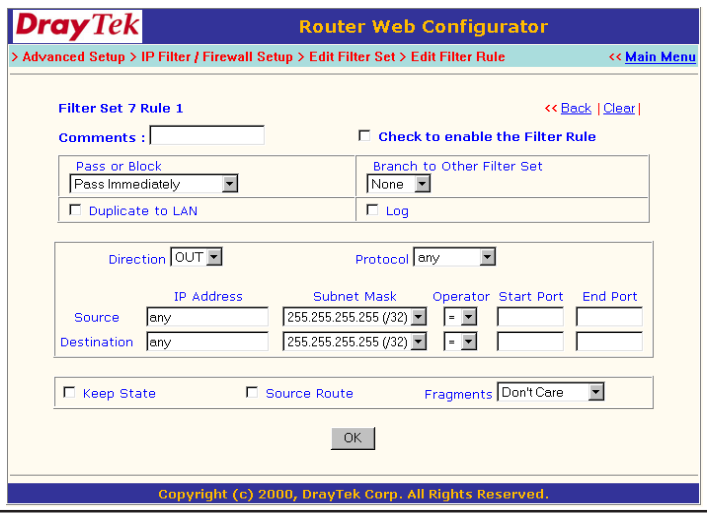
Pass or Block: Specifies the action to be taken when packets match the rule.

Block Immediately: Packets matching the rule will be dropped immediately.

Pass Immediately: Packets matching the rule will be passed immediately.

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** (see page 5-17).

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.

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.