
IP Filter/Firewall Setup

Introduction

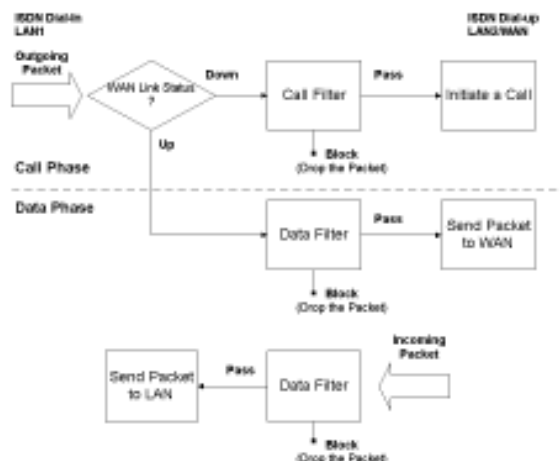
The IP Filter/Firewall function helps protecting your local network against attack from outside. It also provides a method of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection.

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.

> **Advanced Setup > IP Filter / Firewall Setup**
<< [Main Menu](#)

- [General Setup](#)
- [DoS defense](#)
- [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 Setup: The DoS Defense Functionality helps you to detect and mitigate the DoS attacks.

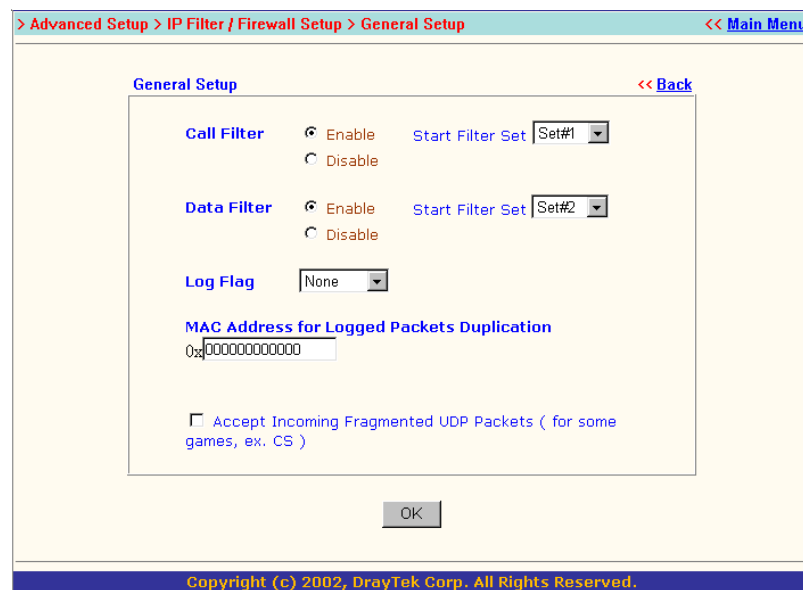
Filter Setup: Here there are 12 filter sets for IP Filter configurations.

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.

MACAddress 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.

Accept Incoming Fragmented UDP Packets:

Some on-line games (for example : Half Life) will use UDP packets with large length to transfer data. It need to be fragmented. As secure firewall, Vigor will reject these kinds of packets to avoid to be attacked by default. You can enable "Accept Incoming fragmented UDP Packet" function to accept these kinds of packets. Then you can play these kinds of on-line games. Of course, it might have some security concern.

DoS defense Setup

The DoS Defense Functionality helps you to detect and mitigate the DoS attacks. Those attacks including the mass attacks and the vulnerability attacks. The mass attacks attempt to use up all your system's resource while the vulnerability attacks try to paralyze the system by attacking the vulnerabilities of the protocol or operation system.

The DoS Defense Engine inspects each 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 Engine monitors the traffic behavior. Any anomaly situation violating the administrator's configuration is reported and the corresponding defense function is performed in order to mitigate the attack.

The following sections will explain in more detail about DoS Defense Setup by using the Web Configurator. It is a sub-functionality of IPFilter/Firewall. There are a total of 15 kinds of defense function for the DoS Defense Setup. By default, the DoS Defense Functionality is disabled. And once the DoS Defense Functionality is enabled, by default the threshold value is set to 300 packets per second and the timeout value is 10 seconds. One thing must be mentioned is that the threshold value should be not less than 150 packets per second while the timeout value should be not less than 5 seconds. A brief description about the defense function is shown below when the defense function is enabled or disabled.

The screenshot shows the 'DoS defense Setup' web configurator interface. At the top, there is a breadcrumb trail: '> Advanced Setup > IP Filter / Firewall Setup > DoS defense Setup' and a link '<< Main Menu'. The main title is 'DoS defense Setup' with a '<< Back' link. The interface contains several sections of settings:

- ☒ 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

Below these settings is a text area with the text: 'Block any IP packets with undefined or reserved protocol types'. At the bottom, there are three buttons: 'Cancel', 'Clear All', and 'OK'.

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. The router will discard the TCP SYN packets coming from the Internet and exceeding a configurable threshold (by default, 300 packets per second) in a period of time (by default, 10 second).

Enable UDP flood defense: Click the Checkbox to activate the UDP flood defense Function. The router will discard the UDP packets coming from the Internet and exceeding a configurable threshold (by default, 300 packets per second) in a period of time (by default, 10 second).

Enable ICMP flood defense: Click the Checkbox to activate the ICMP flood defense Function. The router will discard the ICMP echo requests coming from the Internet and exceeding a configurable threshold (by default, 300 packets per second) in a period of time (by default, 10 second).

Enable Port Scan detection: Click the Checkbox activate the Port Scan detection Function. The router will report a warning message when an intruder try to scan the host in the security zone 300 ports in one second (configurable). The intruder launches port scan to find out more information about the target host in order to perform attack in the future.

Enable Block IP options: Click the Checkbox to activate the Block IP options Function. The router will ignore any IP packets with option field appeared in its header.

Enable Block Land: Click the Checkbox to activate the Block Land Function. The router will discard any spoofed TCP packets having the identical source, destination IP address and the same source, destination port number sent with SYN flag set to a system.

Enable Block Smurf: Click the Checkbox to activate the Block Smurf Function. The router will ignore any ICMP echo request destined to the broadcast address.

Enable Block trace route: Click the Checkbox to activate the Block trace route Function. The router will reject to forward any trace route packets.

Enable Block SYN fragment: Click the Checkbox to activate the Block SYN fragment Function. Any packets with SYN flag set and more fragment bit set is 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 scans including 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, when their machine attempts to re-construct the packets the target's machine hangs. Any packets intend to do this are dropped.

Enable Ping of Death: Click the Checkbox to activate the Block Tear Drop Function. Many machines can be crashed by sending IP packets that exceed the maximum legal length. Any fragmented ICMP packets bigger than 1024 octets are discarded.

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. IP packet has a protocol field in the header to indicate the upper layer protocol. The protocol value bigger than 100 is not well-defined in the standard, therefore these packets should be discarded.

> System Management> Syslog Access Setup << Main Menu

SysLog Access Setup

☒ Enable

Server IP Address 192.168.1.33

Destination Port 514

Cancel Clear OK

The warning message

All the warning message is sent to syslog client when the syslog function is enabled. The administrator can setup the syslog client in the Syslog Setup by using Web Configurator. The administrator can view the warning messages coming from DoS Defense functionality through the Draytek Syslog daemon. The message format is similar to those in IPFilter/Firewall except beginning with the keyword “DoS” and following an name about what kind attack is detected.

DrayTek Syslog

Controls: [Buttons] 192.168.1.1 Vigor2300

LAN Status: TX Packets 5850 RX Packets 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 Information | 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
...

Editing the Filter Sets

The screenshot shows the 'Edit Filter Set' page for Filter Set 7 in the DrayTek Router Web Configurator. The page has a blue header with the DrayTek logo and 'Router Web Configurator'. Below the header is a breadcrumb trail: '> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set'. There are links for '<< Back' and 'Clear'. The 'Filter Set 7' title is at the top left. Below it is a 'Comments' text box. A table with three columns: 'Filter Rule', 'Active', and 'Comments' is shown. The table has 7 rows, numbered 1 to 7. The 'Active' column contains checkboxes, all of which are currently unchecked. Below the table is a 'Next Filter Set' dropdown menu set to 'None'. An 'OK' button is at the bottom center. The footer contains the copyright notice: 'Copyright (c) 2000, DrayTek Corp. All Rights Reserved.'

Filter Rule	Active	Comments
1	<input type="checkbox"/>	
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

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.

The screenshot shows the 'Edit Filter Set' page for Filter Set 1 in the DrayTek Router Web Configurator. The page has a blue header with the DrayTek logo and 'Router Web Configurator'. Below the header is a breadcrumb trail: '> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set'. There are links for '<< Back' and 'Clear'. The 'Filter Set 1' title is at the top left. Below it is a 'Comments' text box containing 'Default Call Filter'. A table with three columns: 'Filter Rule', 'Active', and 'Comments' is shown. The table has 7 rows, numbered 1 to 7. The 'Active' column contains checkboxes. In row 1, the checkbox is checked, and the 'Comments' column contains 'Block NetBios'. Below the table is a 'Next Filter Set' dropdown menu set to 'None'. An 'OK' button is at the bottom center. The footer contains the copyright notice: 'Copyright (c) 2000, DrayTek Corp. All Rights Reserved.'

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

DrayTek Router Web Configurator

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

Filter Set 2 << Back | Clear |

Comments : Default Data Filter

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	xNetBios -> DNS
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

Next Filter Set: None

OK

Copyright (c) 2000, DrayTek Corp. All Rights Reserved.

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.

> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set > Edit Filter Rule << Main Menu

Filter Set 1 Rule 7 << Back | Clear |

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

Source: any Subnet Mask: 255.255.255.255 (/32) Operator: = Start Port: End Port:

Destination: any Subnet Mask: 255.255.255.255 (/32) Operator: = Start Port: End Port:

☐ Keep State Fragments: Don't Care

OK

Copyright (c) 2002, DrayTek Corp. All Rights Reserved.

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.

The screenshot displays the 'Edit Filter Rule' configuration window for 'Filter Set 2 Rule 2'. The breadcrumb trail at the top reads: '> Advanced Setup > IP Filter / Firewall Setup > Edit Filter Set > Edit Filter Rule'. Navigation links '<< Main Menu' and '<< Back | Clear |' are present. The 'Comments' field contains 'WWW'. The 'Check to enable the Filter Rule' checkbox is checked. Under 'Pass or Block', 'Pass Immediately' is selected. 'Branch to Other Filter Set' is set to 'None'. 'Duplicate to LAN' and 'Log' checkboxes are unchecked. The 'Direction' is 'OUT' and the 'Protocol' is 'TCP'. The configuration table below shows: Source IP Address '192.168.1.10' with Subnet Mask '255.255.255.255 (/32)', and Destination 'any' with Subnet Mask '255.255.255.255 (/32)'. Both use the '=' operator. The 'Start Port' is empty and the 'End Port' is '80'. At the bottom, 'Keep State' is unchecked and 'Fragments' is set to 'Don't Care'. An 'OK' button is at the bottom center. The footer states 'Copyright (c) 2002, DrayTek Corp. All Rights Reserved.'

	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	