Conceptronic C100BRS4 Firewall Options

Firewall - Packet Filter

Packet filtering function enables you to configure your Router to block specified internal/external user (**IP address**) from Internet access, or you can disable specific service request (**Port number**) to /from Internet. You must check the **"Enable"** radio button to make the following figure appear for further configuration.

This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is **"or"** operation, which means the router checks these different filter rules one by one, stating from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Add
Click this button to add a new packet filter rule. After click, next figure will appear.

Edit
Check the Rule No. you want to edit. Then, click the "Edit" button.

Delete
Check the Rule No. you want to delete. Then, click the "Delete" button.

Outgoing/Incoming
Determine whether the rule is for outgoing packets or for incoming packets.

Active
Choose "Yes" to enable the rule, or choose "No" to disable the rule.

Packet Type
Specify the packet type (TCP, UDP, ICMP or any) that the rule will be applied to. Select **TCP** if you want to scope for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to scope for the connectionless application service on the remote server using the port number.

Log
Choose "Yes" if you want to generate logs when the filer rule is applied to a packet.

Action When Matched
If any packet matches this filter rule, forward or drop this packet.

Source/destination IP Address
Enter the incoming or outgoing packet's source/destination IP address(s).

Source/destination Port
Check the TCP or UDP packet's source/destination port number(s).

Firewall - MAC Filter

MAC filtering function enables you to configure your router to block specified internal user (MAC address) from Internet access.

MAC Address
Enter the MAC address you want to configure. Then, click the "Add" button to add this MAC address into the following list. If you want to eliminate the MAC address you have already set from the address list, select the MAC address in the list table and click the "Delete" button. The MAC address will no longer exist.

MAC Address List

Include
Select this radio button if you want the MAC addresses in the list to be blocked from accessing the Internet.

Exculde
Select this radio button if you want to block all the PCs in the LAN from Internet access except for those with MAC address listed in the list.

Firewall - Block Hacker Attack

The router can automatically detect and block the **DoS** (Denial of Service) attack if user enables this function.

This kind of attack is not to achieve the confiden tial data of this network; instead, it aims to crush specific equipment or the entire network. If this happens, the users will not be able to access the network resources. The following hacker patterns are implemented.

- IP Spoofing
- IP with Zero Length
- Land Attack
- UDP Port LoopBack
- Snork Attack
- Smurf Attack
- Ping of Death
- TCP XMAS Scan (System scan)
- TCP Null Scan (System scan)
- WinNuke Attack
- TCP SYN Flooding
- Ascend Kill
- IMAP SYN/FIN scan
- Net Bus scan (Trijan NetBus port communicati on with Hacker)
- Back Orifice scan (Trijan BackOrifice port communication with Hacker)

Firewall - Block Wan Request

Check **"Enable"** if you want to exclude outside PING request from reaching on this router.

Firewall - URL Blocking

Always Block
The default condition for all rules are to always enforce.

Blocked Time
To set the time of day range (in 24-hour format) and the day of the week range manually for all rules to be enforced.

Domains Filtering
To access Domains Filtering configuration, click on the button labeled **"Detail"** on the right side of the Domains Filtering.

The router allows you to customize its filtration features by adding or removing groups of sites from the Filter List.

To allow access to a Web site which appears in the Filter List, enter its host name, such as "www.ok-site.com" into the text field labeled Trusted Domains. Do not enter the complete URL of the site- that is, do not include "http://". All subdomains will be allowed. For example, entering "yahoo.com" will also allow "www.yahoo.com", "my.yahoo.com", "sports.yahoo.com", etc.

To block a Web site which does not appear in the Filter List, enter its host name, such as "www.bad-site.com" into the text field labeled Forbidden Domains. Users will no longer be able to access the sites from the LAN.

To remove a site which was previously added, select its name in the list box, and click the **Delete** button to send the update to router.

Disable Web traffic except for Trusted Domains: When the Disable Web traffic except for Trusted Domains box is checked, the router will only allow Web access to sites on the Trusted Domains list. This can be useful for carefully controlling Internet usage by employees or students.

Keywords Filtering
To access Keyword Filtering configuration, click on the button labeled **"Detail"** on the right side of the Keywords Filtering.

The router allows the administrator to block Web URLs containing keywords. This functions as a second line of defense against objectionable material. For example, if the keyword "XXX" were enabled, the pornographic site's URL http://www.new-site.com/xxx.html would be blocked, even if it was not included in the Filter List. Keywords in site names are also blocked (http://www.xxxsite.com would also be blocked).

To add a keyword, enter it in the "Keyword" field and click the **"Add"** button.

To remove a keyword, select it from the list and click the **"Delete"** button.