

Official Tech Documents
The better way to get your HotBrick product up and running

Firewall HotBrick LB-2 e LB-2 VPN

How To

How To Create Groups, Block URLs and Bind Ports on the LB2 and LB2-VPN

USA

7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

EUROPE

Generatorstraat 26
Hengelo (Ov), 7556 RC
Amsterdam - Netherlands
www.hotbrick.nl
support@hotbrick.nl

BRAZIL

Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

How to create Groups, Block URLs, and Bind Ports on the LB2 and LB2-VPN

To insure this procedure works, we will assume that the appliance has already been configured and is working properly on the local network and the internet.

This document may contain some illustrations that may not match your product because screens may vary depending on the firmware version.

In case of problems, please contact support at Hotbrick's website:

www.hotbrick.com/support.asp.

How to use HotBrick's URL Filter to block undesirable sites by groups

The Hotbrick LB-2 / LB-2 VPN have 5 different groups. These groups are part of the product's base functionality and control the permission level imposed by the administrator.

The custom groups consist of Group1, Group2, Group3 and Group4. The fifth group is the "Default" group. If the group is not specified, the computer will belong to the default group.

To block the undesirable URLs by groups, follow this procedure:

- Access the Hotbrick Graphical User Interface;
- Click "Advanced Setup";
- Click "Host IP".
- Select the group, associating the CPUs by the MAC Address* and by the Local IP address that could be reserved using DHCP. If the network uses static IP addresses, the CPU's information will have to be typed manually.
- Click "Add".

The screenshot shows the 'Host IP' configuration page in the HotBrick GUI. The page is titled 'Host IP' and has a 'HELP' icon. It contains two main sections: 'Host Network Identity' and 'Host Network Binding'. Below these is a table titled 'Host & Group List' showing the configuration for a host named '020-hbb'.

Host Network Identity

Host List	020-hbb	Select
Host Name	020-hbb	
MAC Address	00-0B-DB-E0-EE-A6 ex.(FF-FF-FF-FF-FF-FF)	
Select Group	Group 2	
Reserve in DHCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Reserved IP Address	10.10.1.100 ex.(xxx.xxx.xxx.xxx)	

Host Network Binding

Binding WAN Port / Session	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Binding Method	<input type="radio"/> Strict Binding <input checked="" type="radio"/> Loose Binding
Select WAN Port	WAN 1
Select PPPoE Session	Session 1

Host & Group List

Name	MAC Address	Group	DHCP	Reserve IP Address	WAN Binding	WAN Port	PPPoE Session
020-hbb	00-0B-DB-E0-EE-A6	Group 2	Enabled	10.10.1.100	Disabled		

Fig. 1: User Groups Creation

After you have placed the CPUs into groups, create the rules to block the URLs:

- Click "Security Management";
- Click "Block URL";
- Under "Access Group", select the group that will have access blocked;
- Scroll down to "Block Internet Access"; confirm that "Enable" is checked;
- Under "URL/IP/Keyword Blocked On Web Site", input the URLs, IP addresses or Keywords (Keyword - separating by asterisks, for example: *playboy*) will be blocked.
- Click "Submit" to finish.

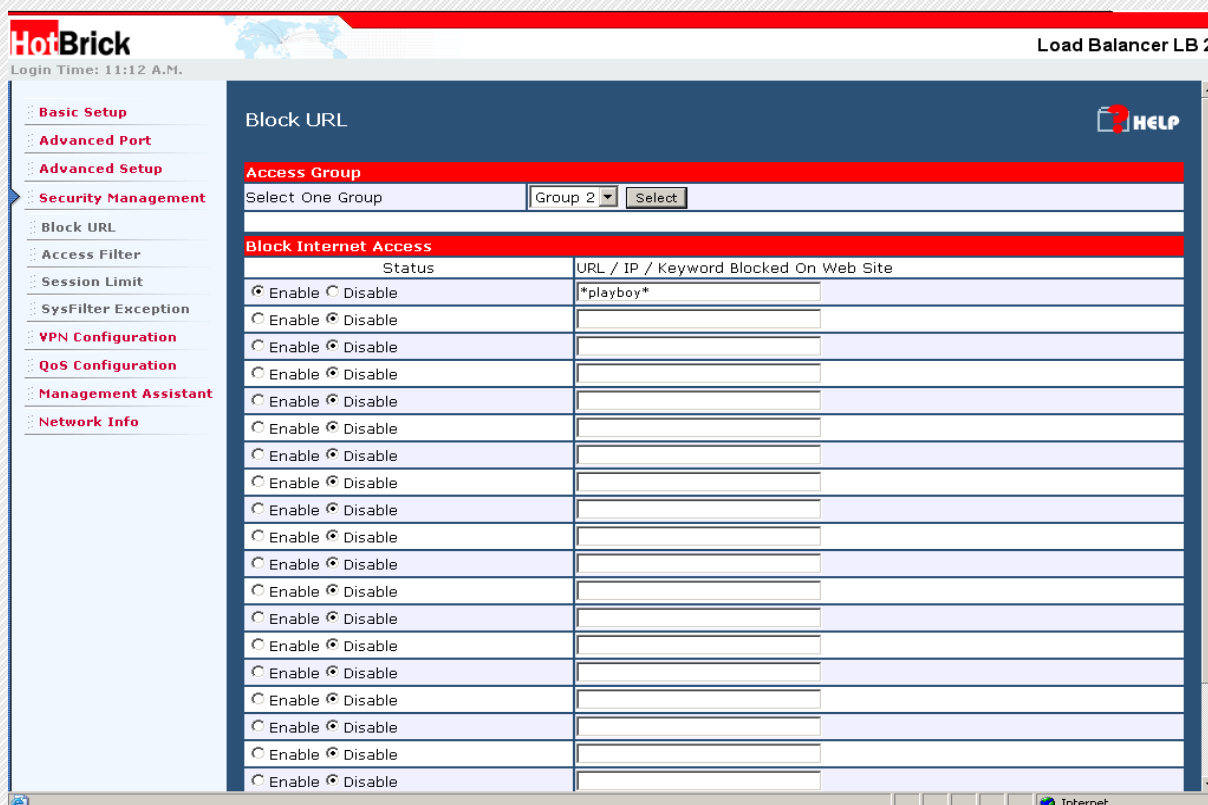


Fig. 2: Access Group Creation

*MAC Address (**Media Access Control address**), is identified by a unique address by the host (PC, Server) and is considered the "ID" of a computer on the network (internet). That is, it is a unique address composed of 6 pairs of letters and numbers that vary from 0 to 9 and from A to F (hexadecimal values), for example: 00-0B-CB-BD-0B-45. These addresses are unique.

How to block services such as MSN Messenger with HotBrick for groups of Users

The Hotbrick LB-2 / LB-2 VPN have 5 different groups. These groups are already available on the products and determine the permission level imposed by the administrator.

The groups are Group1, Group2, Group3 and Group4 and the fifth group is the "Default" group. If a computer does not belong to a specific group, it belongs to the default group.

To block the undesirable URLs by groups, follow this procedure: (Fig. 1)

- Access the Hotbrick Graphical User Interface;
- Click "Advanced Setup";
- Click "Host IP".

- Select the group, associating the CPUs by the MAC Address and by the Local IP address that can be reserved with DHCP. If the network has static IP addresses, the CPU's information will have to be typed manually.
- Click "Add".

After adding the CPUs to the groups, create the rules to block the port:

- Click "Security Management";
- Click "Access Filter" and block the access, selecting by the Group;
- Scroll down to "User Defined Ports to Block";
- Under "Name", input the service name "MSN";
- Under "TCP/UDP Packets", select the TCP protocol;
- Under "Port number Range", input the range with the port 1863~1864;
- Click "Submit";

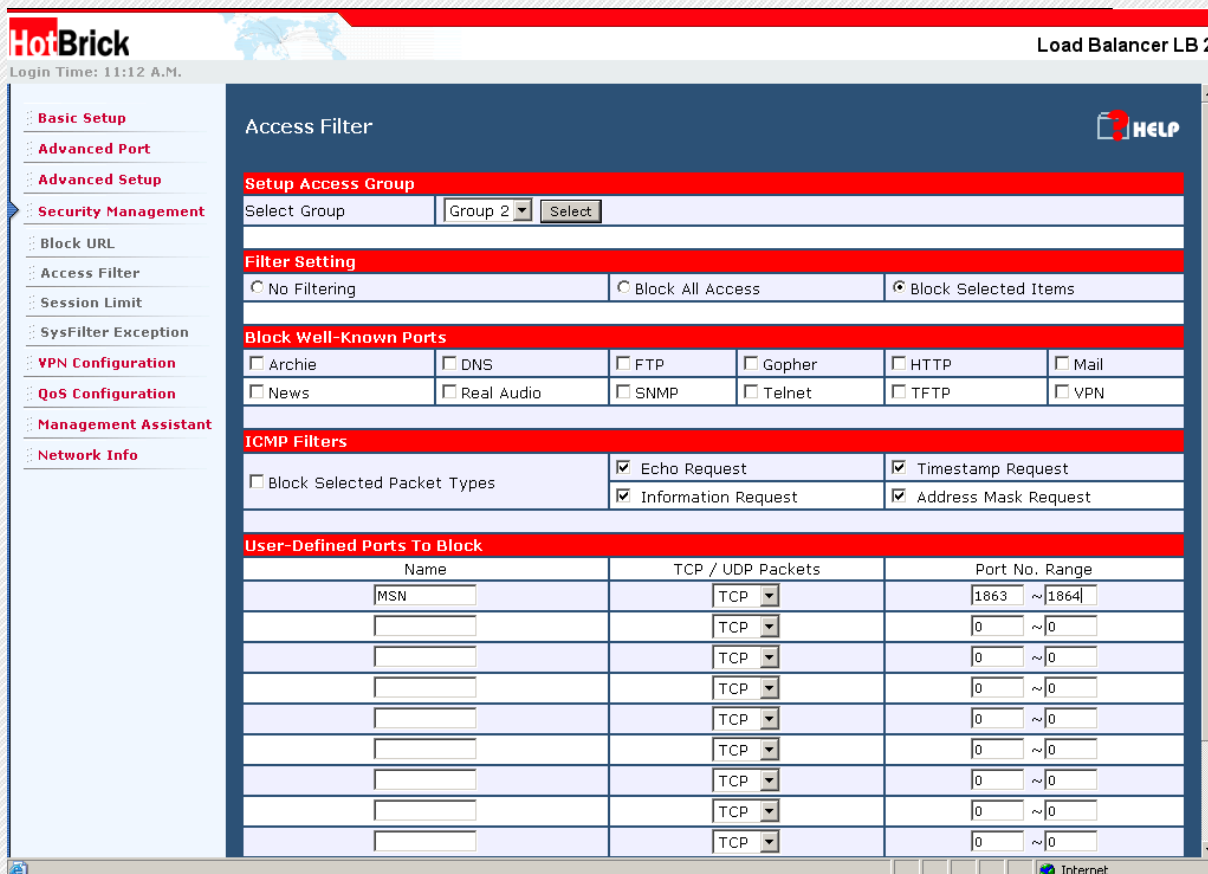


Fig. 3: Port Binding of MSN Ports

After you blocked the port, block the URLs, which use port 80:

- Click "URL Filter";
- Click "Block Internet Access";
- Under "Access Group", select the group that will have the access denied;
- Under "Block Internet Access", certify that the option "Enable" is checked;
- Under "URL/IP/Keyword Blocked On Web Site", input the URLs:
 - * gateway.messenger;
 - * baym-gw*msgr.hotmail.com;

- * e-messenger;
- * webmessenger.msn.com;
- Click "Submit".

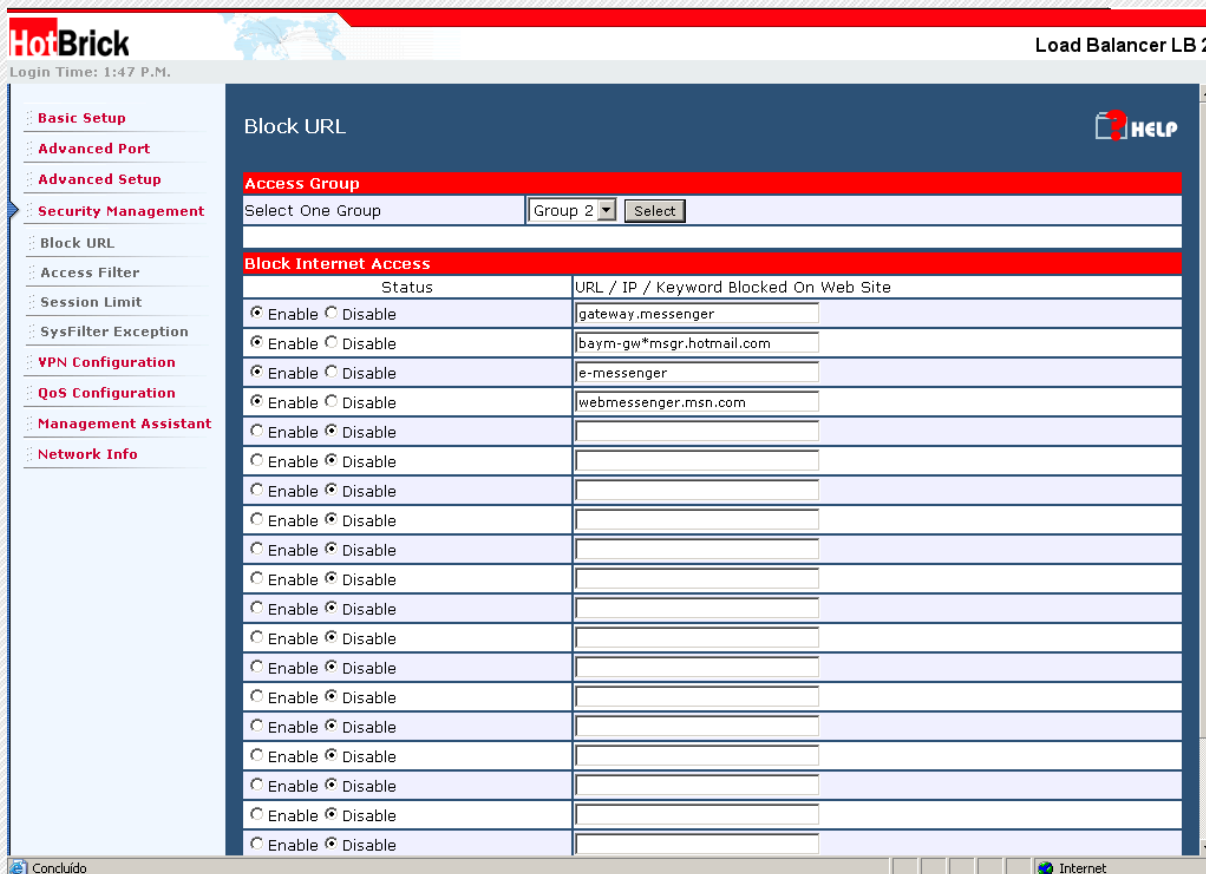


Fig. 4: URL Block of MSN Ports.

***This rule was working as of 05/25/05. The MSN program belongs to another company, therefore the methodology may change so the rule may not work anymore.*

How to block all the access by ports, by user groups using the Hotbrick

To block the ports by groups, follow this procedure: (Fig. 1)

- Access the Hotbrick Graphical User Interface;
- Click "Advanced Setup";
- Click "Host IP".
- Select the group, associating the CPUs by the MAC Address and by the Local IP address, that could be reserved with DHCP. If the network has static IP addresses, the CPU's information will have to be typed manually.
- Click "Add".

After you have assigned the CPUs to a group, create the rules to block the full access:

- Click "Security Management";
- Click "Access Filter", scroll down to "Setup Access Group" and select the group that will have the access blocked;

- Under "Filter Setting", enable the option "Block All Access"
- Click "Submit";

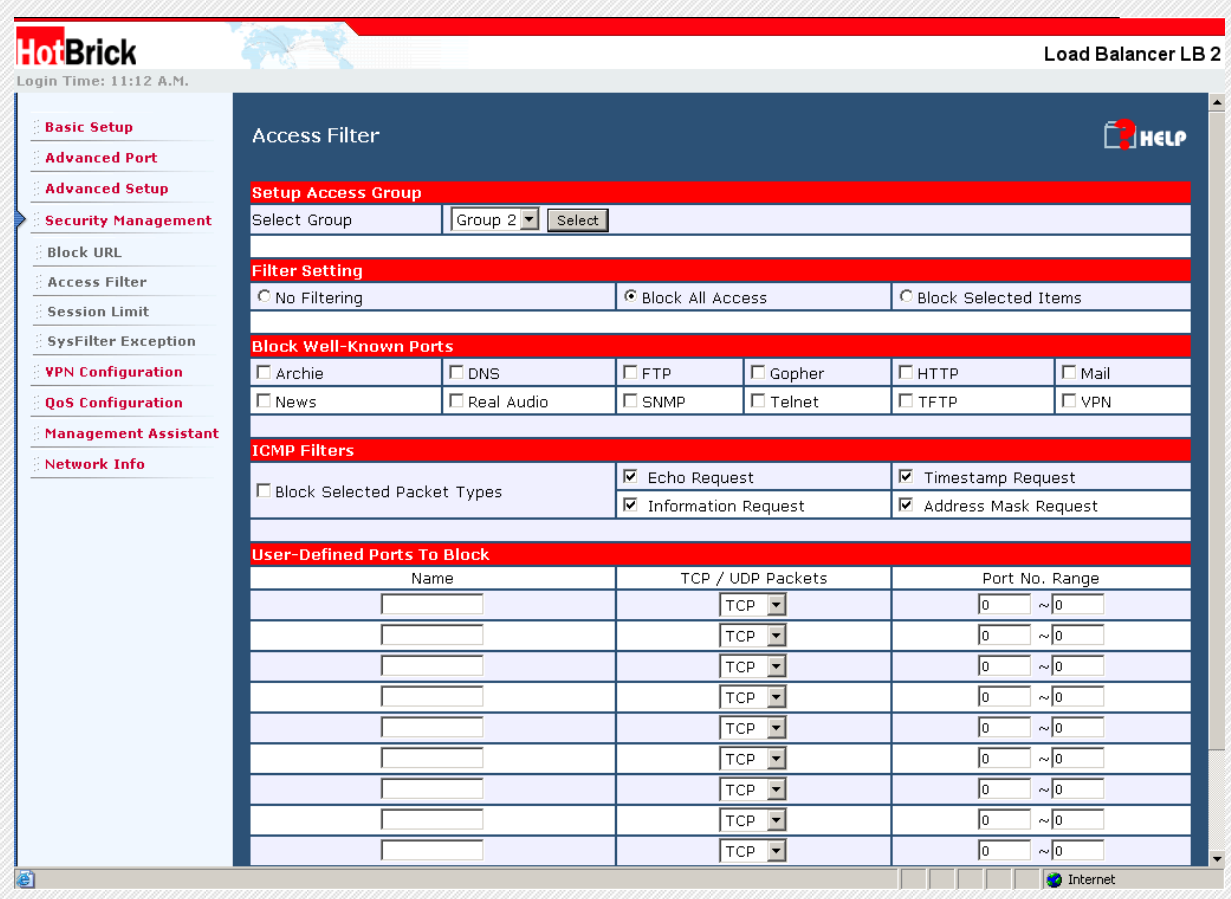


Fig. 5: Total Access Block