Firewall Configuration

Revision History

Revision	Date	Change Description
CPE-AN1500-R	07/16/14	Initial release

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617

Table of Contents

About This Document

Purpose and Audience

This document describes the firewall configuration on the BCA Broadband Router. Configuration of the firewall on the WAN and LAN side, as well as configuration of filters, virtual servers, and DMZ will be discussed.

This document is intended for software and system engineers.

Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use.

For a comprehensive list of acronyms and other terms used in Broadcom documents, go to:
http://www.broadcom.com/press/glossary.php.

Document Conventions

The following conventions may be used in this document:

Convention	Description
Bold	User input and actions: for example, type **exit**, click **OK**, press **Alt+C**
Monospace	Code: `#include <iostream>` HTML: `<td rowspan = 3>` Command line commands and parameters: `wl [-l] <command>`
< >	Placeholders for *required* elements: enter your `<username>` or `wl <command>`
[ ]	Indicates *optional* command-line parameters: `wl [-l]` Indicates bit and byte ranges (inclusive): [0:3] or [7:0]

Technical Support

Broadcom provides customer access to a wide range of information, including technical documentation, schematic diagrams, product bill of materials, PCB layout information, and software updates through its customer support portal (https://support.broadcom.com). For a CSP account, contact your Sales or Engineering support representative.

In addition, Broadcom provides other product support through its Downloads and Support site (http://www.broadcom.com/support/).

Enabling and Disabling the Firewall

The firewall can be enabled and disabled on a per-WAN service and on a per-LAN interface group basis. Typically, the firewall will be enabled on the WAN services and disabled on the LAN services.

WAN Side

To access HTTPD, SSH, and so on, on the modem from the WAN side, first we need to open the ports in **Advanced Setup > Security-IP Filtering > Incoming** (80 for HTTP, 22 for SSH, etc.).

> **Note:** To login from the WAN side, you must use the "support" user name.

LAN Side

Typically, the LAN side firewall is disabled. However, for some applications, such as an access point in a café, the LAN side firewall is also needed. The LAN side firewall can be enabled on a per-interface group basis. So for example, the interface group corresponding to BR0, which is connected via a secure ethernet wire to the office, may have the firewall disabled. However, another interface group corresponding to BR1, which provides general access to the public, may have the firewall enabled.

If you plan to enable the LAN side firewall, first you should create a "hole" for services you might need, such as HTTP. This can also be done on the **Advanced Setup > Security-IP Filtering > Incoming page**.

The firewall blocks access to the Broadband Router's local services. However, it does not block traffic going out the WAN connections.

Change from 3.x

The approach to access control in the 4.x release is significantly different than the 3.x approach. This new approach in the 4.x release can do everything that the 3.x approach can do, and also has the additional benefit of being more fine-grained (because it can control access on a per-interface basis) and being more in line with the TR-098 data model.

Virtual Servers

If a virtual server is added on ports already in use by the Broadband Router, then those internal ports will be redirected to different ports (ex: http 80 > 8080, ssh:22 > 2222, etc.)

> **Note:** To access the Broadband Router's HTTPD from the WAN side you have to use WANIP:8080 and this will be redirected to WANIP:80.

Important! The firewall should still open the original ports only (i.e., for HTTPD, open 80 not 8080).

BROADCOM®

Connecting
e v e r y t h i n g®