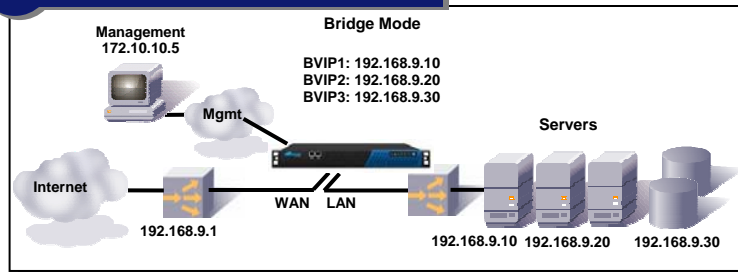


The Barracuda Web Application Firewall is a comprehensive Layer 7 security solution which protects your Web sites and Web application against hackers leveraging protocol and application vulnerabilities to instigate data theft, denial of service or defacement of your Web site. This guide describes the deployment of Barracuda Web Application Firewall in Bridge Mode, which is the factory-shipped default setting. The device can also be deployed as Reverse Proxy (route-path) or One-armed Proxy. The deployment methods and strategies are discussed in detail in the Barracuda Web Application Firewall Administrator's Guide.

3. Connect a standard VGA monitor, PS2 keyboard, and AC power cord to the unit. **Note:** Immediately after connecting an AC power cord to the unit, it may power ON for a few seconds and then power OFF.
4. Press the **POWER** button on the front panel to turn the unit ON.

The Barracuda Web Application Firewall supports Ethernet hard bypass mode. If you set device to hard bypass mode, the only way to access its device management interface is through the Ethernet network management port on the back panel. Consider connecting the management port located on the back panel of the unit to the network.

Bridge Mode



1 Getting Started

This guide provides setup instructions for Barracuda Web Application Firewall. We recommend that you read these instructions fully before proceeding. To begin setting up your Barracuda Web Application Firewall, you will need the following:

- Barracuda Web Application Firewall
- Mounting rails (model 660 and higher)
- AC power cord
- Ethernet cable (crossover cable might be needed)
- VGA monitor and PS2 keyboard (recommended)

2 Physical Installation

To install Barracuda Web Application Firewall:

1. Fasten Barracuda Web Application Firewall to a 19-inch rack or place it in a stable location.
2. Connect the network switch that is currently being used to access the Web site to the **WAN** port on the front panel of Barracuda Web Application Firewall. Connect the back-end server network to the **LAN** port.

3 Configure IP Address and Network Settings

If you have a VGA monitor connected, Barracuda Web Application Firewall displays the Boot Menu initially, and the Administrative Console login prompt once fully booted. To begin the configuration:

1. Login to the Administrative Console using the admin login:
 - **Login:** admin
 - **Password:** admin
2. Configure the **IP address for Barracuda Web Application Firewall, Network Mask, Default Gateway, DNS1, and DNS2** as appropriate for your network.
3. Save your changes.

```
barracuda login admin
password
```

If you do not have a monitor and keyboard, you can set the **System IP address** using the **RESET** button on the front panel, press and hold the **RESET** button per the following table:

IP address	Press and hold RESET for...
192.168.200.200	5 seconds
192.168.1.200	8 seconds
10.1.1.200	12 seconds

Note: The **System IP address** can be accessed using (a) A crossover cable connecting WAN, or (b) An Ethernet cable connecting the WAN to your network switch and accessing the system IP address over the network from your host.

4 Barracuda Web Application Firewall Configuration

Use a computer with a Web browser that is connected to the same network as Barracuda Web Application Firewall and follow these steps:

1. In your Web browser's address bar, enter http:// followed by Barracuda Web Application Firewall's IP address, followed by the default Web Interface HTTP Port (:8000). For example, if you configured Barracuda Web Application Firewall



Barracuda Web Application Firewall - Quick Start Guide

Application Firewall with an IP address of 192.168.200.200, you would type:
<http://192.168.200.200:8000>

- Log in to Barracuda Web Application Firewall's Web interface as the administrator.
Username: admin **Password:** admin
- Go to the **BASIC > IP Configuration** page and configure the following:
LAN IP Configuration: Enter the LAN port IP address and subnet mask that you will connect all of your Real servers to later.
- Go to the **BASIC > Administration** page and specify how and where to deliver system alerts and notifications from the Barracuda Central.
Email Notifications: Specify the SMTP Server, System Alerts Email Address and System Contact Email.
- Click any one of the **Save Changes** buttons to save all of the information.

5 Update the Firmware

- Go to the **ADVANCED > Firmware Update** page.
- Click **Download Firmware**. Click **OK** to acknowledge the download duration message. To avoid damaging Barracuda Web Application Firewall, do not power it OFF during an update or download. To view download progress, refresh your browser. You will be notified when the download is complete.
- On the **ADVANCED > Firmware Update** page, click **Apply Now** to apply the firmware. This will take a few minutes to complete.
- Click **OK** when prompted to reboot.
- After the system reboots, log in to the Web interface again and read the release notes to learn about enhancements and new features. It is also a good practice to verify settings, as new features may have been included with the firmware update.

6 Change the Administrator Password

To avoid unauthorized use, change the default administrator password to a more secure password. You can only change the administrator password for the Web interface. You cannot change the password for the Administrative Console, but this is only accessible via the keyboard, which you can disconnect at any time.

- Go to the **BASIC > Administration** page, and enter your old and new passwords.
- Click **Save Password**.

7 Product Activation

Verify that the Energize Updates feature is activated on your Barracuda Web Application Firewall by going to **BASIC > Status** page. Under **Subscription Status**, make sure the **Energize Updates** is displayed as **Current**. If the

Energize Updates is displayed as **Not Activated**; click the corresponding activation link to go to Barracuda Networks Product Activation page and complete the activation of your subscriptions.

8 Configure your First Service

The Barracuda Web Application Firewall is now ready for testing. For bridge mode deployment, connect the Web server you want to secure to the switch connected to the **LAN** port. Ensure that their IP addresses are within the LAN IP port address and subnet mask defined in Step 4 and LAN port IP address of Barracuda Web Application Firewall is reachable from the Web server.

- Go to **BASIC > Services** page and do the following in the specified fields:
 - Service Name:** Enter the name of the service you wish to create. This is a name you can use to identify the service in the future.
 - IP Address:** Enter the Global IP address of your Web server.
 - Port:** Enter the port on which your Web server responds (normally it is 80 for HTTP traffic and 443 for HTTPS traffic).
 - Type:** Select the service type as either HTTP or HTTPS from the drop-down list. **Note:** A certificate is required when the service type is HTTPS.
- Click **Add**.

The Barracuda Web Application Firewall is now ready for operation; the incoming traffic for your Web site is intercepted by Barracuda Web Application Firewall, inspected for any attacks and then forwarded to the Web server.

9 Test Connectivity

Verify network connectivity by using a machine in your existing network to access the service. Use your browser to access the Web site in the same way as you were doing earlier. For details on how to connect, refer the Bridge Mode illustration.

NOTE: The documentation is available at <http://www.barracuda.com/documentation>. Be sure to check out the Barracuda Networks Support Forum at <http://forum.barracuda.com> for Frequently Asked Questions and other helpful tips for setting up and using your Barracuda Web Application Firewall. For technical support, please contact support@barracuda.com.

Contact and Copyright Information

Barracuda Networks, Inc. 3175 S. Winchester Blvd., Campbell, CA 95008 USA • Phone: 408.342.5400 • www.barracuda.com
Copyright 2008 © Barracuda Networks, Inc. All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice. Barracuda Web Application Firewall is a trademark of Barracuda Networks, Inc. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders. 080408-70v4123-02-0408