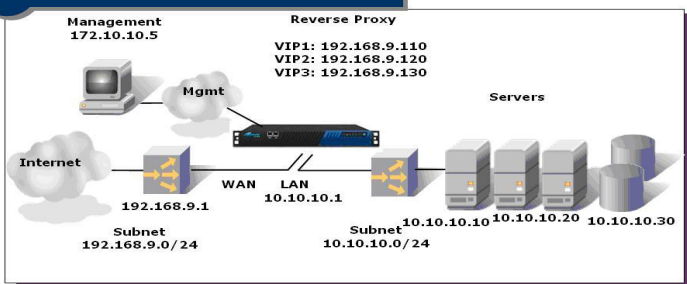


The Barracuda Web Application Firewall is a comprehensive Layer 7 security solution that protects your Web sites and Web applications against hackers who leverage protocol and application vulnerabilities to instigate data theft, denial of service or defacement of your Web site. This guide provides setup instructions for the Barracuda Web Application Firewall, and describes deployment for Reverse Proxy mode, the factory-shipped default setting. More information about other deployment modes and strategies, such as One-Armed Proxy and Bridge modes, can be found in the Barracuda Web Application Firewall Administrator's Guide. We recommend that you read these instructions *fully* before proceeding.

1 Reverse Proxy



1 Getting Started

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 the Barracuda Web Application Firewall:

1. Fasten the 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 the Barracuda Web Application Firewall. Connect the back-end server network to the **LAN** port.
3. Connect a standard VGA monitor, PS2 keyboard, and AC power cord to the unit. AC input voltage range is 110-240 volts at 50/60 Hz. **Note:** Immediately after connecting an AC power cord to the unit, it may power ON for a few seconds and then power OFF. This is because the Barracuda is designed to automatically return to a powered ON state in the event of a power outage.
4. Press the **POWER** button on the front panel to turn ON the system.

3 Configure IP Address and Network Settings

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

1. Log in 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 by pressing and holding 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 (1) a crossover cable connecting WAN, or (2) an Ethernet cable connecting the WAN to your network switch and accessing the system IP address over the network from your host.

4 Open Firewall Ports

If your Barracuda Web Application Firewall is located behind a network firewall, the following ports need to be open:

Port	Direction	TCP	UDP	Usage
22	Out	Yes	No	Only required for Technical Support connections
80	Out	Yes	No	Virus/attack and security def updates
123	Out	No	Yes	Network Time Protocol

5 Configure the Barracuda Web Application Firewall

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

1. In your Web browser's address bar, enter http:// followed by the Barracuda Web Application Firewall's IP address, followed by the default Web Interface HTTP Port (:8000). For example, if you configured the Barracuda Web Application Firewall with an IP address of 192.168.200.200, you would type: <http://192.168.200.200:8000>
2. Log in to the 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 to which you will later connect all of your Real Servers.
- Go to the **BASIC > Administration** page and specify how and where to deliver system alerts and notifications from Barracuda Central.
 - Email Notifications:** Specify the SMTP Server, System Alerts Email Address and System Contact Email Address.
- Click any one of the **Save Changes** buttons to save all of the information.

6 Update the Firmware

- Go to **Advanced > Firmware Update** to check for the latest firmware updates. If none are available, skip to Step 7.
- Click on the **Download Now** button located next to the firmware version that you wish to install. To view download progress, click the **Refresh** button. When the download is complete, the **Refresh** button will be replaced by an **Apply Now** button. To avoid damaging the system, *do not power OFF* during a firmware update or download.
- Click the **Apply Now** button to apply the firmware. This will take a few minutes to complete and will automatically reboot the system.
- After applying the firmware, you will be required to log in again to the Web interface. Make sure to read the release notes to learn about enhancements and new features. It is also good practice to verify settings, as new features may have been included with the firmware update.

7 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.

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

NOTE: This will only change the password used to log into the Web interface. The password for the **admin** user (used to log into the Administrative Console) can be done by logging into the Console.

8 Product Activation

Verify that the Energize Updates feature is activated on your Barracuda Web Application Firewall. From the **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 on the corresponding activation link to visit the Barracuda Networks Product Activation page and complete the activation of your subscriptions.

9 Configure your First Service

The Barracuda Web Application Firewall is now ready for testing. For Reverse

Proxy mode deployment, connect the Web server(s) you want to secure to the switch connected to the **LAN** port. Ensure that the IP address(es) of the Web server(s) are within the LAN port IP address and subnet mask range as defined in Step 4, and that the LAN port IP address of the Barracuda Web Application Firewall is reachable from the Web server.

- Go to the **BASIC > Services** page and do the following in the specified fields:
 - Service Name:** Enter a name for the service you wish to create. This is a name you can use to identify the service in the future.
 - 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.
 - Virtual IP:** Enter a new virtual IP address that would be used for accessing this application.
 - Port:** Enter the port on which your Web server responds (normally it is 80 for HTTP traffic and 443 for HTTPS traffic).
 - Real Servers:** Enter the IP Address of the server that hosts the service. This is the backend server that is protected by the Barracuda Web Application Firewall.
 - Group:** This setting provides the logical grouping for services. Create a new group to add the service under that group. If no group is specified, the service is added under the **default** group.
- Click **Add**.

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

10 Test Connectivity

Verify network connectivity by using a system in your existing network to access a configured Service. You should be able to reach your protected application by using your browser and navigating to the Virtual IP address and port specified in Step 9.1.

NOTE: More 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 2008-2012 © 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. 120127-74v0022-01-0127