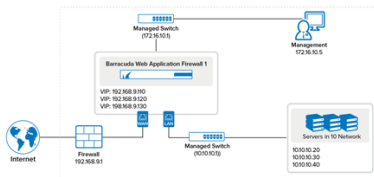


30-Day Evaluation Guide - Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/41113099/>

Use this article as a sample road map for setting up and testing the Barracuda Web Application Firewall in your organization's environment:

1 Evaluate Deployment Options



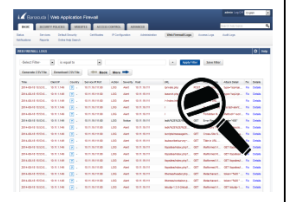
2 Deploy the Barracuda Web Application Firewall and Complete the Initial Setup



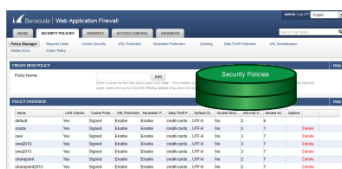
3 Add Services and Default Policies



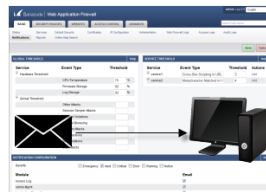
4 Review Logs



5 Fine Tune Security Policies



6 Configure Notification Alert Policies



7 View Reports



8 Configure Syslog Server(s)



Step 1. Evaluate Deployment Options

Before you install the Barracuda Web Application Firewall, determine the deployment option that best suits your environment. The Barracuda Web Application Firewall recommends **One-Arm Reverse Proxy deployment** for the evaluation process. This deployment enables you to perform functionality testing with minimal disruption to the production traffic.

Deployment Options for Hardware Appliances

The Barracuda Web Application Firewall supports both **Reverse Proxy (One-Arm Proxy Deployment or Two-Arm Proxy Deployment)** and **Bridge-Path**. For more detailed information, see [Choosing Your Deployment](#).

Deployment Options for Virtual Appliances

The Barracuda Web Application Firewall Vx supports only **Reverse Proxy (One-Arm Proxy Deployment or Two-Arm Proxy Deployment)**.

Step 2. Deploy the Barracuda Web Application Firewall and Complete the Initial Setup

Complete one of the following sets of instructions based on your deployment:

Hardware Appliances

- Follow the instructions in the Barracuda Web Application Firewall Quick Start Guide included with your appliance.
- (Optional) Complete the steps mentioned in [Step 1: Installing the Barracuda Web Application Firewall](#).

Virtual Appliances

- Download the Barracuda Web Application Firewall Vx image for your hypervisor from the [Barracuda Networks Virtual Appliance Download](#) page.
- Deploy and install the Barracuda Web Application Firewall Vx by following the steps mentioned in [Virtual Deployment](#).
- Complete the steps in [Barracuda Web Application Firewall Vx Quick Start Guide](#).
- (Optional) Complete the steps mentioned in [Step 1: Installing the Barracuda Web Application Firewall](#).

Step 3. Add Services and Default Security Policy

After you install the Barracuda Web Application Firewall based on your deployment mode, go to the **BASIC > Services** page and add HTTP or HTTPS services. For more information on creating a service, see [Step 2: Configuring a Service](#).

If deployed as a Two-Arm Proxy, all production and test traffic to the web applications goes via the Barracuda Web Application Firewall. If deployed as a One-Arm Proxy, you can have separate paths for production and test traffic. The production path bypasses the Barracuda Web Application Firewall so that there is no disruption. You can generate test traffic by browsing the application via the service created on the Barracuda Web Application Firewall. Test traffic should contain few attacks and some normal traffic.

A newly configured service uses the default security policy, typically with mode set to **Passive**. Policy violations are logged but not blocked in passive mode.

Change the mode to **Active** to log and block attacks. All attacks are logged in the **BASIC > Web Firewall Logs** page. For any blocked request that should have been allowed (false positive), navigate to the **BASIC > Web Firewall Logs** page and use the one-click policy tuner to fine tune the policies.

For more information, refer to [Step 5. Fine Tune Security Policies](#).

Step 4. Review Logs

The Barracuda Web Application Firewall applies rules to traffic and generates a log of rule violations, viewable in the **BASIC > Web Firewall Logs** page.

The Barracuda Web Application Firewall provides the following logs:

- **Web Firewall Logs** - Displays the details of the attacks on the web application. For a description of attacks, see [Attacks Description - Action Policy](#).
- **Access Logs** - Logs all requests that are made to the configured service(s).
- **Audit Logs** - Monitors and logs all changes made to the system by the administrator.
- **System Logs** - Logs all error reports, system alerts, diagnostic messages, and status messages of the Barracuda Web Application Firewall from the hardware and software components.
- **Network Firewall Logs** - Logs all network traffic passing through the interfaces (WAN, LAN and MGMT) matching the configured network ACL rule.

For information on how to configure the syslog server and export all logs, see [How to Export Logs from the Barracuda Web Application Firewall](#).

You can use the web firewall logs to evaluate rule violations, and when warranted, create exceptions to the rule violated. Exceptions can apply globally if you modify the security policy, i.e. the security policy affects all services. For a description of attacks, see [Attacks Description - Action Policy](#).

Step 5. Fine Tune Security Policies

You can evaluate the logs and fine tune the web firewall policies in the **BASIC > Web Firewall Logs** page. You can step through the logs and identify false positives, if any, and use the **Fix** button to fine tune the policy.

For more information on how to tune security policies using web firewall logs, see [Tuning Security Rules Using Web Firewall Logs](#).

Step 6. Configure Notification Alert Policies

You can enable notification alerts to send email notifications to the administrator when certain events occur in the module(s) or the configured threshold is exceeded. You can select single or multiple modules and set the severity level requiring email notification alerts. You can also set the threshold limit for the hardware components, attack categories, and each attack type under service(s).

To enable notification alerts for the modules(s), go to the **BASIC > Notifications > Notification Configuration** section. Select the modules and severity level, and then click **Save**.

To enable notification alerts for the hardware components, attack categories, and attack types per service, go to the **BASIC > Notifications > Global Threshold/Service Threshold** section. Set the threshold limit, and then click **Save**.

For more information, see [Configuring Notifications](#).

Step 7. View Reports

You can configure and generate reports of various types in the **BASIC > Reports** page. You can generate a one-time report or configure the Barracuda Web Application Firewall to automatically generate the reports on an hourly, daily, weekly, or monthly basis.

In the **BASIC > Reports** page, you can generate the following reports:

- **Security Reports** - Web attack prevention activity performed by the Barracuda Web Application Firewall.
- **Administrator Audit Reports** - Server details and the login/logout activities performed by different user roles.
- **Traffic Reports** - Web traffic activities monitored by the Barracuda Web Application Firewall.
- **Config Summary Reports** - Barracuda Web Application Firewall features such as Load Balancing, Rate Control, Learning, etc., details of installed certificates, user accounts and their privileges, and profiles and access control rules associated with the service.
- **PCI Reports** - PCI compliance details on the Barracuda Web Application Firewall.

For more information, see [Reporting](#).

Step 8. Configure Syslog Server(s)

You can configure the syslog server(s) and transmit logs (access logs, audit logs, web firewall logs, system logs, and network firewall logs) to your syslog server(s). You can configure a maximum of three (3) syslog servers.

The Barracuda Web Application Firewall initiates the connection and transmits logs to the available syslog server(s).

To configure a syslog server:

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Syslog** section, click **Add Syslog Server**.
3. In the **Add Syslog Server** window:
 - Enter the details of the syslog server (IP address and Port).
 - Select the connection type (UDP, TCP or SSL).
 - Select whether to validate syslog server certificate or not.
 - Select whether you want the Barracuda Web Application Firewall to present certificate while connecting to the syslog server or not.
 - Click **Add**.

For more information, refer to the online help button.

Figures

1. eval_guide.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.