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:

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 to carry out the evaluation process. This deployment enables you to perform functionality testing with minimal disruption to the production traffic.

Deployment Options for Hardware Appliances

You can either deploy in **Reverse Proxy** (**One-Arm Proxy Deployment** or **Two-Arm Proxy Deployment**), or **Bridge-Path**. For detailed information, see Choosing Your Deployment.

Deployment Options for Virtual Appliances

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

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

Depending on whether you are evaluating a hardware or a virtual appliance, complete one of the following sets of instructions:

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 and choose the 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 traffic to the web applications – production and testing – goes via the Barracuda Web Application Firewall. If deployed as a One-Arm Proxy, then you can have separate paths for production traffic and test traffic. The production path bypasses the Barracuda Web Application Firewall, so there is no disruption. 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 originally 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 as well as block the 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. 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 the Attacks Description - Action Policy article.
- **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 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 syslog server and export all logs, see the How to Configure Syslog and other Logs article.

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. it affects all services using that policy. For a description of attacks, see the Attacks Description - Action Policy article.

Step 5. Fine Tune Security Policies

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

For more information on how to tune security policies using web firewall logs, see the Tuning Security Rules Using Web Firewall Logs article.

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. Also, you can set the threshold limit for the hardware components, attack categories and for each attack type under service(s).

To enable notification alerts for the modules, 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** sections, set the threshold limit and click **Save**.

For more information, see the Configuring Notifications article.

Step 7. View Reports

You can configure and generate reports of various types on the **BASIC > Reports** page. It is possible to 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.

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

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

For more information, see the Reporting article.

Step 8. Configure Syslog Server(s)

You can configure 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, set the connection type to transmit the logs on the **ADVANCED > Export Logs > Syslog** section.

The Barracuda Web Application Firewall initiates the connection and transmits logs to the available

syslog server.

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**.

Figures

1. WAF_Eval_Guide_New.png