System Configurations

https://campus.barracuda.com/doc/55312405/

The Barracuda Web Application Firewall system settings should be configured properly to ensure consistency of events, logs, alert,s and security across an organizations infrastructure.

Configure Administrator Email Notifications

The Barracuda Web Application Firewall sends email alerts in response to system and threat alerts. To set the administrator email:

1. Go to the **BASIC > Administration** page.
2. Enter the administrative email address and the mail server configuration information in the **Email Notifications** section.
3. Click **Save**.

> Barracuda Networks highly recommends that administrators configure the administrator email account on the account to receive important notifications.

Configure External Logging Systems

The Barracuda Web Application Firewall stores five types of logs:

Log Type	Description
Web Firewall Logs	Logs all actions/events on the Barracuda Web Application Firewall. These logs help the administrator analyze traffic for suspicious activity and fine-tune the security settings.
Access Logs	Logs all web traffic activities. These logs provide information about the website traffic and performance.
Audit Logs	Logs all administration and configuration activities. This information assists in audits.
System Logs	Logs system events.
Network Firewall Logs	Logs events generated whenever network traffic passing through the interfaces (WAN, LAN and MGMT) matches the configured Network ACL rule.

Logs are stored in a circular queue and are overwritten once the log file reaches the maximum size. Log data can be exported using FTP to an external storage system for archival or exported using

syslog to a Security Information and Event Management (SIEM) for analysis and storage. The Barracuda Web Application Firewalls supports syslog exports to popular SIEM tools, including ArcSight, Splunk, Q1Labs QRadar, RSA enVision, Symantec SIEM, eIQ Networks SecureVue and TriGeo SIM. To set up an external FTP or syslog server, go to the **ADVANCED > Export Logs** page. For more information on Logs, see [Logging, Reporting and Monitoring](#).

> Barracuda Networks highly recommends that administrators set up an external storage or SIEM system to store log data.

Configure SNMP Traps for Health Monitoring

In addition to email alerts, the Barracuda Web Application Firewalls can send traps to notify administrators of system alerts. SNMP traps can be configured on the **BASIC > Administration** page. Documentation of MIB definitions can be found at *http://<WAF-IP Address>/cgi-bin/download_mib.cgi* or by clicking the **Barracuda Web Application Firewall MIB** link provided in the **BASIC > Administration** page, **SNMP Manager** section online help. For more information, see [Simple Network Management Protocol (SNMP)](#).

> Barracuda Networks recommend configuring SNMP traps if an SNMP monitoring tool is available in the network.

Configure System Time

By default, the Barracuda Web Application Firewall will synchronize time with the Barracuda Networks NTP server. It is recommended that administrators configure the Barracuda Web Application Firewall to use the organization's NTP server to ensure time synchronization across the organization's servers.

1. Go to the **ADVANCED > System Configuration** page.
2. Enter the NTP server IP address in the **NTP Server Settings** section.
3. Click **Add**.

It is possible to designate more than one NTP server. When multiple servers are defined, NTP uses the server whose time is most accurate based on various factors like the time variation and distance to the server.