Configuring Access to the Barracuda Web Application Firewall

The Barracuda Web Application Firewall is a critical component of an organizations security infrastructure and any access to the Barracuda Web Application Firewall should be strictly controlled.

Resetting the Factory Admin Password

The Barracuda Web Application Firewall is shipped with an "*Admin*" user account that has full administrative privileges and cannot be deleted from the system.

Barracuda strongly recommends that administrators change the default Admin password to a strong password.

The Barracuda Web Application Firewall does not enforce any rules on passwords, but general best practice guidelines recommend:

- Password lengths of more than 12 characters
- Use randomly generated passwords where feasible
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names,
- romantic links, or biographical information
- Include numbers, and symbols in passwords
- If the system recognizes case as significant, use capital and lower-case letters

Securing Network Access

Network access to the Barracuda Web Application Firewall should be controlled and limited. Recommended best practices include:

Use a Separate Management Network

Setting up a separate management network separates administrative traffic from WAN and LAN traffic. This physically ensures that only users with access to the management network can access the administrative interface on the Web Application Firewall. To set this up:

1. Use the Management (MGMT) port on the Barracuda Web Application Firewall to connect to the management domain.
2. Log into the Barracuda Web Application Firewall web interface
3. Go to the **BASIC > IP Configuration** page
4. In the **Management IP Configuration** section:
    1. Configure the IPv4/IPv6 address, IPv4 Subnet Mask/IPv6 CIDR Mask, IPv4/IPv6 Default Gateway and VLAN ID.
    2. Set **Allow Administration Access** to "*Yes*"..
5. Save the configuration.

Test to see if you can reach the console using the management network. Once you have confirmed you can reach the Web Application Firewall, log back into the Barracuda Web Application Firewall.

1. Go to the **BASIC > IP Configuration** page
2. Set **Allow Administration Access** to "*No*" in the **WAN IP Configuration** section.
3. Set **Allow Administration Access** to "*No*" in the **LAN IP Configuration** section.
4. Save the changes

Use HTTPS-Only for management access

1. Log into the Barracuda Web Application Firewall web interface using HTTPS.
2. Go to the **ADVANCED > Secure Administration** page.
3. Set **HTTPS/SSL Access Only** to *Yes*.

Controlling and Restricting Access

Defining and Assigning Roles

Access to the Barracuda management interface should be guided by the principle of least privilege. User roles ideally should be well-defined and should be limited to the minimal amount required to perform their job functionality.

The Barracuda Web Application Firewall is shipped with eight predefined roles representing the most common user roles used to administer the Web Application Firewall:

Role	Description
Admin	This is the super administrator role. The default 'admin' user is assigned this role. This role has the privilege to perform all system operations. An admin is responsible for creating and assigning roles.
Audit-Manager	User assigned to this role can perform auditing tasks. This role has the privilege to view logs, but is exempted from exporting logs. The role's responsibility is: • View logs • Generate reports
Certificate-Manager	User assigned to this role can perform certificate management tasks. The role's responsibility include: • Uploading certificates • Creating certificates • Uploading trusted certificates
Guest	User assigned to this role can view all configurations, but is exempted from modifying the configuration.
Monitoring-Manager	User assigned to this role can monitor system activities. The role's responsibility include: • View logs • Configuring email notifications • Exporting System logs, Application Logs and FTP access Logs • Generating and scheduling reports
Network-Manager	User assigned to this role can perform network related operations. The role's responsibility include: • Advanced IP configuration • Configuring SNAT and ACL's • Network troubleshooting
Policy-Manager	User assigned to this role can manage security policies on the Barracuda Web Application Firewall.
Service-Manager	User assigned to this role can manage services on the Barracuda Web Application Firewall.

In addition to the predefined roles, the Barracuda Web Application Firewall gives administrators fine grain access control capabilities to create custom roles that best represent what is needed for their teams. Administrators can create their own
custom role in the **ADVANCED > Admin Access Control** page. For more information, see How to Configure Role Based Administration.

Restrict IP Access

In addition to creating a management network and fine grained user roles for access control, it is recommended that administrators restrict IP access on the management network to a limited subnet. This ensures that only a small set of users utilizing designated devices can access the management console of the Barracuda Web Application Firewall. You can configure the IP addresses/networks in the **BASIC > Administration** page, **Allowed API IP/Range** section. The configured IP addresses will be allowed to change configuration information on the Barracuda Web Application Firewall through the Barracuda API..

Be careful when setting up the IP subnet of the management network. Incorrect configurations can lock out access to the Barracuda Web Application Firewall. If locked out, administrators will need to access the Barracuda Web Application Firewall via the serial console.