How to Secure Network Access

https://campus.barracuda.com/doc/2490387/

This article refers to the Barracuda Message Archiver firmware version 5.0 or higher.

To secure your Barracuda Message Archiver on your network, begin by locking down the user interface ports. Barracuda Networks recommends using the non-standard port 8000 for internal access to the web interface, which is configured on the **BASIC > Administration** page. From this page you can also further limit access to the web interface by IP address in the **Administrator/IP Range** section. If no IP address is specified in this field, then all systems are granted access with the correct administrator password.

Barracuda Networks strongly recommends securing external access to the Barracuda Message Archiver with the **Web Interface HTTPS/SSL Port** setting on the **Advanced > Secure Administration** page. Barracuda Networks recommends using port 443 because it is a standard HTTPS/SSL port used for secure web browser communication, and the identity of the remotely connected server can be verified with significant confidence.

SSL Certificates

As described above, Barracuda Networks strongly recommends limiting user interface access to HTTPS to provide the best security, and can be configured on the **ADVANCED > Secure Administration** page along with the use of SSL certificates. There are three types of SSL certificates to choose from:

- Default (Barracuda Networks);
- Private (self-signed);
- Trusted certificate - a certificate signed by a trusted certificate authority (CA).

Configuring SSL certificates is described in the section Enabling SSL for Administrators and Users.

Track Changes to the Configuration and User Login Activities

The syslog function of the Barracuda Message Archiver provides two kinds of logs, capturing:

- User login activities and any configuration changes made on the device;
- Data related to mail traffic. This data is the same information as that used to build the Message Log in the Barracuda Message Archiver.

From the **Advanced > Syslog** page, use the **Monitor Syslog** button to view the mail syslog output.

Integration with External Systems and Services - Security Considerations

Barracuda Message Archiver integrates with other systems and services in your environment, like your authentication server and email system. Barracuda Networks recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy. For more information, see Security for Integrating with Other Systems - Best Practices.