Getting Started

https://campus.barracuda.com/doc/4259901/

Recommended Steps

Barracuda Networks recommends the following steps for choosing the best deployment for your network, installing, and configuring the Barracuda Web Application Firewall.

For best security, deploy the Barracuda Web Application Firewall behind a firewall and limit access to the admin interface. For more information, refer to the "Controlling and Restricting Access" section in the Configuring Access to the Barracuda Web Application Firewall article.

Integration with External Systems and Services - Security Considerations

The Barracuda Web Application Firewall integrates with other systems and services in your environment, such as your authorization 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.

© 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.