
Restricting Direct Traffic

<https://campus.barracuda.com/doc/77401091/>

After you set up Barracuda WAF-as-a-Service for one or more of your applications, ensure that users cannot access your application server directly, without going through Barracuda WAF-as-a-Service.

Configure your application server to accept traffic only from the following Barracuda IP ranges.

- 64.113.48.0/20
- 34.228.125.58/32

Consult your application server documentation for specific instructions on this process. Here are links to some application server documentation sets.

- [Apache HTTP Server](#) documentation
- [Nginx Web Server](#) documentation
- [Unix and Linux](#) Iptables

© Barracuda Networks Inc., 2019 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.