Request Limits

https://campus.barracuda.com/doc/79462586/

Request limits define the validation criteria for incoming requests by enforcing size limits on request header fields, cookie names and values, and overall request length. Requests with properties larger than the specified maximum values are presumed to be buffer overflow attacks and are dropped.

Request Limits are enabled by default. You can change one or more of the default values, as needed. Settings include limits on URL length, cookie length, number of cookies, and number of headers.

Barracuda WAF-as-a-Service examines the request until it hits the default length specified in Request Limits. If only a small number of bytes must be parsed before denying requests, setting smaller limits can lead to a slight performance improvement. Alternatively, if the default values are resulting in too many drops, you can increase the default values.

© 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.