

Header Allow/Deny Rules

<https://campus.barracuda.com/doc/90441921/>

You can enforce strict limitations on incoming headers intended for a service . You can sanitize HTTP headers that carry sensitive information, including information that identifies the client and some application-specific state information, passed as one or more HTTP headers. You can configure a header ACL to prevent specific attack types, block metacharacters, and block specific Header Names.

You can specify whether, when an active rule is broken, the request is blocked or monitored (tracked in a log).

© 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.