Configuring Cloaking

https://campus.barracuda.com/doc/17106002/

Cloaking prevents leakage of information about a website or service that is vulnerable to web attacks. HTTP headers and return codes are concealed before sending a response to a client. The response headers are filtered based on the headers defined in the **Headers to Filter** field found under **Additional Options**.

When **Suppress Return Code** is set to **Yes**, the Barracuda Load Balancer ADC inserts a default or custom response page in case of any error responses from the server. Typically, the Barracuda Load Balancer ADC uses the default response page for error responses from the server. You can also define a custom response page by navigating to the **SECURITY > Libraries** page, scrolling to the **Response Pages** section, and clicking **Add Response Page**.

Cloaking features include:

- Removing banner headers, such as "Server" etc., from responses.
- Blocking client error (status code 4xx) and server error (status code 5xx) responses.

To configure cloaking, complete the following steps:

1. Navigate to **Security > Security Policies**.
2. Select a policy from the **Policy Name** list or create a **New Security Policy**.
3. Scroll to the **Cloaking** section and configure the cloaking settings as necessary. See the online help for additional information.

© 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.