Enabling HSTS for a Service

https://campus.barracuda.com/doc/48660754/

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement specified by a web application using the HTTP response header “Strict-Transport-Security”. This tells the browsers that they should only be communicating using secure HTTPS connections and not plain text HTTP. The HSTS policy protects the web applications from the man-in-the-middle attacks, such as protocol downgrade, SSL stripping, cookie hijacking, etc.

When a service with HSTS policy gets a request using HTTP, it automatically redirects the request to HTTPS the first time and injects the HSTS response header. An HSTS compliant browser will not allow subsequent requests to the same domain or sub-domains (see below) to be sent over HTTP; it will automatically convert these requests to HTTPS before they are sent.

HSTS disallows users to ignore SSL-related warnings and helps mitigate MITM attacks on SSL, such as SSL stripping. It also prevents users from using HTTP links inadvertently embedded in an HTTPS-only application.

HSTS is different from Instant-SSL where all hard coded HTTP links in the responses are re-written as HTTPS on-the-fly by the Barracuda Web Application Firewall.

Many browsers and web clients support the Preloading Directive for HSTS. This directive ensures that the clients connect to a predefined list of domain by using only the HTTPS protocol. The list of domains can be preloaded into your browser (or client). Refer to the respective browser help for more information.

Steps to Enable HSTS for a Service

To enable HSTS for a service:

1. Go to the **BASIC > Services** page.
2. Click **Edit** next to the service you want to enable HSTS policy.
3. Scroll down to the **SSL** section, click **Show Advanced Settings**, and do the following:
    1. **Enable HSTS** – Set to *Yes* to enable.
    2. **HSTS Max-Age** – Specify the maximum time in seconds that the HSTS policy should remain valid for the service.
    3. **Include HSTS Sub-Domains** – When set to *Yes*, the HSTS policy is enforced on all the sub-domains in the service.
    4. Modify the values for the other parameters (if required).

5. Click **Save**.

© 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.