Securing HTTP Cookies

https://campus.barracuda.com/doc/17105995/

Securing cookies is important because they can include sensitive information such as registration and login credentials. If a cookie can be viewed or changed, the system is vulnerable to attack and any sensitive information can be stolen.

On the Barracuda Load Balancer ADC, cookie security is transparent to back-end servers. You can configure the Barracuda Load Balancer ADC to either encrypt or sign cookies that are inserted by the server in a response, before it delivers the response to a client. When a subsequent request from the client returns this cookie, the Barracuda Load Balancer ADC intercepts the request and either decrypts the cookie or verifies the signature of the cookie. If the cookie is unaltered, the Barracuda Load Balancer forwards the original cookie to the server. Altered cookies are removed before the Barracuda Load Balancer ADC forwards the request to the server.

Cookie Signing

Encryption prevents both viewing and tampering with cookies, so it prevents the client from accessing cookie values. For clients who must access cookie values, you can enable signing. When the Barracuda Load Balancer ADC signs cookies, it forwards two cookies to the client browser–one plain text cookie and one signed cookie. If either of these cookies is altered when they are returned in a subsequent request from the client, signature verification fails and the the Barracuda Load Balancer ADC removes the cookies before forwarding the request to the server.

Interaction with HTTP Request Header Limits

When a cookie is encrypted, its length might change but the number of headers in the message remains unchanged. When a cookie is signed, its length can change and one or more headers are appended to the forwarded message.

Signed or encrypted cookies can exceed any limits that are enabled for the size or number of HTTP request headers (in the **SECURITY > Security Policies > Request Limits** section). If this occurs, messages can be incorrectly rejected. These rejected messages are logged on the **BASIC > Web Firewall Logs** page, with the **Action** of **CLOAK**.

Configure Cookie Security

To configure cookie security for a service:

1. Go to the **SECURITY > Security Policies** page.
2. In the left pane, click the name of the security policy that is assigned to the service.
3. In the **Cookie Security** section of the policy settings, review and edit each setting.
4. After you finish configuring the cookie security settings, click **Save Changes**.