Securing HTTP/HTTPS Traffic

https://campus.barracuda.com/doc/4259913/

The Barracuda Web Application Firewall protects your application from the attacks that are categorized by OWASP, as well as additional attacks such as application DDoS attacks, Slow Client attacks, Session hijacking attacks, XML / SOAP based attacks, etc. This is applicable to both HTTP and HTTPS application traffic. The Barracuda Web Application Firewall provides a variety of security policies to protect websites and web services. Security Policies define matching criteria for requests, and specify what actions to take when a request matches. All policies are global and they can be shared among multiple services configured on the Barracuda Web Application Firewall. For HTTPS applications, the Barracuda Web Application Firewall decrypts the SSL traffic before matching the HTTP requests with security policies.

When a Service requires customized settings, the provided security policies can be tuned, or customized policies can be created. Each policy is a collection of nine sub-policies. Modify a policy by editing the value of the parameter(s) on the sub-policy page.

In this Section:

Enabling the features listed below requires the response content from the server to be rewritten. Therefore, a request rewrite rule gets added to remove the **Accept-Encoding** header in the **HTTP Request Rewrite** section on the **Website Translations** page. This instructs the web server to send uncompressed responses. In the Barracuda Web Application Firewall 460 and above, the responses can be compressed using the compression feature. For more information on compression, see Configuring Caching and Compression.

The features to which rewrite rule is added when enabled are:

1. URL Encryption
2. CSRF Protection
3. Hidden Parameter Protection
4. Data Theft Protection
5. Web Scraping
6. DDoS Prevention
7. Instant SSL
8. Response Body Rewrite
9. Learning (Website Profiles)
10. CSRF under Parameter Protection
11. URL Protection (only if CSRF is enabled)