Security Policies

https://campus.barracuda.com/doc/4259878/

Overview

The Barracuda Web Application Firewall associates security policies with HTTP and HTTPS Services. A security policy has preset configured security settings which apply to any associated Service. Security policies are shareable, so once a policy is created, it can be assigned to more than one Service. The security policy rules specify inspection criteria for input or output data, identifying malicious or vulnerable data. Security policies include mostly negative and some positive elements. For most web sites, security policies sufficiently implement good web application security.

Any existing security policy can be refined manually, and new security policies can be created. Security Policies can also be refined using automated tools (see Tuning Security Rules for instructions).

Security policies include general URL and Parameter protection which is applied to all service requests. When required, more customized URL and Parameter protection can be implemented using Web Site Profiles, URL profiles, and parameter profiles.

When is a security policy associated with the Service?

When a Service is created, it is associated with the default security policy and log levels. For more information on how to configure a Service see Configuring a Service, and Configuring Basic Service Settings. The Barracuda Web Application Firewall includes the following pre-configured security policies:

- default
- sharepoint
- sharepoint2013
- owa
- owa2010
- owa2013
- oracle

When needed, the security policy associated with the Service can be changed or refined. Security policies define matching criteria to compare to requests, and rules for matching requests. All security policies are global, that is, they can be shared by multiple Services configured on the Barracuda Web Application Firewall.

When a Service needs refined security settings, the provided security policies can be adjusted, or customized policies can be created. To create a customized security policy, see Steps to Create a New

Policy. Each policy is a collection of nine sub-policies. Modify the following sub-policies by editing the corresponding sub-policy page. The sub-policies include:

- Request Limits
- Cookie Security
- URL Protection
- Parameter Protection
- Cloaking
- Data Theft Protection
- URL Normalization
- Global ACLs
- Action Policy

Steps To Create a New Policy

1. Go to the **SECURITY POLICIES > Policy Manager** page.
2. In the **Create New Policy** section, enter a name in the **Policy Name** text box and click **Add**.
3. The new policy appears in the **Policy Overview** section with the default values.

Related Articles