

Security Policies

<https://campus.barracuda.com/doc/17105990/>

Application security functionality is available in models 540 and higher. See the [Barracuda Load Balancer ADC](#) data sheet for model comparison.

The Barracuda Load Balancer ADC associates security policies with HTTP, HTTPS, and Instant SSL services. A security policy has preset configured security settings which apply to any associated virtual service. Security policies are shareable, so after a policy is created, it can be assigned to more than one virtual 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 websites, security policies sufficiently implement good web application security.

Default and Preconfigured Security Policies

When a virtual service is created, it is associated with the default security policy and log levels. The Barracuda Load Balancer ADC includes the following preconfigured security policies:

- Default
- Oracle
- OWA
- OWA2010
- OWA2013
- Sharepoint
- Sharepoint2013

Security Policy Configuration

When needed, the security policy associated with the virtual 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 Load Balancer ADC.

When a virtual 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

Create a Policy

To create a policy:

1. Go to the **SECURITY > Security Policies** page.
2. Click **New Security Policy**.
3. In the **New Security Policy** window, enter a name for the policy and click **Create**. The policy is created with default settings, that you can edit in the main pane of the page.

Edit a Policy

To edit a configured policy:

1. Go to the **SECURITY > Security Policies** page.
2. In the left pane, click the policy name.
3. In the main pane of the page, edit the policy settings.
4. After you finish editing the policy, click **Save Changes**.

© Barracuda Networks Inc., 2019 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.