
Smart Signatures

<https://campus.barracuda.com/doc/90445705/>

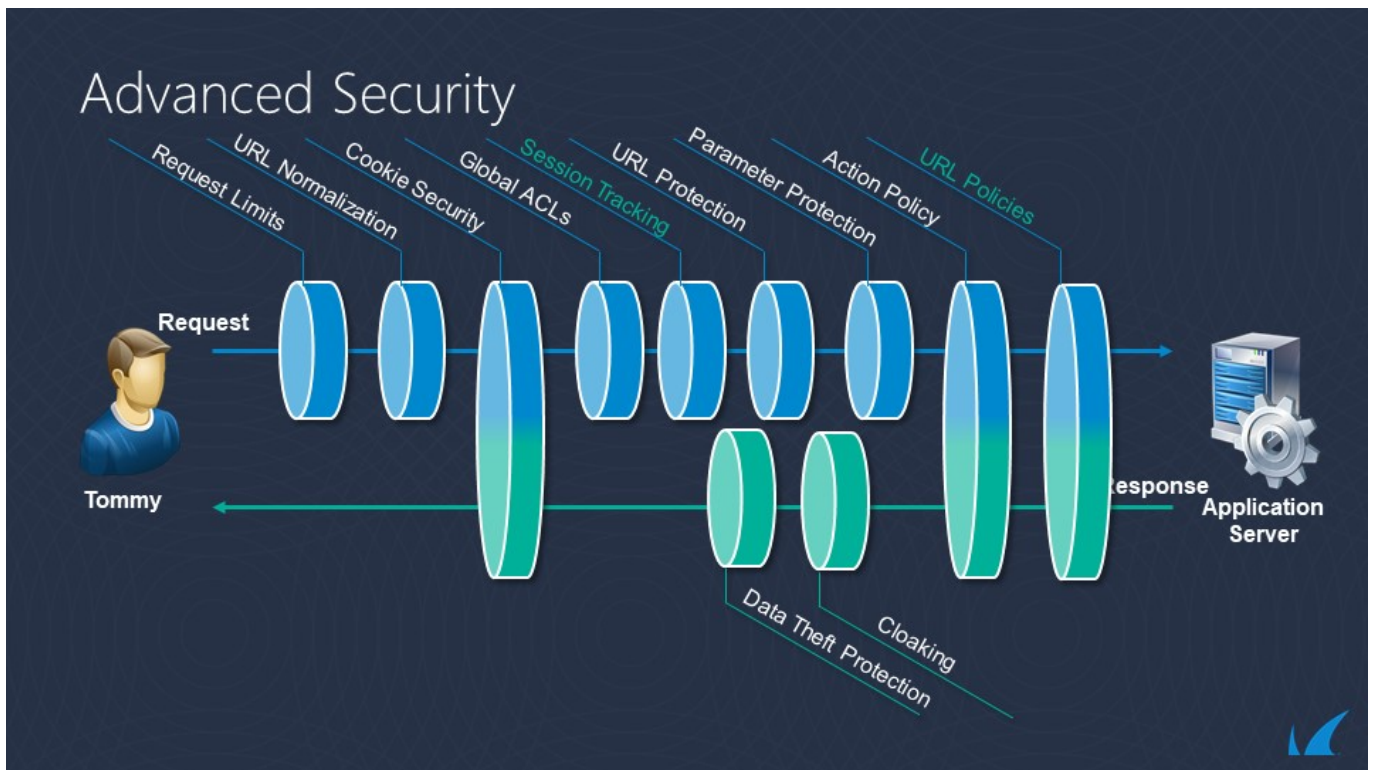
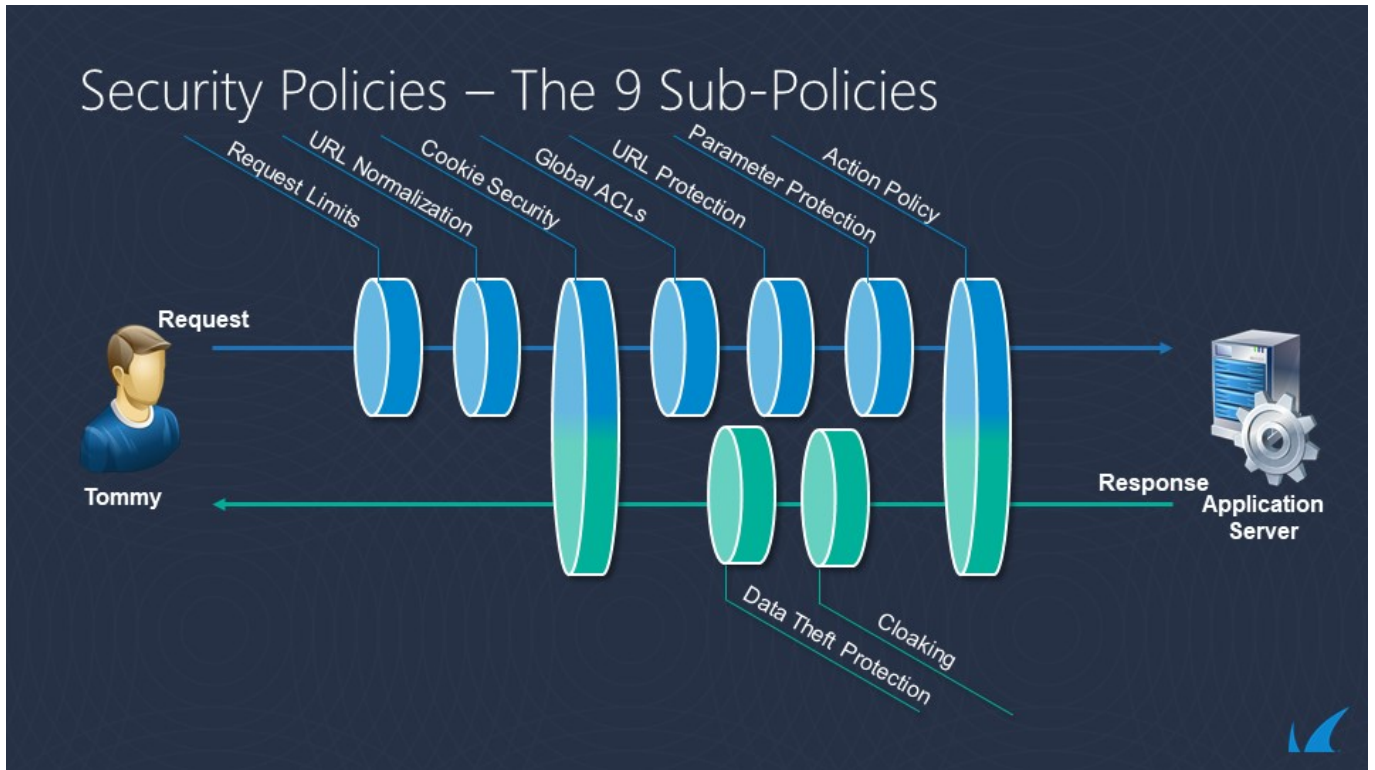
Smart Signatures

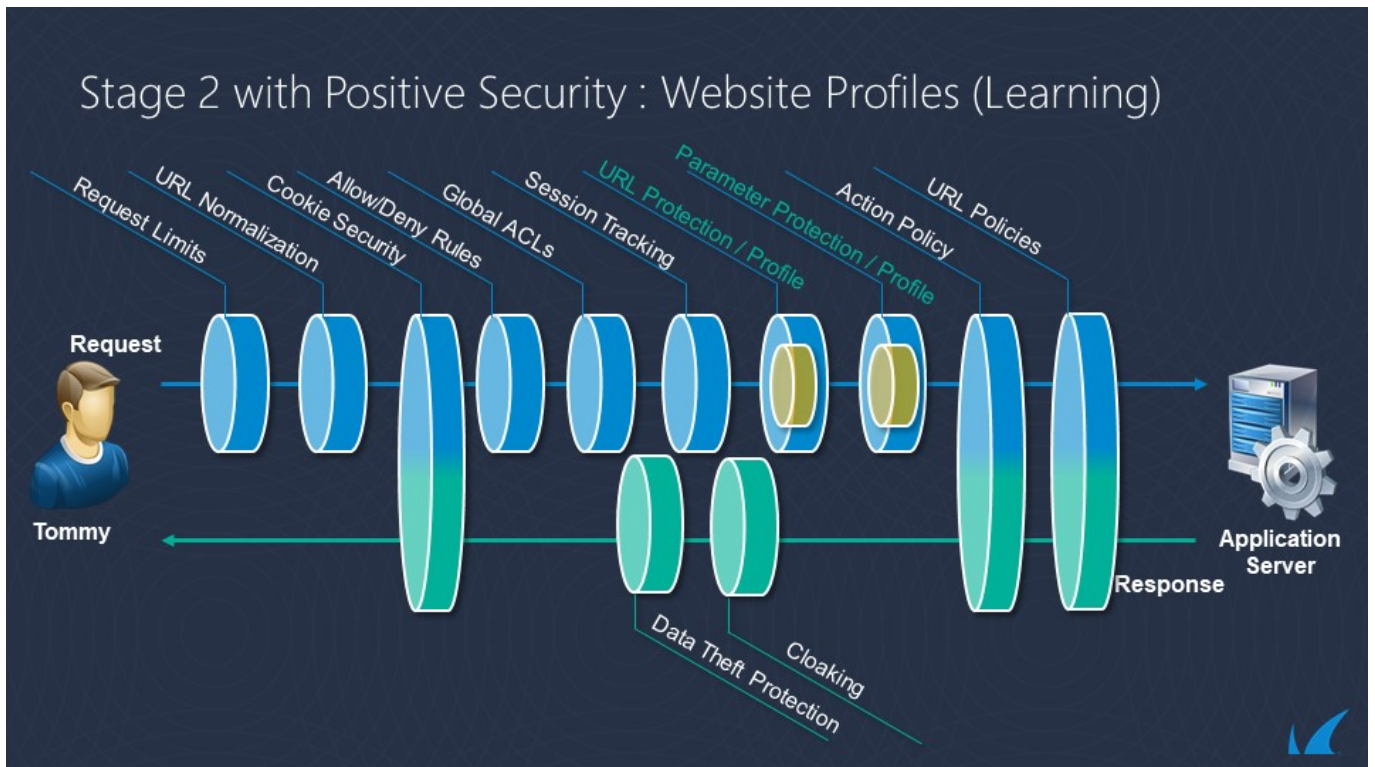
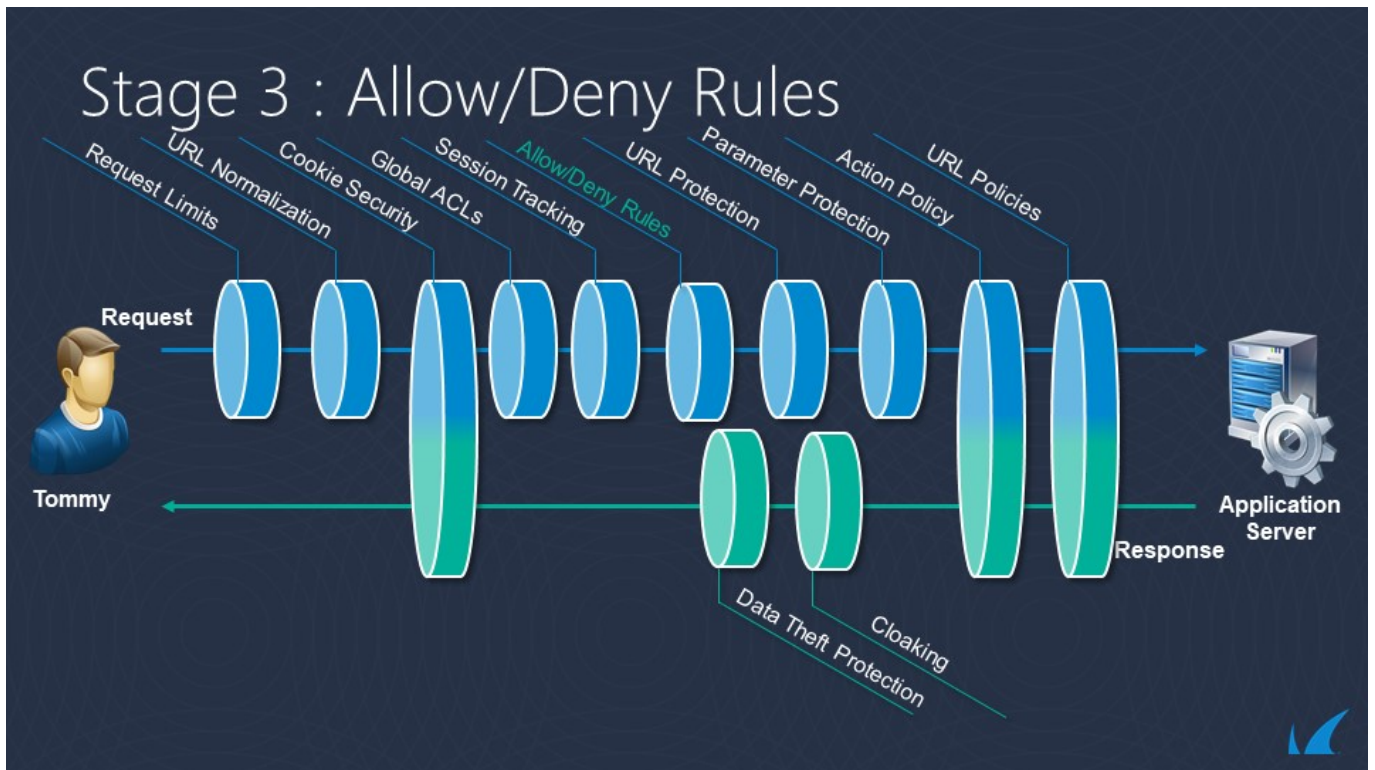
The Barracuda Web Application Firewall layered processing engine passes traffic through multiple layers of security before validating signatures. The data is first normalized before matching the signature, mainly to reduce the number of patterns required by the system, and to make it more efficient. The normalization engine takes care of case sensitivity and various encoding types before submitting any data to the actual signature match engine.

The Barracuda Web Application Firewall uses Smart Signatures developed internally beyond the processing engine. Signatures are batched in signature groups to allow significant memory optimization and speed of detection when compared to static signatures per attack. Each signature in a signature group has the ability to detect attacks found in 40 standard signatures. This is in contrast with the typical signature-based security available with other web application firewalls where, each signature is specific to a vulnerability or attack, and matching them takes significant time.

When new vulnerabilities are identified, Barracuda security analysts validate the vulnerabilities against the existing signature base. Most of the new vulnerabilities are detected by the signature groups. In many cases, the only change required is turning on the stricter attack type (example: SQL Injection versus SQL Injection strict). When an attack is getting through, relevant signatures are created immediately and are made available to the Barracuda Web Application Firewall through attack definition updates. This is performed on an as-needed basis.

The following diagrams show the evaluation flow for Requests and Responses. Smart Signatures are applied at the relevant parts of the evaluation flow depending on the content of the request.





Figures

1. 01 -Stage 1 - Security Policies.jpg
2. 02 - Stage 2 Advanced Security.jpg
3. 03 - Stage 3 Allow Deny Rules.jpg
4. 04 - Stage 2 with Positive Security.jpg

© Barracuda Networks Inc., 2020 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.