epati

Web Server Security

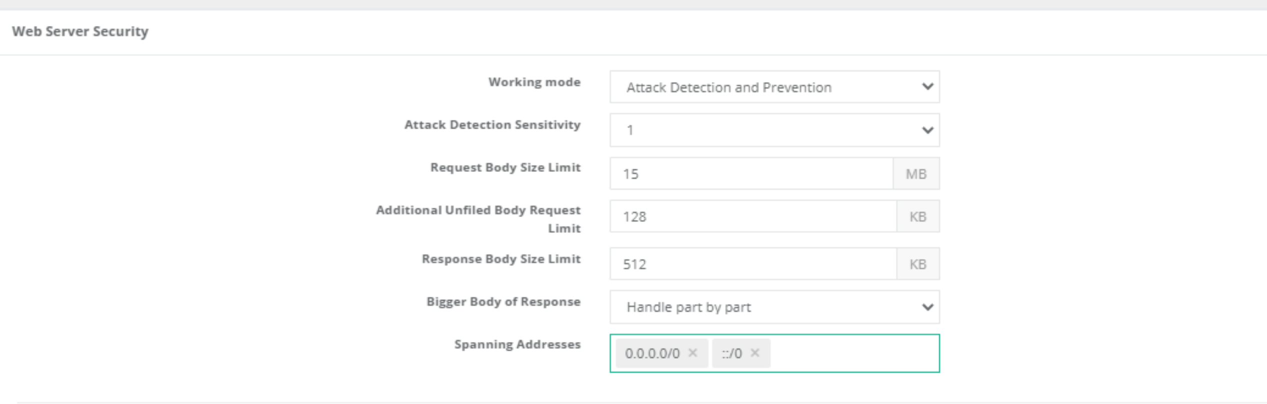
Product: Antikor v2 - Next Generation Firewall

Guides

www.epati.com.tr

Web Server Security

Antikor provides web server security as a gateway in NGFW.

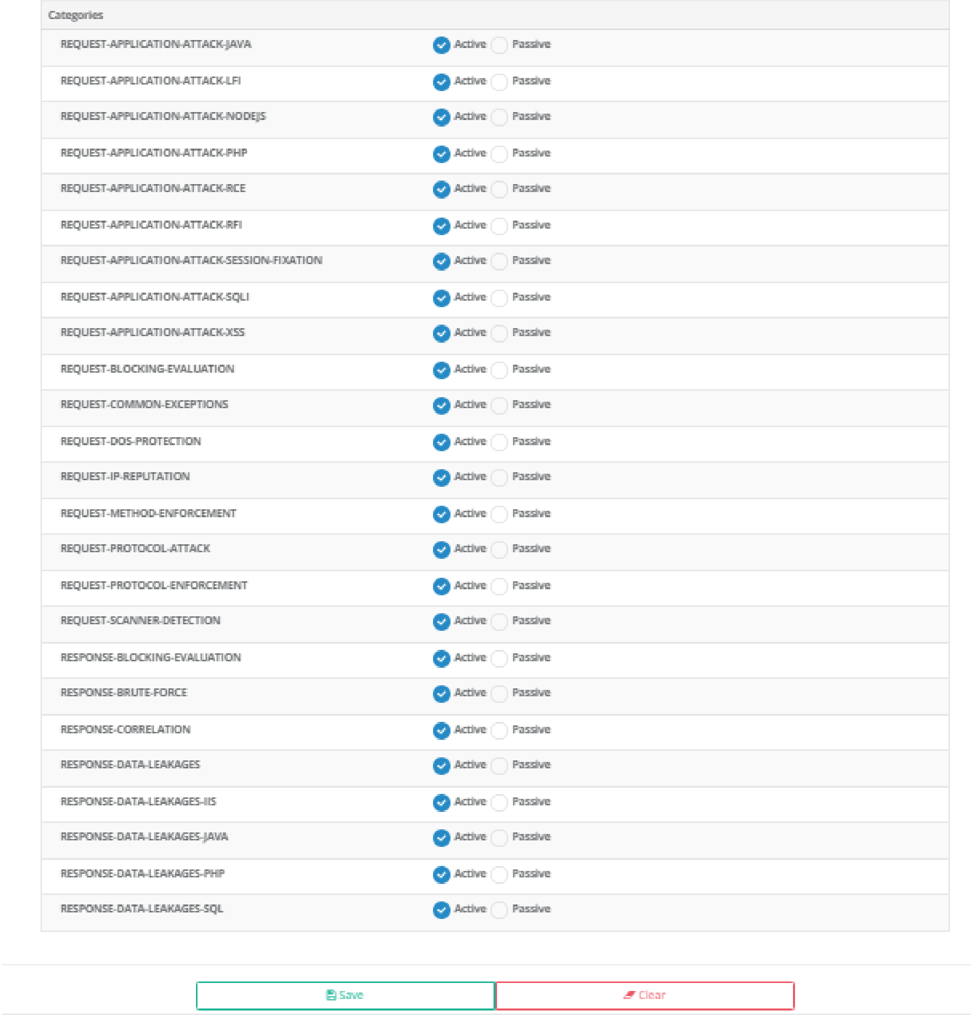


Web Server Security

Working mode	Attack Detection and Prevention
Attack Detection Sensitivity	1
Request Body Size Limit	15 MB
Additional Unfiled Body Request Limit	128 KB
Response Body Size Limit	512 KB
Bigger Body of Response	Handle part by part
Spanning Addresses	0.0.0.0/0 × ::/0 ×

Area	Explanation
Working mode	Active categories must be selected to run in **Intrusion Detection** or **Intrusion Detection and Prevention** mode. In Intrusion Detection and Prevention mode, attacks to web servers are logged and blocked. Only attacks made in intrusion detection mode are logged.
Intrusion Detection Sensitivity	A number between 1 and 4 must be selected. While the number is 4, the attacks are detected in the most sensitive mode, while the sensitivity decreases as the number decreases. It comes by default as 1.
Request Body Size Limit	The package request body size limit is set in MB. The default is 15 MB.
No Attachment File Request Body Limit	The request body limit for packages that do not have an attached file can be determined. The default is 128 KB.
Response Body Size Limit	The Response Body Size Limit is set. The default is 512 KB.
Larger Response Body	If the response body has a response body larger than the size limit, how to take action is selected. The package is processed piecemeal or rejected.
Addresses Covered	IP address scopes to be applied Web Server Security are written.

There are signatures of the following attacks related to Web Server Security. The signature of the attack to be blocked must be active.



Categories	
REQUEST-APPLICATION-ATTACK-JAVA	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-LFI	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-NODEJS	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-PHP	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-RCE	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-RFI	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-SESSION-FIXATION	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-SQLI	● Active ○ Passive
REQUEST-APPLICATION-ATTACK-XSS	● Active ○ Passive
REQUEST-BLOCKING-EVALUATION	● Active ○ Passive
REQUEST-COMMON-EXCEPTIONS	● Active ○ Passive
REQUEST-DOS-PROTECTION	● Active ○ Passive
REQUEST-IP-REPUTATION	● Active ○ Passive
REQUEST-METHOD-ENFORCEMENT	● Active ○ Passive
REQUEST-PROTOCOL-ATTACK	● Active ○ Passive
REQUEST-PROTOCOL-ENFORCEMENT	● Active ○ Passive
REQUEST-SCANNER-DETECTION	● Active ○ Passive
RESPONSE-BLOCKING-EVALUATION	● Active ○ Passive
RESPONSE-BRUTE-FORCE	● Active ○ Passive
RESPONSE-CORRELATION	● Active ○ Passive
RESPONSE-DATA-LEAKAGES	● Active ○ Passive
RESPONSE-DATA-LEAKAGES-IIS	● Active ○ Passive
RESPONSE-DATA-LEAKAGES-JAVA	● Active ○ Passive
RESPONSE-DATA-LEAKAGES-PHP	● Active ○ Passive
RESPONSE-DATA-LEAKAGES-SQL	● Active ○ Passive