Advanced Bot Protection

https://campus.barracuda.com/doc/86541236/

Overview

The Barracuda Web Application Firewall **Advanced Bot Protection** (ABP) capabilities protect your web, mobile, and API-based applications against a variety of bot attacks. ABP uses a combination of on-box capabilities and cloud-based machine learning/artificial intelligence systems to detect advanced bots. This feature provides you with comprehensive insights into bot traffic over your web applications.

ABP provides multiple features that can be used to detect and block specific bot attacks. Some of these features are available on-box without the purchase of an additional license. Other features require the purchase of an Advanced Bot Protection license. The feature-license matrix below shows which features require an additional license:

Feature	ABP License Required	Data is sent to Advanced Bot Protection for analysis
Risk Score	Yes	Yes - Traffic Metadata
Credential Stuffing	Yes	Yes - Hashed Data
Credential Spraying	Yes	Yes - Hashed Data
Auto-Configuration Engine (ACE)	Yes	Yes - Traffic Metric Logs
Advanced Threat-Intelligence Dashboard • Advanced BOT Protection • Client-Side Protection	Yes	Yes - Traffic Metadata
Bot Spam Mitigation Form / Referrer / Comment Spam	No	No
Session Tracking	No	No
Web Scraping	No	No
Client-Side Protection • Content Security Policy • Sub-Resource Integrity	No	ONLY if report-to is configured to send the data to BATIC. You can configure to send the data to other collection end-point.
Google reCAPTCHA (customer should have a Google account with relevant features)	No	It's redirection for authentication
Bot Widget and Reporting (except Credential Stuffing)	No	Yes-Traffic Metadata
Bot Block-list and New IP Reputation categories	No	No

Barracuda ABP Cloud Integration	Yes	
Tarpit	No	No

Feature Categorization

Security Aspect	Feature Name	OWASP Automated Threat (OAT) Identity Number
Bot Mitigation	• Client Fingerprinting • Client Profiling • Risk Scoring • Web Scraping Policy	OAT-004 OAT-018 OAT-014 OAT-011

Securing Accounts / ATO	• Credential Attack Protection
	  ◦ Credential Stuffing
	  ◦ Credential Spraying
	• Brute Force Protection
		OAT-008
		OAT-007
		OAT-019

Bot Spam Protection	• Referrer Spam • Comment Spam • Form Spam	
Application DDoS	• DDoS Policy • Slow Client Attack Prevention • Session Tracking	OAT-015
File Upload Protection	• Anti-virus check • BATP Scan	
Data Theft Protection	Data Theft Protection	
Client-Side Protection	• Content-Security Policy • Sub Resource Integrity	
Configuration Recommendation	Auto-Configuration Engine	

How to Enable Bot Mitigation

To configure ABP features, navigate to the **BOT MITIGATION** tab in the web interface and select the **Bot Mitigation** page. Here you can configure service level configurations to detect and block bot attacks, including credential stuffing, brute force attacks, web scraping, and more.

The Advanced Security and Session Tracking modules from the **WEBSITES > Advanced Security** page have been moved to the **BOT MITIGATION > Bot Mitigation** page. In addition, the **Web Scraping Policies** section from the **WEBSITES > Advanced Security** page has been moved to the **BOT MITIGATION > Bot Mitigation** page.

For an overview of the Advanced Bot Protection feature and to learn about the feature-license matrix, see Advanced Bot Protection Dashboard.