Overview of WAF-as-a-Service Plans

https://campus.barracuda.com/doc/99615198/

Barracuda -WAF-as-a-Service is available in two (2) plans: The table below lists the features that are available in each plan:

Feature	Application Protection Advanced	Application Protection Premium	Description
Web Application Protection			
OWASP Top 10 Protection	✓	✓	Protect against all OWASP Top 10 attacks including SQL Injections, XSS, Cross-Site Request Forgery, and more.
Smart Signatures	✓	✓	Application Protection's layered traffic processing engine and Smart Signatures use fewer attack-detection signatures to detect and block web attacks, including zero-day attacks. Each Smart Signature can detect attacks found in 40 attack-specific signatures, reducing detection time and improving overall detection.
Zero Day Attack Protection	✓	✓	The combination of Smart Signatures and a positive security model ensure that most zero-day attacks are stopped before exploitation. In addition, Barracuda Active Threat Intelligence collects threat data from a large, worldwide network of sensors and customer traffic. This data is processed using machine learning in near real-time and pushed out to connected units immediately, allowing for rapid detection of new threats and attackers.
IP Threat Intelligence	✓	✓	Barracuda Application Protection integrates with the Barracuda Reputational Database and can identify suspicious IP addresses, bots, TOR networks and other anonymous proxies that are often used by attackers to hide their identity and location. Capabilities include the ability to block proxies, VPNs, and entire networks based on the Autonomous System Numbers (ASN).
Geo-IP Intelligence	✓	✓	Using client source addresses, organizations can control access to web resources. Barracuda Application Protection can control access based on GeoIP to limit access only to specified regions.

Data Leak Prevention	✓	✓	Inspects all outbound traffic for sensitive data leakage. Content such as credit card numbers, U.S. social security numbers, or any other custom patterns are identified and can be either blocked or masked without administrator intervention. Also, the information is logged and can be used by administrators to find potential leaks.
Website Supply Chain Protection	✓	✓	Barracuda Application Protection includes Client-Side Protection, a feature that automates the CSP and SRI configuration, reducing admin overhead and configuration errors. In addition to these capabilities, Barracuda Active Threat Intelligence provides visualization and reporting for these configurations, giving you deeper visibility into how these scripts are used.
Anti-Virus for File Uploads	✓	✓	On-board regularly updated antivirus engine scans and detects viruses in file uploads.
Risk-based Attack Detection		✓	Barracuda Active Threat Intelligence automatically classifies each incoming request with risk scores based on the request parameters. These risk scores are used by the backend ML models to identify advanced threats such as bots and complex attackers and block them.
DDoS Protection			
Unlimited Volumetric DDoS Attack Prevention	✓	✓	Barracuda WAF-as-a-Service offers unmetered DDoS protection cloud service that scrubs traffic before it reaches the intended websites. This allows the cloud service to identify patterns of DDOS attacks in the connections and block them.
Unlimited Application DDoS Attack Prevention	✓	✓	Protect against advanced application-layer DDoS with risk-assessment techniques, heuristic fingerprinting and IP reputation to distinguish real users from botnets.
Rate Limiting	✓	✓	Barracuda Application Protection offers rate limiting of incoming client requests based on IP and client fingerprint. Rate limiting is especially useful at peak times where some users may attempt to overload the application by sending rapid requests. Rate limiting can be enforced at an application or URL level using an unlimited number of rules.
DNS Security		✓	Hosting and security for application DNS records, including protection against DDoS attacks.
API Security			

Protect JSON and GraphQL APIs	✓	✓	Barracuda Application Protection protects JSON, and GraphQL APIs against all application attacks, including OWASP Top 10 API threats.
Schema-based API Discovery	✓	✓	Import the schema for your JSON API to automatically create security rules based on the definition of the API. Supported schemas are OpenAPI and Google API formats.
ML-powered JSON API Discovery		✓	Barracuda Application Protection uses machine learning to detect unprotected API endpoints from live traffic analysis and automatically secures them, reducing the attack surface drastically.
ML-powered Shadow API Discovery		✓	Shadow APIs are the APIs deployed by web applications that are not known and secured. Barracuda Application Protection uses machine learning to detect these API endpoints from live traffic analysis and automatically secures them, reducing the attack surface drastically.
Unlimited API Rate Limiting Rules (Tarpit)		✓	Barracuda Application Protection offers rate limiting capabilities for APIs that can be enforced on an endpoint level, reducing the ability of misbehaving clients to slow down or bring down an API.
Advanced Bot Protection			
Web Scraping	✓	✓	Barracuda Application Protection uses a combination of honeypots, behavioral analysis, and signatures to detect and block web scraping.
Bot Spam Detection	✓	✓	Barracuda Application Protection uses a combination of honeypots, behavioral analysis, and spam signatures to detect and block these bot attacks.
Bot Signature Database	✓	✓	Barracuda Application Protection contains a regularly updated bot signature database that contains over 10,000 individual signatures. These signatures can be used to identify and block bots before they reach your application.
CAPTCHA Insertion and Challenges	✓	✓	Barracuda Application Protection has multiple methods of challenging bots and attackers to both slow and stop them down. These methods include JavaScript challenges and CAPTCHAs.
Brute Force Prevention	✓	✓	Barracuda Application Protection can identify brute force attacks – whether they are coming from a single IP/source or multiple IPs/sources in low and slow attacks – and block them, rendering the application safe.

Credential Stuffing Protection	✓	✓	Barracuda Active Threat Intelligence has a database of previously leaked credentials that logins are validated against. If matches are found, these login attempts can be blocked, and admins alerted.
Cloud-backed Active Threat Intelligence		✓	Barracuda Active Threat Intelligence collects threat data from a large, worldwide network of sensors and customer traffic. This data is processed using machine learning in near-real time and pushed out to connected units immediately, allowing for rapid detection of new threats and attackers.
Privileged Account Protection		✓	Privileged Account Protection on the Barracuda Active Threat Intelligence cloud uses behavioral analytics to understand user login and browsing patterns. When the behavior of the user varies from the pattern, admins are alerted to identify and block account takeover attacks.
ML-powered Bot Detection		✓	Barracuda Advanced Bot Protection uses cloud-based machine learning to stop bad bots, easily blocking automated spam, web and price scraping, inventory hoarding, account takeover attacks, and much more.
Client Identification and Control		✓	Barracuda Application Protection can identify individual devices behind an IP address and most modules can enforce blocking at a device level or IP level as desired.
Secure Application Delivery			
Content Delivery Network	✓	✓	Barracuda Application Protection provides an integrated CDN for onboarded applications. The CDN has over 118 PoPs that can serve traffic to the nearest clients across 100 locations worldwide.
Authentication, Authorization, and Access Control	✓	✓	Barracuda Application Protection provides granular AAA capabilities to offload authentication and authorization for applications. Capabilities include Client Certificates, JSON Web Tokens, SAML, and OpenID Connect.
Shared IP	✓	✓	Applications protected by the Application Protection Advanced plan are provided a shared IP public IP address.

Content Routing	✓	✓	Content Routing on Barracuda Application Protection uses a number of parameters on the incoming request to identify and redirect traffic to various parts of an application. This could be anything from redirecting a user to the mobile application based on the HTTP UserAgent or routing traffic for A/B testing or enabling blue-green deployments. Each content route requires an additional App license.
Zero Trust Network Access		✓	Barracuda CloudGen Access is an innovative ZTNA solution that provides secure access to applications and workloads from any device and location. Barracuda Application Protection includes Barracuda CloudGen Access licenses to provide a secure access control surface for your internal applications that are published on the internet.
Load Balancing with Server Health Monitoring	✓ (Upto three (3) servers)	✓	Applications onboarded on Barracuda Application Protection can be configured with multiple servers to spread the load and improve uptime. Barracuda Application Protection also includes Server Health Monitoring capabilities that continuously monitor application servers to switch traffic over in case of failure, improving uptime. When moving from **Premium** to **Advanced**, ensure that you retain three (3) working servers and delete all other servers. If not, the Barracuda WAF-as-a-Service keeps the top three entries and deletes all other servers associated with the application.
Containerized Deployment		✓	Barracuda Application Protection provides an additional deployment module, the Containerized WAF that can work in conjunction with the SaaS model to secure East-West traffic in microservices.
Per-App IP		✓	Applications protected by the Application Protection Premium plan are provided with individual public IP addresses.
Reporting, Analytics, and Services			
Log Export to SIEM	One export server	Multiple export servers	Barracuda Application Protection allows all application logs (traffic and firewall) to be exported to external SIEM solutions for further retention and analysis.
Auto Configuration Engine	✓	✓	Auto Configuration Engine is a service that reviews all your application traffic from connected units and provides application-specific configuration recommendations, reducing admin overhead.

Virtual Patching and Scanner Integration	✓	✓	Barracuda Application Protection leverages our advanced vulnerability scanner to constantly monitor your entire deployment for vulnerabilities. When it finds vulnerabilities – even in apps that are still in development – it can remediate them automatically or with a single click.
Log Storage Duration	30 days	60 days	Duration of firewall and traffic log storage on the Application Protection platform.
Configuration API Access	✓	✓	Barracuda Application Protection is built API-First. What this means in practice is that every capability on the product can be configured and tuned using the Configuration API. Available to all users, code samples and modules for popular automation tools are also provided on our GitHub page for easy integration with your automation toolchain.
Configuration Snapshots	✓	✓	All configuration changes on Barracuda Application Protection are stored as snapshots. These snapshots are created in JSON and are editable – and use our configuration API in the backend. This capability allows easy integration with DevOps/SecOps tools and enables easily repeatable deployments to enforce uniform security policies.
Advanced Reporting and Visualization		✓	Barracuda Active Threat Intelligence Dashboard gives you at-a-glance visibility into traffic patterns and the types of clients who visit your website.

Related Articles:

- Licensing and Licensing Violations

Figures

45. checkmarkIcon.png
46. checkmarkIcon.png
47. checkmarkIcon.png
48. checkmarkIcon.png
49. checkmarkIcon.png
50. checkmarkIcon.png
51. checkmarkIcon.png
52. checkmarkIcon.png
53. checkmarkIcon.png
54. checkmarkIcon.png
55. checkmarkIcon.png
56. checkmarkIcon.png
57. checkmarkIcon.png
58. checkmarkIcon.png
59. checkmarkIcon.png
60. checkmarkIcon.png
61. checkmarkIcon.png
62. checkmarkIcon.png
63. checkmarkIcon.png
64. checkmarkIcon.png
65. checkmarkIcon.png
66. checkmarkIcon.png
67. checkmarkIcon.png
68. checkmarkIcon.png
69. checkmarkIcon.png