







# DDoS Protection vs. WAF vs. Bot Management

DDoS protection, WAF (Web Application Firewall), and bot management protect websites, applications, and APIs from malicious web traffic. But how exactly do they differ, and which solution protects against which threats? Our brief comparison provides answers and helps you find the right solution for your needs.

Feature / Function	 <b>DDoS Protection</b>	 <b>WAF (Web Application Firewall)</b>	 <b>Bot Management</b>
<b>Main objective</b>	Protection against server overload from malicious traffic	Monitoring, filtering, and blocking of malicious HTTP/S traffic	Detection and blocking of automated access by bots
<b>Primary protection goal</b>	Availability	Integrity and confidentiality	Integrity and confidentiality
<b>Protects against</b>	DDoS attacks <ul style="list-style-type: none"> <li>• Volumetric attacks with high bandwidths or packet rates at the network and transport layer</li> <li>• Attacks with malicious requests at the application layer</li> <li>• Traffic spikes caused by botnets</li> </ul>	OWASP Top 10 risks <ul style="list-style-type: none"> <li>• SQL Injection</li> <li>• XSS</li> <li>• CSRF</li> <li>• etc.</li> </ul>	Automated attacks <ul style="list-style-type: none"> <li>• Scraping</li> <li>• Credential Stuffing</li> <li>• Account Creation &amp; Takeover</li> <li>• Skewing</li> <li>• etc.</li> </ul>
<b>Prevents</b>	Outages and malfunctions due to overload	Data theft, manipulation, espionage, unauthorized access	Data theft, manipulation, espionage, unauthorized access
<b>Layer in the OSI model</b>	Network layer (L3) + transport layer (L4) + application layer (L7)	Application layer (L7)	Application layer (L7)

Feature / Function	 <b>DDoS Protection</b>	 <b>WAF (Web Application Firewall)</b>	 <b>Bot Management</b>
<b>Distinguishes humans vs. bots</b>	✗ No	✗ Not primarily	✓ Yes
<b>Using behavioral analysis?</b>	✗ Rarely	○ Partially (e.g., through rules)	✓ Yes
<b>Rate limiting possible?</b>	✓ Yes (e.g., requests per second)	✓ Yes (via IP or URI)	✓ Yes, including dynamic rules
<b>CAPTCHA / challenge functionality</b>	✗ No	○ Partially	✓ Yes (e.g., JavaScript challenges, CAPTCHA)
<b>Allow good bots?</b>	✗ No focus	✗ No focus	✓ Yes (e.g., search engine bots)
<b>Recommended for</b>	IT infrastructure, websites, web applications, APIs	Web applications, APIs	Websites with user accounts, web forms, exclusive content, APIs

## Conclusion: Who Needs Which Solution?

- **DDoS protection** ensures the availability of your website by **preventing overloads** caused by high bandwidths or packet rates – essential for all online services.
- A WAF protects the integrity of your web application by **blocking known attacks via the HTTP/S protocol** – particularly important for interactive and business-critical applications such as online banking and e-commerce.
- **Bot management** distinguishes between humans and machines, **detects unwanted and fraudulent bots**, and protects your business logic – important for login pages, online forms, and APIs, e.g., for e-commerce, ticket providers, media sites, etc.

## Myra Protects What Matters. In the Digital World.

Want to learn more about how our certified solutions protect your applications from a wide range of risks, including DDoS attacks, bot networks, and database attacks? Our experts will be happy to help you develop a customized solution for your organization. Schedule a no-obligation consultation today!