Advanced WAF and Bot Protection

In today's economy, your digital business must be secure and available ... all the time. But your network and applications are under constant attack, making it difficult to ensure that data is secure and online revenues are protected.

Cisco® Secure Web Application Firewall (WAF) and bot protection defends your online presence and ensures that website, mobile applications, and APIs are secure, protected, and "always on."

Bots Target All Channels

Websites

Mobile apps

APIs

Protect your business from data theft, L7 DDoS attacks, denial of inventory, web scraping

80%

of organizations can't distinguish good bots from malicious bots

Advanced WAF and bot management solutions ensure reliable, secure delivery of web and mobile applications while minimizing costs by enabling security policies to easily be deployed across multicloud environments. Advanced bot management uses machine learning and adaptive security to accurately distinguish good bots from malicious bots, ensuring that your network and applications are available to legitimate users.

With business moving online and to the cloud, advanced WAF and bot solutions protect websites, applications, and APIs from attack and ensures that your organization is open for business.

Key benefits

Consistent security policy

- Easily deploy across multicloud to reduce costs and security risks

Comprehensive OWASP coverage

- Protection beyond the OWASP Top 10
- Positive and negative models provide complete protection with minimum false positives
- Advanced security controls inspect and protect APIs from attack and manipulation

Advanced bot protection

- Accurately identifies advanced human-like bots that evade fingerprinting technologies
- Distinguishes good bots from malicious bots with minimum false positives

Auto discovery

- Continuously scans apps for changes and automatically optimizes security policies

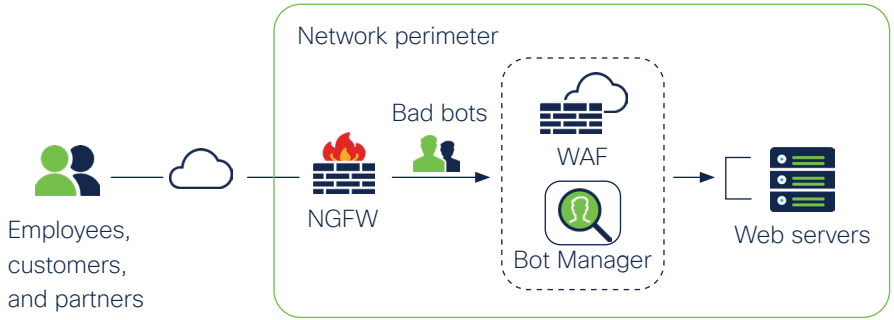
Cisco Advanced WAF and Bot Protection

Cisco WAF protects web servers from cyber attacks...

... and ensures that applications are available

Machine learning enables...

... continuous application protection



Advanced WAF and bot solutions combine positive and negative models with advanced behavioral analytics to accurately identify bad bots and protect your online business.

Cisco application protection solutions deliver:

- Accurate identification and management of bots
- API security
- Protection from denial of service (DoS) attacks
- Continuous monitoring of apps with automatic security updates

Highly effective application security

Negative Security Models

- Used in most WAF solutions
- Block known threats via signatures and rules
- Cannot protect from unknown threats: zero-day attacks

Positive Security Models

- Learn and define what constitutes legitimate traffic
- Block unauthorized access and actions
- Uniquely protect against zero-day and unknown vulnerabilities

Advanced WAF + Bot Manager = Better Together

Security Capability	Bot Manager	Traditional WAFS	WAF + Bot
Protection from simple bots	Yes	Yes	Yes
Fingerprinting of malicious devices	Yes	Yes	Yes
Mitigation of dynamic IP and headless browser attacks	Yes	Limited	Yes
Detection of sophisticated bot attacks	Yes	No	Yes
Risk of blocking legitimate users (false positives)	Very low	High	Very Low
Collective bot intelligence (IPs, fingerprints, behavioral patterns)	Yes	No	Yes
Customized actions against suspicious bot types	Yes	No	Yes
Protection for OWASP Top 10 vulnerabilities	No	Yes	Yes
Protection from API vulnerabilities	Limited	Yes	Yes
Protection for Layer 7 denial of service (DoS)	Limited	Yes	Yes
HTTP traffic inspection	No	Yes	Yes
Masking of sensitive data	No	Yes	Yes
Compliance with HIPAA, PCI	Limited	Yes	Yes
Integration with DevOps	No	Yes	Yes
Blocking of malicious sources at the network level – access control list (ACL)	No	Yes	Yes

WAFs protect websites from application vulnerability exploits like SQL injection, cross-site scripting (XSS), cross-site request forgery, session hijacking, and other web attacks. WAFs typically feature basic bot mitigation capabilities that block bots based only on IPs and fingerprinting.

Unfortunately, most WAFs often fall short when facing advanced, automated threats. Sophisticated next-gen bots mimic human behavior and often go undetected, abusing open-source tools or generating multiple violations in different sessions.

Against today's sophisticated threats, standard WAF solutions just don't get the job done.

More Information

Book a demo or whiteboard session

Contact your Cisco sales representative today to learn how our WAF and bot solutions fit into your application security strategy

Mirai and IoT Botnet eBook, Radware, https://www.radware.com/iot-attack-ebook

Cisco SAFE Designs

See WAF in Cisco SAFE validated designs:

- Cisco SAFE Secure Cloud for Azure
- Cisco SAFE Secure Cloud for AWS

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html#~tab-design

Next Steps

For more information about our portfolio of WAF and bot management solutions, contact your Cisco sales representative today.

Gartner
API & High Security 2020
Ranked #1

Quadrant Knowledge Solutions
Bot Management, 2020
Leader

FORRESTER®
2020 WAF Wave
Strong Performer

kuppingercole ANALYSTS
Kubernetes WAF
Featured for Innovation

Security Standards Compliance and Certifications

Extensive compliance and certifications capabilities, unparalleled by any rival, including industry-specific certifications such as PCI and HIPAA, as well as cloud security standards such as ISO 27001, ISO 27017, ISO 27018, ISO 27032, and others

Learn more: cisco.com/go/secure

PROJ##### 03/21