

WAPPLES

The Intelligent Web Application and API Protection

WAPPLES is a Web Application and API Protection solution(WAAP) that utilizes logical analysis for HTTP and HTTPS traffic, protecting web applications, APIs, and mobile apps from attacks. By safeguarding applications from both known and zero-day vulnerabilities, WAPPLES is an effective solution against sensitive data exposure, website defacement, API schema protection malicious bots, and DoS, helping organizations exceed regulatory compliance.

Feature Highlights

- Logic-based detection COCEP™ engine with predefined rule sets
- OWASP Top 10 web security and OWASP Top 10 API security coverage
- Traffic load balancing with various LB algorithms
- Quick fix of vulnerabilities with virtual patching
- Economical all-in-one license policy
- Deployable on-premises, in virtual appliance, or as cloud-based SaaS
- Compatible with in Inline, Reverse Proxy, Transparent Reverse Proxy, as well as Active-Active and Active-Passive modes



Logic-based Detection : COCEP™ Engine

Set apart from legacy WAFs based on signature-matching detection, WAPPLES does not depend on signature updates or lengthy learning periods. Instead, WAPPLES' COCEP™ engine uses a set of 39 predefined rules, providing coverage for all attack patterns on known and zero-day vulnerabilities, including the OWASP Top 10 web security and OWASP TOP 10 API security. The rules are also capable of virtual patching, fixing vulnerabilities without delay.



Advanced Protection for Web Applications, APIs, and Mobile Apps

Applications are changing to an environment that uses APIs such as XML/JSON/YAML for overall efficiency. However, when the application environment changes, threats coming through APIs increase. WAPPLES blocks such threats by using a dedicated API parser/schema from the COCEP™ engine.



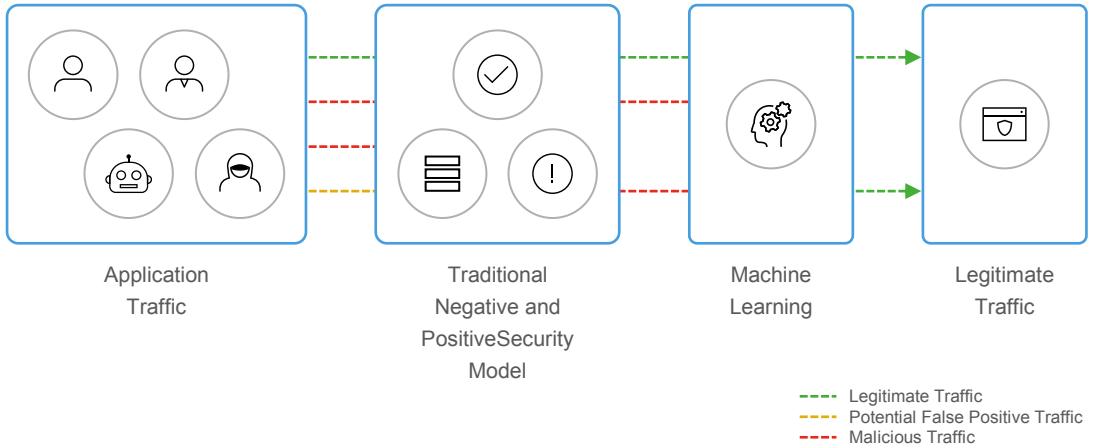
Effective Protection Against Automated Malicious Bots and DoS

A malicious user can anonymously access a website using an automated tool or malicious bots to cover up their identity. WAPPLES protects websites and applications by blocking suspicious access by malicious bots using fingerprinting, CAPTCHA, and various behavior pattern detection techniques.



Exceptionally Low False Positive Rate

WAPPLES' COCEP™ engine is not only highly effective at blocking a variety of known and unknown attack patterns, but the logical rules also ensures that it does not block benign traffic. This helps WAPPLES reach a near-zero false positive rate, helping the application excel in both security and performance.



Simplified Identity and Strong Access Management

All settings and configurations can be managed through WAPPLES Control Center (WCC) and the admin account for WCC is safely protected. The administrator can either create their own dedicated login credential or have it easily integrated with Active Directory. The login process can be further secured with mobile OTPs, protecting the platform from unauthorized access.



Easy Management with Self-Diagnostics and Periodic Inspections

With predefined security rule sets, WAPPLES users enjoy ease of use when deploying and managing the WAAP on its graphical UI. Its self-diagnostics feature detects and alerts any potential issues in the system or with regards to resources. WAPPLES is also capable of virtual patching, fixing vulnerabilities without delay.

FEATURES

Web Protection

- HTTP Compliance Validation
- Brute Force Attack
- Tor Nodes Blocking
- Web Socket Protection
- URL Encryption
- Secure Header

Data Loss Prevention

- Masking of Sensitive Information
- PII Exposure

Application Delivery

- Layer7 Server Load Balancing
- Sticky Session
- HTTP Compression
- SSL Offloading
- HTTP/2.0 Support
- Mutual TLS Support

Application Security Coverage

- OWASP Top 10 Vulnerabilities
- SQL/NoSQL/LDAP/Xpath Injection
- Server-Side Injection
- Application-level DoS
- CAPTCHA and Browser Finger Printing
- Security Patch
- Cross Site Scripting
- Cross Site Request Forgery
- Content Spoofing
- Path Traversal
- Web Scraping Protection
- Application/Server Error Handling
- Remote/Local File Inclusion
- Parameter Manipulation
- Cookie Poisoning
- Malicious File Upload
- Website Defacement
- Bot Protection
- Zero-Day Attack Protection

API Protection

- XML Schema/DoS Protection
- JSON Schema/DoS Protection
- YAML Schema/DoS Protection

Deployment

- Transparent Inline
- Reverse Proxy
- Transparent Reverse Proxy
- Offline Monitoring (Mirroring)

Flexible Inspection Controls

- Custom Rule
- Preconfigured Security Policies
- IP Reputation
- IP Geolocation-based Blocking
- HTTP Header Control
- IP based Access Control
- URL/HTML/Base64 Decoding
- Risk Scoring

Others

- Self-Diagnostics and Alert
- LDAP/Active Directory Integration
- Admin Console Login with 2FA
- Intuitive False Positives Management
- Vulnerable SSL/TLS Version & Cipher Control
- SSL Certificate Management
- IPv6 Ready
- SSL Accelerator
- Secure SSL Key Storage
- Web Access Management

Management & Reporting

- Web/Command Line User Interface
- Customized Report Generation
- Automatic Report Delivery Via Email, Etc.
- OWASP Top 10 Categorized Report
- REST API
- SNMP/SYSLOG and CEF Support
- Real-time Dashboard
- Central Management for Multiple Devices
- Active/Active, Active/Passive Clustering
- Policy Log Synchronization
- Geolocation-based Logging and Monitoring

Hardware Appliance Specifications

Class	Value	Performance			High-End	
Model	WAPPLES-160	WAPPLES-1600	WAPPLES-2600	WAPPLES-4600	WAPPLES-5600	WAPPLES-12000
Throughput	300 Mbps	1 Gbps	2 Gbps	4 Gbps	6 Gbps	10 Gbps
RAM	8 GB	16 GB	32 GB	48 GB	96 GB	192 GB
SSD	1 TB	1 TB	1 TB + 1 TB	1 TB + 1 TB	1 TB + 1 TB	1 TB + 1 TB
Storage Type	Internal	Hot Swap	Hot Swap	Hot Swap	Hot Swap	Hot Swap
RAID	-	-	Optional	Optional	Optional	Optional
Management Port	2 x 1G CU	2 x 1G CU	2 x 1G CU	2 x 1G CU	2 x 1G CU	2 x 1G CU
Default NIC Bypass Port	4 x 1G CU bypass	4 x 1G CU bypass	4 x 1G CU bypass or 2 x 1G Fiber bypass or 2 x 10G Fiber bypass	4 x 1G CU bypass or 2 x 1G Fiber bypass or 2 x 10G Fiber bypass	2 x 1G Copper port 4 x 1G Cooper bypass port 2 x 10G Fiber bypass port	
HA Configuration	Yes	Yes	Yes	Yes	Yes	Yes
Form Factor	1U	1U	2U	2U	2U	2U
WxLxH (mm)	438 x 292 x 44	438 x 292 x 44	438 x 452 x 88	438 x 550 x 88	465 x 594 x 89	465 x 594 x 89
Weight (kg)	4.8 kg	4.8 kg	12.9 kg	16.2 kg	21.4 kg	21.9 kg
Power Supply (100-240V)	150W	150W	Dual 300W	Dual 600W	Dual 800W	Dual 800W

• Specifications subject to change without notice.



[WAPPLES-160]



[WAPPLES-1600]



[WAPPLES-2600]



[WAPPLES-4600]



[WAPPLES-5600]



[WAPPLES-12000]

WAPPLES SA

WAPPLES Virtual Appliance

WAPPLES SA is a Web Application and API Protection solution(WAAP) that protects customers’ business-critical applications from known and zero-day attacks. Besides blocking web attacks such as SQL Injection and Cross-Site Scripting (XSS), WAPPLES SA is an effective solution against sensitive data exposure, website defacement, API schema protection malicious bots, and DoS, helping organizations exceed regulatory compliance.

WAPPLES SA provides robust protection for sensitive assets enabling secure services that customers can trust.

1) **COCEP™** : Contents Classification and Evaluation Processing

Self-Diagnostics Feature

To maintain reliable web services, any interruptions to smooth delivery must be addressed promptly. The Self-Diagnostics feature in WAPPLES SA performs continuous checks on various performance statuses that influence service delivery, automatically triggering remediation and alerts to administrators when any status exceeds minimum safety thresholds.

WAPPLES SA Key Benefits

- Reduce Total Cost of Ownership (TCO)
 - High Availability mode for stable services
 - Elevate trust with industry-leading web security
 - Multi Domain NAT Using L7 Based Hostname
- Wide-ranging partnership and collaboration models
 - Support for the latest protocols HTTP/2 and TLS 1.3
 - Real-time health monitoring with Self-Diagnostics
 - Immediately patch new vulnerabilities with Custom Rule

Virtual Appliance Specifications

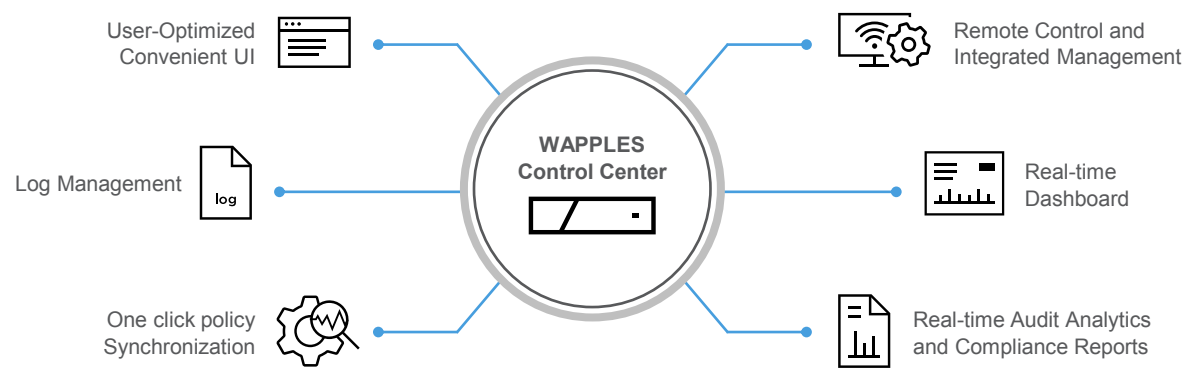
Class	Value	Performance		High-End	
Model	WAPPLES SA-50	WAPPLES SA-100	WAPPLES SA-500	WAPPLES SA-1000	WAPPLES SA-1000
Throughput	100 Mbps	300 Mbps	500 Mbps	1 Gbps	4 Gbps
RAM	4 GB	8 GB	16 GB	32 GB	64 GB
Storage	40 GB	80 GB	100 GB	200 GB	1 TB
HA Support	Yes	Yes	Yes	Yes	Yes
Supported Hypervisors	Vmware, Hyper-V, Xen Server, Linux KVM				
Public Cloud Support	AWS, Microsoft Azure, Google Cloud, Alibaba Cloud				

- Actual performance may vary depending on multiple factors including system configuration, hardware specifications, and network traffic.
- For guaranteed performance of WAPPLES SA, please refer to the following system recommendations:
 - Intel CPU-based server is strongly recommended as performance on AMD and ARM CPU(QEMU64)-based servers may be unstable.
 - Instability may occur under the KVM-QEMU environment configuration of "QEMU virtual CPU (QEMU64)". It is recommended to configure to the Intel CPU model name.

WAPPLES Control Center

Centralized Management for Multiple WAPPPLES

WAPPLES Control Center is an integrated management system that allows to remotely manage multiple WAPPLES installations across multiple network bands using a single management console. WAPPLES Control Center resolves administrative challenges due to redundancy configuration.



Specifications

Class	Value	Performance	High-End
Model Name	2600	4600	5600
The maximum number of Managing Count	8	16	24
Form Factor	2U	2U	2U
Memory	32 GB	48 GB	96 GB
SSD	1 TB + 1TB	1 TB + 1 TB	1 TB + 1 TB



[WAPPLES CC-2600]



[WAPPLES CC-4600]



[WAPPLES CC-5600]