Virtual Web Application Firewall for Your Cloud

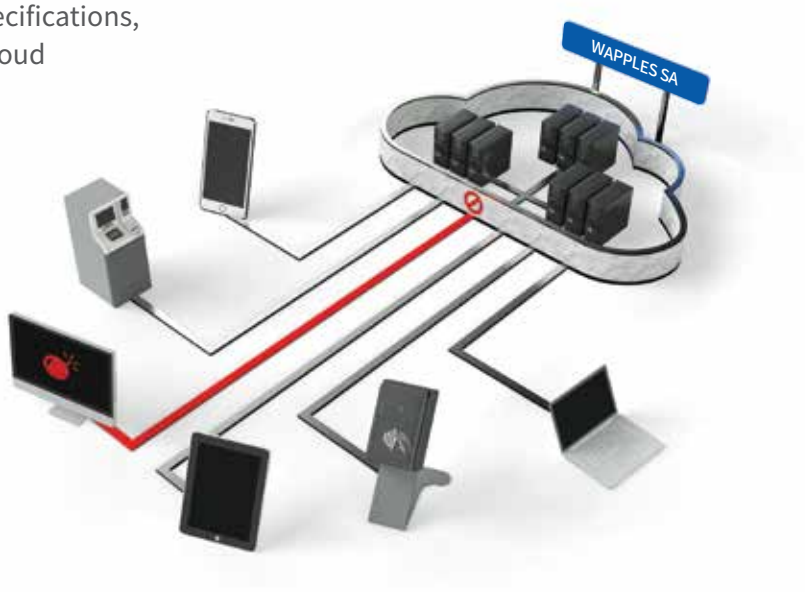
WAPPLES SA

WAPPLES
The Logical Web Application Firewall

No.1 in the Asia-Pacific Web Application Firewall Market

Secure Your Cloud

WAPPLES SA is a virtual web application firewall for the private data center or cloud environment. Based on award-winning WAPPLES technology, the WAPPLES SA can detect and immediately block known, modified, and zero-day attacks with its Contents Classification and Evaluation Processing or COCEP™ engine.
WAPPLES SA is available in a variety of specifications, matching the dynamic scalability of the cloud and providing the most appropriate level of protection for any sized company.



Features

1 High-end Security

- Logic-analysis based COCEP™ engine protects websites against OWASP Top 10 risks
- Extremely low false positive rates through heuristic and semantic traffic analysis
- Utilizes 26 detection rules that can be fine-tuned to create robust custom security policies
- Defense from known, zero-day, and HTTP DDoS attacks
- Validity testing (Luhn : ISO/IEC7812) prevents leakage of sensitive data

2 Easy to Install & Configure

- Minimal changes to existing systems
- Quick setup with preconfigured security policies
- Statistics visualized on centralized dashboard
- Intuitive and easy-to-use GUI management console
- Increased efficiency in web security management

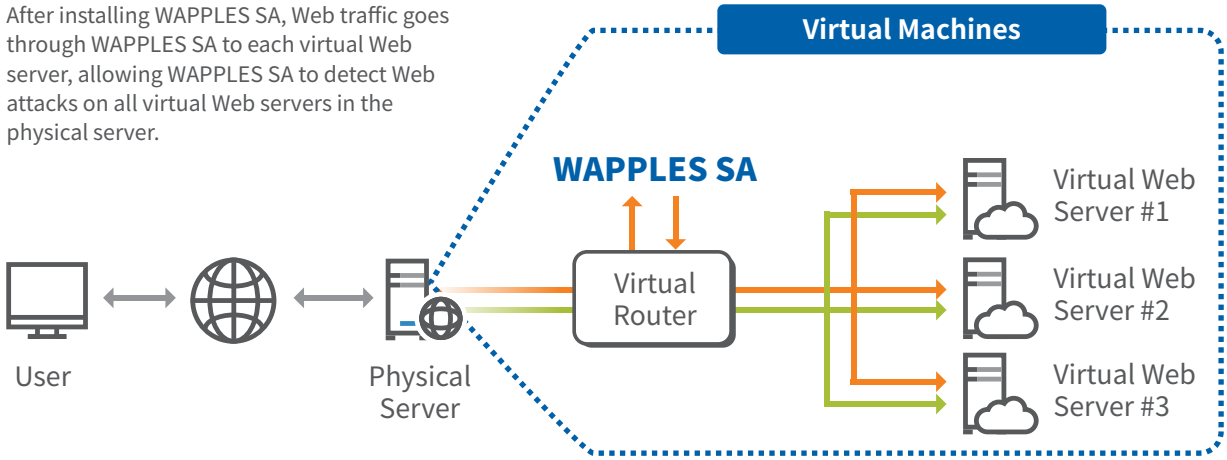
3 Optimized for Cloud Systems

- Virtual appliance web application firewall designed for seamless integration with cloud systems
- Supports multiple virtual platforms (VMware, Citrix Xen, Red Hat KVM)

Diagram

Web traffic flow : Before install After install

After installing WAPPLES SA, Web traffic goes through WAPPLES SA to each virtual Web server, allowing WAPPLES SA to detect Web attacks on all virtual Web servers in the physical server.



WAPPLES SA Allows Cloud Service Providers to

1. Increase cloud service reliability through improved security
2. Build customized management pages with WAPPLES SA' Web API
3. Independently manage H/W servers and S/W protection with a reverse proxy IP
4. Reduce TCO by utilizing a virtual appliance rather than a H/W model
5. Support high availability, complete with policy and log synchronization in real time
6. Provide scalable security products to match the flexibility of the cloud

Product Lineup

Division	V50	V100	V300	V500	V1000
vCPU Core	2 Core	4 Core	6 Core	8 Core	16 Core
Minimum Memory	4 GB				
Throughput	50 Mbps ~ 5,000 Mbps				

▪ Penta Security recommends for every additional vCPU core, add at least 2 GB of memory, e.g. 1 core : 2 GB RAM

Penta SECURITY
cloud · iot · enterprise

Penta Security Systems Inc. (HQ)
25, Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Korea, 07327
TEL. +82-2-780-7728 **FAX.** +82-2-786-5281 / www.pentasecurity.co.kr
INQUIRIES. +82-2-2125-6617 / globalbiz@pentasecurity.com

Penta Security Systems Co.
Houston, Texas www.pentasecurity.com

Penta Security Systems K.K.
Shinjuku-Ku, Tokyo www.pentasecurity.co.jp

Asian Cyber Security Vendor of the Year

171103