Datasheet

Viettel Smart Web Protection
(VCS – SWP)

viettel security

Necessity of solution

In the 21st century, government departments and businesses increasingly face many new challenges in information technology (IT) and media.

The rapid development of technology has allowed many units apply IT to management and business through online news portal, thereby bringing convenience to users in interactions with businesses and government departments.

When applying IT, however, the websites of the units will have to face the risk of attacks from external network into the organization's system, in-depth penetration into the internal network. network or stealing user information, credit card information, etc., which might lead to cause of economic and reputational damage to organizations.

Therefore, equipping a protection solution for web applications is absolutely necessary.

Main features

Comprehensive anti-DDoS attack

Layer 3,4 anti-DDoS attack

- Detecting anomalies based on actual customer traffic profiles
- Detecting and mitigating various types of attacks: UDP flood, ICMP flood, SYN flood, DNS Amplification, NTP Amplification,SSDP, ...
- Defining a list of Good IPs for both the entire network and each client (list of trusted IPs which clients frequently connect to in normal case) so that accesses can be passed quickly without any further processing.

Layer 7 anti-DDoS attack

- Detecting anomalies based on actual customer traffic profiles
- Detecting and mitigating various types of attacks: UDP flood, ICMP flood, SYN flood, DNS Amplification, NTP Amplification,SSDP, ...
- Defining a list of Good IPs for both the entire network and each client (list of trusted IPs which clients frequently connect to in normal case) so that accesses can be passed quickly without any further processing.

Web attack Prevention

Web Application Firewall (WAF)

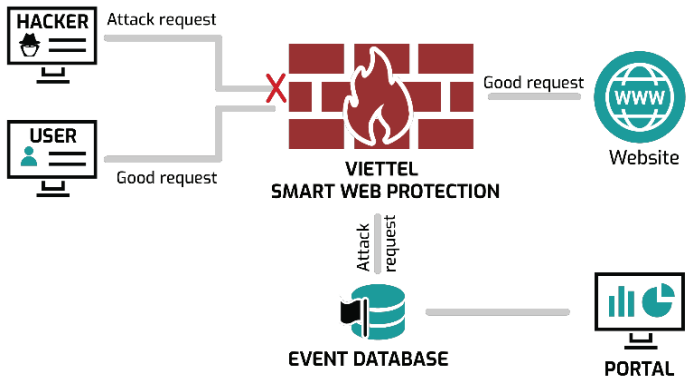
- Protect websites against common web vulnerabilities in the top 10 OWASP: Injection, Unvalidated Input, Broken Authentication and Session Management, Sensitive Data Exposure, XML External Entities (XXE), XML External Entities (XXE), Broken Access Control, Security Misconfiguration, CrossSite Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities.
- User access control and analysis in real time allows to prevent attacks based on packet-level analysis, aggregate access anomalies in request and response data, identify the level of danger and prevent it in time.

Viettel Smart Web Protection

Layer 3,4 & 7 anti-DDoS attack & Web Application Firewall (WAF) supports to get protection the websites against common web vulnerabilities such as: injection, Cross-Site-Script, Remote File Inclusion, XML External Entity....

User access control and analysis system in real time allows to prevent attacks based on analysis and synthesis of anomalies in access, request and response data.

Deploying website system protection is also simple, fast and flexible through Cloud or Virtual Appliance.



Benefits

Real-time Attack Detection

Using intelligent algorithms, the VCS - SWP solution analyzes risks and allows detecting and preventing website attacks immediately, minimizing risks for customers.

Flexibility and Ultimate Protection

Based on the characteristics of the framework, programming language, web server, etc. of each website, the system will give an optimal and accurate rule set. It helps to minimize the number of False Positive Request.

Timely Deployment - Easy Operation

The appliance is packaged in a standardized Virtual Appliance that can be deployed quickly and ensures high performance. The device supports all the features including alarm, management, and required configuration to operate the service on both the Portal and the

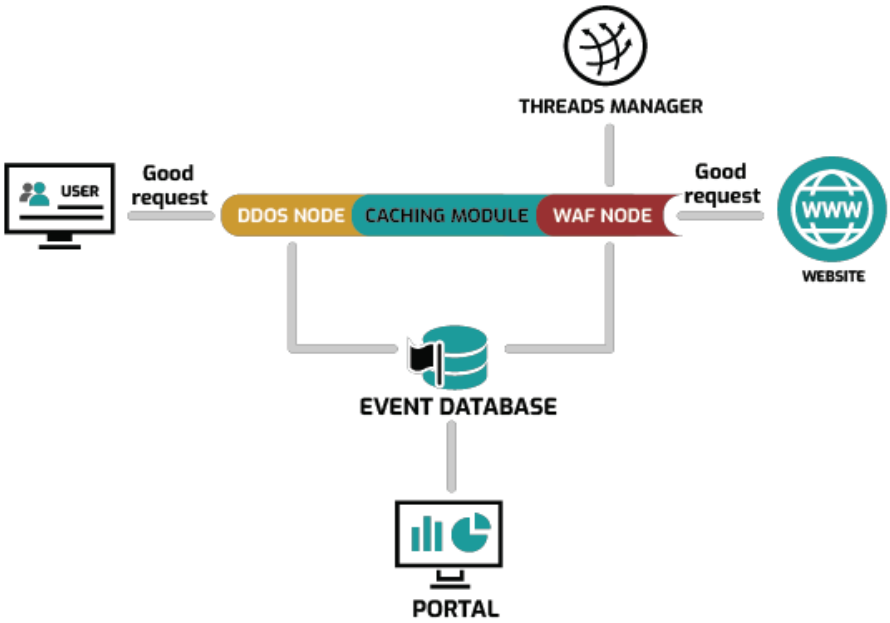
Centralized Management and Monitoring

The centralized administration system helps administrators monitor entirely suspected attacks on websites, detecting existing risks on the system.

Viettel Smart Web Protection
(VCS – SWP)

viettel security

Solution Deployment Model



Incoming packets are processed and intercepted through the anti-attack layers in the following order:

- Network layer DDoS attack prevention (Layer 3, 4): Installed on stand-alone servers and placed in front of web application; Play the role of analyzing and detecting abnormal requests and responses.
- Network layer DDoS attack prevention (Layer 7): Plays the role of DDOS Layer 7 attack protection, load balancing for WAF Nodes and caching data.

Prevent Web Attacks - WAF: The centralized stores anomalous events pushed back from WAF Node, DDOS Node.
The monitoring of interception capabilities, device monitoring, configuration of containment features are done through the following modules:

- Portal: In charge of exchanging information between WAF Node and other components, processing raw data to correlate information security events pushed to the Event Database.
- CLI: System administration, monitoring and monitoring interface

HIGHLIGHTS

1. Real-time attack detection and prevention
2. Rule setting is flexible, high accuracy
3. Centralized management and monitoring of multiple websites
4. Flexible deployment, expansion, easy upgrade.