Datasheet

Viettel Smart Web Protection
(VCS – SWP)

viettel security

Sự cần thiết của giải pháp

Trong thế kỷ 21, các cơ quan chính phủ và doanh nghiệp ngày càng đối mặt với nhiều thách thức mới về công nghệ thông tin (CNTT) và truyền thông. Sự phát triển nhanh chóng về công nghệ đã cho phép nhiều đơn vị áp dụng CNTT vào việc quản lý, kinh doanh qua các cổng thông tin điện tử, qua đó đem lại sự tiện dụng cho người dùng trong việc tương tác với các doanh nghiệp và cơ quan nhà nước. Tuy nhiên, khi áp dụng CNTT, các website của các đơn vị sẽ phải đối mặt với các nguy cơ bị tấn công từ ngoài Internet vào hệ thống của tổ chức để xâm nhập sâu vào bên trong mạng lưới nội bộ hoặc đánh cắp các thông tin người dùng, thông tin về thẻ tín dụng, ..., gây thiệt hại về mặt kinh tế cũng như uy tín cho các tổ chức. Vì vậy, việc trang bị một giải pháp bảo vệ cho các ứng dụng web là hết sức cần thiết

Những tính năng chính

Chống tấn công DDoS toàn diện

Chống tấn công DDoS lớp mạng (Layer 3, 4)

- Phát hiện các dấu hiệu bất thường dựa trên việc profile về lưu lượng thực tế của khách hàng
- Phát hiện và giảm thiểu các loại tấn công: UDP flood, ICMP flood, SYN flood, DNS Amplification, NTP Amplification, SSDP, ...
- Xác định danh sách Good IP đối với toàn mạng và từng khách hàng (là danh sách IP tin cậy mà khách hàng thường xuyên kết nối tới ở trạng thái bình thường) để các truy cập được thông qua nhanh mà không cần xử lý thêm.

Chống tấn công DDoS lớp ứng dụng (Layer 7)

- Phát hiện và ngăn chặn các tấn công DDoS Layer 7: Slowloris, attacks, HTTP Flood, ...
- Tính năng Caching Module hỗ trợ lưu cache tài nguyên dựa trên

Chống tấn công Web

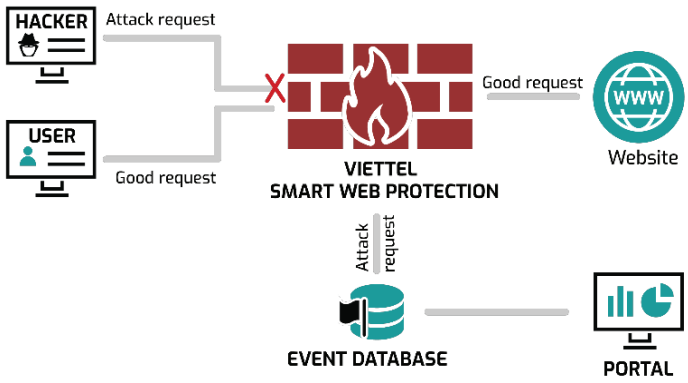
Tường lửa ứng dụng web (Web Application Firewall)

- Bảo vệ các website trước các tấn công lỗ hổng web phổ biến thuộc 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.

- Phân tích và kiểm soát truy cập người dùng theo thời gian thực cho phép ngăn chặn các tấn công dựa trên phân tích mức gói tin, tổng hợp các bất thường trong truy cập trong dữ liệu request, response và xác định mức độ nguy hiểm ngăn chặn kịp thời

Giải pháp Viettel Smart Web Protection

Viettel Smart Web Protection (VCS – SWP) là thiết bị dạng ảo hóa, hỗ trợ các tính năng bảo vệ website tối tân nhất bao gồm các tính năng: Chống tấn công Từ chối dịch vụ layer 3, 4, 7 và Tường lửa ứng dụng web (WAF), giúp bảo vệ các website trước các tấn công lỗ hổng web phổ biến như: SQL injection, Cross-Site-Script, Remote File Inclusion, XML External Entity,...
Hệ thống phân tích và kiểm soát truy cập người dùng theo thời gian thực cho phép ngăn chặn các tấn công dựa trên phân tích, tổng hợp các bất thường trong truy cập, trong dữ liệu request, response. Việc triển khai bảo vệ hệ thống website cũng đơn giản và nhanh chóng, có thể linh hoạt theo hướng Cloud hoặc Virtual Appliance.



Lợi ích

Phát hiện tấn công trong thời gian thực

Sử dụng các thuật toán thông minh, giải pháp VCS - SWP phân tích các nguy cơ và cho phép phát hiện và ngăn tấn công website ngay lập tức, giảm thiểu rủi ro cho khách hàng.

Tập linh hoạt - Bảo vệ tối ưu

Dựa trên đặc điểm framework, ngôn ngữ lập trình, web server,... của từng website, hệ thống sẽ đưa ra tập luật tối ưu và chính xác. Từ đó giúp tối giản số lượng cảnh báo sai (False Positive Request)

Triển khai nhanh - Vận hành dễ dàng

Thiết bị được đóng gói dạng Virtual Appliance chuẩn hóa có thể triển khai nhanh chóng và đảm bảo hiệu năng cao nhất. Thiết bị hỗ trợ tất cả các tính năng cảnh báo, quản lý, cấu hình cần thiết để vận hành dịch vụ trên cả Portal và giao diện Command Line Interface (CLI).

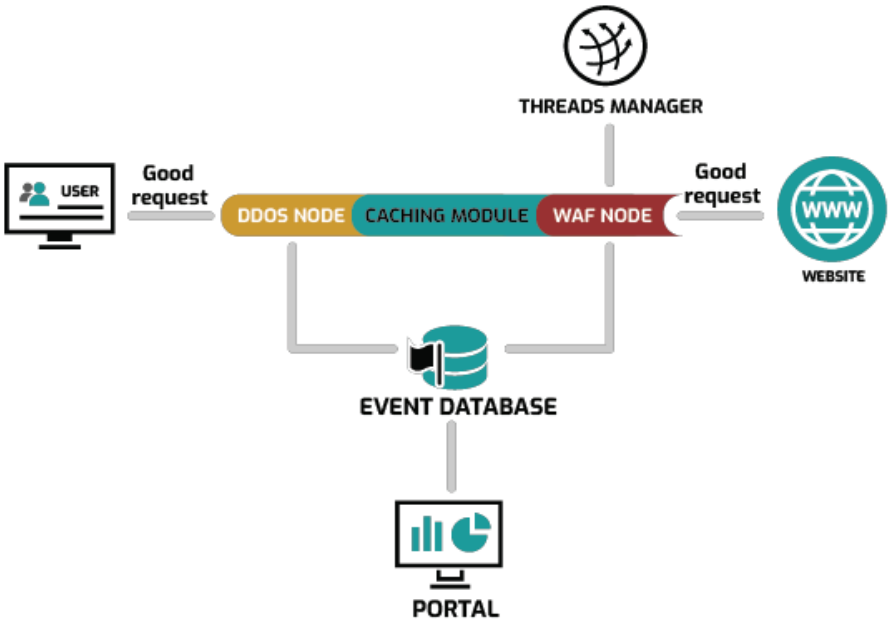
Quản trị và Giám sát tập trung

Hệ thống quản trị tập trung giúp quản trị viên giám sát được toàn bộ hành vi nghi ngờ là tấn công vào các website, từ đó phát hiện ra những rủi ro đang tồn tại trên hệ thống.

Viettel Smart Web Protection
(VCS – SWP)

viettel security

Mô hình triển khai giải pháp



Gói tin đi vào được xử lý và ngăn chặn qua các tầng chống tấn công theo thứ tự:

• Ngăn chặn tấn công DDoS tầng mạng (Layer 3, 4): Được cài đặt trên các server độc lập và đặt trước các ứng dụng web. Đóng vai trò phân tích, phát hiện request, response bất thường.
• Ngăn chặn tấn công DDoS tầng ứng dụng (Layer 7): Đóng vai trò chống tấn công DDOS Layer 7, load balancing cho các WAF Node và caching data.
• Ngăn chặn tấn công Web - WAF: Thành phần lưu trữ tập trung các event bất thường được đẩy về từ các WAF Node, DDOS Node.

Việc giám sát khả năng ngăn chặn, giám sát thiết bị, cấu hình các tính năng ngăn chặn được thực hiện qua các mô đun:

• Portal: Làm nhiệm vụ trao đổi thông tin giữa WAF Node và các thành phần khác, xử lý các dữ liệu thô để tương quan ra các sự kiện an toàn thông tin đẩy về Event Database.
• CLI: Giao diện quản trị, theo dõi, giám sát hệ thống

ƯU ĐIỂM

1. Phát hiện và ngăn chặn tấn công nhanh chóng theo thời gian thực
2. Tập luận (Rule) linh hoạt, có độ chính xác cao
3. Quản trị, giám sát tập trung đồng thời nhiều website
4. Triển khai linh hoạt, mở rộng, nâng cấp dễ dàng.