CÔNG TY TNHH AN NINH AN TOÀN THÔNG TIN CMC – CMC CYBER SECURITY LTD.

Tầng 15 tòa nhà CMC, phố Duy Tân, Dịch Vọng Hậu, Cầu Giấy, Hà Nội | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

15th Floor, CMC Tower, Duy Tan Street, Dich Vong Hau Ward, Cau Giay District, Hanoi | Tel: 84.4.3795 8282 | Fax: 84.4.3984 5053 | www.cmccybersecurity.com

DATASHEET GIẢI PHÁP TƯỜNG LỬA ỨNG DỤNG WEB CMC

Thành viên chính thức của AVAR và ICSA

Hà Nội, 01/08/2019

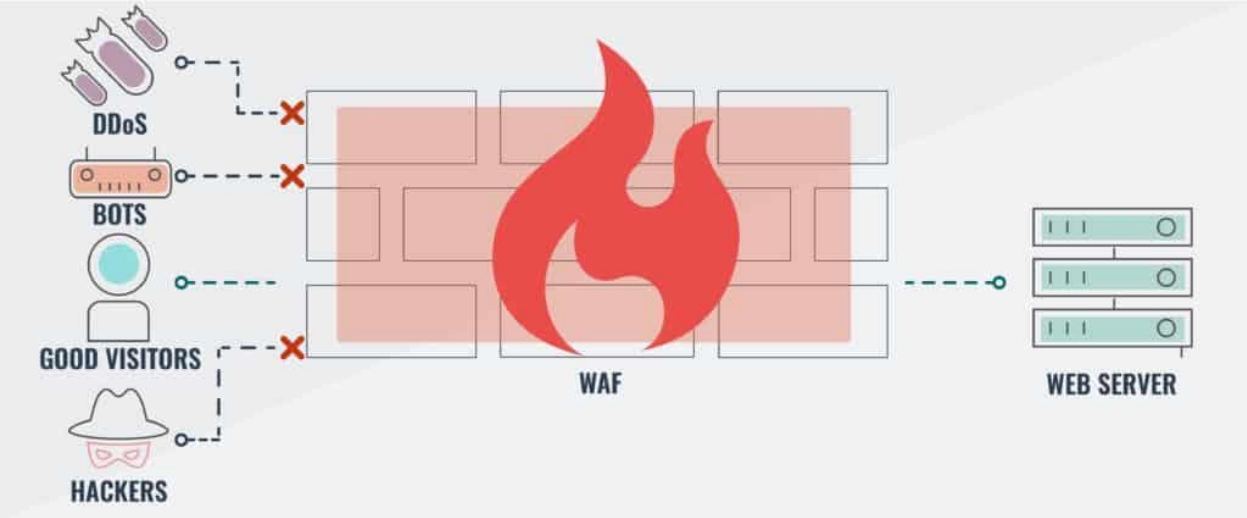
CMC CYBER SECURITY
Aspire to Inspire the Digital World

CÔNG TY TNHH AN NINH AN TOÀN CMC CYBER SECURITY

Version	1.0
Date	01/08/2019
Document Type	Datasheet
Prepared By	Trần Trọng Thắng Nguyễn Thế Nghiệp

CMC Web Application Firewall Cloud-Based (WAF)

Bảo vệ ứng dụng web trước các mối đe dọa, các cuộc tấn công, tích hợp công nghệ CMC SOC AI



Tường lửa ứng dụng web CMC (CMC WAF) là một phần của bộ bảo đảm an toàn thông tin do CMC CS cung cấp cho các doanh nghiệp, dịch vụ tích hợp trên cloud bảo vệ trang web, các API trước các cuộc tấn công, các mối đe dọa đã từng hoặc chưa từng được biết đến bằng các công cụ ruleset mạnh mẽ được tính hợp trí tuệ nhân tạo AI giúp nâng cao hiệu năng hoạt động.

Về cơ chế hoạt động, CMC WAF cung cấp giải pháp bảo vệ liên tục cho website và các ứng dụng sử dụng cơ chế phân tích traffic mạng và chỉ cho phép các yêu cầu truy cập hợp lệ thông qua.

I. Lợi ích khách hàng

- Bảo vệ 24/7 ứng dụng, website trước các mối đe dọa thuộc top 10 OWASP bao gồm Cross-site Scripting và SQL Injection.
- Ứng dụng công nghệ AI và Machine Learning giúp phát hiện các mối đe dọa tức thì.
- Dễ dàng mở rộng quy mô do được tích hợp trên cloud.
- Giao diện dashboard dễ dàng quản lý hoạt động của firewall, traffic mạng.
- Dễ dàng tùy chỉnh các bộ quy tắc (rule) cho firewall phù hợp với đặc thù của khách hàng.
- Tuân thủ tiêu chuẩn bảo mật dữ liệu thẻ PCI-DSS dành cho các ngân hàng.

II. Tính năng nổi bật

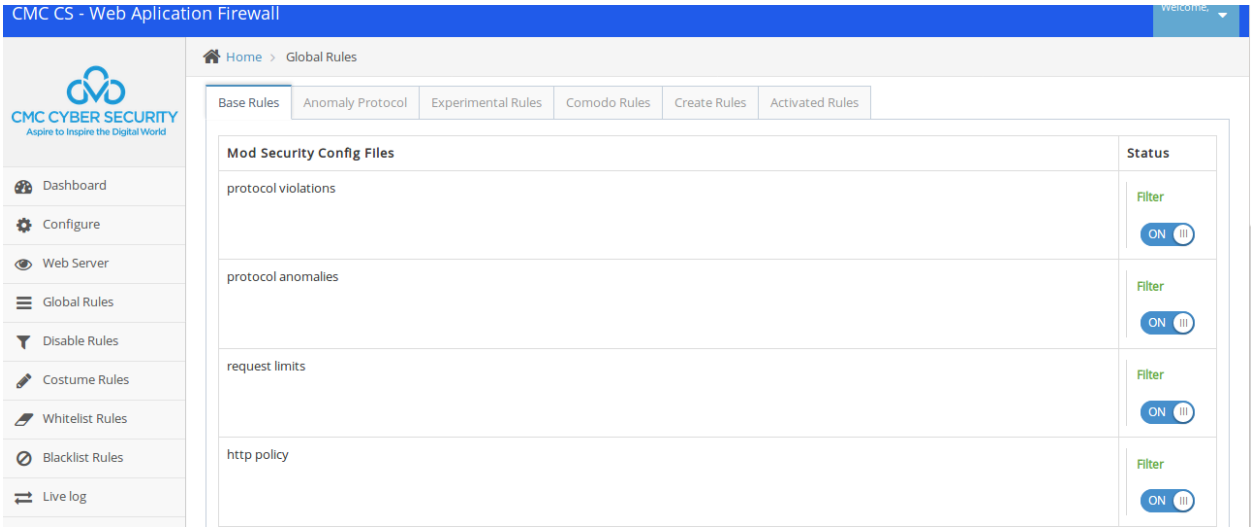
1. Bảo vệ ứng dụng (Application protection)

- ***WAF bảo vệ website trước top 10 mối đe dọa của OWASP bao gồm Cross-Site Scripting (XSS) và SQL Injection.***
    - C - WAF có chức năng phát hiện và ngăn chặn tức thì đối với các cuộc tấn công vào ứng dụng Web thuộc Top 10 OWASP bao gồm:
        - Injection
        - Broken Authentication
        - Sensitive Data Exposure
        - XML External Entities
        - Broken Access Control
        - Security Misconfiguration
        - Cross-Site-Scripting(XSS)
        - Insecure Deserialization
        - Using Components with Know Vulnerabilities
        - Insufficient Logging & Monitoring
    - Ngoài ra, C – WAF còn có tập luật do các chuyên gia CMC Cyber Security phát triển mạnh mẽ và luôn được cập nhật và tối ưu thường xuyên nhờ việc liên tục thu thập thông tin về các mối đe dọa trên thế giới qua hệ thống CMC Threat Intelligence.
- ***Bảo vệ website trước các cuộc tấn công DoS tầng ứng dụng (layer 7): Tất cả lưu lượng truy cập đến được thống kê liên tục và nếu vượt quá ngưỡng sẽ được kiểm tra để xác minh nó đến từ con người.***
    - Một trong số các chức năng của C – WAF là việc phân biệt các hành vi bất thường của người dùng qua đó dễ dàng phát hiện các hành vi độc hại đến từ các botnet đang tấn công vào hệ thống ứng dụng website.
    - C – WAF có khả năng phát hiện ra các dấu hiệu, hành vi của các kỹ thuật tấn công DOS vào hệ thống ứng dụng Website và thực hiện ngăn chặn cuộc tấn công một các tức thì.
    - Cơ chế phát hiện DOS có thể được cấu hình trên các trang và tùy chỉnh các ngưỡng phụ thuộc vào cấu hình, thông số và băng thông của thiết bị chạy ứng dụng Web qua đó có thể dễ dàng áp dụng cho từng Website có chức năng riêng biệt và đặc thù.
- ***Virtual patching vulnerabilities: WAF tạo ra một lá chắn ảo giúp bảo vệ website trước các nguy cơ bị tấn công trong khi các lỗ hổng thực sự đang vá sử dụng công nghệ học máy.***
    - Nhờ tập luật của C – WAF có thể dễ dàng tùy chỉnh hoặc thêm bớt do đó C – WAF cung cấp một bản vá ảo giúp cho website hoạt động bình thường và

phòng chống bị khai thác các lỗ hổng khi các lỗ hổng thực sự đang được các quản trị viên vá.

- C – WAF hướng tới sự nhanh chóng và thực hiện ngắn hạn chính sách bảo mật nhằm ngăn chặn việc khai thác xảy ra do một lỗ hổng mới được phát hiện qua đó bảo vệ Website một cách tối ưu nhất.

- ***HTTPS/SSL qua WAF: Bảo mật liên tục việc truyền dữ liệu giữa người quản trị và người dùng, sử dụng các chứng chỉ SSL (SSL Certificates) của Website.***
  - Những Website chạy HTTPS khi sử dụng C – WAF sẽ được hỗ trợ cấu hình một cách dễ dàng bằng cách sử dụng chứ năng thêm chứng chỉ SSL trực tiếp trên giao diện Website quản trị của C – WAF qua đó người quản trị hệ thống WAF có thể thêm các tùy chỉnh về chứng chỉ SSL một cách dễ dàng nhất và tức thì khi có những thay đổi trong quá trình quản trị hệ thống ứng dụng Website.

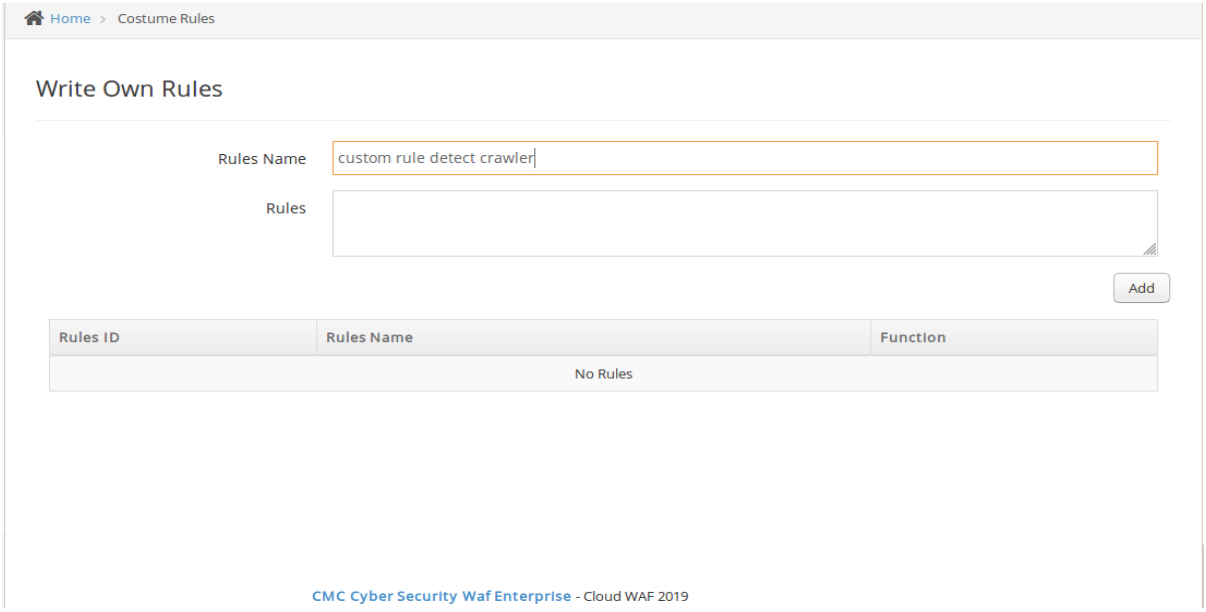


2. Tập quy tắc (rule) mạnh mẽ, dễ dàng tùy chỉnh

- ***Liên tục nghiên cứu và cải thiện việc phát hiện và giảm thiểu nguy cơ đến từ các mối đe dọa. Ngoài ra, WAF cho phép người dùng có thể thêm các quy tắc tùy chỉnh của riêng mình hoặc bật / tắt các quy tắc bất kỳ sẵn có.***
  - Đội ngũ chuyên gia CMC liên tục nghiên cứu và thu thập các thông tin về các mối đe dọa trên thế giới qua đó có thể nhanh chóng cập nhật, tùy chỉnh lại các quy tắc, tập lập để có thể ngăn chặn kịp thời các hình thức tấn công, khai thác mới vào hệ thống ứng dụng Website.
  - C – WAF có chức năng bật tắt các rules để cho người quản trị dễ dàng trong việc sử dụng các tập luật cho các Website sử dụng C – WAF với giao diện dễ dàng sử dụng. Ngoài ra, C – WAF còn có chức năng bât/ tắt các tập luật

cho từng domain Website qua đó có thể dễ dàng tùy chỉnh cho từng Website có chức năng đặc thù.

- Với việc nghiên cứu các phương pháp, hình thức tấn công mới người quản trị cũng có thể sử dụng chức năng Customer Rules để tự mình thiết lập các tập rules mới dựa vào các IOC, signature.



3. Giám sát thời gian thực & Phân tích

- ***WAF cung cấp thông tin chi tiết theo thời gian thực về lưu lượng truy cập web và các sự kiện bảo mật.***
  - C – WAF cung cấp màn hình hiển thị Dashboard các thống kê thông tin về CPU sử dụng, lưu lượng truy cập vào các ứng dụng Website, thống kê thông tin các sự kiện bảo mật theo thời gian(các thông tin sự kiện bảo mật bao gồm cách thức tấn công, IP nguồn, Website bị tấn công,…)
- ***Định vị địa lý***
  - Qua quá trình phân tích C – WAF có thể thống kê các IP thực hiện tấn công, hình thức tấn công theo từng khu vực.
- ***Traffic theo thời gian thực***
  - C – WAF cung cấp biểu đồ lưu lượng mạng sử dụng theo thời gian thực/ mốc thời gian.
  - Giúp người quản trị dễ dàng nắm bắt tình hình bảo mật đối với ứng dụng website đang quản trị
- ***Phân tích sự kiện bảo mật***

- Sau khi thực hiện phân tích các các sự kiện an toàn thông tin, C – WAF sẽ hiển thị, thống kê các sự kiện an toàn thông tin theo Top 10, Top các IP thực hiện tấn công nhiều nhất vào Website,…

4. Phát hiện hành vi bất thường sử dụng AI

Cải thiện khả năng phát hiện các mối đe dọa mới và các lỗ hổng zero-day bằng cách tận dụng công nghệ topic modelin được hỗ trợ bởi CMC SOC AI để phát hiện các yêu cầu ứng dụng bất thường và xác định xem chúng có phải là mối đe dọa hay không.

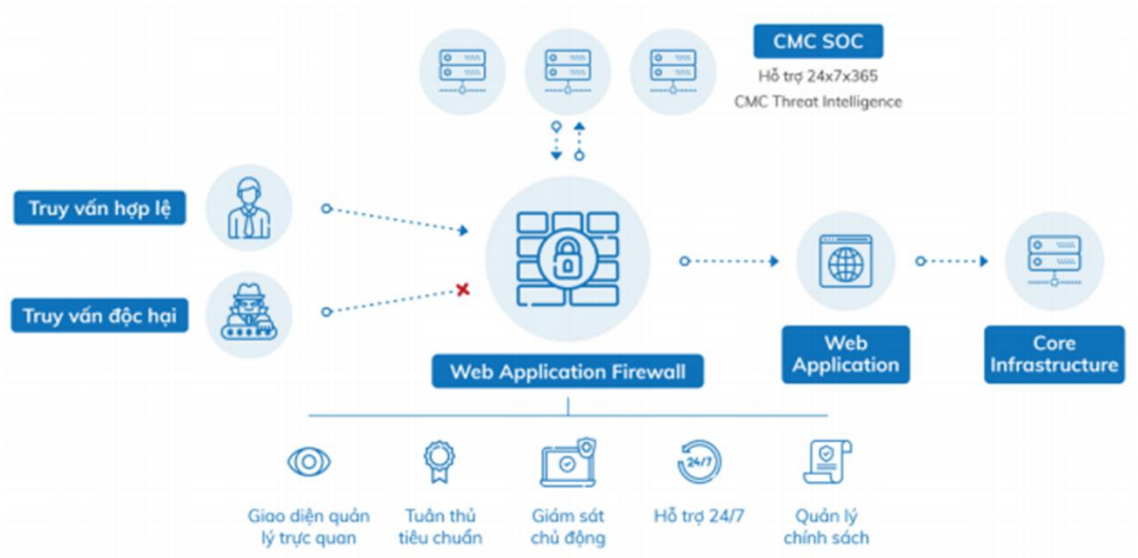
5. Tích hợp CMC Threat Intelligence

WAF sử dụng TI (Threat Intelligence) giúp hỗ trợ phát hiện, ngăn chặn các mối đe dọa tấn công vào website, giúp giảm tỉ lệ phát hiện sai (false positive), giúp tiết kiệm thời gian cho hoạt động quản lý.

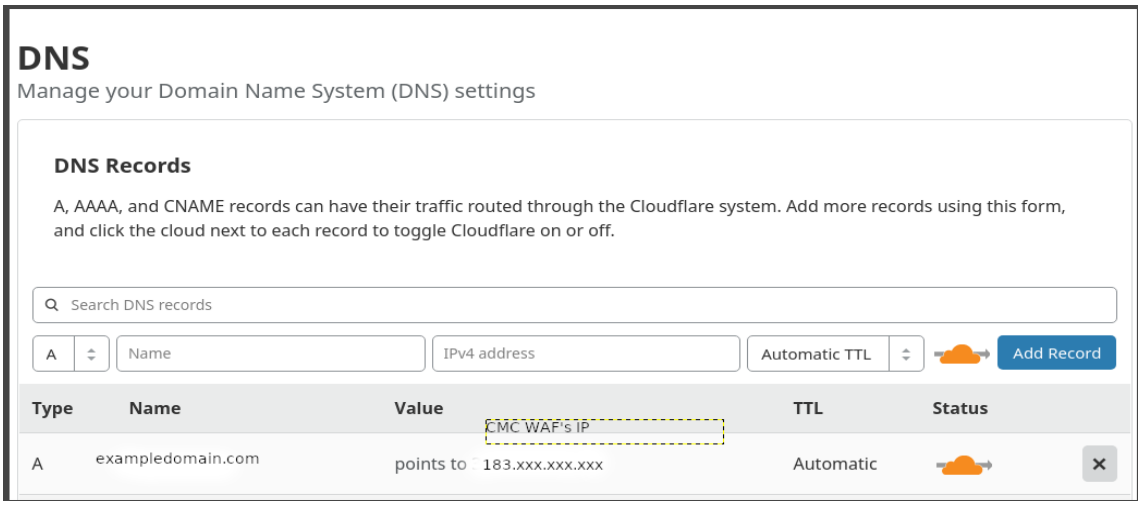
- Theo dõi các mã CVE, 0 - day mới, cập nhật hàng ngày
  - Hệ thống CMC Threat Intelligence luôn cập nhật thường xuyên các các lỗ hổng bảo mật mới trên thới giới từ nhiều nguồn khác nhau qua đó có thể làm giàu dữ liệu, đội ngũ chuyên gia bảo mật liên tục phân tích các thông tin mới nhất về các kỹ thuật cách thức tấn công để làm giàu cho dữ liệu CMC Intelligence và cập nhật vào C – WAF.
- Tự động cập nhật các tập luật, kỹ thuật tấn công mới nhật từ hệ thống.
  - Hệ thống C – WAF kết nối với hệ thống CMC – Threat Intelligence do đó sẽ liên tục cập nhật tự động các tập luật mới theo định kỳ dựa vào các phân tích về các cách thức tấn công, các lỗ hổng mới được phát hiện trên thế giới.

III. Cơ chế hoạt động

CMC WAF cung cấp giải pháp bảo vệ liên tục cho website và các ứng dụng sử dụng cơ chế phân tích traffic mạng và chỉ cho phép các yêu cầu truy cập hợp lệ thông qua.



1. Trỏ website, ứng dụng hoặc API tới CMC WAF.
   - Trong giao diện quản lý DNS, trỏ domain tới CMC WAF IP.
   - Gửi IP của website.
   - Hoàn tất.



2. Xem lại các chính sách WAF tiêu chuẩn đang hoạt động theo mặc định.

3. Vô hiệu hóa hoặc tùy chỉnh bất kỳ chính sách tiêu chuẩn.

4. Tạo, tùy chỉnh các quy tắc (rule) của WAF, danh sách trắng (whitelist) và danh sách đen (blacklist) cho IP nếu cần.

❖ ***Quản lý rules C-WAF:***

Các tập luật được sử dụng trên C – WAF sẽ được thống kê tập trung trên giao diện quản trị Websites, người quản trị qua đó có thể biết được:

- Thống kê các loại rules đang có trên C – WAF
- Các bộ rules nào đang được sử dụng trên C – WAF
- Những rules nào Bât/Tắt theo từng Domain/ SubDomain.

❖ ***Update C-WAF:***

Việc update các chức năng, các rules sẽ được thực hiện định kì theo server C – WAF.