

ĐẠI HỌC BÁCH KHOA HÀ NỘI

# ĐỒ ÁN TỐT NGHIỆP

Xây dựng hệ thống quản lý tường lửa dịch vụ Web

TRẦN VĂN NGỌC

ngoc.tv200443@sis.hust.edu.vn

Ngành Kỹ thuật máy tính

Giảng viên hướng dẫn: ThS. Bùi Trọng Tùng

Chữ kí GVHD

Khoa: Kỹ thuật máy tính

Trường: Công nghệ Thông tin và Truyền thông

HÀ NỘI, 06/2024

# LỜI CẢM ƠN

Để hoàn thành đồ án tốt nghiệp này, em đã nhận được sự giúp đỡ và ủng hộ từ rất nhiều người. Em xin gửi lời cảm ơn chân thành và sâu sắc nhất đến gia đình, thầy cô, bạn bè đã đồng hành cùng em trong suốt quá trình thực hiện đồ án này.

Trước hết, em xin bày tỏ lòng biết ơn sâu sắc tới giảng viên hướng dẫn, thầy Bùi Trọng Tùng, người đã tận tình chỉ dẫn, truyền đạt kiến thức và kinh nghiệm quý báu trong suốt quá trình làm đồ án. Sự tận tụy và kiên nhẫn của thầy đã giúp em vượt qua những khó khăn và hoàn thiện đồ án này.

Đồng thời, em xin chân thành cảm ơn các bạn Hiền, Linh, Nam, Vũ, các bạn ở lớp Kỹ thuật máy tính 01 K65, các anh chị em ở câu lạc bộ SINNO và câu lạc bộ BKSec đã đồng hành cùng em trong suốt 4 năm vừa qua. Em xin cảm ơn các anh chị ở Phòng Sản phẩm MASS, công ty An ninh mạng Viettel đã luôn động viên, chia sẻ và hỗ trợ em trong quá trình thực hiện đồ án. Những góp ý và lời khuyên của các bạn và các anh chị đã giúp em hoàn thiện hơn từng chi tiết nhỏ trong đồ án.

Cuối cùng, em xin gửi lời cảm ơn sâu sắc đến gia đình, đặc biệt là cha mẹ, đã luôn là nguồn động viên, cổ vũ và ủng hộ vô điều kiện trong suốt quá trình học tập và nghiên cứu của em. Sự hy sinh và tình yêu thương của gia đình là động lực lớn nhất giúp em vượt qua mọi thử thách và đạt được thành công hôm nay.

Một lần nữa, em xin chân thành cảm ơn tất cả quý thầy cô, bạn bè và gia đình. Hy vọng rằng những kiến thức và kinh nghiệm thu được từ đồ án này sẽ là hành trang quý báu giúp em vững bước trên con đường sự nghiệp sau này.

# LỜI CAM KẾT

Họ và tên sinh viên: Trần Văn Ngọc

MSSV: 20200443

Điện thoại liên lạc: 0333903703

Email: ngoc.tv200443@sis.hust.edu.vn

Lớp: Kỹ thuật máy tính 01 - K65

Chương trình đào tạo: Kỹ thuật máy tính

Tôi – *Trần Văn Ngọc* – cam kết Đồ án Tốt nghiệp (ĐATN) là công trình nghiên cứu của bản thân tôi dưới sự hướng dẫn của *ThS. Bùi Trọng Tùng*. Các kết quả nêu trong ĐATN là trung thực, là thành quả của riêng tôi, không sao chép theo bất kỳ công trình nào khác. Tất cả những tham khảo trong ĐATN – bao gồm hình ảnh, bảng biểu, số liệu, và các câu từ trích dẫn – đều được ghi rõ ràng và đầy đủ nguồn gốc trong danh mục tài liệu tham khảo. Tôi xin hoàn toàn chịu trách nhiệm với dù chỉ một sao chép vi phạm quy chế của nhà trường.

*Hà Nội, ngày      tháng      năm*

Tác giả ĐATN

*Trần Văn Ngọc*

# TÓM TẮT NỘI DUNG ĐỒ ÁN

Trong bối cảnh hiện nay, các cuộc tấn công vào ứng dụng web ngày càng trở nên phổ biến và nguy hiểm hơn. Để đối phó với các mối đe dọa này, nhiều loại tường lửa ứng dụng web (Web Application Firewall - WAF) đã được phát triển và triển khai. Tuy nhiên, một vấn đề nổi lên là rất ít giải pháp hiện tại có thể quản lý tường lửa ứng dụng web một cách tập trung và đồng bộ. Điều này dẫn đến khó khăn trong việc giám sát và điều khiển các tường lửa phân tán, cũng như không đảm bảo tính nhất quán trong việc thực thi các quy tắc bảo mật.

Đồ án này được thực hiện với mục tiêu xây dựng một hệ thống quản lý tường lửa dịch vụ web, nhằm giải quyết những hạn chế trên. Hướng tiếp cận chính là thiết kế một hệ thống quản lý tập trung, giúp quản trị viên có thể dễ dàng giám sát và điều khiển các tường lửa ứng dụng web thông qua một giao diện duy nhất. Hệ thống bao gồm một thành phần quản lý trung tâm (manager), chịu trách nhiệm quản lý và điều khiển các tường lửa thông qua các tác nhân (agent) được triển khai tại các máy chủ web. Thành phần quản lý trung tâm này sẽ duy trì và cập nhật các quy tắc bảo mật, giám sát log và đảm bảo cơ chế giao tiếp bảo mật với các agent.

Kết quả của đồ án cho thấy hệ thống quản lý tường lửa dịch vụ web không chỉ tăng cường hiệu quả quản lý mà còn nâng cao mức độ bảo mật tổng thể cho các ứng dụng web, góp phần bảo vệ hệ thống trước các mối đe dọa ngày càng tinh vi. Hệ thống này mang lại một giải pháp toàn diện và hiệu quả cho việc quản lý và bảo mật các ứng dụng web trong môi trường mạng phức tạp và đầy thách thức hiện nay.

Sinh viên thực hiện  
(Ký và ghi rõ họ tên)

# ABSTRACT

Nowadays, web application attacks are becoming increasingly common and dangerous. Many types of Web Application Firewalls (WAF) have been developed and deployed to counter these threats. However, a prominent issue is that very few existing solutions can manage web application firewalls in a centralized and synchronized manner. This leads to difficulties in monitoring and controlling distributed firewalls, as well as failing to ensure consistency in enforcing security policies.

This thesis aims to address these limitations by developing a web service firewall management system. The main approach is to design a centralized management system that allows administrators to easily monitor and control web application firewalls through a single interface. The system consists of a central management component (manager), which is responsible for managing and controlling firewalls through agents deployed on web servers. This central management component will maintain and update security policies, monitor logs, and ensure secure communication mechanisms with the agents.

The results of this thesis demonstrate that the web service firewall management system not only enhances management efficiency but also improves the overall security level of web applications, helping to protect systems against increasingly sophisticated threats. This system provides a comprehensive and effective solution for managing and securing web applications in today's complex and challenging network environment.

## MỤC LỤC

|  |           |
|--|-----------|
| <b>CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....</b>                            | <b>1</b>  |
| 1.1 Đặt vấn đề.....  | 1         |
| 1.2 Mục tiêu và nhiệm vụ đề tài.....                               | 2         |
| 1.3 Định hướng giải pháp.....                                      | 3         |
| 1.4 Bố cục đồ án .....   | 4         |
| <b>CHƯƠNG 2. KHẢO SÁT VÀ PHÂN TÍCH YÊU CẦU.....</b>                | <b>6</b>  |
| 2.1 Khảo sát hiện trạng .....                                      | 6         |
| 2.2 Tổng quan chức năng .....                                      | 6         |
| 2.2.1 Biểu đồ use case tổng quát .....                             | 7         |
| 2.2.2 Biểu đồ use case chi tiết Quản lý ngân hàng luật .....       | 9         |
| 2.2.3 Biểu đồ use case chi tiết Quản lý domain.....                | 14        |
| 2.2.4 Biểu đồ use case chi tiết Quản lý báo cáo .....              | 20        |
| 2.2.5 Biểu đồ use case chi tiết Giám sát lịch sử sự kiện .....     | 21        |
| 2.2.6 Biểu đồ use case chi tiết Giám sát thống kê .....            | 22        |
| 2.2.7 Biểu đồ use case chi tiết Xác thực và quản lý tài khoản..... | 23        |
| 2.2.8 Biểu đồ use case chi tiết Quản lý người dùng .....           | 24        |
| 2.2.9 Biểu đồ use case chi tiết Quản lý Firewall Agent .....       | 25        |
| 2.3 Yêu cầu phi chức năng .....                                    | 26        |
| <b>CHƯƠNG 3. THIẾT KẾ GIẢI PHÁP .....</b>                          | <b>28</b> |
| 3.1 Thiết kế kiến trúc.....  | 28        |
| 3.1.1 Mô hình tổng thể hệ thống .....                              | 28        |
| 3.1.2 Lựa chọn kiến trúc phần mềm .....                            | 28        |
| 3.1.3 Thiết kế tổng quan.....                                      | 31        |
| 3.1.4 Thiết kế chi tiết gói .....                                  | 33        |

|  |           |
|--|-----------|
| 3.2 Thiết kế chi tiết.....                               | 34        |
| 3.2.1 Thiết kế cơ sở dữ liệu .....                       | 34        |
| 3.3 Thiết kế hoạt động cho chức năng .....               | 40        |
| 3.3.1 Hoạt động Thêm mới luật toàn cục .....             | 40        |
| 3.3.2 Hoạt động Thêm mới tập luật toàn cục .....         | 41        |
| 3.3.3 Hoạt động Thêm mới tập dữ liệu toàn cục .....      | 42        |
| 3.3.4 Hoạt động Thêm mới agent .....                     | 43        |
| 3.3.5 Hoạt động Thêm mới domain .....                    | 44        |
| 3.3.6 Hoạt động Triển khai cấu hình .....                | 45        |
| <b>CHƯƠNG 4. TRIỂN KHAI VÀ THỬ NGHIỆM HỆ THỐNG.....</b>  | <b>46</b> |
| 4.1 Công nghệ sử dụng .....                              | 46        |
| 4.1.1 Tường lửa ứng dụng web .....                       | 46        |
| 4.1.2 ModSecurity.....                                   | 46        |
| 4.1.3 Ngôn ngữ lập trình Python .....                    | 47        |
| 4.1.4 Typescript và React .....                          | 48        |
| 4.2 Mô hình triển khai .....                             | 48        |
| 4.2.1 Thư viện và công cụ sử dụng .....                  | 48        |
| 4.2.2 Triển khai.....                                    | 50        |
| 4.2.3 Kết quả đạt được .....                             | 51        |
| 4.3 Kiểm thử.....  | 53        |
| 4.4 Hình ảnh tiêu biểu .....                             | 59        |
| <b>CHƯƠNG 5. CÁC GIẢI PHÁP VÀ ĐÓNG GÓP NỔI BẬT.....</b>  | <b>65</b> |
| 5.1 Cơ chế giao tiếp bảo mật giữa agent và manager ..... | 65        |
| 5.1.1 Phân tích .....                                    | 65        |
| 5.1.2 Giải pháp .....                                    | 66        |

|   |           |
|---|-----------|
| 5.2 Phân hệ phân phối và quản lý tập luật .....     | 67        |
| 5.2.1 Phân tích vấn đề.....                         | 67        |
| 5.2.2 Hướng giải quyết.....                         | 67        |
| 5.2.3 Tích hợp vào hệ thống .....                   | 68        |
| 5.3 Quản lý log sự kiện tập trung .....             | 68        |
| 5.4 Tối ưu một số luật bảo mật sẵn có.....          | 71        |
| 5.4.1 Luật chống tấn công CVE-2019-8943 .....       | 71        |
| 5.4.2 Luật chống tấn công CVE-2017-5487 .....       | 72        |
| <b>CHƯƠNG 6. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN .....</b> | <b>75</b> |
| 6.1 Kết luận .....                                  | 75        |
| 6.2 Hướng phát triển.....                           | 76        |
| <b>TÀI LIỆU THAM KHẢO.....</b>                      | <b>79</b> |





## DANH MỤC HÌNH VẼ

|           |   |    |
|-----------|---|----|
| Hình 2.1  | Biểu đồ use case tổng quan . . . . .                              | 8  |
| Hình 2.2  | Biểu đồ use case chi tiết Quản lý ngân hàng luật . . . . .        | 9  |
| Hình 2.3  | Biểu đồ use case chi tiết Quản lý luật toàn cục . . . . .         | 10 |
| Hình 2.4  | Biểu đồ use case chi tiết Quản lý tập luật toàn cục . . . . .     | 10 |
| Hình 2.5  | Biểu đồ use case chi tiết Quản lý tập dữ liệu toàn cục . . . . .  | 11 |
| Hình 2.6  | Biểu đồ use case chi tiết Quản lý domain . . . . .                | 14 |
| Hình 2.7  | Biểu đồ use case chi tiết Quản lý báo cáo . . . . .               | 20 |
| Hình 2.8  | Biểu đồ use case chi tiết Giám sát lịch sử sự kiện . . . . .      | 21 |
| Hình 2.9  | Biểu đồ use case chi tiết Giám sát thống kê . . . . .             | 22 |
| Hình 2.10 | Biểu đồ use case chi tiết Xác thực và quản lý tài khoản . . . . . | 23 |
| Hình 2.11 | Biểu đồ use case chi tiết Quản lý người dùng . . . . .            | 24 |
| Hình 2.12 | Biểu đồ use case chi tiết Quản lý Firewall Agent . . . . .        | 25 |
|           |   |    |
| Hình 3.1  | Mô hình tổng thể hệ thống . . . . .                               | 28 |
| Hình 3.2  | Kiến trúc phần mềm . . . . .                                      | 29 |
| Hình 3.3  | Biểu đồ phụ thuộc gói - Phân hệ Firewall Manager . . . . .        | 31 |
| Hình 3.4  | Biểu đồ phụ thuộc gói - Phân hệ Firewall Agent . . . . .          | 32 |
| Hình 3.5  | Thiết kế chi tiết gói module Quản lý domain . . . . .             | 33 |
| Hình 3.6  | Thiết kế cơ sở dữ liệu . . . . .                                  | 34 |
| Hình 3.7  | Biểu đồ hoạt động Thêm mới luật toàn cục . . . . .                | 40 |
| Hình 3.8  | Biểu đồ hoạt động Thêm mới tập luật toàn cục . . . . .            | 41 |
| Hình 3.9  | Biểu đồ hoạt động Thêm mới tập dữ liệu toàn cục . . . . .         | 42 |
| Hình 3.10 | Biểu đồ hoạt động Thêm mới agent . . . . .                        | 43 |
| Hình 3.11 | Biểu đồ hoạt động Thêm mới domain . . . . .                       | 44 |
| Hình 3.12 | Biểu đồ hoạt động Triển khai cấu hình . . . . .                   | 45 |
|           |   |    |
| Hình 4.1  | Mô hình mạng triển khai thử nghiệm . . . . .                      | 50 |
| Hình 4.2  | Kết quả đánh giá SonarQube của thành phần Backend . . . . .       | 51 |
| Hình 4.3  | Kết quả đánh giá SonarQube của thành phần Frontend . . . . .      | 52 |
| Hình 4.4  | Kết quả đánh giá SonarQube của thành phần Agent . . . . .         | 52 |
| Hình 4.5  | Giao diện quản lý luật . . . . .                                  | 59 |
| Hình 4.6  | Giao diện Thêm luật . . . . .                                     | 59 |
| Hình 4.7  | Giao diện quản lý tập luật . . . . .                              | 60 |
| Hình 4.8  | Giao diện Thêm tập luật . . . . .                                 | 60 |
| Hình 4.9  | Giao diện quản lý tập dữ liệu . . . . .                           | 61 |
| Hình 4.10 | Giao diện quản lý domain . . . . .                                | 61 |