HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Đỗ Hoàng Giang

XÂY DỰNG MÔ HÌNH QUẢN LÝ XÁC THỰC VÀ QUYỀN TRUY CẬP HỆ THỐNG DỰA TRÊN ZERO TRUST

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

TÓM TẮT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

HÀ NỘI - 2024

Đề án tốt nghiệp được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học : ……

(Ghi rõ học hàm, học vị)

Phản biện 1: ……

Phản biện 2: ……..

Đề án tốt nghiệp sẽ được bảo vệ trước Hội đồng chấm đề án tốt nghiệp thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu đề án tốt nghiệp tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

Mở đầu

Trong xu hướng chuyển đổi số hiện nay, an toàn thông tin đã trở thành một vấn đề cực kỳ quan trọng đối với các doanh nghiệp. Với sự phát triển nhanh chóng của công nghệ thông tin và viễn thông, mối đe dọa về mất an toàn thông tin và tấn công mạng ngày càng trở nên phức tạp và tinh vi hơn bao giờ hết.

Các doanh nghiệp, bất kể quy mô, đều phải đối mặt với nguy cơ mất an toàn thông tin. Các cuộc tấn công mạng có thể gây ra những hậu quả nghiêm trọng về tài chính, dữ liệu và uy tín của doanh nghiệp. Việc mất cắp thông tin quan trọng, xâm nhập vào cơ sở dữ liệu và lợi dụng thông tin cá nhân của khách hàng có thể gây tổn thất về tiền bạc, giảm đáng kể lòng tin của khách hàng và ảnh hưởng đến hình ảnh và danh tiếng của doanh nghiệp. Do đó việc xây dựng mô hình quản lý xác thực và quyền truy cập hệ thống an toàn là một vấn đề cực kỳ quan trọng đối với các doanh nghiệp. Trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi và mối đe dọa an ninh đang ngày một gia tăng, việc áp dụng mô hình Zero Trust đã trở thành một hướng đi được đánh giá cao trong việc bảo vệ thông tin và hệ thống của doanh nghiệp.

Mô hình Zero Trust là một mô hình bảo mật dựa trên nguyên tắc không tin tưởng bất kỳ ai hoặc bất kỳ thứ gì bên ngoài mạng nội bộ của doanh nghiệp. Mô hình này cho phép doanh nghiệp kiểm soát chặt chẽ việc truy cập vào hệ thống thông tin, ngay cả khi người dùng hoặc thiết bị đó đã được xác thực.

Việc kết hợp mô hình Zero Trust có thể giúp doanh nghiệp nâng cao hiệu quả bảo mật hệ thống thông tin, chống lại các mối đe dọa mạng ngày càng tinh vi.

Cụ thể, mô hình này có những ưu điểm sau:

- Tăng cường tính bảo mật: Mô hình này xây dựng trên nguyên tắc không tin tưởng bất cứ ai hoặc bất cứ thứ gì, ngay cả khi nằm trong mạng nội bộ của doanh nghiệp. Điều này giúp tăng cường bảo mật bằng cách yêu cầu xác thực liên tục và kiểm soát chặt chẽ việc truy cập.
- Phù hợp cho mọi quy mô doanh nghiệp : Mô hình Zero Trust có thể được triển khai linh hoạt và phù hợp với mọi quy mô doanh nghiệp. Điều này giúp bảo vệ thông tin quan trọng và tài sản kinh doanh ở mức độ cao nhất..
- Giảm thiểu nguy cơ tấn công mạng: Mô hình này cung cấp khả năng kiểm soát tuyệt vời đối với quyền truy cập vào hệ thống thông tin. Ngay cả khi đã xác thực, người dùng và thiết bị cũng sẽ phải trải qua quá trình xác minh liên tục, giảm thiểu nguy cơ tấn công mạng.
- Quản lý truy cập linh hoạt: Zero Trust cho phép doanh nghiệp thiết lập các chính sách truy cập linh hoạt dựa trên vai trò, chức năng và mức độ tin cậy của người dùng.

Vì những lý do trên, đề tài "Xây dựng mô hình quản lý xác thực và quyền truy cập hệ thống cho doanh nghiệp dựa trên Zero Trust" là một đề tài có tính thực tiễn và khả thi cao. Đề tài này có thể giúp doanh nghiệp nâng cao hiệu quả bảo mật hệ thống thông tin, góp phần bảo vệ tài sản và thông tin quan trọng của doanh nghiệp.

Tổng quan về vấn đề nghiên cứu

Theo báo cáo của Bộ Công an, trong năm 2022, doanh nghiệp đã bị tấn công mạng với tần suất tăng cao. Các cuộc tấn công này chủ yếu nhắm vào các hệ thống thông tin quan trọng của doanh nghiệp, như hệ thống tài chính, hệ thống quản lý sản xuất, hệ thống bán hàng,...

Các cuộc tấn công mạng có thể gây ra những thiệt hại nghiêm trọng cho doanh nghiệp, bao gồm:

- Tổn thất tài chính: Các cuộc tấn công mạng có thể dẫn đến việc mất dữ liệu, mất tiền, hoặc gián đoạn kinh doanh.
- Tổn hại uy tín: Các cuộc tấn công mạng có thể làm tổn hại uy tín của doanh nghiệp, khiến doanh nghiệp mất khách hàng và đối tác.
- Rủi ro pháp lý: Các cuộc tấn công mạng có thể dẫn đến các rủi ro pháp lý cho doanh nghiệp, chẳng hạn như trách nhiệm bồi thường thiệt hại.

Đề án này đề xuất việc kết hợp mô hình Zero Trust có thể giúp doanh nghiệp nâng cao hiệu quả bảo mật hệ thống thông tin, chống lại các mối đe dọa mạng ngày càng tinh vi.

Bố cục của luận văn

Nội dung của luận văn sẽ được chia làm 4 chương với cấu trúc từng chương như sau:

Chương 1: Tổng quan về xác thực và quyền truy cập hệ thống

Chương này sẽ trình bày về khái niệm và tầm quan trọng của xác thực và quyền truy cập, phân loại cũng như chỉ ra các ưu, nhược điểm riêng của từng phương pháp.

Chương 2: Tìm hiểu Zero Trust

Chương này sẽ tìm hiểu tổng quan về mô hình Zero Trust, một số hệ thống đã áp dụng mô hình Zero Trust ở trong và ngoài nước, ngoài ra so sánh chúng với mô hình xác thực truyền thống.

Chương 3: Mô hình quản lý xác thực và quyền truy cập dựa trên Zero Trust

Chương này nói về hệ thống do tôi xây dựng dựa trên mô hình Zero Trust, từ thiết kế kiến trúc tổng quan, các công nghệ sử dụng và so sánh nó với các mô hình hiện có.

Chương 4: Triển khai và thử nghiệm mô hình

Chương này nói về phần triển khai và thử nghiệm mô hình, đặt ra các kịch bản có thể xảy ra để kiểm tra độ bảo mật của hệ thống được xây dựng.

CHƯƠNG 1: TỔNG QUAN VỀ XÁC THỰC VÀ QUYỀN TRUY CẬP HỆ THỐNG

1.1. Khái niệm và tầm quan trọng của xác thực và quyền truy cập

1.1.1. Khái niệm và tầm quan trọng của Authentication (xác thực)

Khái niệm:

Xác thực là một dịch vụ bảo mật quan trọng, với quy trình phổ biến nhất là xác minh tên người dùng và mật khẩu, đó là quá trình xác định "người dùng là ai ?" [1]. Trong bối cảnh mạng, điều này thường liên quan đến việc cung cấp và xác minh thông tin đăng nhập như mật khẩu, mã OTP, hoặc các hình thức xác thực sinh trắc học.

Yếu tố xác thực là một loại thông tin được sử dụng để xác minh danh tính của người dùng [2]. Các yếu tố xác thực chính:

- Điều người dùng biết (yếu tố kiến thức) : Đây là yếu tố xác thực phổ biến nhất. Nó xác minh danh tính bằng cách xác nhận người dùng thông qua những thông tin bí mật mà chỉ họ biết, chẳng hạn như thông tin đăng nhập và mật khẩu.
- Thứ người dùng có (yếu tố sở hữu) *:* Người dùng xác minh danh tính của họ bằng một vật thể duy nhất như thẻ truy cập hoặc chìa khóa điện tử, điện thoại di động.
- Đặc điểm cá nhân của người dùng (yếu tố vốn có) : Yếu tố vốn có xác minh danh tính thông qua các đặc điểm sinh trắc học vốn có của người dùng – chẳng hạn như mẫu vân tay, giọng nói hoặc mống mắt.

Tầm quan trọng:

Việc xác thực đóng vai trò quan trọng trong việc ngăn chặn truy cập trái phép và bảo vệ tài nguyên từ các mối đe dọa tiềm tàng. Quá trình xác thực cung cấp một lớp bảo vệ đầu tiên trong bất kỳ hệ thống bảo mật nào, giúp ngăn chặn nguy cơ từ những kẻ tấn công giả danh người dùng hợp pháp.

1.1.2. Khái niệm và tầm quan trọng của Authorization (quyền truy cập)

Khái niệm:

Quyền truy cập, hay còn gọi là phân quyền, là quá trình quyết định xem một người dùng đã xác thực có được phép thực hiện các hoạt động cụ thể trên hệ thống hay không. Quy trình này thường dựa vào các chính sách và quy tắc đã định trước để cấp hoặc từ chối quyền truy cập vào tài nguyên.

Tầm quan trọng:

Phân quyền giúp đảm bảo rằng người dùng chỉ có quyền truy cập vào tài nguyên cần thiết để thực hiện công việc của họ. Điều này không chỉ giúp bảo mật thông tin nhạy cảm mà còn đảm bảo rằng hệ thống và dữ liệu không bị lạm dụng. Quá trình phân quyền cũng giúp các tổ chức tuân thủ các quy định về bảo mật và quyền riêng tư.

Tóm lại, xác thực và phân quyền là hai yếu tố cơ bản và thiết yếu của an ninh mạng, giúp đảm bảo rằng chỉ những người dùng đáng tin cậy mới có quyền truy cập vào hệ thống và tài nguyên. Sự hiểu biết sâu sắc về hai khái niệm này là bước đầu tiên quan trọng trong việc xây dựng và duy trì một hệ thống an toàn và bảo mật.

1.2 Phân loại các phương pháp xác thực

1.2.1 Xác thực truyền thống (Sử dụng username và password)

Xác thực truyền thống yêu cầu người dùng cung cấp một cặp thông tin đăng nhập gồm username và password để truy cập vào hệ thống hoặc tài khoản cá nhân.

1.2.2. Xác thực đa yếu tố (MFA – Multi-Factor Authentication)

Xác thực đa yếu tố (MFA) là một phương thức xác thực yêu cầu người dùng cung cấp hai hoặc nhiều yếu tố xác thực để được xác minh danh tính. Các yếu tố xác thực này có thể bao gồm:

- Kiến thức: Mật khẩu, câu hỏi bí mật, mã PIN, …
- Sở hữu: Thẻ thông minh, điện thoại di động, thiết bị đeo tay, …
- Đặc điểm cá nhân: Dấu vân tay, khuôn mặt, mống mắt, …

1.2.3 Xác thực đăng nhập một lần (Single Sign-On Authentication)

Xác thực đăng nhập một lần (SSO) cho phép người dùng đăng nhập và truy cập nhiều tài khoản cũng như ứng dụng chỉ bằng một bộ thông tin xác thực. Điều này phổ biến nhất trong thực tế với các tài khoản Facebook hoặc Google. Ví dụ khi bạn đăng nhập một ứng dụng chơi game, hệ thống sẽ cho phép bạn lựa chọn đăng nhập bằng tài khoản Facebook hoặc Google. SSO đơn giản hóa việc quản lý tên đăng nhập và mật khẩu, giúp đăng nhập nhanh hơn và dễ dàng hơn.

1.2.4 Sinh trắc học

Xác thực dựa trên sinh trắc học là một phương pháp xác thực danh tính dựa trên việc sử dụng các đặc điểm duy nhất và không thể sao chép từ cơ thể con người. Các đặc điểm này có thể bao gồm vân tay, mống mắt, khuôn mặt, hoặc các đặc điểm sinh trắc học khác. Phương pháp này đang trở thành một trong những giải pháp quan trọng trong lĩnh vực bảo mật và xác thực do sự độc đáo và khó nhằn của các đặc điểm sinh trắc học.

1.2.5 Session-Cookies

Với xác thực dựa trên session-cookies, trạng thái của người dùng sẽ được lưu trên máy chủ. Tức là nó không yêu cầu username hay password sau mỗi lần request mà thay vào đó, sau lần đăng nhập hợp lệ đầu tiên, nó sẽ tạo sessionId cho người dùng. Và gửi nó cho client, phía client cụ thể là browser sẽ lưu sessionId vào trong cookies. Như vậy mỗi là cần có yêu cầu đến server nó chỉ cần gửi theo sessionId.

1.2.6 Token

JSON Web Mã (JWT) là một chuẩn mở (RFC 7519) định nghĩa một cách nhỏ gọn và khép kín để truyền một cách an toàn thông tin giữa các bên dưới dạng đối tượng JSON. Thông tin này có thể được xác minh và đáng tin cậy vì nó có chứa chữ ký số. JWTs có thể được ký bằng một thuật toán bí mật (với thuật toán HMAC) hoặc một public/private key sử dụng mã hoá RSA.

Phương pháp này thay vì sử dụng cookie thì ở đây ta sẽ dùng token. Người dùng sẽ gửi thông tin đăng nhập hợp lệ và server sẽ trả về một token. Token này sẽ được dùng cho các yêu cầu xác thực tiếp theo. Phần lớn token được sử dụng hiện tại đều là Jsonwebtoken(JWT).

1.2.7 Mật khẩu một lần (OTP – One-Time Password)

OTP (One Time Password) nghĩa là mật khẩu sử dụng một lần. Đây là một dãy các ký tự hoặc chữ số ngẫu nhiên được gửi đến điện thoại của bạn để xác nhận bổ sung khi thực hiện

giao dịch, thanh toán qua Internet. Mỗi mã OTP chỉ có thể sử dụng một lần và sẽ mất hiệu lực trong vài phút.

One Time Password (OTP) còn gọi là mật khẩu sử dụng một lần thường được dùng để xác nhận cho việc xác thực danh tính người dùng. OTP là những mã được tạo ngẫu nhiên có thể được sử dụng để xác thực người dùng dựa trên một hệ thống đáng tin cậy. Hệ thống đó có thể là email hoặc số điện thoại đã xác minh.

1.3. Thách thức trong quản lý xác thực và quyền truy cập

Quản lý xác thực và quyền truy cập là một quá trình phức tạp và đầy thách thức. Các tổ chức phải đối mặt với nhiều thách thức trong việc quản lý hiệu quả xác thực và quyền truy cập, bao gồm :

- Đa dạng và phức tạp của các hệ thống và ứng dụng
- Yêu cầu bảo mật liên tục thay đổi
- Tăng trưởng của danh tính số và quản lý truy cập
- Thiếu hụt kỹ năng và nguồn lực
- Các vấn đề về quyền riêng tư và tuân thủ

1.4. Kết luận chương 1

Chương này đã cung cấp cái nhìn toàn diện về hai yếu tố quan trọng trong bảo mật thông tin: xác thực và ủy quyền. Các phương pháp xác thực từ truyền thống đến hiện đại như mật khẩu và sinh trắc học đã được thảo luận, mỗi phương pháp đều có ưu điểm và hạn chế riêng, yêu cầu lựa chọn cẩn thận để đảm bảo an toàn.

Ủy quyền xác định quyền truy cập mà một người dùng được phép sau khi xác thực, với thách thức là cân bằng giữa cấp quyền cần thiết cho hiệu quả công việc và hạn chế quyền để giảm thiểu rủi ro an ninh. Việc quản lý hiệu quả các chiến lược như tối thiểu hóa quyền truy cập và phân quyền dựa trên vai trò là chìa khóa để bảo vệ thông tin.

Những nỗ lực trong việc xây dựng và duy trì các hệ thống xác thực và ủy quyền không chỉ giúp bảo vệ thông tin mà còn là yếu tố quan trọng cho sự phát triển của các hệ thống thông tin trong tương lai. Chương này không chỉ làm sáng tỏ các khái niệm lý thuyết mà còn đề cập đến các hướng tiếp cận thực tiễn trong việc đối mặt với các thách thức an ninh trong thế giới kỹ thuật số hiện đại.

CHƯƠNG 2: TÌM HIỂU ZERO TRUST

2.1. Tổng quan về Zero Trust

Mô hình Zero Trust đã trở thành một tiêu chuẩn vàng trong việc đảm bảo an ninh mạng, áp dụng nguyên tắc "không bao giờ tin tưởng, luôn xác minh" trong mọi hoạt động của hệ thống. Nguyên tắc này yêu cầu mọi yêu cầu truy cập, bất kể từ nội bộ hay bên ngoài, đều phải được xác thực và ủy quyền một cách nghiêm ngặt trước khi được cấp quyền truy cập vào tài nguyên. Điều này đảm bảo rằng chỉ những người dùng và thiết bị được xác thực mới có thể truy cập vào dữ liệu và ứng dụng quan trọng, giúp ngăn chặn các cuộc tấn công từ bên trong lẫn bên ngoài tổ chức.

Các thành phần logic của Zero Trust bao gồm các công nghệ như tường lửa thế hệ mới (NGFW), hệ thống ngăn chặn xâm nhập (IPS), và các giải pháp quản lý danh tính và quyền truy cập (IAM) [3]. Những công nghệ này cùng nhau tạo nên một hệ thống bảo mật đa tầng, trong đó mỗi lớp đều có chức năng bảo vệ và phát hiện các mối đe dọa, đồng thời quản lý và kiểm soát lưu lượng truy cập vào hệ thống.

Triển khai mô hình Zero Trust đòi hỏi sự thay đổi đáng kể về cách thức tổ chức triển khai và quản lý an ninh mạng. Tổ chức cần xác định các tài nguyên quan trọng và áp dụng các chính sách truy cập dựa trên ngữ cảnh cụ thể của người dùng và thiết bị. Điều này đòi hỏi một nền tảng công nghệ mạnh mẽ để hỗ trợ việc đánh giá và thực thi chính sách một cách liên tục.

Mặc dù có nhiều lợi ích, việc áp dụng Zero Trust cũng gặp phải không ít thách thức, bao gồm độ phức tạp trong triển khai, chi phí cao ban đầu, và sự cần thiết phải thay đổi văn hóa và quy trình làm việc trong tổ chức. Các tổ chức cần phải cân nhắc kỹ lưỡng các yếu tố này để đảm bảo rằng việc triển khai mô hình Zero Trust có thể đạt được kết quả mong muốn mà không ảnh hưởng đến hoạt động kinh doanh.

Trên toàn cầu, mô hình Zero Trust đã được nhiều tổ chức lớn và các chính phủ áp dụng để bảo vệ thông tin và hạ tầng mạng của họ khỏi các mối đe dọa ngày càng tinh vi. Ví dụ như Google với mô hình BeyondCorp, đã chứng minh được hiệu quả của Zero Trust trong việc cung cấp một môi trường làm việc an toàn và linh hoạt cho người dùng không kể vị trí địa lý. Sự áp dụng rộng rãi của Zero Trust cho thấy nó không chỉ là một xu hướng bảo mật mà còn là một phần không thể thiếu trong chiến lược an ninh mạng hiện đại.

2.2. Phân quyền quản lý trong Zero Trust

Trong mô hình Zero Trust, phân quyền quản lý là một yếu tố trọng tâm, đảm bảo rằng quyền truy cập được cấp một cách minh bạch và an toàn. Mô hình này tập trung vào việc xác thực và ủy quyền dựa trên ngữ cảnh và rủi ro liên quan đến mỗi yêu cầu truy cập, không chỉ dựa vào vị trí mạng hay vai trò cố định của người dùng.

Phân quyền trong Zero Trust được thực hiện qua nhiều phương thức khác nhau, bao gồm phân quyền dựa trên danh tính (Identity-Based Access Control - IBAC), vai trò (Role-Based Access Control - RBAC), thuộc tính (Attribute-Based Access Control - ABAC), rủi ro (Risk-Based Access Control - RbAC), và mới đây là dựa trên công nghệ blockchain (Blockchain-Based Access Control - BAC). Mỗi phương thức có những ưu điểm riêng biệt nhưng đều chung nguyên tắc là tăng cường bảo mật bằng cách giới hạn quyền truy cập dựa trên nhu cầu thực tế và mức độ rủi ro.

IBAC tập trung vào việc xác thực người dùng hoặc thiết bị dựa trên danh tính, đồng thời theo dõi và kiểm soát hành vi truy cập một cách liên tục. Điều này cho phép phát hiện và ngăn chặn các hành vi truy cập bất thường, từ đó nâng cao độ an toàn của mạng.

RBAC lại phân loại quyền truy cập dựa trên vai trò cụ thể của người dùng trong tổ chức, đơn giản hóa quản lý bảo mật bằng cách phân quyền dựa trên nhóm nghề nghiệp, từ đó tự động hóa việc cấp quyền và giảm thiểu rủi ro truy cập không đúng cách.

ABAC mang đến sự linh hoạt cao hơn bằng cách sử dụng các thuộc tính động của người dùng, thiết bị và ngữ cảnh hoạt động để đưa ra quyết định về quyền truy cập. Điều này cho phép điều chỉnh chính sách truy cập một cách tinh tế và phản ánh chính xác hơn các nhu cầu an ninh và kinh doanh.

RbAC nâng cao khả năng bảo mật bằng cách hạn chế quyền truy cập trong các tình huống có nguy cơ cao và cho phép truy cập khi rủi ro là thấp, phản ứng linh hoạt với các thay đổi trong môi trường an ninh.

Cuối cùng, BAC sử dụng công nghệ blockchain để lưu trữ và quản lý các thông tin liên quan đến quyền truy cập, mang lại một cấp độ bảo mật cao và khả năng chống giả mạo cho quyền truy cập, đồng thời tăng cường độ tin cậy và tính minh bạch trong việc quản lý quyền truy cập.

2.3. Xác thực trong Zero Trust

Trong mô hình Zero Trust, xác thực đóng một vai trò trung tâm trong việc kiểm soát và bảo mật truy cập. Khác biệt cơ bản với các phương pháp truyền thống, xác thực trong Zero Trust không chỉ dựa trên mật khẩu mà còn áp dụng xác thực đa yếu tố (MFA), xác thực liên tục và xác thực ngữ cảnh để đảm bảo an toàn thông tin.

Các cơ chế xác thực truyền thống như mật khẩu đã được thừa nhận là không còn đủ an toàn do các vấn đề như sử dụng lại mật khẩu và tấn công kênh phụ. Trong khi đó, mô hình Zero Trust đòi hỏi việc xác thực phải được thực hiện liên tục và dựa trên nhiều yếu tố, không chỉ giới hạn ở mật khẩu mà còn bao gồm sinh trắc học, mã OTP, và các chứng chỉ kỹ thuật số, đảm bảo rằng chỉ những người dùng và thiết bị được ủy quyền mới có thể truy cập vào tài nguyên hệ thống.

Xác thực ngữ cảnh trong Zero Trust được xem là cách tiếp cận mang tính cách mạng, cho phép hệ thống phân tích và đánh giá ngữ cảnh truy cập của một yêu cầu, bao gồm thời gian, địa điểm, thiết bị truy cập và hành vi truy cập của người dùng. Cách tiếp cận này không chỉ tăng cường bảo mật mà còn đảm bảo rằng hệ thống có thể thích ứng với các thay đổi trong môi trường bảo mật và người dùng.

Hơn nữa, xác thực thiết bị trong Zero Trust đòi hỏi việc kiểm tra các yếu tố như địa chỉ IP và MAC của thiết bị truy cập, đảm bảo rằng chỉ các thiết bị đã được xác thực mới được cấp phép. Cách tiếp cận này nhằm ngăn chặn các mối đe dọa từ thiết bị không được ủy quyền, từ đó tăng cường tính an toàn và bảo mật cho hệ thống.

Cuối cùng, xác thực liên tục là một phần không thể thiếu trong mô hình Zero Trust, nơi mà quá trình xác thực không chỉ diễn ra một lần mà là một quá trình liên tục trong suốt phiên truy cập. Điều này giúp phát hiện và phản ứng kịp thời trước các hành vi bất thường, từ đó giảm thiểu nguy cơ và tăng cường bảo mật cho hệ thống thông tin.

Tóm lại, xác thực trong Zero Trust không chỉ là một quy trình đơn lẻ mà là một hệ thống đa tầng, liên tục và đáp ứng, tạo nên một hàng rào bảo vệ chắc chắn, thông minh và linh hoạt để đối phó với các mối đe dọa ngày càng tinh vi trong môi trường kỹ thuật số hiện đại.

2.4. Kết luận chương 2

Trong chương này, chúng ta đã khám phá chiều sâu của mô hình Zero Trust trong bảo mật mạng, từ nguyên tắc hoạt động, các thành phần logic, đến việc triển khai và ứng dụng mô hình trong thực tế. Mô hình Zero Trust, với nguyên tắc "không tin tưởng mặc định", thách thức các giả định truyền thống về an ninh mạng, đồng thời nâng cao khả năng bảo vệ thông tin trong bối cảnh mối đe dọa mạng ngày càng phức tạp.

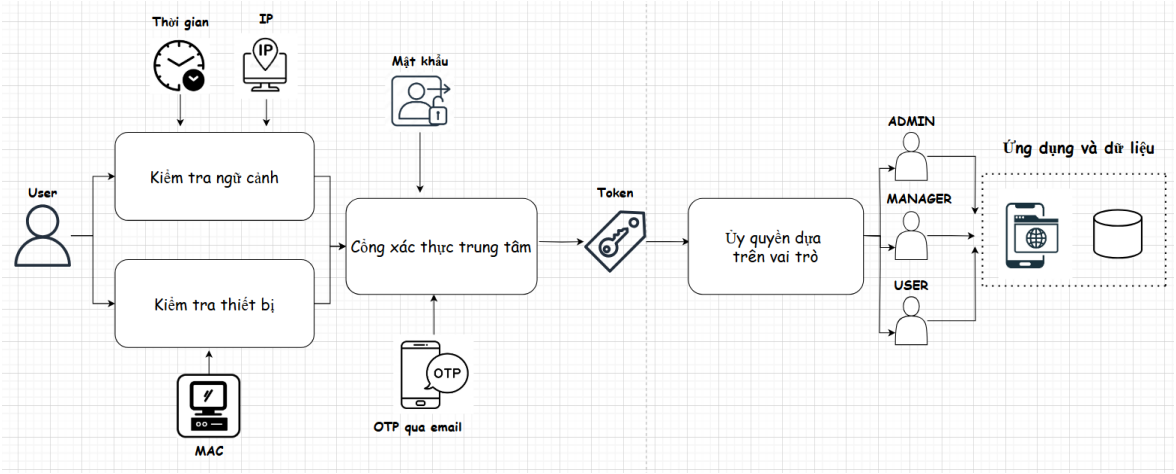
Chúng ta cũng đã xem xét cách thức mà Zero Trust thay đổi cách tiếp cận an ninh từ việc tập trung vào biên giới mạng sang việc bảo vệ từng phân đoạn và tài nguyên cụ thể.

Chương này cũng nhấn mạnh rằng việc áp dụng mô hình Zero Trust đòi hỏi sự thay đổi chiến lược toàn diện, từ cách thức quản lý và xác thực người dùng, thiết bị, cho đến phương pháp quản lý và giám sát dữ liệu. Các thách thức như chi phí triển khai, khả năng tương thích hệ thống và quản lý phức tạp cũng được đề cập, cùng với việc giải quyết những thách thức này để tận dụng tối đa lợi ích của Zero Trust.

CHƯƠNG 3: MÔ HÌNH QUẢN LÝ XÁC THỰC VÀ QUYỀN TRUY CẬP DỰA TRÊN ZERO TRUST

3.1. Thiết kế kiến trúc tổng quan của mô hình

Chương này tập trung vào việc trình bày về cách thức xây dựng và triển khai một mô hình quản lý xác thực và quyền truy cập dựa trên Zero Trust, tập trung vào kiến trúc tổng quan, quy trình xác thực đa yếu tố và ủy quyền dựa trên vai trò. Kiến trúc tổng quan của mô hình như hình 3.1 :



Hình 3.1 Kiến trúc tổng quan của mô hình

Cổng xác thực trung tâm

Bước đầu tiên trong quy trình xác thực là cổng đăng nhập, nơi người dùng nhập mật khẩu của họ. Cổng xác thực trung tâm đóng vai trò như điểm kiểm soát truy cập đầu tiên trong hệ thống. Cổng xác thực trung tâm chịu trách nhiệm xác thực danh tính người dùng thông qua mật khẩu và OTP, đồng thời thực hiện các kiểm tra ngữ cảnh truy cập như thời gian và thông tin thiết bị. Điều này đảm bảo rằng chỉ có những yêu cầu hợp lệ mới được tiếp tục quy trình xác thực.

Dịch vụ xác thực đa yếu tố

Sau khi mật khẩu được xác nhận, một mã OTP (One-Time Password) được gửi đến email của người dùng, yêu cầu họ nhập mã này để hoàn tất quá trình xác thực. Việc sử dụng OTP là một phần của xác thực đa yếu tố (MFA), giúp tăng cường bảo mật bằng cách thêm một lớp xác thực nữa.

Kiểm Tra Điều Kiện Truy Cập

Trước khi cho phép truy cập, hệ thống kiểm tra các điều kiện như khoảng thời gian hợp lệ (8h đến 17h), địa chỉ IP, và địa chỉ MAC của thiết bị. Điều này đảm bảo rằng truy cập chỉ được cấp trong giờ làm việc và từ các thiết bị được phép, tăng cường bảo mật thông tin.

Token Truy Cập

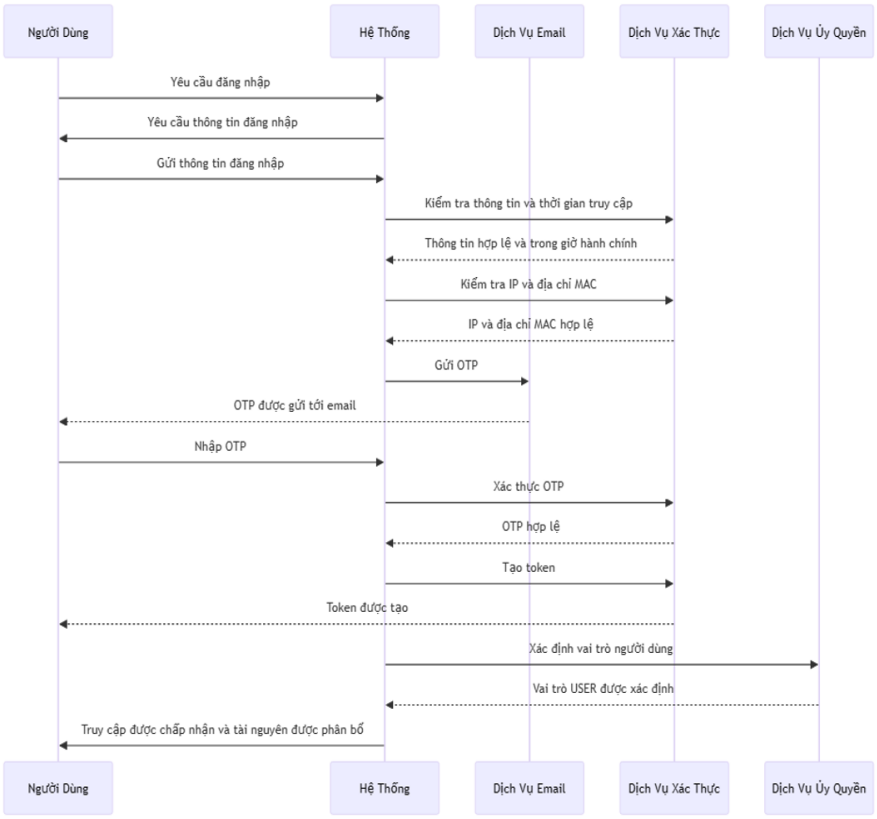
Khi người dùng xác thực thành công, một token truy cập được tạo ra. Token này cần được kèm theo mỗi request trong hệ thống để xác thực danh tính và quyền truy cập của người dùng. Token giúp quản lý truy cập và đảm bảo rằng chỉ những người dùng xác thực mới có thể truy cập vào tài nguyên.

Ủy quyền và kiểm soát truy cập

Sau khi mã OTP được xác nhận và đảm bảo người dùng truy cập hệ thống trong điều kiện đã được chấp thuận, hệ thống sẽ tiến hành bước ủy quyền quan trọng. Mỗi người dùng,

tùy thuộc vào vai trò của họ trong tổ chức, sẽ được cấp một token truy cập có chứa dữ liệu phân quyền chi tiết, phản ánh quyền truy cập hành động của họ đối với tài nguyên hệ thống.

Biểu đồ tuần tự người dùng truy cập hệ thống được mô tả trong hình 3.2.



Hình 3.2 Biểu đồ tuần tự người dùng truy cập hệ thống

Luồng hoạt động :

Người dùng gửi thông tin đăng nhập, sau đó hệ thống sẽ kiểm tra thông tin này cùng với thời gian truy cập. Địa chỉ IP và địa chỉ MAC của người dùng được kiểm tra để xác nhận tính hợp lệ của yêu cầu. Tiếp theo, nếu thông tin mật khẩu nhập là chính xác, một mã OTP (One-Time Password) được gửi đến email của người dùng thông qua dịch vụ email để xác nhận thêm một lớp bảo mật. Người dùng sau đó nhập mã OTP này vào hệ thống. Nếu OTP hợp lệ, quy trình sẽ tiếp tục với việc tạo token truy cập, qua đó cấp quyền truy cập cho người dùng vào các tài nguyên được phân bổ.

Sau khi xác thực thành công, hệ thống tiến hành xác định vai trò của người dùng, đây là bước quan trọng tiếp theo. Vai trò người dùng, như User, Manager hay Admin, quyết định mức độ quyền truy cập và khả năng quản lý tài nguyên hệ thống. Người dùng bình thường sau khi đăng nhập chỉ có thể xem thông tin của chính họ. Quản lý có thể xem thông tin chi tiết của tất cả nhân viên thuộc phòng ban do họ quản lý. Quản trị viên, có vai trò quan trọng hơn, sau khi được xác thực sẽ có khả năng thực hiện các thao tác quản lý như thêm, sửa, xóa thông tin người dùng trong hệ thống (biểu đồ tuần tự cho ADMIN được miêu tả trong toàn văn).

Quá trình phân quyền cho phép hệ thống đảm bảo rằng mỗi người dùng chỉ có quyền truy cập vào các tài nguyên phù hợp với vai trò và trách nhiệm của họ. Điều này không chỉ

tăng cường bảo mật thông tin mà còn tối ưu hóa quản lý nguồn lực, đảm bảo hoạt động hiệu quả và linh hoạt của hệ thống thông tin.

3.2. Xác thực người dùng và thiết bị

Xác thực người dùng và thiết bị là bước đầu tiên và cơ bản nhất trong việc bảo vệ thông tin và tài nguyên hệ thống, đảm bảo rằng chỉ những cá nhân và thiết bị được ủy quyền mới có thể truy cập vào hệ thống, qua đó ngăn chặn hiệu quả các nguy cơ từ việc truy cập trái phép.

Trong mô hình này, xác thực không chỉ dừng lại ở người dùng mà còn bao gồm cả thiết bị, sử dụng các biện pháp như kiểm tra địa chỉ IP và địa chỉ MAC để xác nhận tính hợp lệ của thiết bị trước khi cho phép truy cập. Ngoài ra, mô hình còn tích hợp việc kiểm tra ngữ cảnh truy cập, như xác định thời gian truy cập phù hợp (trong giờ làm việc chính thức) và từ các địa điểm được coi là an toàn, tăng cường khả năng an ninh bằng cách đảm bảo rằng mọi yêu cầu truy cập đều phù hợp với chính sách an ninh của tổ chức.

Việc xác thực người dùng bắt đầu bằng mật khẩu, sau đó tiếp tục với xác thực đa yếu tố (MFA) thông qua mã OTP được gửi đến email của người dùng, tăng cường lớp bảo mật thứ hai. Sau khi xác thực thành công, hệ thống sẽ tạo ra một token truy cập cho người dùng, điều này giúp duy trì phiên làm việc an toàn và kiểm soát quyền truy cập hiệu quả. Tổng thể, phần này thể hiện sự nghiêm ngặt và tinh vi của quy trình xác thực trong mô hình Zero Trust, phản ánh nguyên tắc cốt lõi của mô hình này là "không bao giờ tin tưởng, luôn luôn xác minh".

3.3. Quản lý quyền truy cập dựa trên vai trò

Quản lý quyền truy cập dựa trên vai trò trong mô hình Zero Trust, nhấn mạnh vào tầm quan trọng của việc quản lý hiệu quả quyền truy cập trong bối cảnh an ninh thông tin ngày càng phức tạp. Việc áp dụng quản lý quyền truy cập dựa trên vai trò (RBAC - Role-Based Access Control) giúp đơn giản hóa việc phân quyền và tăng cường an ninh bằng cách chỉ cho phép người dùng truy cập vào những tài nguyên cần thiết cho công việc của họ.

Trong mô hình này, RBAC giảm bớt sự phức tạp trong quản lý quyền truy cập bằng cách phân loại quyền theo vai trò, thay vì gán quyền truy cập cho từng cá nhân, giảm thiểu rủi ro an ninh thông tin do sai sót trong quản lý quyền truy cập và hỗ trợ việc tuân thủ chính sách bảo mật một cách hiệu quả.

RBAC trong hệ thống được triển khai bằng cách xác định các vai trò khác nhau từ người dùng cơ bản đến quản lý, quản trị viên hệ thống, mỗi vai trò được gán với một tập hợp quyền truy cập đến tài nguyên và dịch vụ tùy thuộc vào nhu cầu thực tế và mức độ an ninh yêu cầu. Điều này giúp đảm bảo rằng mỗi người dùng chỉ có quyền truy cập vào tài nguyên cần thiết cho công việc của họ, từ đó tăng cường tính bảo mật và giảm thiểu rủi ro truy cập không phù hợp.

3.4. So sánh với các mô hình xác thực và ủy quyền hiện có

Phần này thực hiện so sánh hệ thống Zero Trust được phát triển với các mô hình xác thực và ủy quyền hiện có như VNIS, Google (BeyondCorp), và Microsoft. Đánh giá này làm nổi bật các khác biệt cơ bản và tiềm năng cải thiện dựa trên cách tiếp cận Zero Trust.

VNIS áp dụng các phương pháp quản lý danh tính truyền thống, hiệu quả trong việc kiểm soát quyền truy cập nhưng lại thiếu sự linh hoạt cần thiết để đối phó với mối đe dọa an ninh ngày càng tăng. VNIS kết hợp xác thực truyền thống với giải pháp đám mây, nhưng mô hình này có thể không đủ để đáp ứng nhu cầu an ninh mạng phức tạp hiện nay [9].

Google's BeyondCorp, một mô hình tiên phong trong việc áp dụng Zero Trust, loại bỏ sự phụ thuộc vào mạng nội bộ. Mô hình này chuyển sang truy cập dựa trên xác thực người dùng và thiết bị, bất kể vị trí, tăng cường bảo mật bằng cách áp dụng chính sách an ninh dựa trên ngữ cảnh và hành vi người dùng [8].

Microsoft, thông qua Azure Active Directory, cung cấp quản lý danh tính và quyền truy cập đám mây, hỗ trợ xác thực đa yếu tố và tinh chỉnh chính sách truy cập dựa trên ngữ cảnh và rủi ro đăng nhập. Hệ thống của Microsoft cung cấp khả năng tích hợp sâu rộng với hệ sinh thái đám mây và tự động hóa quy trình quản lý bảo mật [7].

Nhìn chung, so sánh này làm rõ ràng về lợi thế của Zero Trust trong việc đối phó với các thách thức bảo mật mạng hiện đại. Việc áp dụng nguyên tắc "không tin tưởng mặc định" và "luôn luôn xác minh" trong mô hình Zero Trust cung cấp nền tảng vững chắc cho việc bảo vệ thông tin, khuyến khích sự linh hoạt trong quản lý truy cập và đảm bảo an ninh dữ liệu trong bối cảnh mạng lưới ngày càng mở rộng. Tuy nhiên, các hệ thống kể trên sẽ yêu cầu chia sẻ thông tin của hệ thống với bên thứ ba và cần phải trả phí để có đầy đủ các dịch vụ hỗ trợ đi kèm. Trong khi đó, hệ thống mà tôi phát triển dựa trên mô hình Zero Trust không chỉ đảm bảo tính độc lập và kiểm soát dữ liệu một cách toàn diện mà còn giúp giảm thiểu chi phí liên quan đến việc sử dụng các giải pháp bên ngoài. Bằng cách sử dụng các công nghệ mã nguồn mở và tận dụng các nguồn lực sẵn có trong tổ chức, hệ thống của tôi có thể được tùy chỉnh và mở rộng mà không cần phụ thuộc quá nhiều vào các dịch vụ đám tính phí.

3.5. Kết luận chương 3

Trong chương này, chúng ta đã đi sâu vào việc thiết kế một mô hình quản lý xác thực và quyền truy cập dựa trên Zero Trust, phương pháp tiếp cận ngày càng thiết yếu trong bối cảnh bảo mật thông tin hiện đại. Mô hình này không chỉ tăng cường an ninh mạng mà còn đáp ứng nhu cầu về tính linh hoạt và mở rộng, đặc biệt quan trọng cho các tổ chức trong thời đại số hiện nay.

Qua quá trình thiết kế hệ thống dựa trên mô hình Zero Trust, đã được triển khai các biện pháp xác thực đa yếu tố, kiểm tra ngữ cảnh truy cập và phân quyền dựa trên vai trò. Các biện pháp này tạo nên một lớp bảo mật đa tầng, giúp giảm thiểu rủi ro từ các cuộc tấn công và nỗ lực truy cập trái phép, đồng thời đảm bảo rằng mọi quyền truy cập đều dựa trên sự kiểm soát và đánh giá kỹ lưỡng.

So sánh hệ thống này với các mô hình của VNIS, Google (BeyondCorp), và Microsoft đã cho thấy, mặc dù mỗi mô hình có điểm mạnh và yếu riêng, nguyên tắc Zero Trust cung cấp một nền tảng vững chắc cho việc bảo vệ thông tin trong môi trường mạng ngày càng phức tạp. Sự tích hợp, tự động hóa và áp dụng công nghệ tiên tiến từ các mô hình này mang đến những cái nhìn tổng quan hơn, giúp cải thiện và tối ưu hóa hơn nữa mô hình Zero Trust của tôi.

CHƯƠNG 4: TRIỂN KHAI VÀ THỬ NGHIỆM MÔ HÌNH

4.1. Triển khai hệ thống

Triển khai hệ thống Zero Trust là một quá trình phức tạp đòi hỏi sự cẩn thận trong việc lựa chọn công nghệ, cài đặt, và tích hợp hệ thống. Mục tiêu là đảm bảo mô hình được thực hiện một cách an toàn và hiệu quả, phù hợp với kiến trúc đã được đề ra trong Chương 3.

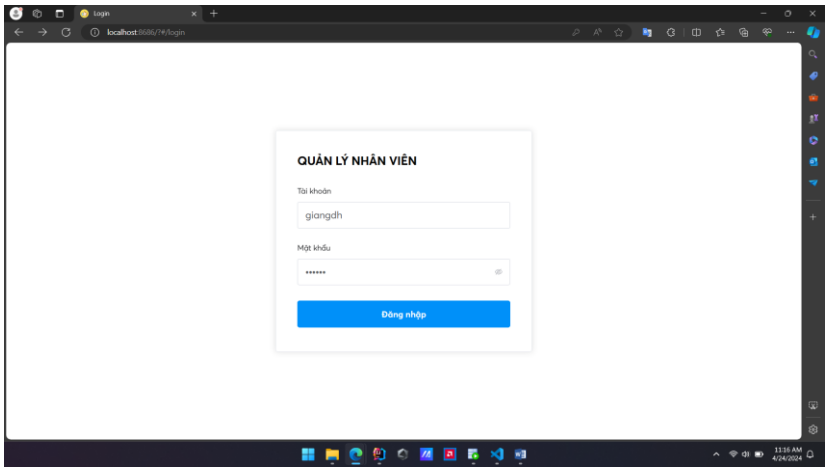
Quá trình cài đặt và cấu hình mô hình Zero Trust bao gồm các bước sau:

Thiết lập các chính sách bảo mật: Thiết lập các chính sách bảo mật chi tiết, bao gồm quản lý tối thiểu quyền truy cập và từ chối mặc định để kiểm soát chặt chẽ quyền truy cập đến các tài nguyên.

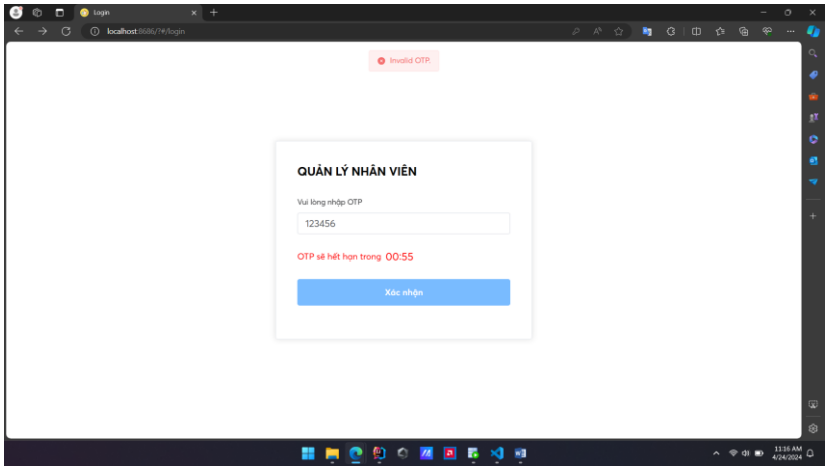
Thiết lập MFA: Triển khai MFA để yêu cầu xác thực đa yếu tố tại mọi điểm truy cập quan trọng, từ xa và trong mạng nội bộ.

Kiểm soát truy cập dựa trên vai trò (RBAC): Hệ thống RBAC được thiết kế để đảm bảo rằng người dùng chỉ có quyền truy cập vào tài nguyên cần thiết cho công việc của họ. Việc triển khai RBAC bao gồm việc xác định các vai trò người dùng và phân quyền truy cập tương ứng.

Hình 4.1 và hình 4.2 mô tả giao diện đăng nhập xác thực mật khẩu và xác thực bằng mã OTP.

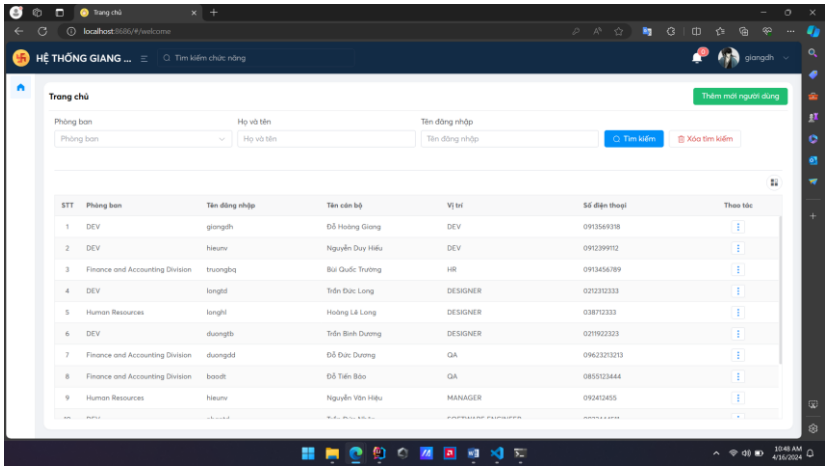


Hình 4.1 Xác thực bằng việc đăng nhập sử dụng tài khoản và mật khẩu



Hình 4.2 Xác thực OTP

Hình 4.3 mô tả màn hình sau khi đăng nhập thành công của người dùng với quyền ADMIN



Hình 4.3 Giao diện đăng nhập của người dùng quyền ADMIN

4.2. Thử nghiệm hệ thống

Để đảm bảo hệ thống an ninh mạng Zero Trust hoạt động hiệu quả và an toàn, việc thực hiện thử nghiệm kỹ lưỡng là cần thiết. Hệ thống đang được chạy trên một máy tính với các thông số kỹ thuật sau:

CPU: AMD Ryzen 7 7735HS, 8 cores

RAM: 16 GB DDR5

Hệ điều hành: Windows 11

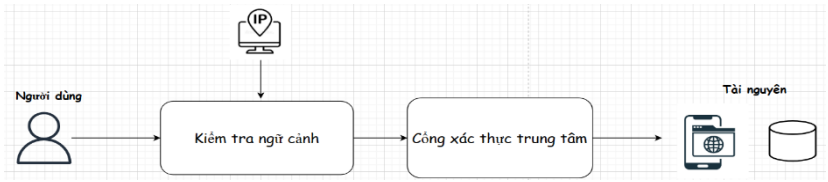
Thử nghiệm bắt đầu bằng việc kiểm tra cơ chế xác thực và ủy quyền của hệ thống để đảm bảo chúng hoạt động chính xác theo các chính sách bảo mật đã định. Điều này bao gồm kiểm tra xác thực đa yếu tố, kiểm soát quyền truy cập dựa trên vai trò, và các quy trình xác thực ngữ cảnh. Hệ thống của tôi cấu hình để truy cập được cho phép trong thời gian hành chính từ thứ 2 đến thứ 6 trong khoảng từ 8 AM đến 5 PM, đặc biệt là khả năng phát hiện và chặn các yêu cầu truy cập bất thường từ IP hoặc MAC địa chỉ không được ủy quyền.

Một kịch bản thử nghiệm để kiểm tra địa chỉ IP và MAC cho phép truy cập được mô tả dưới đây.

Trường hợp nằm trong vùng mạng cho phép

```
# IPs allowed
allowed:
  ips:
    - "192.168.56."
    - "192.168.9."
    - "192.168.1."
```

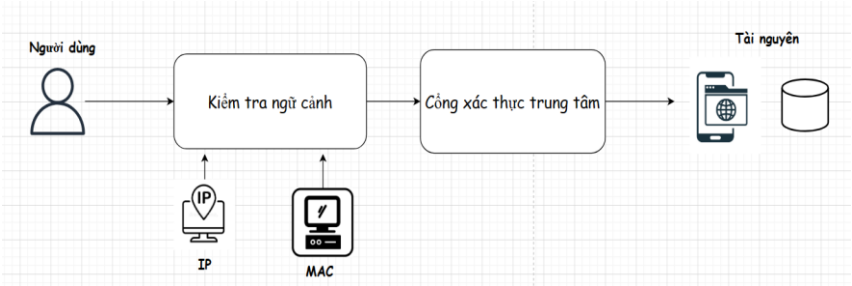
Hình 4.4. Cấu hình dải IP cho phép truy cập



Hình 4.5. Xác thực qua địa chỉ IP

Trong trường hợp thiết bị sử dụng truy cập hệ thống có địa chỉ IP nằm trong dải IP cho phép của hệ thống (Được mô tả ở hình 4.4) thì sẽ xác thực thành công và chuyển đến phần xác thực OTP.

Trường hợp nằm ngoài vùng mạng cho phép



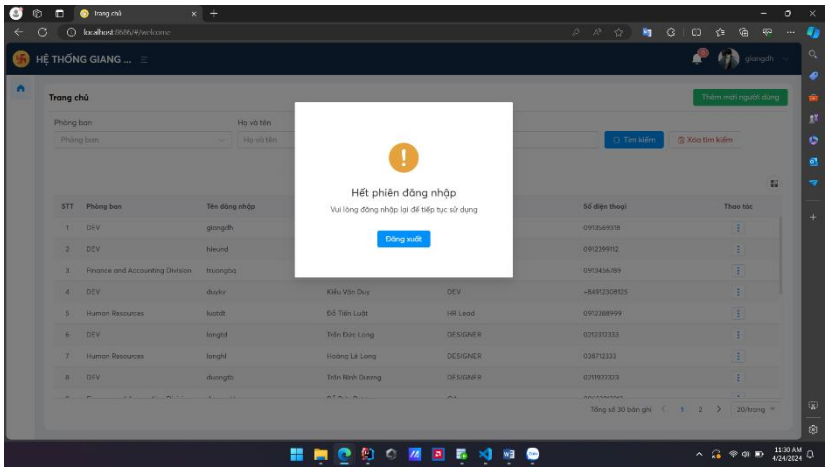
Hình 4.6. Xác thực qua địa chỉ MAC

	EMPLOYEE_ID	MAC	DEVIC...	STATUS
1	41	51:F2:2B:71:74:A8	1	1
2	2	28:00:7F:6C:22:8C	1	0
3	1	0B:DF:CF:32:72:9C	1	1
4	(null)	C8:D4:A9:91:A4:7E	1	0
5	(null)	B7:68:13:8D:01:59	1	0
6	(null)	EB:7A:C8:6F:F5:97	1	0
7	(null)	BF:87:A6:2B:B4:FE	1	0
8	(null)	43:00:45:4F:71:45	1	0
9	(null)	B4:46:9A:5E:07:BF	1	0
10	(null)	DE:D5:1F:53:DD:AA	1	0
11	(null)	43:94:E7:F2:39:82	1	0
12	(null)	33:1B:2F:01:08:3D	1	0
13	(null)	D2:92:D6:A7:CB:11	1	0
14	(null)	7A:C8:F6:F7:54:80	1	0
15	(null)	D7:D3:15:6E:75:98	1	0
16	(null)	97:E3:6F:17:55:42	1	0
17	(null)	17:DE:C4:18:AF:AC	1	0

Hình 4.7 Bảng lưu trữ thông tin địa chỉ MAC được phép truy cập hệ thống

Trong trường hợp thiết bị sử dụng truy cập hệ thống đang có địa chỉ IP không nằm trong dải IP cho phép của hệ thống (Được mô tả ở hình 4.4) nên ta xét đến địa chỉ MAC của thiết bị truy cập hệ thống. Nếu địa chỉ MAC của thiết bị không nằm trong dải MAC thiết bị cho phép truy cập (Được mô tả ở hình 4.7) thì xác thực thất bại.

Một điểm nổi bật khác trong các thử nghiệm là việc kiểm tra tự động xác thực lại người dùng sau một khoảng thời gian nhất định. Điều này phản ánh nguyên tắc của mô hình Zero Trust về việc không bao giờ tin tưởng hoàn toàn vào bất kỳ phiên đăng nhập nào và luôn yêu cầu xác minh lại để đảm bảo an ninh. Việc tự động xác thực lại giúp ngăn chặn nguy cơ bảo mật phát sinh từ các phiên đăng nhập dài, đồng thời giảm thiểu rủi ro do tấn công lấy cắp phiên làm việc.



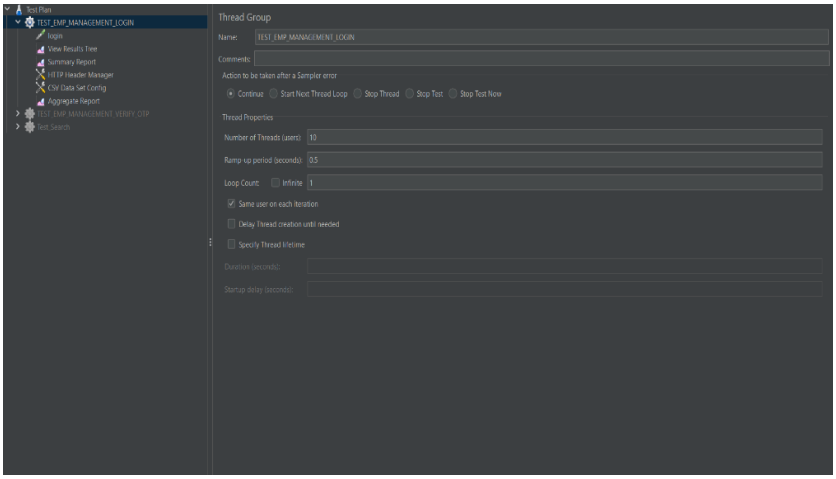
Hình 4.8 Tự động xác thực sau khoảng thời gian

Đặc biệt, thử nghiệm cũng bao gồm việc kiểm tra cơ chế phân quyền dựa trên vai trò, đáp ứng nguyên tắc tối thiểu của mô hình Zero Trust. Hệ thống được thiết lập để cấp quyền truy cập chỉ dựa trên nhu cầu thực tế của người dùng trong công việc của họ, nhằm mục đích hạn chế quyền truy cập không cần thiết và tăng cường an ninh tổng thể.

Tất cả các kịch bản thử nghiệm này cung cấp dữ liệu quan trọng về hiệu quả và độ tin cậy của hệ thống Zero Trust trong một loạt các điều kiện và tình huống, từ đó giúp nhận diện các điểm mạnh và cơ hội cải tiến hệ thống để đạt hiệu quả tối ưu trong môi trường thực tế.

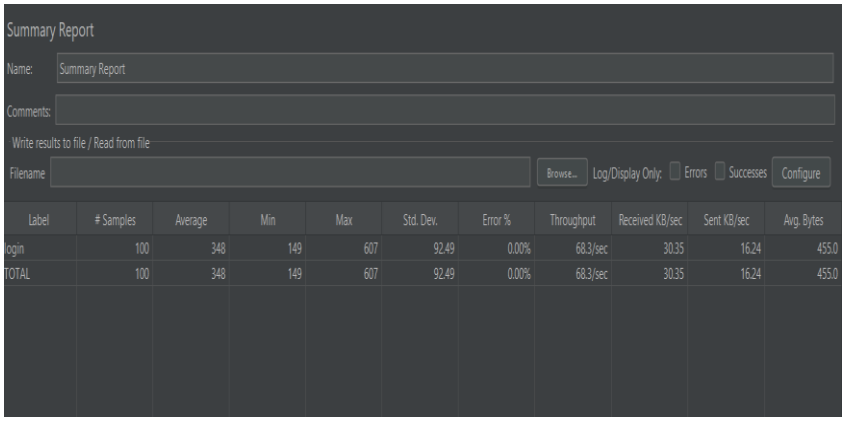
4.3. Đánh giá hoạt động của hệ thống

Phần này mô tả quá trình mô phỏng, đánh giá tải của hệ thống khi có nhiều người dùng cùng sử dụng. Việc kiểm tra được thực hiện sử dụng công cụ JMeter được, cho phép phân tích chi tiết hiệu suất của hệ thống dưới các cấu hình và điều kiện khác nhau, từ đó đảm bảo hệ thống có thể đáp ứng nhu cầu về tốc độ và ổn định trong các tình huống thực tế. Cài đặt thông số cho Jmeter được mô tả như hình 4.9



Hình 4.9 Cài đặt thông số kiểm thử trên Jmeter

Quá trình thử nghiệm bắt đầu bằng việc đánh giá khả năng xử lý tải của các API cốt yếu của hệ thống. Kết quả kiểm tra API Đăng nhập được mô tả trong hình 4.10



Hình 4.10 Kết quả kiểm tra API Đăng nhập với 100 người dùng

Các bài thử nghiệm cho thấy, dưới tải từ thấp đến cao, hệ thống duy trì được thời gian phản hồi trung bình tốt và không ghi nhận lỗi, chứng tỏ khả năng xử lý đồng thời nhiều yêu cầu mà không ảnh hưởng đến hiệu quả hoạt động. Khi số lượng người dùng tăng lên, hệ thống vẫn duy trì được hiệu suất cao.

Bên cạnh đó, việc đánh giá hoạt động của hệ thống cũng bao gồm kiểm tra khả năng của hệ thống trong việc phát hiện và đối phó với các hành vi bất thường. Việc kiểm tra tự động xác thực lại người dùng sau khoảng thời gian nhất định nhằm đảm bảo rằng mọi phiên làm việc đều được xác thực liên tục, giảm thiểu nguy cơ từ các cuộc tấn công như chiếm quyền phiên làm việc.

4.4. Kết luận chương 4

Trong chương 4, qua quá trình triển khai và thử nghiệm mô hình Zero Trust, tôi đã thu được những kết quả đáng giá cho thấy khả năng cao trong việc nâng cao bảo mật thông tin và hệ thống mạng. Các bài thử nghiệm đã chứng minh được sự linh hoạt và tính ứng biến cao của hệ thống trước những thách thức về bảo mật, từ việc kiểm soát truy cập nghiêm ngặt theo thời gian và địa điểm, cho đến đối phó với các hành vi truy cập không phù hợp từ cả bên trong và bên ngoài tổ chức.

Những thử nghiệm trên hệ thống Zero Trust đã cung cấp một cái nhìn thực tế về việc triển khai công nghệ này trong môi trường doanh nghiệp. Mô hình đã thể hiện khả năng đáp ứng nhanh với các yêu cầu truy cập và duy trì hiệu suất ổn định. Đồng thời, các biện pháp bảo mật đa lớp đã chứng tỏ được hiệu quả trong việc bảo vệ dữ liệu nhạy cảm và hạn chế rủi ro an ninh thông tin.

Tuy nhiên không có hệ thống bảo mật nào là hoàn hảo và mô hình dựa trên Zero Trust do tôi xây dựng cũng vậy. Có những thách thức và cơ hội cải thiện cần được xem xét, từ việc tối ưu hóa quy trình xác thực người dùng cho đến nâng cao khả năng phát hiện và phản ứng trước các mối đe dọa an ninh mạng.

Chương này không chỉ kết thúc với việc hoàn tất giai đoạn thử nghiệm của mô hình, mà còn mở ra một chặng đường mới cho việc cải tiến liên tục, đảm bảo rằng hệ thống bảo mật sẽ phát triển và thích nghi với mọi thay đổi trong môi trường an ninh mạng ngày càng phức tạp.

KẾT LUẬN

Qua quá trình nghiên cứu và phát triển, luận văn này đã đi sâu vào việc khám phá và thực nghiệm mô hình Zero Trust, một tiếp cận an ninh mạng hiện đại, được xây dựng trên nguyên tắc không tin cậy mặc định và yêu cầu xác minh liên tục.

Luận văn cũng đã trình bày cặn kẽ các nguyên tắc của Zero Trust, từ việc "Không bao giờ tin tưởng, luôn luôn xác minh" cho đến quản lý quyền truy cập dựa trên cơ sở quyền hạn tối thiểu. Các thành phần kỹ thuật từ xác thực đa yếu tố đến quản lý danh tính và quyền truy cập đã được thảo luận chi tiết, cùng với việc đánh giá sâu rộng về tính bảo mật và hiệu suất của chúng qua quá trình triển khai thực tế và thử nghiệm hệ thống.

Mô hình Zero Trust đã chứng minh rằng nó không chỉ là một khái niệm lý thuyết mà còn là một giải pháp thiết thực, có thể được áp dụng và mang lại kết quả tích cực trong việc bảo vệ dữ liệu và tài nguyên mạng của tổ chức. Nhưng điều này không đồng nghĩa với việc không còn đối mặt với thách thức: từ sự phức tạp trong việc quản lý và thực thi chính sách, cho đến cần thiết phải đào tạo nhân viên về các phương pháp và công cụ mới.

Luận văn đã trình bày chi tiết về việc xây dựng và triển khai một mô hình quản lý xác thực và quyền truy cập dựa trên khái niệm Zero Trust. Qua đó, hệ thống đã được thiết kế để thích ứng với các yêu cầu bảo mật ngày càng cao và đa dạng của môi trường mạng hiện đại. Hệ thống này không chỉ áp dụng các biện pháp xác thực đa yếu tố mà còn tích hợp các kiểm soát ngữ cảnh và phân quyền dựa trên vai trò để tăng cường bảo mật và hiệu quả quản lý.

Ngoài ra, luận văn cũng đã mô phỏng, đánh giá thực tế hệ thống, qua đó kiểm tra hiệu suất, khả năng chịu tải khi đồng thời nhiều người dùng cùng truy cập hệ thống tại một thời điểm. Các kết quả thu được đã chứng minh khả năng của mô hình trong việc bảo vệ tài nguyên thông tin một cách hiệu quả, ngay cả trong điều kiện áp lực cao.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Chandra, J. V., Challa, N., & Pasupuletti, S. K. (2019). Authentication and authorization mechanism for cloud security. *International Journal of Engineering and Advanced Technology*, *8*(6), 2072-2078.

[2] AlQahtani, A. A. S., El-Awadi, Z., & Min, M. (2021, October). A survey on user authentication factors. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0323-0328). IEEE.

[3] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE Access*, *10*, 57143-57179.

[4] Alappat, M. R. (2023). *Multifactor Authentication Using Zero Trust*. Rochester Institute of Technology.

[5] Wylde, A. (2021, June). Zero trust: Never trust, always verify. In *2021 international conference on cyber situational awareness, data analytics and assessment (cybersa)* (pp. 1-4). IEEE.

[6] Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, *2021*, 1-10.

[7] "Microsoft," Oct 23, 2023. [Online]. Available: Implementing a Zero Trust security model at Microsoft - Inside Track Blog (accessed 3/2024)

[8] "GoogleCloud," August 11, 2022. [Online]. Available: Zero Trust and BeyondCorp Google Cloud | Google Cloud Blog (accessed 3/2024)

[9] "VNIS," May 09, 2023. [Online]. Available: Zero Trust - Mô hình an ninh mạng đáp ứng thách thức bảo mật (vnis.vn)