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

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2024

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**

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. ĐINH TRƯỜNG DUY

HÀ NỘI – 2024

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong đề án tốt nghiệp là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tác giả đề án tốt nghiệp ký và ghi rõ họ tên

Mục lục

DANH SÁCH HÌNH VẼ

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
ABAC	Attribute-Based Access Control	Phân quyền dựa trên thuộc tính
ACL	Access Control List	Danh sách kiểm soát truy cập
BAC	Blockchain-Based Access Control	Phân quyền dựa trên Blockchain
CDM	Continuous Diagnostics and Mitigation	Hệ thống chẩn đoán và giảm thiểu liên tục
CAMFA	Context-Aware Multimodal FIDO Authentication	Xác thực FIDO đa phương thức nhận thức ngữ cảnh
ECG	Electrocardiography	Điện tâm đồ
EEG	Electroencephalography	Điện não đồ
EMG	Electromyography	Điện cơ đồ
FIDO	Fast IDentity Online	Xác thực danh tính nhanh
FISMA	Federal Information Security Management Act	Đạo luật Quản lý An ninh Thông tin Liên bang
IAM	Identity and Access Management	Quản lý danh tính và truy cập
IBAC	Identity-Based Access Control	Phân quyền dựa trên danh tính
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IoT	Internet of Things	Internet vạn vật
IDoT	Identity-Driven Traffic	Lưu lượng dựa trên danh tính
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập
MFA	Multi-Factor Authentication	Xác thực đa yếu tố
NGFW	Next Generation Firewall	Tường lửa thế hệ mới
OT	Operational Technology	Công nghệ vận hành
OTP	One-Time Password	Mật khẩu một lần
PAM	Privileged Access Management	Quản lý truy cập đặc quyền
PA	Policy Administration	Quản lý chính sách
PE	Policy Enforcement	Thực thi chính sách
PEP	Policy Enforcement Point	Điểm thực thi chính sách
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai

PoLP	Principle of Least Privilege	Nguyên tắc Tối thiểu hóa Quyền truy cập
PUFs	Physically Unclonable Functions	Chức năng không thể sao chép vật lý
RBAC	Role-Based Access Control	Phân quyền dựa trên vai trò
RbAC	Risk-Based Access Control	Phân quyền dựa trên rủi ro
RP LoA	Relying Party Level of Authentication	Cấp độ xác thực của bên sử dụng
SIEM	Security Information and Event Management	Quản lý thông tin và sự kiện bảo mật
SOAR	Security Orchestration, Automation and Response	Hệ thống dàn xếp, tự động hóa và phản ứng bảo mật
UBA	User Behavior Analytics	Phân tích hành vi người dùng
VPN	Virtual Private Network	Mạng riêng ảo
ZTA	Zero Trust Architecture	Kiến trúc Zero Trust
ZTD	Zero Trust Deployment	Triển khai Không tin cậy

LÝ DO CHỌN ĐỀ TÀI

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.

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. 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 quan trọng của xác thực và quyền truy cập

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

Khái niệm Authentication (xác thực)

Authentication (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 an ninh thông tin, Authentication đảm bảo rằng chỉ những người đã được xác minh mới có thể truy cập vào tài liệu, dịch vụ hoặc các phần quan trọng của hệ thống.

Khi quá trình xác thực thành công, người dùng sẽ được cấp quyền truy cập theo các cấp độ hoặc phạm vi đã được quy định trước. Authentication là một phần quan trọng trong bảo mật thông tin và đảm bảo tính riêng tư của người dùng.

Nó đóng vai trò chống lại các tấn công giả mạo và bảo vệ khỏi việc truy cập trái phép vào hệ thống hoặc dữ liệu quan trọng.

Hình 1.1 Authentication (Xác thực)

Các yếu tố xác thực

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

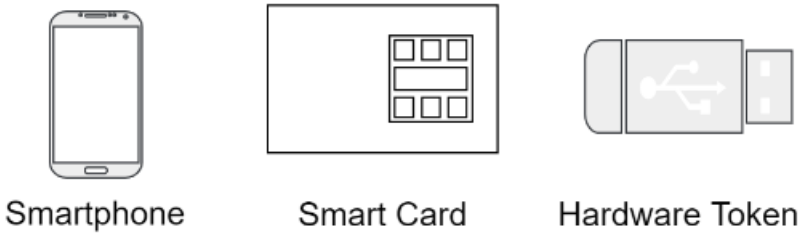
Điều người dùng biết (yếu tố kiến thức) :

- 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.

Hình 1.2 Yếu tố kiến thức trong xác thực

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. Việc xác thực này loại bỏ được rủi ro khi người dùng quên mật khẩu. Tuy nhiên, điều đó có nghĩa là người dùng phải mang theo đồ vật đó bất cứ khi nào họ cần để truy cập vào hệ thống. Và những đồ vật này có thể bị mất, đánh cắp hoặc hư hỏng trong quá trình di chuyển.



Hình 1.3 Yếu tố sở hữu trong xác thực

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. Ưu điểm của xác thực sinh trắc học là chúng khó bị mất hoặc bị sao chép. Tuy nhiên các phương thức xác thực này có thể tốn kém hơn các yếu tố xác thực truyền thống.

Hình 1.4 Yếu tố đặc điểm cá nhân người dùng trong xác thực

Tầm quan trọng của Authentication

Xác thực là quá trình xác minh danh tính của người dùng hoặc thiết bị. Đây là bước đầu tiên và quan trọng nhất trong việc bảo mật hệ thống và dữ liệu. Xác thực giúp đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào hệ thống và dữ liệu. Những lý do khiến việc xác thực trở nên quan trọng là:

- Bảo vệ dữ liệu quan trọng: Authentication đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào thông tin và dữ liệu quan trọng. Điều này giúp ngăn chặn truy cập trái phép từ những người không có quyền truy cập.
- Đảm bảo độ tin cậy: Xác thực danh tính của người dùng đảm bảo rằng người dùng thật sự là người mà họ tuyên bố là. Điều này giúp xây dựng tính đáng tin cậy và uy tín cho người dùng và tổ chức.
- Giữ an toàn cho thông tin cá nhân: Authentication bảo vệ tài khoản cá nhân của người dùng khỏi việc bị truy cập trái phép hoặc đánh cắp thông tin. Từ đó giúp bảo vệ thông tin cá nhân của họ không bị lợi dụng bởi những kẻ lừa đảo.
- Tuân thủ quy định pháp luật: Trong một số ngành như tài chính và y tế, các quy định pháp luật yêu cầu việc bảo mật và xác thực dữ liệu. Authentication giúp đảm bảo rằng tổ chức tuân thủ các quy định này và tránh các vấn đề pháp lý.
- Đảm bảo trải nghiệm người dùng: Authentication cung cấp trải nghiệm an toàn hơn cho người dùng trên các ứng dụng hoặc nền tảng trực tuyến. Nhờ vậy họ có thể tự tin sử dụng và truy cập mà không lo ngại về vấn đề bảo mật.

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

Khái niệm Authorization (quyền truy cập)

Ủy quyền truy cập là quá trình thiết lập ranh giới cho phép truy cập, tức là mức độ người dùng có thể truy cập được [1].

Ủy quyền truy cập là một phần quan trọng của bảo mật hệ thống vì nó giúp bảo vệ dữ liệu và hệ thống khỏi truy cập trái phép. Nó cũng có thể giúp tuân thủ các quy định và tiêu chuẩn.

Hình 1.5 Authorization (Quyền truy cập)

Tầm quan trọng của Authorization

Authorization (Ủy quyền) là một khía cạnh quan trọng khác của bảo mật thông tin và hệ thống. Trong ngữ cảnh của bảo mật hệ thống, ủy quyền là quá trình kiểm soát và quản lý quyền lợi của người dùng, ứng dụng, hay dịch vụ đối với các tài nguyên cụ thể trong hệ thống. Dưới đây là một số chi tiết về tầm quan trọng của ủy quyền:

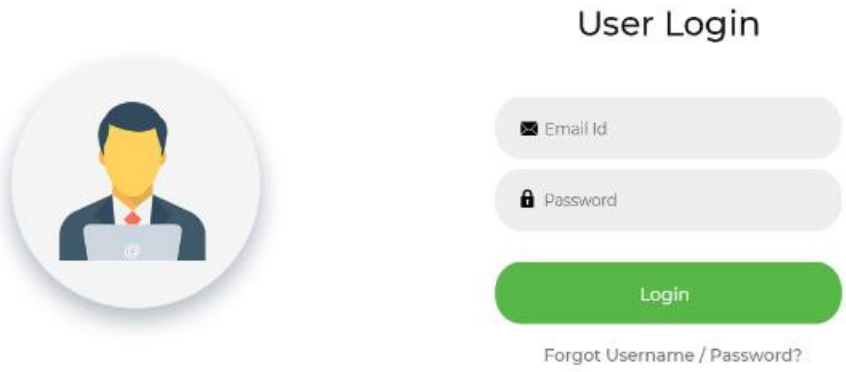
- Bảo vệ dữ liệu và hệ thống khỏi truy cập trái phép: Chỉ những người dùng được ủy quyền mới có thể truy cập dữ liệu và hệ thống. Điều này giúp ngăn chặn tin tặc và những kẻ xâm nhập khác truy cập thông tin nhạy cảm.
- Đảm bảo tính toàn vẹn của dữ liệu: Quyền truy cập có thể giúp ngăn chặn người dùng trái phép sửa đổi hoặc xóa dữ liệu. Điều này giúp đảm bảo tính toàn vẹn của dữ liệu và tính chính xác của các quyết định kinh doanh.
- Tuân thủ các quy định và tiêu chuẩn: Nhiều quy định và tiêu chuẩn yêu cầu các tổ chức triển khai các biện pháp kiểm soát quyền truy cập để bảo vệ dữ liệu.

- Giảm nguy cơ vi phạm dữ liệu: Quyền truy cập có thể giúp giảm nguy cơ vi phạm dữ liệu bằng cách hạn chế số lượng người có quyền truy cập vào dữ liệu nhạy cảm.

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, như trong hình 1.3



Hình 1.6 Xác thực sử dụng username và password

Hoạt động:

1. Người dùng cung cấp username: Người dùng nhập thông tin tài khoản của mình, thường là một tên đăng nhập duy nhất.
2. Người dùng cung cấp password: Người dùng nhập mật khẩu mà chỉ có họ biết để xác minh danh tính.
3. Hệ thống xác thực: Hệ thống so sánh thông tin đăng nhập được cung cấp với dữ liệu đã lưu trữ. Nếu thông tin khớp, người dùng được cho phép truy cập vào tài khoản hoặc hệ thống.

Ưu điểm:

- Đơn giản và dễ triển khai: Xác thực truyền thống sử dụng username và password là một phương pháp đơn giản và dễ dùng. Người dùng chỉ cần nhớ thông tin đăng nhập và nhập vào để truy cập vào hệ thống.
- Phổ biến và rộng rãi: Xác thực truyền thống đã được sử dụng rộng rãi trong nhiều ứng dụng và hệ thống. Đa số người dùng đã quen thuộc và có kiến thức về cách sử dụng username và password.
- Linh hoạt và tiện ích: Người dùng có thể tạo và quản lý nhiều tài khoản với các username và password khác nhau cho từng dịch vụ hoặc nền tảng. Điều này mang lại tính linh hoạt và tiện ích cho người dùng khi quản lý thông tin đăng nhập.

Nhược điểm:

- Bảo mật yếu: Xác thực truyền thống sử dụng username và password đơn lẻ, làm cho nó dễ bị tấn công và đánh cắp. Nếu một người khác có thể tìm hiểu hoặc đoán được thông tin đăng nhập, họ có thể tiếp cận và xâm nhập vào tài khoản.
- Nguy cơ về mất mật khẩu: Người dùng có thể quên mật khẩu hoặc mất mật khẩu, đặc biệt khi sử dụng nhiều tài khoản khác nhau. Điều này tạo ra sự phiền toái và cần thực hiện quy trình khôi phục mật khẩu.
- Độc quyền và chia sẻ thông tin: Username và password thường được sử dụng riêng cho mỗi người dùng. Tuy nhiên, người dùng có thể cung cấp thông tin đăng nhập cho người khác, gây ra rủi ro về bảo mật và truy cập trái phép vào tài khoản.
- Các hình thức tấn công: Xác thực truyền thống dễ bị tấn công bởi các hình thức như tấn công dò mật khẩu (brute force), tấn công từ điển (dictionary attack) và tấn công phishing. Những hình thức tấn công này có thể thành công nếu người dùng chọn mật khẩu yếu hoặc không cẩn thận trong việc chia sẻ thông tin đăng nhập.

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, …

Hình 1.7 Xác thực đa yếu tố

Hoạt động:

1. Người dùng nhập thông tin đăng nhập (yếu tố kiến thức) vào hệ thống.
2. Hệ thống yêu cầu người dùng cung cấp thêm một yếu tố xác thực khác.
3. Người dùng cung cấp yếu tố xác thực thứ hai (ví dụ: mã OTP được gửi qua tin nhắn SMS).
4. Hệ thống xác minh cả hai yếu tố xác thực và cấp cho người dùng quyền truy cập.

Ưu điểm:

- Bảo mật cao hơn: MFA tăng cường bảo mật bằng cách yêu cầu nhiều yếu tố xác thực. Một hacker cần phải chiếm được cả hai hoặc nhiều yếu tố để xâm nhập vào tài khoản, làm cho việc tấn công trở nên khó khăn hơn.
- Phòng ngừa tấn công đánh cắp thông tin đăng nhập: Với MFA, việc đánh cắp mật khẩu đơn lẻ không đủ để truy cập vào tài khoản. Kẻ tấn công sẽ phải có cả yếu tố sở hữu của người dùng, như thiết bị di động hoặc thẻ thông minh, để thành công.
- Tăng cường tính nhất quán: MFA giúp đảm bảo rằng người dùng thực sự là chủ sở hữu của tài khoản bằng cách kết hợp nhiều yếu tố xác thực. Điều này giúp ngăn chặn các hình thức giả mạo và đảm bảo tính nhất quán trong quá trình xác thực.
- Tùy chỉnh và linh hoạt: MFA cho phép người dùng lựa chọn các yếu tố xác thực phù hợp với nhu cầu và sự thuận tiện của họ. Người dùng có thể chọn sử dụng mật khẩu, mã OTP, dấu vân tay, hoặc các phương pháp xác thực khác tùy theo sự ưa thích và tính tiện lợi.

Nhược điểm:

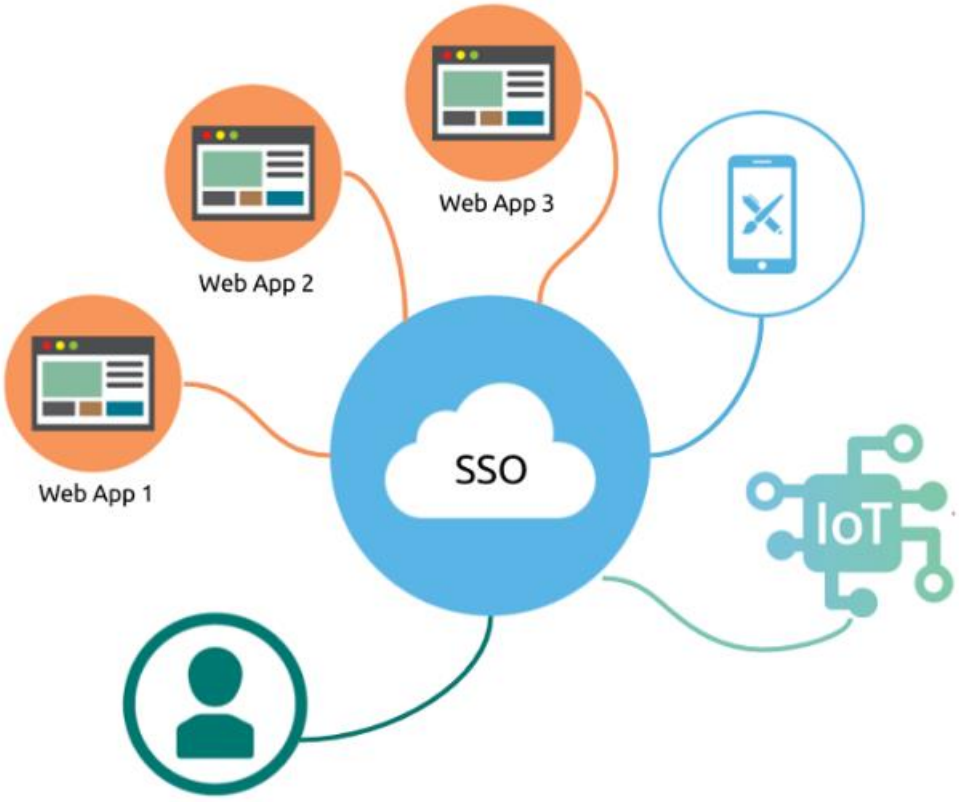
- Phức tạp và không tiện lợi: MFA đòi hỏi người dùng phải thực hiện nhiều bước xác thực, làm tăng độ phức tạp và thời gian để truy cập vào hệ thống. Điều này có thể gây phiền toái và giảm trải nghiệm người dùng, đặc biệt là khi họ cần truy cập thường xuyên.
- Chi phí và hạ tầng: MFA yêu cầu sự đầu tư trong cơ sở hạ tầng và công nghệ phù hợp. Điều này có thể đòi hỏi các tổ chức phải đầu tư vào phần cứng và phần mềm mới, gây ra chi phí cao và đòi hỏi sự triển khai và quản lý phức tạp.
- Rủi ro đối với yếu tố sở hữu: Một trong những yếu tố xác thực trong MFA là yếu tố sở hữu, chẳng hạn như thiết bị di động hoặc thẻ thông minh. Nếu người

dùng mất thiết bị hoặc thẻ, hoặc nếu chúng bị đánh cắp, sẽ có nguy cơ cao rằng kẻ tấn công có thể sử dụng chúng để xâm nhập vào tài khoản.

- Độ phức tạp trong triển khai: Triển khai MFA đòi hỏi sự tích hợp và cấu hình đúng đắn với hệ thống hiện có. Điều này có thể phức tạp và đòi hỏi sự hiểu biết kỹ thuật cao, có thể gây khó khăn cho các tổ chức hoặc người dùng không có kiến thức chuyên môn.
- Phụ thuộc vào yếu tố thứ ba: MFA thường dựa vào nhà cung cấp dịch vụ bên thứ ba để cung cấp các yếu tố xác thực, chẳng hạn như mã OTP qua tin nhắn văn bản hoặc ứng dụng di động. Điều này có nghĩa là MFA phụ thuộc vào tính sẵn có và sự tin cậy của nhà cung cấp dịch vụ, và nếu có vấn đề với nhà cung cấp, sẽ ảnh hưởng đến quá trình xác thực.

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. Bạn có thể thấy 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.



Hình 1.8 Xác thực đăng nhập một lần

Hoạt động:

SSO xác lập tín nhiệm giữa ứng dụng hoặc dịch vụ với nhà cung cấp dịch vụ bên ngoài, còn được gọi là nhà cung cấp danh tính (IdP). Việc này được thực hiện thông qua một loạt các bước xác thực, xác nhận và giao tiếp giữa ứng dụng và dịch vụ SSO tập trung. Quy trình của SSO như sau:

1. Khi người dùng đăng nhập vào một ứng dụng, ứng dụng sẽ tạo mã thông báo SSO và gửi yêu cầu xác thực đến dịch vụ SSO.
2. Dịch vụ sẽ kiểm tra xem người dùng đã được xác thực trước đó trong hệ thống hay chưa. Nếu đã xác thực, dịch vụ sẽ gửi một phản hồi xác nhận xác thực đến ứng dụng để cấp quyền truy cập cho người dùng.
3. Nếu người dùng không có thông tin chứng thực đã xác minh, dịch vụ SSO sẽ chuyển hướng người dùng đến hệ thống đăng nhập trung tâm và nhắc người dùng gửi tên người dùng và mật khẩu của họ.

4. Sau khi gửi, dịch vụ xác mình thông tin chứng thực của người dùng và gửi phản hồi tích cực cho ứng dụng.
5. Nếu không, người dùng sẽ nhận được thông báo lỗi và phải nhập lại thông tin chứng thực. Nhiều lần đăng nhập không thành công có thể dẫn đến việc dịch vụ chặn người dùng thử đăng nhập lại trong một khoảng thời gian cố định.

Ưu điểm:

- Tiện lợi cho người dùng: Người dùng chỉ cần nhớ một bộ thông tin đăng nhập duy nhất để truy cập nhiều ứng dụng hoặc hệ thống.
- Tăng cường bảo mật: SSO có thể giúp giảm nguy cơ tấn công mạng vì người dùng không cần phải sử dụng lại mật khẩu trên nhiều ứng dụng hoặc hệ thống.
- Dễ dàng quản lý: SSO giúp việc quản lý tài khoản người dùng trở nên dễ dàng hơn.

Nhược điểm:

- Phụ thuộc vào dịch vụ SSO: Nếu dịch vụ SSO gặp sự cố, người dùng sẽ không thể truy cập bất kỳ ứng dụng hoặc hệ thống nào được ủy quyền.
- Rủi ro bảo mật: Nếu dịch vụ SSO bị tấn công, thông tin đăng nhập của người dùng có thể bị đánh cắp.
- Quyền truy cập quá rộng: Nếu một người dùng đăng nhập thành công vào SSO, họ sẽ có quyền truy cập vào tất cả các ứng dụng và dịch vụ được kết nối. Nếu tài khoản SSO bị xâm phạm, kẻ tấn công có thể truy cập vào tất cả các tài nguyên.
- Chi phí triển khai: Triển khai SSO có thể tốn kém, đặc biệt là cho các tổ chức lớn.

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.

Hình 1.9 Xác thực dựa trên sinh trắc học

Hoạt động:

1. Thu thập dữ liệu sinh trắc học: Dữ liệu sinh trắc học được thu thập bằng cách sử dụng các cảm biến hoặc thiết bị chuyên dụng. Ví dụ: máy quét dấu vân tay, camera nhận diện khuôn mặt, máy quét mống mắt, v.v.
2. Xử lý dữ liệu sinh trắc học: Dữ liệu sinh trắc học được xử lý để trích xuất các đặc điểm độc đáo của người dùng.
3. So sánh dữ liệu sinh trắc học: Dữ liệu sinh trắc học được so sánh với dữ liệu mẫu đã được lưu trữ trong cơ sở dữ liệu.
4. Xác minh danh tính: Nếu dữ liệu sinh trắc học khớp với dữ liệu mẫu, danh tính của người dùng được xác minh.

Ưu điểm:

- Bảo mật cao: Sinh trắc học cung cấp mức độ bảo mật cao hơn so với các phương thức xác thực truyền thống như mật khẩu hoặc thẻ ID.
- Tiện lợi: Sinh trắc học dễ sử dụng và không yêu cầu người dùng ghi nhớ mật khẩu hoặc mang theo thẻ ID.

- Khó giả mạo: Các đặc điểm sinh trắc học rất khó giả mạo.

Nhược điểm:

- Chi phí cao: Thiết bị và phần mềm sinh trắc học có thể tốn kém.
- Yêu cầu về độ chính xác cao: Thiết bị sinh trắc học cần có độ chính xác cao để tránh xác minh sai.
- Lo ngại về quyền riêng tư: Việc thu thập và lưu trữ dữ liệu sinh trắc học có thể gây ra lo ngại về quyền riêng tư.

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.

Ví dụ về Thông tin về session được lưu trong cookies:

Hoạt động:

1. Client gửi một thông tin xác nhận hợp lệ về phía server.
2. Sau khi server xác định danh tính nó tạo ra một sessionId và lưu nó. Và rồi phản hồi client bằng cách thêm nó vào HTTP với Set-Cookie ở header.
3. Client nhận được sessionId sẽ lưu ở cookie của browser. Sau đó với mỗi lần request tiếp theo sẽ gửi về server.

Ưu điểm:

- Vì thông tin nằm trong các request của HTTP lúc này chỉ còn là sessionId, nên sẽ bảo mật tốt hơn so với phương thức HTTP ở trên.
- Các lần đăng nhập tiếp theo nhanh hơn, vì thông tin đăng nhập không bắt buộc.
- Khá dễ thực hiện.

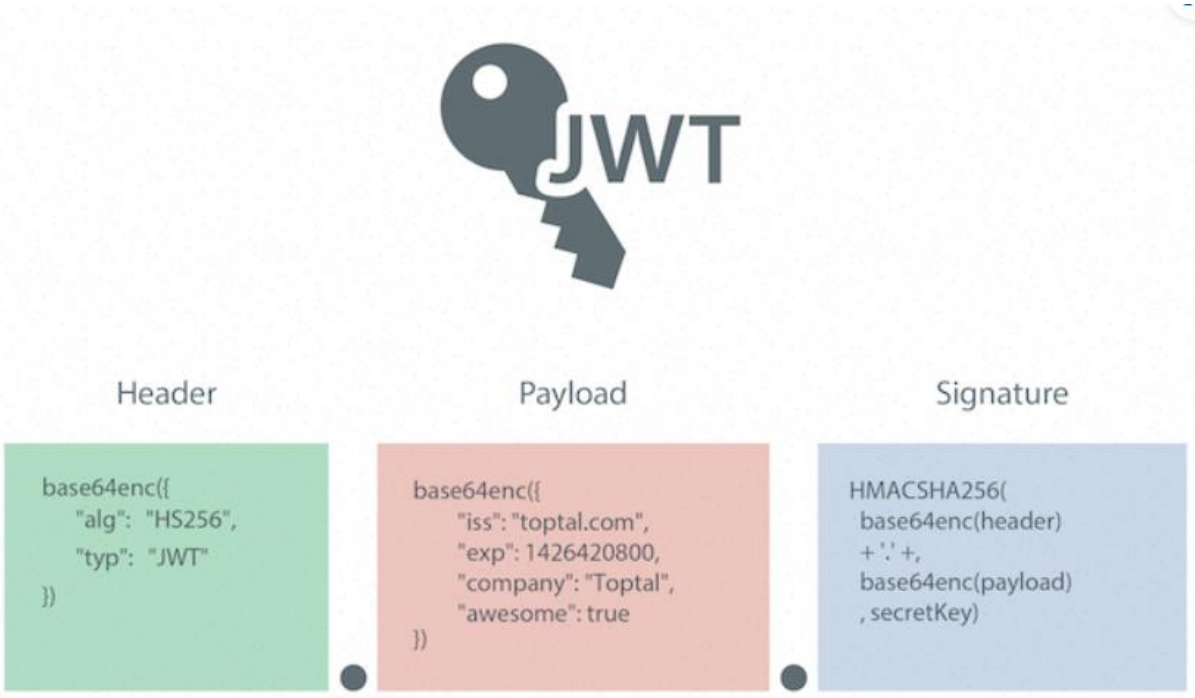
Khuyết điểm:

- Phía server sẽ phải lưu trữ session cho tất cả client, tức là nó sẽ phải lưu trữ một số lượng lớn các sessionId, điều này sẽ gây ra áp lực server quá mức. Nếu server mà chúng ta đang triển khai dạng cluster (cụm), để đồng bộ hóa trạng thái đăng nhập, sessionId cần phải được đồng bộ hóa cho từng máy, điều này vô hình trung làm tăng chi phí bảo trì server.
- Sẽ gặp khó khi triển khai sang các nền tảng khác (như ứng dụng di động vì nó không cookie để lưu).

1.2.6 Token

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).

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.



Hình 1.10 Cấu trúc JSON Web Mã

Một chuỗi JWT bao gồm 3 phần là:

- Header: chứa kiểu dữ liệu, và thuật toán sử dụng để mã hóa ra chuỗi JWT.
- Payload: chứa các thông tin mình muốn đặt trong chuỗi token như userName, userId, author, ...
- Signature: được tạo ra bằng cách mã hóa phần header, payload kèm theo một chuỗi secret (khóa bí mật)

Hoạt động:

1. Client sẽ gửi thông tin đăng nhập hợp lệ cho phía server.
2. Server sau khi xác thực được người dùng sẽ gửi về cho client một token.
3. Client sẽ lưu token này ở phía mình, với từng yêu cầu xác thực tiếp theo client sẽ cần gửi token về server.
4. Tại đây server sẽ decode token, và lấy thông tin người dùng ở phần payload. Sao khi xác thực xong nó thực hiện yêu cầu và gửi phản hồi về cho client.

Ưu điểm:

- Vì token được lưu ở client nên nó sẽ giảm chi phí cho server. Đồng thời cũng thuận lợi cho phát triển ứng dụng di động vì nó có thể lưu token ở AsyncStorage.
- Phù hợp với kiến trúc RESTful API và Single-Page-Application.

Khuyết điểm

- Vẫn có thể bị tấn công XSS (vào localStorage) hay CSRF (vào cookie).
- Các token không thể xoá mà chỉ có thể hết hạn, nên cần thiết lập thời hạn token ở mức ngắn (để tránh tình trạng kẻ xấu lấy được token và làm bậy)

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.

Mỗi mã OTP chỉ có thể sử dụng một lần, và chúng hết hạn sau một khoảng thời gian ngắn. Vì có lớp bảo mật bổ sung nên OTP thường được dùng cho các dữ liệu nhạy cảm như các giao dịch online.

Hình 1.11 Xác thực dựa trên mật khẩu một lần

Hoạt động:

1. Người dùng yêu cầu đăng nhập vào tài khoản.
2. Hệ thống tạo một mã OTP duy nhất và gửi nó đến người dùng thông qua một kênh riêng biệt, chẳng hạn như tin nhắn văn bản, ứng dụng di động hoặc email.
3. Người dùng nhập mã OTP vào trang đăng nhập.
4. Hệ thống so sánh mã OTP được nhập với mã OTP được tạo ra bởi hệ thống. Nếu hai mã khớp nhau, người dùng được cho phép truy cập vào tài khoản.

Ưu điểm:

- Tăng cường bảo mật: OTP giúp bảo vệ tài khoản của người dùng khỏi các cuộc tấn công mạng, vì kẻ tấn công không thể đoán được OTP và chỉ có thể sử dụng nó trong một khoảng thời gian ngắn.
- Dễ sử dụng: OTP dễ sử dụng và không yêu cầu người dùng cài đặt phần mềm hoặc thiết bị đặc biệt.
- Tiết kiệm chi phí: OTP là giải pháp bảo mật tương đối tiết kiệm chi phí so với các giải pháp khác như thẻ thông minh hoặc mã thông báo bảo mật.

Nhược điểm:

- Phụ thuộc vào kết nối mạng: OTP được gửi qua tin nhắn SMS, email hoặc ứng dụng di động, vì vậy người dùng cần có kết nối mạng để nhận OTP.
- Có thể bị đánh cắp: OTP có thể bị đánh cắp nếu kẻ tấn công có quyền truy cập vào điện thoại di động hoặc email của người dùng.
- Khó khăn cho người dùng không có điện thoại thông minh: OTP có thể khó khăn cho người dùng không có điện thoại thông minh hoặc không có kết nối mạng.

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 :

Tính phức tạp:

Số lượng tài nguyên: Hệ thống IT ngày càng có nhiều ứng dụng, dịch vụ và thiết bị. Việc quản lý xác thực và quyền truy cập cho từng tài nguyên là một quá trình thủ công tốn thời gian và dễ xảy ra lỗi.

Tính đa dạng: Hệ thống sử dụng nhiều loại phương thức xác thực khác nhau (mật khẩu, sinh trắc học, token,...) và mô hình ủy quyền (dựa trên vai trò, thuộc tính,...). Việc quản lý đồng bộ các phương thức và mô hình này gây khó khăn cho người dùng và quản trị viên.

Bảo mật:

Nguy cơ tấn công: Hệ thống luôn đối mặt với nguy cơ tấn công mạng tinh vi, nhắm vào lỗ hổng trong quản lý xác thực và quyền truy cập.

Quản lý mật khẩu: Mật khẩu là phương thức xác thực phổ biến nhưng dễ bị tấn công. Việc quản lý mật khẩu hiệu quả (tạo mật khẩu mạnh, thay đổi mật khẩu thường xuyên,...) là một thách thức lớn.

Tuân thủ:

Quy định và tiêu chuẩn: Các tổ chức phải tuân thủ nhiều quy định và tiêu chuẩn về bảo mật dữ liệu (GDPR, HIPAA,...) yêu cầu các biện pháp kiểm soát xác thực và quyền truy cập chặt chẽ.

Chứng minh tuân thủ: Việc thu thập và lưu trữ bằng chứng để chứng minh tuân thủ các quy định là một quá trình phức tạp và tốn kém.

Chi phí:

Triển khai giải pháp: Việc triển khai các giải pháp quản lý xác thực và quyền truy cập chuyên dụng có thể tốn kém, đặc biệt cho các tổ chức nhỏ và vừa.

Đào tạo nhân viên: Việc đào tạo nhân viên về các biện pháp bảo mật tốt nhất cũng cần đầu tư thời gian và chi phí.

Tiện lợi cho người dùng:

Tính dễ sử dụng: Các giải pháp xác thực và quyền truy cập cần có giao diện thân thiện, dễ sử dụng cho người dùng.

Cân bằng bảo mật và tiện lợi: Việc tăng cường bảo mật thường đi kèm với sự giảm tiện lợi cho người dùng. Việc tìm kiếm sự cân bằng giữa hai yếu tố này là một thách thức.

1.4. Kết luận chương 1

Chương này đã cung cấp một cái nhìn sâu sắc về xác thực và ủy quyền trong bảo mật thông tin, hai yếu tố không thể tách rời trong việc đảm bảo tính an toàn và đáng tin cậy của các hệ thống thông tin. Xác thực, như chúng ta đã thấy, là cốt lõi của việc xác định danh tính người dùng, từ các phương pháp truyền thống như mật khẩu đến những phương pháp tiên tiến như xác thực đa yếu tố và sinh trắc học. Mỗi phương pháp có ưu và nhược điểm riêng, phản ánh sự cần thiết của việc cân nhắc kỹ lưỡng trong việc chọn lựa và triển khai.

Ủy quyền, mặt khác, xác định phạm vi và mức độ truy cập mà người dùng được cấp. Thách thức ở đây là làm thế nào để cân bằng giữa việc cấp quyền truy cập cần thiết cho người dùng để thực hiện công việc của họ một cách hiệu quả và việc hạn chế quyền truy cập để giảm thiểu rủi ro an ninh. Các chiến lược như tối thiểu hóa quyền truy cập và quyền truy cập dựa trên vai trò là những cách tiếp cận phổ biến trong việc quản lý ủy quyền.

Những nỗ lực trong việc xây dựng và duy trì các hệ thống xác thực và ủy quyền đáng tin cậy không chỉ giúp bảo vệ thông tin từ các mối đe dọa bên ngoài mà còn từ các nguy cơ tiềm ẩn bên trong. Điều này càng trở nên quan trọng trong bối cảnh ngày càng có nhiều dữ liệu nhạy cảm và quan trọng được xử lý và lưu trữ trực tuyến.

Qua đó, chúng ta thấy rằng việc quản lý xác thực và ủy quyền đòi hỏi một sự hiểu biết sâu sắc về cả công nghệ và chính sách bảo mật. Điều này không chỉ cần thiết cho việc bảo vệ thông tin mà còn cho sự phát triển và tích hợp của các hệ thống thông tin trong tương lai. Vì vậy, chương này không chỉ cung cấp một nền tảng lý thuyết mà còn mở ra những hướng tiếp cận thực tiễn trong việc giải quyết các thách thức liên quan đến xác thực và ủy quyền trong thế giới kỹ thuật số hiện đại.

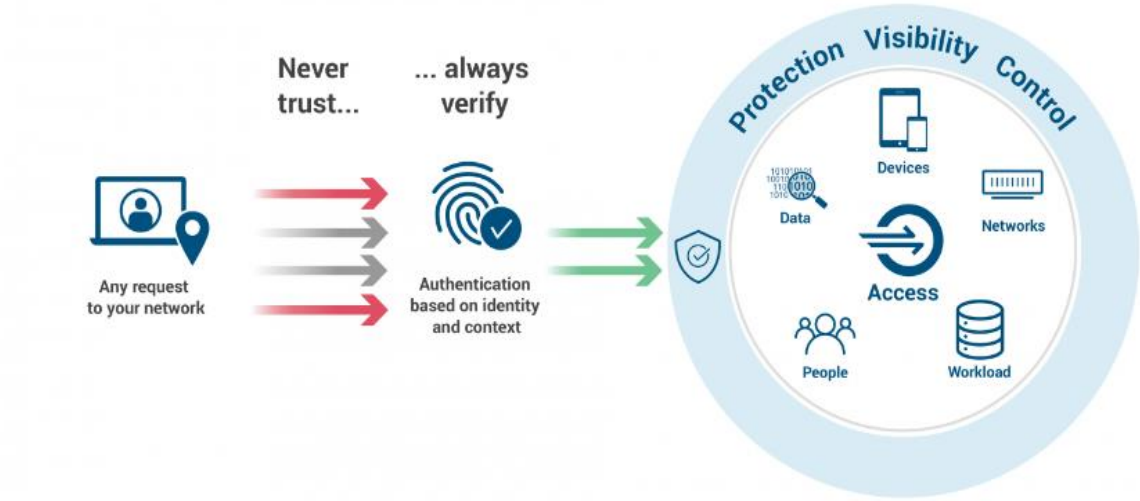
CHƯƠNG 2: TÌM HIỂU ZERO TRUST

2.1. Tổng quan về Zero Trust

Zero Trust là một mô hình quản lý an ninh mạng mới mẻ, đặt sự chú trọng vào việc kiểm soát truy cập vào hệ thống mạng một cách nghiêm ngặt. Theo đó, mô hình này không tin tưởng vào bất kỳ ai hoặc bất kỳ thiết bị nào trong mạng, ngay cả khi chúng đã được xác thực. Ý tưởng cơ bản của Zero Trust là tất cả các yếu tố trong mạng đều phải được xem xét và xác minh trước khi được cấp quyền truy cập vào tài nguyên.

Với mô hình bảo mật truyền thống, mạng được chia thành các phân đoạn, và người dùng được cấp quyền truy cập vào toàn bộ mạng hoặc phân đoạn cụ thể. Mô hình này dựa trên giả định rằng tất cả người dùng bên trong mạng đều được tin cậy. Tuy nhiên, giả định này không còn đúng trong thời đại hiện nay, khi mà các mối đe dọa mạng ngày càng tinh vi và phức tạp.

Mô hình Zero Trust ra đời nhằm đối phó với nguy cơ an ninh mạng ngày càng phức tạp, từ việc tấn công mạng từ bên trong đến các cuộc tấn công từ bên ngoài nhắm vào các điểm yếu của hệ thống. Trong bối cảnh môi trường kinh doanh ngày nay, nơi mà dữ liệu và ứng dụng được lưu trữ và truy cập từ mọi nơi, Zero Trust trở thành một phương pháp hiệu quả để bảo vệ hệ thống mạng, đồng thời giúp doanh nghiệp đáp ứng các yêu cầu về tuân thủ quy định và bảo vệ thông tin cá nhân.



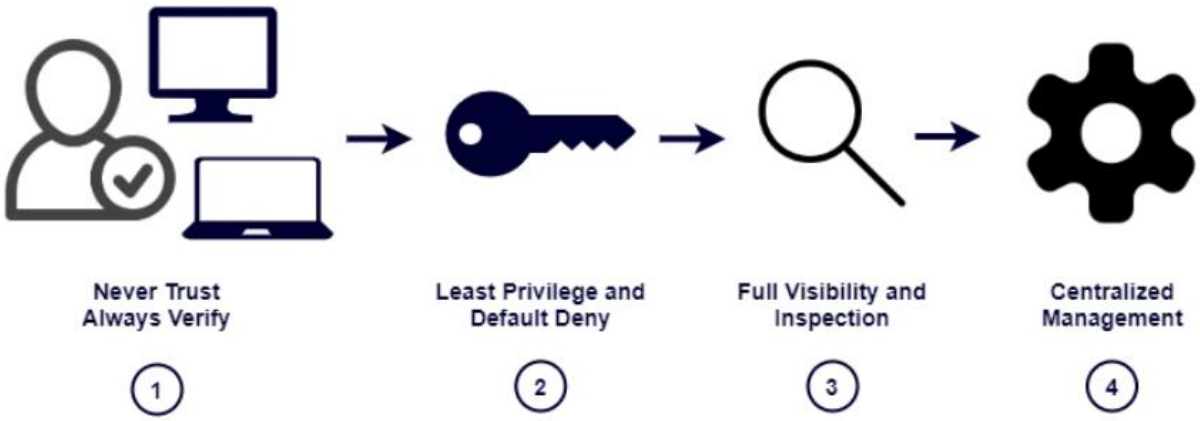
Hình 2.1 Khái niệm Zero Trust

2.1.1. Nguyên tắc hoạt động của Zero Trust

Nguyên tắc hoạt động của Zero Trust là một phương pháp an ninh mạng tiên tiến, trong đó mọi yếu tố trong mạng đều được xem xét và xác minh một cách cẩn

thận, không tin tưởng vào bất kỳ yếu tố nào mặc định. Zero Trust đặt sự chú trọng vào việc kiểm soát quyền truy cập và xác thực người dùng, thiết bị, ứng dụng và dữ liệu trong môi trường mạng. Điều này đòi hỏi việc áp dụng các phương pháp bảo mật nghiêm ngặt để đảm bảo rằng chỉ những người dùng được ủy quyền và thiết bị được tin cậy mới có thể truy cập vào các tài nguyên mạng quan trọng.

Mô hình Zero Trust hoạt động theo nguyên tắc "Không có ai đáng tin cậy" và tập trung vào việc xác thực và kiểm tra tính hợp lệ của từng yêu cầu truy cập để bảo vệ hệ thống thông tin. Hình 2.2 mô tả các nguyên tắc hoạt động chính của mô hình Zero Trust:



Hình 2.2 Nguyên tắc hoạt động của Zero Trust

2.1.1.1. Không bao giờ tin tưởng. luôn luôn xác minh

Trong mô hình Zero Trust, nguyên tắc "Không bao giờ tin tưởng. luôn luôn xác minh" phản đối quan niệm an ninh mạng truyền thống dựa trên sự bảo vệ biên giới của mạng. Nguyên tắc này đề cao việc kiểm tra liên tục và không phụ thuộc vào vị trí mạng hay quá khứ xác minh của người dùng hoặc thiết bị. Mọi yêu cầu truy cập đều phải được xác thực một cách cẩn trọng, dù là từ bên trong hay bên ngoài mạng của tổ chức. Việc áp dụng nguyên tắc này đòi hỏi việc triển khai một loạt các biện pháp kiểm soát và xác thực an ninh. Cụ thể:

- Xác Thực Đa Yếu Tố (MFA): Mỗi lần đăng nhập, người dùng phải chứng minh danh tính thông qua nhiều phương thức khác nhau, chẳng hạn như mật khẩu, mã OTP, hoặc sinh trắc học.
- Kiểm Tra Ngữ Cảnh Đăng Nhập: Xác minh ngữ cảnh đăng nhập bao gồm thời gian, địa điểm, và thiết bị sử dụng, để đánh giá mức độ rủi ro liên quan đến mỗi yêu cầu truy cập.
- Phân Tích Hành Vi Người Dùng: Sử dụng AI và học máy để phân tích mẫu hành vi và phát hiện bất kỳ dấu hiệu bất thường nào có thể chỉ ra nguy cơ an ninh.

- Kiểm Tra Liên Tục: Thay vì chỉ xác thực tại điểm đầu cuối, hệ thống cần tiến hành kiểm tra liên tục trong suốt phiên làm việc để đảm bảo rằng người dùng vẫn là người được ủy quyền.

2.1.1.2. Quyền hạn tối thiểu và chính sách từ chối mặc định

Trong mô hình Zero Trust, nguyên tắc "Quyền hạn tối thiểu và chính sách từ chối mặc định" (Least Privilege and Default Deny) là một tiêu chuẩn an ninh quan trọng. "Least Privilege" yêu cầu rằng mỗi người dùng chỉ nên có đúng những quyền cần thiết để thực hiện công việc của họ, không hơn. Điều này hạn chế khả năng của kẻ tấn công khi cố gắng sử dụng tài khoản bị xâm phạm để truy cập vào các phần không liên quan của hệ thống. "Default Deny" thì làm cho việc truy cập bất kỳ tài nguyên nào không được cấp phép trước là không thể.

Để áp dụng nguyên tắc này, tổ chức cần xác định rõ các vai trò công việc và tài nguyên mà mỗi vai trò đó cần truy cập. Các quy tắc truy cập nên được thiết lập dựa trên phân tích kỹ lưỡng về nhu cầu thực tế và tiềm năng an ninh mạng. Việc này yêu cầu sự hiểu biết sâu sắc về các quy trình nội bộ và cách thức làm việc của tổ chức.

Các hệ thống quản lý quyền truy cập nâng cao như Identity and Access Management (IAM) và Privileged Access Management (PAM) sẽ giúp tự động hóa quá trình cấp quyền và theo dõi quyền truy cập hiện hành. Một chính sách "Default Deny" đòi hỏi mọi quyền truy cập phải được duyệt qua một quá trình xác minh và phê duyệt nghiêm ngặt trước khi được cấp phép.

Việc triển khai nguyên tắc này đôi khi cũng đối mặt với thách thức, bao gồm khó khăn trong việc xác định và duy trì các mức độ quyền truy cập chính xác cho người dùng đa dạng và đôi khi cần sự phản hồi nhanh chóng trong môi trường làm việc linh hoạt. Điều này đòi hỏi các hệ thống phải có khả năng thích nghi nhanh chóng và chính xác với thay đổi về người dùng và nhu cầu của họ.

Ngoài ra, việc duy trì một chính sách "Default Deny" cần sự cân nhắc kỹ lưỡng để không làm giảm hiệu suất làm việc của nhân viên với những ràng buộc không cần thiết. Các tổ chức cần cân nhắc giữa việc bảo vệ tài nguyên và duy trì năng suất làm việc của nhân viên.

Tóm lại, "Least Privilege and Default Deny" là nguyên tắc cốt lõi trong Zero Trust, giúp cải thiện an ninh thông tin mạng nhưng cũng đòi hỏi sự quản lý chặt chẽ và khả năng thích ứng cao từ các tổ chức để có thể triển khai một cách hiệu quả.

2.1.1.3. Giám sát và kiểm tra toàn diện

Giám sát và kiểm tra toàn diện (Full Visibility and Inspection) đóng vai trò then chốt trong mô hình Zero Trust, cho phép theo dõi và kiểm tra mọi hoạt động trong hệ thống để phát hiện và ngăn chặn các mối đe dọa an ninh mạng. Việc triển

khai hiệu quả khả năng này giúp nâng cao đáng kể mức độ bảo mật và khả năng kiểm soát của hệ thống.

Mục tiêu

- Thu thập dữ liệu đầy đủ về tất cả các hoạt động trong hệ thống, bao gồm truy cập người dùng, hoạt động ứng dụng, lưu lượng mạng và các thay đổi cấu hình.
- Phân tích dữ liệu thu thập được để phát hiện các hành vi bất thường và các mối đe dọa tiềm ẩn.
- Ngăn chặn các hành vi truy cập trái phép, lạm dụng dữ liệu và các cuộc tấn công mạng.

Một số công nghệ quan trọng được sử dụng :

Giám sát lưu lượng mạng:

- Firewalls thế hệ tiếp theo (NGFW): NGFW cung cấp khả năng giám sát và kiểm tra lưu lượng mạng tiên tiến hơn so với firewalls truyền thống. NGFW có thể phân tích sâu hơn các gói tin, xác định các ứng dụng và giao thức cụ thể, và áp dụng các chính sách bảo mật phù hợp.
- Hệ thống phát hiện xâm nhập (IDS): IDS theo dõi lưu lượng mạng để phát hiện các hoạt động đáng ngờ có thể là dấu hiệu của một cuộc tấn công mạng. IDS có thể sử dụng nhiều phương pháp khác nhau để phát hiện các mối đe dọa, bao gồm phân tích chữ ký, phân tích hành vi và học máy.
- Hệ thống ngăn chặn xâm nhập (IPS): IPS hoạt động tương tự như IDS, nhưng có khả năng ngăn chặn các hoạt động đáng ngờ trước khi chúng gây hại. IPS có thể tự động chặn các gói tin nguy hiểm hoặc gửi cảnh báo đến quản trị viên để xử lý.

Giám sát hệ thống:

- Hệ thống quản lý thông tin và sự kiện bảo mật (SIEM): SIEM thu thập dữ liệu nhật ký từ các hệ thống khác nhau trong hệ thống mạng và lưu trữ chúng ở một nơi tập trung. SIEM có thể phân tích dữ liệu nhật ký để phát hiện các mối đe dọa, chẳng hạn như các cuộc tấn công mạng hoặc các hành vi truy cập trái phép.
- Hệ thống dàn xếp, tự động hóa và phản ứng bảo mật (SOAR): SOAR tự động hóa các quy trình phản ứng bảo mật bằng cách kết hợp dữ liệu từ SIEM và các công cụ bảo mật khác. SOAR có thể tự động thực hiện các hành động như cách ly các thiết bị bị nhiễm virus, chặn các địa chỉ IP nguy hiểm hoặc gửi cảnh báo đến quản trị viên.

Giám sát người dùng:

- Hệ thống quản lý truy cập và danh tính (IAM): IAM kiểm soát truy cập vào hệ thống và tài nguyên bằng cách xác minh danh tính người dùng và cấp quyền truy cập phù hợp. IAM có thể sử dụng nhiều phương pháp xác thực khác nhau, bao gồm mật khẩu, mã OTP và xác thực sinh trắc học.
- Hệ thống phát hiện hành vi bất thường của người dùng (UBA): UBA theo dõi hành vi của người dùng để phát hiện các hành vi bất thường có thể là dấu hiệu của một cuộc tấn công mạng hoặc lạm dụng dữ liệu. UBA có thể sử dụng nhiều phương pháp khác nhau để phát hiện các mối đe dọa, bao gồm phân tích thống kê, học máy và phân tích mạng xã hội.

2.1.1.4. Quản lý tập trung

Quản lý tập trung là một nguyên tắc cốt lõi trong mô hình Zero Trust, đóng vai trò thiết yếu trong việc đơn giản hóa và nâng cao hiệu quả bảo mật. Nó tập trung vào việc quản lý tất cả các khía cạnh bảo mật Zero Trust từ một vị trí trung tâm, giúp củng cố khả năng kiểm soát, khả năng hiển thị và tính nhất quán trong việc thực thi chính sách.

Mục tiêu:

- Cung cấp điểm quản lý duy nhất cho tất cả chính sách bảo mật Zero Trust.
- Giảm thiểu sự phức tạp và chi phí vận hành.
- Nâng cao khả năng kiểm soát và khả năng hiển thị toàn diện các hoạt động bảo mật.
- Đảm bảo tính nhất quán trong việc thực thi chính sách, giảm thiểu rủi ro và lỗ hổng.

Thành phần chính:

Hệ thống quản lý chính sách:

- Lưu trữ và quản lý tập trung các chính sách truy cập, xác thực và ủy quyền.
- Sử dụng cơ sở dữ liệu, giao diện người dùng, công cụ kiểm tra và phân tích để đảm bảo tính hợp lệ, nhất quán và hiệu quả của chính sách.

Hệ thống quản lý danh tính:

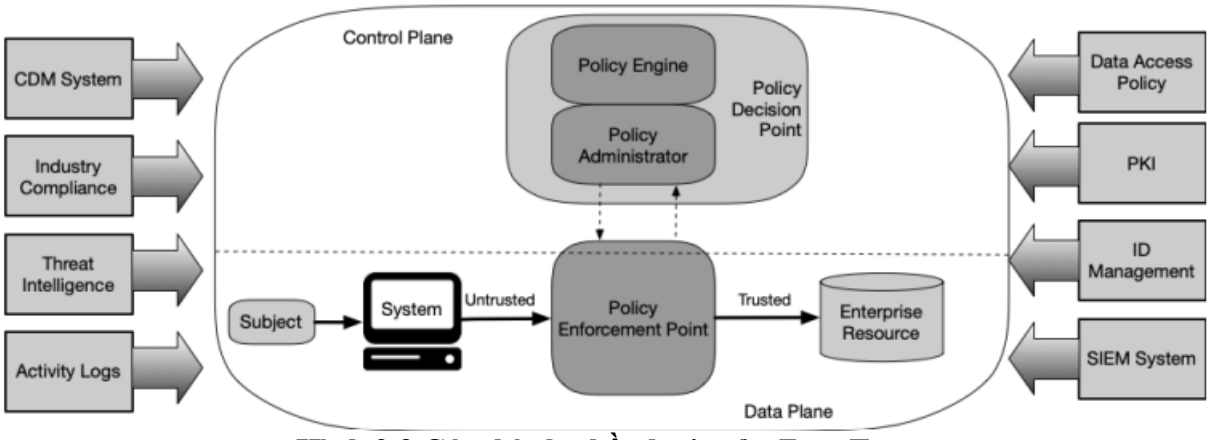
- Quản lý danh tính của tất cả người dùng, thiết bị và ứng dụng trong hệ thống.
- Sử dụng cơ sở dữ liệu danh tính, hệ thống xác thực, ủy quyền và quản lý vòng đời danh tính để đảm bảo bảo mật và truy cập hợp lý.

Hệ thống giám sát và báo cáo:

- Thu thập dữ liệu từ các hệ thống Zero Trust, cung cấp khả năng hiển thị và báo cáo toàn diện.
- Sử dụng công cụ thu thập dữ liệu, phân tích dữ liệu và báo cáo để phát hiện sớm các mối đe dọa, vi phạm và cải thiện hiệu quả bảo mật.

2.1.2. Các thành phần logic của Zero Trust

Mô hình Zero Trust trong doanh nghiệp bao gồm nhiều thành phần logic, hoạt động qua dịch vụ tại chỗ hoặc dịch vụ đám mây. Các thành phần logic của Zero Trust sử dụng một mặt phẳng điều khiển riêng để giao tiếp, trong khi dữ liệu ứng dụng được truyền đạt trên mặt phẳng dữ liệu. Hình 2.3 mô tả các thành phần logic của Zero Trust [3]:



Hình 2.3 Các thành phần logic của Zero Trust

Cơ chế chính sách (PE): Thành phần quan trọng nhất, chịu trách nhiệm ra quyết định cuối cùng về việc cấp quyền truy cập cho một người dùng (subject) đối với một tài nguyên. PE sử dụng chính sách của doanh nghiệp, kết hợp với dữ liệu từ các nguồn bên để chạy qua thuật toán tin cậy và quyết định cho phép, từ chối hoặc thu hồi quyền truy cập.

Quản trị chính sách (PA): Chịu trách nhiệm thiết lập và/hoặc đóng đường truyền thông giữa người dùng và tài nguyên (thông qua lệnh gửi cho các PEP liên quan). PA tạo ra bất kỳ xác thực cụ thể cho phiên và mã thông báo xác thực được dùng để truy cập tài nguyên. PA phụ thuộc chặt chẽ vào PE và dựa trên quyết định của nó để cho phép hoặc từ chối phiên.

Điểm thực thi chính sách (PEP): Hệ thống này chịu trách nhiệm cho việc kích hoạt, giám sát, và cuối cùng chấm dứt kết nối giữa một đối tượng và tài nguyên doanh nghiệp. PEP giao tiếp với PA để chuyển tiếp yêu cầu và/hoặc nhận cập nhật chính sách từ PA

Ngoài các thành phần cốt lõi, ZTA còn dựa vào nhiều nguồn dữ liệu để cung cấp thông tin và quy tắc chính sách cho PE khi đưa ra quyết định truy cập. Các nguồn này bao gồm:

- Hệ thống chẩn đoán và giảm thiểu liên tục (CDM): Cung cấp thông tin về trạng thái hiện tại của tài sản doanh nghiệp và áp dụng các bản cập nhật cho cấu hình và phần mềm.
- Hệ thống tuân thủ quy định ngành: Đảm bảo doanh nghiệp tuân thủ các quy định liên quan (ví dụ: FISMA, an ninh thông tin trong ngành y tế hoặc tài chính).
- Nguồn cung cấp thông tin về mối đe dọa: Cung cấp thông tin từ các nguồn bên trong hoặc bên ngoài để hỗ trợ PE đưa ra quyết định truy cập.
- Nhật ký hoạt động mạng và hệ thống: Cung cấp phản hồi theo thời gian thực (hoặc gần thời gian thực) về tình trạng bảo mật của hệ thống thông tin doanh nghiệp.
- Chính sách truy cập dữ liệu: Quy định về thuộc tính, quy tắc và chính sách truy cập tài nguyên doanh nghiệp.
- Cơ sở hạ tầng khóa công khai doanh nghiệp (PKI): Quản lý việc tạo và ghi nhật các chứng chỉ được cấp cho tài nguyên, người dùng, dịch vụ và ứng dụng.
- Hệ thống quản lý ID: Chịu trách nhiệm tạo, lưu trữ và quản lý tài khoản người dùng và hồ sơ nhận dạng.

2.1.3. Triển khai mô hình Zero Trust

Mô hình Zero Trust dựa trên khái niệm "Không tin tưởng ai theo mặc định". Thay vì chỉ triển khai các biện pháp bảo mật ở biên giới mạng, mô hình này tập trung vào việc đưa các biện pháp bảo mật đến gần nhất với bề mặt thực tế cần được bảo vệ. Điều này bao gồm việc tăng cường xác thực người dùng và xác nhận thiết bị trên mạng.

Mô hình Zero Trust không chỉ đơn thuần là việc cài đặt công nghệ, nó còn là một thay đổi về cách tiếp cận trong quản lý và bảo vệ thông tin. Bằng cách loại bỏ giả định rằng mọi thứ bên trong mạng đều an toàn, Zero Trust yêu cầu một cách tiếp cận nghiêm ngặt hơn, trong đó mọi yêu cầu truy cập - dù từ bên trong hay bên ngoài mạng - đều phải được xác thực và kiểm soát một cách cẩn thận.

Để triển khai mô hình Zero Trust trong tổ chức của bạn, các bước sau đây nên được tuân theo [6]:

1. *Xác Định và Phân Đoạn Dữ Liệu*

Bước đầu tiên trong việc triển khai Zero Trust là xác định và phân loại dữ liệu. Điều này bao gồm việc xác định dữ liệu nào là nhạy cảm và cần được bảo vệ nghiêm ngặt. Sau đó, sử dụng micro-segmentation để chia nhỏ chu vi bảo mật thành các khu vực nhỏ, từ đó cho phép truy cập độc lập vào các khu vực khác nhau của mạng. Điều này đảm bảo rằng quyền truy cập vào một khu vực không tự động mở ra quyền truy cập vào khu vực khác.

2. *Triển Khai Xác Thực Đa Yếu Tố (MFA)*

MFA là một phần không thể thiếu của mô hình Zero Trust, bởi nó hỗ trợ nguyên tắc "không tin tưởng, luôn luôn xác minh". MFA yêu cầu người dùng phải cung cấp nhiều hình thức xác thực trước khi được cấp quyền truy cập. Các phương thức xác thực này bao gồm:

Kiến Thức: Như mật khẩu hoặc PIN.

Sở Hữu: Các vật thể như thẻ thông minh hoặc ATM.

Đặc Điểm Cá Nhân: Bao gồm sinh trắc học như dấu vân tay hoặc quét mống mắt.

3. *Áp Dụng Nguyên Tắc Quyền Hạn Tối Thiểu (PoLP)*

Nguyên tắc quyền hạn tối thiểu giúp giảm thiểu nguy cơ bị tấn công trong mạng bằng cách hạn chế quyền hạn của người dùng và quản trị viên. Việc áp dụng nguyên tắc này đối với các điểm cuối (endpoints) giúp ngăn chặn việc phần mềm độc hại (malware) lợi dụng quyền hạn cao để mở rộng quyền truy cập, cài đặt hoặc thực thi chương trình độc hại. Quyền truy cập đối với ứng dụng, hệ thống, quy trình và thiết bị nên được hạn chế chỉ với những quyền cần thiết để thực hiện các công việc đã được phê duyệt.

4. *Xác Thực Tất Cả Các Thiết Bị Điểm Cuối*

Trong mô hình Zero Trust, mọi thiết bị, dù là của người dùng hay thiết bị điểm cuối, đều cần phải qua quá trình xác thực nghiêm ngặt. Điều này được thực hiện bằng cách áp dụng các biện pháp quản lý và kiểm soát chặt chẽ dựa trên danh tính đối với mọi thiết bị điểm cuối. Điều này có nghĩa là mỗi thiết bị sử dụng để truy cập tài nguyên phải được đăng ký và xác minh danh tính trước khi có thể sử dụng.

2.1.4. Thách thức trong việc áp dụng mô hình Zero Trust

Dưới đây là các thách thức khi áp dụng mô hình Zero Trust :

Thách Thức Kỹ Thuật

Mô hình Zero Trust yêu cầu việc phân đoạn dữ liệu và tài nguyên (micro-segmentation) cũng như giám sát tất cả các hoạt động trong tổ chức. Tuy nhiên, hầu hết các hệ thống hiện tại không đáp ứng được yêu cầu về micro-segmentation của mô hình Zero Trust, gây ra khó khăn trong việc thực hiện.

Hệ Thống Lâu Đời (Legacy Systems)

Các hệ thống lâu đời thường không áp dụng nguyên tắc quyền hạn tối thiểu, và mô hình Zero Trust lại yêu cầu nhiều lớp xác thực khi người dùng cố gắng truy cập tài nguyên. Do đặc trưng của các hệ thống này, việc giám sát lưu lượng mạng gần như không thể do yêu cầu mã hóa cao của mô hình Zero Trust.

Công Nghệ Ngang Hàng (Peer-to-Peer Technologies)

Nhiều hệ thống, bao gồm cả hệ điều hành Windows và mạng lưới không dây dạng mesh, áp dụng mô hình ngang hàng (P2P), hoạt động một cách phi tập trung và phá vỡ mô hình micro-segmentation của Zero Trust.

Điện Toán Đám Mây Hỗn Hợp (Hybrid Cloud)

Mô hình micro-segmentation gặp vấn đề khi cả hai dịch vụ đám mây, tức là công cộng và riêng tư, làm việc cùng nhau và kết hợp để cung cấp một dịch vụ chung, điều này phá hủy mô hình Zero Trust.

Chuyển Đổi Từ Hệ Thống Tách Biệt Sang Trung Tâm Dữ Liệu

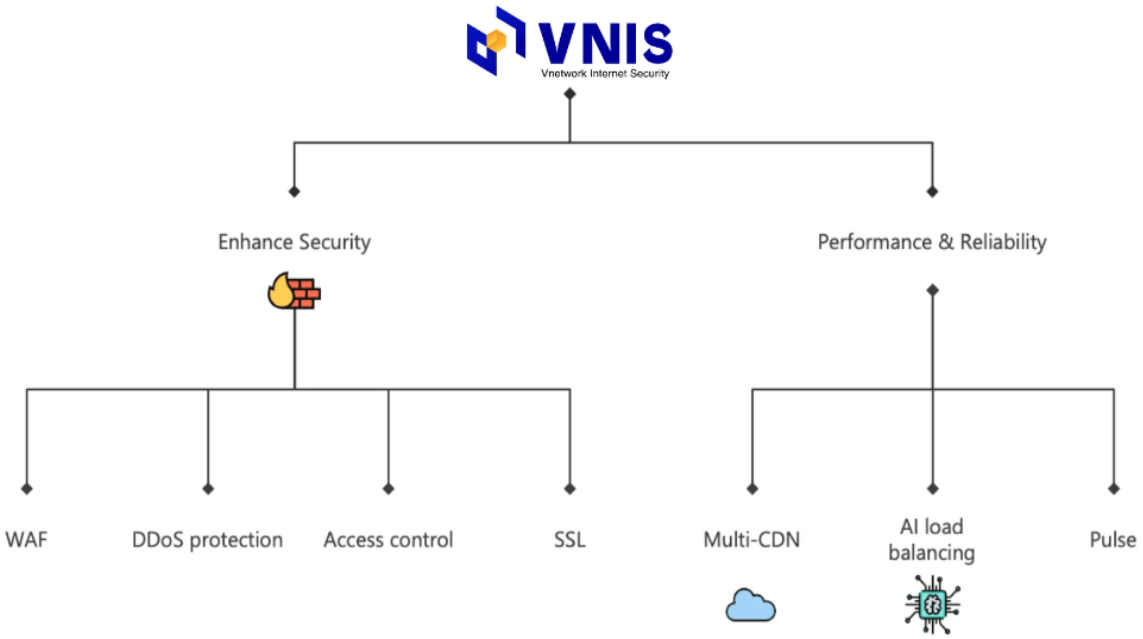
Đa số hệ thống đang sử dụng là hệ thống tách biệt chứa cả thông tin nhạy cảm và thông tin chung. Vì mô hình Zero Trust dựa hoàn toàn vào dữ liệu để xác thực và kiểm soát truy cập, việc phân đoạn hiệu quả trở nên cần thiết. Hiện tại, hầu hết các hệ thống yêu cầu một kiến trúc lớn hơn để đáp ứng được yêu cầu này.

Mô hình Zero Trust, với nguyên tắc cơ bản là "Không có ai đáng tin cậy", đang dần trở thành tiêu chuẩn vàng trong bảo mật mạng hiện đại. Tuy nhiên, trong quá trình áp dụng mô hình này, các tổ chức có thể đối mặt với nhiều thách thức và phức tạp. Những thách thức này không chỉ liên quan đến mặt kỹ thuật mà còn bao gồm cả vấn đề về hệ thống cũ (legacy systems), công nghệ ngang hàng, điện toán đám mây hỗn hợp, và sự chuyển đổi từ hệ thống dữ liệu tách biệt sang trung tâm dữ liệu. Hiểu rõ và giải quyết những thách thức này là bước quan trọng để áp dụng mô hình Zero Trust một cách hiệu quả.

2.1.5. Ứng dụng mô hình Zero Trust trong và ngoài nước

Trong nước:

Công ty VNETWORK: Để đảm bảo an ninh mạng hiệu quả, VNETWORK đã phát triển một giải pháp bảo mật tiên tiến dựa trên xu hướng Zero Trust với tên gọi VNIS (VNETWORK Internet Security) [9]. Mô hình VNIS dựa trên Zero Trust được VNETWORK triển khai như hình 2.4 dưới đây:



Hình 2.4 Mô hình VNIS

Web Application Firewall (WAF):

- Bảo vệ website khỏi các cuộc tấn công OWASP Top 10 và các lỗ hổng bảo mật web phổ biến khác.
- Ngăn chặn các bot độc hại và traffic truy cập bất thường.
- Cho phép tùy chỉnh các quy tắc bảo mật theo nhu cầu cụ thể của website.

Content Delivery Network (CDN):

- Tăng tốc độ tải trang web bằng cách phân phối nội dung tĩnh (như hình ảnh, JavaScript, CSS) từ các server gần nhất với người dùng.
- Giảm tải cho server web, giúp nâng cao hiệu suất và khả năng mở rộng.
- Bảo vệ website khỏi các cuộc tấn công DDoS.

Multi-Factor Authentication (MFA):

- Tăng cường bảo mật tài khoản người dùng bằng cách yêu cầu thêm một bước xác minh khi đăng nhập.
- Hỗ trợ nhiều phương thức xác minh khác nhau như OTP qua SMS, Google Authenticator, email.
- Giúp ngăn chặn các cuộc tấn công brute force và credential stuffing.

DDoS Protection:

- Bảo vệ website khỏi các cuộc tấn công DDoS ở tầng ứng dụng và tầng mạng.

- Hỗ trợ các công nghệ chống DDoS tiên tiến như machine learning và anomaly detection.
- Giúp đảm bảo website luôn hoạt động ổn định và sẵn sàng phục vụ người dùng.

Bot Management:

- Phân biệt bot tốt và bot xấu, ngăn chặn các bot độc hại truy cập website.
- Bảo vệ website khỏi các hoạt động scraping dữ liệu, spam, clickjacking.
- Tối ưu hóa trải nghiệm người dùng bằng cách chỉ cho phép bot có ích truy cập website.

Hoạt động của mô hình :

Người dùng truy cập hệ thống :

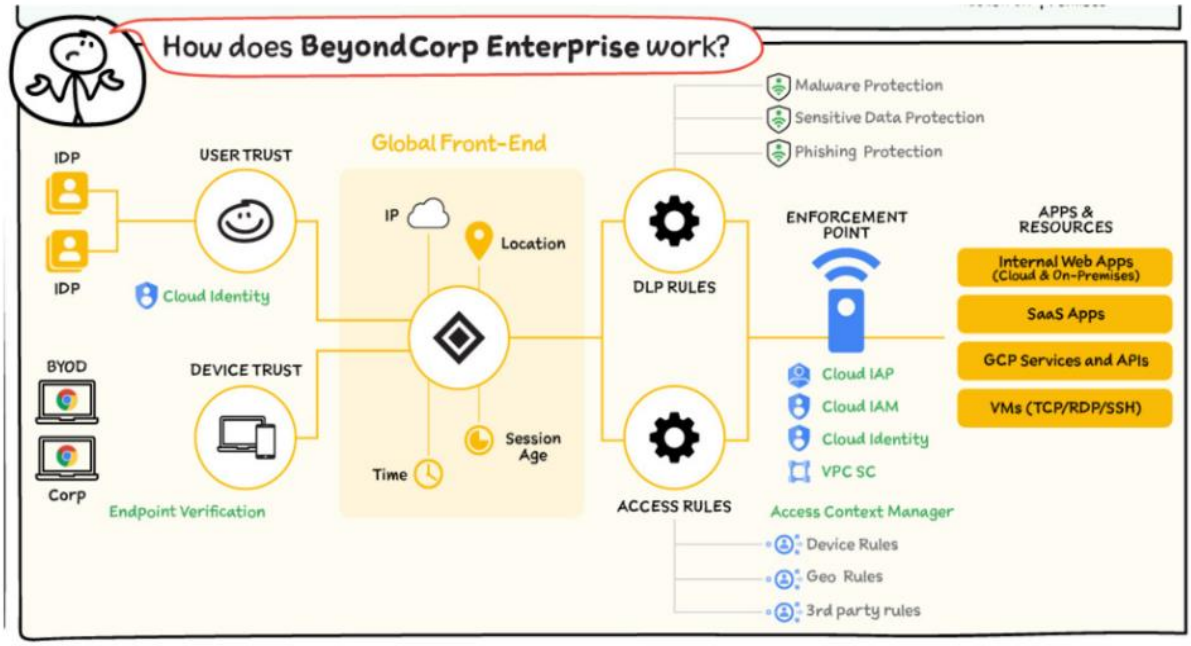
- Người dùng truy cập ứng dụng web thông qua mạng lưới được bảo vệ bởi WAF, DDoS protection, Multi-CDN.
- WAF kiểm tra các yêu cầu truy cập và ngăn chặn các tấn công web phổ biến.
- Multi-CDN giúp tăng tốc độ truy cập web và cải thiện trải nghiệm người dùng.
- Người dùng đăng nhập vào hệ thống bằng SSO và sử dụng MFA để xác thực nhằm đảm bảo bảo mật tài khoản.
- RBAC kiểm soát quyền truy cập của người dùng vào các tài nguyên hệ thống.

Giám sát và phân tích :

- Hệ thống giám sát và phân tích thu thập dữ liệu nhật ký từ các thành phần khác nhau trong mô hình.
- SIEM tổng hợp dữ liệu và phát hiện các hành vi bất thường.
- Các mối đe dọa tiềm ẩn được ngăn chặn và các sự cố bảo mật được xử lý kịp thời.

Ngoài nước:

Google : Google đã triển khai mô hình Zero Trust thông qua BeyondCorp Enterprise [8], đây là cách tiếp cận bảo mật mà họ đã phát triển. BeyondCorp chuyển từ mô hình bảo mật truyền thống dựa trên việc bảo vệ "biên giới mạng" sang mô hình không cần "biên giới" - nghĩa là không phân biệt giữa người dùng bên trong và bên ngoài mạng công ty. Mô hình BeyondCorp được Google triển khai như hình 2.5 dưới đây:



Hình 2.5 Mô hình BeyondCorp của Google

Xác thực người dùng : Người dùng được xác thực thông qua Identity Provider (IDP). Có thể sử dụng cả IDP doanh nghiệp hoặc IDP đám mây để đảm bảo rằng danh tính của người dùng được xác thực mạnh mẽ.

Xác thực thiết bị : Thiết bị, bao gồm cả thiết bị cá nhân và thiết bị do công ty cung cấp cần phải trải qua quá trình xác minh đầu cuối để đảm bảo rằng chúng đáp ứng các tiêu chuẩn an ninh của Google.

Giao diện toàn cầu : Đây là điểm kiểm soát truy cập, nơi mà thông tin như địa chỉ IP, vị trí, thời gian và tuổi của phiên đăng nhập (Session Age) được sử dụng để áp dụng các quy tắc DLP (Data Loss Prevention) và quy tắc truy cập, nhằm kiểm soát người dùng và thiết bị truy cập vào tài nguyên của công ty.

Điểm thực thi : Đây là nơi thực hiện các biện pháp bảo vệ như chống malware, bảo vệ dữ liệu nhạy cảm và chống phishing. Các quy tắc được thực thi ở đây đảm bảo rằng chỉ các yêu cầu truy cập đáng tin cậy mới có thể tiếp cận tài nguyên.

Ứng dụng và tài nguyên : Các ứng dụng nội bộ và SaaS cũng như dịch vụ và API của GCP (Google Cloud Platform) và máy ảo (VMs) được bảo vệ bởi mô hình Zero Trust. Truy cập đến các tài nguyên này được kiểm soát chặt chẽ dựa trên tin cậy người dùng và thiết bị, cũng như các điều kiện đặc biệt khác.

Quản lý ngữ cảnh truy cập : Quản lý ngữ cảnh truy cập cho phép Google cấu hình chính sách truy cập dựa trên một loạt các yếu tố như quy tắc thiết bị, quy tắc địa lý và quy tắc từ bên thứ ba.

Hoạt động của mô hình :

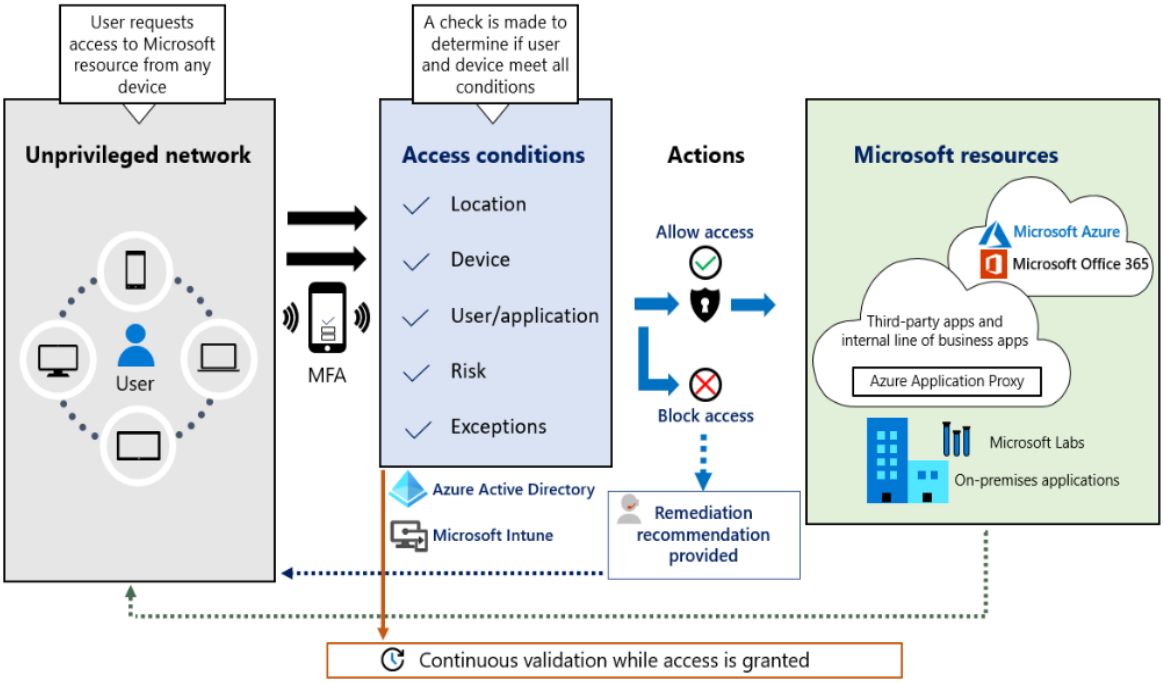
Người dùng truy cập hệ thống :

- Người dùng truy cập trang web BeyondCorp hoặc ứng dụng di động. BeyondCorp xác minh danh tính của người dùng bằng cách sử dụng MFA, chẳng hạn như : Xác minh SMS, Xác minh bằng ứng dụng Google Authenticator, Khóa bảo mật.
- BeyondCorp đánh giá rủi ro của thiết bị và mạng của người dùng bằng cách sử dụng các yếu tố sau: Hệ điều hành của thiết bị, Trình duyệt web, Cài đặt bảo mật, Vị trí mạng.
- BeyondCorp cấp quyền truy cập cho người dùng vào các tài nguyên mà họ cần, dựa trên chính sách truy cập được xác định trước. Chính sách truy cập có thể được cấu hình dựa trên các yếu tố sau: Vai trò của người dùng, Nhóm của người dùng, Vị trí của người dùng , Thiết bị của người dùng.

Quản trị hệ thống :

- Quản lý tài khoản:
  - Quản trị viên có thể tạo và quản lý tài khoản người dùng.
  - Quản trị viên có thể đặt lại mật khẩu, khóa tài khoản và xóa tài khoản.
- Cấu hình chính sách:
  - Quản trị viên có thể cấu hình chính sách truy cập cho các tài nguyên.
  - Chính sách truy cập có thể được cấu hình dựa trên các yếu tố sau: Loại tài nguyên, Vị trí tài nguyên, Độ nhạy của tài nguyên
- Quản lý thiết bị:
  - Quản trị viên có thể quản lý các thiết bị được phép truy cập vào BeyondCorp.
  - Quản trị viên có thể yêu cầu người dùng đăng ký thiết bị của họ với BeyondCorp.
  - Quản trị viên có thể xóa thiết bị khỏi BeyondCorp.
- Giám sát:
  - Quản trị viên có thể giám sát hoạt động của người dùng và hệ thống.
  - Quản trị viên có thể xem nhật ký truy cập, báo cáo và cảnh báo

Microsoft: Microsoft đã triển khai Zero Trust để bảo vệ hệ thống mạng và tài nguyên của Microsoft [7]. Mô hình Zero Trust được Microsoft triển khai như hình 2.5 dưới đây :



Hình 2.6 Kiến trúc Zero Trust của Microsoft

Xác thực danh tính :

- Tất cả người dùng, thiết bị và ứng dụng phải được xác thực trước khi có thể truy cập vào bất kỳ tài nguyên nào.
- Microsoft sử dụng nhiều phương pháp xác thực khác nhau, bao gồm tên người dùng và mật khẩu, MFA và xác thực sinh trắc học.
- Microsoft đã triển khai MFA cho tất cả người dùng, bao gồm cả người dùng truy cập từ bên ngoài mạng nội bộ. Microsoft đã chuyển từ xác thực bằng thẻ thông minh sang phương thức dựa trên điện thoại và ứng dụng Microsoft Azure Authenticator.

Xác minh thiết bị :

- Microsoft sử dụng device management để xác thực thiết bị. Device management cho phép Microsoft kiểm soát các thiết bị truy cập vào tài nguyên của họ, bao gồm các yếu tố như hệ điều hành, phiên bản phần mềm, cập nhật bảo mật và chính sách bảo mật.
- Microsoft đã triển khai device management cho tất cả các thiết bị của họ, bao gồm cả thiết bị được sở hữu bởi Microsoft và thiết bị được sở hữu bởi người dùng.

Xác minh truy cập :

- Quyền truy cập vào tài nguyên chỉ được cấp dựa trên các yếu tố như danh tính người dùng, danh tính thiết bị, vị trí và mức độ nhạy cảm của tài nguyên.
- Microsoft sử dụng phân quyền dựa trên thuộc tính để xác thực truy cập. Phân quyền dựa trên thuộc tính cho phép Microsoft kiểm soát quyền truy cập dựa trên các yếu tố này.
- Microsoft đã triển khai conditional access cho tất cả các ứng dụng và dịch vụ của họ, bao gồm cả Microsoft 365 và VPN.

Xác minh dịch vụ :

- Microsoft sử dụng các biện pháp bảo mật khác nhau để xác thực dịch vụ, bao gồm xác thực và ủy quyền, chứng nhận và khóa mã hóa.
- Microsoft đã triển khai các biện pháp bảo mật này cho tất cả các ứng dụng và dịch vụ của họ.

Hoạt động của mô hình :

- Người dùng yêu cầu truy cập vào tài nguyên của Microsoft từ bất kỳ thiết bị nào thông qua mạng không được ưu tiên.
- Trước khi cấp quyền truy cập, hệ thống thực hiện xác minh đa yếu tố để đảm bảo rằng yêu cầu đến từ người dùng hợp lệ.
- Hệ thống kiểm tra một loạt các điều kiện bao gồm vị trí, thiết bị, người dùng/ứng dụng, rủi ro và ngoại lệ để xác định xem liệu người dùng và thiết bị có đáp ứng tất cả các điều kiện cần thiết hay không.
- Dựa trên kết quả kiểm tra, hệ thống sẽ quyết định cấp hoặc chặn quyền truy cập. Nếu quyền truy cập bị chặn, hệ thống có thể cung cấp khuyến nghị để khắc phục vấn đề.
- Khi truy cập được cho phép, người dùng có thể truy cập vào các tài nguyên của Microsoft như Azure, Office 365, và các ứng dụng bên thứ ba cũng như các ứng dụng nội bộ thông qua Azure Application Proxy và các ứng dụng tại chỗ.
- Trong khi người dùng được cấp quyền truy cập, mô hình Zero Trust đòi hỏi việc xác minh liên tục để đảm bảo tính xác thực và an toàn của phiên làm việc.

Phân tích:

Việc triển khai Zero Trust mang lại nhiều lợi ích cho các tổ chức và doanh nghiệp, bao gồm:

- Nâng cao khả năng bảo mật: Zero Trust giúp giảm thiểu rủi ro truy cập trái phép và tấn công mạng.
- Tăng cường khả năng kiểm soát: Các tổ chức và doanh nghiệp có thể kiểm soát chặt chẽ hơn việc truy cập vào tài nguyên mạng.

- Cải thiện khả năng thích ứng: Zero Trust có thể dễ dàng điều chỉnh để phù hợp với nhu cầu thay đổi của các tổ chức và doanh nghiệp.

Tuy nhiên, việc triển khai Zero Trust cũng có một số thách thức, bao gồm:

- Chi phí triển khai: Việc triển khai Zero Trust có thể tốn kém, đặc biệt là đối với các tổ chức và doanh nghiệp có quy mô lớn.
- Khả năng tương thích: Việc triển khai Zero Trust có thể gặp khó khăn nếu các hệ thống và ứng dụng hiện có của tổ chức và doanh nghiệp không tương thích.
- Khả năng quản lý: Việc quản lý hệ thống Zero Trust có thể phức tạp, đòi hỏi đội ngũ nhân viên có chuyên môn cao.

2.2. Phân quyền quản lý trong Zero Trust

2.2.1. Phân quyền dựa trên danh tính (Identity-Based Access Control)

Trong mô hình Zero Trust, Identity-Based Access Control (IBAC) đóng một vai trò then chốt. IBAC dựa trên nguyên tắc rằng quyền truy cập được xác định dựa trên danh tính của người dùng hoặc thiết bị. Khác biệt với các hệ thống truyền thống nơi quyền truy cập thường dựa trên vị trí mạng, IBAC trong Zero Trust chú trọng vào việc xác minh danh tính của người dùng hoặc thiết bị như là tiêu chí chính để cấp quyền truy cập.

Phương pháp này cho phép hệ thống Zero Trust kiểm soát một cách chặt chẽ hơn người dùng nào được phép truy cập vào tài nguyên của mạng. Ví dụ, trong một môi trường doanh nghiệp, mỗi nhân viên có thể được cấp một danh tính số duy nhất, và dựa trên danh tính đó, hệ thống quyết định họ có quyền truy cập vào tài nguyên nào. Điều này giúp đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào dữ liệu và ứng dụng quan trọng.

Một yếu tố quan trọng khác của IBAC trong Zero Trust là khả năng theo dõi và kiểm soát liên tục. Trong môi trường ZTA, hệ thống không chỉ xác minh danh tính tại thời điểm truy cập ban đầu mà còn liên tục giám sát hành vi truy cập của người dùng. Điều này cho phép hệ thống phát hiện bất kỳ hành vi bất thường nào và điều chỉnh quyền truy cập một cách thích hợp, nâng cao đáng kể tính bảo mật của mạng.

Ưu điểm:

- Xác Thực Chính Xác: IBAC tập trung vào việc xác thực người dùng hoặc thiết bị dựa trên danh tính, tăng cường độ chính xác trong việc cấp quyền truy cập.
- Cải Thiện An Ninh: Bằng cách liên tục xác minh danh tính, IBAC giúp phát hiện và ngăn chặn các hành vi truy cập bất thường.
- Phù Hợp với Quy Định: Cung cấp khả năng tuân thủ các quy định bảo mật thông tin và quyền riêng tư.

Nhược điểm:

- Khả Năng Mở Rộng Hạn Chế: Việc xác thực dựa trên danh tính có thể trở nên phức tạp khi số lượng người dùng và thiết bị tăng lên.
- Quản Lý Phức Tạp: Cần phải duy trì và quản lý cơ sở dữ liệu danh tính một cách cẩn thận và liên tục cập nhật.
- Rủi Ro Tập Trung: Tập trung vào danh tính có thể tạo ra điểm yếu tập trung nếu cơ sở dữ liệu danh tính bị tấn công hoặc lợi dụng.

2.2.2. Phân quyền dựa trên vai trò (Role-Based Access Control)

Role-Based Access Control (RBAC) trong Zero Trust tập trung vào việc phân loại quyền truy cập dựa trên vai trò cụ thể của người dùng trong một tổ chức. Trong mô hình này, quyền truy cập không được xác định dựa trên danh tính cá nhân, mà dựa vào vai trò công việc. Điều này đơn giản hóa quản lý bảo mật bằng cách phân quyền dựa trên các nhóm nghề nghiệp, giúp tự động hóa việc cấp quyền và giảm rủi ro truy cập không đúng cách.

RBAC làm tăng cường bảo mật mạng bằng cách chỉ cho phép truy cập tài nguyên dựa trên nhu cầu công việc cụ thể. Ví dụ, nhân viên IT có quyền truy cập hệ thống khác với nhân viên kế toán. Quyền truy cập có thể được điều chỉnh dễ dàng khi có sự thay đổi trong vai trò hoặc trách nhiệm công việc, đảm bảo rằng người dùng chỉ có quyền truy cập vào những tài nguyên cần thiết cho công việc của họ. Điều này không chỉ giúp giảm thiểu rủi ro an ninh thông tin mà còn hỗ trợ việc tuân thủ chính sách bảo mật và quy định pháp lý.

Ưu điểm :

- Tăng cường an ninh : RBAC giúp ngăn chặn truy cập không phù hợp bằng cách chỉ cấp quyền dựa trên nhu cầu công việc cụ thể.
- Dễ dàng quản lý : Quản lý quyền truy cập trở nên dễ dàng hơn khi thay đổi vai trò hoặc trách nhiệm công việc của người dùng.
- Giảm rủi ro : Hạn chế quyền truy cập không cần thiết giúp giảm thiểu rủi ro an ninh thông tin.

Nhược điểm :

- Không đủ linh hoạt : RBAC có thể không đủ linh hoạt để đối phó với các tình huống phức tạp hoặc thay đổi nhanh chóng trong môi trường công việc.
- Quản lý vai trò phức tạp : Việc xác định và quản lý các vai trò có thể trở nên phức tạp trong các tổ chức lớn.
- Thách thức với người dùng đa vai trò : RBAC có thể gặp khó khăn trong việc quản lý người dùng đảm nhận nhiều vai trò khác nhau.

2.2.3. Phân quyền dựa trên thuộc tính (Attribute-Based Access Control)

Attribute-Based Access Control (ABAC) trong Zero Trust là một phương pháp linh hoạt và mạnh mẽ để quản lý quyền truy cập. ABAC sử dụng các thuộc tính của người dùng, thiết bị, và cả ngữ cảnh hoạt động để đưa ra quyết định về quyền truy cập. Khác biệt so với RBAC, ABAC không phụ thuộc vào vai trò cố định, mà xem xét một loạt các thuộc tính động để kiểm soát quyền truy cập một cách chi tiết hơn.

Trong mô hình Zero Trust, ABAC được sử dụng để xác định các thuộc tính của người dùng, thiết bị và tài nguyên. Các thuộc tính này có thể bao gồm:

- Thuộc tính của người dùng: tên người dùng, chức vụ, bộ phận, vị trí, IP, ….
- Thuộc tính của thiết bị: địa chỉ MAC, hệ điều hành, phiên bản phần mềm, ….
- Thuộc tính của tài nguyên: vị trí, ….

Khi người dùng xác thực trong mô hình Zero Trust, các thuộc tính của người dùng, thiết bị và tài nguyên sẽ được xác định. Các thuộc tính này sẽ được sử dụng để quyết định xem người dùng có được cấp quyền truy cập vào tài nguyên hay không. Điều này cho phép các tổ chức tạo ra các chính sách truy cập phù hợp và chính xác với các tình huống cụ thể, từ đó tăng cường an toàn và bảo mật thông tin. Ví dụ, trong ABAC, quyền truy cập có thể dựa trên vị trí địa lý, thời gian trong ngày, hoặc thậm chí trạng thái an ninh cụ thể của mạng. Điều này cho phép tổ chức áp dụng các chính sách bảo mật một cách tinh tế và phản ánh chính xác hơn các nhu cầu an ninh và kinh doanh.

Ưu điểm:

- Tính linh hoạt cao: ABAC cho phép điều chỉnh quyền truy cập dựa trên các thuộc tính động và đa dạng, tạo ra các chính sách truy cập tinh tế và phản ánh chính xác nhu cầu an ninh.
- Tính tùy chỉnh: Có thể tùy chỉnh chính sách truy cập cho từng trường hợp cụ thể, tăng cường khả năng bảo mật và sự phù hợp với yêu cầu kinh doanh.

Nhược điểm:

- Độ phức tạp cao: Quản lý và xử lý các chính sách truy cập trong ABAC có thể trở nên phức tạp do sự đa dạng của các thuộc tính và quy tắc.
- Yêu cầu tài nguyên: Việc triển khai ABAC đòi hỏi tài nguyên hệ thống và chuyên môn kỹ thuật cao hơn so với các phương pháp truyền thống.

2.2.4. Phân quyền dựa trên rủi ro (Risk-Based Access Control)

Risk-Based Access Control (RbAC) trong Zero Trust là một phương pháp tiếp cận độc đáo và hiệu quả trong việc quản lý quyền truy cập dựa trên đánh giá rủi ro. Trong RbAC, quyền truy cập được xác định không chỉ dựa trên danh tính hoặc vai trò mà còn dựa trên mức độ rủi ro liên quan đến người dùng hoặc hoạt động cụ thể.

RbAC tập trung vào việc đánh giá liên tục nguy cơ an ninh mạng và điều chỉnh quyền truy cập dựa trên mức độ rủi ro đó. Phương pháp này cho phép tổ chức phản ứng nhanh chóng với các mối đe dọa và thay đổi an ninh, đồng thời duy trì sự linh hoạt trong việc quản lý truy cập. RbAC đặc biệt hiệu quả trong việc giảm thiểu rủi ro bằng cách hạn chế quyền truy cập trong các tình huống có nguy cơ cao, nhưng vẫn cho phép truy cập khi rủi ro là thấp. Ví dụ, một doanh nghiệp có thể sử dụng RbAC để cho phép chỉ các nhân viên trong bộ phận tài chính truy cập vào dữ liệu tài chính, nhưng chỉ khi dữ liệu tài chính đang được truy cập từ bên trong văn phòng.

Trong mô hình Zero Trust, RbAC được sử dụng để xác định mức độ rủi ro của các tài nguyên. Mức độ rủi ro của các tài nguyên có thể được xác định dựa trên các yếu tố như:

- Tính nhạy cảm của dữ liệu: dữ liệu tài chính, dữ liệu khách hàng, dữ liệu bí mật.
- Tầm quan trọng của tài nguyên: hệ thống mạng, hệ thống ứng dụng, hệ thống cơ sở hạ tầng.
- Vị trí của tài nguyên: tài nguyên nội bộ, tài nguyên bên ngoài.

Ưu điểm :

- Tăng cường bảo mật: RbAC giúp ngăn chặn kẻ tấn công truy cập vào các tài nguyên nhạy cảm, ngay cả khi họ có thể giả mạo danh tính của một người dùng hợp pháp.
- Giảm rủi ro: RbAC giúp giảm rủi ro xảy ra các cuộc tấn công mạng.
- Tăng cường kiểm soát: RbAC giúp doanh nghiệp kiểm soát quyền truy cập vào các tài nguyên.

Nhược điểm :

- Độ phức tạp cao: Đòi hỏi khả năng phân tích dữ liệu phức tạp và đưa ra quyết định trong thời gian thực.
- Cần công nghệ tiên tiến: Việc triển khai RbAC có thể cần đến công nghệ học máy và trí tuệ nhân tạo để đánh giá rủi ro một cách chính xác.

2.2.5. Phân quyền dựa trên Blockchain (Blockchain-Based Access Control)

Blockchain-Based Access Control trong Zero Trust Architecture là một phương pháp tiên tiến và đổi mới. Sử dụng công nghệ blockchain, phương pháp này mang lại một cấp độ bảo mật cao và khả năng chống giả mạo cho quyền truy cập. BAC sử dụng blockchain để lưu trữ và quản lý các thông tin liên quan đến quyền truy cập, bao gồm:

- Các tài nguyên: dữ liệu, ứng dụng, hệ thống, ….
- Các người dùng: nhân viên, khách hàng, đối tác, ….

- Các quyền: quyền đọc, quyền ghi, quyền thực thi, ….

Trong mô hình Zero Trust, BAC được sử dụng để xác định các quyền truy cập của người dùng hoặc thiết bị. Các quyền truy cập của người dùng hoặc thiết bị được xác định dựa trên các thông tin được lưu trữ trên blockchain.

Khi người dùng hoặc thiết bị truy cập vào một tài nguyên, BAC sẽ xác minh các quyền truy cập của người dùng hoặc thiết bị đó. Nếu các quyền truy cập của người dùng hoặc thiết bị đáp ứng các yêu cầu truy cập vào tài nguyên, thì người dùng hoặc thiết bị sẽ được cấp quyền truy cập. Điều này giúp tăng cường độ tin cậy và tính minh bạch trong việc quản lý quyền truy cập. Ngoài ra, blockchain cho phép tự động hóa việc phân phối và quản lý quyền truy cập một cách an toàn, giảm thiểu nguy cơ rò rỉ thông tin hoặc truy cập trái phép. Ví dụ, một doanh nghiệp có thể sử dụng BAC để cho phép chỉ các nhân viên trong bộ phận tài chính truy cập vào dữ liệu tài chính. Các quyền truy cập của nhân viên trong bộ phận tài chính sẽ được lưu trữ trên blockchain. Khi một nhân viên trong bộ phận tài chính truy cập vào dữ liệu tài chính, BAC sẽ xác minh các quyền truy cập của nhân viên đó. Nếu nhân viên có các quyền truy cập cần thiết, thì nhân viên sẽ được cấp quyền truy cập vào dữ liệu tài chính.

Ưu điểm:

- Tính bảo mật cao: BAC cung cấp một cấp độ bảo mật cao thông qua việc sử dụng blockchain, làm cho dữ liệu không thể bị thay đổi và tăng tính minh bạch.
- Tự động hóa và phân tán: Blockchain cho phép tự động hóa việc phân phối quyền truy cập và quản lý một cách phân tán, giảm thiểu nguy cơ trung tâm hóa và rủi ro liên quan.

Nhược điểm:

- Yêu cầu công nghệ cao: Việc triển khai BAC đòi hỏi hạ tầng mạnh mẽ và kiến thức chuyên sâu về blockchain.
- Thách thức về tính khả thi: Việc triển khai có thể phức tạp và tốn kém, đặc biệt trong các môi trường có hạ tầng công nghệ thông tin hạn chế.

2.2.6. So sánh phân quyền trong mô hình Zero Trust và mô hình truyền thống

Sự khác biệt giữa mô hình Zero Trust và mô hình truyền thống về phân quyền là một trong những yếu tố cốt lõi phản ánh cách tiếp cận bảo mật của hai mô hình này. Dưới đây là một số điểm khác biệt chính:

Phân quyền :

- Mô hình truyền thống: Phân quyền thường dựa trên vai trò và vị trí trong mạng. Một khi đã được cấp quyền truy cập vào mạng, người dùng có thể truy cập

vào tài nguyên dựa trên vai trò hoặc nhóm mà họ thuộc về, thường là thông qua các danh sách kiểm soát truy cập (ACLs) tĩnh.

- Mô hình Zero Trust: Phân quyền dựa trên nguyên tắc tối thiểu quyền truy cập cần thiết và thường được thực hiện thông qua quản lý quyền truy cập dựa trên vai trò (RBAC) hoặc quản lý quyền truy cập dựa trên chính sách (PBAC). Mỗi yêu cầu truy cập đều được đánh giá dựa trên ngữ cảnh, bao gồm người dùng, thiết bị, vị trí, và mức độ rủi ro; và quyền truy cập chỉ được cấp khi cần thiết cho công việc cụ thể.

Tính linh hoạt :

- Mô hình truyền thống: Các quyền truy cập thường được cấp một cách tĩnh và không thường xuyên được điều chỉnh dựa trên thay đổi trong vai trò công việc hoặc môi trường bảo mật.
- Mô hình Zero Trust: Quyền truy cập được quản lý một cách động, có thể thích ứng với các thay đổi trong hành vi truy cập, mối đe dọa bảo mật, và các yêu cầu công việc. Điều này đảm bảo rằng quyền truy cập luôn được kiểm soát chặt chẽ và chỉ được cấp khi thực sự cần thiết.

Tính minh bạch và kiểm soát :

- Mô hình truyền thống: Có thể thiếu sự minh bạch và kiểm soát đối với việc người dùng truy cập vào tài nguyên, vì một khi đã vào được mạng, họ có thể tự do sử dụng tài nguyên mà ít bị hạn chế.
- Mô hình Zero Trust: Tăng cường sự minh bạch và kiểm soát thông qua việc ghi lại và phân tích mọi yêu cầu truy cập. Điều này không chỉ giúp ngăn chặn các hành vi độc hại mà còn cung cấp dữ liệu quan trọng cho việc phân tích rủi ro và tuân thủ.

2.3. Xác thực trong Zero Trust

2.3.1. Các cơ chế xác thực người dùng truyền thống và vấn đề liên quan

Xác thực người dùng là yếu tố quan trọng đối với cả thiết bị cá nhân và dịch vụ trực tuyến. Tuy nhiên, các phương pháp xác thực truyền thống đã cho thấy những hạn chế rõ ràng, làm tăng nguy cơ bị xâm nhập và thách thức đối với an ninh mạng.

Vấn đề với Mật Khẩu

Mật khẩu là phương pháp xác thực phổ biến nhất nhưng cũng chứa đựng nhiều rủi ro. Người dùng thường chọn mật khẩu dễ đoán, và việc tái sử dụng mật khẩu trên nhiều tài khoản làm tăng nguy cơ bảo mật. Nếu một tài khoản bị xâm phạm, các tài khoản khác cũng dễ bị ảnh hưởng. Ngay cả những mật khẩu mạnh cũng có thể bị tin tặc tấn công thông qua các kỹ thuật tinh vi như tấn công kênh phụ (side channel attacks).

Xác Thực Dựa Trên Sinh Trắc Học

Các phương pháp xác thực dựa trên sinh trắc học như dấu vân tay, nhận diện khuôn mặt, và quét mống mắt không khó để bị đánh lừa. Chẳng hạn, dấu vân tay có thể được sao chép từ một bề mặt, nhận diện khuôn mặt có thể bị lừa bởi ảnh của nạn nhân hoặc bản in 3D của người dùng. Các phương pháp dựa trên mống mắt cũng có thể bị bỏ qua bằng cách sử dụng ảnh mống mắt của người dùng đặt trên kính áp tròng.

Vấn đề với 2FA (Xác thực 2 yếu tố)

Trong bối cảnh trên, xác thực đa yếu tố (MFA) ngày càng trở nên phổ biến. Một hình thức MFA phổ biến là xác thực hai yếu tố (2FA), kết hợp hai trong ba yếu tố xác thực truyền thống: kiến thức (ví dụ: mật khẩu), bản chất (ví dụ: dấu vân tay), và sở hữu (ví dụ: token phần cứng hoặc phần mềm). 2FA tăng cường bảo mật bằng cách nếu một yếu tố (như mật khẩu) bị xâm phạm, yếu tố khác (như token) vẫn còn để ngăn chặn truy cập trái phép. Tuy nhiên sự phụ thuộc vào thiết bị thứ hai (như điện thoại di động) là một hạn chế lớn của 2FA. Nếu thiết bị này bị mất, đánh cắp, hết pin hoặc không hoạt động, dịch vụ phụ thuộc vào nó có thể không truy cập được. Ngoài ra, việc yêu cầu tương tác nhiều từ người dùng (như chờ đợi mã và nhập mã) là một lý do cho tỷ lệ áp dụng 2FA thấp

Token Phần Cứng và Phần Mềm

- Token Phần Cứng: Cần người dùng mang theo thiết bị phần cứng, thường sinh ra mã xác thực duy nhất (OTC). Tuy nhiên, người dùng thường thấy việc mang theo thiết bị này không tiện lợi, và phương pháp này cũng tạo chi phí thêm cho nhà cung cấp dịch vụ.
- Token Phần Mềm: Mã OTC được gửi qua SMS đến số điện thoại đã đăng ký của người dùng. Tuy nhiên, phương pháp này dễ bị nghe lén và có thể gây ra vấn đề về quyền riêng tư khi người dùng cung cấp số điện thoại cá nhân cho nhiều nhà cung cấp dịch vụ.

Trong khuôn khổ của Zero Trust, việc xác thực người dùng đòi hỏi phải đáp ứng mức độ an ninh cao hơn và linh hoạt hơn so với những phương pháp truyền thống. Điều này dẫn đến việc khám phá và phát triển các giải pháp xác thực mới, như sử dụng sinh trắc học hành vi, để cải thiện tỷ lệ áp dụng cũng như khả năng bảo mật.

2.3.2. Xác thực dựa trên ngữ cảnh

Trong môi trường an ninh mạng hiện đại, việc nhận biết và đáp ứng linh hoạt theo ngữ cảnh đang trở thành một yếu tố quan trọng. Ngữ cảnh, trong trường hợp này, có thể được hiểu là bất kỳ thông tin nào giúp xác định tình huống của một thực thể, như danh tính, vị trí địa lý, hay thời gian. Điều này mở ra hướng tiếp cận mới trong việc xác thực người dùng, đặc biệt là trong các mô hình như Zero Trust.

Thiết bị di động hiện đại với các cảm biến như GPS đang làm tăng cường khả năng tính toán và hỗ trợ cho xác thực ngữ cảnh. Ví dụ, khi người dùng cố gắng đăng nhập vào dịch vụ ngân hàng trực tuyến từ một địa chỉ IP mới, hệ thống có thể yêu cầu họ trả lời các câu hỏi bổ sung. Địa chỉ IP ở đây không chỉ là thông tin kỹ thuật mà còn là ngữ cảnh giúp xác định liệu người dùng có phải là kẻ tấn công hay không, dù họ có cung cấp đúng thông tin xác thực.

Một số nghiên cứu đã đề xuất việc sử dụng thông tin ngữ cảnh, như vị trí di động của người dùng, để tạo ra một lớp xác thực bổ sung. Hệ thống có thể điều chỉnh yêu cầu xác thực dựa trên đánh giá rủi ro từ thông tin vị trí. Điều này không chỉ tăng cường an ninh mà còn cải thiện trải nghiệm người dùng, bằng cách giảm bớt sự cần thiết của xác thực hoạt động trong các tình huống nhất định.

Một trong những phát triển đáng chú ý trong lĩnh vực xác thực ngữ cảnh là CAMFA (context-aware multimodal FIDO authentication) cho điện thoại di động. CAMFA, phù hợp với tiêu chuẩn FIDO (Fast IDentity Online), là một hệ thống xác thực đa dạng và ngữ cảnh. Trong hệ thống này, máy chủ FIDO xác định mức độ xác thực (RP LoA - Relying Party Level of Authentication) cần thiết cho việc truy cập một dịch vụ cụ thể.

Cách Thức Hoạt Động của CAMFA :

- Xác thực đa dạng: CAMFA sử dụng cả phương pháp xác thực rõ ràng (như PIN, nhận diện khuôn mặt) và ngầm (như nhận diện vị trí, cách đặt điện thoại).
- Đánh giá rủi ro dựa trên ngữ cảnh: Hệ thống này theo dõi mức độ rủi ro dựa trên thông tin ngữ cảnh, như vị trí hoặc cách điện thoại được đặt (trong tay, trên bàn, trong túi). Khi thông tin hành vi người dùng phù hợp với ngữ cảnh, mức rủi ro được đánh giá thấp.
- Kết hợp phương pháp xác thực: CAMFA kết hợp các phương pháp xác thực khác nhau dựa trên mức độ rủi ro đã đánh giá và yêu cầu LoA của dịch vụ đang được truy cập.

Tuy nhiên, các hệ thống như CAMFA và các cơ chế xác thực ngữ cảnh khác đều đối mặt với thách thức trong việc triển khai rộng rãi. Chúng phụ thuộc nhiều vào các cảm biến và thông tin ngữ cảnh có sẵn, điều này có thể không phù hợp với tất cả các loại thiết bị. Điều này đặt ra nhu cầu phát triển cơ chế xác thực có thể tận dụng thông tin ngữ cảnh phong phú nhưng cũng dễ sử dụng trên nhiều loại thiết bị khác nhau.

2.3.3. Xác thực liên tục

Xác thực liên tục được nhìn nhận như một giải pháp an ninh mạng tiên tiến, đáp ứng nhu cầu xác định liên tục danh tính của người dùng, thiết bị hoặc quy trình sau khi đã qua giai đoạn đăng nhập. Điều này quan trọng vì các phương pháp xác

thực truyền thống như mật khẩu và sinh trắc học chỉ cung cấp bảo mật tại điểm nhập mà không kiểm soát liên tục sau đó. Vì mật khẩu thường xuyên bị rò rỉ hoặc hack, việc xác thực liên tục trở thành một yếu tố quan trọng trong việc bảo vệ các dịch vụ quan trọng.

Các phương pháp xác thực liên tục :

- Xác thực dựa trên hành vi người dùng : Một số nghiên cứu sử dụng hành vi gõ phím của người dùng, như thời gian giữ phím và thời gian giữa các phím khi người dùng gõ để xác thực liên tục. Ngoài ra một số nghiên cứu cũng tập trung vào mô hình hóa cử động của người dùng, như cách họ đi bộ.
- Xác thực dựa trên sinh trắc học thụ động : Một số phương pháp tận dụng sinh trắc học thụ động như hoạt động não (EEG), nhịp tim (ECG), hoặc hoạt động cơ (EMG), không yêu cầu sự tương tác tích cực từ người dùng.
- Xác thực dựa trên thông tin môi trường : Các phương pháp khác như sử dụng thông tin RF, ánh sáng, nhiệt độ, và âm thanh mà thiết bị có thể thu thập mà không cần tương tác của con người, được đề xuất để xác thực liên tục cho các thiết bị.

Các giải pháp được nói trên mặc dù mang lại nhiều lợi ích, cũng tiềm ẩn những vấn đề không nhỏ cần được giải quyết :

- Giới hạn đối với thiết bị cụ thể : Một trong những rào cản lớn nhất chính là tính chất đặc thù của thiết bị mà các phương pháp xác thực liên tục hướng đến. Hầu hết các giải pháp hiện tại được thiết kế cho một loại thiết bị cụ thể và không thể áp dụng trực tiếp lên các loại thiết bị khác. Điều này đặt ra thách thức trong việc mở rộng phạm vi áp dụng của xác thực liên tục, đặc biệt khi người dùng ngày nay thường sử dụng nhiều loại thiết bị khác nhau để truy cập các dịch vụ trực tuyến.
- Hạn chế trong các tình hướng sử dụng : Nhiều phương pháp xác thực hiện tại chỉ phù hợp với những tình huống nhất định. Ví dụ, xác thực dựa trên dáng đi người dùng chỉ có hiệu quả khi người dùng đang di chuyển, trong khi phương pháp phân tích hành vi gõ phím chỉ hữu ích khi người dùng thực sự đang sử dụng bàn phím. Điều này hạn chế sự linh hoạt và khả năng áp dụng của xác thực liên tục trong nhiều hoàn cảnh khác nhau.
- Thách thức trong thiết kế thiết bị : Để tích hợp xác thực liên tục, các thiết bị cần được thiết kế hoặc cải tiến với các cảm biến và thành phần mới. Điều này không chỉ là một thách thức về mặt kỹ thuật mà còn ảnh hưởng đến chi phí sản xuất và thậm chí là thiết kế tổng thể của thiết bị.
- Quyền riêng tư và khả năng sử dụng : Vấn đề quyền riêng tư và khả năng sử dụng là một mối quan ngại lớn trong xác thực liên tục. Việc thu thập liên tục dữ liệu nhạy cảm từ người dùng, như hình ảnh hoặc các tín hiệu y tế, có thể bị

người dùng phản đối do lo ngại về quyền riêng tư. Ngoài ra, một số phương pháp có thể gây phiền toái hoặc làm giảm trải nghiệm người dùng.

2.3.4. Xác thực thiết bị

2.3.4.1. Tổng quan về xác thực thiết bị

Trong môi trường an ninh mạng hiện đại, xác thực thiết bị đóng vai trò quan trọng trong hệ thống Zero Trust. Zero Trust không chỉ giới hạn ở việc xác thực người dùng mà còn mở rộng sang việc xác thực thiết bị, nhất là trong thời đại IoT đang bùng nổ. Trong Zero Trust, mọi thiết bị kết nối mạng đều được coi là một nguồn tiềm ẩn rủi ro, từ máy chủ, máy trạm cho đến các thiết bị di động.

Thiết bị được chia thành hai loại chính: doanh nghiệp sở hữu và cá nhân. Mỗi loại yêu cầu một cách tiếp cận khác nhau trong việc quản lý và xác thực, phù hợp với mức độ an ninh và nguy cơ tiềm ẩn. Đối với việc triển khai Zero Trust, việc xác định chính xác tất cả thiết bị kết nối đến mạng là thiết yếu. Điều này bao gồm việc nhận dạng thiết bị, cũng như quản lý quyền truy cập và hoạt động của chúng trên mạng.

Zero Trust Device (ZTD) là nguyên tắc cốt lõi trong Zero Trust, cho phép doanh nghiệp phân đoạn, bảo vệ và hạn chế quyền truy cập của các thiết bị. Mục tiêu của ZTD là không chỉ xác định mà còn quản lý chặt chẽ mọi thiết bị kết nối mạng, từ việc xác định danh tính cho đến việc kiểm soát quyền truy cập và hoạt động của chúng trên mạng. Điều này đặc biệt quan trọng với các thiết bị IoT và OT, vốn thường hoạt động mà không cần sự can thiệp trực tiếp của con người.

Một yếu tố quan trọng khác trong ZTD là việc phân loại thiết bị. Mỗi loại thiết bị, từ máy chủ, máy trạm, thiết bị di động, đến IoT và thiết bị công nghệ vận hành (OT), đều có những yêu cầu xác thực khác nhau. việc này giúp xác định rõ ràng nhu cầu xác thực và mức độ truy cập phù hợp cho từng loại thiết bị. Trong môi trường Zero Trust, mọi thiết bị kết nối đều phải được xác định một cách rõ ràng và chính xác để đảm bảo an toàn mạng.

Tuy nhiên việc xác thực các thiết bị IoT và OT mang lại nhiều thách thức độc đáo:

- *Tính Độc Lập của Thiết Bị IoT và OT* : Thiết bị IoT và OT thường hoạt động mà không cần sự hỗ trợ của con người, điều này làm cho các phương pháp xác thực truyền thống liên quan đến con người trở nên không phù hợp.
- *Giao Tiếp Máy-Máy (M2M)* : Trong mạng IoT và OT, sự giao tiếp M2M đòi hỏi cách tiếp cận xác thực mới, chẳng hạn như xác thực tương hỗ, để đảm bảo tính xác thực của các thiết bị.
- *Hạn Chế về Tính toán của Thiết Bị IoT* : Nhiều thiết bị IoT có hạn chế về khả năng tính toán, làm cho việc áp dụng các phương pháp xác thực truyền thống trở nên khó khăn hoặc không khả thi.

- *Nhu Cầu Xác Thực Liên Tục và Đa Dạng* : Đối với hệ thống IoT hoặc OT, việc xác thực liên tục và đa dạng hóa các phương pháp xác thực là cần thiết để đối phó với số lượng lớn thiết bị kết nối mạng.

2.3.4.2. Danh tính thiết bị và IdoT (Identity-Driven Traffic)

Danh tính của thiết bị là quá trình xác định danh tính của một thiết bị. Danh tính của thiết bị là cần thiết để xác thực thiết bị trước khi cấp quyền truy cập vào các tài nguyên. Danh tính của thiết bị bao gồm các thông tin như:

- Địa chỉ MAC
- Tên thiết bị
- Hệ điều hành
- Phiên bản phần mềm
- Chứng chỉ

Trong khuôn khổ Zero Trust, việc xác định và quản lý danh tính của các thiết bị, đóng vai trò quan trọng. Tuy nhiên, các thuộc tính đơn giản như số IMEI hoặc thông tin nhà sản xuất không còn đủ để đảm bảo an toàn. Điều này dẫn đến nhu cầu phát triển một hệ thống IDoT (Identity-Driven Traffic) có khả năng hỗ trợ định danh duy nhất, chống làm giả và không thể sao chép, cũng như có khả năng thích ứng với các hình thức xác thực và kiểm soát truy cập khác nhau.

Một trong những phương pháp nổi bật trong việc xác định danh tính là sử dụng Physically Unclonable Functions (PUFs). PUFs là các đặc trưng thiết kế độc đáo, chỉ tồn tại trong một phần cứng cụ thể. Phản ứng của PUF khi gặp kích thích điện tử cho phép tạo ra hệ thống mật mã dựa trên danh tính, nhẹ nhàng nhưng an toàn. Tuy nhiên, cách tiếp cận này cũng tiềm ẩn rủi ro bị tấn công mô hình hóa, có thể dùng để sao chép và phân phối lại.

Trong thực tế, Public Key Infrastructure (PKI) đã được áp dụng rộng rãi để cung cấp danh tính độc đáo cho thiết bị IoT. Tuy nhiên, việc quản lý chứng chỉ trong PKI cần sự chú ý đặc biệt, bao gồm việc phân phối, thu hồi, lưu trữ và cấp phát. Một giải pháp khác, Intrinsic ID, sử dụng SRAM PUF để tạo ra danh tính duy nhất, cung cấp một giải pháp gọn nhẹ hơn. Công cụ quản lý danh tính IoT như nền tảng IAM của Ericsson và IoT IAM phi tập trung của Vouch cũng đang được sử dụng để mở rộng IAM ra ngoài khuôn khổ truyền thống dành cho con người.

2.3.4.3. Các phương pháp xác thực thiết bị trong Zero Trust

Có nhiều phương pháp xác thực thiết bị có thể được sử dụng trong mô hình Zero Trust. Các phương pháp này có thể được kết hợp với nhau để tăng cường bảo mật.

Xác thực dựa trên địa chỉ MAC

Xác thực dựa trên địa chỉ MAC là phương pháp xác thực thiết bị đơn giản nhất. Phương pháp này sử dụng địa chỉ MAC của thiết bị để xác thực.

Địa chỉ MAC là một địa chỉ vật lý được gán cho mỗi thiết bị mạng. Địa chỉ MAC được sử dụng để xác định một thiết bị cụ thể trên mạng.

Xác thực dựa trên địa chỉ MAC có thể dễ bị tấn công, vì kẻ tấn công có thể dễ dàng giả mạo địa chỉ MAC của một thiết bị hợp pháp.

Xác thực dựa trên chứng chỉ

Xác thực dựa trên chứng chỉ là phương pháp xác thực thiết bị an toàn hơn xác thực dựa trên địa chỉ MAC. Phương pháp này sử dụng chứng chỉ kỹ thuật số để xác thực.

Chứng chỉ kỹ thuật số là một tập tin điện tử chứa thông tin về danh tính của một người hoặc thiết bị. Chứng chỉ kỹ thuật số được ký bởi một cơ quan chứng nhận (CA) đáng tin cậy.

Xác thực dựa trên chứng chỉ giúp ngăn chặn kẻ tấn công giả mạo danh tính của một thiết bị hợp pháp, ngay cả khi chúng biết địa chỉ MAC của thiết bị.

Xác thực dựa trên danh sách kiểm soát truy cập (ACL)

Xác thực dựa trên danh sách kiểm soát truy cập (ACL) là phương pháp xác thực thiết bị đơn giản và hiệu quả. Phương pháp này sử dụng ACL để xác định các thiết bị được phép truy cập vào các tài nguyên.

ACL là một tập hợp các quy tắc được sử dụng để kiểm soát truy cập vào các tài nguyên. ACL có thể được sử dụng để xác định các thiết bị được phép truy cập vào một mạng, một máy chủ hoặc một ứng dụng.

Xác thực dựa trên ACL có thể dễ bị tấn công, vì kẻ tấn công có thể dễ dàng thay đổi ACL để cho phép thiết bị của chúng truy cập vào các tài nguyên bị hạn chế.

2.3.5. So sánh xác thực trong mô hình Zero Trust và mô hình truyền thống

Xác thực là một phần quan trọng trong việc bảo mật hệ thống và dữ liệu. Nó đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập vào các tài nguyên. Hai mô hình xác thực phổ biến là mô hình truyền thống và mô hình Zero Trust có sự khác nhau về xác thực như sau :

Phương thức xác thực:

- Mô hình truyền thống: Sử dụng mật khẩu là phương thức xác thực chính.
- Mô hình Zero Trust: Sử dụng xác thực đa yếu tố (MFA), bao gồm mật khẩu, sinh trắc học, mã OTP, v.v.

Vị trí xác thực:

- Mô hình truyền thống: Xác thực diễn ra tại biên giới mạng khi người dùng truy cập vào mạng nội bộ.
- Mô hình Zero Trust: Xác thực diễn ra bất kỳ đâu người dùng truy cập vào tài nguyên, bất kể họ đang ở bên trong hay bên ngoài mạng nội bộ.

Mức độ tin cậy:

- Mô hình truyền thống: Tin tưởng các thiết bị và người dùng trong mạng nội bộ.
- Mô hình Zero Trust: Không tin tưởng bất kỳ ai và luôn xác minh mọi yêu cầu truy cập.

Kiểm soát truy cập:

- Mô hình truyền thống: Cung cấp quyền truy cập rộng rãi cho người dùng dựa trên vai trò và nhóm.
- Mô hình Zero Trust: Cung cấp quyền truy cập tối thiểu cần thiết dựa trên ngữ cảnh truy cập, hành vi của người dùng và mức độ rủi ro.

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. Sự chuyển đổi này không chỉ cải thiện khả năng bảo mật thông tin mà còn tạo ra sự linh hoạt và khả năng thích ứng cao với môi trường kinh doanh ngày nay.

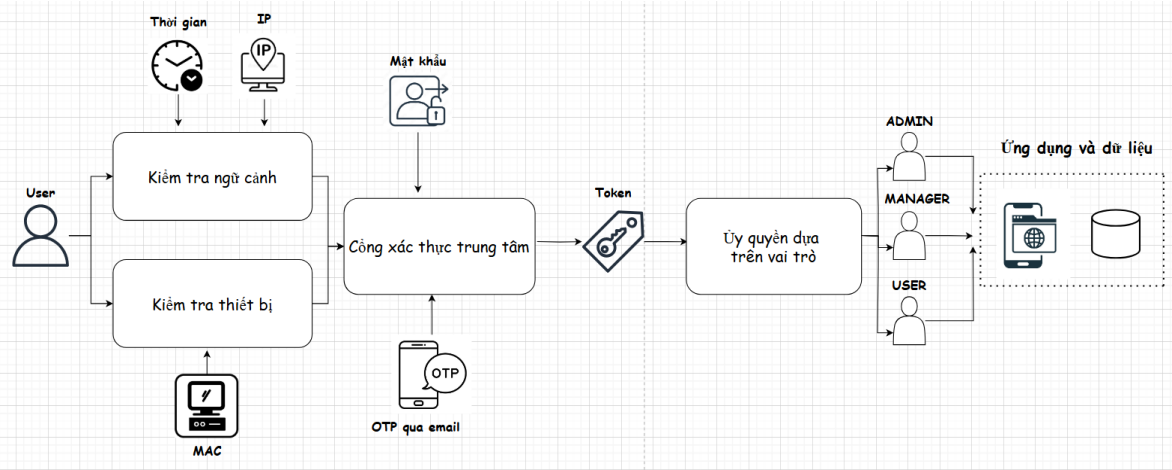
Chương này cũng nhấn mạnh rằng việc áp dụng mô hình Zero Trust đòi hỏi sự thay đổi chiến lược toàn diện, từ cách thức quản lý và xác thực người dùng, thiết bị, cho đến phương pháp quản lý và giám sát dữ liệu. Các thách thức như chi phí triển khai, khả năng tương thích hệ thống và quản lý phức tạp cũng 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

3.1.1. Thành phần kiến trúc

Trong thế giới ngày càng kỹ thuật số và mạng lưới hóa, việc bảo vệ thông tin và dữ liệu trở nên quan trọng hơn bao giờ hết. Mô hình Zero Trust được thiết kế để đối phó với những thách thức bảo mật thông tin trong môi trường mạng ngày nay, bằng cách không tự động tin cậy bất kỳ yếu tố nào mà không qua xác thực. Trong chương 3 này, tôi sẽ trình bày về cách thức xây dựng và triển khai một mô hình quản lý xác thực và quyền truy cập dựa trên mô hình 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. Nguyên tắc Zero Trust được áp dụng ở đây bằng cách không tin tưởng mặc định bất kỳ yêu cầu truy cập nào mà luôn yêu cầu xác thực danh tính người dùng mỗi khi người dùng thực hiện đăng nhập vào hệ thống. 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. Nguyên tắc Zero Trust được áp dụng bằng cách yêu cầu xác thực nhiều yếu tố để đảm bảo danh tính người dùng một cách chắc chắn hơn.

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. Dữ liệu đã được phân đoạn dựa trên xác minh ngữ cảnh đối với thời gian, địa chỉ IP và xác minh thiết bị đối với địa chỉ MAC. Điều này đảm bảo rằng truy cập chỉ được cấp trong giờ làm việc và từ các thiết bị được phép, đảm bảo rằng mọi truy cập đều phải được kiểm tra và xác thực một cách nghiêm ngặt.

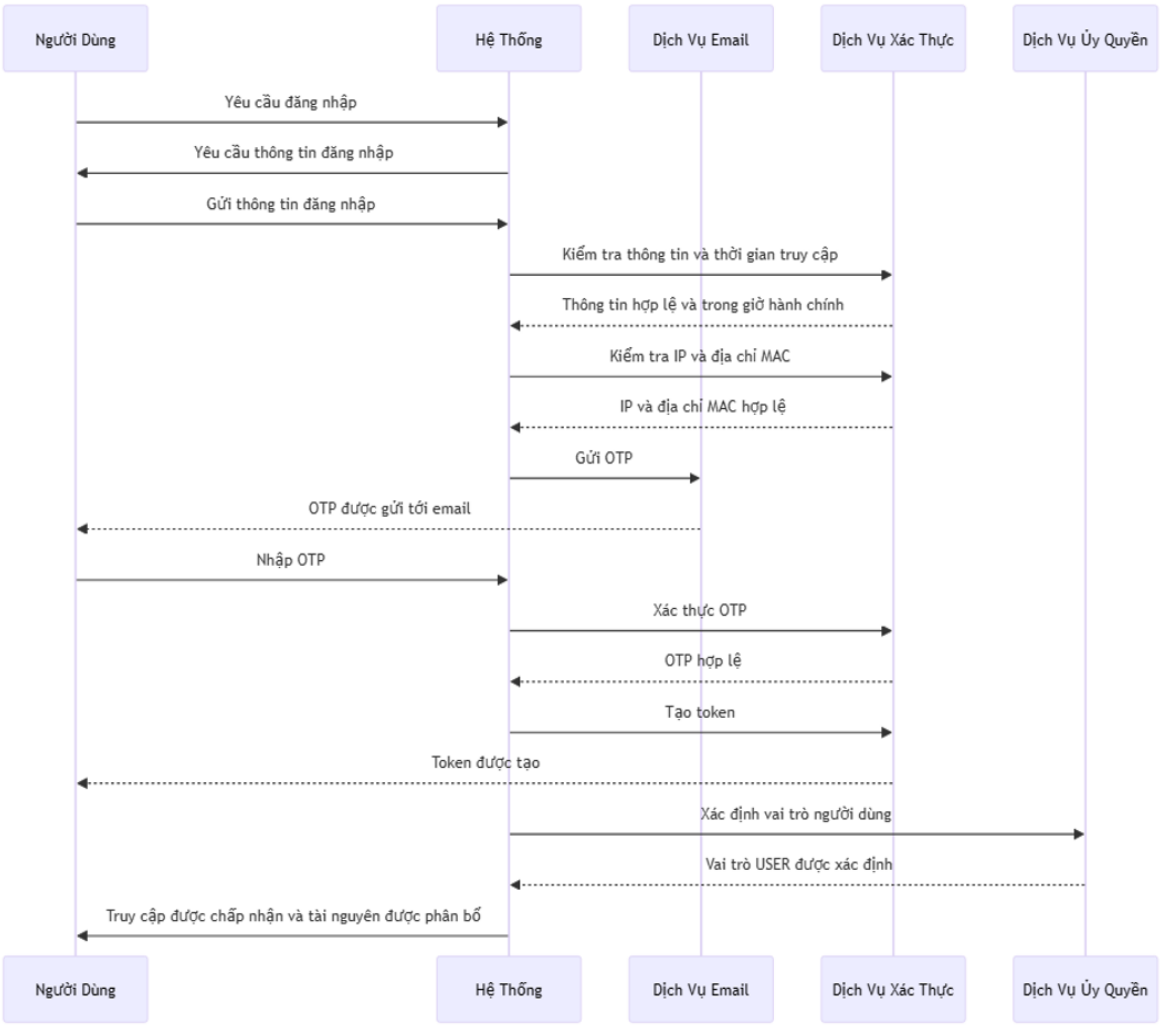
Token Truy Cập

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.

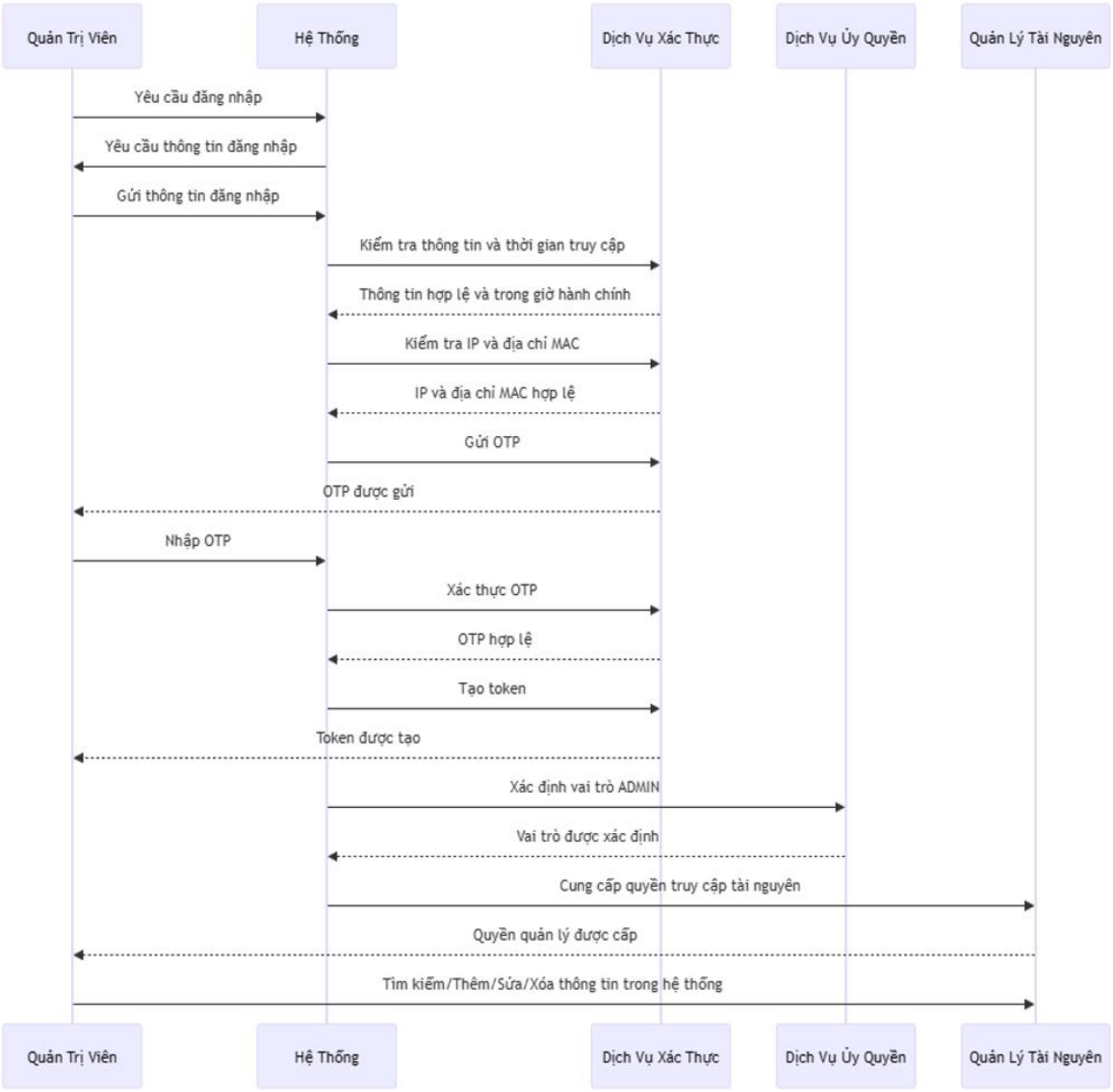
Ủy quyền và kiểm soát truy cập

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.

3.1.2. Biểu đồ tuần tự người dùng truy cập dịch vụ



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



Hình 3.3 Biểu đồ tuần tự quản trị viên 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. 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.

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.

3.1.3. Sự phù hợp của kiến trúc trong quản lý xác thực và quyền truy cập

Mô hình quản lý dựa trên Zero Trust phù hợp với việc quản lý xác thực và quyền truy cập vì nhiều lý do:

Tăng cường bảo mật

Bằng cách yêu cầu xác thực từ nhiều tầng và kiểm tra ngữ cảnh truy cập, kiến trúc này giảm thiểu rủi ro từ các cuộc tấn công và nỗ lực truy cập trái phép. Điều này đặc biệt quan trọng trong môi trường hiện nay, nơi mối đe dọa bảo mật ngày càng phức tạp và tinh vi.

Tính linh hoạt và mở rộng

Mô hình Zero Trust có thể dễ dàng được tùy chỉnh và mở rộng để phù hợp với nhu cầu cụ thể của mỗi tổ chức. Các thành phần của nó có thể được điều chỉnh hoặc thêm vào, cho phép tổ chức áp dụng các chính sách bảo mật phù hợp với sự phát triển và thay đổi của họ.

Tính đồng nhất và quản lý tập trung

Mô hình Zero Trust tạo ra một cách tiếp cận đồng nhất trong việc quản lý xác thực và quyền truy cập, giảm bớt sự phức tạp và tăng cường khả năng kiểm soát và giám sát. Quản lý tập trung qua Bộ quản lý chính sách truy cập cho phép tổ chức dễ dàng duy trì và cập nhật các chính sách bảo mật, đồng thời phản ứng nhanh chóng trước các thách thức bảo mật mới.

3.2. Xác thực người dùng và thiết bị

Trong mô hình Zero Trust, xác thực được xem như là bước đầu tiên và quan trọng nhất trong việc bảo vệ thông tin và tài nguyên hệ thống. Xác thực giúp đảm bảo rằng chỉ có người dùng và thiết bị được phép mới có quyền truy cập vào hệ thống, qua đó ngăn chặn các nguy cơ từ việc truy cập trái phép. Phần này sẽ phân tích chi tiết cách thức xác thực người dùng và thiết bị trong hệ thống do tôi xây dựng.

Kiểm tra ngữ cảnh truy cập

Bên cạnh việc xác thực người dùng và thiết bị, mô hình Zero Trust cũng tích hợp việc kiểm tra ngữ cảnh truy cập. Điều này bao gồm việc xác định thời gian truy cập - chỉ cho phép truy cập trong giờ làm việc hành chính (từ thứ 2 đến thứ 6 trong khoảng 8h đến 17h),

```
boolean isAllowedTime = vnTime.isAfter(LocalTime.of( hour: 8,  minute: 0)) && vnTime.isBefore(LocalTime.of( hour: 17,  minute: 0));
boolean isAllowedDay = dayOfWeek != DayOfWeek.SATURDAY && dayOfWeek != DayOfWeek.SUNDAY;
```

Hình 3.4 Kiểm tra ngữ cảnh dựa trên yếu tố thời gian

và đảm bảo rằng truy cập từ những vị trí được cho là an toàn. Ngoài ra, quản trị viên có thể chỉnh sửa thời gian cho phép truy cập để phù hợp với nhu cầu và thời gian làm việc của công ty. Kiểm tra ngữ cảnh này giúp tăng cường an ninh bằng cách đảm bảo rằng mọi yêu cầu truy cập đều phù hợp với chính sách an ninh của tổ chức.

Xác Thực Thiết Bị

Xác thực thiết bị là một phần quan trọng trong quy trình xác thực, đặc biệt trong mô hình Zero Trust. Trong mô hình do tôi xây dựng, việc này được thực hiện thông qua kiểm tra địa chỉ IP và địa chỉ MAC của thiết bị.

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

Hình 3.5 Xác thực thiết bị dựa trên địa chỉ IP và MAC

Nếu IP của thiết bị người dùng sử dụng để truy cập hệ thống thuộc dải IP cho phép thì người dùng đó sẽ được phép truy cập hệ thống, trong trường hợp IP không thuộc dải cho phép ta sẽ xét đến địa chỉ MAC của thiết bị có nằm trong danh sách địa chỉ MAC cho phép không. Điều này nhằm đảm bảo chỉ những thiết bị được phép trước mới có quyền truy cập vào hệ thống, đồng nghĩa với việc mọi thiết bị đều phải được xác thực trước khi có thể truy cập vào các tài nguyên. Quy trình này giúp ngăn chặn việc truy cập trái phép từ thiết bị không được ủy quyền, tăng cường tính an toàn và bảo mật cho hệ thống.

Xác Thực Người Dùng

Quy trình xác thực người dùng trong mô hình Zero Trust bắt đầu bằng việc sử dụng mật khẩu - phương thức xác thực cơ bản nhất. Tuy nhiên, mật khẩu một mình không đủ để đáp ứng tiêu chuẩn an ninh của mô hình Zero Trust. Do đó, quy trình tiếp tục với bước xác thực đa yếu tố (MFA), thông qua mã OTP được gửi đến email của người dùng. Mã OTP này đóng vai trò như một lớp bảo mật thứ hai, đảm bảo rằng người dùng thực sự là chủ sở hữu của tài khoản đang cố gắng truy cập.

Token Truy Cập và Quản Lý Phiên

Sau khi quá trình xác thực người dùng và thiết bị thành công, hệ thống sẽ khởi tạo một token truy cập cho người dùng. Token này cần được kèm theo trong mỗi yêu cầu truy cập sau đó để xác thực và duy trì phiên làm việc. Sử dụng token truy cập giúp đảm bảo tính liên tục và an toàn trong quản lý phiên làm việc, đồng thời cho phép theo dõi và kiểm soát truy cập một cách hiệu quả.

Việc áp dụng MFA và xác thực thiết bị, kết hợp với việc đánh giá ngữ cảnh truy cập, tạo nên một hệ thống bảo mật đa tầng, phản ánh nguyên tắc cốt lõi của mô hình Zero Trust. Bằng cách thực hiện các biện pháp này, hệ thống không chỉ bảo vệ thông tin từ việc truy cập trái phép mà còn đảm bảo rằng mọi quyền truy cập đều dựa trên sự kiểm soát và đánh giá kỹ lưỡng. Qua đó, tăng cường sự an toàn và ổn định cho hệ thống thông tin trong một môi trường mạng ngày càng phức tạp và thách thức.

3.3. Quản lý quyền truy cập dựa trên vai trò

Trong môi trường bảo mật thông tin đa tầng và phức tạp hiện nay, việc quản lý quyền truy cập một cách hiệu quả là vô cùng quan trọng. Xây dựng hệ thống dựa trên mô hình Zero Trust, yêu cầu một phương pháp tiếp cận linh hoạt và đa dạng để xác định quyền truy cập dựa trên vai trò cụ thể của người dùng và thiết bị trong tổ chức. Phần này sẽ thảo luận chi tiết về cách thức và lợi ích của việc áp dụng quản lý quyền truy cập dựa trên vai trò trong hệ thống.

Quản lý quyền truy cập dựa trên vai trò (RBAC - Role-Based Access Control) là một cách tiếp cận trong việc quản lý quyền truy cập vào tài nguyên và dịch vụ, dựa trên vai trò công việc của người dùng trong tổ chức. Mỗi vai trò được gán với một tập hợp quyền truy cập cụ thể, giúp đơn giản hóa quản lý quyền truy cập và tăng cường an ninh bằng cách đảm bảo rằng người dùng chỉ có quyền truy cập vào tài nguyên cần thiết cho công việc của họ.

RBAC giúp giảm bớt phức tạp trong việc quản lý quyền truy cập bằng cách phân loại quyền theo vai trò, thay vì gán quyền truy cập cho từng cá nhân. Phương pháp này giảm thiểu rủi ro về an ninh thông tin do sai sót trong quản lý quyền truy cập và tạo điều kiện cho việc tuân thủ chính sách bảo mật một cách hiệu quả.

Trong hệ thống, việc áp dụng RBAC bắt đầu bằng cách xác định các vai trò khác nhau trong tổ chức, từ người dùng cơ bản đến quản trị viên hệ thống. Mỗi vai trò này sau đó 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.

Vai trò và quyền được phân định như sau :

- ADMIN: Vai trò ADMIN (Quản trị viên) được trao quyền quản lý cao nhất trong hệ thống, bao gồm khả năng cấu hình hệ thống, quản lý người dùng, thiết lập quyền truy cập và thực hiện các thay đổi chính sách an ninh. Vai trò này thường được giới hạn cho một số ít người dùng có kỹ năng và trách nhiệm cao, nhằm đảm bảo hệ thống hoạt động ổn định và an toàn.
- MANAGER: Đây là vai trò quản lý trung gian, nằm giữa ADMIN và USER. MANAGER có quyền hạn giống như một USER bình thường, bao gồm việc truy cập vào các ứng dụng và dữ liệu cần thiết cho công việc hàng ngày. Điểm khác biệt chính của MANAGER so với USER thông thường là khả năng xem thông tin của tất cả USER thuộc phòng ban mà họ quản lý.
- USER: Vai trò USER (Người dùng) được cấp quyền truy cập cơ bản, phù hợp với nhu cầu hàng ngày như truy cập vào ứng dụng, dữ liệu, và thực hiện các nhiệm vụ cụ thể không yêu cầu quyền quản trị hệ thống. Quyền của người dùng này được thiết kế để tối đa hóa hiệu suất công việc trong khi giữ an ninh thông tin ở mức cao nhất.

Trong hệ thống, quyền truy cập được quản lý thông qua một hệ thống trung tâm, nơi các chính sách truy cập được định nghĩa rõ ràng cho từng vai trò. Sự phân biệt rõ ràng giữa ADMIN, MANAGER và USER cho phép hệ thống tự động áp dụng các quyền truy cập phù hợp ngay khi tài khoản được tạo hoặc khi vai trò của người

dùng thay đổi. Ngoài ra hệ thống kiểm tra quyền truy cập của người dùng cho từng yêu cầu được gọi đến, đảm bảo rằng chỉ những người dùng có thẩm quyền mới có thể thực hiện các hành động tương ứng. Hình 3.6 mô tả các yêu cầu đều phải kiểm tra vai trò người dùng trước khi cho phép thực hiện hành động:

```
.antMatchers(HttpMethod.GET, "/employee/search").hasAnyAuthority( ...authorities: "ADMIN", "MANAGER")
.antMatchers(HttpMethod.POST, "/employee/**").hasAuthority("ADMIN")
.antMatchers(HttpMethod.PUT, "/employee/change-password").hasAnyAuthority( ...authorities: "ADMIN", "MANAGER", "USER")
.antMatchers(HttpMethod.PUT, "/employee/**").hasAuthority("ADMIN")
.antMatchers(HttpMethod.DELETE, "/employee/**").hasAuthority("ADMIN")
```

Hình 3.6. Kiểm tra vai trò người dùng cho từng yêu cầu trong hệ thống

Việc kiểm tra vai trò người dùng cho mỗi request đảm bảo rằng hệ thống luôn duy trì nguyên tắc của mô hình Zero Trust, cụ thể là liên tục xác minh danh tính và quyền hạn của người dùng. Điều này giúp ngăn chặn các truy cập trái phép và bảo vệ dữ liệu nhạy cảm của hệ thống. Hơn nữa, việc sử dụng RBAC giúp phân quyền một cách rõ ràng và quản lý dễ dàng hơn, đảm bảo rằng mỗi người dùng chỉ có thể truy cập vào các tài nguyên mà họ có thẩm quyền.

Việc áp dụng phân quyền dựa trên vai trò ADMIN, MANAGER và USER trong hệ thống do tôi xây dựng mang lại nhiều lợi ích:

- Tăng cường an ninh: Sự phân biệt rõ ràng giữa các quyền truy cập của ADMIN, MANAGER và USER giúp hạn chế tối đa khả năng truy cập không được phép, từ đó bảo vệ hệ thống khỏi các mối đe dọa tiềm ẩn.
- Tối ưu hóa quyền truy cập: Phân quyền dựa trên vai trò giúp đảm bảo rằng mỗi người dùng chỉ có quyền truy cập cần thiết cho công việc, giảm thiểu rủi ro từ việc truy cập quá mức cần thiết.
- Hiệu quả quản lý: Quản lý quyền truy cập thông qua vai trò giúp đơn giản hóa quy trình quản lý, giảm thiểu công sức cần thiết cho việc cập nhật và duy trì các chính sách truy cập.

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

Trong phần này, chúng ta sẽ đi sâu vào việc so sánh hệ thống mà tôi đã xây dựng dựa trên mô hình Zero Trust với các mô hình xác thực và ủy quyền hiện có đã được trình bày ở chương 2 là VNIS, Google (BeyondCorp), và Microsoft . So sánh

sẽ tập trung vào khía cạnh xác thực và ủy quyền, đánh giá sự khác biệt và tương đồng giữa các mô hình để rút ra những bài học và cơ hội cải thiện cho hệ thống.

Mô hình xác thực và ủy quyền của VNIS

VNIS, một tổ chức chuyên về giải pháp an ninh mạng, tập trung vào việc sử dụng công nghệ tiên tiến để bảo vệ thông tin. Sử dụng các phương pháp IAM truyền thống, chú trọng vào việc quản lý danh tính và quyền truy cập thông qua một hệ thống tập trung. Mặc dù cách tiếp cận này mang lại hiệu quả trong việc kiểm soát quyền truy cập, nhưng nó thường không đủ linh hoạt để đối phó với các mối đe dọa an ninh mạng ngày càng phức tạp. Ngoài ra, VNIS áp dụng các phương pháp xác thực truyền thống kết hợp với giải pháp đám mây để cung cấp bảo mật tại điểm cuối và tập trung vào việc kiểm soát truy cập mạng.

Google's BeyondCorp

BeyondCorp là một bước đột phá của Google trong việc áp dụng mô hình Zero Trust, loại bỏ sự phụ thuộc vào mạng nội bộ tin cậy và chuyển sang "truy cập tin cậy" dựa trên xác thực người dùng và thiết bị. BeyondCorp tập trung vào việc tạo điều kiện truy cập an toàn và linh hoạt cho nhân viên từ bất kỳ đâu, loại bỏ sự cần thiết của VPN truyền thống và chuyển sang xác thực dựa trên người dùng và thiết bị, không phụ thuộc vào vị trí mạng. BeyondCorp có lợi thế về việc tích hợp sâu rộng với hệ sinh thái dịch vụ đám mây của Google, mang lại khả năng mở rộng và linh hoạt cao. Ngoài ra, nhờ việc áp dụng công nghệ học máy trong việc phân tích hanh vi truy cập, BeyondCorp có thể tập trung hơn vào việc điều chỉnh chính sách an ninh dựa trên ngữ cảnh truy cập cụ thể và hành vi người dùng.

Microsoft

Microsoft thông qua Azure Active Directory (Azure AD) và các giải pháp bảo mật khác, cung cấp một hệ thống quản lý danh tính và quyền truy cập mạnh mẽ hỗ trợ xác thực đa yếu tố và quản lý danh tính dựa trên đám mây. Microsoft mang lại khả năng tích hợp sâu rộng với hệ sinh thái đám mây, cung cấp khả năng mở rộng và quản lý tập trung. Mô hình này cho phép xác định các điều kiện truy cập dựa trên ngữ cảnh, như vị trí, trạng thái thiết bị, và rủi ro đăng nhập, và áp dụng MFA.

So sánh :

Xác thực người dùng và thiết bị

- Mô hình hệ thống của tôi : Áp dụng xác thực đa yếu tố (MFA) kết hợp với kiểm tra ngữ cảnh truy cập như thời gian và các yếu tố liên quan đến thiết bị như IP, MAC. Mật khẩu và mã OTP gửi qua email là hai yếu tố chính được sử dụng trong quy trình xác thực, cung cấp một lớp bảo mật cao hơn và được tăng cường bởi token truy cập động cho các phiên làm việc.

- VNIS: Có thể tập trung vào xác thực thông qua mật khẩu và chứng chỉ số, với một số hệ thống có thể áp dụng MFA trong môi trường mạng nội bộ. VNIS có xu hướng ưu tiên cho giải pháp an ninh tận cùng và giám sát truy cập mạng.
- BeyondCorp của Google: Xác thực dựa trên ngữ cảnh, không chỉ kiểm tra danh tính người dùng và thiết bị mà còn dựa vào dữ liệu ngữ cảnh để quyết định quyền truy cập. BeyondCorp loại bỏ sự cần thiết của VPN bằng cách sử dụng proxy truy cập ứng dụng để quản lý truy cập dựa trên chính sách xác thực chi tiết.
- Microsoft: Cho phép thiết lập chính sách truy cập dựa trên ngữ cảnh như vị trí, thiết bị, ứng dụng, và rủi ro của phiên truy cập. Microsoft tích hợp mạnh mẽ với Azure AD, cung cấp khả năng tự động hóa và tinh chỉnh chính sách truy cập một cách linh hoạt.

Quản lý quyền truy cập

- Mô hình hệ thống của tôi : Phân quyền truy cập dựa trên vai trò người dùng (ADMIN và USER), với ADMIN có quyền quản trị cao nhất bao gồm cấu hình hệ thống và quản lý người dùng, trong khi USER giới hạn ở quyền truy cập cơ bản.
- VNIS: Có thể không cung cấp sự linh hoạt tương tự như mô hình Zero Trust trong việc áp dụng quyền truy cập dựa trên ngữ cảnh và thay đổi. VNIS có thể chủ yếu tập trung vào quản lý quyền truy cập thông qua ACL (Access Control Lists) và chính sách tĩnh, với một số tích hợp quản lý danh tính.
- BeyondCorp của Google: Áp dụng quản lý quyền truy cập dựa trên ngữ cảnh và danh tính người dùng và thiết bị. Quyền truy cập được quản lý thông qua proxy truy cập ứng dụng, cho phép tinh chỉnh chính sách truy cập dựa trên đánh giá liên tục về rủi ro và ngữ cảnh.
- Microsoft: Sử dụng Azure AD để cung cấp quản lý quyền truy cập tinh vi, cho phép định nghĩa chính sách truy cập phức tạp dựa trên ngữ cảnh đăng nhập và đánh giá rủi ro. Hệ thống này cho phép tạo ra môi trường truy cập linh hoạt, an toàn, phản ánh nhu cầu đặc thù của doanh nghiệp.

Điểm khác biệt chính và các yếu tố cải thiện

- Tính linh hoạt và động: Mô hình hệ thống của tôi áp dụng nguyên tắc Zero Trust thông qua xác thực đa yếu tố và phân quyền dựa trên vai trò. Tuy nhiên, so với BeyondCorp và Microsoft, cơ hội cải thiện có thể nằm ở việc tăng cường khả năng tích hợp với các dịch vụ và ứng dụng khác nhau, từ đó tạo điều kiện cho một môi trường làm việc linh hoạt và an toàn hơn từ bất kỳ đâu, không chỉ trong mạng nội bộ. Về mặt chi phí, các giải pháp của Microsoft và Google có thể đòi hỏi phí bản quyền hoặc phí đăng ký dựa trên số lượng người dùng và mức độ dịch vụ, điều này cần được cân nhắc kỹ lưỡng khi so sánh với mô

hình hiện tại có thể đòi hỏi ít chi phí hơn do sử dụng công nghệ nội bộ hoặc mã nguồn mở.

- Áp dụng ngữ cảnh truy cập: Mô hình hệ thống của tôi đã áp dụng ngữ cảnh truy cập như một phần của quy trình xác thực, song việc mở rộng và sâu sắc hóa việc áp dụng ngữ cảnh có thể mang lại lợi ích lớn. BeyondCorp của Google chứng minh rằng việc sử dụng dữ liệu ngữ cảnh một cách thông minh có thể tạo ra một môi trường bảo mật mạnh mẽ, điều chỉnh chính sách truy cập dựa trên đánh giá liên tục về rủi ro và điều kiện truy cập. Điều chỉnh chính sách truy cập theo ý muốn của người quản lý trong hệ thống của tôi cũng được hỗ trợ, nhưng có thể không đạt độ linh hoạt như các giải pháp của Microsoft và Google, điều này là một lĩnh vực cần được cải tiến.
- Tự động hóa và học máy: Mô hình hệ thống của tôi có thể đáp ứng nhu cầu cơ bản về xác thực và quản lý quyền truy cập, song việc sử dụng công nghệ tự động hóa và học máy trong quản lý bảo mật và quyền truy cập có thể là một lĩnh vực quan trọng để khai thác và khám phá. Microsoft và Google đều áp dụng học máy và tự động hóa trong việc phát hiện mối đe dọa và quản lý quyền truy cập, cho phép tự động điều chỉnh chính sách truy cập dựa trên đánh giá rủi ro liên tục, một mục tiêu cần hướng tới trong cải tiến hệ thống của tôi trong tương lai.

3.5. Kết luận chương 3

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

Qua việc thiết kế hệ thống dựa trên mô hình Zero Trust, hệ thống của tôi đã áp dụng các biện pháp xác thực đa yếu tố, kiểm tra ngữ cảnh truy cập và phân quyền truy cập dựa trên vai trò, tất cả đều tạo nên một lớp bảo mật đa tầng, giảm thiểu rủi ro từ các cuộc tấn công và nỗ lực truy cập trái phép. Điều này không chỉ giúp bảo vệ thông tin và tài nguyên hệ thống mà còn đảm bảo rằng mọi quyền truy cập đều dựa trên sự kiểm soát và đánh giá kỹ lưỡng.

So sánh hệ thống với các mô hình của VNIS, Google (BeyondCorp), và Microsoft đã cho thấy rằng, mặc dù mỗi mô hình đều có những điểm mạnh và yếu riêng, song 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 như học máy từ các mô hình khác nhau 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.

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

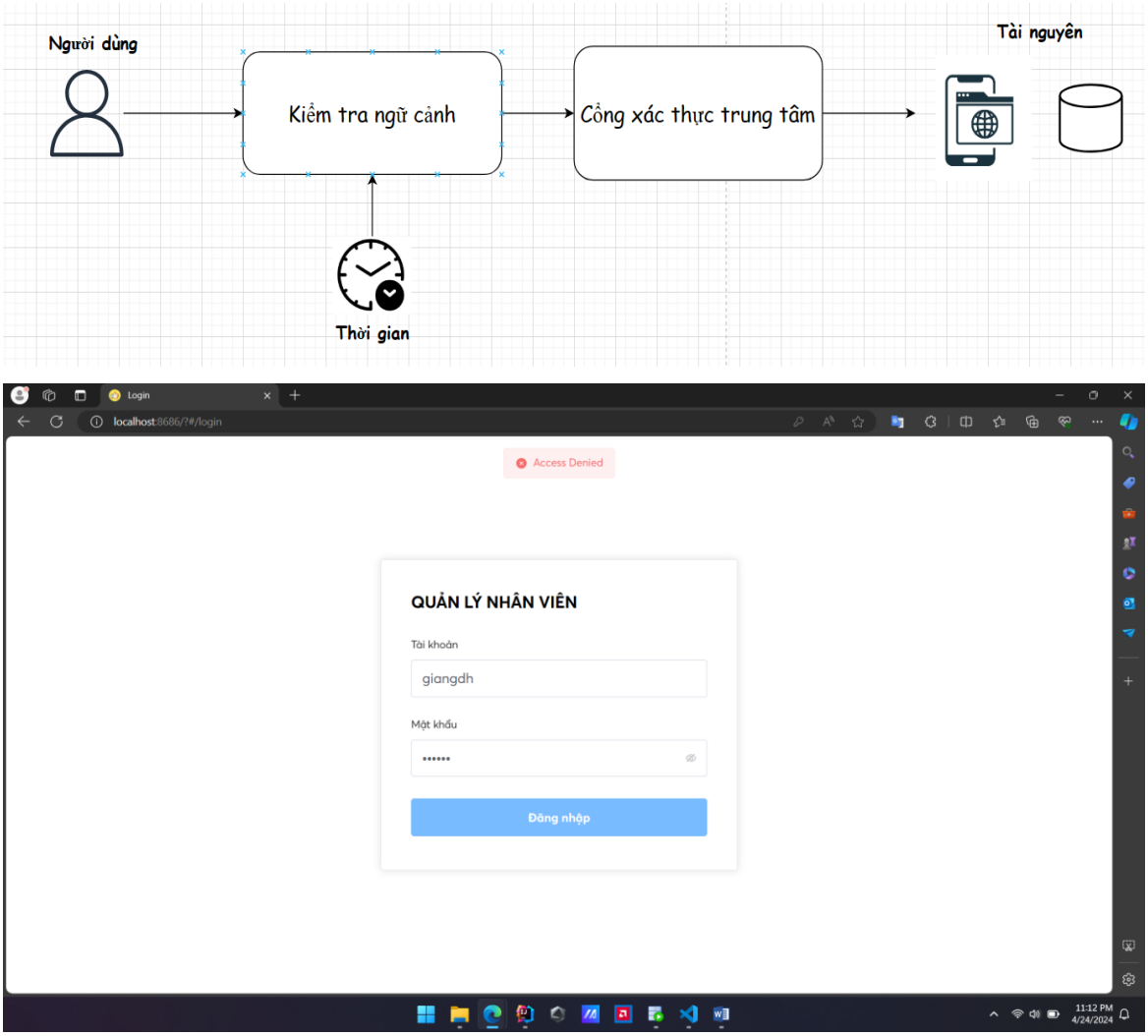
RAM: 16 GB DDR5

Hệ điều hành: Windows 11

Các kịch bản thử nghiệm dưới đây được thiết kế để kiểm tra mọi khía cạnh của hệ thống:

Kiểm tra thời gian cho phép truy cập

Mục tiêu: Đảm bảo rằng hệ thống chỉ cho phép truy cập vào giờ làm việc hành chính, từ 8 giờ sáng đến 5 giờ chiều.

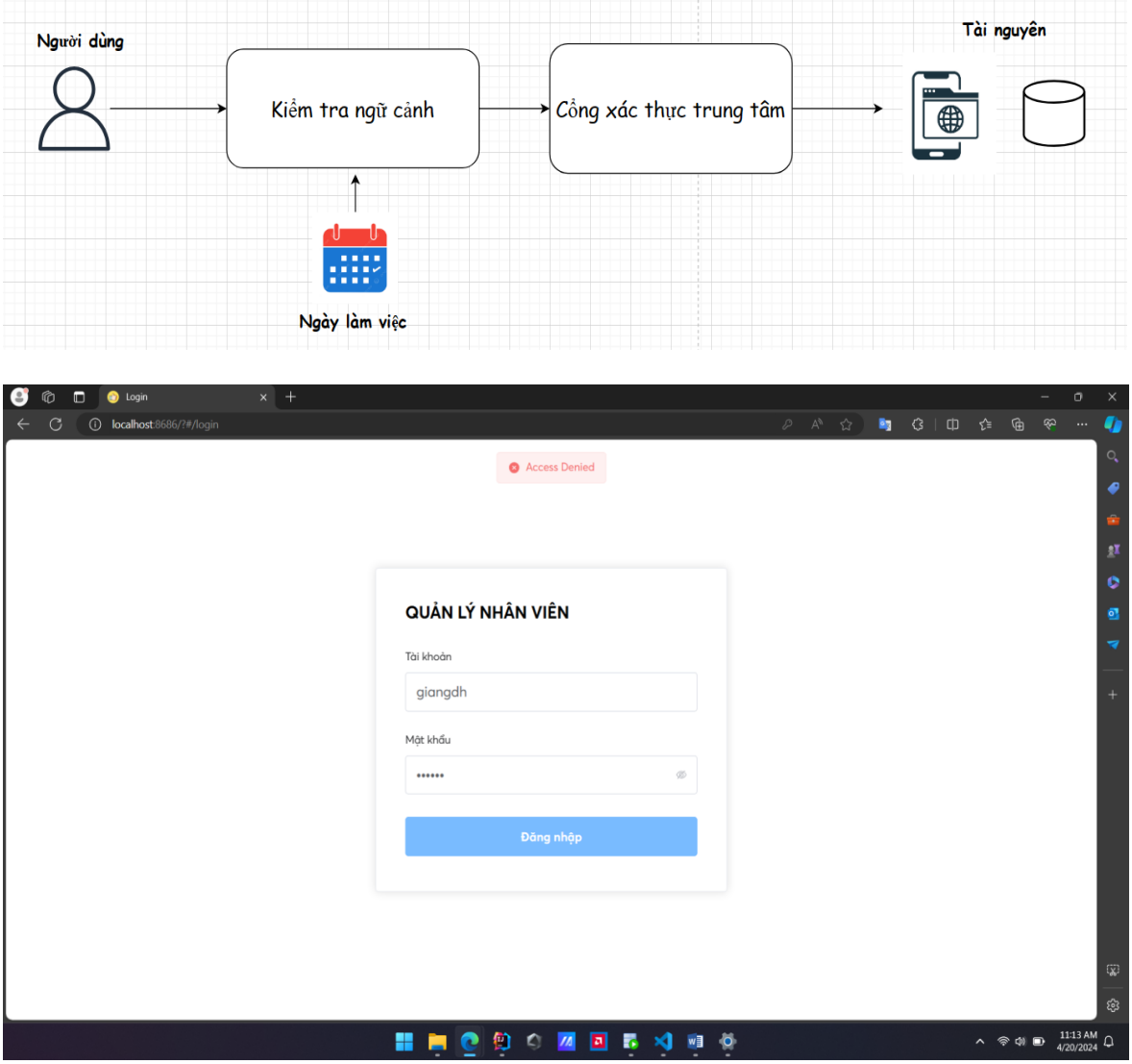


Hình 4.1 Xác thực dựa trên yếu tố giờ làm việc

Trong trường hợp khoảng thời gian truy cập không nằm trong khoảng thời gian cho phép thì xác thực thất bại.

Kiểm tra ngày cho phép truy cập

Mục tiêu: Đảm bảo rằng hệ thống chỉ cho phép truy cập vào ngày làm việc hành chính, từ thứ 2 đến thứ 6.



Hình 4.2 Xác thực dựa trên yếu tố ngày làm việc

Trong trường hợp khoảng thời gian truy cập thuộc thứ bảy hoặc chủ nhật thì xác thực thất bại.

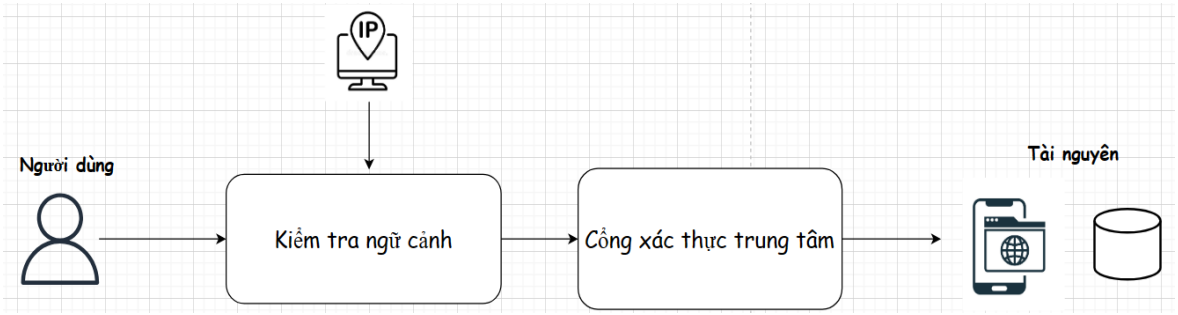
Kiểm tra địa chỉ IP và địa chỉ MAC cho phép truy cập

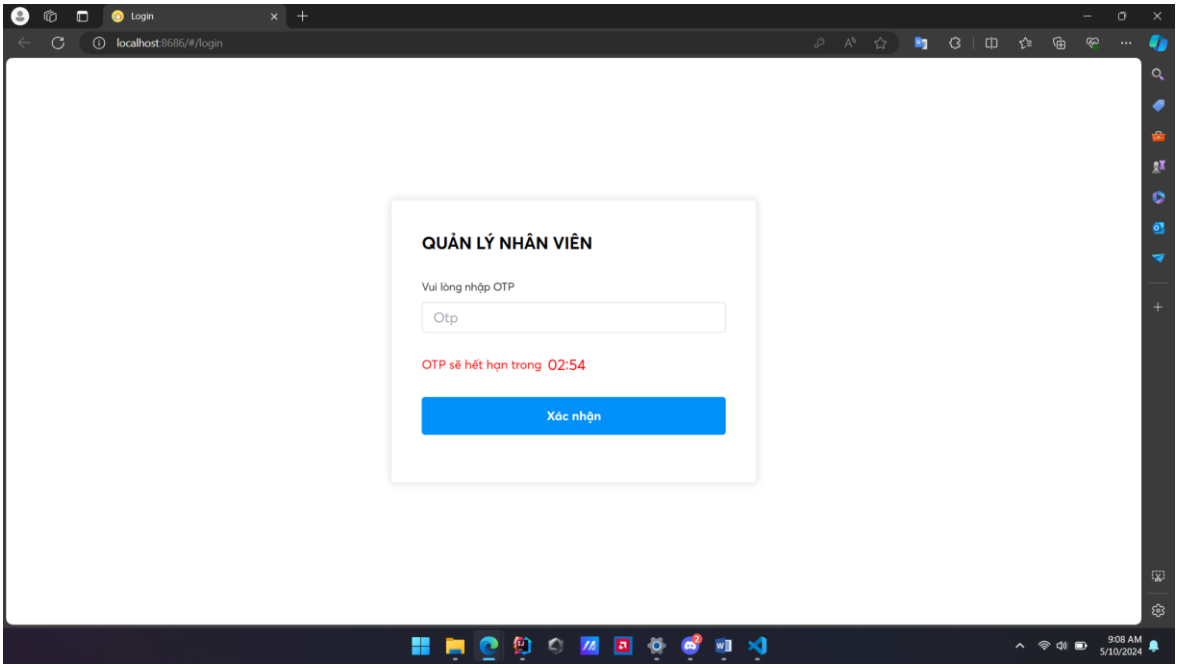
Mục tiêu: Đảm bảo rằng hệ thống chỉ cho phép thiết bị với dải IP cho phép được truy cập, trong trường hợp IP thiết bị không thuộc dải IP cho phép thì kiểm tra địa chỉ MAC thiết bị có nằm trong danh sách MAC được cho phép truy cập không.

Trường hợp nằm trong vùng mạng cho phép

```
Link-local IPv6 Address . . . . . : fe80::5c55:e758:a4e2:592d%13(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.1.176(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Hình 4.3 Cấu hình IPv4 thiết bị





Hình 4.4 Xác thực dựa trên yếu tố địa chỉ IP

Trong trường hợp này, thiết bị sử dụng truy cập hệ thống đang có địa chỉ IP là 192.168.1.176, nằm trong dải IP cho phép của hệ thống (Được mô tả ở hình 3.5) nên xác thực thành công và chuyển đến phần xác thực OTP.

Trường hợp nằm ngoài vùng mạng cho phép

	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

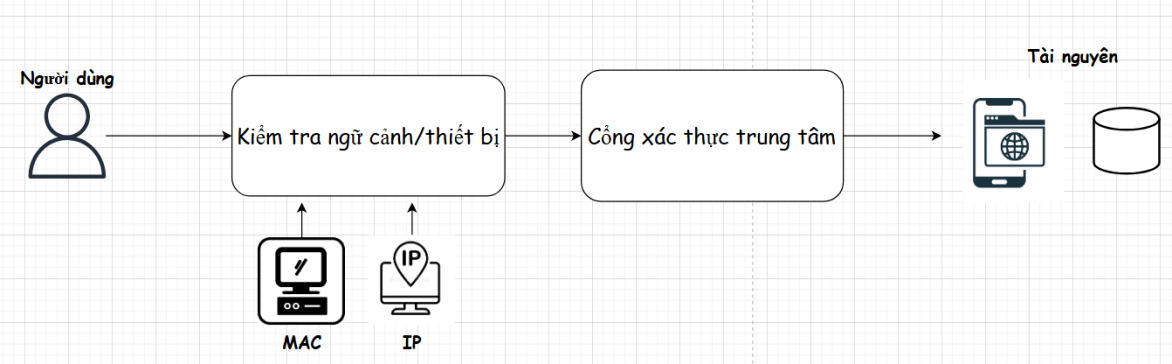
Hình 4.5 Bảng lưu trữ thông tin địa chỉ MAC được phép truy cập hệ thống

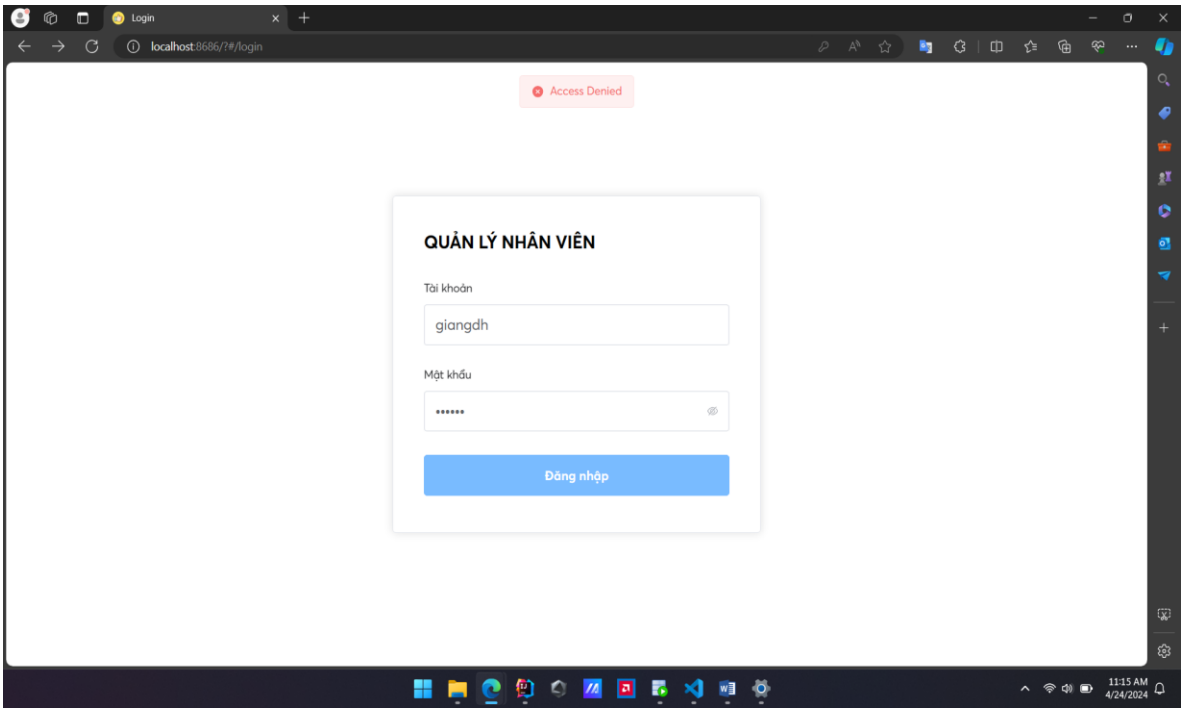
```
Physical Address    Transport Name
=================== ============================================================
10-68-38-15-8B-85   \Device\Tcpip_{C3F3F810-DDE7-4B3A-B2C1-A741A3EFF277}
C8-7F-54-A5-CF-74   Media disconnected
10-68-38-15-8B-84   Media disconnected
```

Hình 4.6 Địa chỉ MAC thiết bị truy cập hệ thống

```
IPv6 Address. . . . . . . . . . . : 2001:ee0:22f:3409:bd25:4cb3:1f44:75c4(Preferred)
Temporary IPv6 Address. . . . . . : 2001:ee0:22f:3409:7110:520f:6713:6f20(Preferred)
Link-local IPv6 Address . . . . . : fe80::5c55:e758:a4e2:592d%13(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.74.213(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Hình 4.7 Địa chỉ IP thiết bị truy cập hệ thống

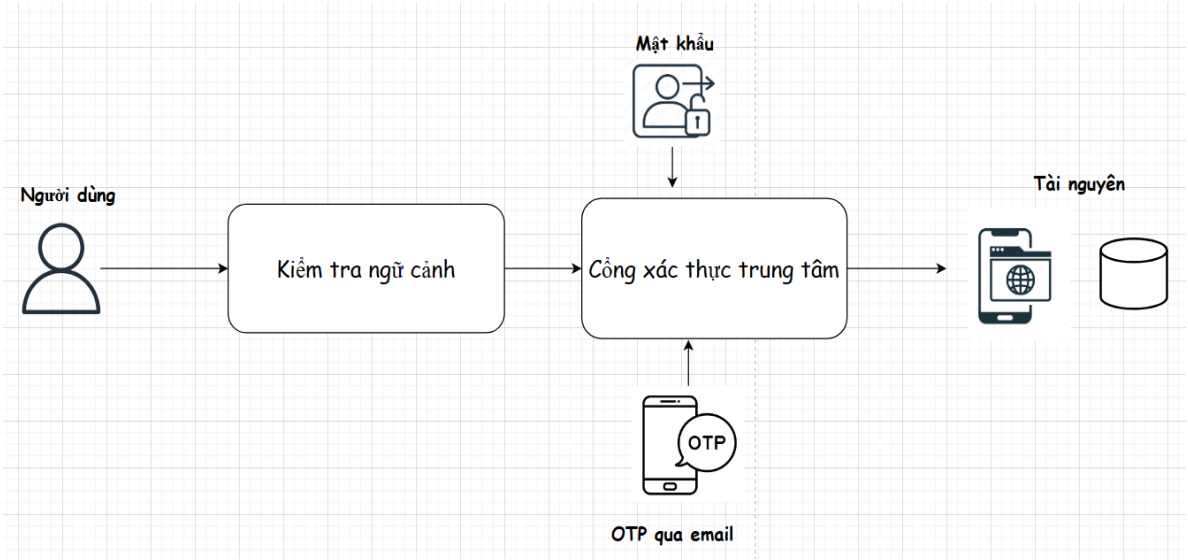


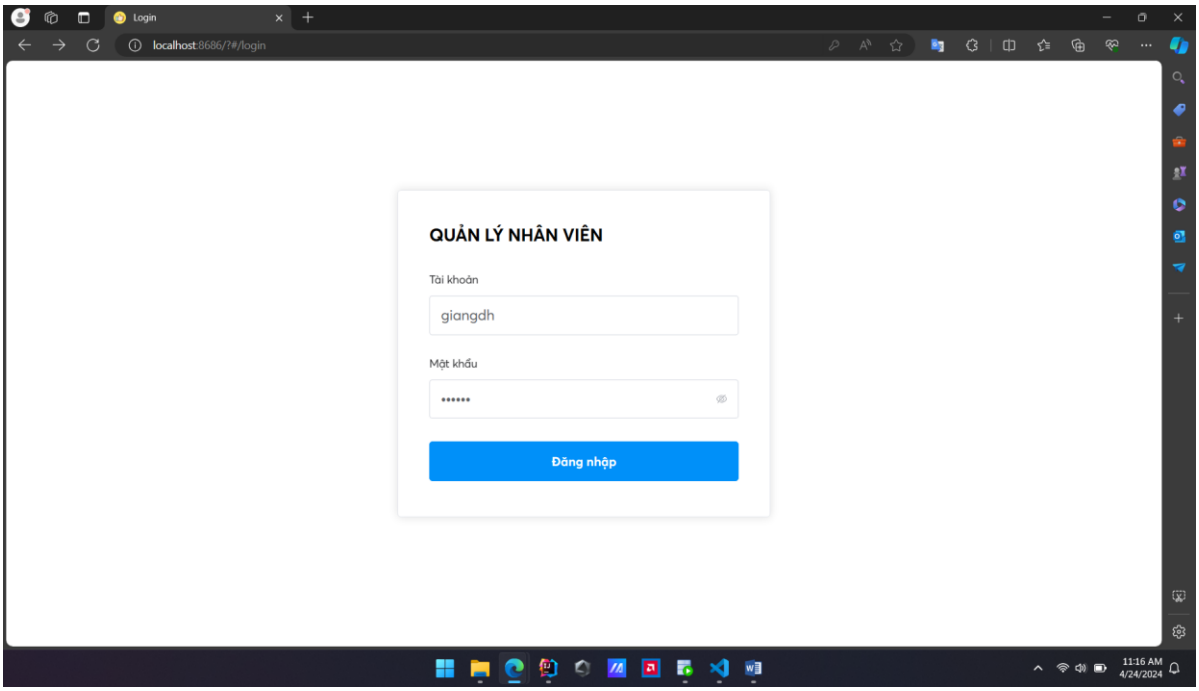


Hình 4.8 Xác thực dựa trên địa chỉ MAC

Trong trường hợp này, thiết bị sử dụng truy cập hệ thống đang có địa chỉ IP là 192.168.74.213, không nằm trong dải IP cho phép của hệ thống (Được mô tả ở hình 3.5) nên ta xét đến địa chỉ MAC của thiết bị truy cập hệ thống. Ta thấy địa chỉ MAC của thiết bị không nằm trong dải MAC thiết bị cho (Được mô tả ở hình 4.5 và hình 4.6) nên xác thực thất bại.

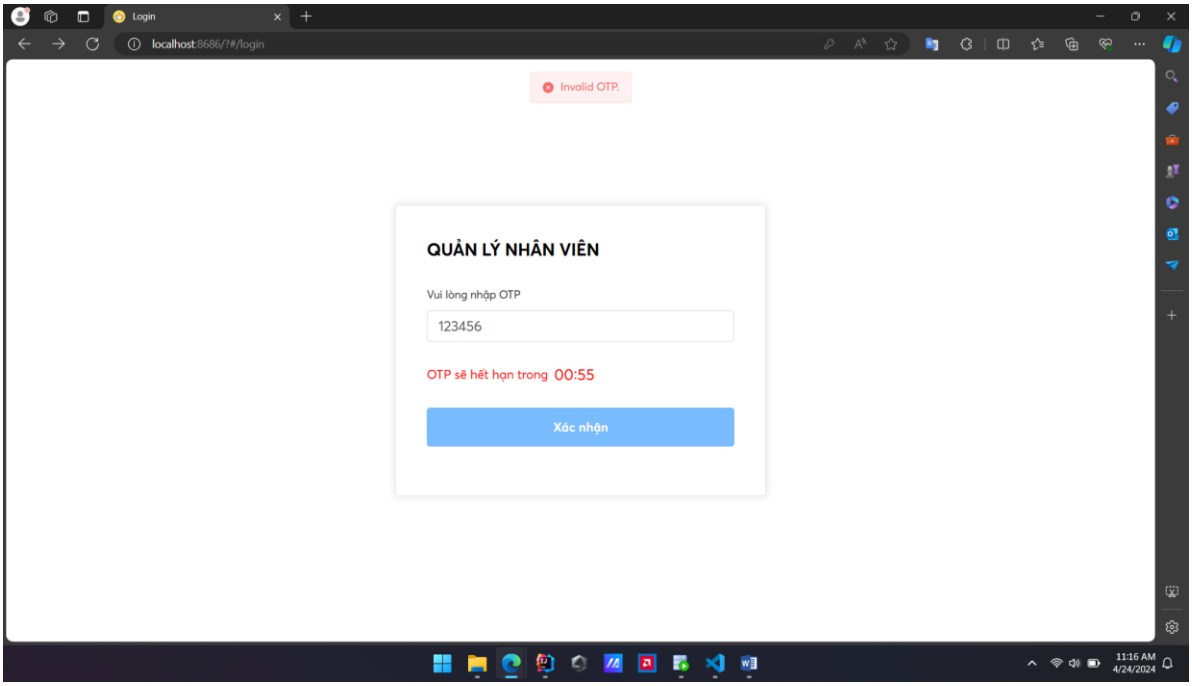
Kiểm tra xác thực đa yếu tố





Hình 4.9 Xác thực bằng việc đăng nhập sử dụng tài khoản và mật khẩu

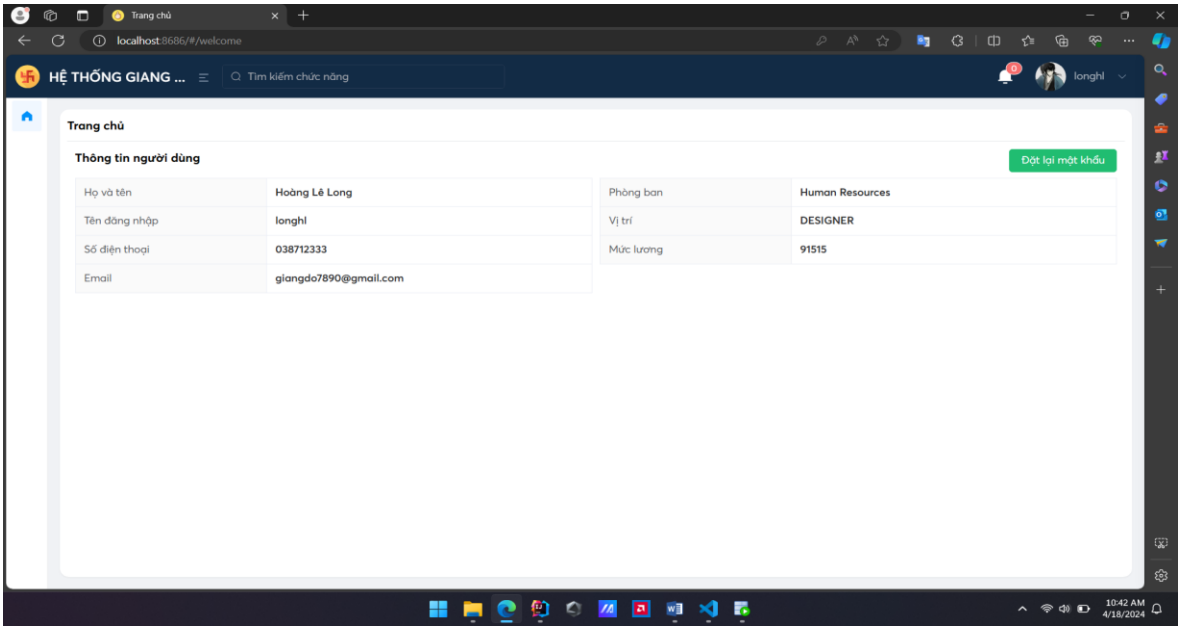
Sau khi đăng nhập với tài khoản và mật khẩu thành công, một mã OTP gồm 6 chữ số sẽ được gửi về email của người dùng, thời gian hiệu lực là 3 phút.



Hình 4.10 Xác thực OTP

Trong trường hợp nhập sai mã OTP, xác thực thất bại.

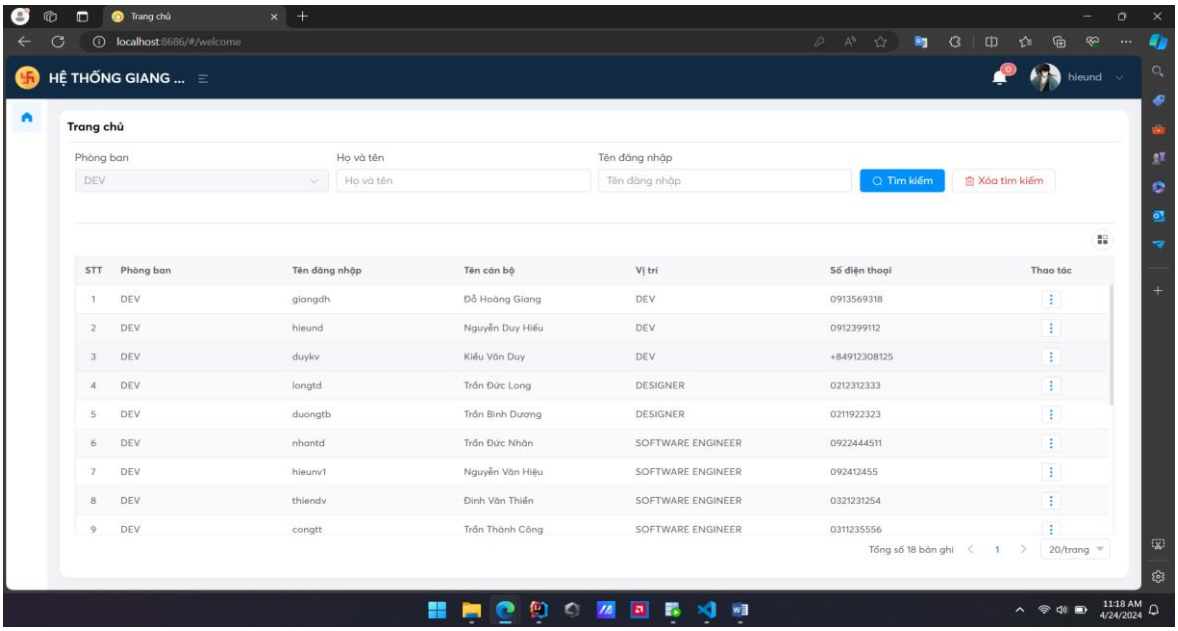
Phân quyền cho vai trò USER



Hình 4.11 Giao diện đăng nhập của người dùng quyền USER

Sau khi đáp ứng đủ các yêu cầu xác thực chính sách bảo mật và xác thực đa yếu tố. Người dùng với vai trò USER đăng nhập có giao diện như hình 4.11. Người dùng với quyền USER sẽ chỉ xem được thông tin của chính họ.

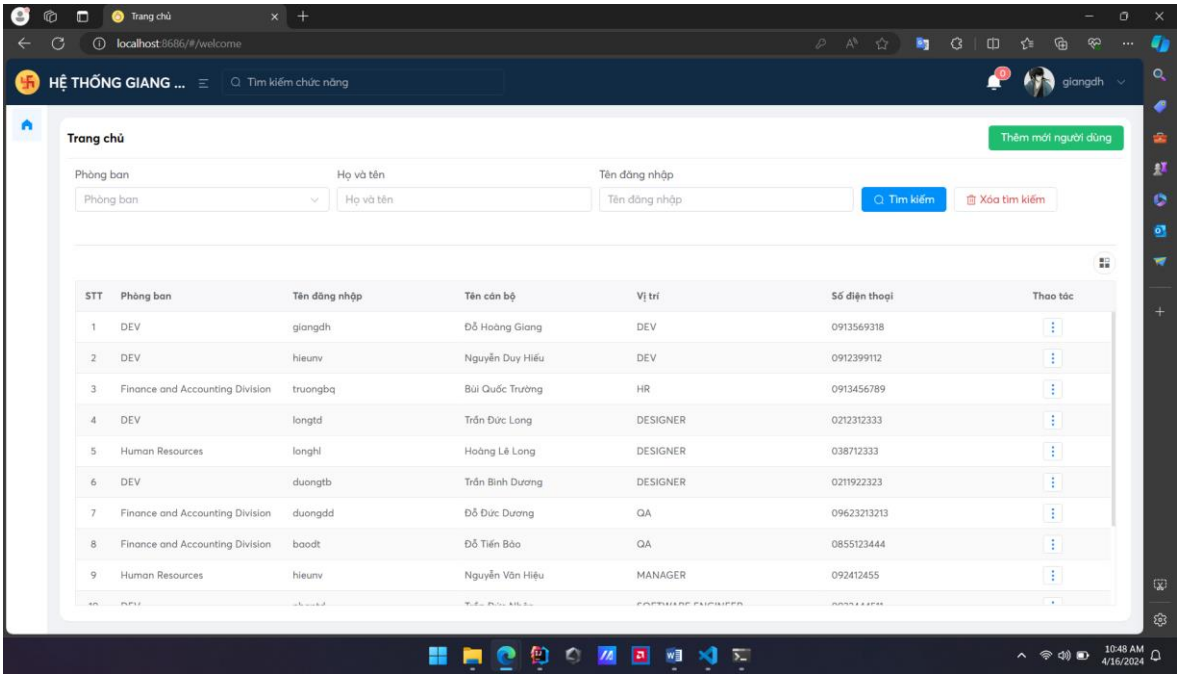
Phân quyền cho vai trò MANAGER



Hình 4.12 Giao diện đăng nhập của người dùng quyền MANAGER

Sau khi đáp ứng đủ các yêu cầu xác thực chính sách bảo mật và xác thực đa yếu tố. Người dùng với vai trò MANAGER đăng nhập có giao diện như hình 4.12. Người dùng với vai trò MANAGER có thể tìm kiếm thông tin của tất cả người dùng thuộc phòng ban do MANAGER quản lý, cụ thể như trong hình 4.12 người dùng sẽ xem được thông tin của tất cả người dùng thuộc phòng DEV.

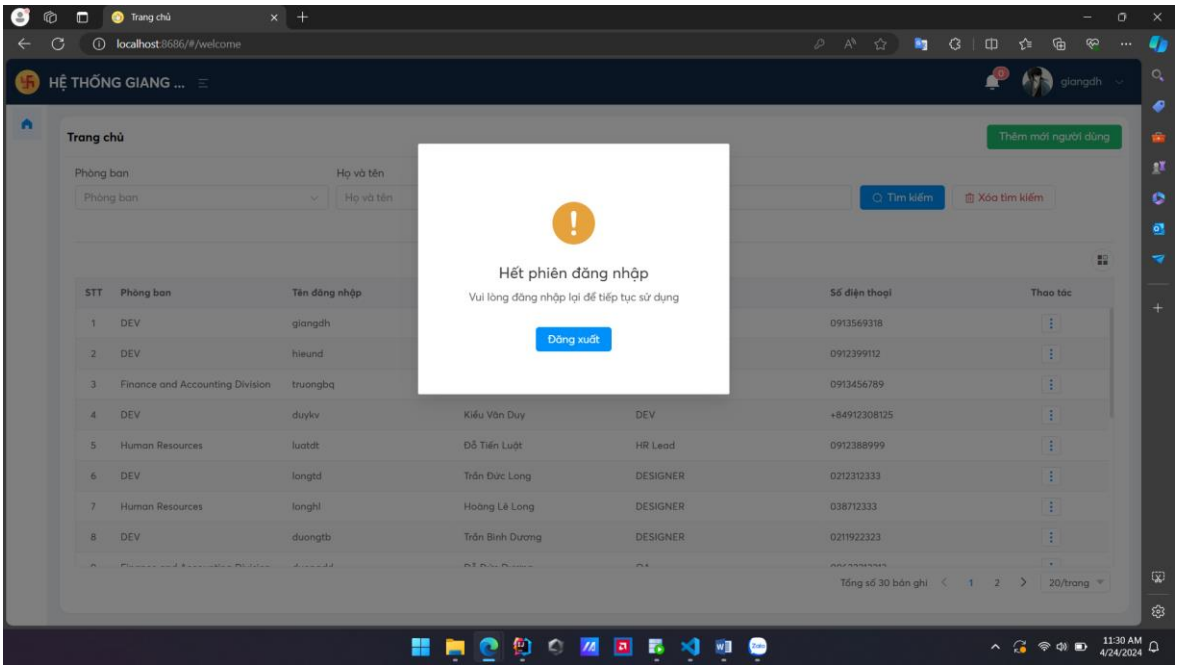
Phân quyền cho vai trò ADMIN



Hình 4.13 Giao diện đăng nhập của người dùng quyền ADMIN

Sau khi đáp ứng đủ các yêu cầu xác thực chính sách bảo mật và xác thực đa yếu tố. Người dùng với vai trò ADMIN đăng nhập có giao diện như hình 4.13. Người dùng với vai trò ADMIN có thể tìm kiếm thông tin của tất cả người dùng trong tổ chức, thêm mới, sửa thông tin và xóa người dùng khác.

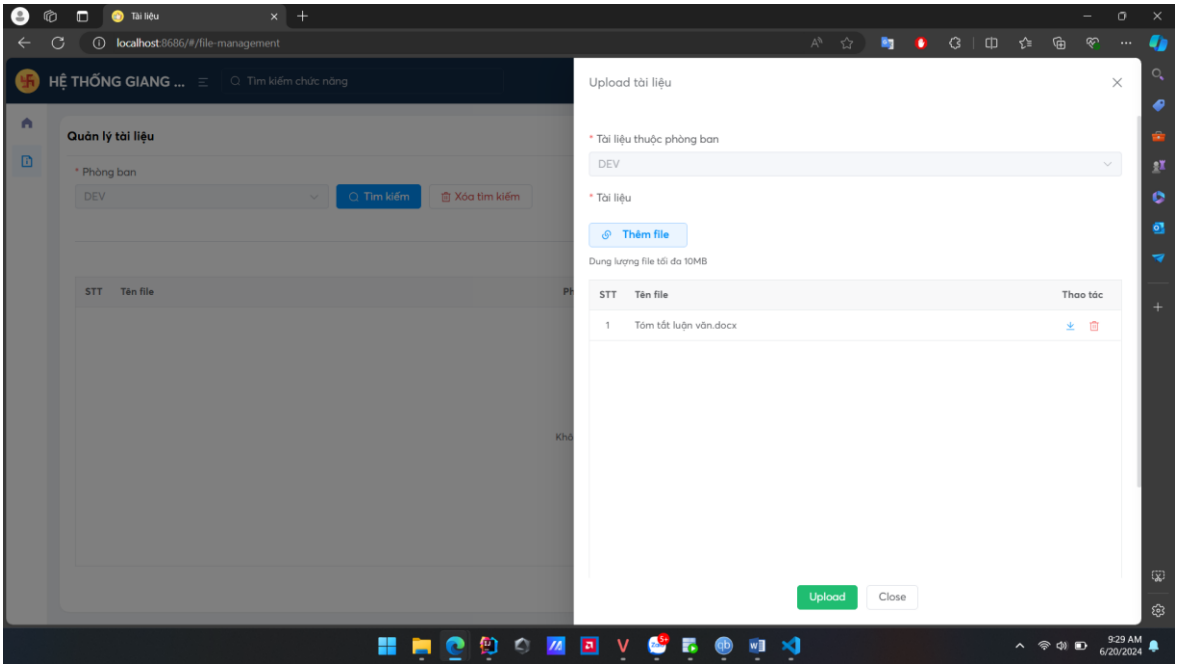
Tự động xác thực lại sau khoảng thời gian



Hình 4.14 Tự động xác thực sau khoảng thời gian

Hệ thống cũng đã được cấu hình để mặc định sau 30 phút sẽ yêu cầu người dùng đăng xuất và cần đăng nhập lại để xác thực thông tin.

Phân quyền cho việc tải lên và tải xuống file



Hình 4.15 Phân quyền cho việc tải lên và tải xuống file

Quản trị viên có quyền tải xuống và tải lên bất kỳ file nào từ mọi phòng ban, điều này cần thiết để quản lý hệ thống tổng thể và thực hiện các tác vụ bảo mật. Người dùng và quản lý chỉ có quyền tải xuống các file thuộc về phòng ban của họ. Ví dụ, người dùng với vai trò MANAGER_DEV và USER thuộc phòng ban DEV có thể tải xuống các file do MANAGER_DEV tải lên, nhưng không thể truy cập file từ phòng HR hoặc Finance. Điều này giúp ngăn chặn việc truy cập trái phép và bảo vệ dữ liệu nhạy cảm của từng phòng ban.

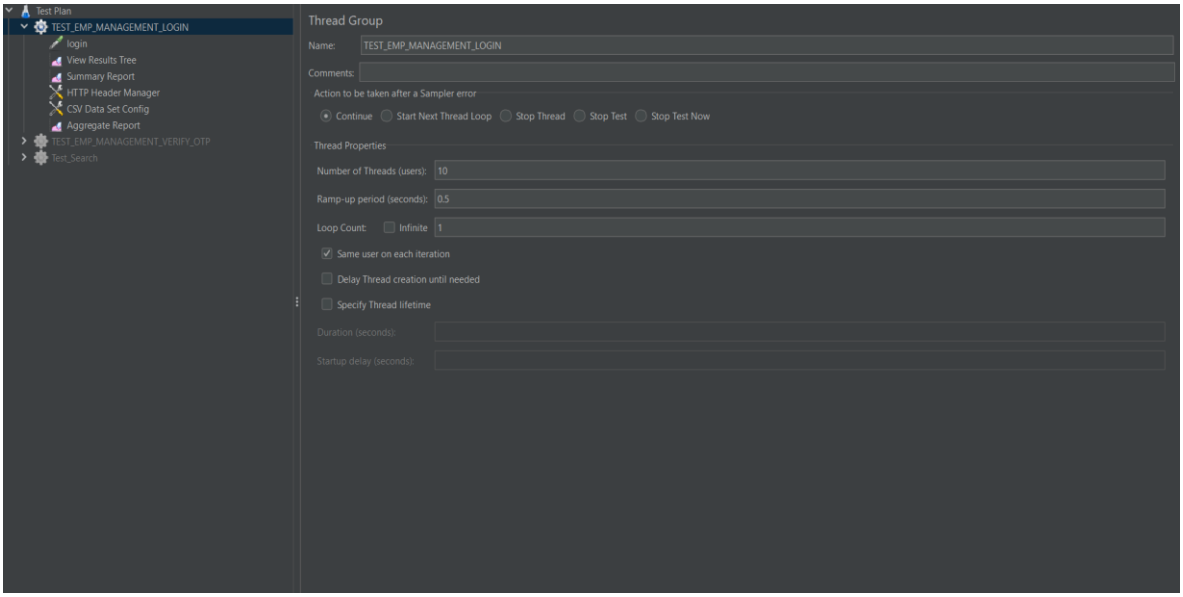
Phân quyền được thực hiện thông qua việc kiểm tra vai trò và phòng ban của người dùng trong quá trình yêu cầu truy cập. Hệ thống sẽ xác thực danh tính người dùng, kiểm tra quyền truy cập và phòng ban trước khi cho phép tải lên hoặc tải xuống file. Chính sách này giúp bảo vệ dữ liệu một cách hiệu quả, đảm bảo rằng chỉ những người dùng có thẩm quyền mới có thể truy cập vào tài nguyên cần thiết.

4.3. Đánh giá hiệu suất và tính bảo mật của mô hình

4.3.1 Kiểm tra hiệu suất hệ thống

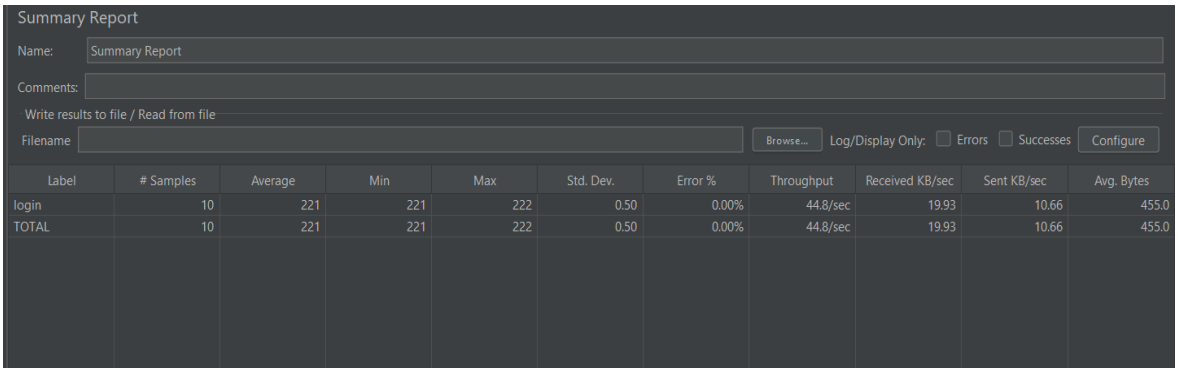
Để đánh giá hiệu suất của hệ thống, tôi đã sử dụng Jmeter để kiểm tra hiệu suất. Tôi đã cài đặt để kiểm tra hiệu suất cho từng API cụ thể. Ở phần này tôi sẽ tập trung vào việc kiểm tra hiệu suất các API dùng chung nhiều.

API Đăng nhập



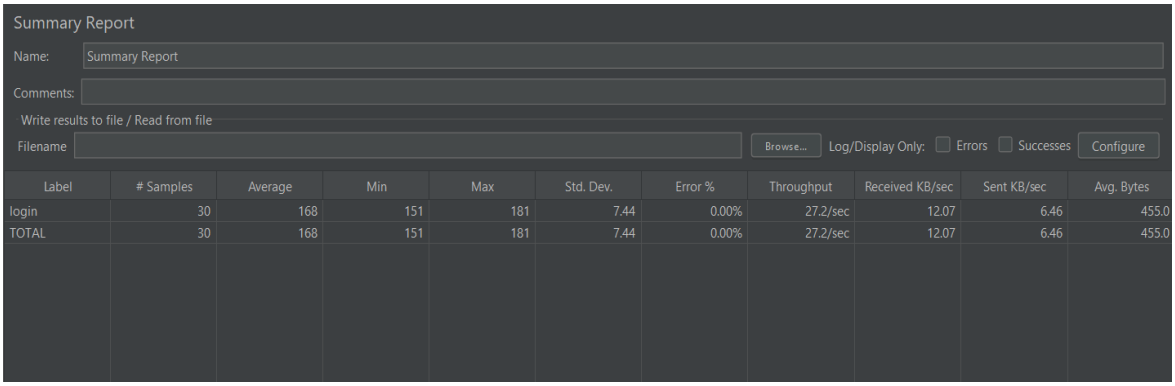
Hình 4.16 Cài đặt thông số kiểm thử trên Jmeter

Tôi đã cài đặt kiểm thử đối với 10 threads (tương ứng với 10 users) và thời gian để khởi động toàn bộ 10 threads là 0.5s. Kết quả đầu ra đạt được như ảnh dưới:



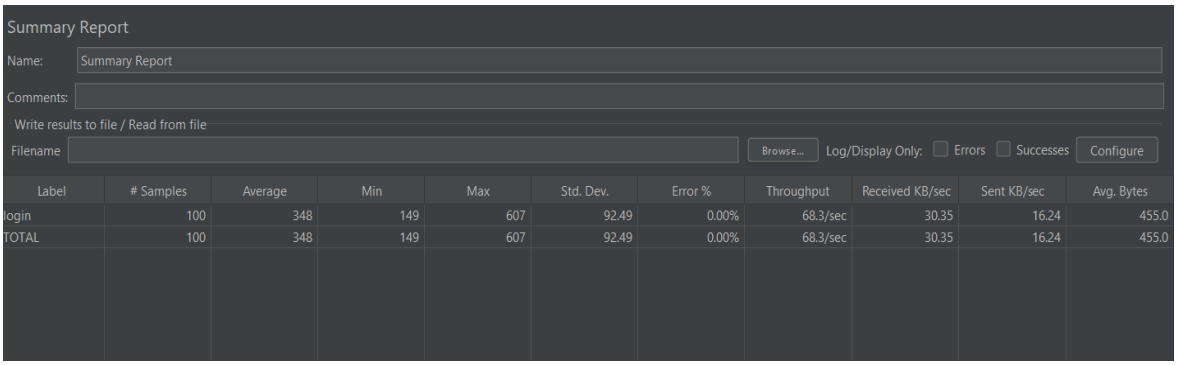
Hình 4.17 Kết quả kiểm tra API Đăng nhập với 10 người dùng

Ta có thể thấy thời gian phản hồi ngắn nhất và dài nhất ghi nhận là 221 ms và 222 ms, tương ứng, cho thấy rằng thời gian phản hồi có độ biến thiên rất thấp và ổn định. Độ lệch chuẩn của thời gian phản hồi là 0.50 ms, cho thấy thời gian phản hồi giữa các mẫu rất gần với giá trị trung bình và ổn định. Không có lỗi nào được ghi nhận, chứng tỏ tất cả yêu cầu đăng nhập đều thành công. Tốc độ xử lý là 44.8 yêu cầu mỗi giây, phản ánh khả năng xử lý tải của hệ thống.



Hình 4.18 Kết quả kiểm tra API Đăng nhập với 30 người dùng

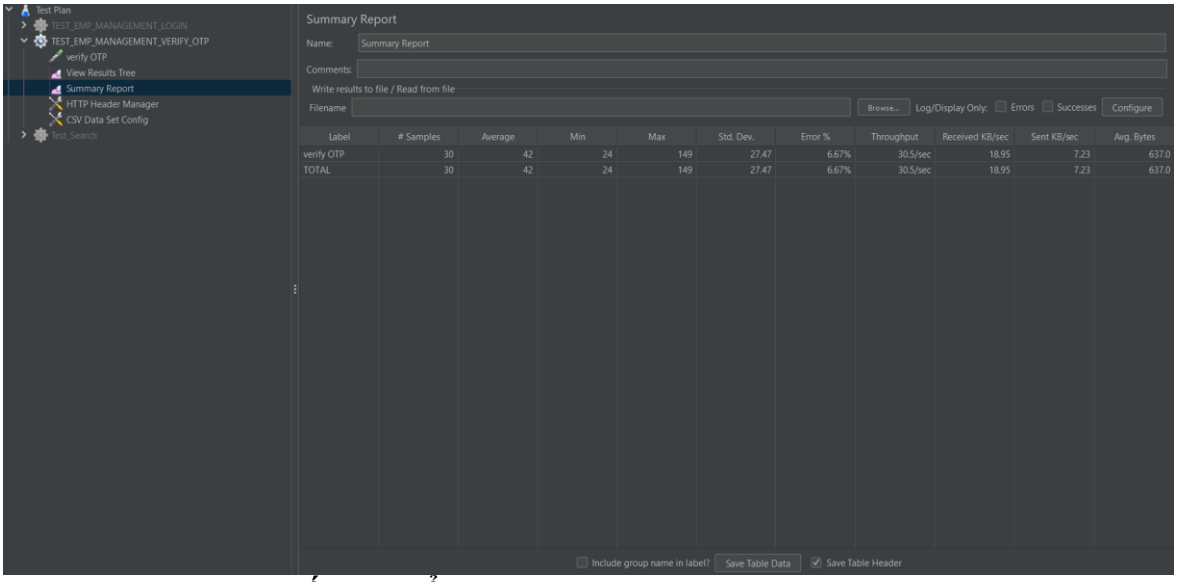
Tiếp đến tôi thử kiểm tra với 30 threads và thời gian hoàn thành trong 1s. Thời gian phản hồi trung bình của yêu cầu là 168 milliseconds. Điều này cho thấy API đáp ứng nhanh chóng, đồng thời duy trì thời gian phản hồi thấp ngay cả khi số lượng yêu cầu tăng lên. Thời gian phản hồi nhanh nhất và chậm nhất lần lượt là 151 và 181 milliseconds, phản ánh biên độ thời gian phản hồi từ tốt nhất đến xấu nhất. Sự chênh lệch này vẫn nằm trong giới hạn chấp nhận được cho trải nghiệm người dùng. Độ lệch chuẩn là 7.44, chỉ ra một phần mức độ biến động trong thời gian phản hồi giữa các lần thử. Mặc dù có sự biến động, nhưng nó không đáng kể và không ảnh hưởng tiêu cực đến hiệu suất chung của API. Số lượng yêu cầu xử lý trên giây là 27.2, cho thấy khả năng xử lý tốt dưới tải cao.



Hình 4.19 Kết quả kiểm tra API Đăng nhập với 100 người dùng

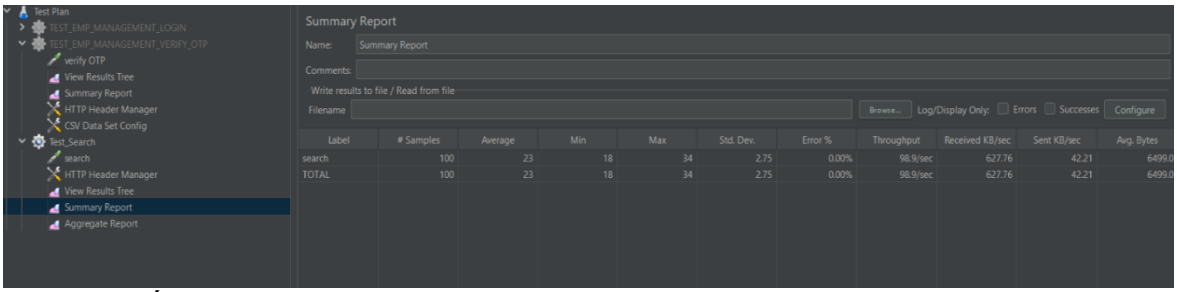
Tiếp đến tôi thử kiểm tra với 100 threads và thời gian hoàn thành trong 1s. Thời gian phản hồi trung bình là 348 milliseconds, tăng đáng kể so với thử nghiệm trước, phản ánh việc tải lớn hơn có ảnh hưởng tới thời gian xử lý yêu cầu. Độ lệch chuẩn cao ở mức 92.49, điều này chỉ ra sự không nhất quán lớn trong thời gian phản hồi, có thể do hệ thống bị áp lực bởi số lượng yêu cầu cao. Tuy nhiên số lượng yêu cầu trên giây là 68.3, tăng đáng kể so với kiểm thử trước, cho thấy hệ thống vẫn có khả năng xử lý một số lượng lớn yêu cầu.

API Xác thực OTP



Hình 4.20 Kết quả kiểm tra API Xác thực OTP với 30 người dùng

Tôi kiểm tra hiệu suất API xác thực OTP với đầu vào là 30 threads và thời gian hoàn thành là 1s. Kết quả đạt được như ảnh. Thời gian phản hồi trung bình là 42 milliseconds, cho thấy rằng API rất nhanh chóng xử lý yêu cầu OTP. Thời gian phản hồi nhanh nhất và chậm nhất lần lượt là 24 và 149 milliseconds, cho thấy sự dao động của thời gian phản hồi nhưng vẫn trong phạm vi chấp nhận được. Độ lệch chuẩn là 27.47 milliseconds, một con số tương đối thấp, cho thấy sự nhất quán trong phản hồi của API dù có sự biến động nhất định. Số lượng yêu cầu được xử lý mỗi giây là 30.5, phản ánh khả năng xử lý của API dưới tải.



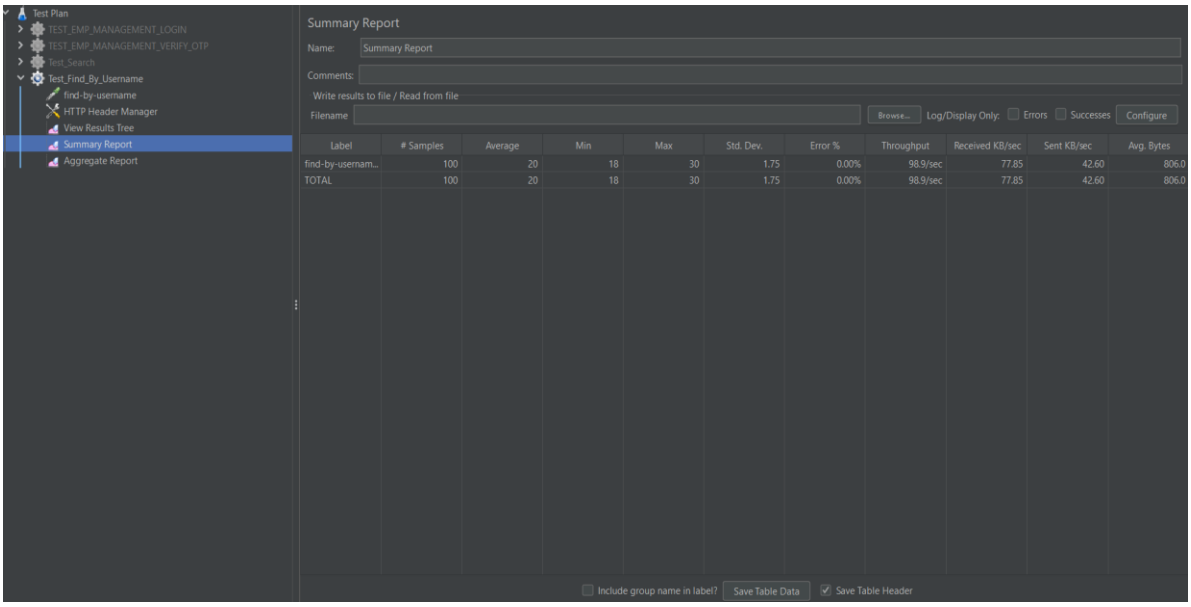
API tìm kiếm thông tin người dùng

Hình 4.21 Kết quả kiểm tra API Tìm kiếm thông tin với 100 người dùng

Tôi kiểm tra hiệu suất API tìm kiếm thông tin với đầu vào là 100 threads và thời gian hoàn thành là 1s. Kết quả đạt được như ảnh. Thời gian phản hồi trung bình cho mỗi

yêu cầu là 23 ms, điều này chỉ ra rằng API rất nhanh và hiệu quả trong việc xử lý các yêu cầu tìm kiếm. Thời gian phản hồi nhanh nhất và chậm nhất lần lượt là 18 và 34 milliseconds, cho thấy sự nhất quán và đáng tin cậy của API dưới tải. Độ lệch chuẩn là 2.75 milliseconds, một con số thấp, phản ánh mức độ biến động rất thấp trong thời gian phản hồi giữa các yêu cầu. API xử lý được 98.9 yêu cầu mỗi giây, một kết quả ấn tượng cho thấy rằng hệ thống có thể duy trì hiệu suất cao ngay cả khi gặp áp lực lớn từ yêu cầu của người dùng.

API xem chi tiết thông tin người dùng



Hình 4.22 Kết quả kiểm tra API Xem chi tiết với 100 người dùng

Tôi kiểm tra hiệu suất API xem chi tiết thông tin người dùng với đầu vào là 100 threads và thời gian hoàn thành là 1s. Kết quả đạt được như ảnh. Thời gian phản hồi trung bình là 20 milliseconds, cho thấy API xử lý yêu cầu một cách nhanh chóng. Độ lệch chuẩn thấp, ở mức 1.75 milliseconds, chỉ ra rằng phản hồi của hệ thống rất ổn định qua các lần thực hiện. Số lượng yêu cầu xử lý mỗi giây là 98.9, phản ánh khả năng xử lý tốt của hệ thống.

4.3.2 Đánh giá hoạt động của hệ thống

Qua trình bày ở phần trước, ta có thể thấy xác thực mạnh mẽ thông qua OTP và quy trình đăng nhập đa yếu tố đã được triển khai, như được chứng minh qua các

bước kiểm thử hiệu suất. Hệ thống được đánh giá dựa trên sự gia tăng dần dần số lượng threads, mỗi thread mô phỏng một người dùng đồng thời gửi yêu cầu tới hệ thống. Kết quả cho thấy rằng khi số lượng threads đạt đến 100, thời gian phản hồi trung bình vẫn duy trì ở mức thấp, và không có lỗi nào được ghi nhận, cho thấy rằng hệ thống có thể chịu đựng ít nhất 100 người dùng đồng thời mà không bị ảnh hưởng đáng kể về hiệu suất. Tất cả các yêu cầu đăng nhập đều được kiểm tra với một khoảng thời gian phản hồi trung bình chỉ 20 milliseconds, cho thấy quá trình xác thực không những nhanh chóng mà còn đáng tin cậy. Ủy quyền được thực hiện thông qua việc kiểm tra chặt chẽ các quyền truy cập đối với mỗi hành động người dùng, đảm bảo rằng mọi yêu cầu đều phù hợp với chính sách và quyền lợi đã được đặt ra. Tất cả dữ liệu truyền tải đều được mã hóa bằng các giao thức an toàn nhất hiện nay, và kích thước phản hồi trung bình ở mức 806.0 bytes cho thấy một lượng dữ liệu phù hợp để đảm bảo tính bảo mật mà không làm giảm hiệu suất hệ thống. Mã hóa end-to-end giúp bảo vệ thông tin người dùng và dữ liệu quan trọng khỏi sự nhìn ngó của kẻ tấn công.

Mô hình bảo mật được đánh giá là vượt trội, không chỉ trong việc bảo vệ dữ liệu và ngăn chặn truy cập không được phép, mà còn trong việc đảm bảo rằng hiệu suất hệ thống không bị ảnh hưởng tiêu cực dưới tải lớn hoặc trong tình huống khẩn cấp. Kiểm thử hiệu suất bảo mật đã chứng minh rằng mô hình không những đáp ứng được các yêu cầu về tốc độ và ổn định, mà còn cung cấp một lớp bảo vệ vững chắc, phù hợp với nguyên tắc Zero Trust, qua đó đặt nền tảng vững chắc cho một môi trường làm việc số an toàn và đáng tin cậy.

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)