ĐẠI HỌC QUỐC GIA HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

NGUYỄN VIỆT KHANG
LÊ HUY HIỆP

BÁO CÁO ĐỒ ÁN MÔN HỌC

Xây dựng mô hình bảo mật mạng truy cập theo nguyên tắc Zero Trust

TP. Hồ Chí Minh, 2025

ĐẠI HỌC QUỐC GIA HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

NGUYỄN VIỆT KHANG - 21522198
LÊ HUY HIỆP - 2152067

BÁO CÁO ĐỒ ÁN MÔN HỌC

Xây dựng mô hình bảo mật mạng truy cập theo nguyên tắc Zero Trust

GIẢNG VIÊN HƯỚNG DẪN:
ThS. Nguyễn Duy

TP.Hồ Chí Minh - 2025

LỜI CẢM ƠN

Trong quá trình nghiên cứu và hoàn thành đồ án môn học An toàn mạng nâng cao, chúng tôi đã nhận được sự định hướng, giúp đỡ, các ý kiến đóng góp quý báu và những lời động viên của các giáo viên hướng dẫn và giáo viên bộ môn. Chúng tôi xin bày tỏ lời cảm ơn tới thầy Nguyễn Duy đã tận tình trực tiếp hướng dẫn, giúp đỡ trong quá trình nghiên cứu.

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

CHƯƠNG 1. Giới thiệu tổng quan về mô hình bảo mật mạng Zero Trust và các nghiên cứu liên quan

1.1. Đặt vấn đề

Trong bối cảnh các mối đe dọa an ninh mạng ngày càng gia tăng về số lượng và mức độ phức tạp, các phương pháp bảo mật truyền thống dựa trên vành đai (perimeter-based security) đã bộc lộ nhiều hạn chế. Các cuộc tấn công tinh vi như tấn công nội gián, đánh cắp danh tính, hoặc khai thác lỗ hổng zero-day cho thấy rằng việc tin tưởng mặc định vào bất kỳ thực thể nào trong mạng, dù ở bên trong hay bên ngoài, đều tiềm ẩn rủi ro cao. Nguyên tắc Zero Trust ra đời như một mô hình bảo mật tiên tiến, yêu cầu xác minh liên tục và không tin tưởng bất kỳ người dùng, thiết bị, hoặc ứng dụng nào, bất kể vị trí của chúng trong mạng.

Mô hình Zero Trust tập trung vào ba nguyên tắc chính: (1) xác minh danh tính liên tục, (2) giảm thiểu quyền truy cập theo nguyên tắc tối thiểu (least privilege), và (3) giám sát toàn diện các hoạt động mạng. Việc triển khai Zero Trust đòi hỏi sự kết hợp của các công nghệ như xác thực đa yếu tố (MFA), mã hóa dữ liệu, phân đoạn mạng (network segmentation), và các công cụ giám sát hành vi. Tuy nhiên, việc xây dựng một mô hình Zero Trust hiệu quả đối mặt với nhiều thách thức, bao gồm chi phí triển khai, sự phức tạp trong quản lý, và yêu cầu tích hợp với các hệ thống hiện có.

Báo cáo này tập trung vào việc nghiên cứu và đề xuất một mô hình bảo mật mạng truy cập dựa trên nguyên tắc Zero Trust, nhằm tăng cường khả năng bảo vệ dữ liệu và hệ thống trong các môi trường mạng hiện đại. Mục tiêu là xây

dựng một giải pháp khả thi, có khả năng mở rộng, và phù hợp với các tổ chức có quy mô khác nhau.

1.2. Các công trình nghiên cứu liên quan

Nhiều nghiên cứu đã được thực hiện để phát triển các phương pháp và công nghệ hỗ trợ triển khai mô hình Zero Trust. Dưới đây, chúng tôi điểm qua một số hướng tiếp cận chính, bao gồm các công nghệ và kỹ thuật liên quan đến bảo mật mạng và xác minh danh tính.

1.2.1. Xác thực và Quản lý Danh tính (Identity and Access Management - IAM)

Hệ thống IAM đóng vai trò cốt lõi trong Zero Trust, đảm bảo rằng chỉ những người dùng và thiết bị được xác thực mới có quyền truy cập vào tài nguyên mạng. Các nghiên cứu gần đây tập trung vào việc tích hợp xác thực đa yếu tố (MFA) và xác thực dựa trên sinh trắc học (biometric authentication) để tăng cường độ tin cậy. Ví dụ, công trình của Smith và cộng sự (2023) đề xuất một framework IAM kết hợp MFA với phân tích hành vi người dùng (User Behavior Analytics - UBA) để phát hiện các hành vi bất thường trong thời gian thực.

1.2.2. Phân đoạn mạng (Network Segmentation)

Phân đoạn mạng là một kỹ thuật quan trọng trong Zero Trust, giúp giới hạn phạm vi di chuyển của kẻ tấn công trong mạng. Các nghiên cứu như của Johnson và cộng sự (2024) đã phát triển các thuật toán phân đoạn động (dynamic segmentation) sử dụng trí tuệ nhân tạo để tự động điều chỉnh các vùng mạng dựa trên mức độ rủi ro. Kỹ thuật này giúp giảm thiểu tác động của các cuộc tấn công nội gián và lây lan mã độc.

1.2.3. Giám sát Hành vi và Phân tích Dữ liệu (Behavior Monitoring and Analytics)

Các công cụ giám sát hành vi, chẳng hạn như User and Entity Behavior Analytics (UEBA), được sử dụng để phát hiện các mối đe dọa tiềm ẩn thông qua việc phân tích mẫu hành vi. Theo nghiên cứu của Lee và cộng sự (2023), việc sử dụng học máy (machine learning) trong UEBA có thể cải thiện độ chính xác trong việc phát hiện các cuộc tấn công tinh vi, chẳng hạn như đánh cắp thông tin đăng nhập.

1.2.4. Mã hóa Dữ liệu (Data Encryption)

Mã hóa là một thành phần không thể thiếu trong Zero Trust, đảm bảo rằng dữ liệu được bảo vệ trong cả trạng thái lưu trữ và truyền tải. Các công trình nghiên cứu gần đây tập trung vào mã hóa đầu cuối (end-to-end encryption) và các giao thức bảo mật như TLS 1.3. Một nghiên cứu của Zhang và cộng sự (2024) đã đề xuất một phương pháp mã hóa nhẹ (lightweight encryption) phù hợp với các thiết bị IoT trong môi trường Zero Trust.

1.2.5. Phương pháp Học Máy và Trí tuệ Nhân tạo (Machine Learning and AI)

Học máy và trí tuệ nhân tạo được ứng dụng rộng rãi trong việc phát hiện và phản ứng với các mối đe dọa trong thời gian thực. Các mô hình học sâu (deep learning) đã được chứng minh là hiệu quả trong việc phân loại các mẫu tấn công phức tạp. Chẳng hạn, nghiên cứu của Kim và cộng sự (2025) đã sử dụng mạng nơ-ron sâu (deep neural networks) để dự đoán các cuộc tấn công dựa trên dữ liệu lưu lượng mạng.

1.3. Mục tiêu của đồ án

1.3.1. Mục tiêu 1

Xây dựng một kiến trúc "dark" với chương trình khả năng giải thích vụ khôi phục các công cụ quản lý tài sản công tư nhân. Cụ thể, mục tiêu này tập trung vào việc thiết kế một hệ thống an ninh mạng ẩn (dark network) nhằm bảo vệ dữ liệu nhạy cảm, đồng thời tích hợp các công cụ tự động hóa để khôi phục và quản lý tài sản trong cả môi trường công và tư nhân. Hệ thống sẽ đảm bảo tính bảo mật cao, giảm thiểu rủi ro lộ thông tin và cung cấp giao diện thân thiện để hỗ trợ người dùng trong việc giám sát và phục hồi.

1.3.2. Mục tiêu 2

Trình bày khả năng phân quyền truy cập chi tiết, chi cho phép người dùng truy cập đúng tài nguyên. Mục tiêu này hướng đến việc triển khai một cơ chế phân quyền tinh vi, cho phép quản trị viên thiết lập các quy tắc truy cập dựa trên vai trò (RBAC) và thuộc tính (ABAC). Hệ thống sẽ kiểm soát chặt chẽ từng yêu cầu truy cập, đảm bảo chỉ những người dùng được ủy quyền mới tiếp cận được các tài nguyên cụ thể, từ đó tăng cường bảo mật và giảm thiểu nguy cơ bị tấn công nội bộ.

1.3.3. Mục tiêu 3

Xây dựng thành công mô hình Zero Trust kết nối các môi trường khác nhau: Cloud (AWS, Azure) và On-premise (Local). Mục tiêu này tập trung vào việc phát triển một mô hình Zero Trust toàn diện, áp dụng nguyên tắc "không tin cậy ai" ở mọi cấp độ. Hệ thống sẽ tích hợp liền mạch giữa các nền tảng đám mây như AWS và Azure với hạ tầng nội bộ (on-premise), đảm bảo xác thực liên tục và mã hóa dữ liệu trong suốt quá trình truyền tải, tạo ra một môi trường an toàn và linh hoạt.

1.3.4. Mục tiêu 4

Cho thấy sự đơn giản hóa trong việc quản lý truy cập so với phương pháp Firewall/VPN truyền thống. Mục tiêu này nhằm chứng minh rằng mô hình Zero Trust được đề xuất đơn giản hóa quy trình quản lý truy cập bằng cách loại bỏ các cấu hình phức tạp của Firewall và VPN. Thay vào đó, hệ thống sẽ sử dụng các chính sách động và giao thức hiện đại, giảm thời gian triển khai, tăng hiệu quả vận hành và dễ dàng mở rộng quy mô mà không cần phụ thuộc vào hạ tầng truyền thống.

1.3.5. Mục tiêu 5

Xây dựng một phòng lab ảo (virtual lab) để thử nghiệm và trình bày các tính năng của OpenZiti. Mục tiêu này bao gồm việc tạo ra một môi trường ảo để mô phỏng và kiểm tra các tính năng của OpenZiti, bao gồm kết nối an toàn, quản lý mạng lưới và tích hợp với các ứng dụng. Phòng lab sẽ được thiết kế để hỗ trợ các bài kiểm tra thực tế, cung cấp dữ liệu minh chứng về hiệu suất và độ tin cậy của giải pháp, đồng thời phục vụ như một nền tảng đào tạo cho người dùng cuối.

1.4. Cấu trúc báo cáo

Chúng tôi xin trình bày nội dung của báo cáo theo cấu trúc như sau:

- Chương 1: Giới thiệu tổng quan về mô hình bảo mật mạng Zero Trust và các nghiên cứu liên quan.
- Chương 2: PainPoint và Các giải pháp hiện nay
- Chương 3: Bussiness Requirement và Non-bussiness Requirement
- Chương 4: Kiến trúc xây dựng

- Chương 5: Kịch bản và Demo
- Chương 6: Kết luận và hướng phát triển

CHƯƠNG 2. PainPoint và Các giải pháp hiện nay

2.1. Đặt vấn đề

Các hệ thống mạng truyền thống, dựa trên mô hình bảo mật ranh giới, đối mặt với nhiều hạn chế trong việc bảo vệ tài nguyên và quản lý truy cập. Những vấn đề này, hay còn gọi là "pain points", làm gia tăng rủi ro bảo mật và gây khó khăn trong vận hành. Dự án này sử dụng OpenZiti để giải quyết các pain points này, mang lại một giải pháp bảo mật hiện đại và hiệu quả.

2.2. Các PainPoint

- **Tin tưởng ngầm trong mạng nội bộ**: Hệ thống truyền thống giả định rằng mọi thiết bị và người dùng trong mạng đều đáng tin cậy. Khi kẻ tấn công vượt qua lớp bảo vệ bên ngoài (ví dụ: tường lửa), họ có thể di chuyển tự do bên trong mạng mà không bị kiểm soát chặt chẽ, do thiếu cơ chế kiểm soát truy cập chi tiết nội bộ.

- **Phản ứng chậm**: Khi phát hiện một thiết bị bị xâm nhập, việc thu hồi quyền truy cập thường rất chậm và phức tạp. Quản trị viên phải thực hiện nhiều thao tác như thu hồi chứng chỉ VPN, cập nhật danh sách kiểm soát truy cập (ACL), hoặc thay đổi quy tắc firewall trên nhiều hệ thống.

- **Tấn công tầm nhìn (Visibility Attacks)**: Các dịch vụ như Web Server hay Database phải mở cổng trên firewall để cho phép truy cập từ bên ngoài. Điều này khiến chúng dễ bị phát hiện và tấn công bởi các công cụ quét như nmap hoặc Shodan.

- **Quy trình xử lý sự cố phức tạp**: Việc quản lý quy tắc truy cập được

thực hiện trên nhiều hệ thống khác nhau (firewall, VPN, nhóm bảo mật đám mây), dẫn đến sự phức tạp trong vận hành, khó kiểm toán, và tiềm ẩn nguy cơ lỗi cấu hình bảo mật.

- **Lãng phí nguồn nhân lực**: Quản trị viên phải dành nhiều thời gian cho các công việc thủ công như cấu hình firewall, cập nhật ACL, hay xử lý sự cố, thay vì tập trung vào các nhiệm vụ chiến lược như thiết kế chính sách bảo mật.

2.3. Giải pháp với OpenZiti

OpenZiti là một nền tảng mã nguồn mở được thiết kế để triển khai mạng Zero Trust, giải quyết các pain points trên thông qua các tính năng sau:

- **Mạng "Tối" (Dark Network)**: OpenZiti loại bỏ nhu cầu mở cổng dịch vụ ra Internet. Các dịch vụ như Web Server và Database trở nên vô hình đối với kẻ tấn công, ngăn chặn hoàn toàn các cuộc tấn công quét cổng.

- **Phân đoạn vi mô (Micro-segmentation)**: OpenZiti không tin tưởng vào mạng cơ sở. Quyền truy cập được cấp phát cho từng dịch vụ cụ thể, đảm bảo rằng Web Server và Database Server không thể "thấy" nhau trừ khi được phép. Điều này ngăn chặn di chuyển ngang của kẻ tấn công trong mạng.

- **Thu hồi quyền truy cập tức thời**: Khi phát hiện một client bị xâm nhập, quản trị viên chỉ cần thực hiện một lệnh duy nhất trên OpenZiti Controller để thu hồi quyền truy cập, không cần khởi động lại dịch vụ hay thay đổi cấu hình phức tạp.

- **Quản lý tập trung**: Tất cả chính sách truy cập được quản lý tập trung thông qua OpenZiti Controller, dựa trên danh tính và ngữ cảnh thay vì địa chỉ IP hay quy tắc firewall. Điều này đơn giản hóa vận hành và kiểm toán.

- **Tự động hóa và tối ưu hóa**: OpenZiti hỗ trợ quản lý qua API, cho phép tự động hóa quy trình cấp phát và thu hồi quyền truy cập. Đội ngũ quản trị có thể tập trung vào thiết kế chính sách thay vì thực hiện các thao tác thủ công.

CHƯƠNG 3. Business Requirement và Non-Business Requirement

3.1. Đặt vấn đề

Để triển khai mạng Zero Trust với OpenZiti, cần xác định rõ các yêu cầu kinh doanh (Business Requirements) và yêu cầu phi kinh doanh (Non-Business Requirements). Các yêu cầu này đảm bảo rằng hệ thống không chỉ đáp ứng mục tiêu bảo mật mà còn đạt được hiệu suất, khả năng mở rộng, và trải nghiệm người dùng tốt.

3.2. Business Requirements

Các yêu cầu kinh doanh tập trung vào việc giải quyết các vấn đề bảo mật và vận hành:

ID	Yêu cầu	Mục tiêu
BR-01	Tấn công tầm nhìn	Ngăn chặn các cuộc tấn công quét cổng và dò tìm dịch vụ từ Internet.
BR-02	Phát hiện tấn công	Ngăn chặn khả năng di chuyển ngang của kẻ tấn công trong mạng nội bộ.
BR-03	Phản ứng tấn công	Đảm bảo khả năng thu hồi quyền truy cập nhanh chóng khi phát hiện thiết bị bị xâm nhập.

BR-04	Săn tìm tấn công	Cung cấp log chi tiết và khả năng giám sát tập trung để điều tra các sự cố bảo mật.
BR-05	Quy trình xử lý sự cố	Đơn giản hóa quy trình cấp phát và thu hồi quyền truy cập, giảm thiểu sai sót.
BR-06	Tối ưu hóa nhân lực	Giảm công sức quản trị thủ công, cho phép đội ngũ tập trung vào các nhiệm vụ chiến lược.

3.3. Non-Business Requirements

Các yêu cầu phi kinh doanh tập trung vào kỹ thuật và trải nghiệm người dùng:

- **Bảo mật**:
  - Mã hóa TLS 1.2 trở lên cho tất cả các kết nối.
  - Xác thực dựa trên chứng chỉ x509.
  - Hỗ trợ xác thực đa yếu tố (MFA) và tích hợp với nhà cung cấp danh tính (IdP) trong tương lai.
  - Ủy quyền theo nguyên tắc tối thiểu (Least Privilege).
  - Ghi log đầy đủ, tích hợp với hệ thống SIEM để phân tích sự cố.
- **Hiệu suất**:
  - Độ trễ tăng thêm do hệ thống Zero Trust nhỏ hơn 50ms.
  - Thông lượng tối thiểu đạt 100 Mbps.
  - Thời gian thiết lập kết nối nhỏ hơn 2 giây.

- **Khả năng mở rộng**:
  - Hỗ trợ thêm router mới mà không làm gián đoạn dịch vụ.
  - Tự động hóa triển khai và quản lý thông qua API.
  - Đảm bảo tính sẵn sàng cao (High Availability - HA) cho Controller và Router.
- **T**rải nghiệm người dùng:
  - Cài đặt đơn giản, kết nối trong suốt đối với người dùng cuối (end-user).
  - Cung cấp giao diện dòng lệnh (CLI) và Ziti Admin Console (ZAC) mạnh mẽ, dễ sử dụng cho quản trị viên.

CHƯƠNG 4. Kiến trúc xây dựng

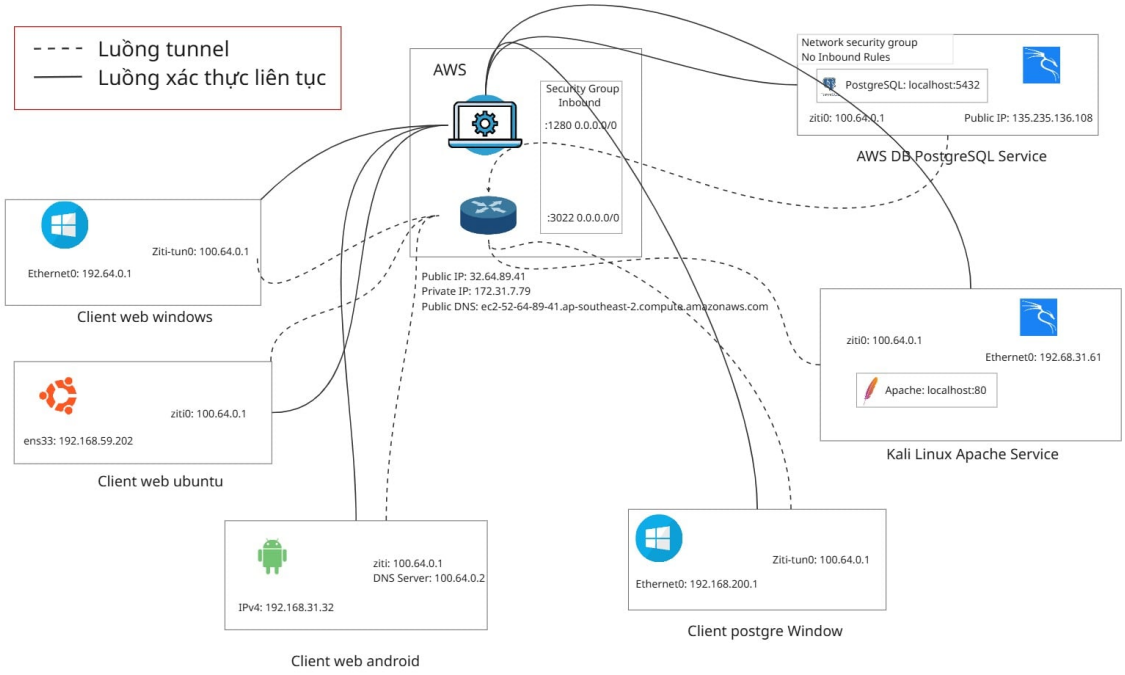
4.1. Đặt vấn đề

Kiến trúc mạng Zero Trust với OpenZiti được thiết kế để kết nối an toàn các môi trường phức tạp, bao gồm đám mây (AWS, Azure) và tại chỗ (On-premise). Kiến trúc này đảm bảo rằng các dịch vụ được bảo vệ trong mạng "tối", quyền truy cập được kiểm soát chặt chẽ, và quản lý được thực hiện tập trung.

4.2. Kiến trúc hạ tầng

Hệ thống bao gồm các thành phần chính:

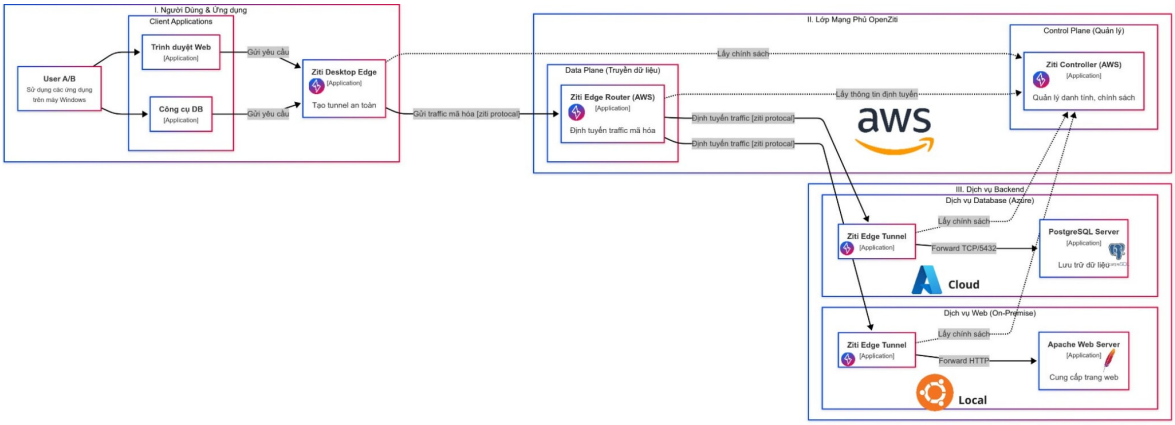
- **Client**: Các thiết bị Windows và Android, sử dụng Ziti client để kết nối an toàn đến các dịch vụ. Ví dụ, người dùng trên Windows có thể truy cập Web Server qua trình duyệt, trong khi người dùng Android sử dụng ứng dụng để kết nối.
- **Controller và Router**: Được triển khai trên AWS (Inbound Controller + Router), Azure, và máy chủ Ubuntu tại chỗ (Local). Router đảm bảo kết nối an toàn giữa các client và dịch vụ, trong khi Controller quản lý chính sách truy cập.
- **Dịch vụ**: Bao gồm Web Server (Apache) và Database (PostgreSQL), được cấu hình để chỉ có thể truy cập qua mạng Ziti, không mở cổng ra Internet.



Hình 4.1: *Kiến trúc hạ tầng*

4.3. Kiến trúc ứng dụng và bảo mật

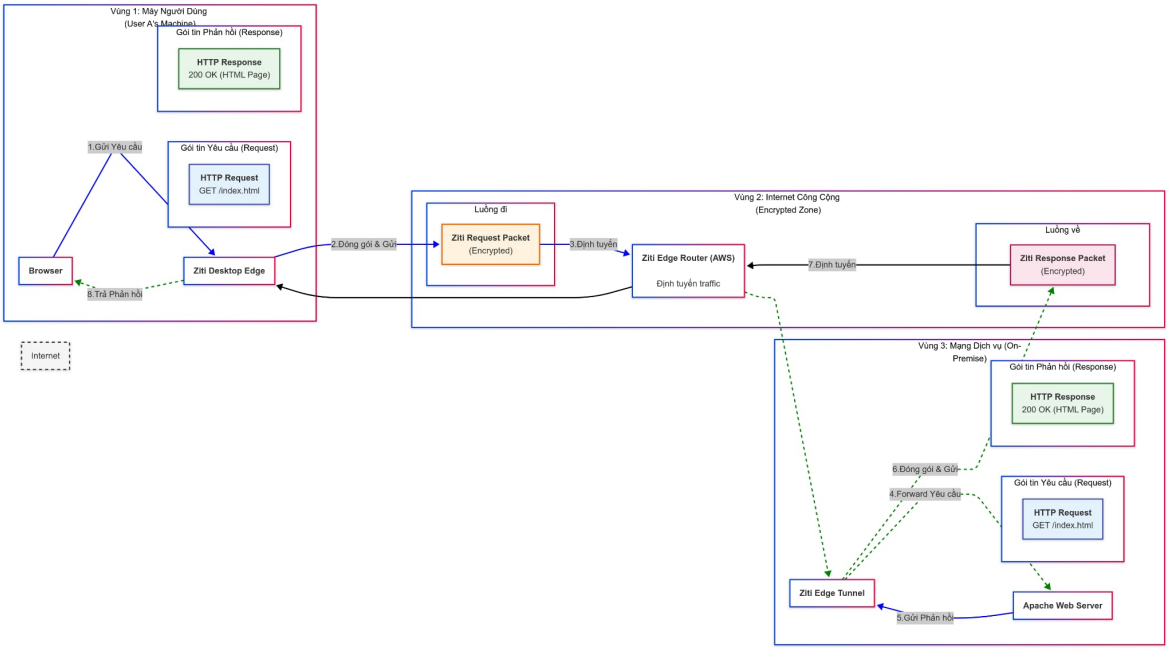
- **Ứng dụng**: Người dùng truy cập dịch vụ thông qua tên dịch vụ (ví dụ: my-apache.ziti, my-postgres-db.ziti) thay vì địa chỉ IP hoặc cổng. Điều này đảm bảo rằng các dịch vụ không bị lộ ra Internet và chỉ có thể truy cập bởi các client được ủy quyền.
- **Bảo mật**:
  - Mã hóa end-to-end sử dụng TLS.
  - Xác thực danh tính dựa trên chứng chỉ x509, đảm bảo chỉ các client hợp lệ mới được kết nối.
  - Phân quyền chi tiết dựa trên vai trò, ví dụ: User A chỉ được truy cập Web Server, trong khi User B được phép truy cập Database.



Hình 4.2: *Kiến trúc ứng dụng*

4.4. Kiến trúc dữ liệu

Dữ liệu trong hệ thống được quản lý tập trung thông qua OpenZiti Controller, lưu trữ thông tin về danh tính, dịch vụ, và chính sách truy cập. Các log hoạt động được ghi lại để hỗ trợ giám sát và phân tích sự cố, tích hợp với hệ thống SIEM nếu cần.



Hình 4.3: *Kiến trúc dữ liệu*

CHƯƠNG 5. Kịch bản và Demo

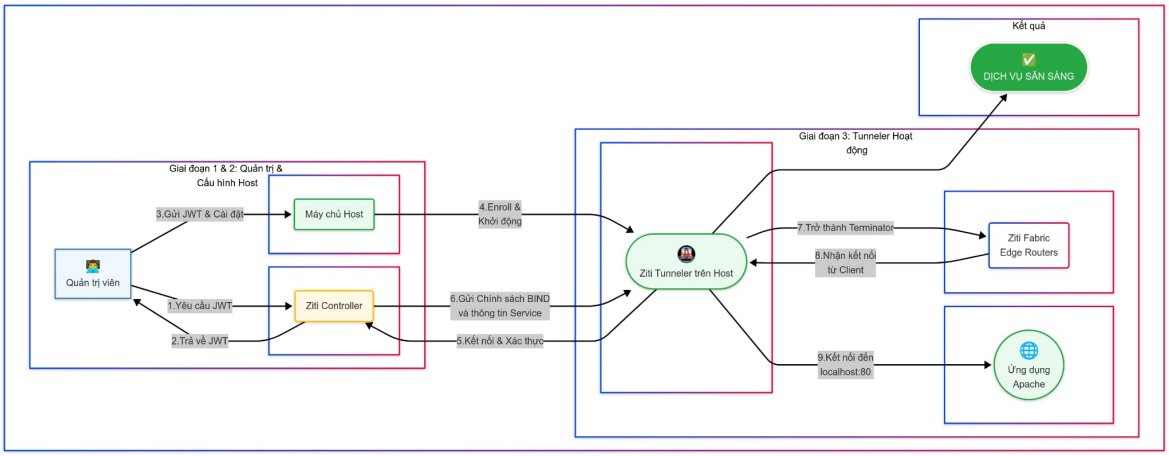
5.1. Đặt vấn đề

Các kịch bản triển khai được thiết kế để chứng minh khả năng của OpenZiti trong việc xây dựng mạng Zero Trust, bao gồm bảo vệ dịch vụ, kiểm soát truy cập chi tiết, và phản ứng nhanh với sự cố.

5.2. Kịch bản triển khai

1. **Cấp phát token và truy cập tài nguyên**:

   - Trên máy Windows 1 (User A), người dùng mở trình duyệt và truy cập http://my-apache.ziti để vào Web Server.
   - Trên máy Windows 2 (User B), người dùng sử dụng công cụ client DB (như DBeaver hoặc psql) để kết nối đến my-postgres-db.ziti trên cổng 5432.



Hình 5.1: *Quá trình cấp phát và truy cập tài nguyên*

- *Kết quả mong đợi*: Cả hai truy cập đều thành công, chứng minh rằng OpenZiti cho phép truy cập an toàn dựa trên danh tính.

2. **Truy cập thất bại do sai vai trò**:

   - Trên máy Windows 1 (User A), người dùng thử kết nối đến my-postgres-db.ziti:5432, vốn chỉ được phép cho User B.
   - *Kết quả mong đợi*: Truy cập thất bại, thể hiện khả năng phân quyền chi tiết của OpenZiti.

3. **Chứng minh mạng "tối"**:

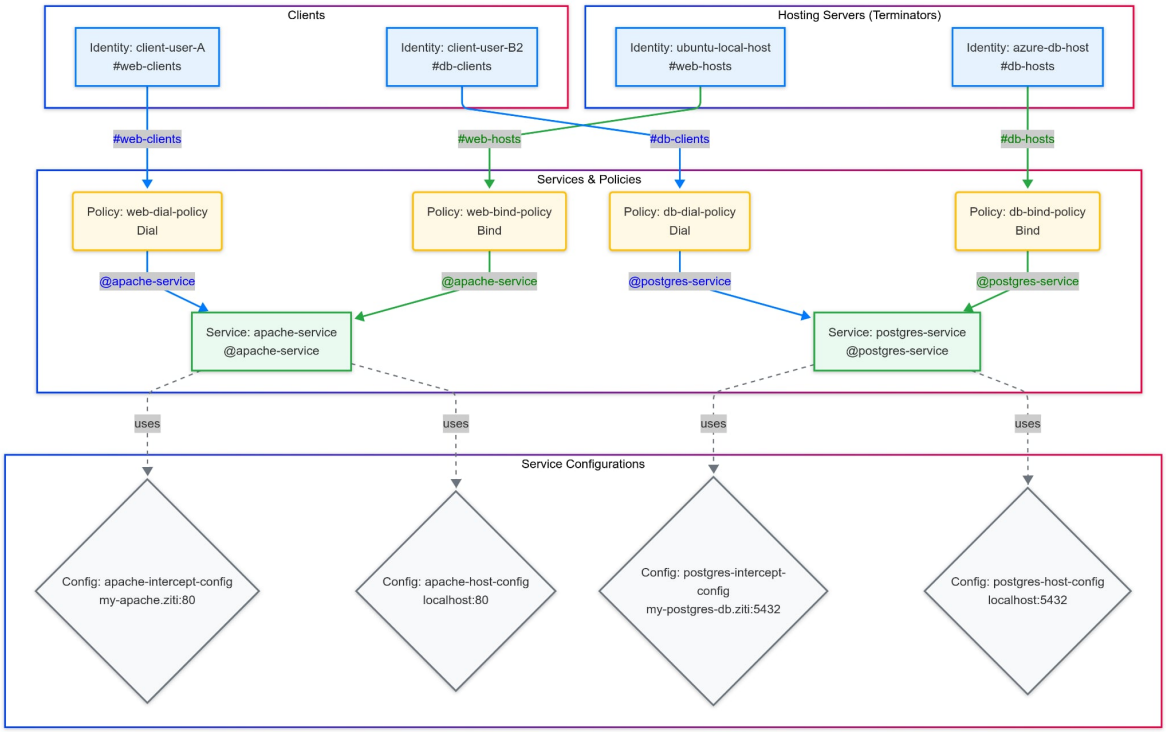
   - Từ một máy tính không cài Ziti client, sử dụng nmap hoặc ping để quét địa chỉ IP public của máy Ubuntu Local và máy Azure.
   - *Kết quả mong đợi*: Không phát hiện cổng 80 (Apache) hoặc 5432 (PostgreSQL), chứng minh rằng các dịch vụ hoàn toàn vô hình với Internet.

4. **Thu hồi quyền truy cập tức thời**:

   - Trên Ziti Controller, quản trị viên chạy lệnh thu hồi quyền truy cập của User B.
   - User B thử tải lại dịch vụ PostgreSQL trên DBeaver.
   - *Kết quả mong đợi*: Truy cập thất bại ngay lập tức mà không cần khởi động lại dịch vụ, thể hiện khả năng phản ứng nhanh của OpenZiti.

5.3. Chi tiết cấu hình

- **Danh tính**:
  - client-user-A: Người dùng truy cập Web Server.
  - client-user-B: Người dùng truy cập Database.
  - ubuntu-local-host: Máy chủ tại chỗ chạy dịch vụ.



Hình 5.2: *Chi tiết cấu hình*

  - aws-edge-router: Router trên AWS.
  - azure-do-host: Máy chủ trên Azure.

- **Dịch vụ**:
  - apache-service: Dịch vụ Web Server với chiến lược smartrouting.
  - postgres-service: Dịch vụ Database với chiến lược smartrouting.

- **Cấu hình**:
  - postgres-host-config, apache-host-config: Cấu hình cho các dịch vụ.
  - postgres-intercept-config, apache-intercept-config: Cấu hình chặn và chuyển tiếp yêu cầu.

CHƯƠNG 6. Kết luận và hướng phát triển

6.1. Đặt vấn đề

Dự án này đã hoàn thành việc triển khai và kiểm chứng một mạng Zero Trust sử dụng nền tảng OpenZiti, thể hiện khả năng đáp ứng các yêu cầu bảo mật, hiệu suất, và vận hành trong các môi trường phức tạp như đám mây (AWS, Azure) và tại chỗ (On-premise). Thông qua các kịch bản thực tế, bao gồm bảo vệ dịch vụ trong mạng "tối", kiểm soát truy cập chi tiết, và phản ứng nhanh với các sự cố bảo mật, dự án đã chứng minh tiềm năng của OpenZiti trong việc thay thế các mô hình bảo mật truyền thống như VPN và tường lửa. Tuy nhiên, để tối ưu hóa hơn nữa và thích nghi với các yêu cầu thực tiễn trong tương lai, việc xem xét các hướng phát triển là cần thiết để nâng cao hiệu quả và khả năng mở rộng của hệ thống.

6.2. Kết luận

Dựa trên kết quả triển khai và thử nghiệm, có thể rút ra các kết luận quan trọng sau:

- **Giải pháp mạnh mẽ của OpenZiti**: OpenZiti cung cấp một nền tảng linh hoạt để triển khai mạng Zero Trust, với các tính năng nổi bật như tạo mạng "tối" (dark network) để ẩn dịch vụ khỏi các cuộc tấn công quét cổng, áp dụng phân đoạn vi mô (micro-segmentation) để kiểm soát truy cập chi tiết giữa các dịch vụ, và quản lý tập trung thông qua OpenZiti Controller. Những tính năng này đã giúp giảm thiểu rủi ro bảo mật một cách hiệu quả.
- **Hiệu quả của kịch bản triển khai**: Các kịch bản thực tế, như cấp phát token cho client, truy cập thất bại do sai vai trò, chứng minh mạng "tối",

và thu hồi quyền truy cập tức thời, đã minh chứng rằng OpenZiti có khả năng bảo vệ tài nguyên khỏi các mối đe dọa bên ngoài và phản ứng nhanh chóng với các sự cố nội bộ. Ví dụ, việc không phát hiện cổng 80 hay 5432 khi quét bằng nmap từ máy không có Ziti tunnel đã khẳng định tính ẩn danh của dịch vụ.

- **Đơn giản hóa vận hành**: Hệ thống OpenZiti đã chứng minh khả năng đơn giản hóa quy trình quản lý thông qua giao diện tập trung và tự động hóa dựa trên API. Điều này không chỉ giảm thiểu công sức thủ công của đội ngũ quản trị mà còn tăng cường khả năng kiểm toán và điều chỉnh chính sách một cách linh hoạt, đặc biệt trong các môi trường phức tạp với nhiều dịch vụ và người dùng.

- ỗ trợ mở rộng: Việc triển khai thành công trên các nền tảng đa dạng (AWS, Azure, Local) cho thấy OpenZiti có tiềm năng mở rộng để phục vụ các tổ chức lớn hơn, với khả năng tích hợp thêm router và dịch vụ mới mà không làm gián đoạn hoạt động hiện tại.

6.3. Hướng phát triển

Dựa trên kết quả đạt được và những hạn chế còn tồn tại, các hướng phát triển sau đây được đề xuất để nâng cao hiệu quả và khả năng ứng dụng của hệ thống OpenZiti trong tương lai:

- **Tích hợp với SIEM**: Mở rộng khả năng ghi log chi tiết và phân tích để tích hợp với các hệ thống quản lý thông tin và sự cố bảo mật (SIEM) như Splunk hoặc ELK. Điều này sẽ cho phép theo dõi và phát hiện các hành vi bất thường một cách chủ động, cung cấp dữ liệu chi tiết để điều tra sâu hơn sau các sự cố bảo mật. Ví dụ, tích hợp SIEM có thể tự động gửi cảnh báo khi phát hiện truy cập trái phép.

- **H**ỗ trợ xác thực đa yếu tố (MFA): Triển khai MFA để tăng cường lớp bảo

mật bổ sung cho người dùng, đặc biệt trong các môi trường có nguy cơ cao. Việc tích hợp với các nhà cung cấp danh tính như Okta hoặc Google Authenticator sẽ giúp đảm bảo rằng ngay cả khi mật khẩu bị lộ, kẻ tấn công vẫn không thể truy cập mà không có yếu tố thứ hai (như mã OTP).

- **M**ở rộng quy mô: Thêm các router và dịch vụ mới để hỗ trợ các tổ chức lớn hơn, với khả năng xử lý hàng trăm hoặc hàng nghìn người dùng cùng lúc. Điều này đòi hỏi tối ưu hóa hiệu suất của Controller và Router, cũng như phát triển các công cụ tự động hóa để triển khai nhanh chóng trong quy mô lớn.

- **T**ối ưu hóa hiệu suất: Giảm độ trễ xuống dưới 50ms và tăng thông lượng vượt 100 Mbps để đáp ứng các ứng dụng yêu cầu băng thông cao như video hội nghị hoặc truyền tải dữ liệu lớn. Việc này có thể thực hiện thông qua tối ưu hóa giao thức smartrouting của OpenZiti hoặc nâng cấp phần cứng cho các thành phần mạng.

- **T**ích hợp với các nền tảng đám mây khác: Mở rộng hỗ trợ cho các nhà cung cấp đám mây khác như Google Cloud hoặc Alibaba Cloud, đảm bảo tính tương thích và linh hoạt trong các môi trường đa đám mây (multi-cloud).

- **P**hát triển giao diện người dùng (UI/UX): Cải thiện Ziti Admin Console (ZAC) và giao diện dòng lệnh (CLI) để cung cấp trải nghiệm quản lý thân thiện hơn, đặc biệt với các quản trị viên không chuyên sâu về kỹ thuật.

- **N**ghiên cứu bảo mật nâng cao: Tích hợp các kỹ thuật bảo mật tiên tiến như phát hiện xâm nhập dựa trên AI hoặc mã hóa lượng tử trong tương lai để đối phó với các mối đe dọa mới.