



# Zero Trust Network Access với Openziti

GVHD: Ths. Nguyễn Duy

Lê Huy Hiệp - 21522067

Nguyễn Việt Khang - 21522198

# Nội dung

01. Bối cảnh

02. Xu hướng & Giải pháp Áp dụng

03. Mục tiêu của đồ án

04. Requirements

05. Architectures

06. Kịch bản triển khai



# 01. Bối cảnh





# Bối cảnh

## Tin tưởng ngầm trong mạng nội bộ

Hệ thống truyền thống mặc định tin tưởng mọi thiết bị và người dùng bên trong mạng. Khi kẻ tấn công vượt qua được lớp bảo vệ bên ngoài, họ có thể tự do di chuyển bên trong mà không bị kiểm soát chặt chẽ, do thiếu cơ chế kiểm soát truy cập chi tiết nội bộ.

## Visibility attacks (Tấn công về tầm nhìn)

Các dịch vụ như Web Server và Database phải mở cổng trên firewall để có thể truy cập, khiến chúng bị "phơi" ra Internet. Kẻ tấn công có thể dễ dàng dùng các công cụ như nmap, Shodan để quét và tìm ra các điểm yếu.

## Phản ứng chậm

Khi một client bị nghi ngờ là đã bị xâm nhập, việc thu hồi quyền truy cập rất chậm và phức tạp. Phải thu hồi chứng chỉ VPN, cập nhật danh sách ACL, thay đổi quy tắc firewall trên nhiều hệ thống

## Incident Processes (Quy trình phức tạp)

Việc quản lý các quy tắc truy cập được thực hiện trên nhiều hệ thống khác nhau (danh sách ACL của tường lửa, cấu hình VPN, quy tắc của nhóm bảo mật đám mây). Điều này tạo ra sự phức tạp trong vận hành, khó kiểm toán và tiềm ẩn nguy cơ cao gây ra lỗi cấu hình bảo mật.



# Bối cảnh

---

## **Human Resources (Lãng phí nguồn nhân lực)**

Đội ngũ IT/Security tốn quá nhiều thời gian vào các tác vụ thủ công như quản lý IP, mở/đóng cổng, thay vì tập trung vào các công việc có giá trị cao hơn.

## 02. Xu hướng & Giải pháp Áp dụng





# Xu hướng

---

## Zero Trust Network Access (ZTNA)

Thay thế các mô hình Perimeter-based Security (VPN, tường lửa) bằng nguyên tắc "không tin tưởng bất kỳ ai, luôn xác thực". Truy cập được cấp phát dựa trên danh tính của người dùng/thiết bị và ngữ cảnh, không phải vị trí mạng.

## Secure Access Service Edge (SASE)

Là sự hội tụ của các dịch vụ mạng (như SD-WAN) và các dịch vụ bảo mật (như ZTNA, SWG, CASB, FWaaS) vào một nền tảng duy nhất, được cung cấp trên nền tảng đám mây. Nó đưa bảo mật đến gần hơn với người dùng và thiết bị, bất kể họ ở đâu.

## Identity-Aware Proxy (IAP)

Dịch vụ proxy ngược (reverse proxy) hoạt động ở tầng ứng dụng (Lớp 7). Người dùng truy cập vào proxy, proxy sẽ xác thực danh tính của họ (thường qua một nhà cung cấp danh tính như Google, Okta), và nếu hợp lệ, nó sẽ chuyển tiếp yêu cầu đến ứng dụng web hoặc SSH/RDP ở phía sau.



# Xu hướng

## So sánh

Hướng tiếp cận	Vành đai bảo mật	Mức độ chi tiết	Hỗ trợ ứng dụng
IAP	Ứng dụng (Application)	Cao (URL/API)	Hạn chế (Web, SSH)
SDP / ZTNA (OpenZiti)	Danh tính (Identity)	Rất cao (Service/API)	Tất cả (TCP/IP)
SASE	Danh tính + Nội dung	Rất cao	Tất cả



# Giải pháp áp dụng

---

Giải quyết Painpoint 1 (Visibility): → Tạo Mạng "Tối" (Dark Network): không có cổng dịch vụ nào cần mở ra Internet. Cả Web Server và Database Server đều trở nên vô hình. Kẻ tấn công không thể quét hay tìm thấy chúng.

Giải quyết Painpoint 2 (Detection): → Phân đoạn Vi mô (Micro-segmentation): OpenZiti không tin tưởng vào mạng. Truy cập được cấp phát cho từng dịch vụ cụ thể. Web Server và Database Server không thể "thấy" nhau trừ khi được cho phép. Kẻ tấn công không thể di chuyển ngang.

Giải quyết Painpoint 3 (Response): → Thu hồi Quyền truy cập Tức thời: Khi một client bị xâm nhập, chỉ cần một lệnh duy nhất hoặc một cú click trên giao diện ZAC để vô hiệu hóa danh tính đó. Quyền truy cập sẽ bị thu hồi ngay lập tức trên toàn bộ hệ thống.

Giải quyết Painpoint 4 (Process): → Quản lý Tập trung, Định nghĩa bằng Phần mềm: Tất cả các chính sách truy cập được quản lý tập trung tại OpenZiti Controller. Việc cấp quyền dựa trên danh tính và thuộc tính, không còn phụ thuộc vào địa chỉ IP hay quy tắc firewall phức tạp.

Giải quyết Painpoint 5 (Human Resources): → Tự động hóa và Tối ưu hóa: Toàn bộ mạng có thể được quản lý qua API, cho phép tự động hóa quy trình cấp phát quyền. Đội ngũ IT có thể tập trung vào việc thiết kế chính sách thay vì thực thi công.

# 03. Project Objectives





# Project Objectives

Objectives	
Objective 1	Xây dựng một kiến trúc "dark" và chứng minh khả năng ẩn giấu dịch vụ khỏi các công cụ quét cổng và tấn công từ bên ngoài.
Objective 2	Trình diễn khả năng phân quyền truy cập chi tiết, chỉ cho phép đúng người dùng truy cập đúng tài nguyên.
Objective 3	Xây dựng thành công một mạng Zero Trust kết nối các môi trường phức tạp: Cloud (AWS, Azure) và On-premise (Local).
Objective 4	Cho thấy sự đơn giản hóa trong việc quản lý truy cập so với phương pháp Firewall/VPN truyền thống.
Objective 5	Xây dựng một phòng lab ảo (virtual lab) đầy đủ chức năng để kiểm chứng và trình diễn các tính năng của OpenZiti.

# 04. Requirements





# Business Requirements

ID	Business Requirement	Mục tiêu
BR-01	<b>Visibility Attack</b>	Ngăn chặn các cuộc tấn công quét cổng, dò tìm dịch vụ.
BR-02	<b>Detect Attack</b>	Ngăn chặn khả năng di chuyển ngang của kẻ tấn công trong mạng.
BR-03	<b>Response Attack</b>	Đảm bảo khả năng thu hồi quyền truy cập nhanh chóng khi bị xâm nhập.
BR-04	<b>Hunt Attack</b>	Cung cấp log và khả năng giám sát tập trung để điều tra sự cố.
BR-05	<b>Incident Procedure</b>	Đơn giản hóa quy trình cấp phát và thu hồi quyền truy cập.
BR-06	<b>Human Resource Optimization</b>	Giảm thiểu công sức quản trị thủ công.



# Non-Business Requirements

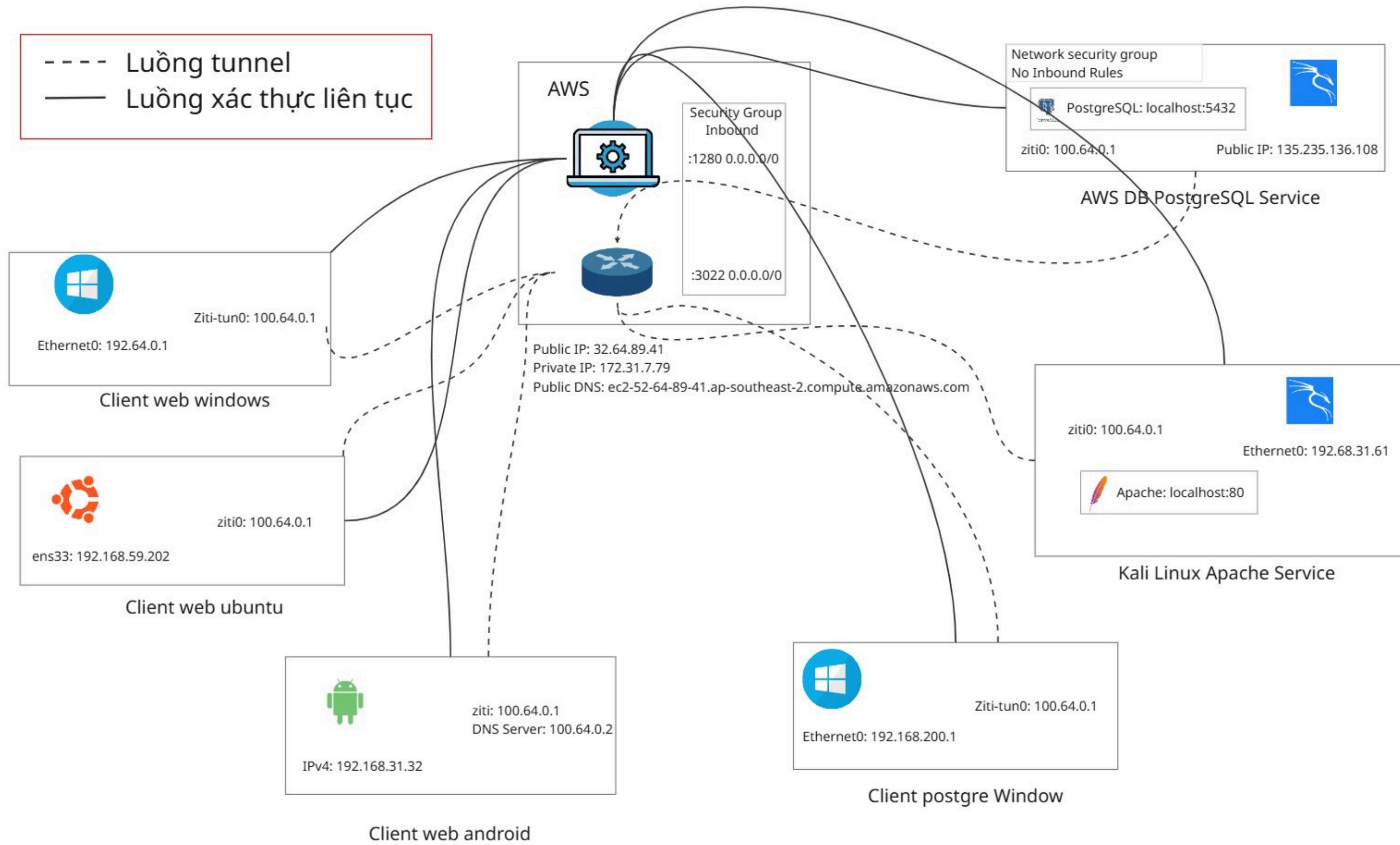
STT	Danh mục	Yêu cầu chi tiết	STT	Danh mục	Yêu cầu chi tiết
1	Business Volume	<ul style="list-style-type: none"><li>- 4 danh tính hoạt động</li><li>- 2 người dùng đồng thời</li><li>- Đảm bảo hoạt động độc lập không ảnh hưởng nhau</li></ul>	5	Security	<ul style="list-style-type: none"><li>- Mã hóa TLS 1.2 trở lên</li><li>- Xác thực x509</li><li>- Hỗ trợ MFA/IdP tương lai</li><li>- Ủy quyền theo nguyên tắc tối thiểu</li><li>- Ghi log đầy đủ, tích hợp SIEM</li></ul>
2	Độ tin cậy & Khôi phục	<ul style="list-style-type: none"><li>- RTO: &lt; 5 phút</li><li>- RPO: &lt; 1 phút</li><li>- Hỗ trợ CLI/ZAC thao tác nhanh</li></ul>	6	Performance	<ul style="list-style-type: none"><li>- Độ trễ tăng thêm &lt; 50ms</li><li>- Thông lượng tối thiểu: 100 Mbps</li><li>- Thời gian thiết lập kết nối: &lt; 2 giây</li></ul>
3	Backup & Restore	<ul style="list-style-type: none"><li>- Có quy trình sao lưu &amp; phục hồi</li><li>- Controller đơn: Sao lưu db và PKI</li><li>- Controller HA: Giám sát và thay thế node</li></ul>	7	Scalability	<ul style="list-style-type: none"><li>- Dễ mở rộng router mới- Hỗ trợ automation qua API</li><li>- Hỗ trợ HA cho Controller &amp; Router</li></ul>
4	Computing & Storage	<ul style="list-style-type: none"><li>- Hỗ trợ đa nền tảng: AWS, Azure, On-premise</li><li>- Client: Windows, Linux, Android</li></ul>	8	Usability	<ul style="list-style-type: none"><li>- End-user: Cài đặt đơn giản, kết nối trong suốt</li><li>- Admin: CLI và ZAC mạnh mẽ, dễ quản lý</li></ul>

# 05. Architectures (Kiến Trúc Hệ Thống)





# Infrastructure Architecture





# Infrastructure Architecture

## Inbound Controller + Router AWS

sgr-0480570ce0ffab40d	Custom TCP	TCP	3022	Custom	0.0.0.0/0	Clien to router	Delete
sgr-08c8f2dba29ed180c	SSH	TCP	22	Custom	0.0.0.0/0		Delete
sgr-0b9173f9e5629e5ff	Custom TCP	TCP	1280	Custom	0.0.0.0/0	Ziti Controller Management API and controller plane	Delete

## Cấu hình DB server Azure

```
Last login: Sun Jun 15 07:59:51 2025 from 171.226.36.106
ubuntu@ubuntuVM:~$ sudo netstat -tulpn | grep :5432
tcp        0      0 127.0.0.1:5432          0.0.0.0:*
LISTEN      30607/postgres
ubuntu@ubuntuVM:~$
```

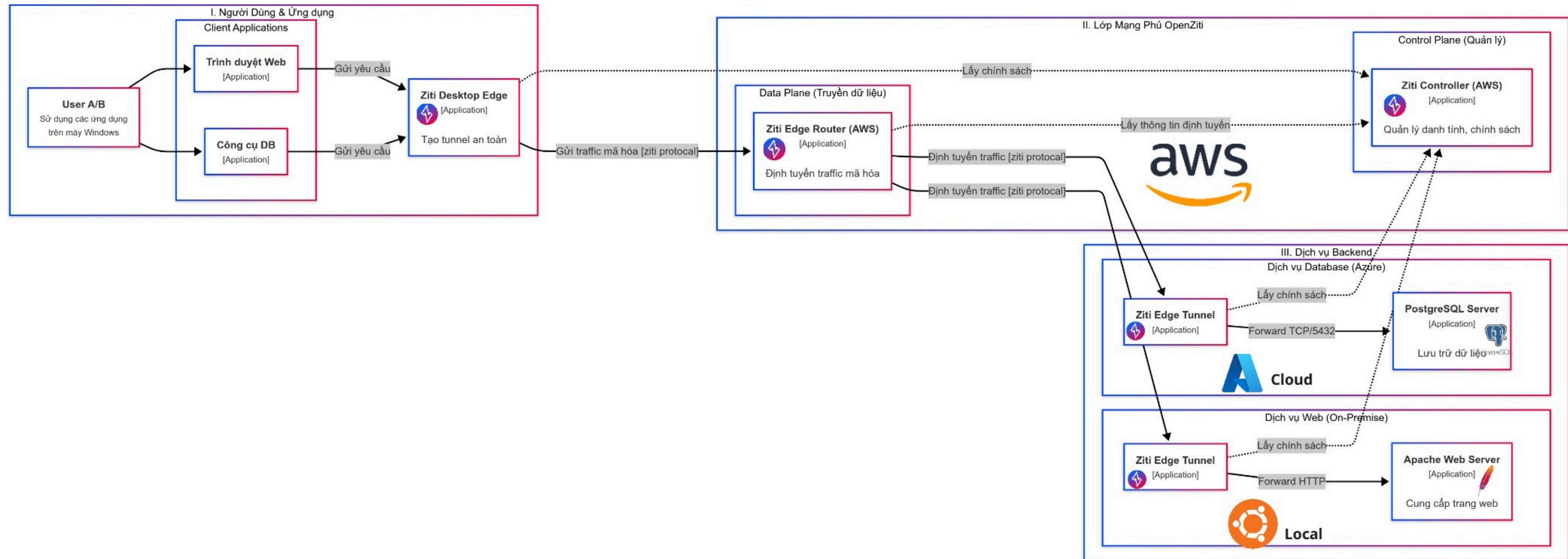
## Cấu hình web server local

```
(kali㉿kali)-[~/Desktop]
$ sudo netstat -tulpn | grep :80
[sudo] password for kali:
tcp        0      0 127.0.0.1:80          0.0.0.0:*
LISTEN      1058/apache2

(kali㉿kali)-[~/Desktop]
```

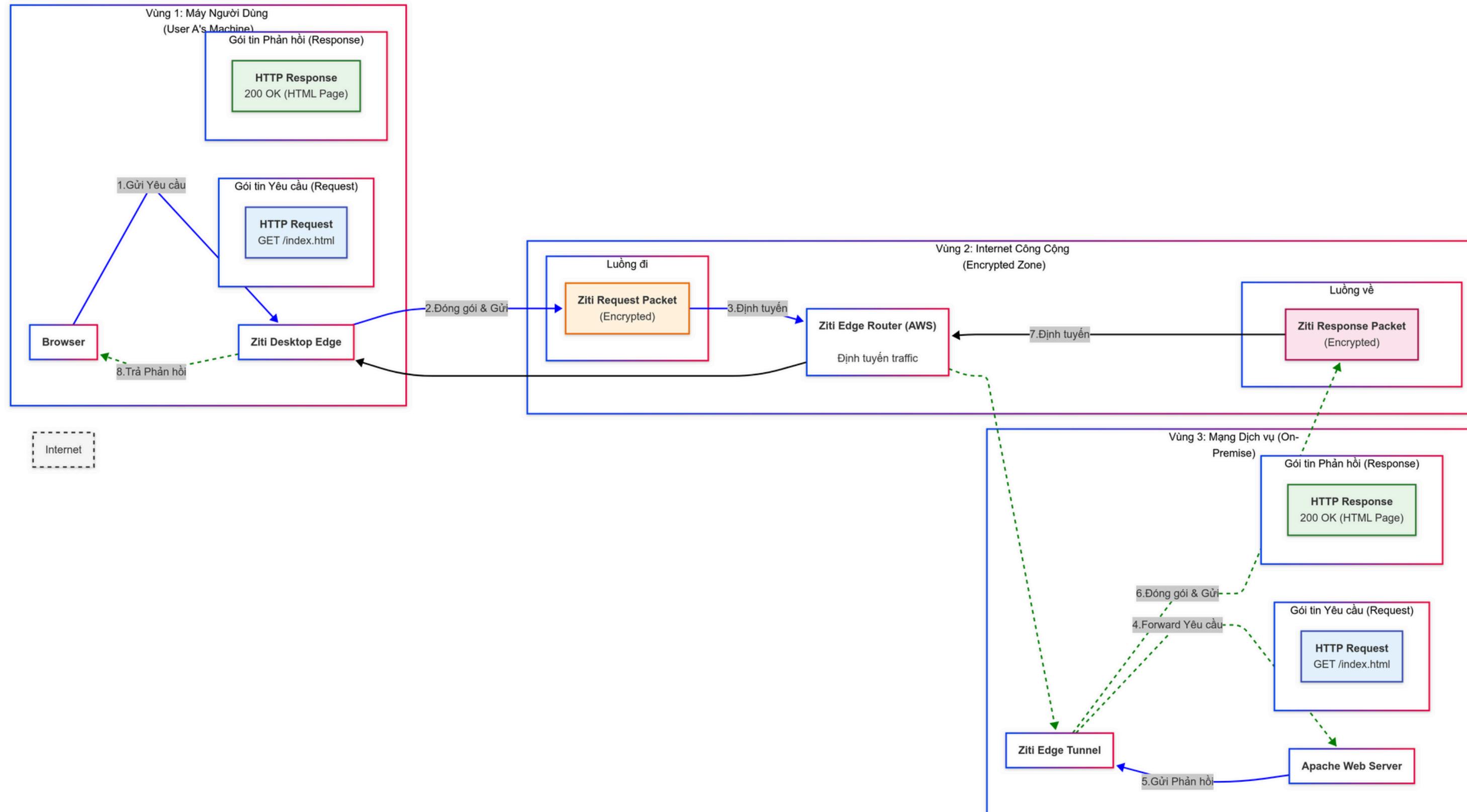


# Application/Function Architecture



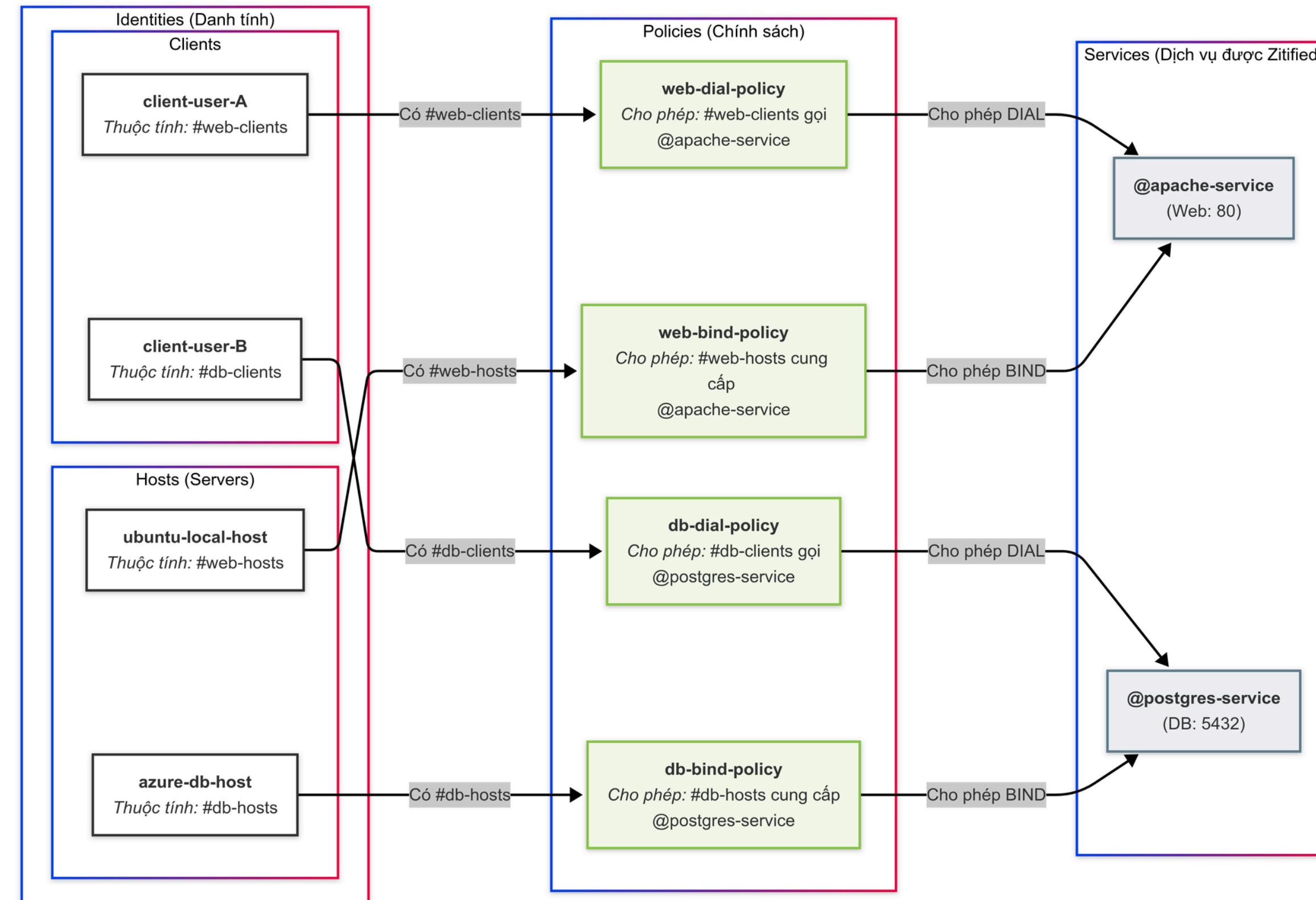


# Data Architecture





# Security Architecture



# 06. Kịch bản triển khai





# Kịch bản triển khai

Kịch bản 1: Cấp phát token, host service và client truy cập tài nguyên:

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

Kết quả mong đợi: Thành công.

Kịch bản 2: Truy cập Thất bại do Sai vai trò:

Trên máy Windows 1 (User A), thử kết nối đến database tại my-postgres-db.ziti:5432.

Kết quả mong đợi: THẤT BẠI.

Kịch bản 3: Chứng minh Mạng "Tối" (Dark Network):

Từ một máy tính không có tunnel đến service và có tunnel bằng 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. Lệnh quét sẽ không tìm thấy cổng 80 hay 5432 đang mở. Các dịch vụ hoàn toàn vô hình với Internet.

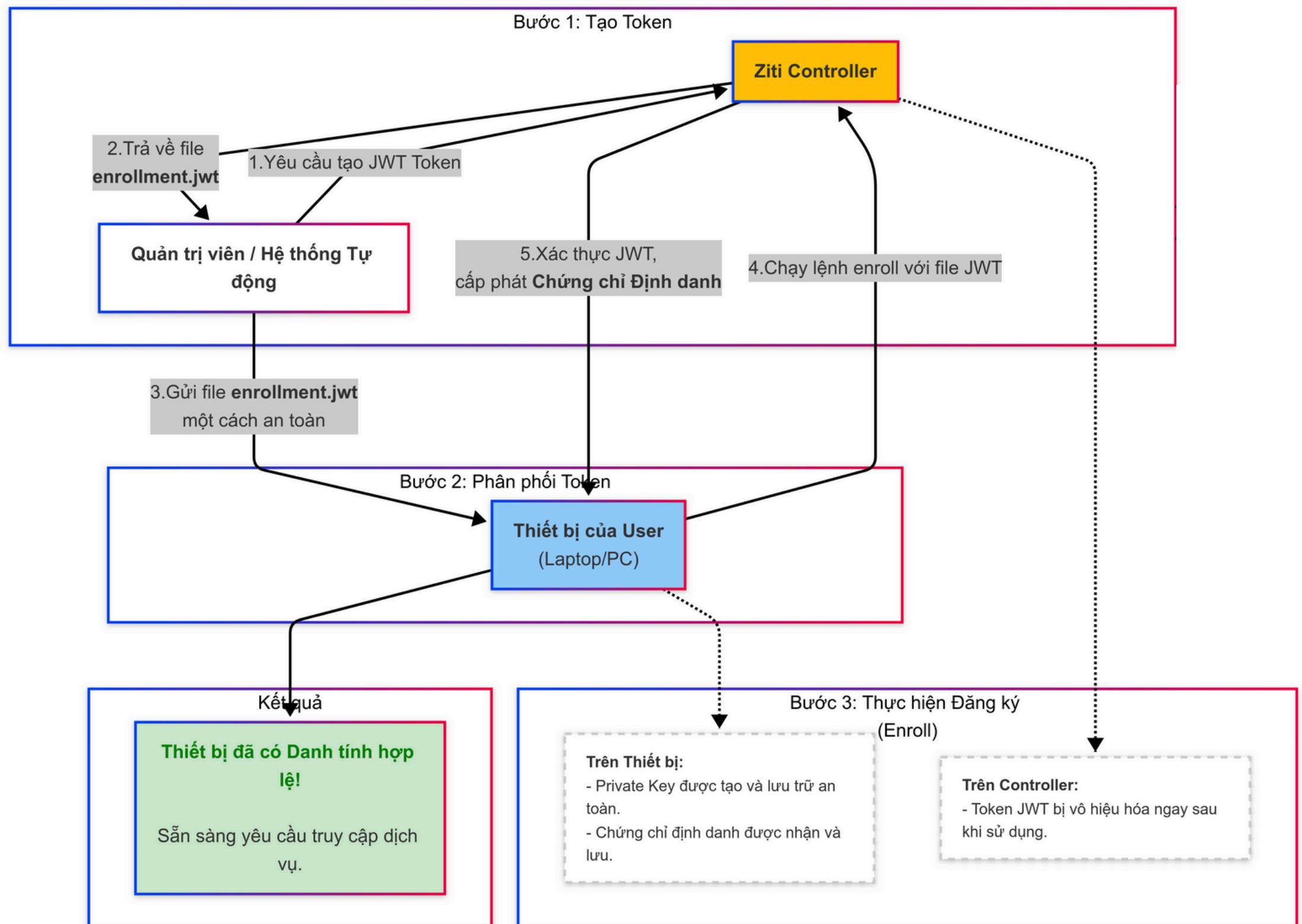
Kịch bản 4: Thu hồi Quyền truy cập Tức thời và cấp lại quyền truy cập:

Trên Ziti Controller, chạy lệnh thu hồi thuộc tính truy cập của client.

Kết quả mong đợi: TỨC THỜI. Ngay sau đó, User B thử tải lại dịch vụ PostgreSQL trên Dbeaver sẽ thất bại. Quyền truy cập bị thu hồi ngay lập tức mà không cần khởi động lại bất kỳ dịch vụ nào.



# Enroll processing

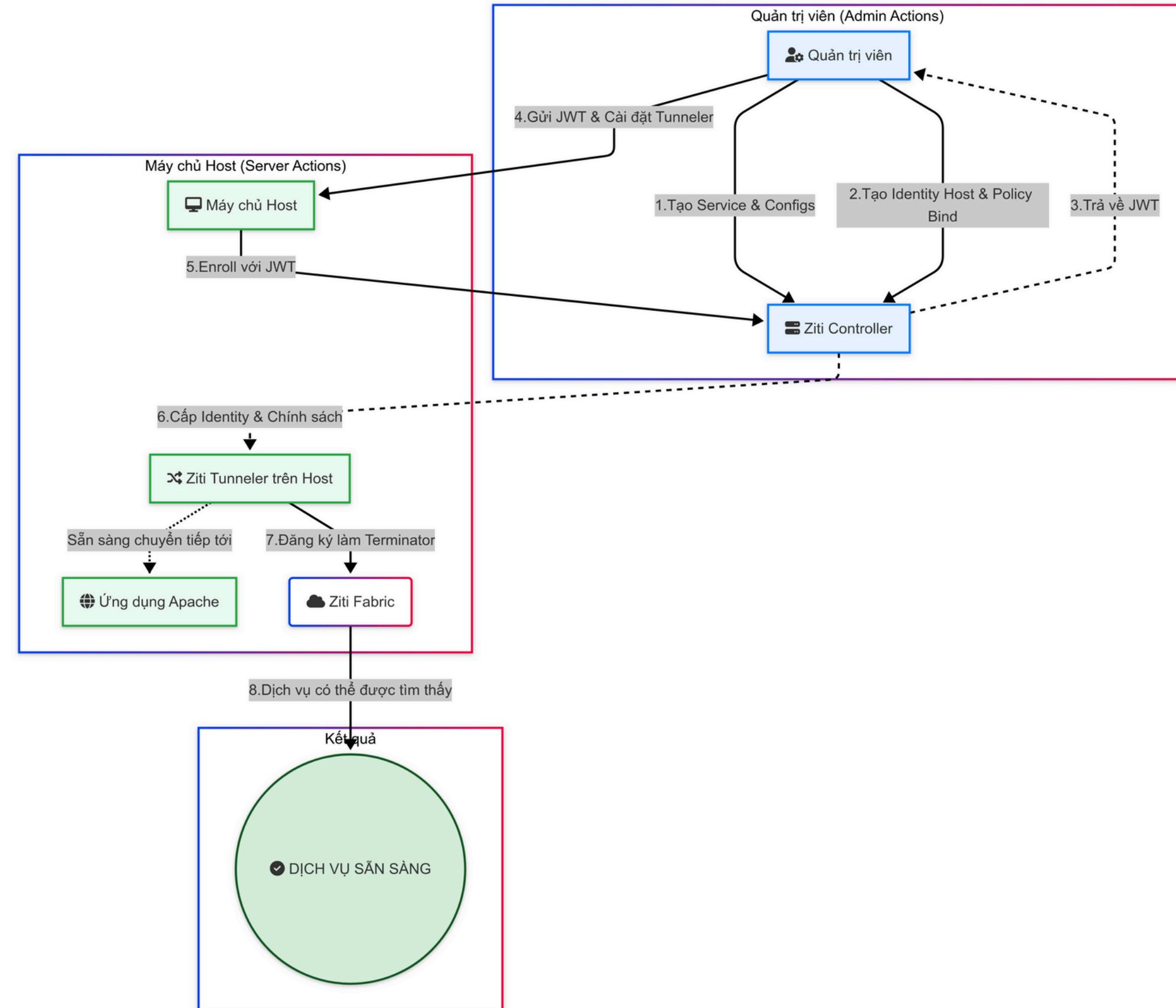


**Client**



# Enroll processing

## Service





# Chi tiết cấu hình

```
ubuntu@ip-172-31-7-79:~$ ziti edge list identities
```

ID	NAME	TYPE	ATTRIBUTES	AUTH-POLICY
3Y6YRgY56p	client-user-A	Default	web-clients	Default
AJ.DvSIM4u	client-user-B	Default	db-clients	Default
Jm9DvSEMNu	ubuntu-local-host	Default	web-hosts	Default
Ndtc.SEM4u	aws-edge-router	Router		Default
Uzo2RhWv2	Default Admin	Default		Default
cWMpZSIU4u	azure-db-host	Default	db-hosts	Default

```
ubuntu@ip-172-31-7-79:~$ ziti edge list services
```

ID	NAME	ENCRYPTION REQUIRED	TERMINATOR STRATEGY	ATTRIBUTES
1Sr0bnRatsKMTDTjCit757	postgres-service	true	smartrouting	
5TjtRTesfA5aU5OMf6W8PC	apache-service	true	smartrouting	

```
results: 1-2 of 2
```



# Chi tiết cấu hình

```
ubuntu@ip-172-31-7-79:~$ ziti edge list configs
```

ID	NAME	CONFIG TYPE
31pTpCstw2qiCCWqJk3ode	postgres-host-config	host.v1
3BK9RR9RT3WtaWVlzJz02j	apache-host-config	host.v1
3PVES2xBGWBAZS7WPIz0y9	postgres-intercept-config	intercept.v1
A5CZKMxTNqXt1Rb5q5vrg	apache-intercept-config	intercept.v1

```
# --- Dịch vụ cho PostgreSQL Database ---
# Config chặn traffic DB
ziti edge create config "postgres-intercept-config" intercept.v1
'{"protocols":["tcp"], "addresses":["my-postgres-db.ziti"], "portRanges":[{"low":5432, "high":5432}]}'
# Config host traffic DB
ziti edge create config "postgres-host-config" host.v1 '{"protocol":"tcp", "address":"localhost",
"port":5432}'
# Tạo dịch vụ DB
ziti edge create service "postgres-service" --configs "postgres-intercept-config", "postgres-host-config"
```

```
ubuntu@ip-172-31-7-79:~$ ziti edge list service-policies
```

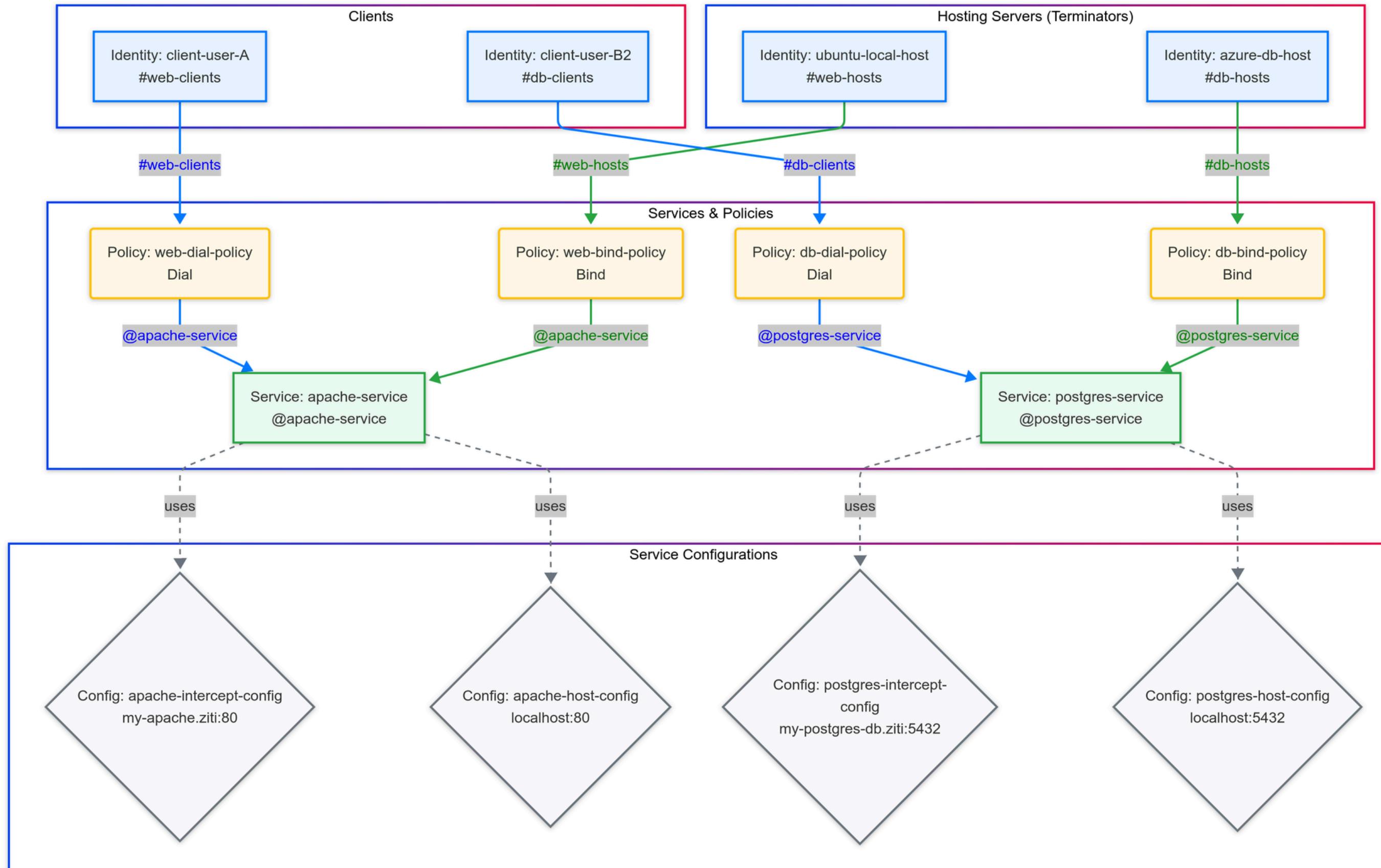
ID	NAME	SEMANTIC	SERVICE ROLES	IDENTITY ROLES	POSTURE CHECK ROLES
1diPex7wxhsTuTHu9Q1eHt	db-bind-policy	Anyof	@postgres-service	#db-hosts	
2XR8IvN0RtWzAIz6pBCag7	db-dial-policy	Anyof	@postgres-service	#db-clients	
FRssGAzyPNEYlV1GpaqIf	web-bind-policy	Anyof	@apache-service	#web-hosts	
LbGxP52XI0Vmub1tcHTC6	web-dial-policy	Anyof	@apache-service	#web-clients	

```
results: 1-4 of 4
```

```
ubuntu@ip-172-31-7-79:~$ █
```



# Chi tiết cấu hình



# Kịch bản 1: Cấp phát token, host service và client truy cập tài nguyên:

## Các bước

- Tạo token
- Sử dụng token đã cấp phát để host cho service enroll dial cho client
- Check log service kiểm tra kết nối
- Truy cập tài nguyên
- Quản lý các kết nối trong controller

[Link](#)

### Thông tin các session kết nối

```
INFO[00000] [2023-08-15T10:49:58.950Z]  
ubuntu@ip-172-31-7-79:~$ ziti edge list sessions
```

ID	API SESSION ID	SERVICE NAME	TYPE
cmbxcquh000velro4wknnvv29	cmbxcqtcu00valro4t3hupvdn	postgres-service	Bind
cmbxcrhz100wb1ro4yjwmoq2w	cmbxcr8mf00vx1ro4pld67htt	apache-service	Bind
cmbxcz5w5016alro44povg5og	cmbxcwt3b01381ro4tgbgbt0t	apache-service	Dial
cmbxdg25a01silro4mp6y4bos	cmbxdd8b101oolro4tht24zk7	postgres-service	Dial

```
results: 1-4 of 4
```

```
ubuntu@ip-172-31-7-79:~$ █
```

# Kịch bản 1: Cấp phát token, host service và client truy cập tài nguyên:

Client Windows sau khi connect xem thông tin mạng

```
C:\Users\Admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . : localdomain
  Link-local IPv6 Address . . . . . : fe80::25c4:85fb:6779:1a93%3
  IPv4 Address . . . . . : 192.168.59.184
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.59.2

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

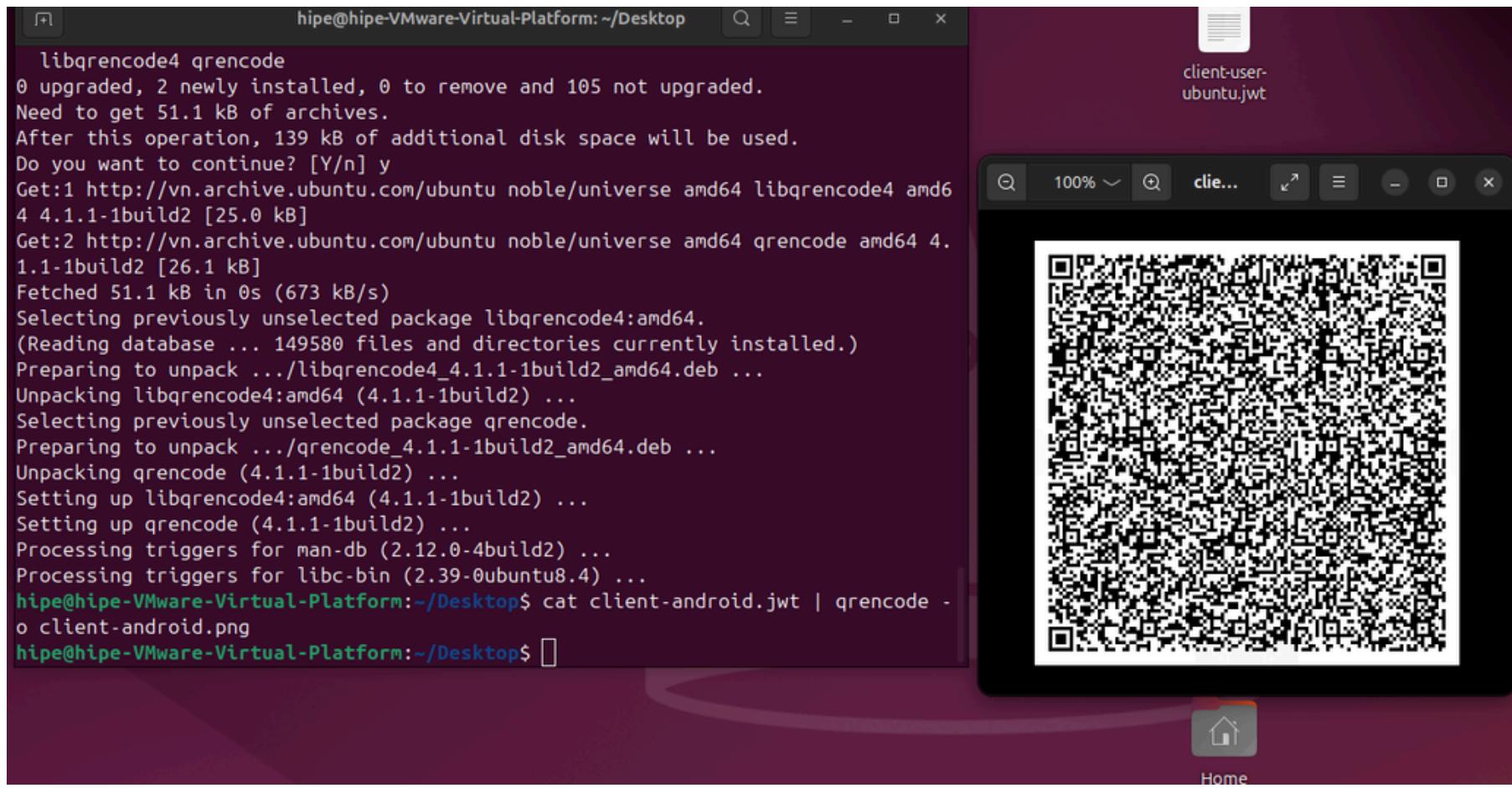
Unknown adapter ziti-tun0:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::c540:4cd:1cec:8786%25
  IPv4 Address . . . . . : 100.64.0.1
  Subnet Mask . . . . . : 255.192.0.0
  Default Gateway . . . . . :

C:\Users\Admin>ping 8.8.8.8
```

# Kịch bản 1: Android cấp chứng chỉ và truy cập tài nguyên

## Tạo mã QR android bằng token cấp phát



The first screenshot shows the 'Tap To Connect' screen with a green checkmark icon and a timer at 00:03:30 STOP. It displays download and upload speeds of 344,0 and 208,0 bps respectively.

The second screenshot shows the 'my-apache.ziti' screen with the Apache2 Debian Default Page content: "It works!". It includes a 'Configuration Overview' section detailing the Apache2 configuration layout on Debian systems.

The third screenshot shows the 'client-android' screen with a list of services. It shows a single service 'apache-service' with the status 'Enabled' and the URL 'https://ec2-52-64-89-41.ap'.



## Kịch bản 2: Truy cập Thất bại do Sai vai trò:

---

Từ client với quyền truy cập web service cố truy cập vào DB sersever

[Link](#)



# Kịch bản 3: Chứng minh dark network

## Link

Sử dụng nmap để quét public IP của service trong hai trường hợp đã kết nối và không kết nối

```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nvkha>nmap -Pn -p 5432 135.235.136.108
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-15 16:45 +0700
Nmap scan report for 135.235.136.108
Host is up.

PORT      STATE      SERVICE
5432/tcp  filtered  postgresql

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds

C:\Users\nvkha>
```

cổng 5432 không thể  
bị phát hiện từ Internet,  
tức là chúng hoàn toàn vô hình  
đối với internet.

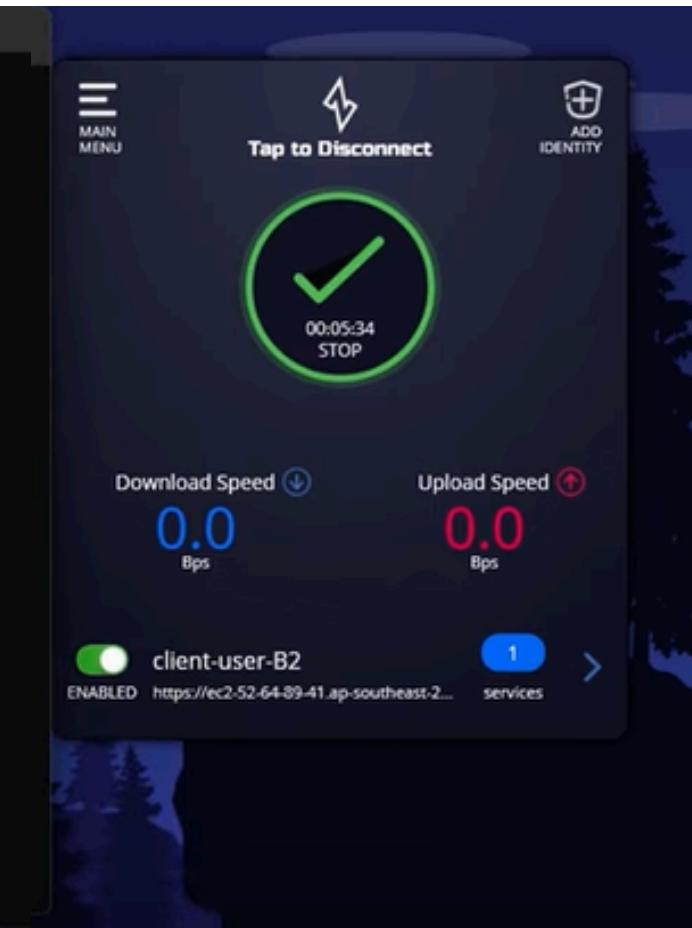
```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nvkha>nmap -Pn -p 80,5432 135.235.136.108
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-15 16:59 +0700
Nmap scan report for 135.235.136.108
Host is up.

PORT      STATE      SERVICE
80/tcp    filtered  http
5432/tcp  filtered  postgresql

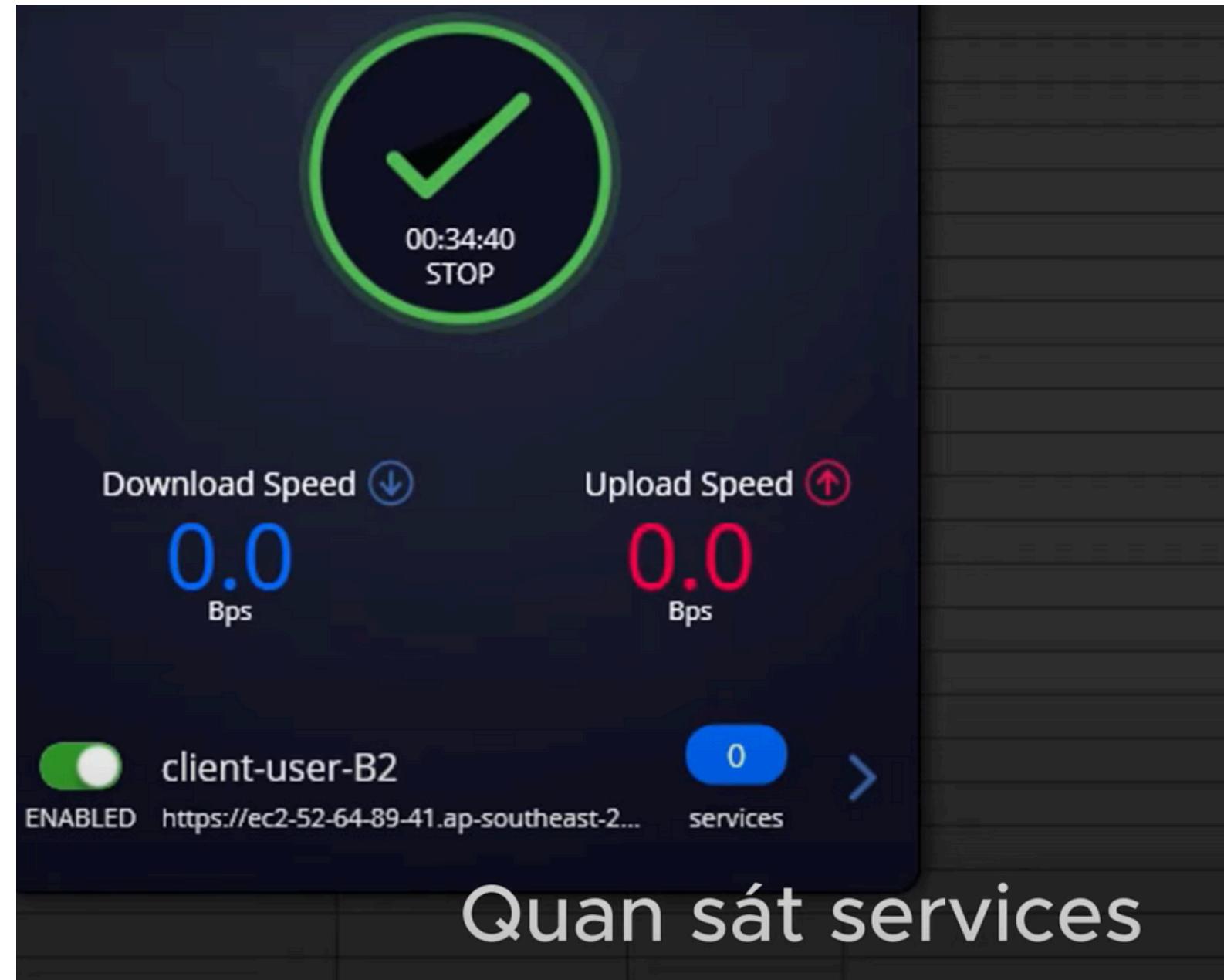
Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

C:\Users\nvkha>nmap -Pn -p 80,5432 135.235.136.108
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-15 17:00 +0700
```



## Kịch bản 4: Thu hồi Quyền truy cập Tức thời và cấp lại quyền truy cập:

[Link](#)



**THANK YOU**