



Khoa Mạng máy tính và truyền thông  
BÁO CÁO ĐỒ ÁN MÔN HỌC



## Next-Generation Firewall

NT534.P21.ANTN

Bùi Vương Tâm Anh  
Trần Đình Khoa

*Trường ĐH Công nghệ Thông Tin, ĐHQG Tp. HCM*

# AGENDA

---

- I. Context**
- II. Technology Trends**
- III. Project Objectives (Scope & Out of Scope)**
- IV. Business & Non-Business Requirements**
- V. Architectures**
- VI. Scenarios Demo**
- VII. Conclusion & Future Work**



# I. Context

## Pain Points:

1. Stateful Firewall thiếu Application Awareness: Chỉ hoạt động ở Layer 3/4 (IP, Port), không phân biệt được Facebook và traffic web thông thường trên cùng port 443. Dễ bị bypass bằng cách chạy dịch vụ trên port lạ.
2. Các công cụ bảo mật bị phân mảnh (Siloed Security Tools) như IDS/IPS, Web Filter, Antivirus... là các hệ thống riêng biệt, khó quản lý, khó tương quan sự kiện để thấy bức tranh tấn công tổng thể.
3. Các giải pháp bảo mật chỉ phát hiện các tấn công đã có signature, không chủ động ngăn chặn các mối đe dọa mới từ các IP/domain độc hại đang hoạt động trên Internet.
4. Khó khăn trong quản lý và điều tra: Cần xem log từ nhiều nguồn khác nhau, quy trình xử lý sự cố phức tạp.
5. Các giải pháp NGFW thương mại có chi phí bản quyền rất cao.



# AGENDA

---

**I. Context**

**II. Technology Trends**

**III. Project Objectives (Scope & Out of Scope)**

**IV. Business & Non-Business Requirements**

**V. Architectures**

**VI. Scenarios Demo**

**VII. Conclusion & Future Work**



## II. Technology Trends

### **Solutions for Pain Points:**

1. Deep Packet Inspection (DPI) & Application Control: Công nghệ cốt lõi của NGFW.
2. Kiến trúc hợp nhất - Unified Architecture: Tích hợp nhiều chức năng - IDS/IPS, Web Filter, AV - vào một luồng xử lý duy nhất.
3. Tích hợp Threat Intelligence: Chủ động cập nhật và chặn các IoCs từ các nguồn tin cậy.
4. Centralized Logging & Reporting.
5. Xây dựng hệ thống dựa trên Open-source.



# AGENDA

---

- I. Context
- II. Technology Trends
- III. Project Objectives (Scope & Out of Scope)**
- IV. Business & Non-Business Requirements
- V. Architectures
- VI. Scenarios Demo
- VII. Conclusion & Future Work



# III. Project Objectives

Xây dựng một hệ thống Next-Generation Firewall dưới dạng Proof-of-Concept, tích hợp các công nghệ mã nguồn mở để cung cấp các lớp bảo vệ đa dạng cho hệ thống mạng.

## In Scope:

1. Triển khai IDS/IPS với khả năng phát hiện dựa trên Signature và một số hành vi cơ bản.
2. Xây dựng tính năng lọc Web (URL Filtering) và kiểm soát truy cập dựa trên tên miền.
3. Tích hợp hệ thống quét Virus/Malware cho lưu lượng web tải về.
4. Tích hợp nguồn tin Threat Intelligence để chủ động ngăn chặn các địa chỉ IP độc hại.
5. Xây dựng môi trường máy ảo để kiểm thử & minh họa các tính năng.

## Out of Scope:

1. Giải mã và kiểm tra lưu lượng HTTPS (SSL Inspection).
2. Xây dựng giao diện quản trị đồ họa (GUI).
3. Tích hợp Sandboxing để phân tích file nâng cao.
4. Tối ưu hóa hiệu năng ở quy mô lớn.



# AGENDA

---

- I. Context
- II. Technology Trends
- III. Project Objectives (Scope & Out of Scope)
- IV. Business & Non-Business Requirements**
- V. Architectures
- VI. Scenarios Demo
- VII. Conclusion & Future Work





## IV. Requirements

### **Business Requirement:**

1. Tăng khả năng nhận diện và kiểm soát các ứng dụng đang sử dụng trong mạng.
2. Ngăn chặn nhân viên truy cập vào các trang web không phù hợp hoặc nguy hiểm.
3. Bảo vệ người dùng khỏi việc vô tình tải về virus hoặc mã độc qua web.
4. Chủ động phòng chống các cuộc tấn công từ các nguồn đã biết trên Internet.
5. Phát hiện và cảnh báo sớm các hành vi tấn công mạng như quét cổng, dò quét lỗ hổng.
6. Có một hệ thống bảo vệ tập trung, thay vì phải quản lý nhiều thiết bị/phần mềm riêng lẻ.



## IV. Requirements

### Non-Business Requirements:

Type	Description
Functional	<ul style="list-style-type: none"><li>• Khả năng lọc gói tin stateful.</li><li>• Kiểm tra gói tin dựa trên signature của Suricata.</li><li>• Chuyển hướng traffic HTTP/HTTPS đến proxy.</li><li>• Lọc URL dựa trên danh sách đen.</li><li>• Gọi dịch vụ ICAP để quét virus.</li><li>• Ghi lại log chi tiết cho các sự kiện bảo mật.</li></ul>
Non-Functional	<ul style="list-style-type: none"><li>• Triển khai trên nền tảng Ubuntu Server 22.04.</li><li>• Latency khi duyệt web không bị ảnh hưởng đáng kể (best-effort).</li><li>• Danh sách Threat Intelligence &amp; signature của AV có khả năng cập nhật định kỳ.</li><li>• Hệ thống hoạt động ổn định trong môi trường thử nghiệm.</li></ul>



# AGENDA

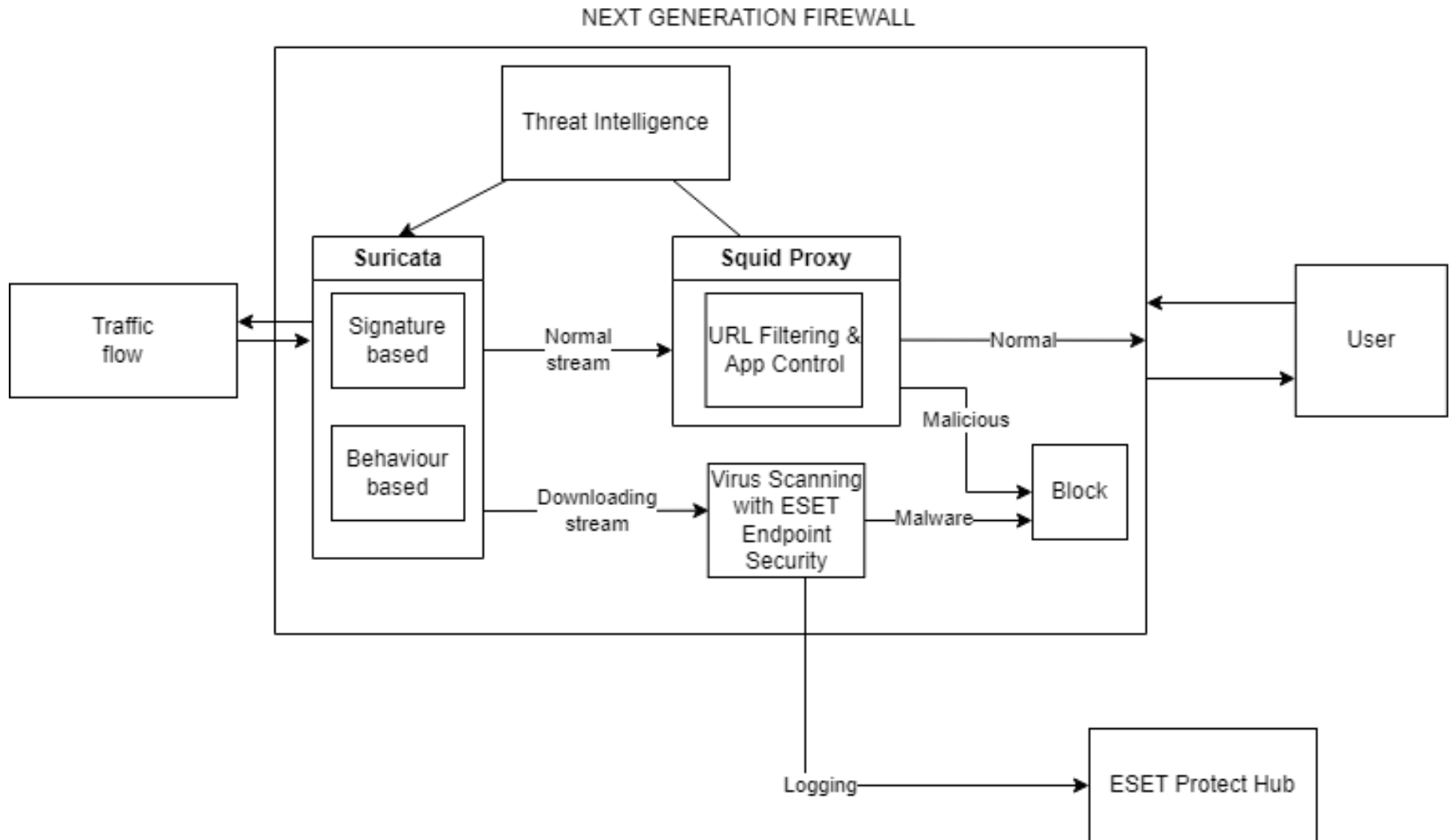
---

- I. Context
- II. Technology Trends
- III. Project Objectives (Scope & Out of Scope)
- IV. Business & Non-Business Requirements
- V. Architectures**
- VI. Scenarios Demo
- VII. Conclusion & Future Work



# V. Architectures

## Application/Component Architecture:



# V. Architectures

---

## Infrastructure Architecture:



# V. Architectures

## Security Architecture - Defense in Depth:

- Layer 1 - Edge:  
Threat Intelligence chặn các kết nối độc hại ngay từ đầu.
- Layer 2 - Network:  
IDS/IPS phân tích sâu traffic mạng, phát hiện tấn công, hành vi lạ, kiểm soát ứng dụng.
- Layer 3 - Application:  
Squid Proxy kiểm soát truy cập web (URL Filtering), là điểm trung chuyển để quét virus.
- Layer 4 - Content:  
AV quét nội dung file tải về.



# V. Architectures

**Signature-based Detection:** Phát hiện dựa trên các mẫu tấn công đã biết.

- Công cụ: **Suricata**.
- Cài đặt:

```
sudo apt-get install software-properties-common && sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
```
- `/etc/suricata/suricata.yaml`:

```
af-packet:
- interface: <interface trong ip addr>
- cluster-id: 99
- cluster-type :cluster_flow
- defrag: yes
- tpacket-v3: yes
```
- Set rule trong `/var/lib/suricata/rules`:

```
alert http any any -> any any (msg:"HTTP test string detected"; content:"test"; sid:10000002; rev:1;)
```
- Cập nhật rule & restart server:

```
sudo suricata-update && sudo systemctl restart suricata
```



# V. Architectures

**Behaviour-based:** Phát hiện các hành vi bất thường, không dựa vào signature cụ thể.

- Cấu hình suricata.yaml:

flow:

memcap: 16mb // dung lượng bộ nhớ tối đa cho các kết nối.

hash-size: 100000

expire: // cấu hình thời gian hết hạn của các kết nối không sử dụng.

default: 60. // kết nối không có lưu lượng sẽ hết hạn sau 60 giây.

tcp-established: 3600

- Về phát hiện hành vi:

- Port Scanning: phát hiện dựa trên số lượng kết nối đến nhiều cổng khác nhau từ một nguồn.
- Kết nối bất thường: Số lượng lớn kết nối DNS, kết nối đến các IP/port lạ.
- Anomalies trong giao thức HTTP/DNS/TLS.





# V. Architectures

**Bot management:** Phát hiện và ngăn chặn traffic từ các botnet.

- Thresholding: cấu hình threshold trong suricata.yaml:

threshold:

type: threshold

values:

limit:

# Giới hạn số lượng yêu cầu (gói tin) từ một địa chỉ IP trong một khoảng thời gian

- count: 100

seconds: 60

action: alert

msg: "Possible DDoS attack detected"

→ Đã triển khai thành công IDS/IPS với Suricata, có khả năng phát hiện dựa trên signature và một số hành vi cơ bản, cũng như các cơ chế ban đầu cho Bot Management.



# V. Architectures

**Threat Intelligence:** Sử dụng thông tin về các mối đe dọa đã biết (IPs, domains độc hại) để chủ động chặn.

- Nguồn IoCs: nhà phân phối uy tín như [abuse.ch](https://abuse.ch), [PhishTank](https://phishTank.com), và FireHOL Level 1.
- Thêm các URL đáng nghi vào blocked domain list của Squid thì hoàn tất tích hợp Threat Intelligence vào hệ thống.



# V. Architectures

---

**Virus Scanning:** Quét virus/malware cho các file tải về.

- Sử dụng EDET Security Endpoint có thể tích hợp vào Firewall.
- Install link: [link](#).



# V. Architectures

---

## Conclusion:

→ Tích hợp thành công Threat Intelligence để chặn IP/domain độc hại và hệ thống quét virus cho traffic web.



# V. Architectures

## URL filtering + Application Control:

- Chức năng: Kiểm soát truy cập web dựa trên URL hoặc danh mục trang web. Nhận diện & kiểm soát các ứng dụng mạng.
- Cài đặt:  
`sudo apt-get update && sudo apt-get install squid`
- Cấu hình squid proxy squid.conf:  
`acl localnet src 192.168.1.0/24 // Cho phép máy internal network`  
`http_access allow localnet`  
`acl blocked_sites dstdomain "/etc/squid/blocked_sites.txt"`  
`http_access deny blocked_sites`  
`http_access allow all`
- Kiểm thử (set up connect từ port squid kiểm soát):  
`sudo systemctl restart squid.service`  
`curl -x http://127.0.0.1:3128 http://example.com`



## Conclusion:

- Thành công triển khai web filtering trong đó có thể kiểm soát được các URL có thể kết nối được từ trong mạng nội bộ.
- Để làm application control, có thể chặn truy cập đến các tên miền mà các ứng dụng phổ biến sử dụng.

# AGENDA

---

- I. Context**
- II. Technology Trends**
- III. Project Objectives (Scope & Out of Scope)**
- IV. Business & Non-Business Requirements**
- V. Architectures**
- VI. Scenarios Demo**
- VII. Conclusion & Future Work**



# VI. Scenarios Demo

---

- Demo 1 - Phát hiện Signature (IDS)
- Demo 2 - Lọc URL (URL Filtering)
- Demo 3 - Chặn IP độc hại (Threat Intelligence)
- Demo 4 - Quét Virus





# VI. Scenarios Demo

---

- Demo 1 - Phát hiện Signature (IDS)
- Demo 2 - Lọc URL (URL Filtering)
- Demo 3 - Quét Virus các file tải về và thông báo



# VI. Scenarios Demo

## - Demo 1: IDS

```
Ubuntu 64 2204 X
Activities Terminal
Thg 5 10 22:12
haventz2110@ubuntu: ~/Desktop

haventz2110@ubuntu:~/Desktop$ sudo tail -f /var/log/suricata/fast.log
[sudo] password for haventz2110:

05/10/2025-18:10:46.175395 00000001:1 HTTP test string detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.11.128:58304 -> 13.35.186.17:80
05/10/2025-18:21:27.657660 00000001:1 HTTP test string detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.11.128:32954 -> 13.35.186.17:80
05/10/2025-18:29:35.402881 00000001:1 HTTP test string detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.11.128:55692 -> 18.155.192.22:80
05/10/2025-21:43:57.748041 00000001:1 HTTP test string detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.11.128:57546 -> 108.157.32.27:80
05/10/2025-22:12:43.688438 00000001:1 HTTP test string detected [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.11.128:38170 -> 108.157.32.27:80

haventz2110@ubuntu: /tmp

haventz2110@ubuntu:/tmp$ curl http://testmyids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
haventz2110@ubuntu:/tmp$
```



# VI. Scenarios Demo

## - Demo 2: URL Filtering

The screenshot shows a terminal window with two panes. The left pane shows the output of a curl command, and the right pane shows the Squid proxy access logs.

**Left Pane (Terminal Output):**

```
havertz2110@ubuntu: ~/Desktop$ curl -x http://127.0.0.1:3128 http://youtube.com
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (c) 1996-2020 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
/*
 * Copyright (c) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
 * Stylesheet for Squid Error pages
 * Adapted from design by Free CSS Templates
 * http://www.freecsstemplates.org
 * Released for free under a Creative Commons Attribution 2.5 License
 */

/* Page basics */
* {
    font-family: verdana, sans-serif;
}

html body {
    margin: 0;
    padding: 0;
    background: #efefef;
    font-size: 12px;
    color: #1e1e1e;
}

/* Page displayed title area */
#titles {
    margin-left: 15px;
    padding: 10px;
    padding-left: 100px;
    background: url('/squid-internal-static/icons/SN.png') no-repeat left;
```

**Right Pane (Terminal Output):**

```
havertz2110@ubuntu: ~/nextgenwaf/squid/squid-build$ sudo tail -f /var/log/squid/access.log
1746948818.960 0 127.0.0.1 TCP_DENIED/403 3855 GET http://example.com/ - HIER_NONE/
- text/html
1746948841.248 0 127.0.0.1 TCP_DENIED/403 3855 GET http://example.com/ - HIER_NONE/
- text/html
1746948905.155 0 127.0.0.1 TCP_DENIED/403 3855 GET http://youtube.com/ - HIER_NONE/
- text/html
1746948920.706 70 127.0.0.1 TCP_MISS/301 290 GET http://threads.com/ - HIER_DIRECT/5
7.144.144.192 text/plain
1746948952.950 67 127.0.0.1 TCP_MISS/301 294 GET http://www.threads.com/ - HIER_DIRECT/57.144.144.192 text/plain
1746948958.525 165 127.0.0.1 TCP_MISS/301 465 GET http://www.wikipedia.com/ - HIER_DIRECT/103.102.166.226 text/html
```





```
<div id="titles">
<h1>ERROR</h1>
<h2>The requested URL could not be retrieved</h2>
</div>
<hr>

<div id="content">
<p>The following error was encountered while trying to retrieve the URL: <a href="http://
youtube.com/">http://youtube.com/</a></p>

<blockquote id="error">
<p><b>Access Denied.</b></p>
</blockquote>


<p>Access control configuration prevents your request from being allowed at this time. P
lease contact your service provider if you feel this is incorrect.</p>


<p>Your cache administrator is <a href="mailto:webmaster?subject=CacheErrorInfo%20-%20ERR
R_ACCESS_DENIED&amp;body=CacheHost%3A%20ubuntu%0D%0AErrPage%3A%20ERR_ACCESS_DENIED%0D%0A
Err%3A%20%5Bnone%5D%0D%0ATimeStamp%3A%20Sun,%2011%20May%202025%2007%3A35%3A05%20GMT%0D%0
A%0D%0AClientIP%3A%20127.0.0.1%0D%0A%0D%0AHTTP%20Request%3A%0D%0AGET%20%2F%20HTTP%2F1.1%
0AUser-Agent%3A%20curl%2F7.81.0%0D%0AAccept%3A%20*%2F*%0D%0AProxy-Connection%3A%20Keep-A
live%0D%0AHost%3A%20youtube.com%0D%0A%0D%0A%0D%0A">webmaster</a>.</p>
<br>
</div>

<hr>
<div id="footer">
<p>Generated Sun, 11 May 2025 07:35:05 GMT by ubuntu (squid/5.9)</p>
<!-- ERR_ACCESS_DENIED -->
</div>
```

# VI. Scenarios Demo

- Demo 3: Quét Virus các file tải về và thông báo

 PROTECT



QUICK LINKS ▾

HELP ▾

ANH BUI VUONG TAM

LOGOUT

DASHBOARD

COMPUTERS

INCIDENTS

Detections

Reports

Tasks

Installers

Policies

Notifications

Status Overview

Platform Modules

More

Submit Feedback

COLLAPSE

< BACK

REFRESH

GENERATE AND DOWNLOAD ▾

### Report: Drill Down - Detailed information

Server Name

Generated at  
May 13, 2025 12:34:46 (UTC+07:00)

Number of records  
7

Filters  
Filter count: 3

Computer name	Static group name	Severity	Time of occurrence	Detection type	Detection name	Scanner	Object URI	Detection handled	Restart required	User	Process name	Adapter IPv4 address	IPv4 subnetwork	Adapter IPv6 address	IPv6 subnetwork	Detection engine	First seen time	Hash of detected file	Detection resolved
desktop-sd83ab8	Lost & found	Warning	May 13, 2025 10:17:14	Test file	Eicar	HTTP filter	https://secure.eicar.org/eicar.com	yes	no	DESKTOP - SD83AB8 \buivu	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	192.168.1.1130	192.168.1.1.0		192.168.1.1.0	31188 (20250513)		3395856C E81F2B73 82DEE726 02F798B6 42F14140	yes
desktop-sd83ab8	Lost & found	Warning	May 13, 2025 10:18:18	Test file	Eicar	HTTP filter	https://secure.eicar.org/eicar.com	yes	no	DESKTOP - SD83AB8 \buivu	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	192.168.1.1130	192.168.1.1.0		192.168.1.1.0	31188 (20250513)		3395856C E81F2B73 82DEE726 02F798B6 42F14140	yes



# AGENDA

---

- I. Context**
- II. Technology Trends**
- III. Project Objectives (Scope & Out of Scope)**
- IV. Business & Non-Business Requirements**
- V. Architectures**
- VI. Scenarios Demo**
- VII. Conclusion & Future Work**

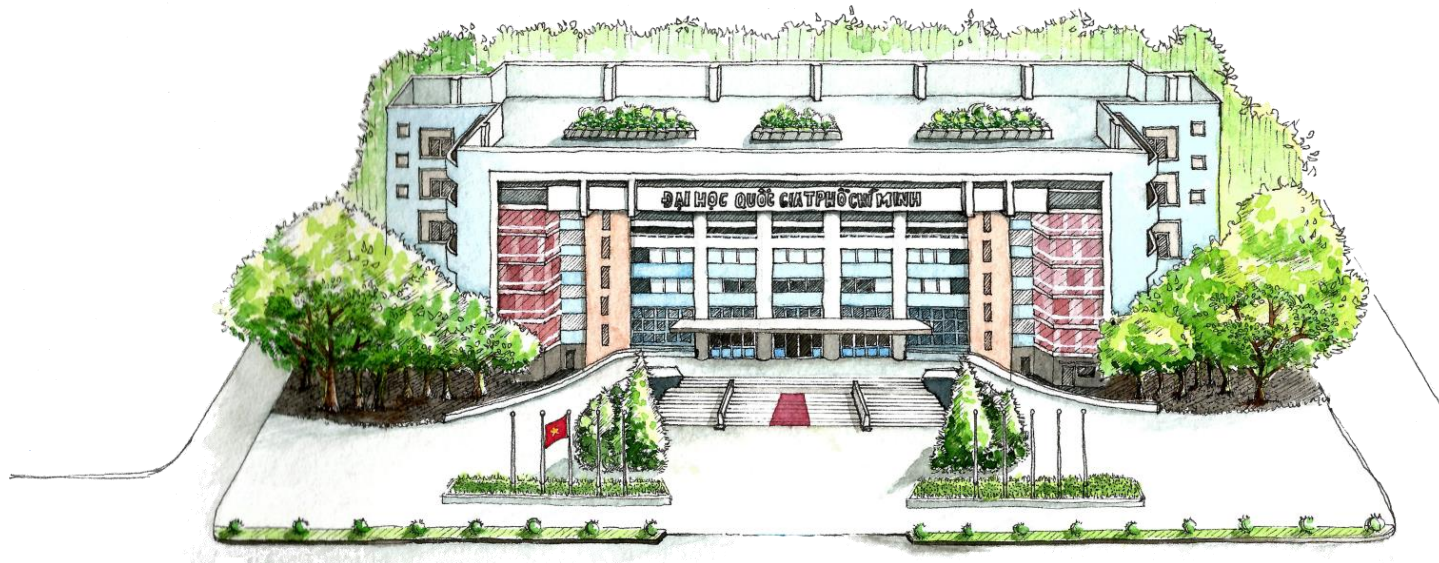




Trường ĐH Công nghệ Thông tin  
Đại Học Quốc Gia TP. HCM



ĐẠI HỌC  
QUỐC GIA  
TP. HỒ CHÍ MINH



**Xin cảm ơn.**