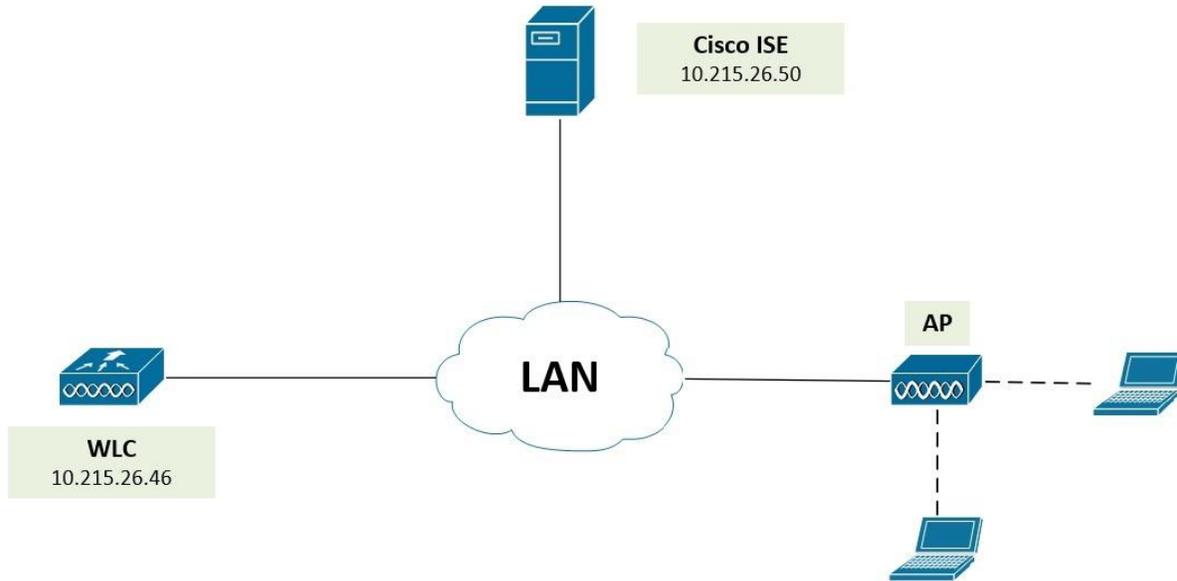


Lab – Wireless Guest Hotspot (Cấu hình Manual trên WLC và Cisco ISE)

1. Sơ đồ



2. Cấu hình trên WLC

- Đầu tiên ta phải cấu hình để AP Join vào WLC hay chưa, vào mục Wireless để kiểm tra

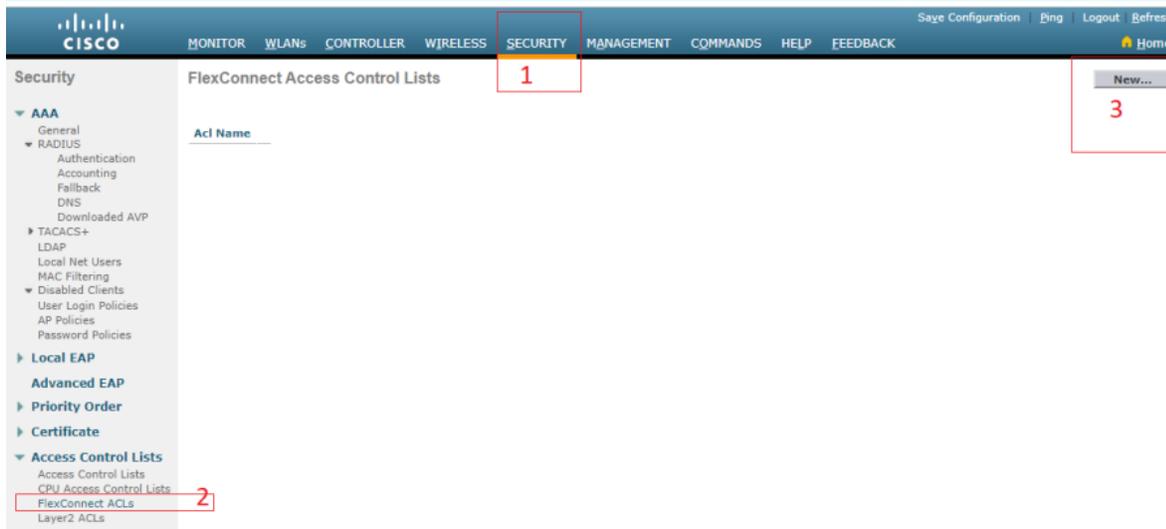
AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Speed Eth0
3602-1925	10.215.26.219	AIR-CAP3602I-A-K9	30:f7:0d:f6:ff:90	6 d, 07 h 27 m 57 s	Enabled	REG	PoE/Full Power	100 Mbps
AP1928	192.168.3.167	AIR-CAP3602I-N-K9	d4:8c:b5:93:1e:52	0 d, 04 h 33 m 05 s	Enabled	REG	PoE/Full Power	100 Mbps

- Ta cấu hình khai báo Radius Server (Cisco ISE) với WLC như sau: vào mục Security -> AAA-> Radius -> Authentication -> New

- Ta khai báo các tham số của Authentication bao gồm các thông tin sau như sau:
 - (1) Địa chỉ IP của Radius Server
 - (2) Shared Secret: lưu ý thông tin Shared secret phải giống nhau giữa WLC và Radius Server, điền lại thông tin shared secret 1 lần nữa tại mục Confirm
 - (3) Enable Support CoA
 - (4) Enable Network User

Chọn Apply để lưu cấu hình Authentication Server.

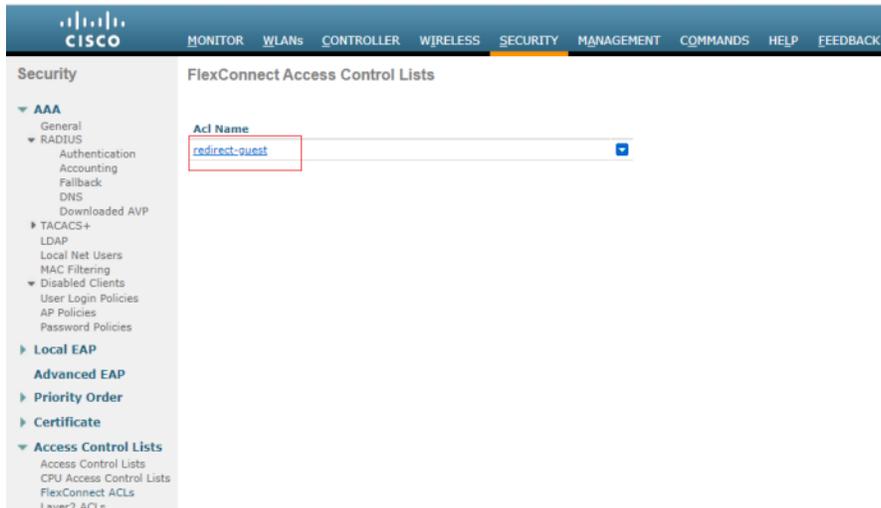
- Tại mục Security này, ta phải tạo ra 1 ACL để có thể Redirect traffic xác thực của Guest đến được Cisco Ise, ta tạo như sau: Tại tab Security -> Access Control List -> Chọn FlexConnect ACLs -> Chọn New



- Ta tiến hành đặt tên cho ACL này và chọn Apply để lưu lại



- Sau khi Apply, ta sẽ có 1 ACL được tạo ra như bên dưới



- Tuy nhiên ACL này vẫn chưa có bất kì hành động nào, ta sẽ tiếp hành tạo hành động cho ACL này bằng cách click vào ACL vừa tạo và tiến hành tạo rule cho ACL này như sau: click vào Add New Rule và tạo hành động giống như hình bên dưới

Security > Access Control Lists > Edit

General

Access List Name: redirect-guest

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.215.26.49 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.215.26.49 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any

Security > Access Control Lists > Edit

General

Access List Name: redirect-guest

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.215.26.49 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.215.26.49 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any

Lưu ý: địa chỉ IP trên ACL là địa chỉ IP của Cisco Ise

- Tiếp theo ta sẽ tạo SSID trên WLC: Chọn WLAN -> tại mục Create new chọn Go

WLANs > WLANs

Current Filter: None [Change Filter] [Clear Filter]

Create New [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
---------	------	--------------	-----------	--------------	-------------------

- Điền thông tin Profile name và SSID (2 thông tin này không nhất thiết phải giống nhau) -> Chọn Apply để lưu lại cấu hình

WLANs > New

Type: WLAN

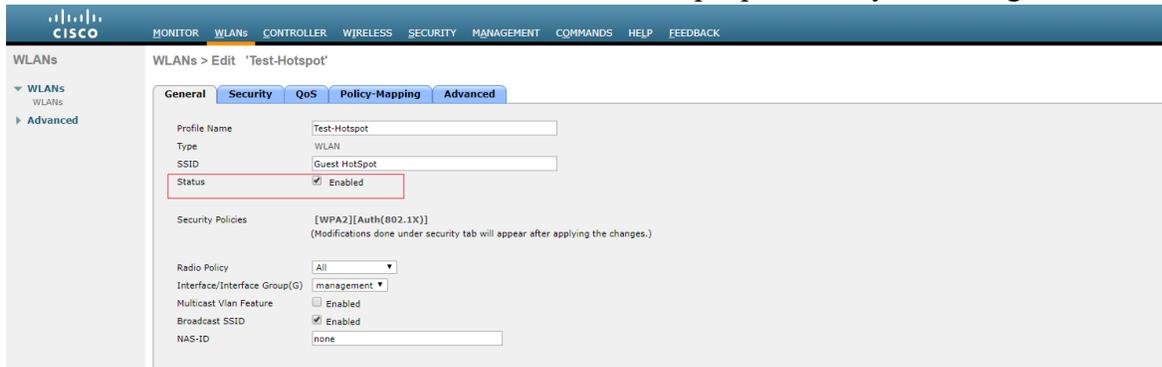
Profile Name: Test-Hotspot

SSID: Guest HotSpot

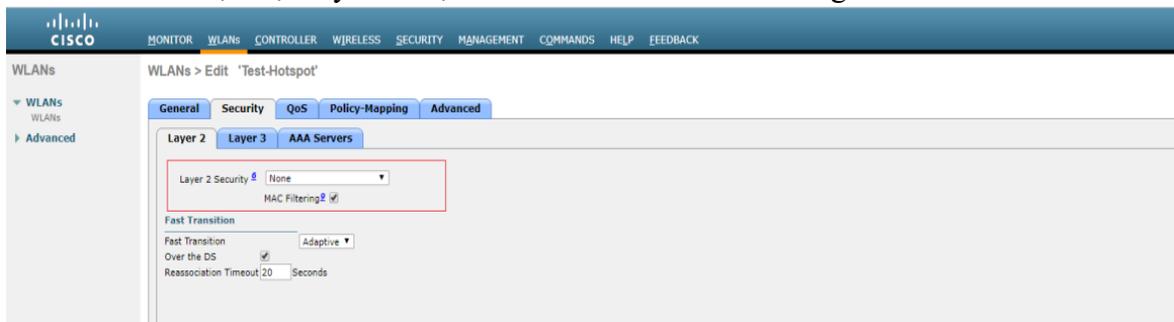
ID: 1

[Apply]

- Tại tab General -> Enable Status SSID để cho phép SSID này hoạt động



- Qua tab Security,
 - o Tại mục layer 2 chọn None và check Mac Filtering



- o Tại mục layer 3 chọn None, qua mục AAA server chọn đến địa chỉ Authentication Server mà chúng ta đã cấu hình lúc này



- Qua tab Advanced -> Check Allow AAA override, tìm đến mục NAC -> chọn ISE NAC -> Apply để lưu cấu hình

- Tiếp tục cấu hình để AP có thể Redirect user khi kết nối đến SSID thì chúng ta cần cấu hình như sau: qua tab Wireless -> chọn AP đang kết nối -> qua tab Flexconnect -> Click vào External WebAuthentication ACLs

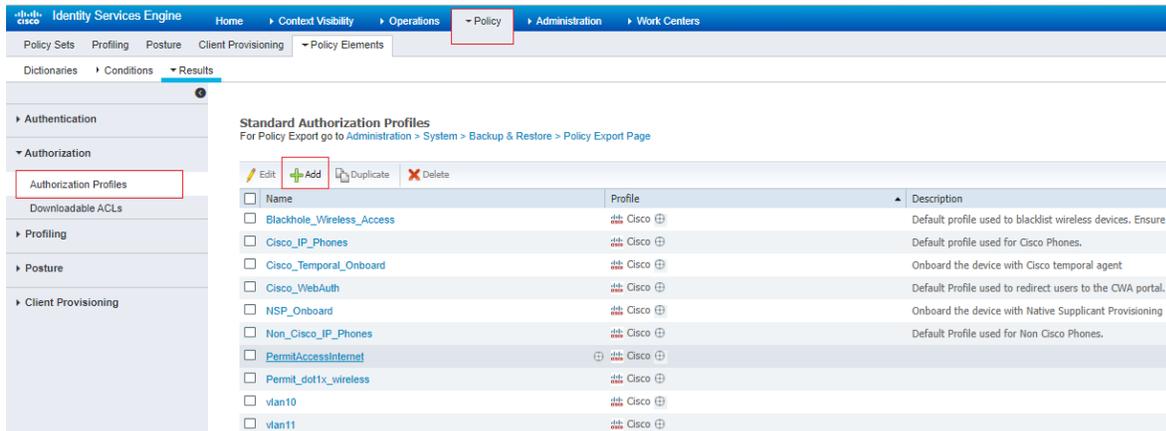
- Tại mục Policy -> click Add ACL mà chúng ta đã tạo lúc này -> chọn Apply để lưu lại cấu hình

- Bây giờ chúng ta sẽ tiến hành cấu hình Portal trên Cisco ISE để Guest xác thực khi kết nối vào SSID là Guest HotSpot, chúng ta có thể sử dụng Portal default trên Cisco ISE hoặc ta có thể tạo mới 1 Portal khác trên Cisco ISE (ở đây mình sẽ sử dụng Portal default trên Cisco ISE)
- Đầu tiên đăng nhập vào Cisco ISE và Add thiết bị WLC vào Cisco ISE -> chọn Administration -> Chọn Network devices, sau khi cửa sổ hiện ra chọn ADD để tiến hành Add WLC vào Cisco ISE bao gồm Tên WLC (1), địa chỉ IP của WLC (2), sau đó click vào Radius Authentication Setting -> điền thông tin Shared Secret vào (lưu ý Shared Secret phải giống với WLC) -> chọn Submit để lưu cấu hình

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices. The left sidebar shows 'Network Devices' selected. The main content area is titled 'Network Devices List > New Network Device'. The form contains the following fields:

- Name:** WLC (marked with a red box and '1')
- Description:** (empty)
- IP Address:** 10.215.26.46 / 32 (marked with a red box and '2')
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:** (empty)
- Location:** All Locations (Set To Default)
- IPSEC:** Is IPSEC Device (Set To Default)
- Device Type:** All Device Types (Set To Default)
- RADIUS Authentication Settings:** (checked, marked with a red box and '3')
 - Protocol:** RADIUS
 - Shared Secret:** (masked with dots, marked with a red box and '4')
 - CoA Port:** 1700 (Set To Default)
 - RADIUS DTLS Settings:**
 - DTLS Required:** (unchecked)
 - Shared Secret:** radius/dtls
 - CoA Port:** 2083 (Set To Default)
 - Issuer CA of ISE Certificates for CoA:** Select if required (optional)
 - DNS Name:** (empty)
 - General Settings:**
 - Enable KeyWrap:** (unchecked)

- Tiếp theo, ta sẽ tạo Result cho việc Authentication trên Cisco ISE, ta làm như sau: Chọn Policy -> Result -> chọn Authentication Profiles -> Add



Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Name	Profile	Description
<input type="checkbox"/> Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure t
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplciant Provisioning
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> PermitAccessInternet	Cisco	
<input type="checkbox"/> Permit_dot1x_wireless	Cisco	
<input type="checkbox"/> vlan10	Cisco	
<input type="checkbox"/> vlan11	Cisco	

- Một cửa sổ mới hiện ra ta điền các thông tin cho Authentication như bên dưới, đầu tiên là Tên của profile này và Action Types là Access_Accept, tại mục Common Tasks -> tìm đến Web Redirction (CWA, MDM, NSP, CPP) -> chọn HotSpot -> tại ô ACL ta điền tên ACL mà chúng ta đã tạo ở WLC vào -> tại mục Value chọn HotSpot Guest Portal (default), tại mục này ta điền thông tin địa chỉ IP của Cisco ISE vào mục Static IP/ Host name/FQDN, sau đó chọn Submit để lưu cấu hình

- Tiếp theo ta sẽ tạo Policy cho việc truy cập vào SSID Guest HotSpot như sau: Chọn Policy -> Policy Set -> chọn biểu tượng Setting và click vào Insert new row above.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Dot1x_Radius		Wired_802.1X	Default Network Access	120	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

- Ta có thể sửa tên cho Policy vừa tạo, ở đây mình đặt là Wireless_HotSpot -> Tại mục Condition chọn kiểu xác thực là Wireless_MAB, tại mục Allowed Protocol/ Server Sequence chọn Default Network Access -> chọn Save để lưu cấu hình sau đó chọn biểu tượng mũi tên > để tiếp tục cấu hình cho Policy này

The screenshot shows the 'Policy Sets' page in the Identity Services Engine. A table lists three policy sets: 'Dot1x_Radius', 'Wireless_HoSpot', and 'Default'. The 'Wireless_HoSpot' row is highlighted with a red box. To its right, the 'Wireless_MAB' condition is also highlighted with a red box. The 'Allowed Protocols / Server Sequence' column shows 'Default Network Access' for each set, with a 'Hits' column showing 120 for Dot1x_Radius and 0 for the others.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Action
✔	Dot1x_Radius		Wired_802.1X	Default Network Access	120	⚙️
✔	Wireless_HoSpot		Wireless_MAB	Default Network Access	0	⚙️
✔	Default	Default policy set		Default Network Access	0	⚙️

- Tại mục Authentication Policy, tại mục USE chọn Internal Endpoint, tại mục option -> If User not found chọn Continue

The screenshot shows the configuration page for the 'Wireless_HoSpot' policy set. Under the 'Authentication Policy (1)' section, a table lists the 'Default' rule. The 'Use' column is set to 'Internal Endpoints'. Under the 'Options' section, 'If User not found' is set to 'CONTINUE'. The 'Internal Endpoints' dropdown and the 'CONTINUE' option are highlighted with red boxes.

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Endpoints	0	⚙️

Options

- If Auth fail: REJECT
- If User not found: CONTINUE
- If Process fail: DROP

- Tiếp tục kéo xuống mục Authorization Policy, Click vào biểu tượng Setting -> Chọn Insert new row above để tạo ra cách thức xác thực cho SSID Guest HotSpot

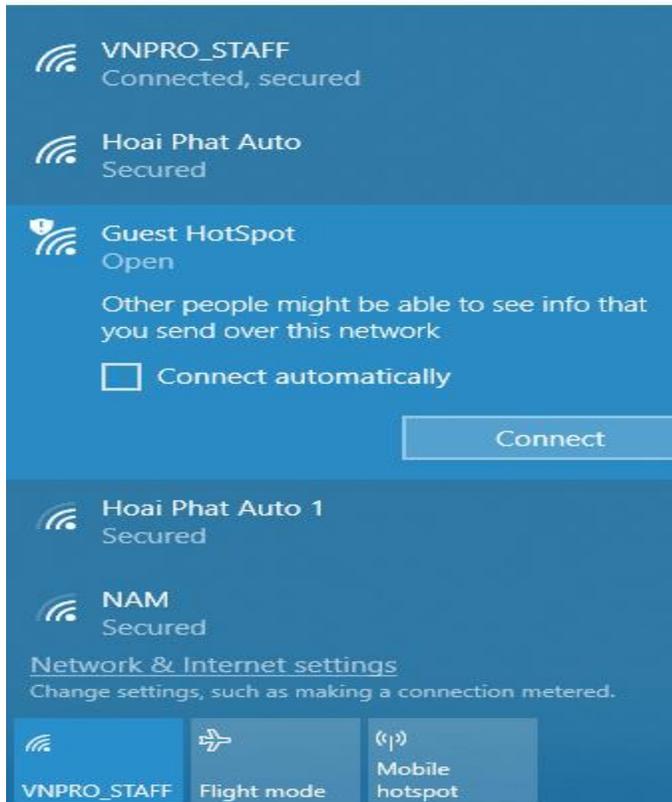
- Cấu hình như hình bên dưới, sau khi tạo xong các Row chọn Save để lưu lại cấu hình

- Ta có thể cấu hình cho Portal HotSpot này tự động Redirect đến Website của doanh nghiệp của mình như sau: vào mục Work Centers -> Guest Access -> Portals & Components

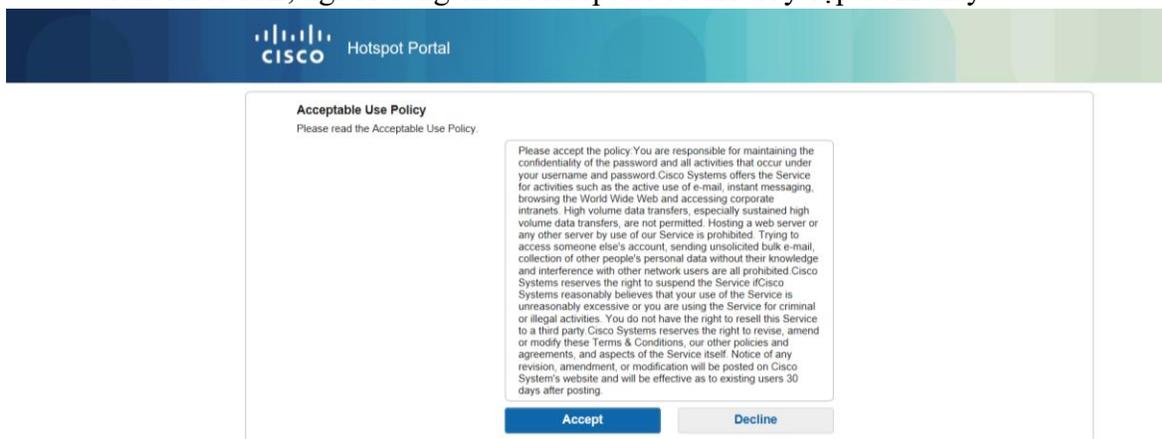
- Tại mục Guest Portal -> Click vào HotSpot Guest Portal (default) để cấu hình cho Portal này

- Tìm đến mục Authentication Success Settings và làm như hình bên dưới để Redirect tới một Website nào đó -> chọn Save để lưu lại cấu hình Portal này

- Kiểm tra SSID như sau, mở card mạng Wireless -> chọn SSID cần kết nối là Guest HotSpot -> Connect để kết nối



- Sau khi connect vào SSID này, Web browser sẽ truy cập đến Cisco để mở trang Portal trên Cisco ISE, người dùng click Accept để có thể truy cập SSID này



- Sau khi Click Accept, Web browser sẽ redirect đến Website mà chúng ta đã cấu hình lúc này



CÔNG TY TNHH TƯ VẤN VÀ DỊCH VỤ CHUYÊN VIỆT
TRUNG TÂM TIN HỌC VNPRO

ĐC: 276 - 278 Ung Văn Khiêm, P. Thanh Mỹ Tây, Tp. Hồ Chí Minh
ĐT: (028) 35124257 | **Hotline:** 0933427079 **Email:** vnpro@vnpro.org
