

Cấu hình AuthPoint Multi-factor Authentication (MFA) cho PfSense OpenVPN kết hợp với Active Directory (Radius)



ITMAP
ASIA

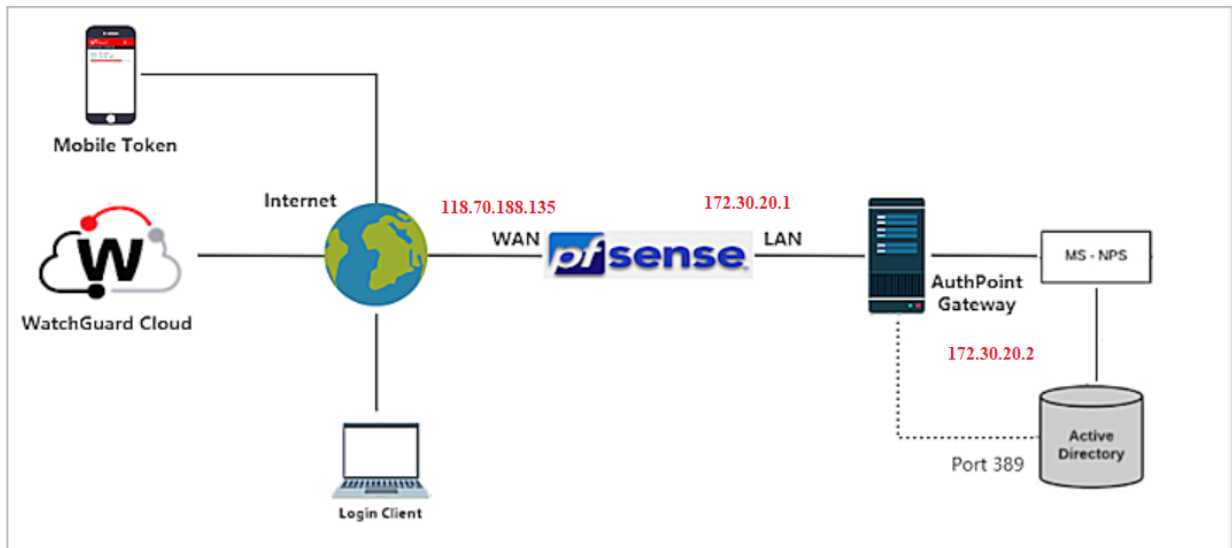
555 Trần Hưng Đạo, P. Cầu Kho, Q.1, TP.HCM

Tel: 028 5404 0717 - 5404 0799. www.itmapasia.com | info@itmapasia.com

Content

1. Topology
2. WatchGuard MFA
3. Cấu hình NPS server
4. Cấu hình Pfsense OpenVPN – RADIUS
5. Kiểm tra kết nối OpenVPN – MFA

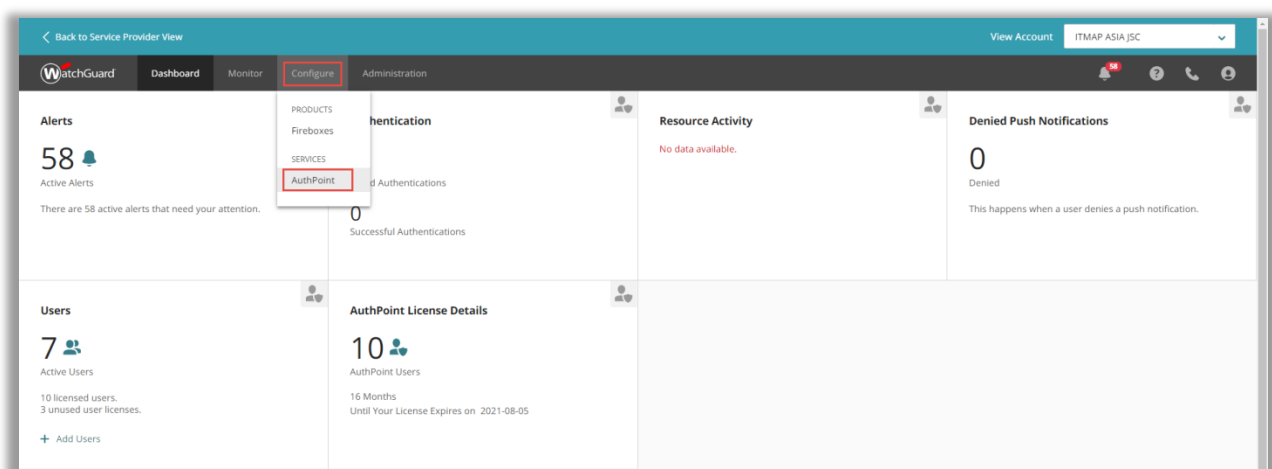
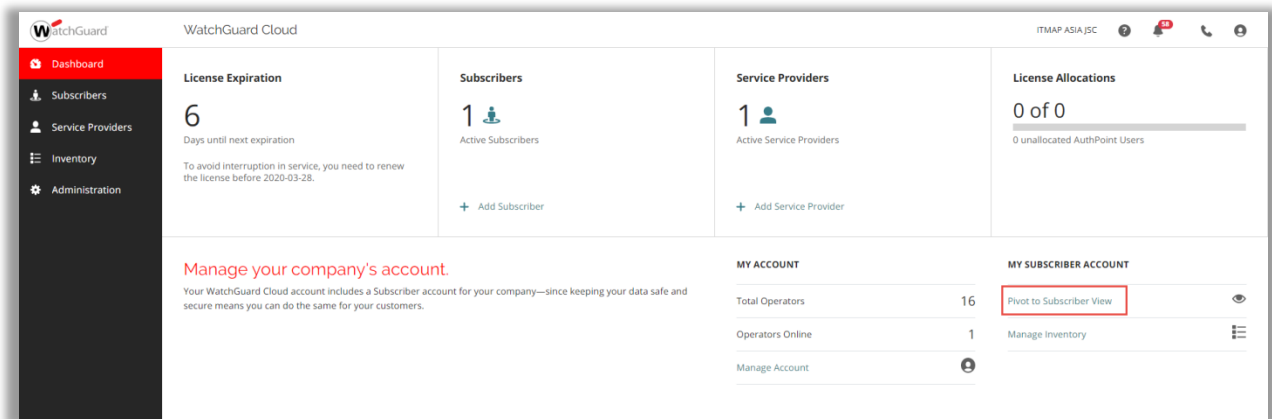
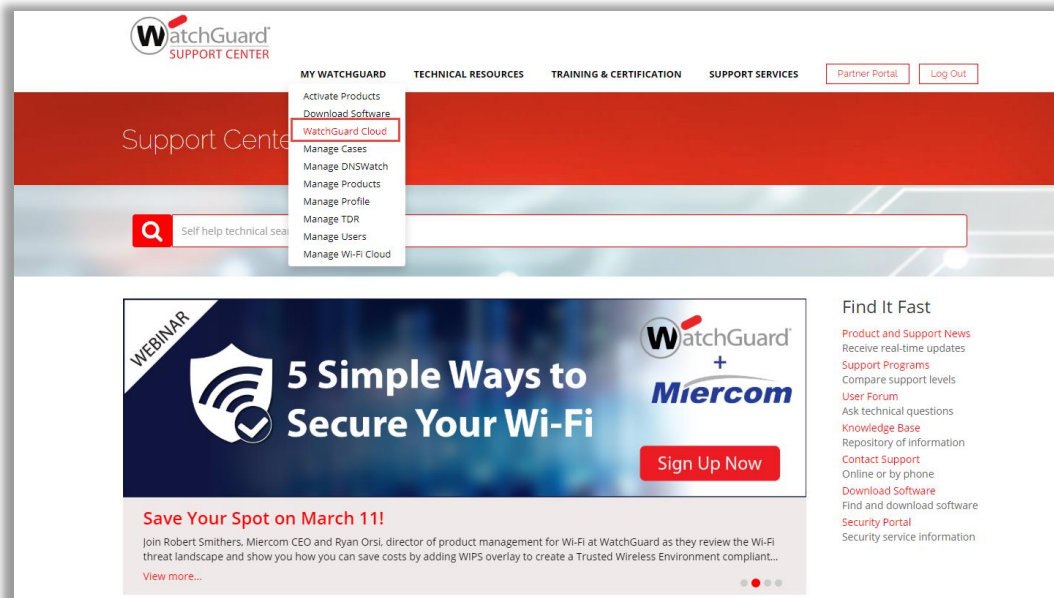
1. Topology



Quy trình xác thực MFA - OPENVPN:

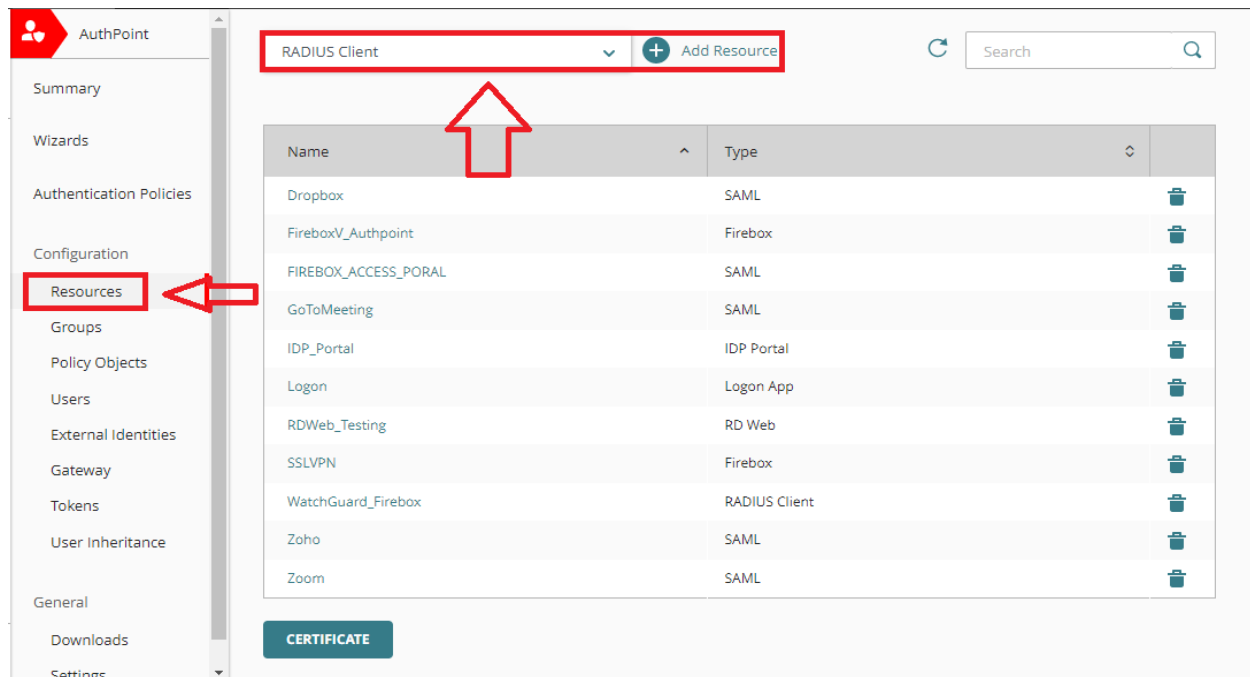
- 1.1. User tiến hành quay VPN Client-to-site vào PFSENSE (OpenVPN Server) kèm các trường xác thực Server, User name và Password.
- 1.2. Pfsense dựa trên trường User name thực hiện chuyển tiếp yêu cầu xác thực đến AuthPoint Gateway (AuthPoint Gateway là phần mềm có thể cài đặt trực tiếp trên Active Directory Server hoặc một máy tính nằm trong mạng nội bộ)
- 1.3. AuthPoint Gateway nhận yêu cầu từ Pfsense và chuyển tiếp đến WatchGuard Cloud nhằm kiểm tra trường User name (có thể tích hợp RADIUS hoặc LDAP để tổ chức dữ liệu user)
- 1.4. WatchGuard Cloud thực hiện kiểm tra Access Policy chung trên mỗi user name đã được định nghĩa trong AuthPoint Group.
- 1.5. Nếu user tồn tại trên AuthPoint Group, WatchGuard Cloud sẽ tiến hành gửi xác thực MFA đến Smartphone và yêu cầu xác thực. Sau khi User thực hiện xác thực, thông tin MFA sẽ được gửi trả về cho WatchGuard Cloud để tiến hành kiểm tra tính hợp lệ của Access Policy.
- 1.6. Sau khi đã hoàn tất việc kiểm tra, thông tin xác thực MFA của User sẽ được gửi về AuthPoint Gateway.
- 1.7. AuthPoint Gateway thực hiện phản hồi kết quả xác thực đến Pfsense, Pfsense sẽ dựa trên kết quả xác thực và tiến hành cho phép user kết nối.
- 1.8. Pfsense thực hiện cấp phép và kiểm soát việc truy cập của user.

2. **WatchGuard MFA:** Cần tài khoản WatchGuard, nếu chưa có thì tham khảo tài liệu tạo tài khoản

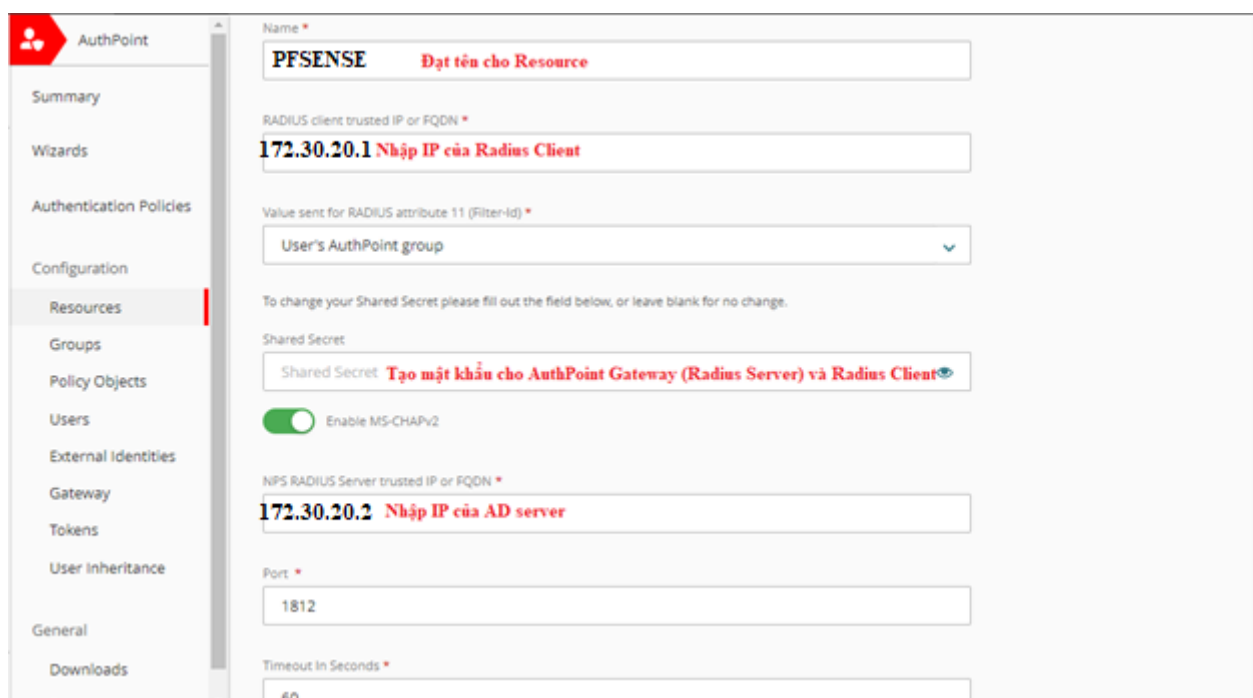


2.1. RADIUS Client Resource in AuthPoint: Mục đích để tạo kết nối giữa AuthPoint Gateway (RADIUS Server với IP 172.30.20.2) và Pfsense có IP 172.30.20.1 kèm Shared Secret

- **Bước 1:** Chọn “Resource” → Bấm “Choose a Resource Type” → “RADIUS Client” → “Add Resource”.

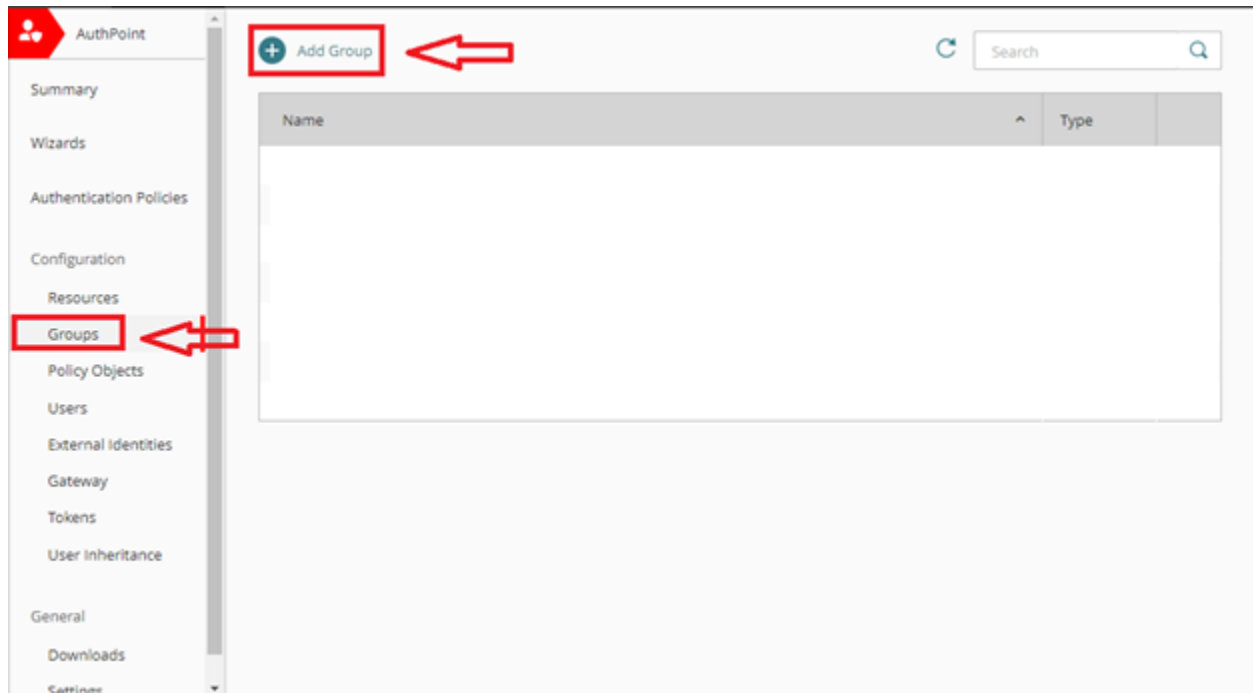


- **Bước 2 :** Làm theo hướng dẫn như trong ảnh → Save.

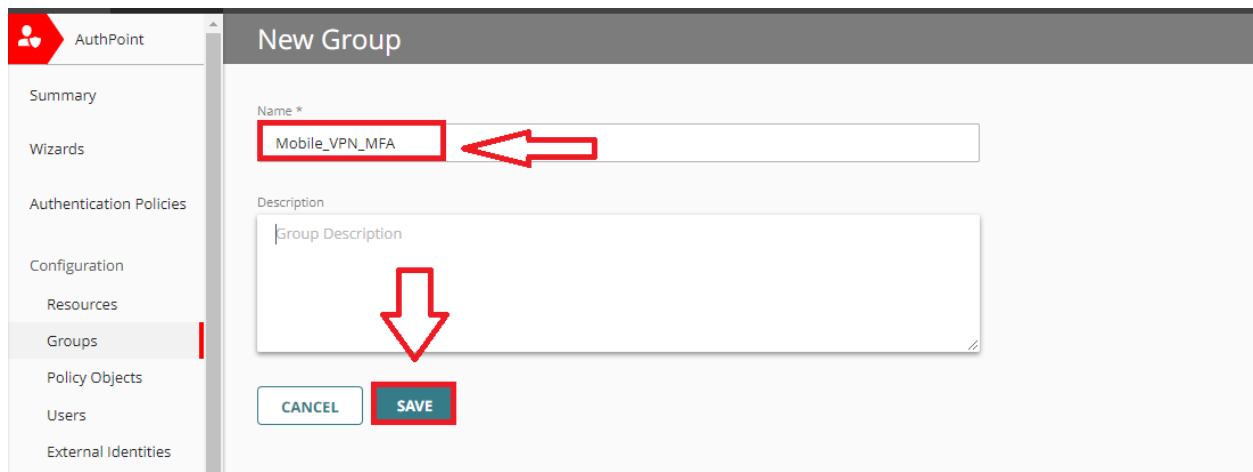


2.2. **Group in AuthPoint:** Group này phải trùng tên với Group trên AD server và Group trên Firebox.

- **Bước 1:** Groups → Add Group

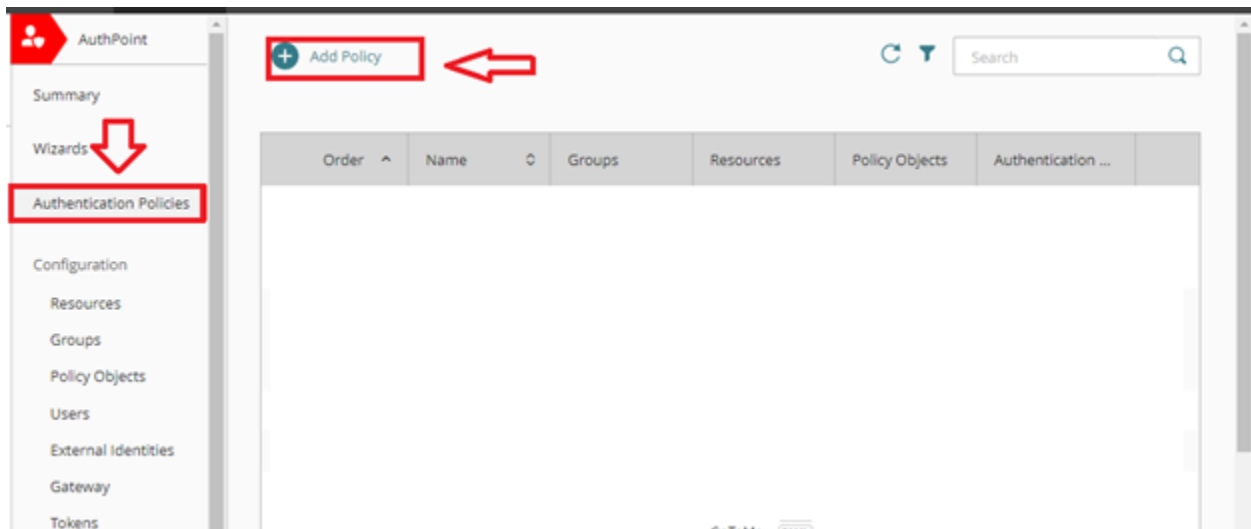


- **Bước 2:** Nhập tên Group → Save (Group này phải cùng tên với group trên AD server và PfSense)

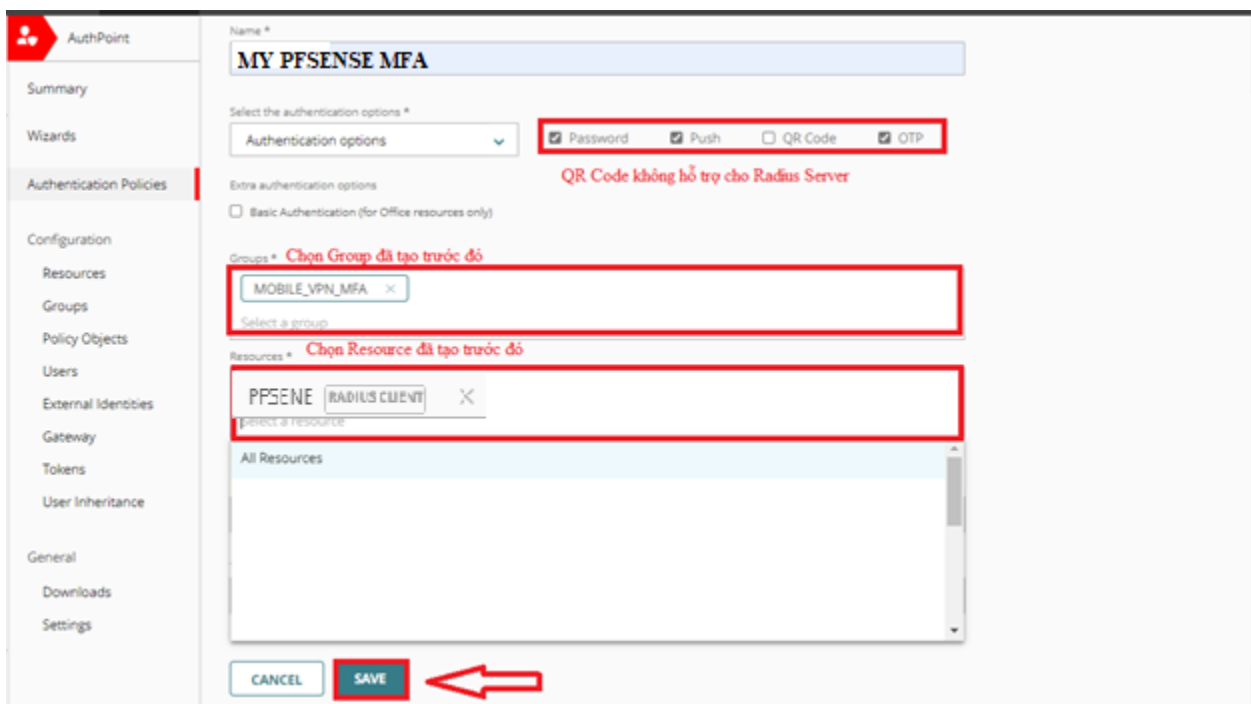


2.3. Authentication Policy to AuthPoint:

- **Bước 1:** Authentication Policies → Add Policy

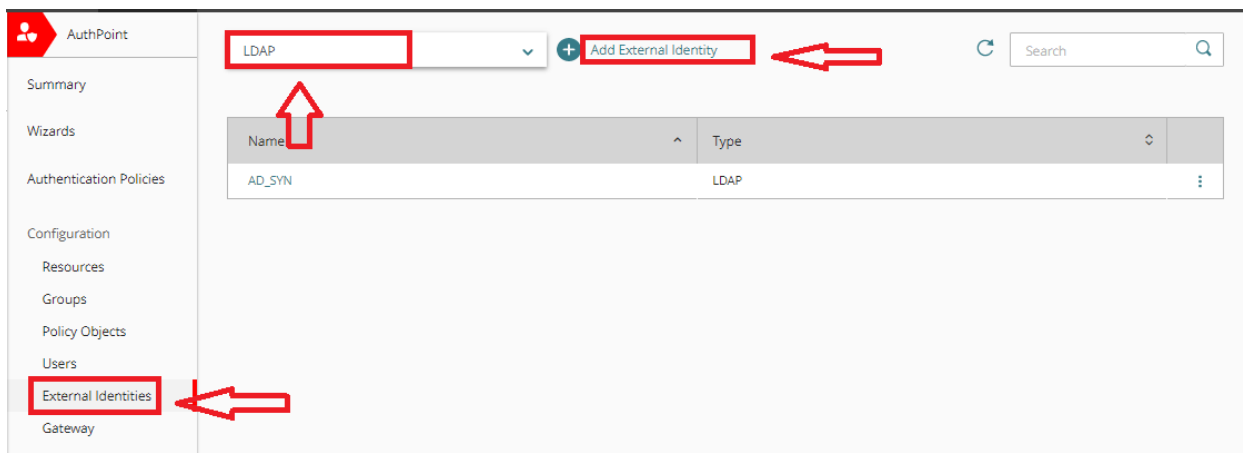


- **Bước 2:** Làm theo hướng dẫn như trong ảnh. Nếu bạn chọn Push và OTP thì Radius dùng Push



2.4. Tạo External Identity cho Gateway:

- **Bước 1:** Chọn “External Identities” → Bấm “Choose an External Identity Type” → “LDAP” → “Add External Identity”



- **Bước 2:** Làm theo hướng dẫn trong hình

LDAP Configuration

Name *

Sync Users From Bali

LDAP Search Base *

dc=bali,dc=local

☒ If your system account user is not in the Users CN, enable this option and type the user's DN below.

System Account DN *

CN=Administrator,CN=Users,DC=bali,DC=local

Passphrase *

Mật Khẩu có quyền admin trên AD server. Ở trên mình dùng tài khoản của Administrator

..... Tuy nhiên bạn có thể tạo account mới ngang quyền với Administrator

Synchronization Interval *

Every 24 hours at 12 pm

Type

☒ Active Directory ☐ Others

Domain *

bali.local

Attribute related to the first name *

Attribute related to the last name *

Attribute related to the user email *

Main attribute to the LDAP user *

Attribute related to the user login *

Attribute related to the mobile number *


Server Address * Gõ địa chỉ IP của AD Server


☒ LDAPS


Server Port *

2.5. Gateway:

- **Bước 1:** Chọn Gateway → Add Gateway


AuthPoint


Add Gateway


Search

Summary
Wizards
Authentication Policies
Configuration
Resources
Groups
Policy Objects
Users
External Identities
Gateway
Tokens
User Inheritance

- **Bước 2 :** Làm theo hướng dẫn trong hình → Save. (Nếu AD server đã tồn tại Radius server dùng port 1812 và 1645 thì hãy đổi port cho Gateway này, Đây là port giao tiếp giữa AuthPoint Gateway và Radius Client)

Name *

GW_Bali_FF

RADIUS

Port *

18121

Nếu AD server đã tồn tại Radius server dùng port 1812 và 1645 thì hãy đổi port cho Gateway này. Ở đây mình đổi thành 18121

Select a RADIUS resource

PFSENE

Select a RADIUS

Chọn Resource đã tạo trước đó

ADFS

Select an ADFS resource

Select an ADFS

LDAP

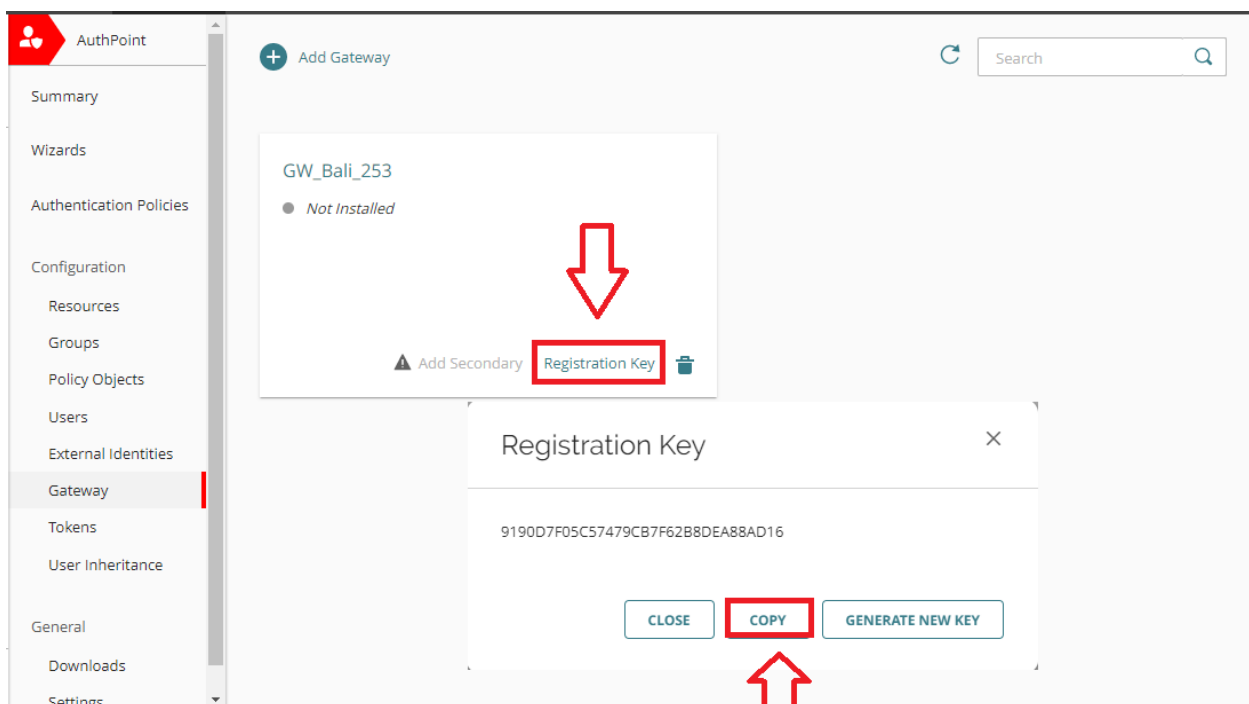
Select an LDAP external identity

SYNC USERS FROM BALI

Chọn External Identify đã tạo trước đó

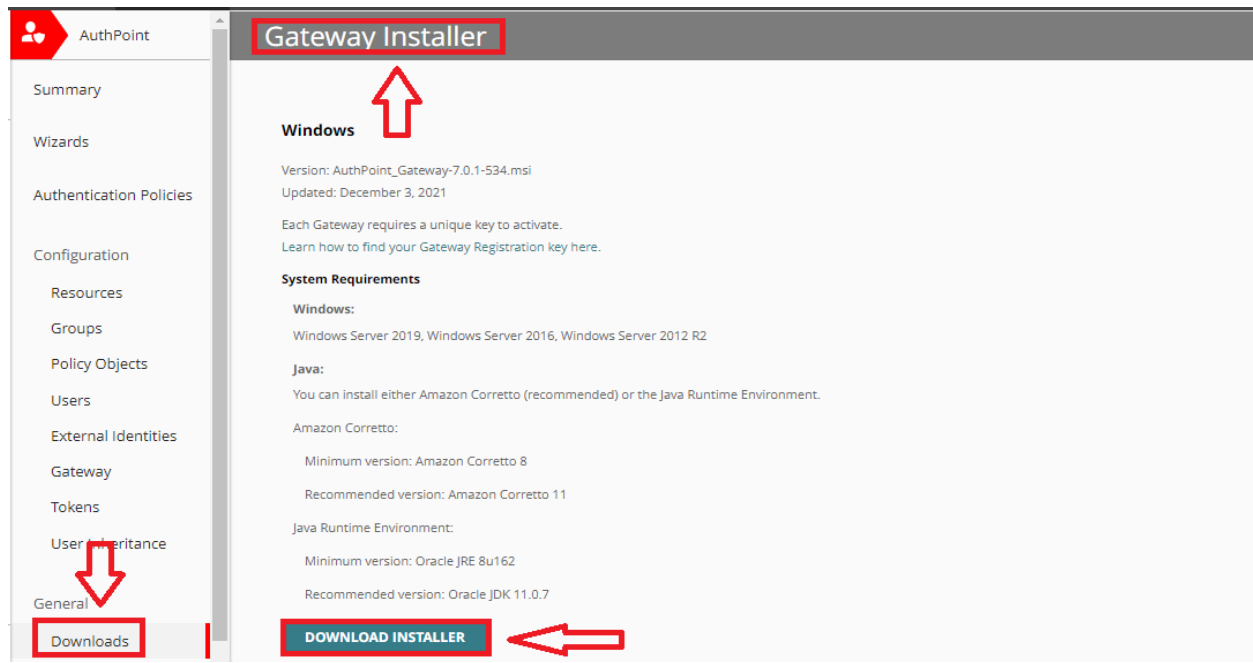
Select a LDAP

- **Bước 3:** Bấm “Registration Key” → Copy → Close. (Registration Key này dùng để xác thực khi cài đặt Gateway trên AD Server)

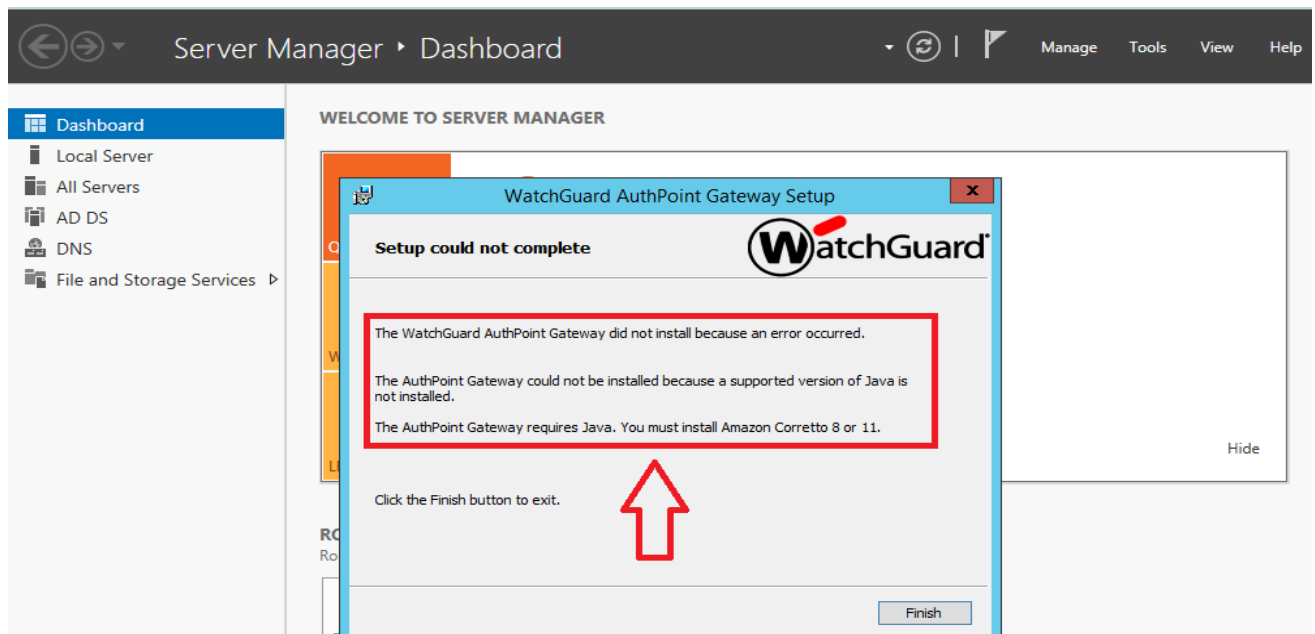


2.6. Download và cài đặt Gateway cho AD Server:

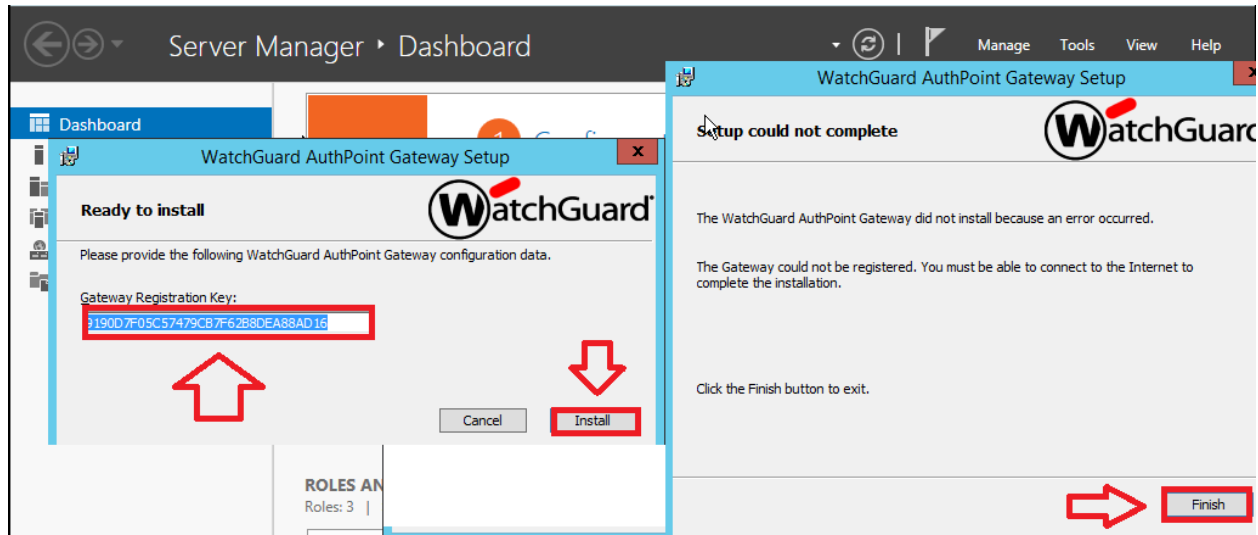
- **Bước 1:** Để Download Gateway → Download → Gateway Installer → Download Installer



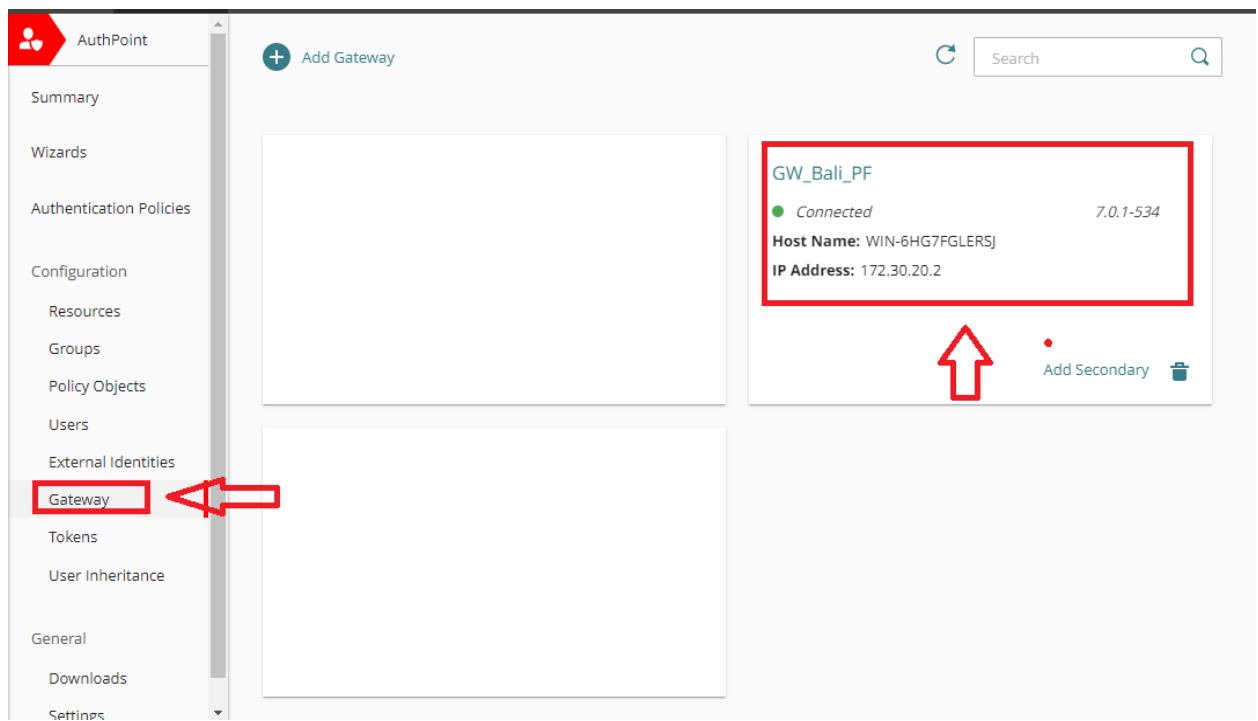
- **Bước 2:** Vào AD Server để cài đặt Gateway vừa Download (AuthPoint_Gateway-7.0.1-534) → Nếu bạn nhận thông báo lỗi không thể cài đặt, xin hãy vào đường dẫn này <https://aws.amazon.com/corretto/> để Download Amazon Corretto 8 và cài đặt → Cài đặt lại Gateway lần nữa.




- **Bước 3:** Nhập Registration Key mà bạn đã copy ở bước 3 của phần 2.5 → Install → Finish.
Nếu bạn đã cài đặt Gateway nhưng vẫn không kết nối được thì hãy vào lại bước 3 của phần 2.5 rồi bấm “Registration Key” và chọn “Generate Key” để tạo lại Key mới và cài đặt lại Gateway với Key mới lần nữa.

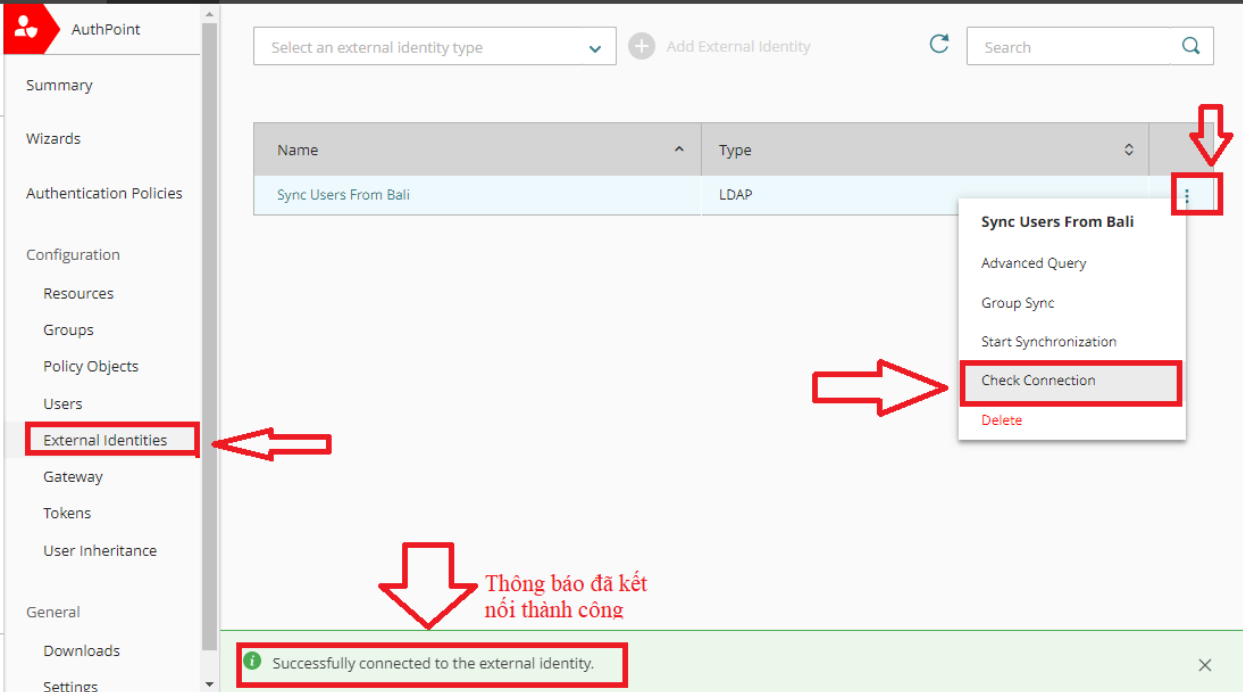


- **Bước 4:** Kiểm tra lại kết nối của Gateway. Nếu Gateway vẫn hiện **Not Installed** → Tắt phần mềm diệt virus hoặc firewall trên AD server. Đảm bảo rằng port 1812, 1645 với UDP phải được mở trên AD server và các services của WatchGuard AuthenPoint đảm bảo Running.



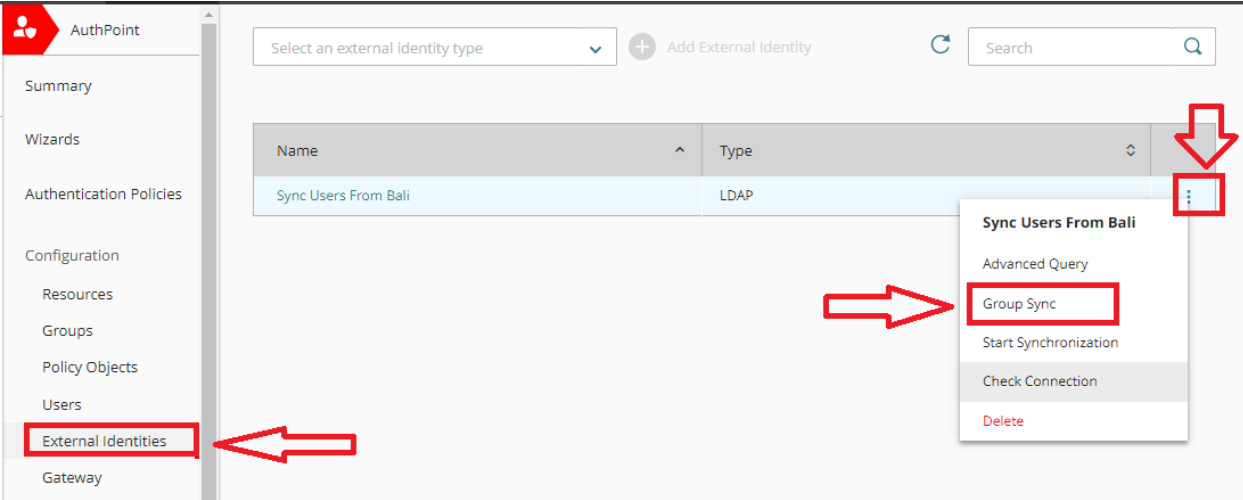
2.7. Sync Users từ AD server

- **Bước 1:** Kiểm tra kết nối của External Identity. External Identity → Bấm  → Chọn Check Connection



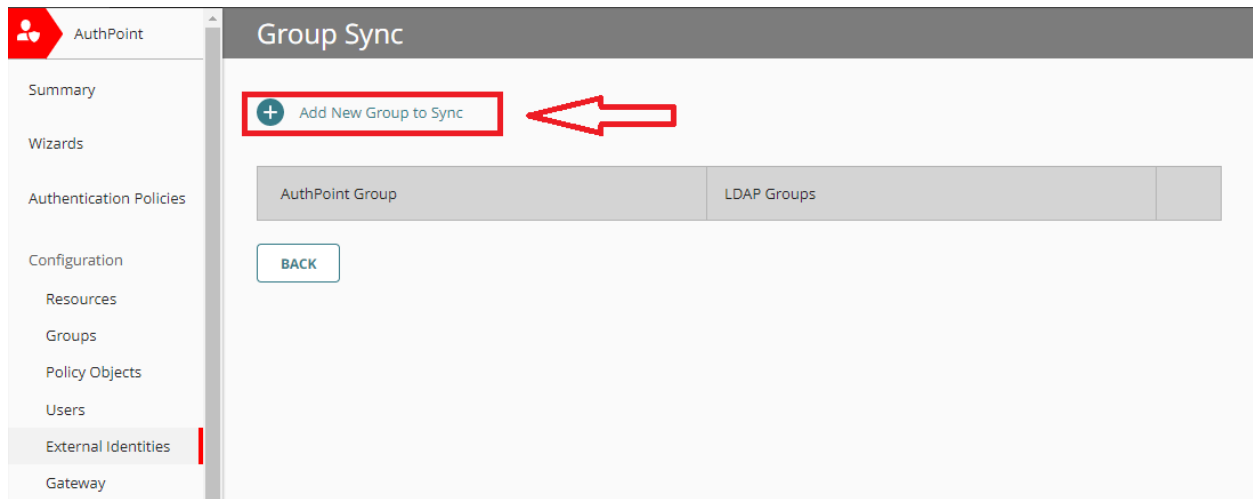
The screenshot shows the WatchGuard AuthPoint interface. On the left sidebar, the 'External Identities' menu item is highlighted with a red box and an arrow. The main panel displays a table with two columns: 'Name' and 'Type'. The first row is 'Sync Users From Bali' with type 'LDAP'. A red box highlights the three-dot menu icon at the end of this row. A context menu is open, showing options: 'Advanced Query', 'Group Sync', 'Start Synchronization', 'Check Connection' (highlighted with a red box and arrow), and 'Delete'. Below the table, a green notification bar states 'Successfully connected to the external identity.' with a red arrow pointing to it and the text 'Thông báo đã kết nối thành công'.

- **Bước 2:** Sync Group. External Identity → Bấm  → Chọn Group Sync

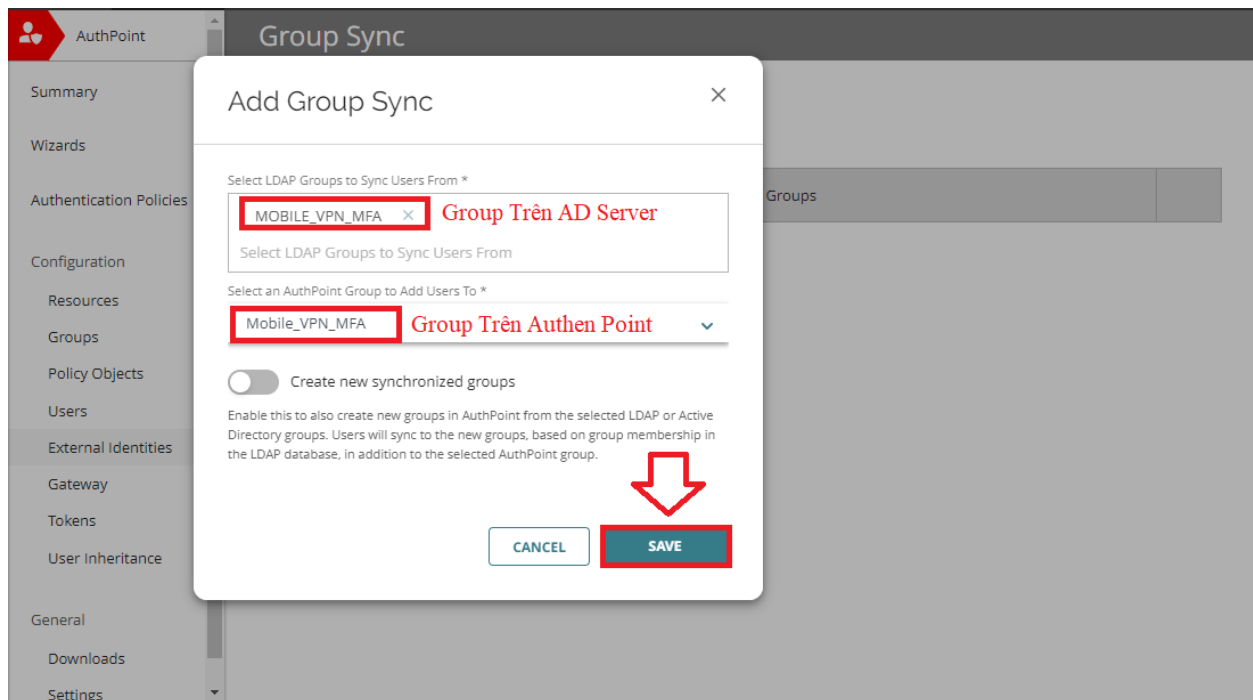


This screenshot is similar to the previous one, showing the 'External Identities' section. The 'Sync Users From Bali' entry is selected, and the context menu is open. In this step, the 'Group Sync' option is highlighted with a red box and an arrow, instead of 'Check Connection'. The notification bar is not present in this image.

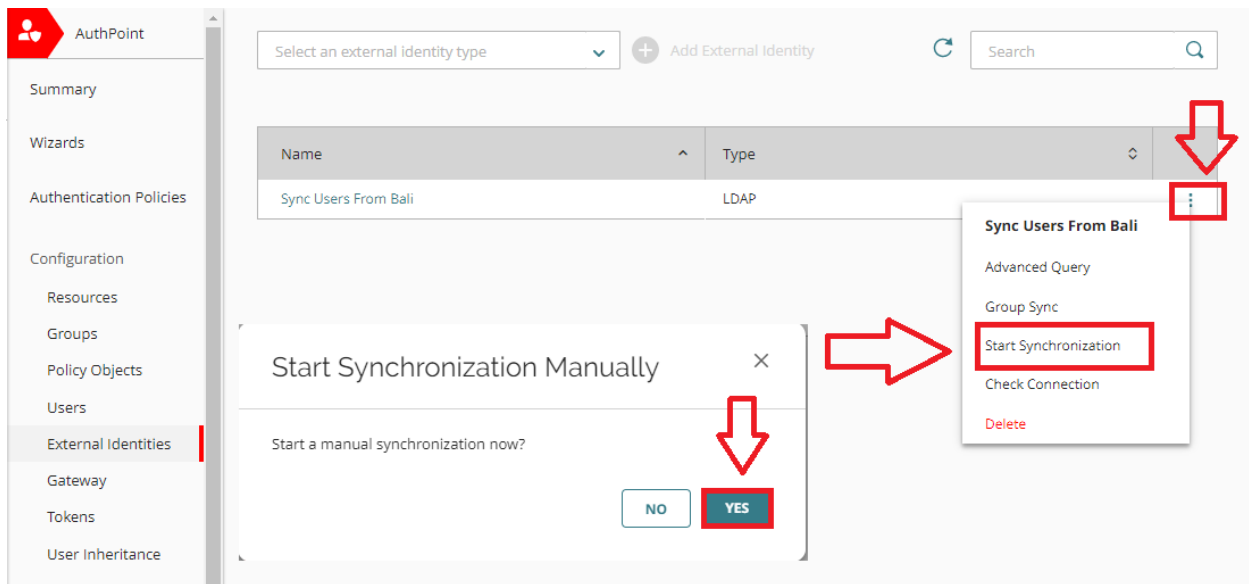
- **Bước 3:** Click “Add New Group to Sync”



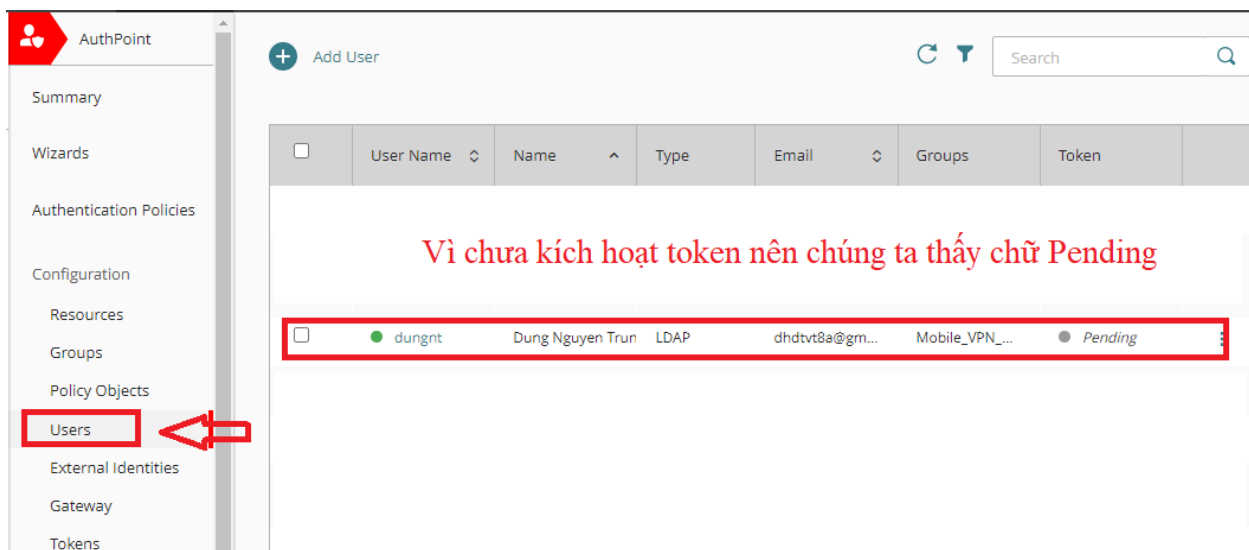
- **Bước 4:** Chọn Group trên AD Server → Chọn Group trên AthenPoint → Save.



- **Bước 5 :** Bấm → Chọn Start Synchronization → Yes. Nếu User của AD Server thiếu first name, user name, or email address thì sẽ không được đồng bộ.

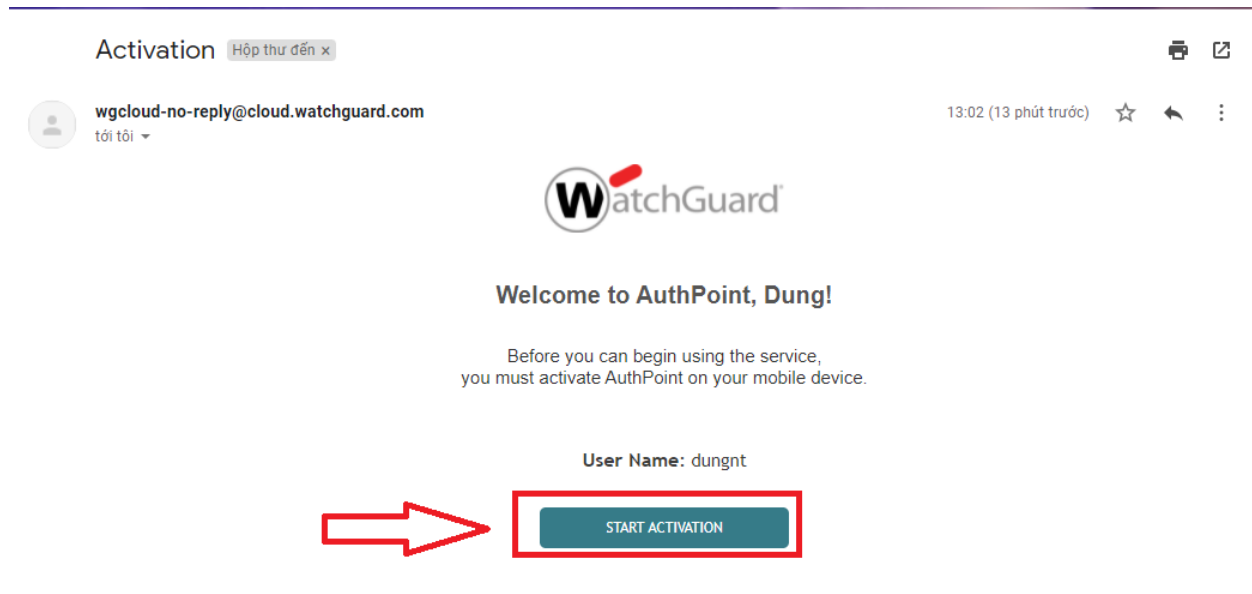


- **Bước 6 :** Kiểm tra việc đồng bộ AD users lên Authpoint Users. Nếu việc đồng bộ thành công, thông tin Authpoint users sẽ hiển thị (ký tự LDAP) như hình bên dưới.

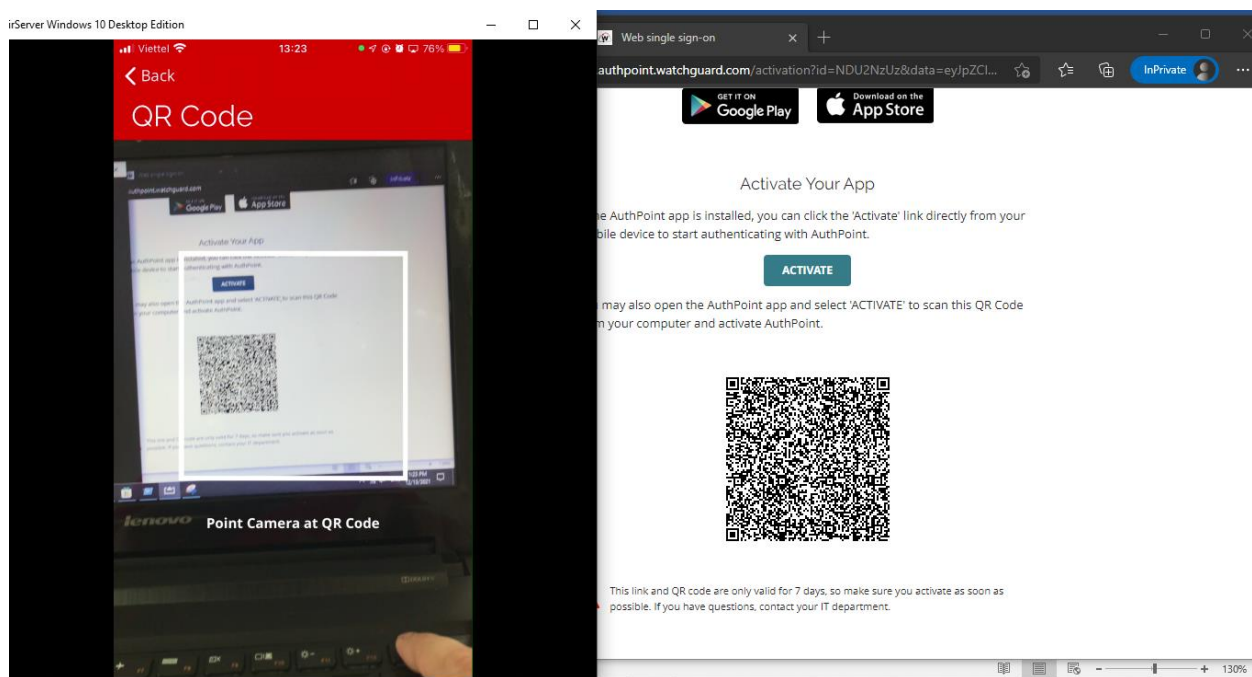


2.8. Kích hoạt Token

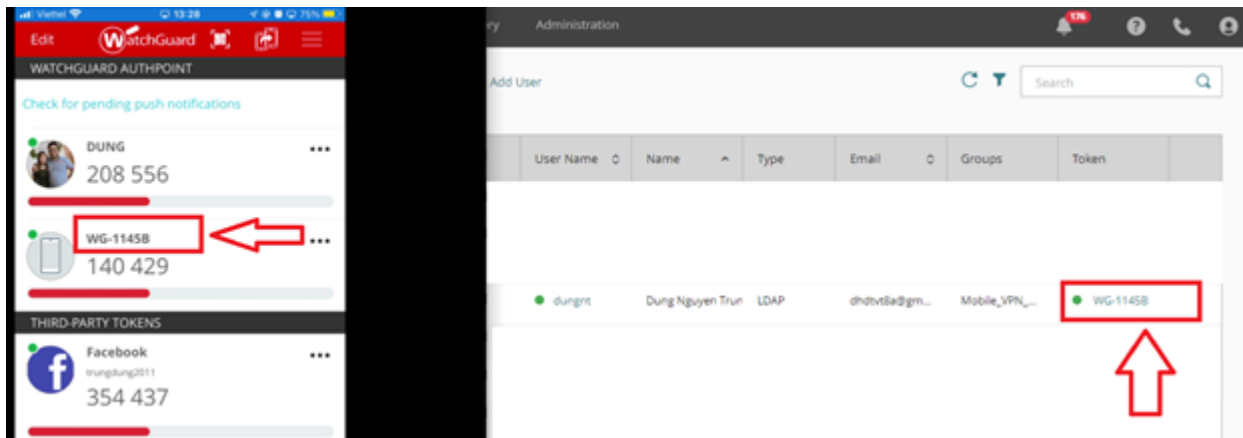
- **Bước 1 :** Truy cập vào email để kích hoạt Token → Bấm Start Activation



- **Bước 2 :** Dùng điện thoại để kích hoạt Token bằng QR

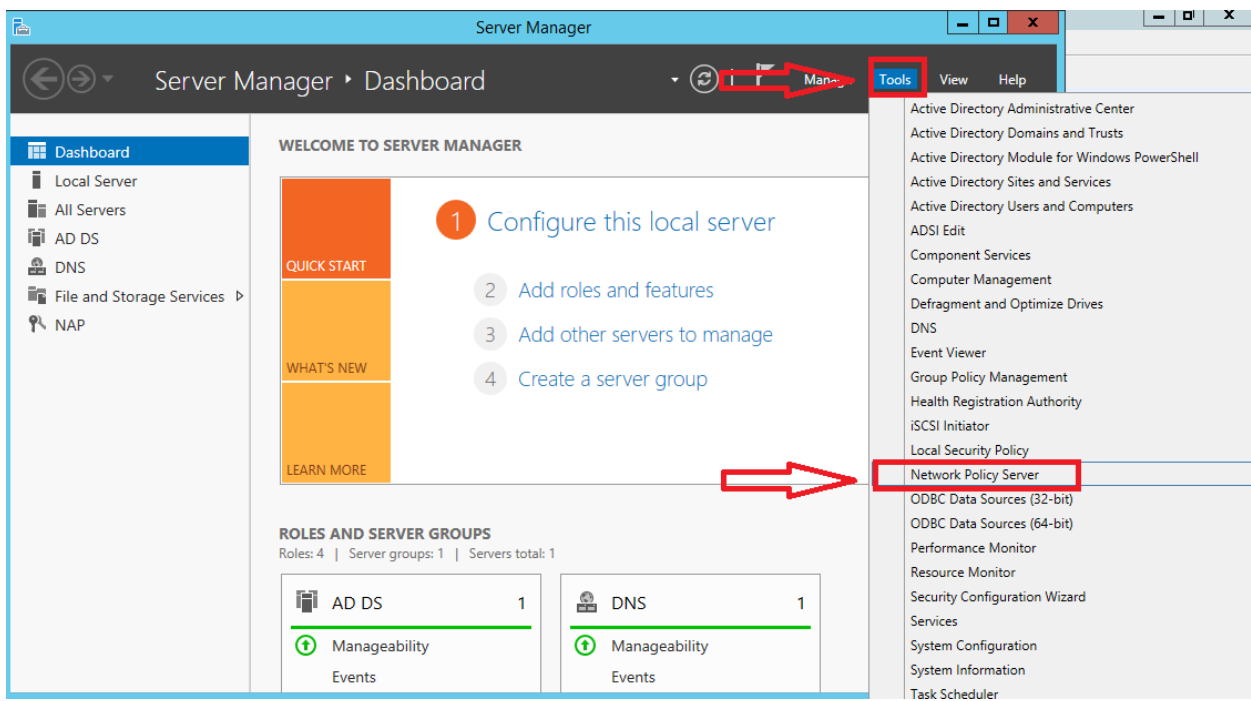


- **Bước 3 :** Kiểm tra Token đã được tạo trên điện thoại và AuthenPoint Cloud

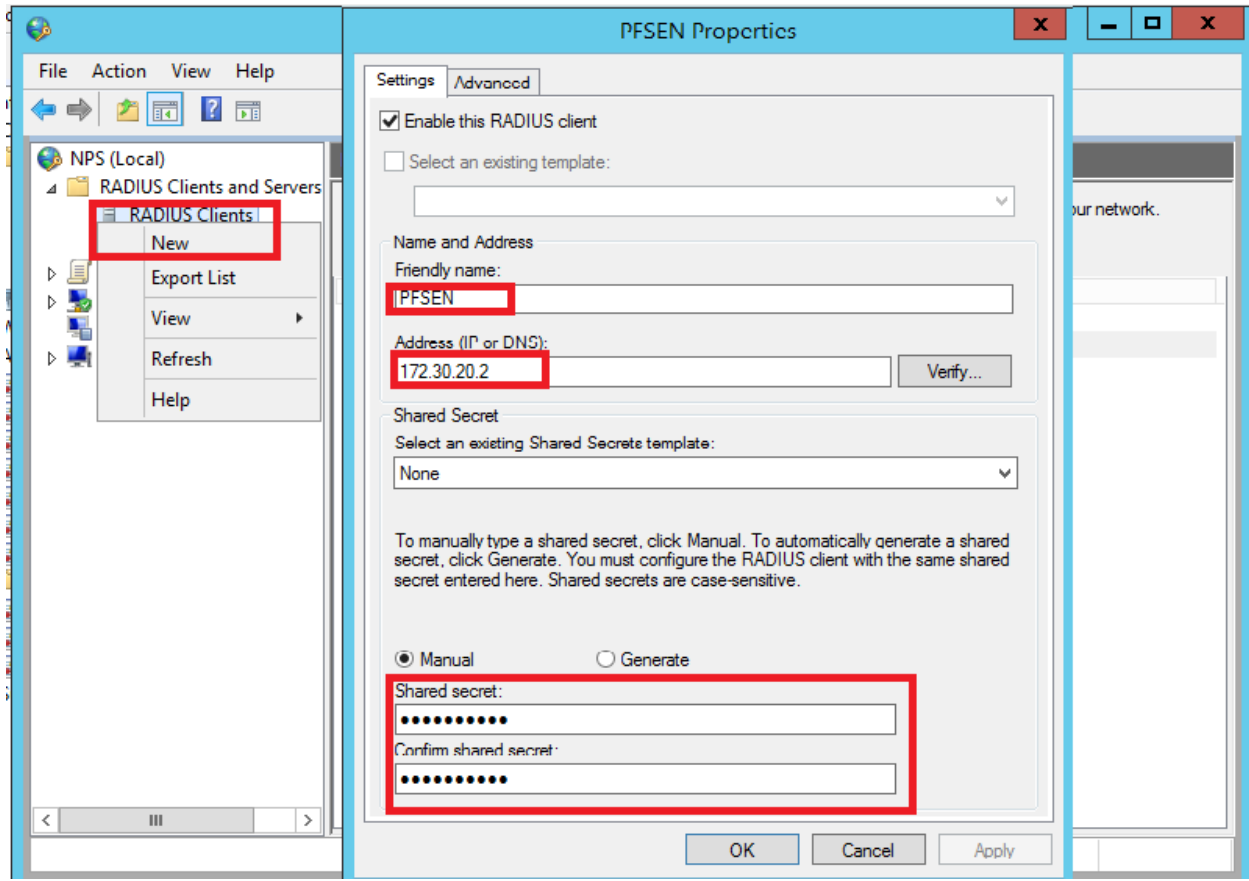


3. **Cấu hình NPS Server trên AD:**

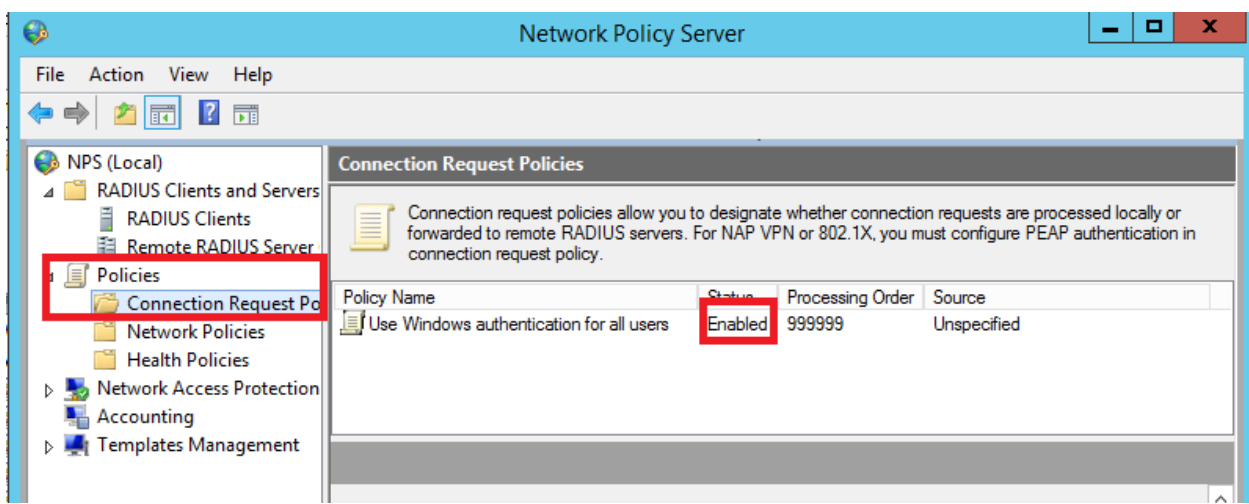
- **Bước 1 :** Trên Windows Server → Server Manager → Tool → Network Policy Server.



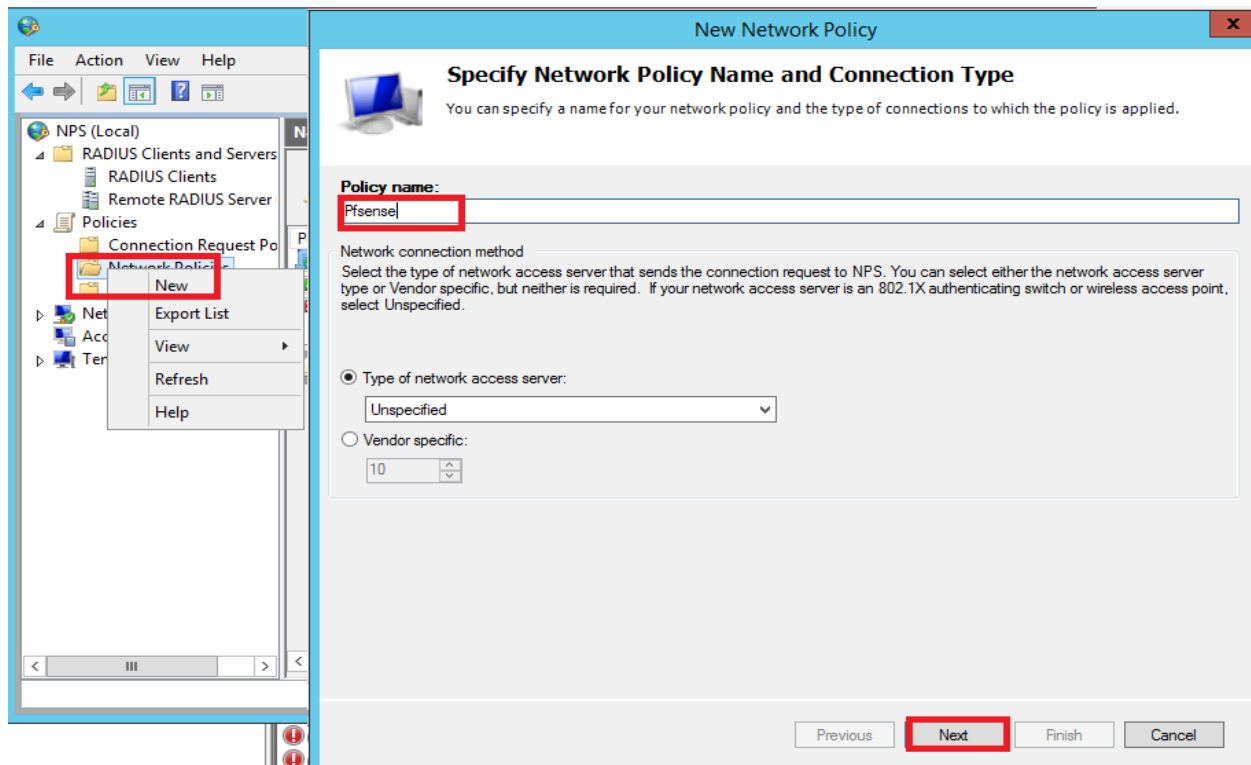
- **Bước 2 :** Chọn RADIUS Clients and Servers > RADIUS Clients > Chuột phải RADIUS Clients và chọn NEW > điền thông số như trong hình > Bấm OK.



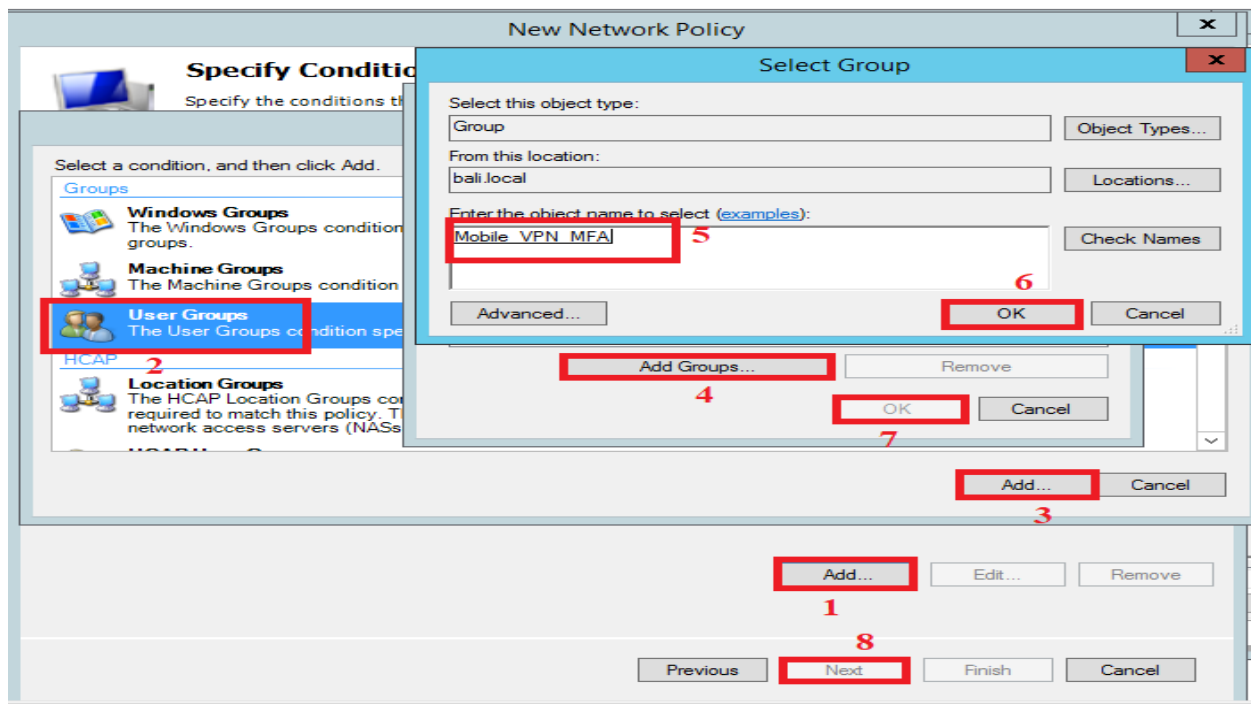
- **Bước 3 :** Chọn Policies > Connection Request Policies. Đảm bảo đã Enable.



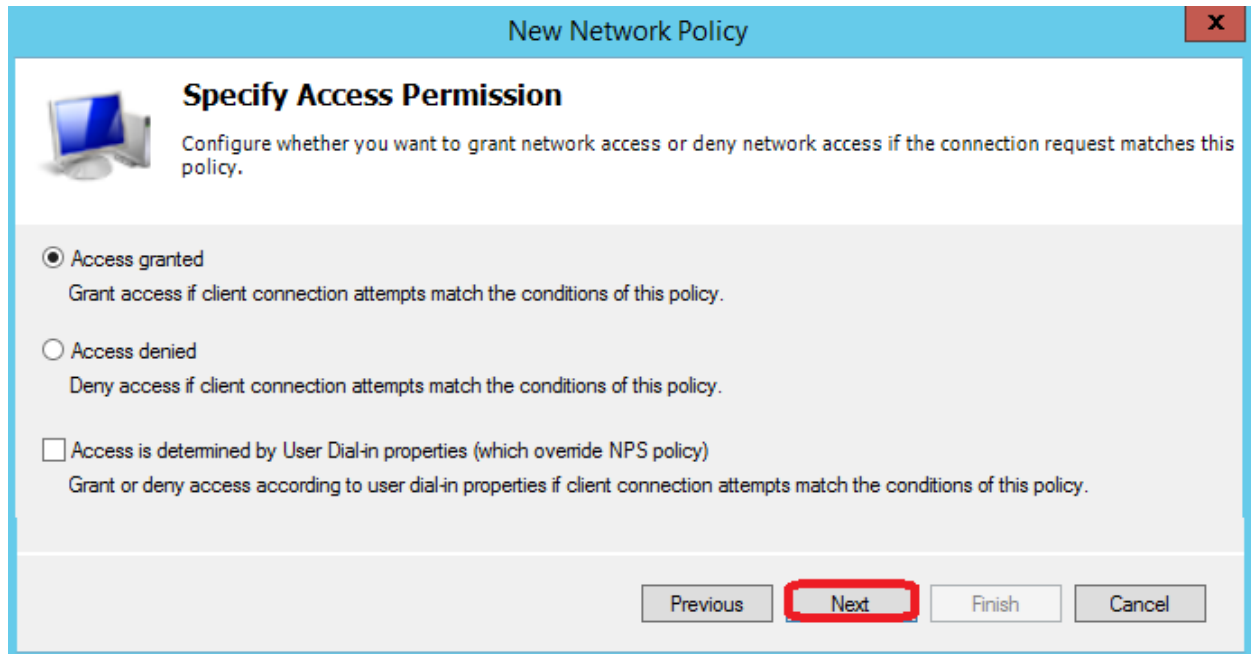
- **Bước 4 :** Chuột phải Network Policies > New > Gõ tên Policy > Next



- **Bước 5 :** Add > Chọn User Groups > Add > Add Groups > Gõ tên Group (Group này phải giống với Group trên Radius của Pfsense và AuthPoint) > OK > OK > Next



- **Bước 6 :** Next



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

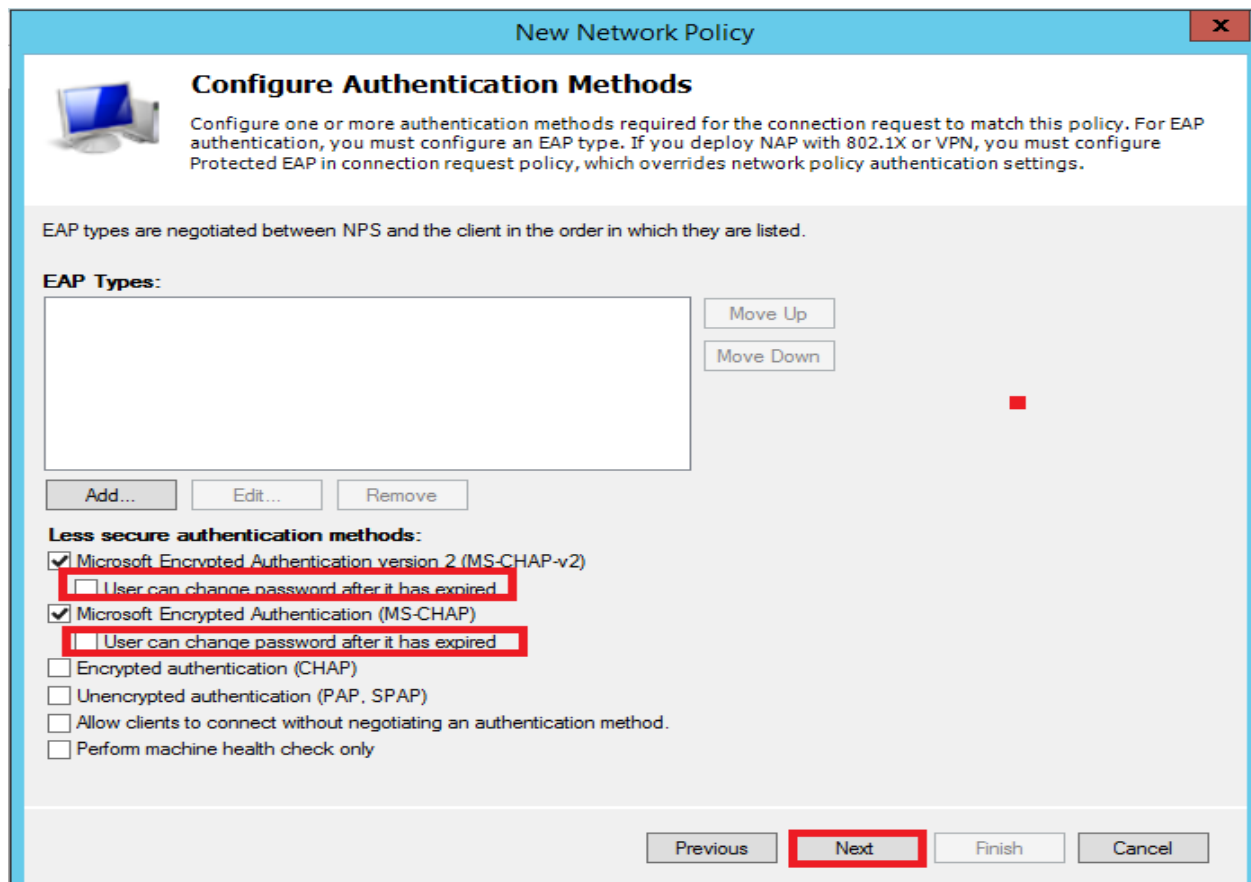
☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous **Next** Finish Cancel

- **Bước 7 :** Bỏ tích *User can change password after it has expired* > Next



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☐ User can change password after it has expired

☒ Microsoft Encrypted Authentication (MS-CHAP)
☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

Previous **Next** Finish Cancel

- **Bước 8 :** Next

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Constraints**
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

Previous **Next** Finish Cancel

- **Bước 9 :** Add > Filter-Id > Add > Add > Gõ tên Group (Group này phải giống với Group trên Radius của Pfsense và AuthPoint) > OK > OK > Close > Next

Attribute Information

To add an attribute to the policy, click Add. To add a custom or proprietary attribute, click Add.

Access type: All

Attributes:

- Name
- Acct-Interim-Interval
- Callback-Number
- Class
- Filter-Id**
- Framed-AppleTalk-L
- Framed-AppleTalk-M
- Framed-AppleTalk-S

Description: Specifies the name of filter list

Attribute name: Filter-Id

Attribute number: 11

Attribute format: Octet String

Enter the attribute value in:

☒ String

☐ Hexadecimal

Mobile_VPN_MFA

OK Cancel

Add... Edit... Remove Move Up Move Down

Add... Close

Previous **Next** Finish Cancel

- **Bước 10** : Finish

Policy conditions:

Condition	Value
User Groups	BALI\Mobile_VPN_MFA

Policy settings:

Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v2
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

Previous Next **Finish** Cancel

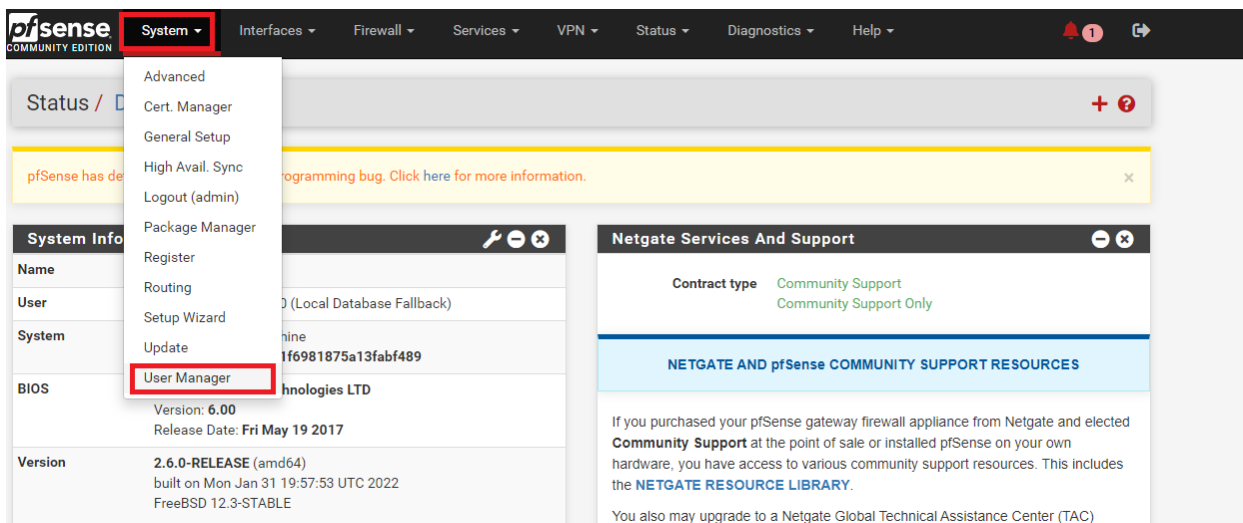
- **Bước 11** : Chuột phải NPS (Local) và chọn Register server in Active Directory > OK > OK



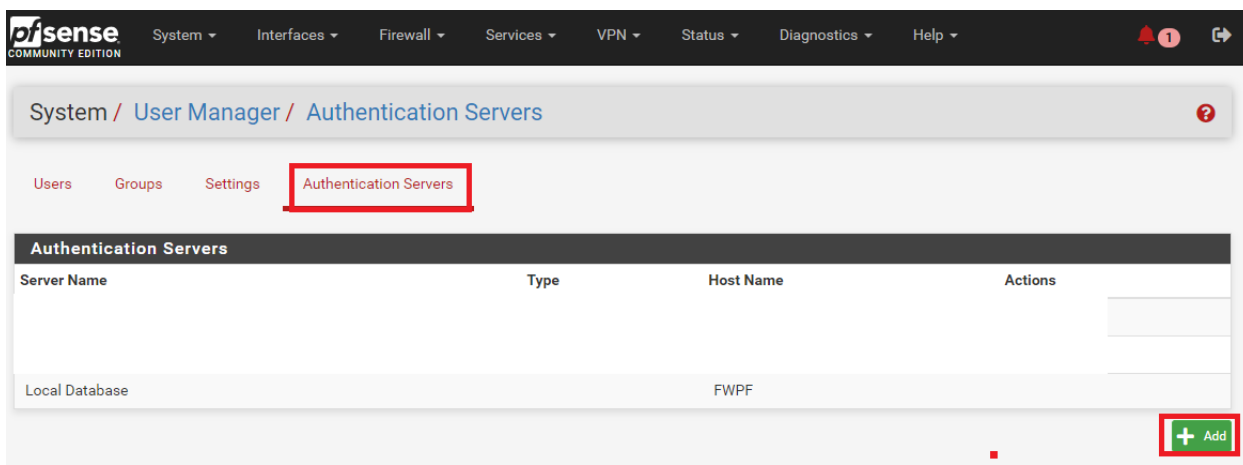
4. Cấu hình Pfsense OpenVPN – RADIUS

4.1. Cấu hình RADIUS Authentication Server

- **Bước 1 :** System → User Manager



- **Bước 2 :** Authentication Servers → Add.



- Server Settings

Descriptive name

Radius_Mobile_VPN_MFA

Type

RADIUS

Chọn Radius

RADIUS Server Settings

Protocol

MS-CHAPv2

Hostname or IP address

172.30.20.2

IP của thiết bị đã cài AuthPoint Gateway

Shared Secret

.....

Services offered

Authentication and Accounting

Authentication port

18121

Phải cùng port với AuthPoint đã cấu hình ở bước 2 phần 2.5

Accounting port

1813

Authentication Timeout

5

This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP Attribute

LAN - 172.30.20.1

Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Save

- **Bước 1** : System → Certificate Manager → CAs. → Add → Configure.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate Manager / CAs

CAs Certificates Certificate Revocation

Search

Search term Both ▾ Search Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
<div> <div>+</div> <div>Add</div> </div>						

- **Bước 2 :** Đặt tên > Chọn Method như ảnh > Save

Create / Edit CA	
Descriptive name	<input type="text" value="Test VPN CA"/>
Method	<input type="text" value="Import an existing Certificate Authority"/>
Trust Store	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.
Existing Certificate Authority	
Certificate data	<pre>-----BEGIN CERTIFICATE----- MIIEQTCCAymgAwIBAgIIM0UYJps4SoEwDQYJKoZIhvcNAQELBQAwbz EUMBIGA1UE AxMLeW50ZXJ0YyYwY2E5CzA3BgtNBAYTA1ZOMQswCQYDVQIQIEwJDDQ ENMAsGA1UE -----</pre> <p>Paste a certificate in X.509 PEM format here.</p>
Certificate Private Key (optional)	<pre>-----BEGIN PRIVATE KEY----- MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQDGSa HqktzpKDZR K+uCyTQEvwPAQ9XiFnC6rb0zEbbLjsfFatSIFGR+E1GoLKD4xE+kNy vI08tzOBik -----</pre> <p>Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).</p>
Next Certificate Serial	<input type="text" value="2"/> Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.
<input type="button" value="Save"/>	

4.3. Create an Internal Certificate

- **Bước 1 :** System → Certificate Manager → Certificates → Add/Sign. Chọn Certificate Type chọn Server Certificate.

Add/Sign a New Certificate	
Method	<input type="text" value="Create an internal Certificate"/>
Descriptive name	<input type="text" value="vpn-test-wg"/>
Internal Certificate	
Certificate authority	<input type="text" value="Test VPN CA"/> Chọn Certificate Authority đã tạo trước đó
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	<input type="text" value="sha256"/> The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.
Certificate Attributes	
Lifetime (days)	<input type="text" value="3650"/> The length of time the signed Server certificates should not
Common Name	<input type="text" value="vpn-test-wg"/> The following certificate subjects
Country Code	<input type="text" value="VN"/>
State or Province	<input type="text" value="CA"/>
City	<input type="text" value="HCMC"/>
Organization	<input type="text" value="ITMAPASIA JSC"/>
Organizational Unit	<input type="text" value="ITMAPASIA JSC"/>
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed in selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.
Certificate Type	<input type="text" value="Server Certificate"/>
Alternative Names	Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions. Type: <input type="text" value="FQDN or Hostname"/> Value: <input type="text"/> Enter additional identifiers for the certificate in this list. The Common Name field is automatically populated. The signing CA may ignore or change these values.
<input type="button" value="+ Add"/>	
<input type="button" value="Save"/>	

- **Bước 2 :** Tiếp tục bấm Add/Sign.

Add/Sign a New Certificate

Method
Create an internal Certificate

Descriptive name
pfuser

Internal Certificate

Certificate authority
Test VPN CA

Key type
RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days)
3650
The length of time the signed Server certificates should not

Common Name
pfuser

Country Code
VN

State or Province
CA

City
HCMC

Organization
ITMAPASIA JSC

Organizational Unit
ITMAPASIA JSC

Certificate Type
Server Certificate

Alternative Names
FQDN or Hostname
Type
Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically populated by the signing CA may ignore or change these values.

Add
+ Add

Save

Chon Certificate Authority đã tạo trước đó

4.4. Cấu hình OpenVPN Server

- **Bước 1 :** VPN → OpenVPN → Servers → Add → Điền thông số như sau :

General Information	
Description	MFAOPENVPN <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>
Unique VPN ID	Server 1 (ovpns1)
Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	LDAP Radius_Mobile_VPN_MFA Local Database Chọn Radius đã tạo trước đó
Device mode	tun - Layer 3 Tunnel Mode <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</small>
Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN <small>The interface or Virtual IP address where OpenVPN will receive client connections.</small>
Local port	1194 <small>The port used by OpenVPN to receive client connections.</small>
Peer Certificate Authority	
Peer Certificate Authority	Test VPN CA
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
Server certificate	vpn-test-wg (Server: Yes, CA: Test VPN CA, In Use)
DH Parameter Length	2048 bit <small>Diffie-Hellman (DH) parameter set used for key exchange. i</small>
ECDH Curve	Use Default <small>The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.</small>
Data Encryption Negotiation	<input type="checkbox"/> Enable Data Encryption Negotiation <small>This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.</small>
Data Encryption Algorithms	<div> <div> <div>AES-192-CFB8 (192 bit key, 128 bit block)</div> <div>AES-192-GCM (192 bit key, 128 bit block)</div> <div>AES-192-OFB (192 bit key, 128 bit block)</div> <div>AES-256-CBC (256 bit key, 128 bit block)</div> <div>AES-256-CFB (256 bit key, 128 bit block)</div> <div>AES-256-CFB1 (256 bit key, 128 bit block)</div> <div>AES-256-CFB8 (256 bit key, 128 bit block)</div> <div>AES-256-GCM (256 bit key, 128 bit block)</div> <div>AES-256-OFB (256 bit key, 128 bit block)</div> <div>ARIA-128-CBC (128 bit key, 128 bit block)</div> </div> <div> <div>AES-256-CBC</div> </div> </div> <div> <div>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</div> <div>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</div> </div> <p>The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i</p>

Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.	
Auth digest algorithm	SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.	
Hardware Crypto	No Hardware Crypto Acceleration
Certificate Depth	One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.	
Strict User-CN Matching	<input type="checkbox"/> Enforce match When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
Client Certificate Key Usage Validation	<input checked="" type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings	
IPv4 Tunnel Network	172.31.21.0/24 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network	 This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	<input checked="" type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel
IPv6 Local network(s)	 IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent connections	 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure) Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack. Asymmetric compression allows an easier transition when connecting with older peers.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	<input type="checkbox"/> Allow communication between clients connected to this server
Duplicate Connection	<input type="checkbox"/> Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet -- One IP address per client in a common subnet <small>Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</small>
Ping settings	
Inactive	0 <small>Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.</small>
Ping method	keepalive -- Use keepalive helper to define ping configuration <small>keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows: ping = interval ping-restart = timeout*2 push ping = interval push ping-restart = timeout</small>
Interval	10
Timeout	60

Advanced Client Settings	
DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	ball.local
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	172.30.20.2
DNS Server 2	
DNS Server 3	
DNS Server 4	
Block Outside DNS	<input type="checkbox"/> Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update	<input type="checkbox"/> Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	<input type="checkbox"/> Provide an NTP server list to clients
NetBIOS enable	<input type="checkbox"/> Enable NetBIOS over TCP/IP <small>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</small>

Còn lại phía sau chúng ta để như mặc định

- **Bước 2** : Bấm Save

4.5. Cấu hình Firewall :

- **Bước 1 :** Firewall > Rules > WAN > Add. Điền thông số như ảnh

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol UDP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match WAN address Destination Address /

Destination Port Range OpenVPN (1194) OpenVPN (1194)
From Custom To Custom

- **Bước 2 :** Bấm Apply Changes

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

[Apply Changes](#)

Floating **WAN** LAN IPsec OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 UDP	*	WAN address	1194 (OpenVPN)	*	none			Add Edit Copy Delete

- **Bước 3 :** Chọn OpenVPN > Add

Firewall / Rules / OpenVPN

Floating WAN LAN IPsec **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	none			Add Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

- **Bước 4** : Chuyển Protocol sang Any rồi bấm Save

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	OpenVPN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match any Source Address /
Destination	
Destination	<input type="checkbox"/> Invert match any Destination Address /
Extra Options	

- **Bước 5** : Bấm Apply Changes

4.6. Install the OpenVPN Client Export Package

- **Bước 1** : System > Package Manager > Available Packages > Tìm openvpn-client-export > Bấm Install > Confirm

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

openvpn

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
openvpn-client-export	1.4.23_2	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.

Package Dependencies:

[openvpn-client-export-2.4.9](#)
[openvpn-2.4.9](#)
[zip-3.0_1](#)
[p7zip-16.02_2](#)

Install

- **Bước 2 :** Đợi vài phút để pfSense-pkg-openvpn-client-export hoàn tất install

System / [Package Manager](#) / [Package Installer](#)

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages **Package Installer**

Package Installation

```
[2/4] Extracting zip-3.0_1: ..... done
[3/4] Installing p7zip-16.02_2...
[3/4] Extracting p7zip-16.02_2: ..... done
[4/4] Installing pfSense-pkg-openvpn-client-export-1.4.23_2...
[4/4] Extracting pfSense-pkg-openvpn-client-export-1.4.23_2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```


- **Bước 3 :** VPN > OpenVPN > Client Export. Download profile

OpenVPN Clients

User	Certificate Name	Export
Certificate with External Auth	pfuser	<p>- Inline Configurations:</p> <p> Most Clients Android OpenVPN Connect (iOS/Android) </p> <p>- Bundled Configurations:</p> <p> Archive Config File Only </p> <p>- Current Windows Installer (2.5.2-1x01):</p> <p> 64-bit 32-bit </p> <p>- Legacy Windows Installers (2.4.11-1x01):</p> <p> 10/2016/2019 7/8/8.1/2012x2 </p> <p>- Viscosity (Mac OS X and Windows):</p> <p> Viscosity Bundle Viscosity Inline Config </p>


5. Kiểm tra kết nối OpenVPN – MFA

- Tải Profile rồi Import lên Điện Thoại và Mở phần mềm OpenVPN → Connect.



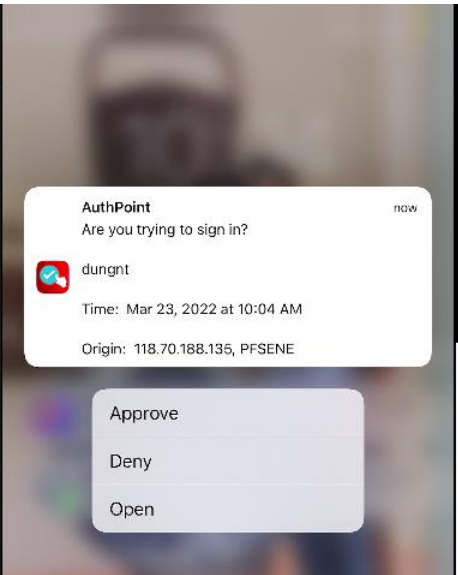
DISCONNECTED

OpenVPN Profile
118.70.188.135 [FWPF-UDP4-1194-
pfuser-ios-config]



CONNECTED

OpenVPN Profile
118.70.188.135 [FWPF-UDP4-1194-
pfuser-ios-config]



AuthPoint
Are you trying to sign in?
dungnt
Time: Mar 23, 2022 at 10:04 AM
Origin: 118.70.188.135, PFSENE

Approve
Deny
Open

DURATION
00:01:02

PACKET RECEIV
7 sec ago

YOU
dungnt

YOUR PRIVATE IP
172.31.21.2

SERVER
118.70.188.135

SERVER PUBLIC IP
118.70.188.135