|  |  |  |
| --- | --- | --- |
| **QTSC** | **HƯỚNG DẪN**  **KHAI BÁO DỊCH VỤ VPN ANYCONNECT** | **Mã số: HD.07/TTVT**  **Ngày hiệu lực: 20/09/2023**  **Số trang: 19 trang** |
| **Biên soạn** | **Xem xét** | **Phê duyệt** |
| Tên: Lê Minh Tuấn  Chức vụ: Tổ trưởng Tổ kỹ thuật mạng  Chữ ký: | Tên: Nguyễn Thanh Sơn  Chức vụ: Phó TTVT Phó TTVT  Chữ ký: | Tên: Trần Hoàng Nam  Chức vụ: Trưởng TTVT  Chữ ký: |
| **Yêu cầu/Tiêu chuẩn** | **Kiểm soát tài liệu** | **Mô tả thay đổi/lần 04** |
| Phụ lục A.1.8.5  Tiêu chuẩn ISO/IEC 27001:2022 | Nguyễn Thị Kim Bình | Cập nhật theo cơ cấu tổ chức mới của TTVT |

# MỤC ĐÍCH

Hướng dẫn này này thực hiện:

* Cấu hình cung cấp dịch vụ VPN (Client to Site).
* Thực hiện xác thực người dùng cho kết nối bên ngoài.
* Thực hiện phân tách trên mạng.
* Cách ly hệ thống nhạy cảm.
* Cho phép kết nối từ xa, làm việc trên thiết bị di động.

# PHẠM VI

Hướng dẫn này áp dụng cho dịch vụ VPN do QTSC cung cấp.

# TRÁCH NHIỆM

* Trưởng, Phó TTVT có trách nhiệm duy trì và kiểm soát việc thực hiện hướng dẫn này.
* Chuyên viên hệ thống mạng (network) có trách nhiệm thực hiện nội dung hướng dẫn này.

# ĐỊNH NGHĨA VÀ CÁC TỪ VIẾT TẮT

* VPN: Dịch vụ này cho phép khách hàng truy cập vào mạng nội bộ công ty (Intranet) bằng kết nối VPN từ bên ngoài qua Internet.
* TTVT: Trung tâm Viễn thông.
* QTSC: Công ty TNHH một thành viên Phát triển Công viên phần mềm Quang Trung.

# NỘI DUNG HƯỚNG DẪN

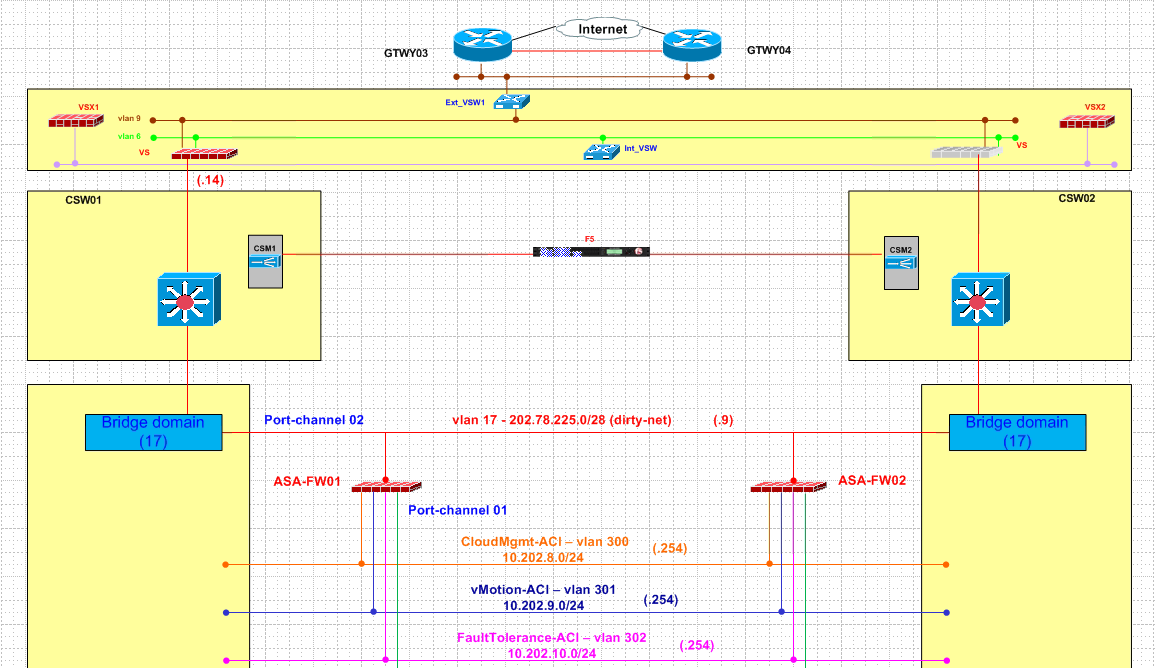
1. **Lưu đồ:**

Cấu hình AnyConnect Profile

Tạo user Syspass + LDAP

Khai báo trên Client

1. **Nội dung hướng dẫn**

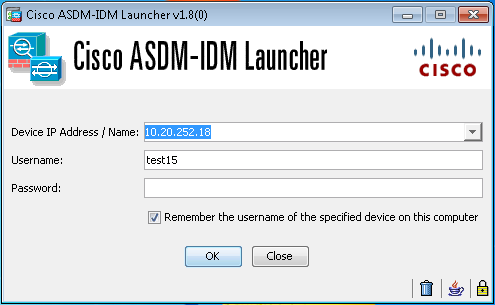


Hình – VPN access via Internet

* **CẤU HÌNH**

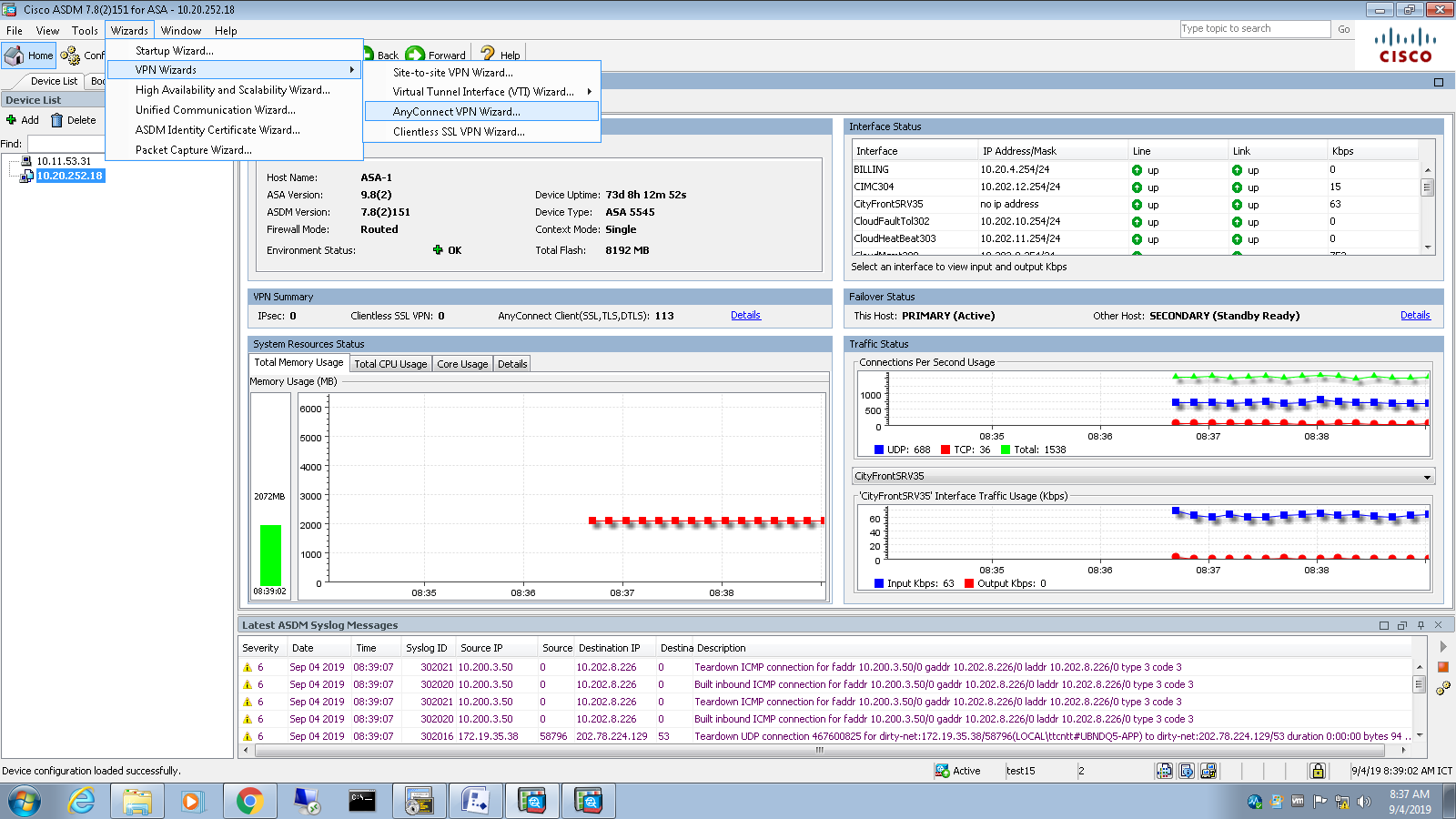
Để tạo AnyConnect Connection Profile cho khách hàng dựa trên ASDM, thực hiện các bước sau:

**Step 1** –Thực hiện đăng nhập vào Cisco ASDM**.**



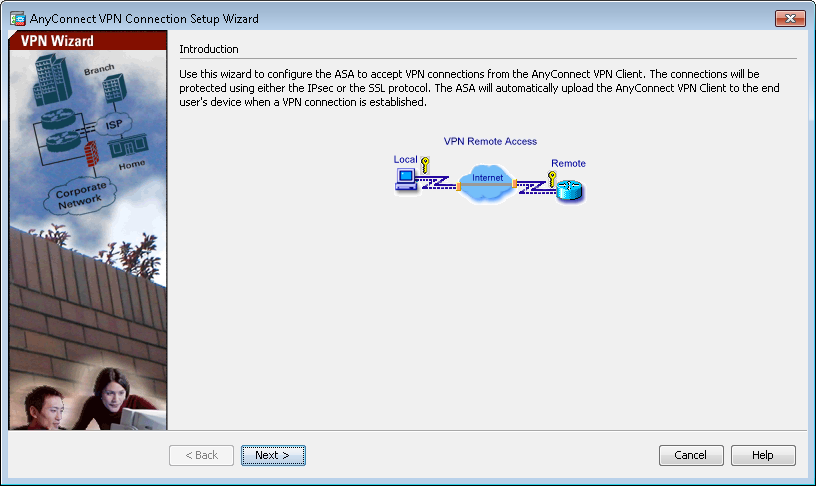
– Khai báo AnyConnect VPN Profile bằng VPN Wizard:

*+ Vào tab: Wizard>VPN Wizards>AnyConnect VPN Wizard*.



**Step 2** –Thực hiện khai báo theo Cisco ASDM wizard**.**

1. Introduction: >>Next.

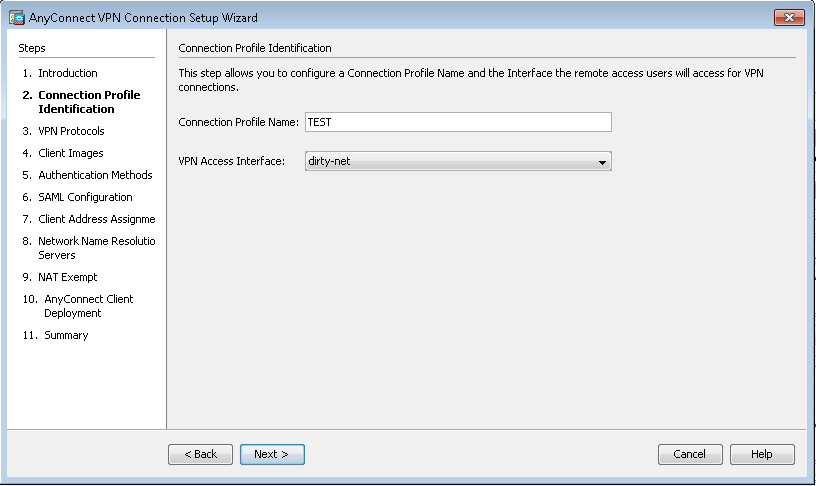


1. **Connection Profile Identification:**

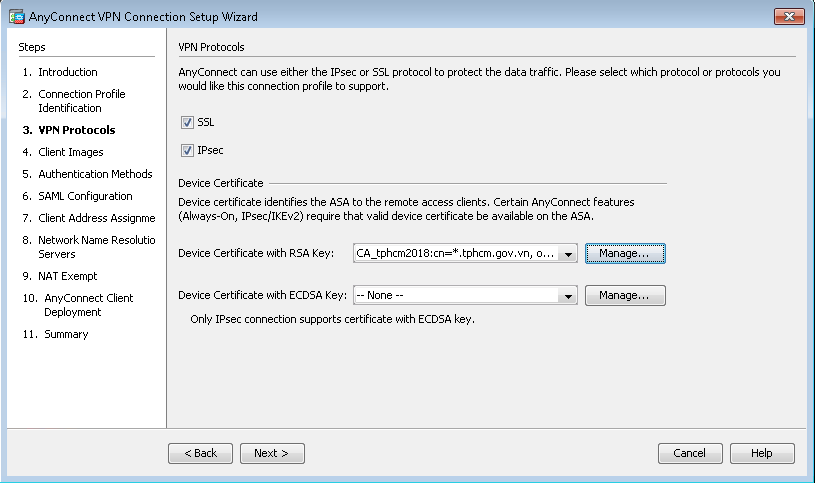
- Connection Profile Name: [TEST] tên Group VPN.

- VPN Access Interface: [dirty-net] chọn Interface mà vùng mạng Internet bên ngoài kết nối vào.

>> Next.



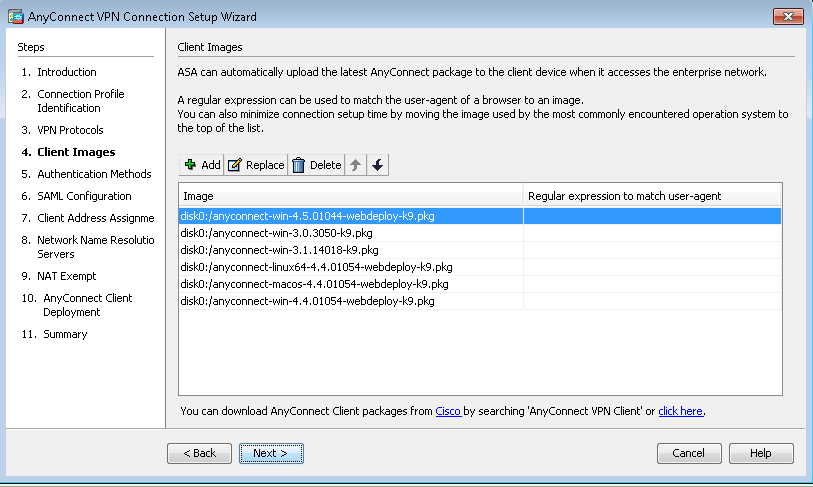
1. **VPN Protocols:** >>Next



1. **Client Images:**

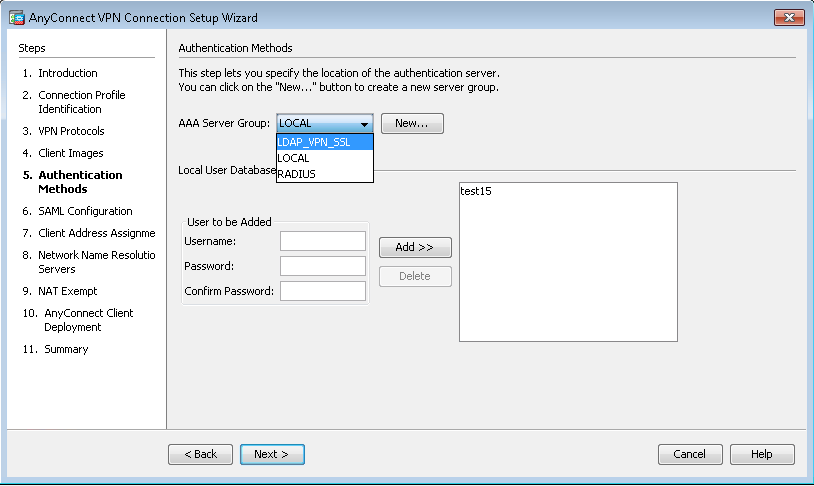
- Chọn image client cho VPN Profile**:** mặc định cho dòng đầu tiên.

**>>**Next.

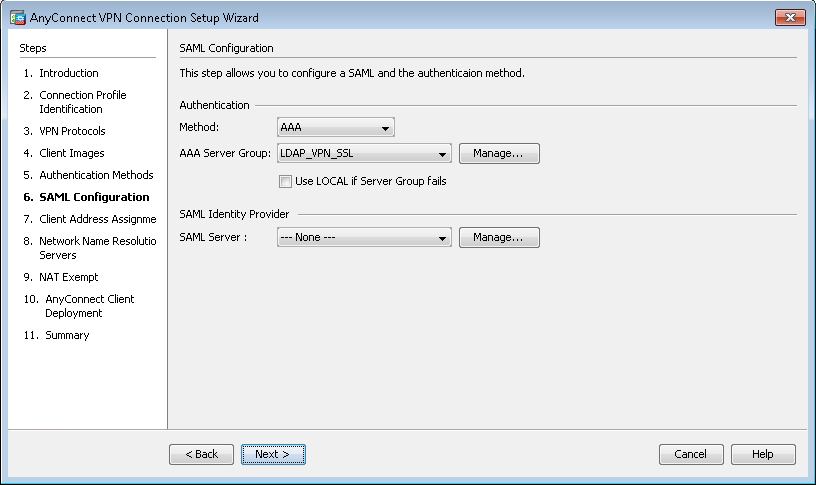


1. **Authentication Methods:** chọn phương thức xác thực giữa user và server.

* AAA Server Group: [LDAP\_VPN\_SSL] chọn xác thực theo LDAP server.
* >>Next.

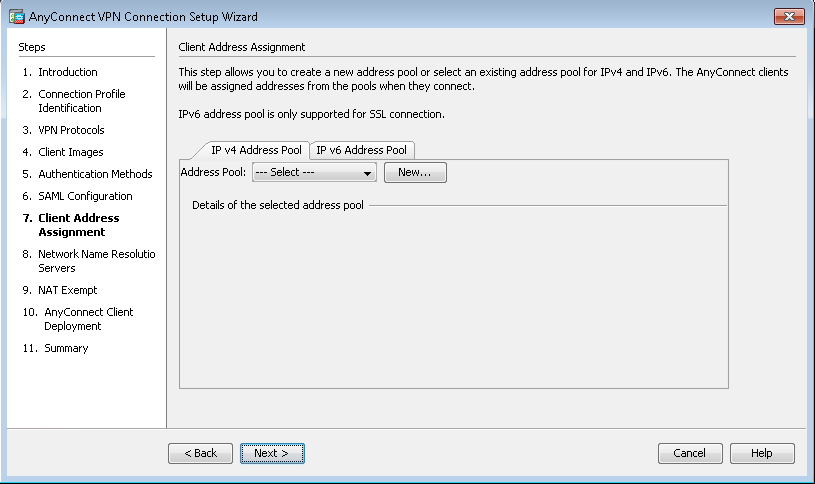


1. **SAML Configuration:** >>Next

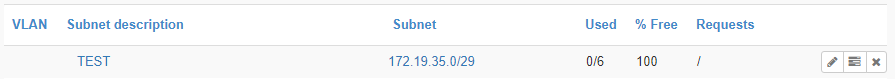


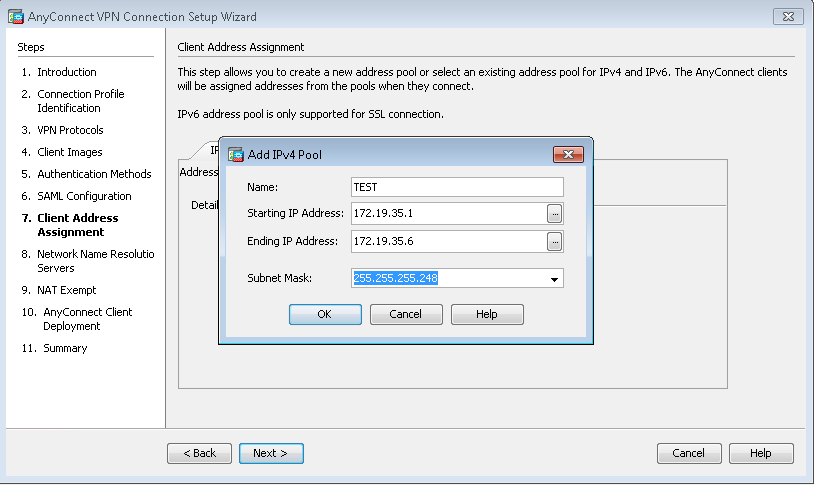
1. **Client Address Assignment:** Tạo pool IP cấp phát cho các user trong Group.

* **Tab:** >IPv4 Address Pool >New



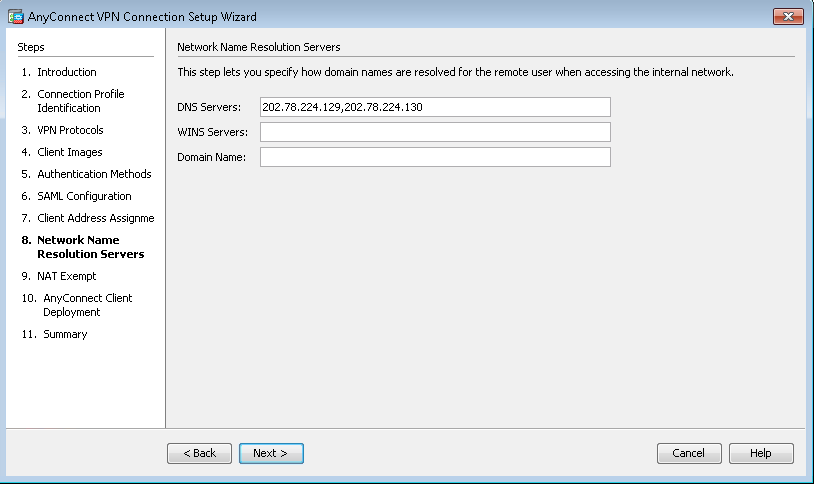
* Chuẩn bị Pool IP cần cấp phát cho Group VPN TEST.



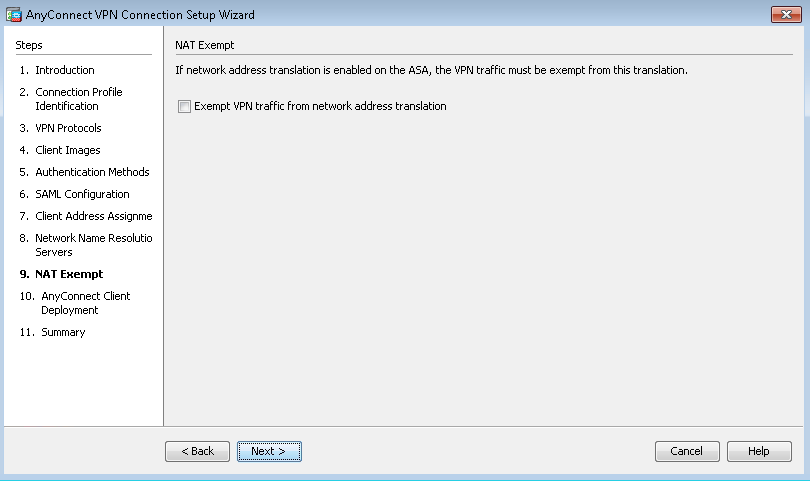


1. **Network Name Resolution Servers:** Khai báo IP DNS:

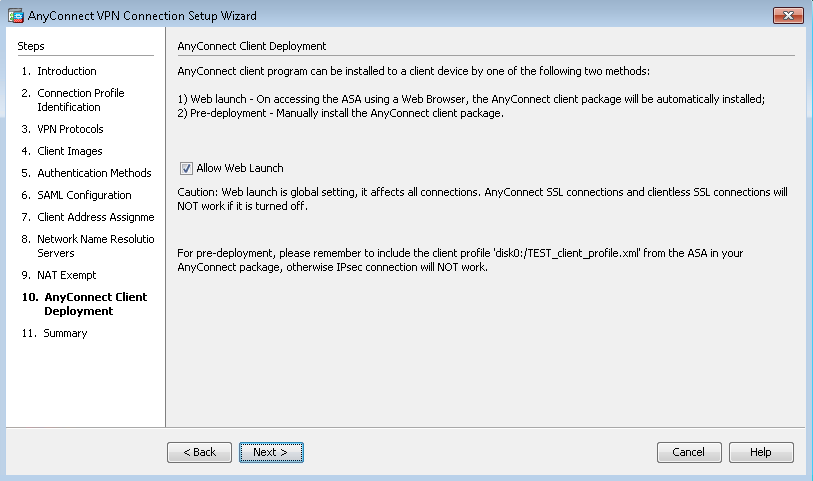
>>Next.



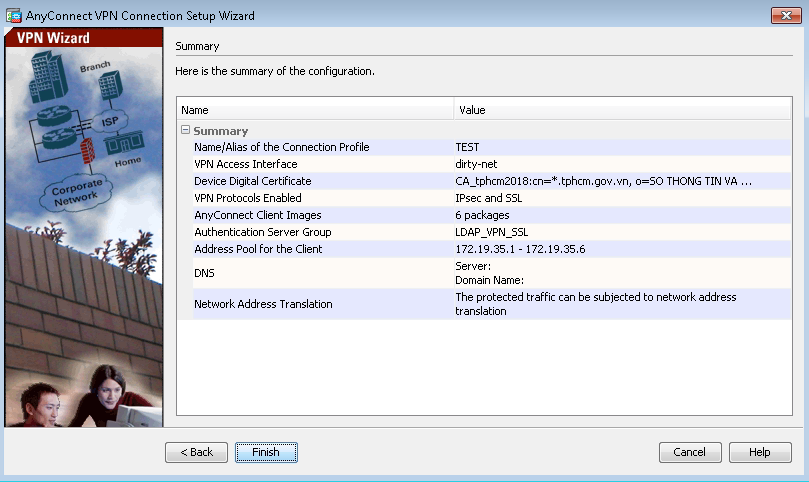
1. **NAT Exempt**: >>Next



1. **AnyConnect Client Deployment:** >>Next.



1. **Finish:**



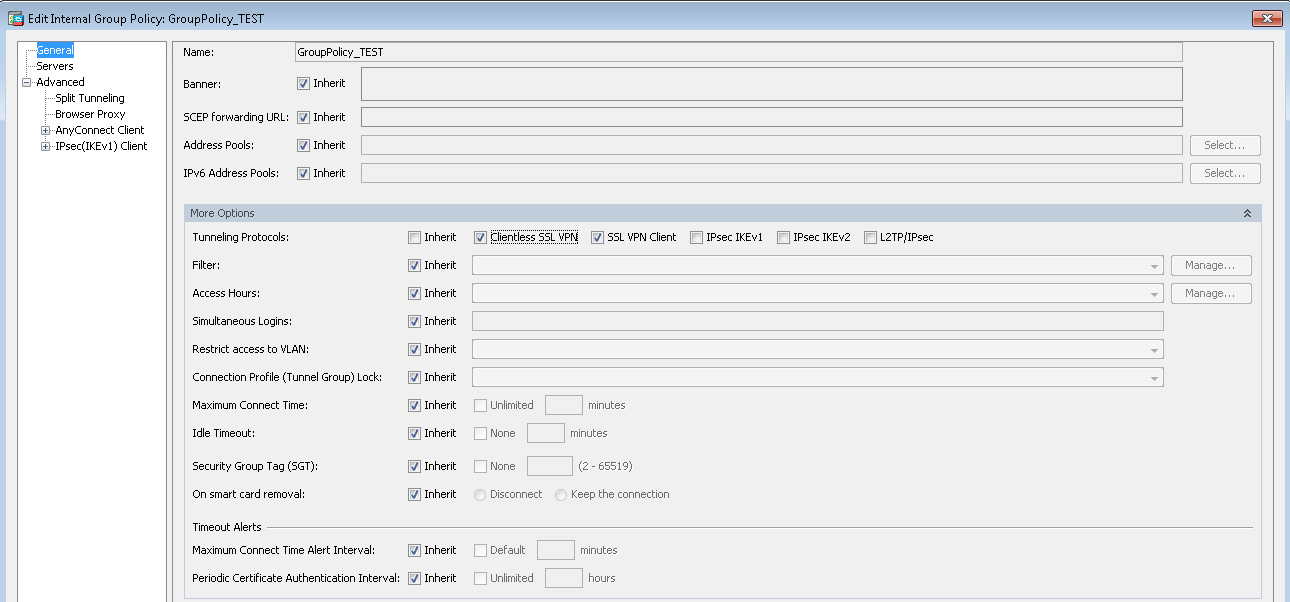
**Step 3**: Điều chỉnh các thông số về Protocols và tạo Access Control List cho phép từ Internet truy cập vào 1 vùng mạng cụ thể.

Edit Internal Group Policy

Tab: Genneral >Tunneling Protocols:

🗹 Clientless SSL VPN

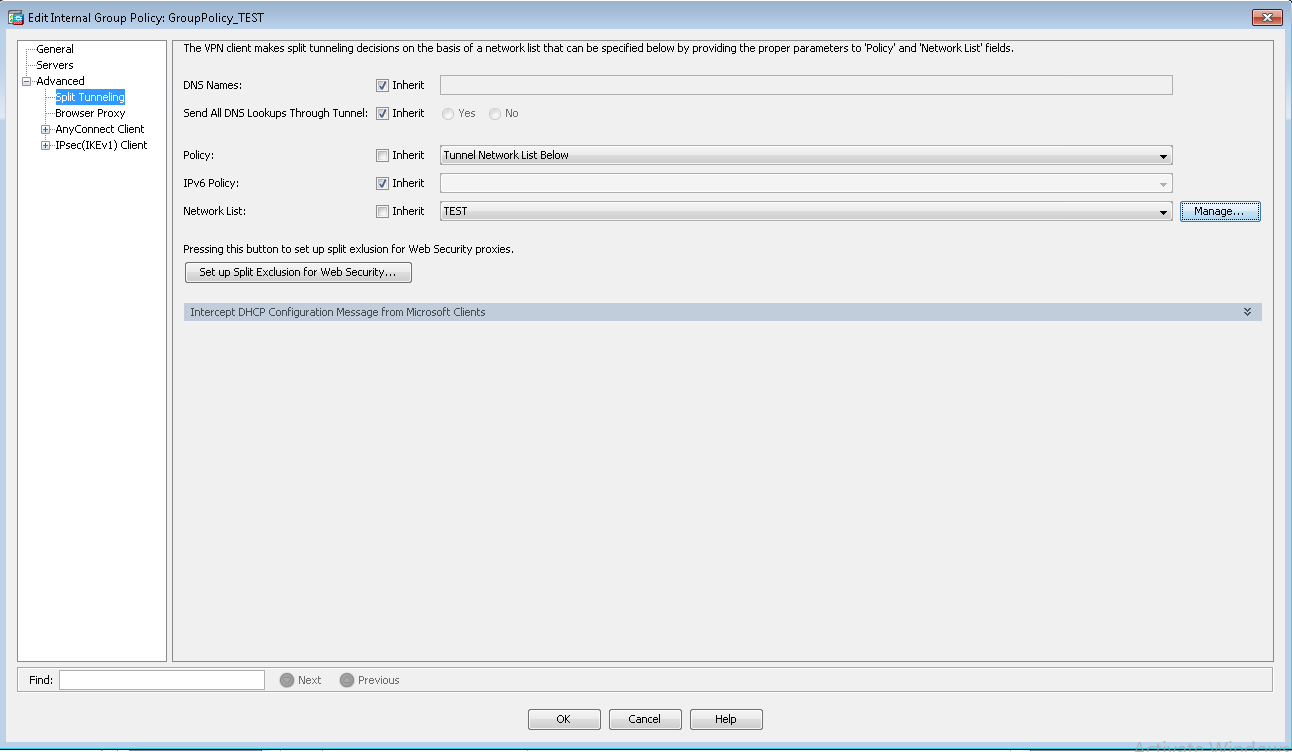
🗹 SSL VPN Client.



Tab: Advanced >Splipt Tunneling

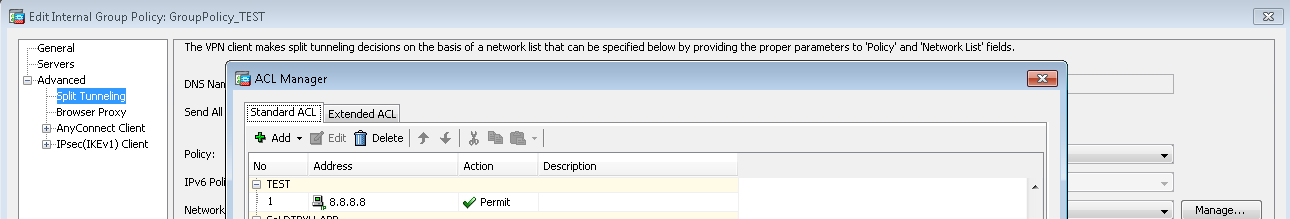
Policy: chọn Tunnel Network List Below.

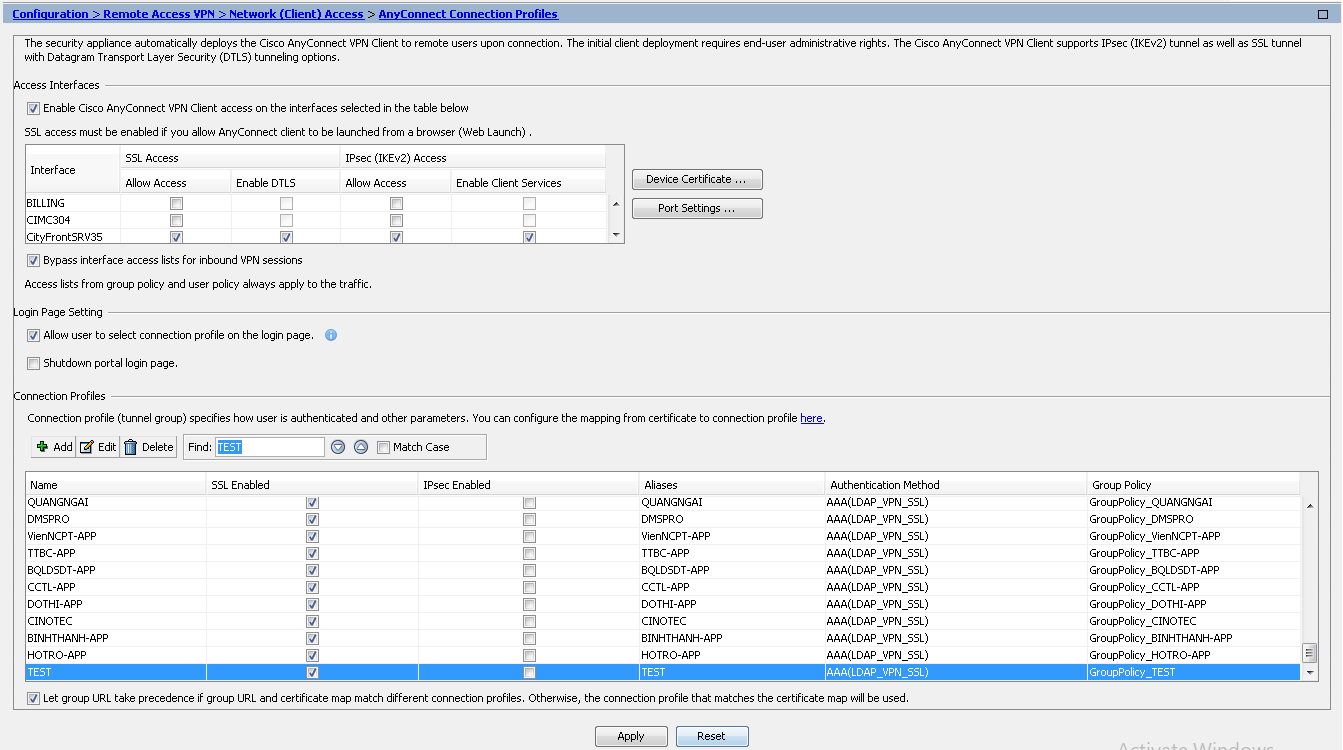
Network List: TEST



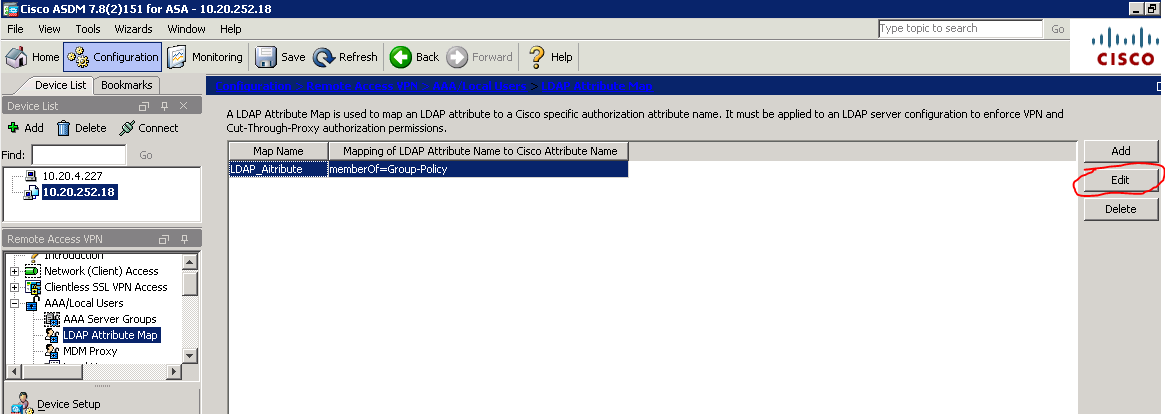
Network List: định nghĩa vùng mạng đích hoặc host đích mà vùng mạng VPN muốn đến. Bằng cách tạo một Standard ACL.

>Manage >Standard ACL > ACL.

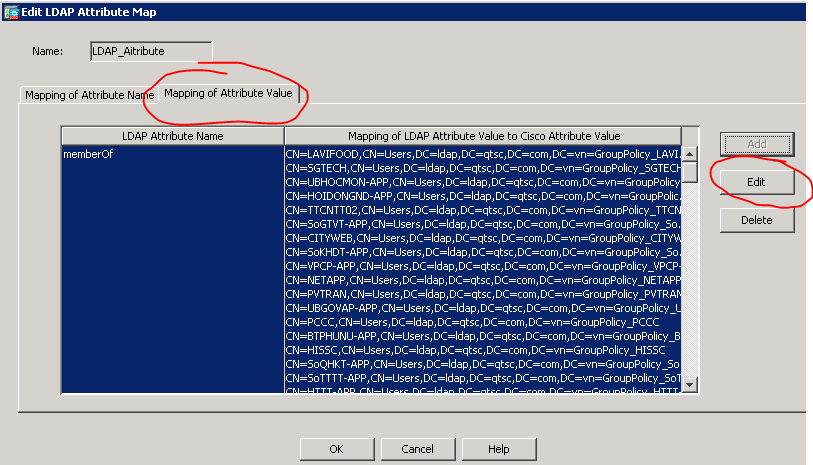


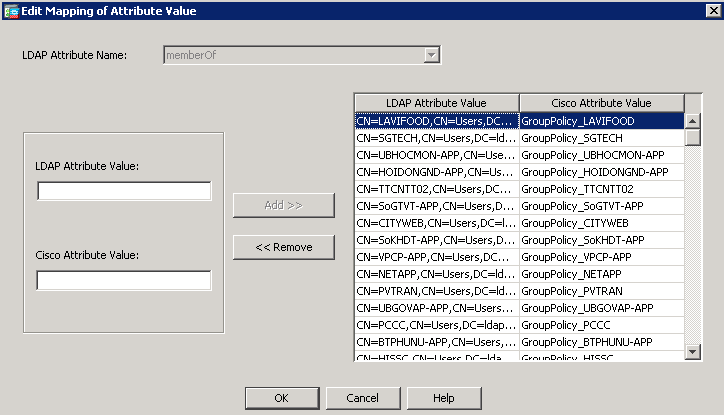


* Chọn LDAP Attribute theo đường dẫn, chọn Edit

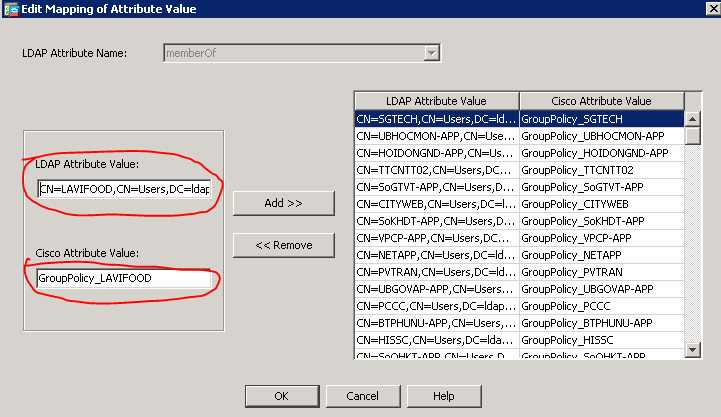


* Chọn tab Mapping of Attibute Value, chọn Edit

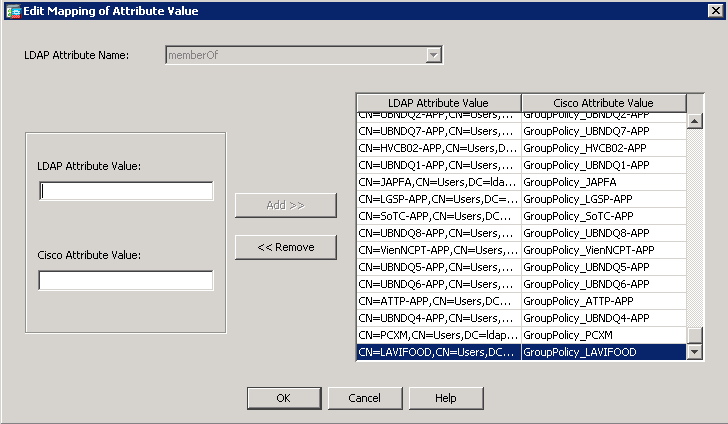


***Thao tác từ đây phải tuyệt đối chính xác*** 

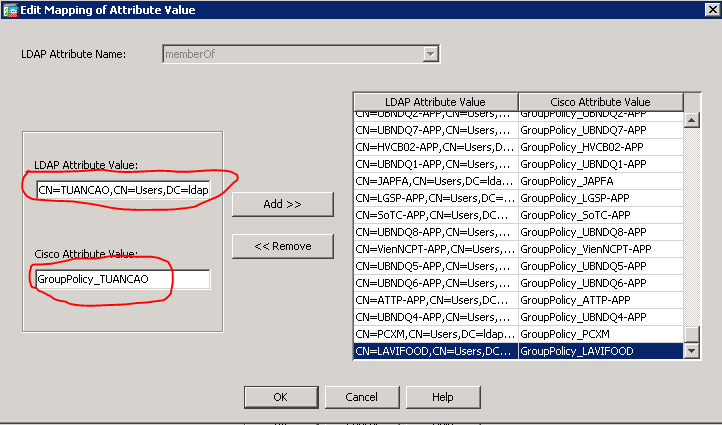
* Chọn arttribute đầu tiên (hình ví dụ là LAVIFOOD), chọn Remove để copy nội dung attribute.



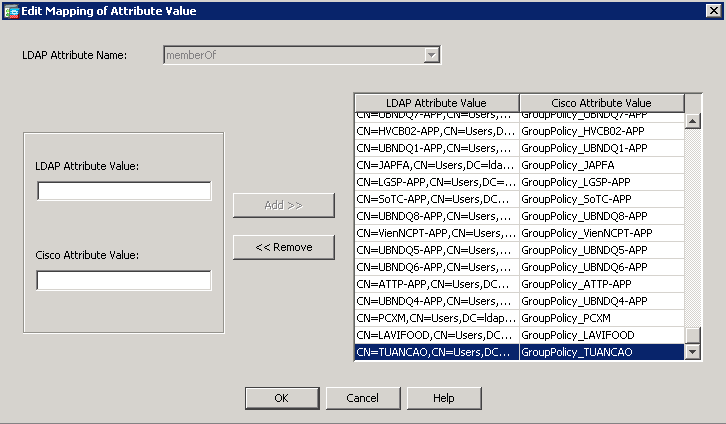
* Sau khi copy thông số attribute, chọn Add >> để trả attribute LAVIFOOD về lại bảng map.



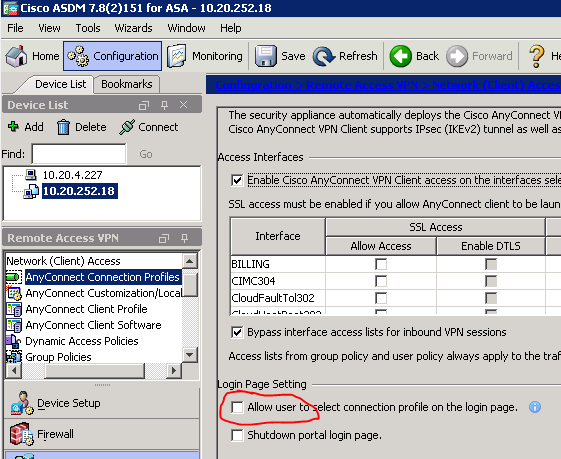
* Paste attribute, sửa lại CN theo đúng tên profile ở bước 1 và sửa tên GroupPolicy\_NAME



* Chọn Add >>, sẽ cho kết quả như hình. OK để hoàn tất việc Mapping attribute.



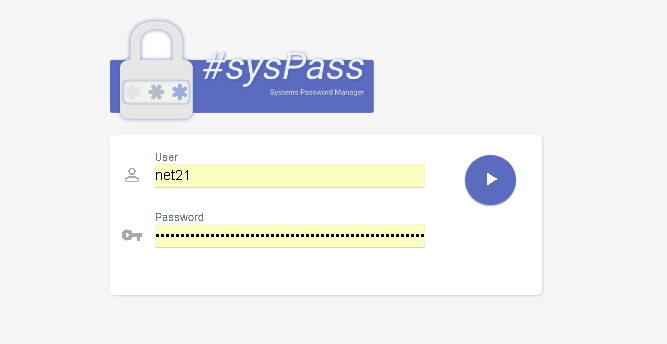
* Đảm bảo không tick như hình trước khi thoát ASDM (ASA tự tick mỗi lần create/edit config)



>>APPLY

**Step 4** Tạo user trong Syspass và khai báo vào LDAP server

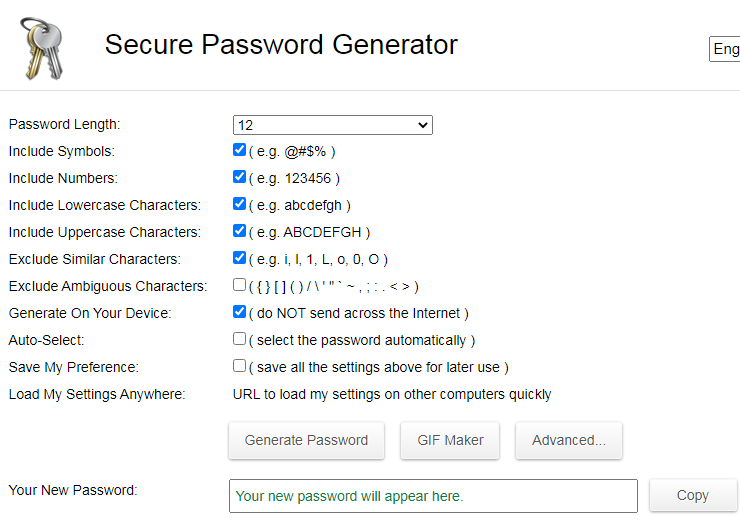
1. Tạo user trong Syspass:



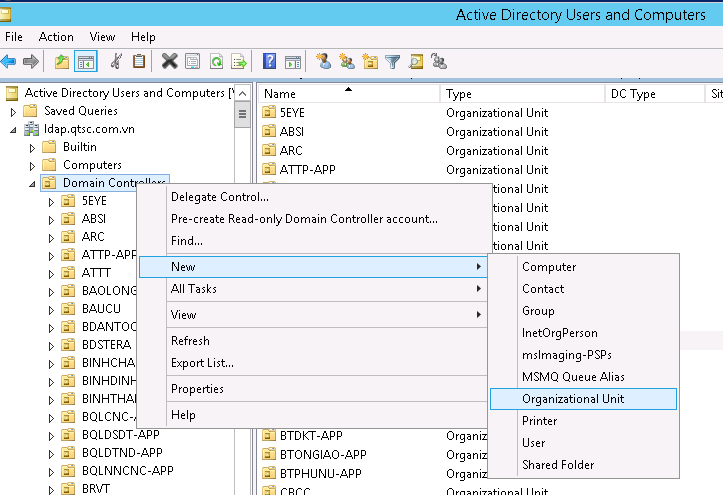




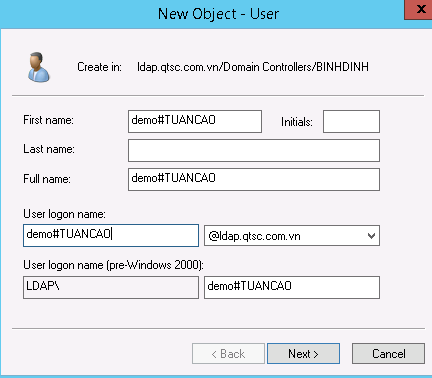
1. Khai báo thông tin user vừa chuyển vào LDAP server:
2. Rdp vào LDAP 10.20.3.47:9289
3. Truy cập <https://passwordsgenerator.net/> , chọn stick như hướng dẫn để tạo pass



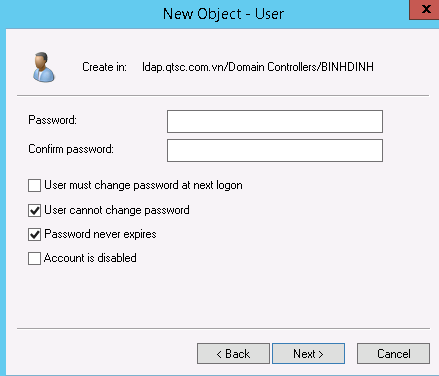
1. Tạo mới OU tại OU Domain Controllers như hình



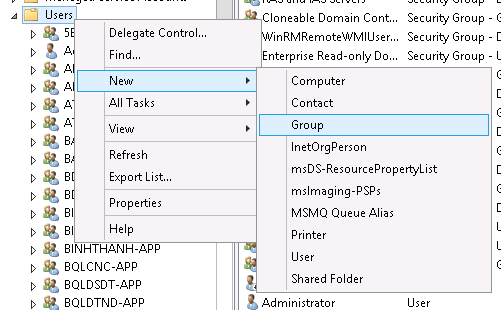
1. Tạo mới user trong OU vừa tạo.



1. Stick như hướng dẫn, dán password đã copy vào.



1. Tạo mới Group tại container Users theo đúng tên profile vừa tạo. (ASA sẽ tìm tên group này theo CN vừa add mới trong LDAP Attribute)



1. Add User vào Group vừa tạo.

**Step 5** Hướng dẫn khai báo tại thiết bị người dùng:

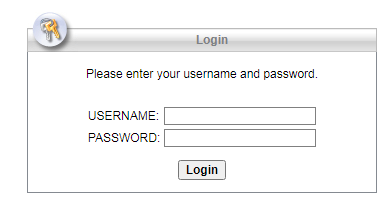
a) Cấu hình yêu cầu cho client:

Các thông số cần kiểm tra:

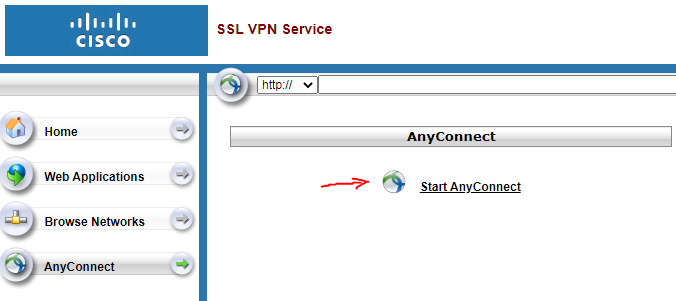
* CPU: Pentium ® (tối thiểu)
* Hệ điều hành: Windows 7 trở lên.
* Ổ cứng còn trống: 20MB.
* Ram: Tối thiểu 2G cho tất cà các hệ điều hành.

b) Cài đặt:

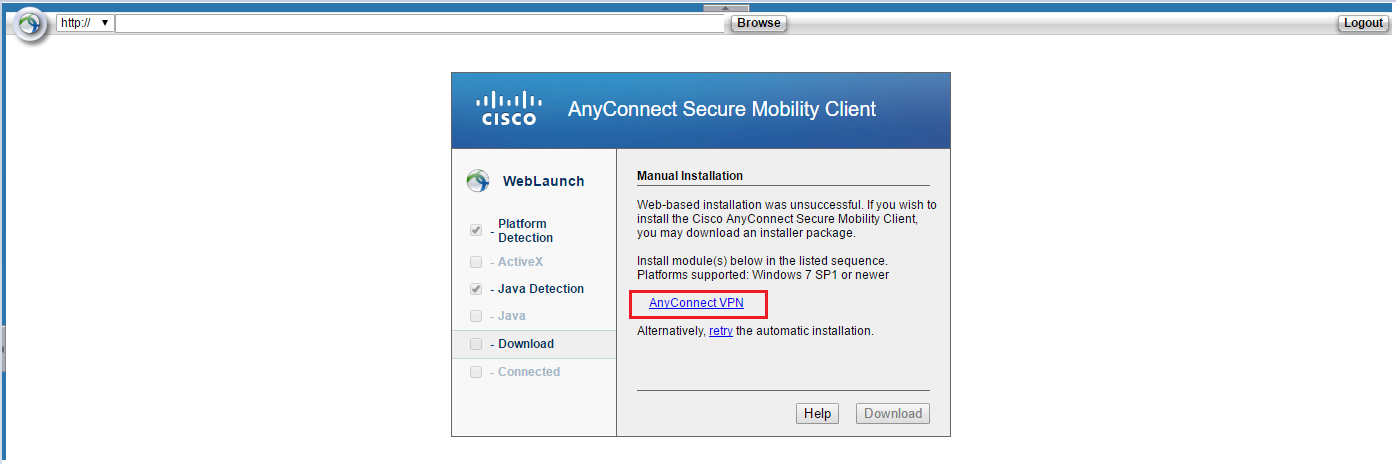
**b.1:** Truy cập link <https://vpn.tphcm.gov.vn> đang nhập với user và password đã được cấp.



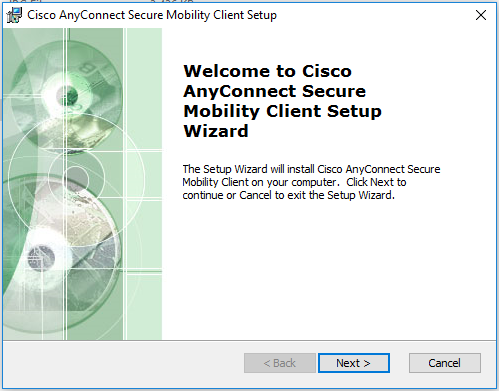
* Chọn chương trình AnyConnect

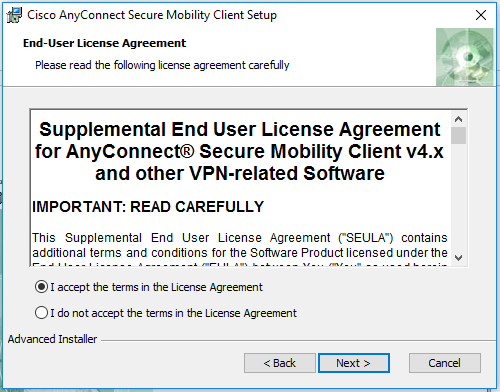


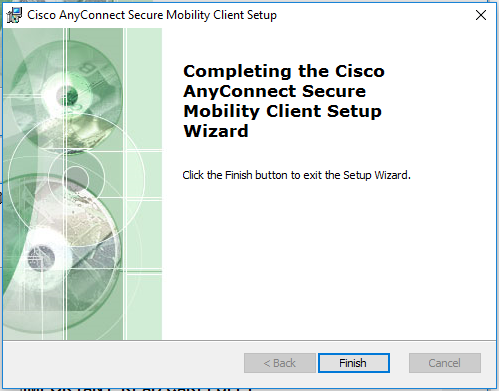
* Tại thời điểm này, hệ thống sẽ tự động kiểm tra hệ điều hành của client và đề xuất phiên bản phù hợp tốt nhất cho người dùng 🡪 Chọn AnyConnectVPN để tải phần mềm về máy.



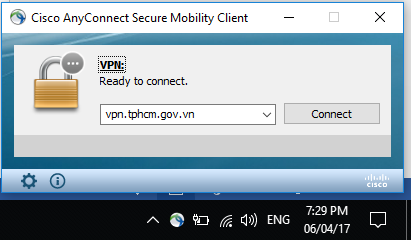
**b.2**: Tiến hành cài đặt phần mềm vào máy.



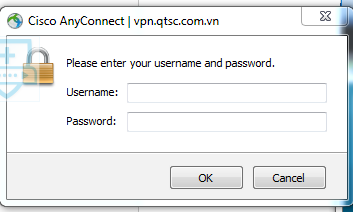




* Sau khi quá trình cài đặt đã thành công, ta tiến hành chạy chương trình và nhập domain vpn.tphcm.gov.vn vào góc dưới bên phải màn hình và chọn Connect.



* Đăng nhập với User và Password đã được cấp vào khung bên dưới.



* Sau khi kết nối thành công góc dưới bên trái màn hình sẽ hiện thông báo như sau:



# BIỂU MẪU SỬ DỤNG

Không có.

# TÀI LIỆU THAM KHẢO

* Tài liệu ISO/IEC 27001:2022.
* Tài liệu IETF RFC2246.