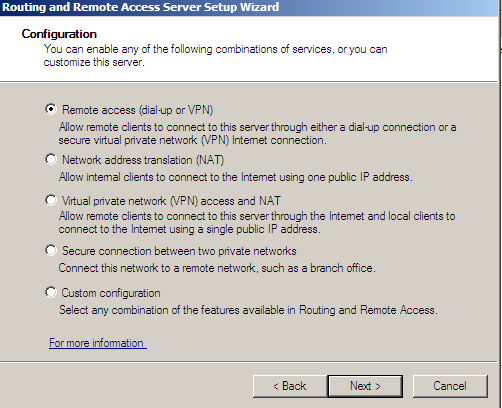
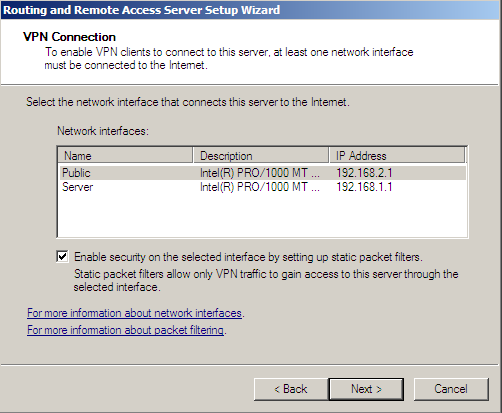
**5.Truy cập từ xa**

**5.1 Cài đặt**

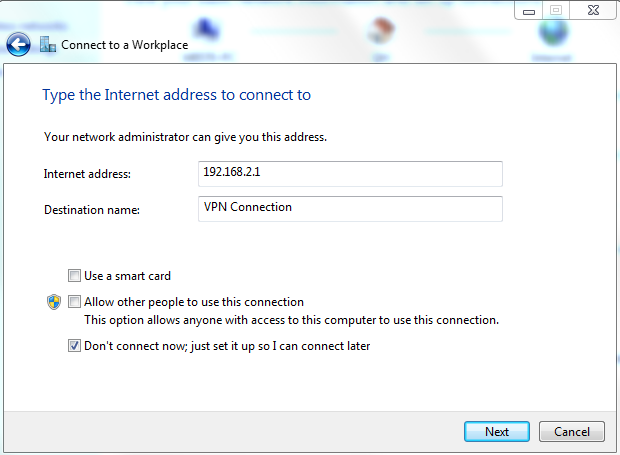
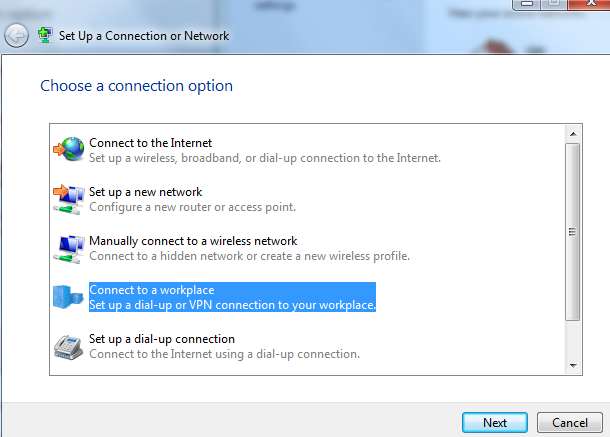
a)Windows server 2008

Để sử dụng dịch vụ truy cập từ xa trong windows server, thông thường ta sử dụng mạng riêng ảo VPN (Virtual Private Networks). Dịch vụ VPN được cung cấp thông qua dịch vụ truy nhập từ xa và định tuyến RRAS (Routing and Remote Access Services). Trên máy chạy windows server, truy cập vào “Server Manager” → “Add Roles” → tích chọn “Network Policy and Access Services” → tích vào ‘Routing and Remote Access Services” và cài đặt

Tiếp theo, người quản trị cần cài đặt cấu hình cho máy chủ RRAS. Trên máy chạy windows server vào “Server Manager” → “Routing and Remote Access” → click chuột phải chọn “Configure and Enable Routing and Remote Access” → “Remote access (dial-up or VPN) → tích chọn VPN → Lựa chọn card mạng có kết nối với mạng công cộng như mạng Internet để VPN clients có thể truy cập→ Chọn khoảng cấp địa chỉ IP hoặc để tự động → Tích vào lựa chọn không sử dụng RADIUS server và hoàn thành phần cài đặt. Sau đó, máy chủ sẽ khởi động lại dịch vụ RRAS.



Để người dùng truy cập được máy chủ thông qua VPN, người dùng cần vào “Network and Sharing Center” → “Set up a new connection or network” → “Connect to a workplace” → Use my Internet connection (VPN) → Điền địa chỉ IP cho dịch vụ VPN và tên điểm đến → Nhập user name và password mà người quản trị đã cung cấp và kết nối.



b) Ubuntu server

Để sử dụng dịch vụ truy cập từ xa, ta sẽ sử dụng phiên bản miễn phí của dịch vụ truy nhập bảo mật SSH (Secure Shell) là OpenSSH. Trên máy chủ Unbutu, người quản trị sử dụng câu lệnh để cài đặt

***sudo apt-get install openssh-server***

Sau khi cài đặt, khởi động lại bằng câu lệnh:

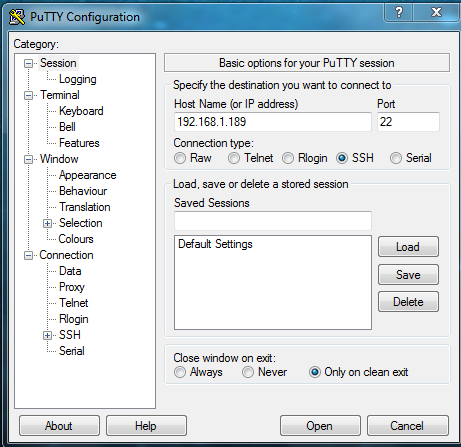
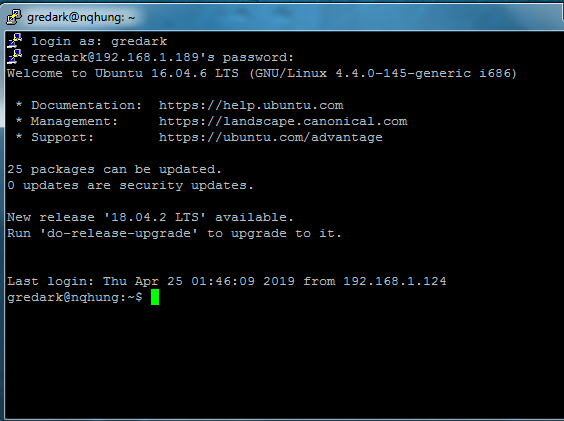
***sudo service ssh restart***

Để người dùng truy cập từ xa vào máy chủ Ubuntu server, trên máy chạy linux, người dùng sử dụng câu lệnh

**sudo apt-get install openssh-client**

Sau đó sử dụng câu lệnh sau để kết nối:

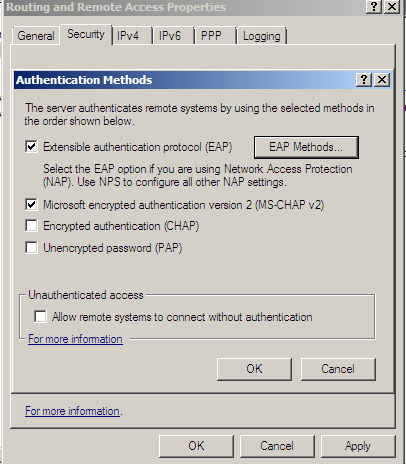
***ssh tên\_người\_dùng@máy\_chủ\_SSH***

Còn trên máy chạy windows, ta sử dụng phần mềm PuTTY. Người dùng điền địa chỉ IP của máy chủ Ubuntu, cổng mặc định sẽ là 22 và ấn Open. Màn hình đăng nhập hiện lên để người dùng nhập tên người dùng và mật khẩu của tài khoản trên máy chủ Ubuntu.

**5.2 Quản trị**

a) Windows Server 2008

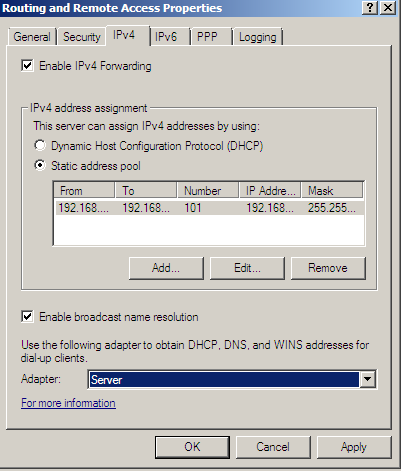
Trên máy chủ đã cài dịch vụ RRAS, vào “Server Manager” → click chuột phải trong phần “Routing and Remote Acces” chọn “Properties”.

-**Security**: người quản trị có thể chọn phương thức xác thực cho kết nối VPN. Windows Server 2008 cung cấp 4 phương thức xác nhận:

+Extensible authentication protocol (EAP): cho phép người dùng xác thực qua smart card hoặc digital certificates.

+Microsoft encryted authentication version 2 ( MS-CHAP v2): phương thức này cung cấp xác thực tương hỗ và cho phép mã hóa cả dữ liệu xác thực và dữ liệu kết nối.

+Encryted authentication (CHAP): phương thức này mã hóa dữ liệu xác thực bằng MD5 hashing.

+Unencrypted password (PAP) : khi sử dụng phương thức này, dữ liệu xác minh sẽ không được mã hóa mà truyền thẳng qua mạng ở dạng bản rõ.

-**IPv4:** cho phép người quản trị chỉ rõ dải địa chỉ mà người dùng có thể được gán thông qua

+Dynamic Host Configuration Protocol (DHCP): sử dụng DHCP server để tự động gán địa chỉ cho người dùng

+Static address pool: gán một khoảng địa chỉ IP tĩnh mà người quản trị muốn gán cho người dùng

b) Ubuntu server

Trên máy chủ Ubuntu, thông tin cấu hình được lưu trong file ***/etc/ssh/sshd\_config***. Để sửa đổi thông tin cấu hình, người quản trị sử dụng câu lệnh

***sudo nano /etc/ssh/sshd\_config***

Trong file cấu hình, người quản trị có thể thay đổi một số tham số tiêu biểu sau:

-Cổng mà SSH server sử dung: *Port 20*

-Hoạt động trên địa chỉ: *ListenAddress 192.168.1.189*

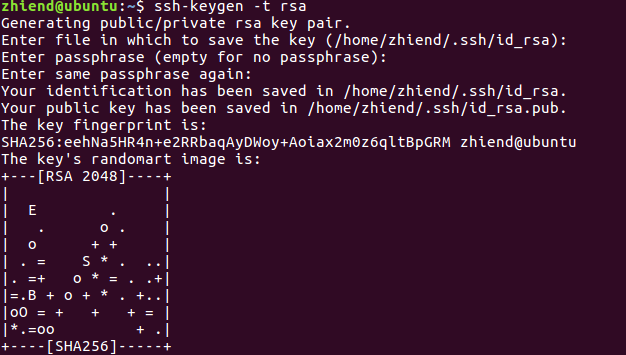
-Áp dụng xác thực RSA: *RSAAuthentication yes*

-Áp dụng xác thực mã khóa công khai: *PubkeyAuthentication yes*

-Hiện thông báo trong file issue.net khi đăng nhập: *Banner /etc/issue.net*

-Cho phép người dùng sử dụng SSH: *AllowUser tên\_người\_dùng*

-Cấm người dùng sử dụng SSH: *DenyUsers tên\_người\_dùng*

SSH server có cung cấp **SSH key** cho phép xác thực giữa hai host mà không cần mật khẩu giúp việc đăng nhập dễ dàng và an toàn vào máy chủ Ubuntu. SSH key bao gồm khóa công khai và khóa bí mật. Để tạo 2 khóa này, người dùng sử dụng câu lệnh:

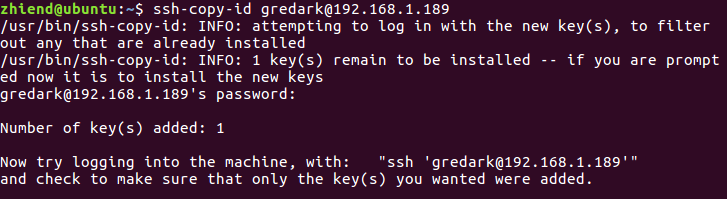
***ssh-keygen –t rsa***

Khóa công khai được lưu tại *~/.ssh/id\_rsa.pub*

còn khóa bí mật lưu tại *~/.ssh/id\_rsa*.

Để sử dụng khóa công khai trong quá trình xác thực, người dùng cần chép khóa vào máy chủ qua câu lệnh

***ssh-copy-id tên\_người\_dùng@máy\_chủ\_ssh***



Cuối cùng, kiểm tra quyền truy cập file chứa khóa xác thực ***authorized\_key***, chỉ có người dùng đã được xác thực mới có quyền đọc hoặc ghi. Nếu quyền truy nhập vào file chứa khóa xác thực chưa phù hợp thì phải cập nhật lại theo câu lệnh sau:

***chmod 600 .ssh/authorized\_keys***